AI智能体的合约账本自动化

下一代智能支付系统

Ying Willam Zhang · SCDO Laboratory · 2026 · v2



免責聲明：本書內容僅供學習與科普，不構成投資、法律或税務建議。

1、比特币（从 AI 账本与机器人说起）

SCDO Lab · 《AI智能体的合约账本自动化》· 下一代智能支付系统 · v2
全书从 **AI 智能体合约账本** 与 **机器人按次商务** 切入：先理解为何机器需要可验证账本与钥匙，再回到比特币——点对点现金与 PoW 的原点。
非投资建议。



开篇：AI Ledger、Bots，然后才是比特币

当你让一个 **AI agent** 替你调用 API、付稳定币、或把工作摘要写进账本时，它需要：

1. **自持钥匙**（谁签名谁负责）；
2. **可核对痕迹**（Agent Ledger / 合约事件）；
3. **小额结算**（HTTP 402 / x402、约 1¢ 直觉）。

这些能力不是从天而降——它们站在比特币开启的 **公开账本** + **私钥签名** + **PoW 防伪** 传统之上。本章用大白话讲比特币，作为后文 SCDO 五链、挖矿、Bots 与智能支付的地基。

SCDO Lab · Web3 新人必读指南 v2
本章用大白话讲清：比特币是什么、为什么互联网本身转不了“唯一的钱”、节点和挖矿怎么协作、钥匙与钱包、矿场与矿池。
不是投资建议。 任何涨跌幅故事都只是历史现象，不构成荐币。

开篇：先把人话说明白

比特币（Bitcoin，常写作 BTC）是一套**没有公司老板、没有总行清算中心**的数字货币系统。全世界有很多人运行同一种开源软件（节点），一起维护一份公开的交易账本——大家常说的**区块链**，在比特币里就是这条不断往后接的账本链。

你可以把它想成三件事叠在一起：

1. **一套规则**（协议与软件）：谁能记账、钱怎么转、总量怎么发。
2. **一张全球共享的账本**：转账记录公开可查，但不必绑定你的身份证姓名。
3. **一种记账奖励**：谁按规则成功打包新区块，谁就有机会拿到新发行的比特币和手续费——这就是挖矿激励。

比特币总量有规则上限（常见说法是约 **2100 万**枚），新币通过挖矿按计划进入流通，大约四年有一次“减半”，挖矿奖励变少。没有哪家央行可以一句话多印比特币；真要改规则，得说服网络里足够多的参与者——实际上极难。

下面分五块讲：双花问题、运作方式、它为何仍特殊、共识机制入门、钥匙钱包、矿场矿池。

什么是比特币?



2008 年，署名单名“中本聪”（Satoshi Nakamoto）的白皮书提出了点对点电子现金的设想；2009 年网络启动。十几年里，它经历过暴涨暴跌、分叉争论、监管风暴，也成了许多人认识区块链的第一课。

新人最该先问的不是“会不会涨”，而是：

互联网已经能传照片、传文件，为什么传“钱”以前必须找微信、支付宝、银行当中间人？比特币凭什么说自己能补上这块拼图？

互联网的“最后一块拼图”？——双花问题

网上发照片很简单：你发给我一张，你电脑里那张通常还在。传的是**副本**。

钱不行。如果我“发给”你 100 块，我这边还能继续花这 100，那就变成两个人都在花同一笔钱——这叫**双花**（double-spending）。

纯靠“复制粘贴式”的互联网传输，解决不了双花。现实生活中我们靠谁解决？靠**中介账本**：

- 你用支付宝转 100，本质是支付宝在自己的中心数据库里：我的余额 −100，你的余额 +100。
- 银行转账、银联刷卡，逻辑类似：有一个（或一组）受信任的机构说了算。

中介很有用，但也带来代价：要开户、要合规审核、可能冻结、可能服务中断、要抽手续费、数据在别人服务器上。你信任的是**机构**，不是数学和公开规则本身。

比特币要做的是：在**不依赖单一巨头账房**的前提下，让“我付你 1 个 BTC”这件事，全网最终承认**我少了、你多了**，且很难被偷偷改回去。做到这一点的底层账本技术，常被称作“价值互联网”的一块基石——这句话有点口号，但方向是对的：互联网补的是信息传输，比特币补的是**稀缺数字价值的转移**。

注意两个分寸：

- 比特币并不是“完全匿名现金”。账本公开，地址像化名；若地址和你身份挂钩，轨迹可被分析。更准确说是**假名（pseudonymous）**。
- “不需要中介”指的是**结算与记账不必经过某一家支付公司**；你仍然可能通过交易所、托管钱包等中心化服务买卖，那些环节另有风险。

比特币是如何运作的？——把网络想成一场公开游戏

可以把比特币网络想成一场**自愿参加的大型协作游戏**（规则写在软件里）：

1. **谁都能进退**：你有一台能联网的电脑，就可以下载软件当节点，保存（或验证）账本；不玩了就退出。
2. **记账要抢，也要烧成本**：大约每十分钟，网络会产出一个新区块。想争取记账权的人（矿工）要比拼算力，不断做一种很难碰巧做对、但别人很容易核对的计算——这就是后面说的 **PoW（工作量证明）**。算力越大，短期内撞上正确答案的概率越高，但没有人能保证“下一秒一定是我”。
3. **转账要广播**：你发起转账，交易会传给节点；矿工挑选交易打包进区块。全网节点按规则校验：签名对不对、你有没有花过这些币、有没有双花。
4. **改规则、改历史极难**：想改已经确认的账，或强行改发币规则，需要压倒性的算力与社会共识；多数参与者会拒绝非法分支。

为什么有人愿意一辈子耗电记账？因为成功出块有**区块奖励**（新币）和用户付的**手续费**。激励让陌生人愿意维护安全：攻击网络往往贵到不划算，遵守规则反而能赚钱——这是比特币把“密码学 + 经济学”焊在一起的关键。

和支付宝对比一句话：

- 支付宝：一家公司改两行余额。
- 比特币：成千上万台机器按同一规则，把这笔变动写进公共账本，并层层确认。

和“Q 币、游戏点券”对比一句话：点券是公司数据库里的一串数字，公司能改能停服；比特币余额是公共账本上、由你私钥控制的未花费输出，没有“总公司客服”能一键给你回档。

为何比特币仍特殊?



（原稿这里大段粘贴了机构研报编译。v2 **不转载**。下面用我们自己的话，把新人真正需要的判断框架说短。）

市场上代币成千上万，为什么很多人仍把比特币单独一列？不是因为它“永远涨”，而是因为它的设计取舍和其他链常常不一样。

1. 网络和币是绑死的

“比特币”既指**网络**（大家跑的那套协议），也指**币**（网络里的原生单位）。你可以复制代码另开一条链，但那是**另一个网络、另一种币**，不会自动变成“正统比特币”。币也不能像拷文件一样无损搬到任意其他链上还能叫同一个 BTC（跨链桥是另一套信任假设，后面章节再讲）。

2. 更像“数字时代的货币商品”，不像公司股票

比特币不派息、没有CEO财报。人们看重的往往是：可转移、可分割、可验证稀缺、难以单方面增发。它更常被讨论成**价值储存 / 结算资产**候选，而不是“下一家独角兽股权”。这不保证它胜出，只说

明**评价框架不同**：别拿 PE 估值那套硬套。

3. 稀缺规则难改，是社会共识 + 激励，而不只是一行代码

2100 万上限写在规则里，但代码理论上能改。真正让上限“硬”起来的是：持币人、矿工、交易所、钱包、节点运营者——多数人不愿意接受稀释自己的增发。改上限等于跟自己的经济利益作对，协调成本极高。所以新人要理解：**安全不只来自密码学，也来自一群人不愿合谋改规矩**。

4. “改进比特币”往往是换一套取舍，不是免费升级

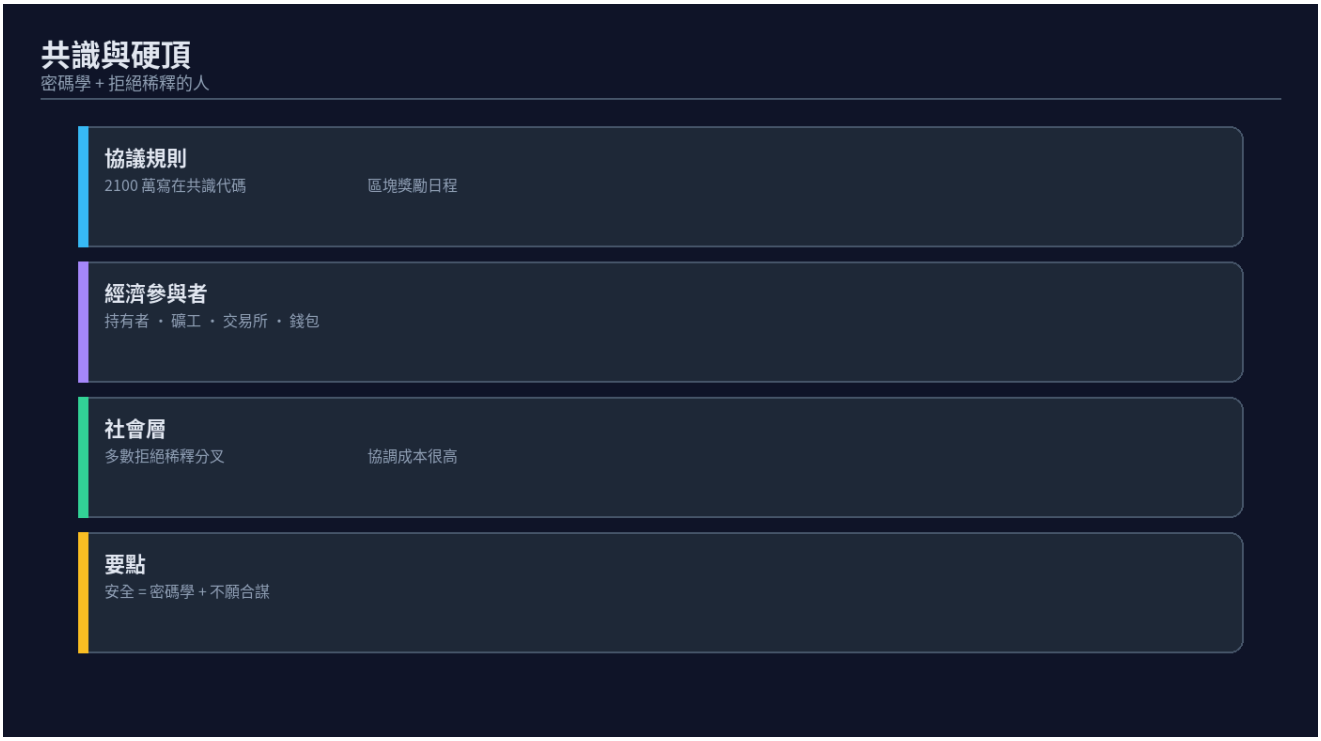
后来的公链常在速度、智能合约、手续费上更激进，但通常要在**去中心化、安全性、简单性**上付出代价。比特币刻意保守：脚本能力有限、升级极慢，换来的是长期抗审查与“少动刀”。其他项目可以服务别的需求（合约、游戏、DeFi），和比特币不必互相消灭；但若你的目标是“最保守的数字稀缺资产”，评估标准就应不同。

5. 到了 2026，外部世界也在变

机构通道（例如部分市场的现货 ETF）、托管与合规交易，改变的是**普通人接触 BTC 的入口**，没有改掉账本本身的规则。入口变方便，不代表你把币放在交易所就等于“自己掌控比特币”——托管风险另算。扩容方面，主链保持相对克制，更多小额高频需求会走到闪电网络等二层思路上（后文 Layer2 章会从以太坊侧展开，比特币侧同理：一层求稳，二层求快）。

一句话：比特币特殊，是因为它把“谁说了算”降到最低，并把稀缺和安全当成第一优先级；其他链特殊，往往是因为它们优先可编程与性能。选哪条路，取决于你要解决什么问题。

读懂区块链共识机制：PoW、PoS、DPoS



刚入门会一直撞上 PoW、PoS 这些缩写。别被英文吓到：**共识机制 = 一群互不信任的人，用什么规则决定“下一页账谁写、写得对不对”**。

家里投票去哪旅游：少数服从多数——那是一种共识。区块链要在全球、有人可能作恶的环境下记账，规则就得更硬，并且常常绑定真金白银的奖惩。

常见入门三分法如下（世界上还有更多变种，先掌握这三种就够读新闻）：

PoW（Proof-of-Work，工作量证明）

- **怎么选记账人**：拼算力，做大量哈希运算，谁先找到满足难度的解，谁大致获得出块权。
- **优点**：准入相对开放；攻击要砸真金白银的硬件和电费；比特币用的就是 PoW。
- **缺点**：耗能与硬件军备竞赛；普通笔记本早已挖不动 BTC。
- **人话**：谁愿意持续付出可验证的“体力劳动”（计算），谁才有较高概率记账分红。

PoS（Proof-of-Stake，权益证明）

- **怎么选记账人**：把币质押（stake）进来当保证金，按规则抽选或轮流出块；作恶可能被罚没（slashing）。
- **优点**：一般远比 PoW 省电；确认可以设计得更快。
- **缺点**：容易让人担心“币多的人话语权更大”；质押与流动性、惩罚规则都更复杂。
- **2026 提醒**：**以太坊已在 2022 年完成合并（The Merge），主网不再靠 PoW 挖矿，而是 PoS 质押验证**。 老文章里“以太坊矿工显卡挖 ETH”属于历史。比特币仍然是 PoW，两套路线并存。

DPoS（Delegated Proof-of-Stake，委托权益证明）

- **怎么选记账人**：像股东选董事——持币人投票选出少数代表节点来出块。
- **优点**：节点少，协作快，吞吐往往更高。
- **缺点**：更像“选出来的小委员会”，去中心化程度通常弱于大规模 PoW/PoS；要盯防贿选与寡头。

小结

没有完美共识，只有取舍：安全、去中心化、速度（常被称作“不可能三角”的简化版）。读项目时先问：谁有权出块？作恶成本是什么？普通用户能不能自己跑节点验证？比特币的选择很明确——**偏安全和去中心化，接受链上吞吐不高**。

什么是比特币私钥、账户与钱包?



和用户关系最紧的三样东西：**私钥、地址（账户）、钱包软件**。下面按直觉讲，故意少堆公式。

公钥密码体制（直觉版）

现代密码学可以生成一对钥匙：

- **私钥**：只有你能有的秘密，用来**签名**（证明“这笔花费是我同意的”）。
- **公钥**：可以从私钥推导出来，别人用来**验证**签名，却很难反推私钥。

在比特币里：私钥掌控币；网络用数学检查签名，不必让你把私钥亮给全世界。

什么是私钥?

私钥本质上是一个**极大空间里随机出来的数**（通常再编码成一串字符）。谁掌握私钥，谁就能花对应地址上的币。

因此：

- **泄露 ≈ 丢币**，而且往往无法冻结追回。
- **丢失且无备份 ≈ 币其实还在链上，但你永远花不出去**。
- 不要截图存在相册、不要发聊天软件、不要存在他人“帮你保管”的不明网页。

什么是比特币账户 / 地址?

日常说的“比特币账户”，多半指**地址**：由公钥经过哈希等步骤变成的一串字符（不同地址格式外观不同）。别人给你转账，是转到地址；链上记录的是这些地址之间的支付关系。

更精确一点：比特币用的是 UTXO 模型——你的“余额”是若干笔**还没花掉的交易输出**之和，不是银行那种单一账户字段。入门阶段记住一句即可：**地址用来收款；私钥用来授权付款**。

什么是钱包?

钱包主要是**帮你保管密钥、展示余额、构造并签名交易**的工具。
钱包里通常并不“存着一堆币文件”，币在链上；钱包里是钥匙。

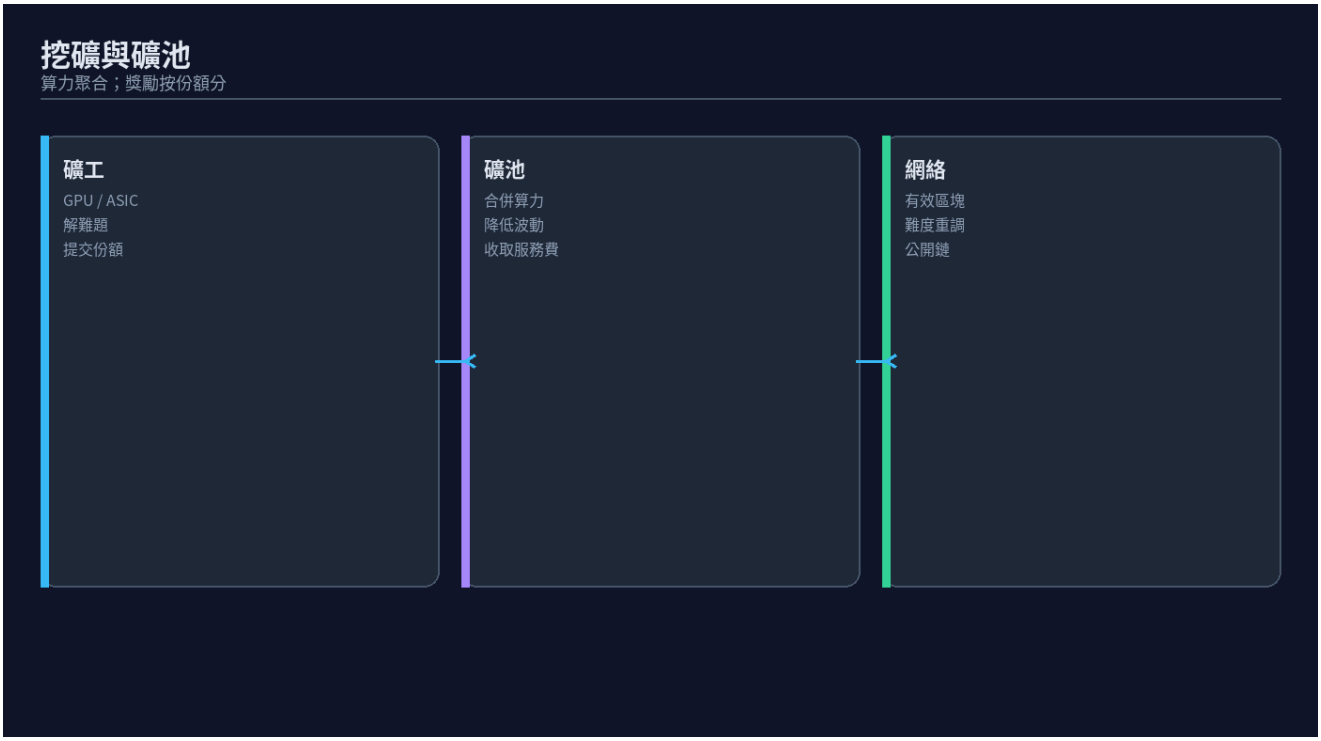
常见分类:

类型	特点	适合
热钱包	联网的手机/浏览器/桌面应用，方便	小额日常
冷钱包	私钥离线（如硬件钱包、离线签名）	大额长期
托管钱包	交易所等替你持股	图方便，但你承担平台风险

首次创建钱包时常见 **助记词（种子短语）**：一串单词能推导出私钥。助记词 = 总钥匙，任何人拿到都能掏空。只写在离线介质、多重备份、永不联网打字上传。

转账时你在本地签名，再把已签名交易广播出去；矿工打包后，经过若干确认，对方才宜视为到账。

什么是比特币矿场和矿池?



挖矿从“笔记本玩玩”演变成高度专业化的产业。三个词常混:

1、矿机

专用计算设备。简史可以记一条进化线：

CPU → GPU → FPGA → ASIC（专用芯片）

如今比特币主流是 ASIC 矿机：只会（或主要）干挖矿相关的哈希，效率远高于普通电脑。家用电脑参与 BTC 挖矿基本没有经济意义。

2、矿场

把大量矿机集中放置、供电、散热、运维的场所。为什么要集中?

- **电费**往往是最大成本，场址靠近廉价稳定电力；
- 专业运维（宕机、更换板子、监控）比家里散养可靠；
- 噪音、散热、合规用电，家用环境很难扛。

矿场是**物理与运维层**的生意：托管机器、保障在线率。

3、矿池

挖矿像不断买彩票：算力小，可能很久不开一张“中奖票”（出块），收入波动极大。于是矿工把算力**逻辑上集中**到矿池：

- 矿池分配计算任务；
- 谁贡献了多少有效份额，按规则分奖励（具体分成模式各异）；
- 小矿工获得更平滑的现金流，常不必自己操心完整出块流程。

人话：**矿场是厂房；矿池是项目组组长**。
矿机可以放在甲矿场，算力接到乙矿池——物理托管与逻辑分红可以分开选。

矿池变大也会带来中心化担忧（少数矿池占比过高）。健康的网络希望矿池分散、矿工可迁移。对新人：如果你不挖矿，只需理解——**网络安全预算很大一部分，来自这些为奖励而竞争的算力**。

本章收束

若你只带走五句话：

1. 互联网擅长复制信息；**钱不能靠复制**，否则双花。
2. 中心化支付靠机构账本；比特币靠**全球复制的规则账本 + 激励**。
3. 比特币刻意保守，强调稀缺与抗审查；**和其他公链是不同考卷**。
4. **私钥 = 所有权**；钱包是钥匙串，不是银行金库本身。
5. 矿机/矿场/矿池让 PoW 安全变得工业化；你不挖矿也可以当节点验证规则。

下一章我们离开“单个货币系统”，讲 **Web3** 这个更大的筐：当账户、合约、身份和应用都往链上搬时，新人到底会碰到什么——以及哪些是泡沫话术、哪些是真能上手的能力。

（第 1 章完 · v2 原创重写 · SCDO Lab）

2、Web3

> SCDO Lab · Web3 新人必读指南 v2 · 华语彩图版
> 英文版：`02-web3.en.md` · 插图目录：`assets/ch02/`
> 上一章讲比特币这一种“数字现金系统”。这一章把镜头拉远：口头上的 **Web3** 到底指什么、和天天用的 App 差在哪、2026 年真正落地了什么、新人从哪下手。
> **不是投资建议，也不是“风口号召书”。**

开篇：先把泡沫话术关小一点

一提 Web3，网上常见三种声音：

1. **万能药**：要取代谷歌、银行、政府，明天就到来。
2. **骗局筐**：凡是带链、带币的全是割韭菜。
3. **黑话迷宫**：DAO、DApp、TVL、账户抽象……新人听三分钟就想关网页。

我们选第四种：**工程与产品视角**。
Web3 不是一个公司、也不是一条链，而是一批人想用**区块链 + 密码学钥匙 + 开源协议**，把一部分互联网服务从“必须信某家平台”，改成“规则公开、关键动作可验证”。做得到的地方很具体；吹过头的地方也很具体。读完本章，你应该能分清两者。

术语说明：业界混用 **Web3** 和 **Web 3.0**。早期有人写 Web 3.0；今天口语里 **Web3** 更常见。下文统一用 Web3。它和“语义网 Web 3.0”（偏数据互联的另一套老概念）不是一回事——听到别人说 3.0，先问清楚指的是哪条线。

Web3 究竟是什么?

一句话版本

Web3 ≈ 用区块链等技术，让用户能自己持有数字资产与身份凭证，并在较少依赖单一平台“说了算”的前提下，使用在线应用。

更短一句：**少一点“你必须信这家公司”，多一点“你自己能核对”。**



这个说法能追溯到以太坊联合创始人之一等人在 2010 年代中期提出的方向（原稿访谈长文 v2 **不转载**）。核心是工程态度：系统尽量减少对权威机构的盲目信任，把可验证性做进协议里。我们同意方向，但必须补一句 2026 的现实——**完全去掉所有中介还不存在**；交易所、浏览器、手机系统、域名、稳定币发行方，仍然处处是中介。Web3 改的是**哪一段可以不信单一账房**，不是让你生活在真空里。

为什么要有 Web3?

今天的主流互联网（常称 Web2）极其好用：社交、购物、支付、视频，几个巨头就能覆盖大半生活。问题也叠在好用上面：

- **账户在别人那里**：封号、改规则、改推荐算法，你往往只能接受或走人，数据带走很难。
- **钱和积分在别人那里**：游戏皮肤、平台余额、创作收益，停服或改条款就可能归零。
- **信任成本高但证据少**：你相信“后台会按公告执行”；真出纠纷，个人很难审计数据库。

Web3 想对准的痛点是：把**所有权和控制权**尽量交回用户手里——用私钥签名证明“这是我授权的”，用公开账本证明“这笔状态变更新过”。它不自动等于公平社会，只是多了一种技术选项。

少一点盲目信任，多一点可验证

这里的“信任”不是劝你别相信朋友，而是系统工程里的意思：

> 你不得不假设某个黑盒会诚实、会一直在线、会按承诺不改规则——却拿不到独立证据。

比特币转账：全网可核对“有没有双花”。
智能合约兑换：你（或你信任的浏览器工具）可以读合约代码与链上结果，而不是只读 App 文案。

反过来：若你把币放在中心化交易所，你又回到了“信这家公司的账本”。**工具是 Web3，用法可以完全是 Web2**。 新人常在这里自我感动。

打破垄断，可能吗?

愿景里常有“打破科技巨头垄断”。诚实回答：**部分削弱锁定，很难一夜推翻**。

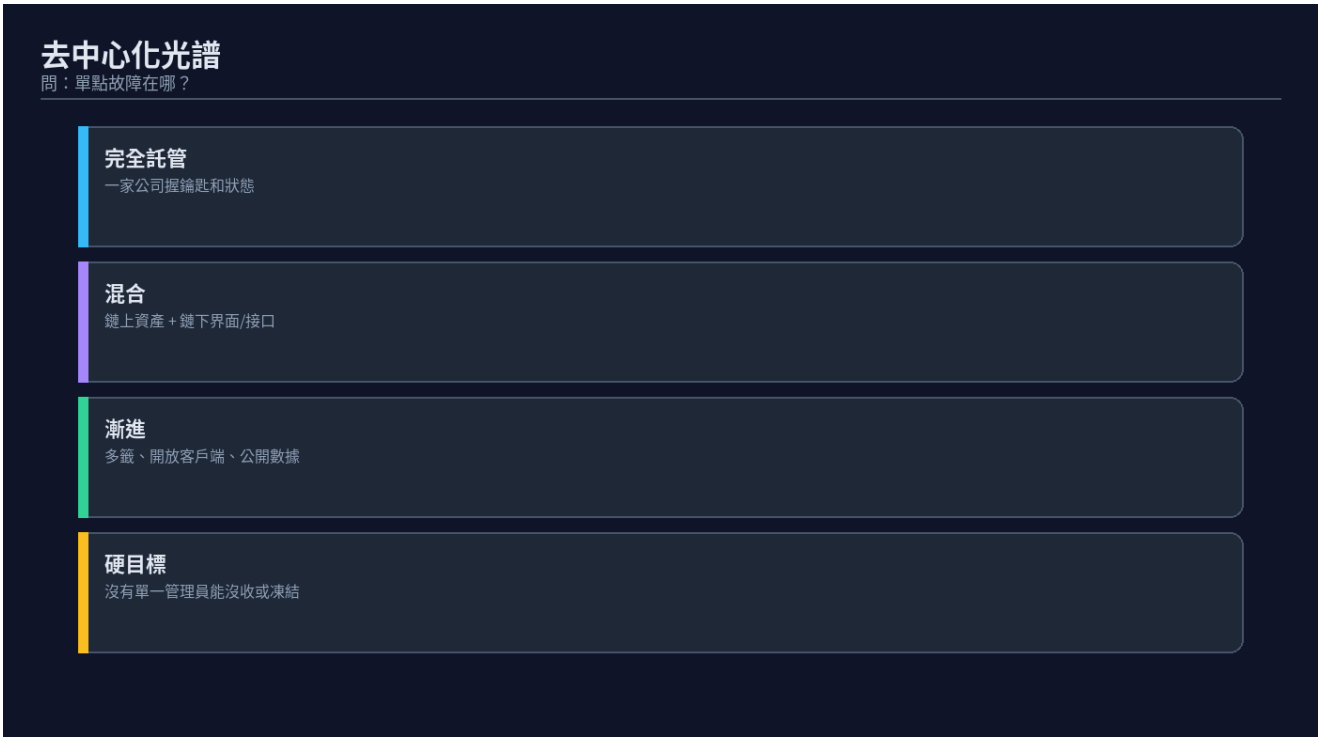
- 密码学让普通人也能加密通信、自持资产——巨头不容易单方面抹掉你链上的币（司法与托管场景另说）。
- 但流量、法币出入金、手机应用商店、合规牌照，仍高度中心化。
- 许多“Web3 应用”前端还是普通网站，域名被掐、接口被关，体验照样挂。

更靠谱的目标不是“消灭公司”，而是：**关键资产与身份不要只活在一家公司的数据库里**；公司可以提供更好用的界面，却不易单方面抹掉你的链上权利。

什么是去中心化?

去中心化（decentralization）被说烂了。我们用可检查的定义：

有没有单点，能单独让系统停摆、改历史、或不经你同意动你的资产?



- **完全去中心化**：现实里几乎没有纯形态。
- **足够去中心化**：作恶或故障的成本高、替代路径多，普通用户可自建节点或换钱包继续用。
- **伪去中心化**：币在链上，但升级多签、排序器、桥、预言机全是一小撮人——要看清。

去中心化 ≠ 无政府、无法律。合规、税务、反诈在多数司法辖区仍然适用。把它理解成“技术上降低单点霸权”，而不是“法外之地”。

Web3 的世界长什么样?（2026 实景，不画大饼）



已经能摸到的：

层	你可能碰到的东西
资产	BTC、ETH、稳定币、各类代币；有人通过交易所或（部分市场）ETF 接触
应用	DeFi 兑换/借贷、NFT 凭证、链游道具、链上社交协议
入口	浏览器钱包、手机钱包、交易所 App、渐渐出现的智能钱包 / 账户抽象
基础设施	公链、Layer2、跨链桥、预言机、索引服务

还经常做不到或很难用的：

- 完全无需学习私钥/助记词的“零摩擦大众体验”（在变好，未结束）；
- 全球统一、无缝、无桥风险的多链体验；
- 用链上应用完全替代超级 App 级社交与支付的日常习惯。

2026 年的诚实结论：Web3 已经从“只有极客挖矿”变成“有一批真实在跑的金融与凭证基础设施”，但距离“下一代互联网已经全面替换 Web2”还很远。把它当**增量工具箱**，比当宗教稳妥。

几个最常见的误会（先排雷）

1. **“上了链 = 一定去中心化、一定安全”**
   合约可以有后门升级；桥可以多签；前端可以钓鱼。链只保证**按当前规则执行**，不保证规则对你有利，也不保证你点的是真网站。

2. **“有币、有 NFT 就是 Web3 创业成功”**
   代币是激励与协调工具，也可以是空气。看有没有真实用户、真实现金流或真实凭证需求，比看

有没有发币重要。

3. **“去中心化应用不用管法律”**
   开发者、发行方、法币通道、宣传方式，在多数地方仍可能落入现有金融与消费者保护法。技术叙事替不了合规功课。

4. **“我装了浏览器钱包，所以我已经很 Web3 了”**
   若资产主要在中心化交易所、从不开区块浏览器、见签名就点允许——习惯仍是 Web2。工具不等于素养。

5. **“AI + 链 = 自动赚钱机器人”**
   2026 年 AI agent 确实开始能调 API、甚至发起支付；但权限过大时，出错与被盗速度也更快。自动化必须配**额度、白名单、可审计日志**——这也是我们强调 Agent Ledger 的原因：先能讲清楚机器做了什么，再谈效率。

普通人如何参与?

原稿常见“风口”口气。我们改成：**你若好奇，怎么低成本、低风险地弄懂**。

Web1 → Web2 → Web3：三句话就够



不必背长历史，记用户角色变化：

1. **Web1（大约只读）**：门户、静态页——你主要是读者。
2. **Web2（读写 + 平台）**：你发内容、做交易，但账号、粉丝、数据、推荐权多在平台。

3. **Web3（读写 + 可持有）**：你仍用 App，但关键资产与部分身份可以用钥匙自持；规则尽量写在协议/合约里。

有人把 Web3 概括成“用户控制信息/资产”。方向对，但请加限制词：**在你真的自持钥匙、并理解签名在干什么的前提下**。

为什么还值得了解？

即使你不“All in”，也值得懂，因为：

- 数字所有权争议会越来越多（门票、会员、创作分成、游戏道具）；
- 金融机构与大公司已经在用链或链上资产做试验与产品；
- 骗子话术大量借用 Web3 黑话——**不懂概念更容易被收割**。

不值得的是：听信“再不进场就晚了”、把生活费梭哈、或把学习外包成代操作（代操作≈把钥匙交给陌生人）。

和 Web2 比，实际不同在哪？

维度	Web2 典型	Web3 典型
登录	手机号 / 统一登录	钱包地址 + 签名（也在向邮箱社交登录演化）
资产	平台余额	链上代币 / NFT（或仍托管在交易所）
改规则	公司发公告	常需治理投票或合约升级，过程可观察
出错了	找客服	多数情况无客服回滚；安全自负
透明	黑盒数据库	账本公开，但可读性需工具

最大的体验冲击往往不是“去中心化理想”，而是：**撤销很难**。 签错授权、转错地址，链上通常不认“我手滑了”。第 9 章会专讲安全。

能带来什么？（按已验证程度排序）

相对扎实的：

- **可编程支付与金融积木（DeFi）**：兑换、借贷、抵押——好用，也有清算与合约风险。
- **公开可查的凭证（NFT 等）**：票务、徽章、会员、道具证明“你持有过/持有着”。
- **跨境价值传输的另一条轨道**：在合规允许的前提下，作为补充通道存在。

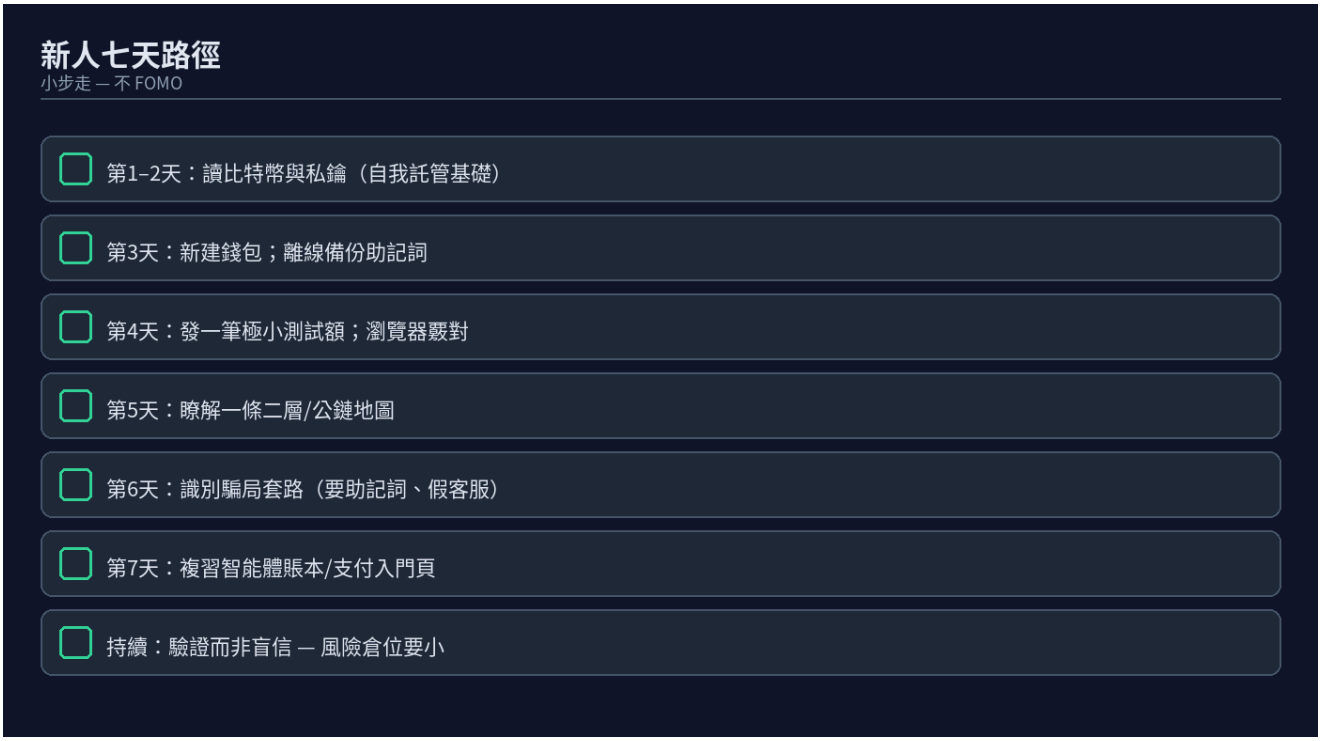
仍在早期、噪音大的：

- 链上社交要取代超级 App 级产品；
- 元宇宙地产叙事；
- “人人 DAO 协作取代公司”。

我们（SCDO Lab）怎么看落地——轻提一句：
真正有用的往往不是更炫的故事，而是**可验证的记录与激励是否服务真实业务**——比如代理/自动化程

序（AI agent）替你执行动作时，有没有可审计的账本与权限边界。我们把这类方向叫 Agent Ledger 哲学：机器可以自动，责任与痕迹不能糊。后面公链、安全章会再碰到，这里不展开产品说明书。

新人七天行动清单（不涉及充值也能做）



1. 分清：**链上自持** vs **交易所托管**。
2. 装一个信誉较好的钱包，**只转一笔你亏得起的小额**做实验（或先用官方测试网）。
3. 学会看：地址、网络（别转错链）、浏览器（区块浏览器）上的交易状态。
4. 读懂一次签名弹窗：授权（approve）可以非常危险。
5. 助记词离线备份；不向任何人透露。
6. 把社交网络/群里的“稳赚”“内部额度”默认当高风险。
7. 选一条主线深入：比特币、以太坊 + L2、或纯安全习惯——比同时追二十个空投强。

司法辖区不同，买卖与营销规则不同；请遵守你所在地法律。本书不提供任何地区的操作规避建议。

Web3 术语速查（精简版）

原稿有上百条词典，重复且易过时。这里只留**读后文够用**的一组；细节在后面章节展开。

基础设施

- **区块链 / 公链**：公开账本与执行环境；任何人可验证（见第 3 章）。
- **节点**：运行软件、保存或验证账本的计算机。
- **共识**：谁有权出块、如何惩罚作恶（PoW / PoS 等，见第 1 章）。
- **Layer2（L2）**：挂在主链安全之下的扩容层，用来降低费用、提高吞吐（第 4 章）。
- **智能合约**：部署在链上的程序，满足条件就按代码执行（第 3 章）。

- **预言机**：把链下数据（价格等）喂给合约的机制；本身常是信任点。
- **跨链桥**：让资产/消息在不同链间传递；历史上事故高发，慎用。

账户与资产

- **钱包**：管理钥匙、发起签名的工具。
- **私钥 / 助记词**：控制权本身。
- **地址**：收款与身份的公开标识（假名）。
- **代币（Token）**：链上可转移的单位；同质化（如 ERC-20）或非同质化 NFT（如 ERC-721）。
- **稳定币**：锚定法币等资产的代币；要区分储备与风险。
- **Gas / 手续费**：让矿工或验证者处理交易的费。

应用与组织

- **DApp**：前端 + 智能合约等组成的去中心化应用（去中心化程度参差不齐）。
- **DeFi**：去中心化金融应用集合（第 5 章）。
- **DAO**：用代币/规则协调的链上组织实验；治理质量天差地别。
- **TVL**：锁在协议里的资产估值；可参考，可被刷，不能单看。
- **NFT**：非同质凭证；不等于“一定值钱的图”。
- **账户抽象 / 智能钱包**：让登录、恢复、代付 Gas 更像普通 App（进行中）。
- **AI agent**：能自动调工具/合约的程序；权限与审计比“会不会聊天”更重要。

安全口头禅

- **授权（Allowance）**：你允许某合约动用你的代币额度——过量授权是被盗重灾区。
- **钓鱼**：假网站、假空投、假客服要你签名或导出助记词。
- **自托管**：自己握钥匙；**托管**：别人代握——方便与风险互换。

插图一览

文件	用途
`assets/ch02/fig01-web1-web2-web3.png`	Web1→2→3 角色变化
`assets/ch02/fig02-trust-vs-verify.png`	盲目信任 vs 可验证
`assets/ch02/fig03-decentralization-spectrum.png`	去中心化光谱
`assets/ch02/fig04-web3-2026-ships.png`	2026 交付与仍难之处
`assets/ch02/fig05-newcomer-path.png`	新人七天路径

（均为 SCDO Lab 原创示意图，无第三方商标仿制。）

本章收束

带走五句：

1. Web3 的核心承诺是 **可验证与自持**，不是保证暴富。
2. Web1 只读、Web2 平台读写、Web3 尝试 **读写 + 所有权**——现实是混合的。
3. 去中心化要问 **单点在哪**，不要停在口号。
4. 2026 年已有真东西（资产、DeFi、L2、凭证），也有大量未兑现叙事。
5. 新人第一技能是 **钥匙与签名安全**，第二才是看项目。

下一章进入 **公链**：什么叫公共区块链、以太坊为什么重要、智能合约和代币标准怎么拼成应用世界，以及 2026 年的公链地图（不做超长安利名单）。

（第 2 章完 · v2 华语彩图版 · SCDO Lab）

3、公链

SCDO Lab · Web3 新人必读指南 v2
上一章把 Web3 说成“可验证 + 可自持”的工具箱。这一章讲工具箱底下的**操作系统**：公有区块链（公链）。
重点：公链是什么、以太坊为什么重要、智能合约与 ERC 标准、难度炸弹如何走完历史、2026 年怎么看 L1 格局。
不做项目安利清单，不写倍数字叙事。不是投资建议。

什么是公链?



人话定义

公链（Public Blockchain） = 一套对全世界开放的区块链网络：理论上任何人可以读账本、发交易、按规则跑节点（或轻客户端），没有一家公司能单独说“今天账本改成这样”。

对比三种常见形态，脑子更清楚：

类型	谁能参加	典型用途
公链	默认对所有人开放	比特币、以太坊等
联盟链	受邀的一批机构	企业结算、供应链试点
私有链	单一组织内部控制	内部实验、权限账本

Web3 新人说的“上链”，十有八九指的是**公链**（或挂在公链安全之下的 Layer2，下一章细讲）。

公链像不像“操作系统”？

有个常用比喻：公链 ≈ Web3 里的操作系统——提供账户、算力/验证、存储交易、跑程序（如果有智能合约）的底座；上面再长出钱包、DeFi、游戏、社交。

比喻有用，但别神话：

- 真正的 OS 很少每周改共识；公链升级要社区协调，有时还会**硬分叉**成两条链。
- “开放”不等于“免费好用”：有 Gas、有拥堵、有桥和跨链风险。
- 安全来自密码学 + 经济激励 + 足够分散的验证者/矿工，不是来自一句白皮书。

公链通常具备的属性（检查清单）

读一条新链时，可以用这几条自问：

1. **开放性**：能否无许可读/写？跑节点门槛多高？
2. **共识与安全预算**：PoW 算力还是 PoS 质押？作恶怎么罚？
3. **状态与执行**：只会转账，还是能跑通用智能合约？
4. **原生资产**：手续费用什么付？通胀/通缩规则是否清晰？
5. **客户端多样性**：是不是只有一个团队的客户端？单点风险多大？
6. **生态与退出权**：应用多不多？不喜欢规则时，用户资产能否相对容易迁走？

没有满分卷。比特币在“简单、保守、难改”上极强；以太坊在“可编程生态”上极强；许多新 L1 在“速度与费用”上更激进，往往在去中心化或战斗考验上更短。

什么是以太坊？



从比特币到“可编程的世界计算机”

比特币证明了：不靠银行，也能在全球账本上转移稀缺数字资产。
但它的脚本能力刻意很弱——更像一台功能单一的计算器。

以太坊（Ethereum） 的核心想法是：做一台**分布式计算机**——节点一起维护状态，任何人都能部署程序（智能合约），按规则自动执行。原生币是 **ETH**，用来付 Gas、在 PoS 时代也用于质押。

常说的口号：

- 比特币 ≈ 区块链 1.0（数字现金 / 结算资产）
- 以太坊 ≈ 区块链 2.0（智能合约平台）

这是教学简化，不是官方等级制度。今天大量价值与创新仍发生在以太坊及其 Layer2 上；其他 L1 则在性能、语言、模块化等方向竞争。

Vitalik 与早期故事（极简）

以太坊由 **Vitalik Buterin（V 神）** 等人推动：大约 2013–2014 年提出构想与众筹，**2015 年**主网启动。细节八卦不必背；新人记住一点即可——它从第一天就瞄准“可编程”，因此后来长出 ICO 浪潮、DeFi、NFT、L2 等一整棵树（好坏都有）。

和比特币差在哪？（对照表）

	比特币	以太坊（2026）
主要定位	稳健的数字稀缺与结算	通用合约平台 + 结算层
共识	仍是 **PoW** 挖矿	**2022-09 合并后为 PoS**

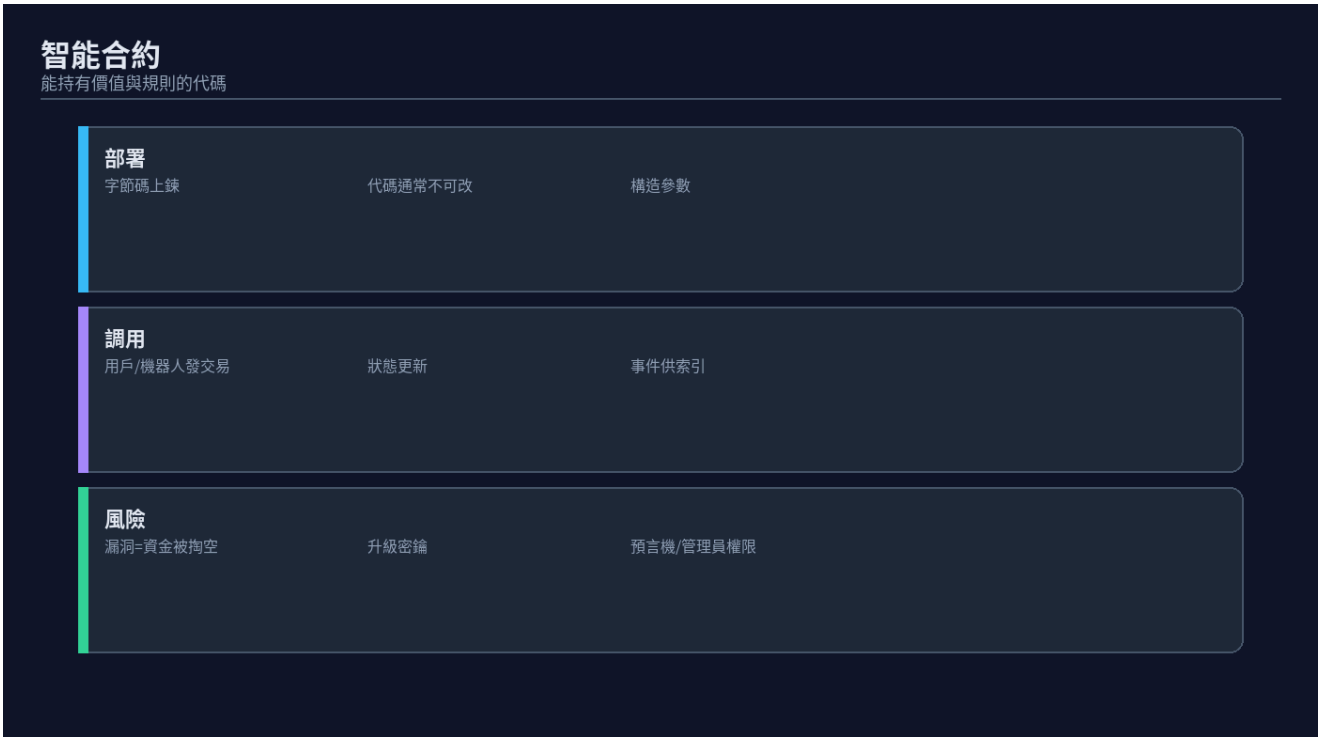
	比特币	以太坊（2026）
编程	脚本有限	EVM 智能合约（图灵完备，有 Gas 限制）
账户模型	UTXO	账户余额 + 合约账户
费用	BTC 手续费	ETH Gas（可很贵；许多用户改走 L2）
升级节奏	极保守	有路线图，但仍需广泛共识

关键事实（务必记住）：以太坊已经完成 **The Merge（合并）**，主网不再靠显卡/ASIC 挖 ETH；验证者质押 ETH 出块。若仍把“以太坊矿工靠显卡挖 ETH”“难度炸弹还在逼迁”当新闻读，就过时了。

EVM 是什么?

EVM（Ethereum Virtual Machine） 是以太坊上执行合约字节码的虚拟机。许多其他链宣称“EVM 兼容”，意思是：开发者能用类似工具/语言（如 Solidity）把应用迁过去，用户地址和钱包体验也更眼熟。兼容降低迁移成本，**不自动等于**与以太坊同级的安全与去中心化。

什么是智能合约?



定义

智能合约 = 部署在区块链上的程序：当交易触发它、且条件满足时，按代码更新链上状态（转账、铸币、改权限等）。
“智能”不是真有人工智能，而是**自动执行、结果可验证**；“合约”也不是自动具备法律效力——法律效力要看司法辖区与额外安排。

人话例子：

- 众筹合约：凑够额度才放款，否则退回。
- 兑换合约：按公式用代币 A 换 B（DeFi 常干的事）。
- 凭证合约：发给你一个独一无二的 NFT 表示门票。

合约一旦部署，代码对用户通常是透明可查的（是否有人去读是另一回事）。若设计了升级代理、管理员钥匙，则“不可篡改”要打折——读项目时要问：**谁能改规则?**

能力与坑

能力：减少对某家“后台手动执行”的依赖；让陌生人按公开规则协作。
坑：

- 代码有漏洞会被盗（历史无数）；
- 依赖错误的预言机价格会崩；
- 用户签错授权等于把门钥匙给人；
- Gas 贵或拥堵时，再好的合约也难用——这正是 L2 兴起的原因。

智能合约是公链变成“应用平台”的开关；也是安全章节必须单独开一篇的原因。

ERC-20 与 ERC-721：代币为什么要“标准”？



以太坊上的 **ERC**（Ethereum Request for Comments）是社区约定的接口标准。有了标准，钱包、交易所、浏览器才知道怎么显示余额、怎么转账，而不用为每个项目写一套特制软件。

ERC-20：可互换代币（同质化）

- 每一个单位彼此相同：像人民币的一块钱，或游戏里的金币。
- 标准规定了名字、符号、总量、转账、授权（`approve`/`transferFrom`）等接口。
- 用途：治理币、稳定币、积分、DeFi 里的 LP 凭证等等。
- **授权机制极强大也极危险**：你允许某个合约动用你的额度后，恶意合约可能转走代币。用钱包的授权管理、不要见签名就盲点。

ERC-721：非同质化代币（NFT）

- 每一个 tokenId **独一无二**：像房产证编号、演唱会座位、一副数字藏品。
- 用途：艺术品/头像、门票、会员牌、游戏道具、成就证明……
- NFT **不等于**“一定值钱的图”；本质是**链上唯一凭证**。值不值取决于权利、社区与流动性——多数会归零或无人问津，这是正常分布。

一眼区分

	ERC-20	ERC-721
互换性	同质，可互换	每个都不同
余额含义	数量	持有哪些 ID
典型问题	通胀、授权盗刷	假地板价、钓鱼 soft mint

此外还有 **ERC-1155**（一个合约里混同质+非同质）等，入门先握住 20 与 721 即可。其他链也有类似标准（名字不同，思想相近）。

附录：以太坊「难度炸弹」——一段已经走完的历史

有些旧文仍用“现在进行时”写难度炸弹，仿佛合并尚未发生。**本章按历史课来写**。

它是什么?

难度炸弹（Difficulty Bomb） 是以太坊 PoW 时期写进协议的机制：挖矿难度会在某个阶段指数级上升，出块变慢，最终让 PoW 挖矿无利可图。目的之一，是**倒逼社区完成向 PoS 的迁移**，减少“永远卡在挖矿时代”的拖延，也降低有人长期顽固停在旧链上的吸引力。

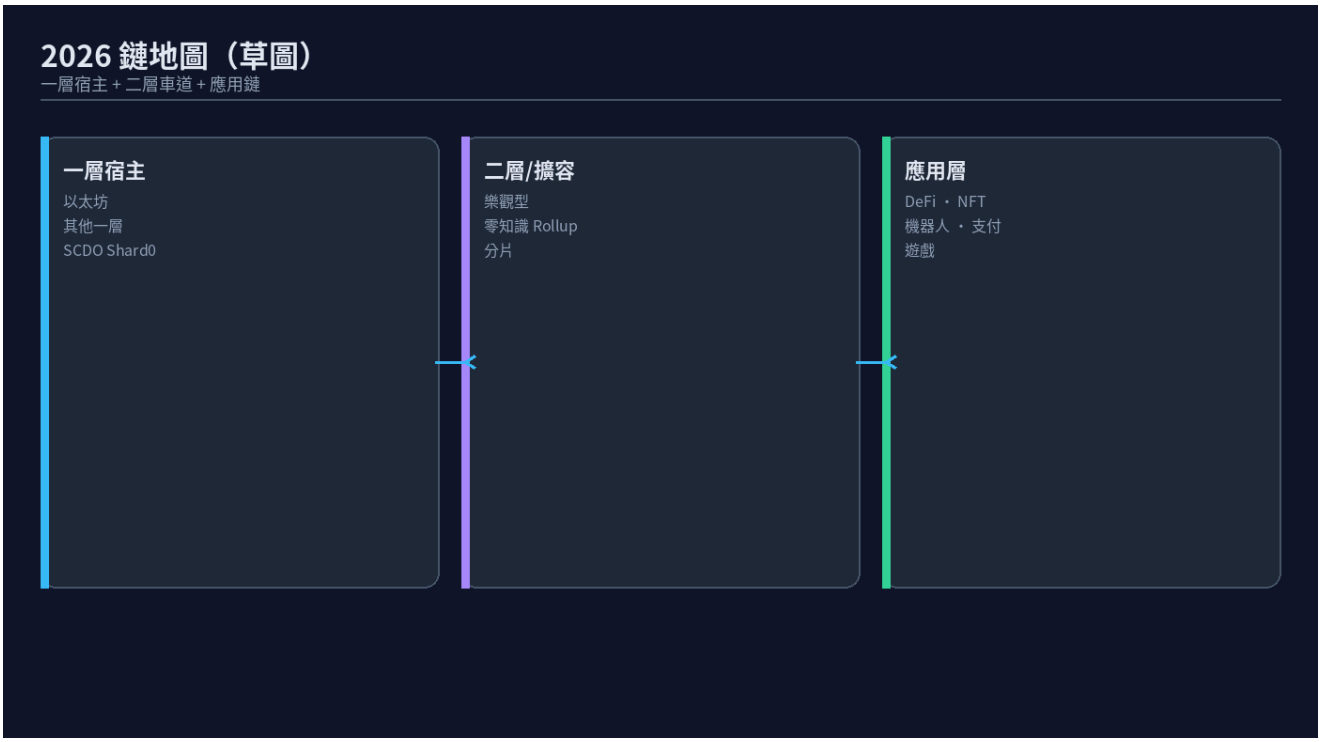
实际演进中，炸弹被多次**推迟**，以配合路线图；社区用硬分叉调整参数是常态，而不是“引爆炸弹毁灭网络”的科幻片。

结局是什么?

2022 年 9 月，以太坊完成合并（The Merge）：执行层与信标链合并，共识改为 **PoS**。主网 PoW 挖矿结束；难度炸弹作为“逼迁工具”的历史使命基本结束。
仍运行 PoW 的是**其他链**（例如经典分叉叙事下的某些网络），不要和今天的以太坊主网混为一谈。

新人读到 2017–2021 的旧文，看到“拆除炸弹”“冰河时代”，当作档案即可，**不要当成当前操作指南**。

公链创新方向与 2026 地图（精选，不灌水）



原稿里那类“明年看几十上百条新链、牛市百倍”的盘点——**整段不收**。下面只留**看懂地图的坐标**，不发项目推荐清单。

以太坊 vs 新 L1：竞争的是取舍，不是同一道填空题

- **以太坊路径**：L1 求安全与结算；大量用户活动迁到 **Layer2**；生态深、工具全、战斗测试久。
- **独立 L1 路径**：用新虚拟机、新共识、更高吞吐或更低费用吸引开发者；要自己冷启动流动性与安全口碑。
- **EVM 兼容链**：降低迁移成本，常靠生态位（交易平台资源、垂直场景）差异化；安全与去中心化程度需个案看。

没有“下一个以太坊”的单选题。更常见的是：**多链并存 + 桥与意图路由连接流动性**——桥的风险请默认高。

Layer 1 / 2 / 3（先建立分层直觉）

- **Layer1**：自己有共识与安全根的底链（比特币、以太坊、其他独立公链）。
- **Layer2**：依托 L1 数据/安全（尤其是以太坊 Rollup）扩容；下一章专题。
- **Layer3**：更偏应用专用或递归扩容的说法，定义仍在演化；新人不必先背，知道“还可以再分层”即可。

几条技术路线（知道名字级即可）

1. **高性能 / 并行执行 L1**：追求低延迟高 TPS，常对硬件与节点门槛有要求。
2. **Move 等资产导向语言**：强调资源类型安全，减少一类误写资产的漏洞（语言不是银弹）。
3. **模块化**：把执行、结算、数据可用性拆开，让团队像拼乐高一样组链（例：独立 DA 层 + 执行层）。好处是灵活；复杂度与安全假设也上升。
4. **专注垂直场景的应用链**：游戏、DeFi、隐私等——流动性与冷启动仍是难题。
5. **比特币旁路生态**：铭文、二层实验等——与“智能合约 L1”不是同一套考卷，但同属广义公链宇宙。

2026 年怎么看，而不看“60 条名单”

用问题代替清单：

- 钱与用户主要在哪几条结算层?
- 新应用更常部署在 L1 还是 L2?
- 这条链的客户端、验证者/矿工分布是否健康?
- 跨链时你信任的是谁?
- 监管与稳定币通道是否影响真实使用?

SCDO Lab 的轻观点：公链竞争的终局不太像“只剩一链”，更像**可验证记录成为默认基础设施**——哪条链胜出，取决于安全、费用、开发者体验与真实业务是否咬合。我们更关心“动作能否被审计、权限能否被约束”（Agent Ledger 一类问题），而不是今年叙事哪个最响。

新人怎么“摸”一条公链（十分钟实验）

理论不够，动手一次记忆更深（用你亏得起的小额或官方测试网）：

1. 打开该链的**区块浏览器**，搜一笔自己的交易：看成功/失败、Gas、从哪到哪。
2. 看一个热门代币合约页：持有人数量、是否可验证源码、有没有代理升级。
3. 问自己：我走的是**主网 L1**还是某个 **L2/侧链**？手续费计价单位是什么?
4. 若要跨链：默认假设桥可能出事，先搞懂锁定/铸造模型，再决定要不要大额。

能完成这四步，你就已经比只转发“公链排名截图”的人更接近真实用户。

本章收束

1. 公链是开放的公共账本与（常常）可编程执行环境，是 Web3 的底座。
2. 以太坊把智能合约做成主流；**已是 PoS**；许多用户活动在 L2。
3. ERC-20 / ERC-721 让代币可被钱包与市场统一理解；授权与炒作风险并存。
4. 难度炸弹是 PoW→PoS 路上的历史装置，不是 2026 年新闻。
5. 不背超长公链名单；学会用开放性、安全、执行、生态四问读地图。

下一章 **Layer2**：为什么以太坊还要叠一层、侧链和 Rollup 差在哪、Optimism / Arbitrum / ZK 系在 2026 年各自处在什么位置——用短卡片代替原稿那本“扩容百科全书”。

（第 3 章完 · v2 原创重写 · SCDO Lab）

4、Layer2

SCDO Lab · Web3 新人必读指南 v2
公链（尤其是以太坊）要安全、要开放，链上就会挤、Gas 就会贵。Layer2 是把大量计算挪到“二层”、把结果锚回一层的扩容思路。
原稿有近百页扩容百科——v2 **大幅压缩**为概念 + 短卡片。修正旧名「zkSync2.0 / zkSnyc」。**不是投资建议**。

为什么要扩容?



一条公链同时追求三件事时会打架（简化版“不可能三角”）：

1. **安全**（作恶很贵）
2. **去中心化**（很多人能验证）
3. **高吞吐低费用**（每秒很多笔、很便宜）

比特币、以太坊主网优先前两项时，普通人直接在 L1 上频繁交互就会痛：排队、贵、体验差。
扩容 = 在尽量少牺牲安全与可验证性的前提下，让更多人用得起。

两类大方向：

方向	做法	例子
链上扩容	改 L1 本身（更大区块、分片等）	历史上的区块大小争论；以太坊路线图里的部分升级

方向	做法	例子
链下 / Layer2	多数执行在二层，定期向 L1 交代	Rollup、部分通道方案

2026 年对以太坊用户更常见的路径是：**资产与结算信任 L1，日常操作走 L2**。

Layer2、侧链、Rollup：先分清亲戚关系



Layer2（L2）人话定义

挂在某条 L1（常指以太坊）安全假设之下的执行层：交易在 L2 上打包处理，关键数据或证明提交回 L1，让人仍能（在理想设计下）靠主网规则约束二层。

不是所有自称 L2 的东西安全等级都一样——要问：**出了事，能否靠 L1 的数据/证明把钱救回来?**

侧链（Sidechain）

独立一条链，有自己的共识与验证者；用桥和主链互转资产。
安全主要靠侧链自己，不是自动继承以太坊级安全。历史里游戏侧链被盗的案例，提醒新人：便宜≠同等安全。

Polygon 等生态里既有更偏侧链的设计，也有向 Rollup / 更强继承安全演进的产品线——**看具体产品，不要只看品牌名**。

Rollup（汇总）

当前以太坊扩容的主流叙事：

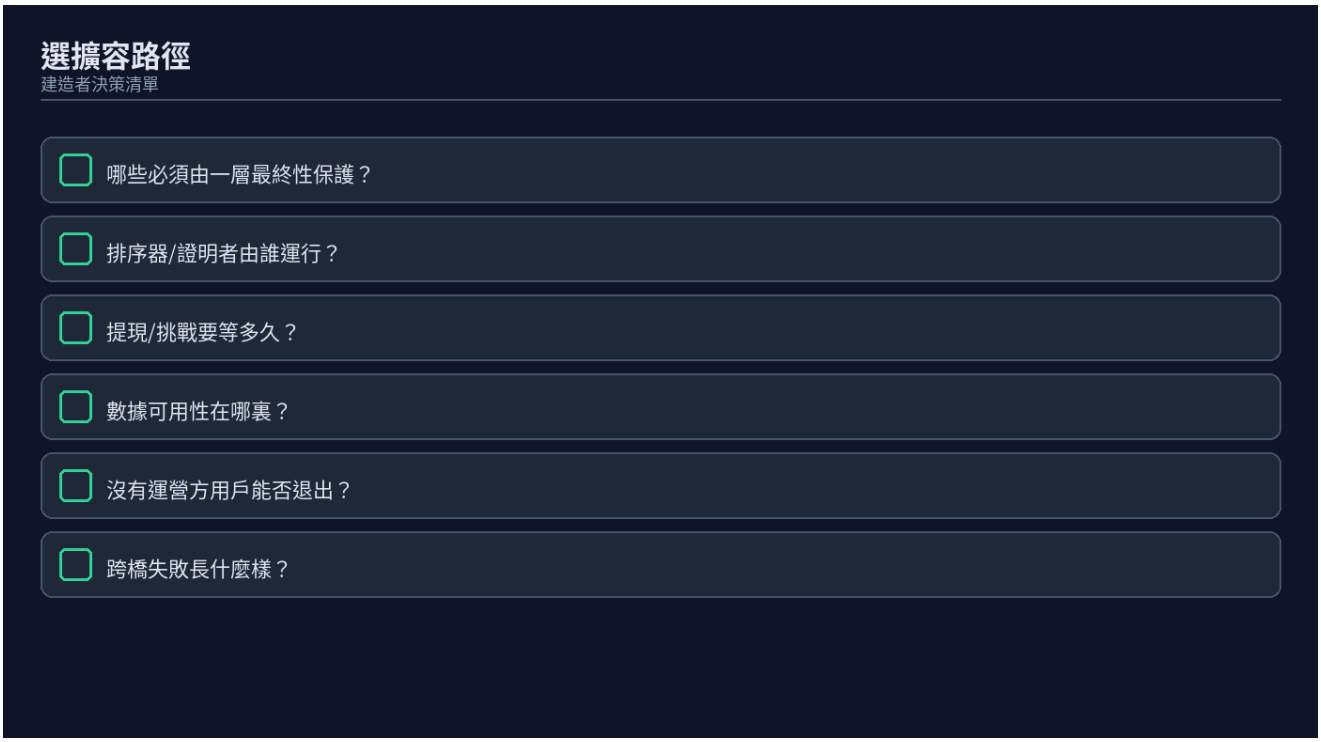
1. 在 L2 执行一堆交易；
2. 把压缩后的数据（或承诺）发到 L1；
3. 用一种机制保证“二层没乱记账”——要么靠欺诈证明，要么靠有效性证明。

两大派：

类型	怎么保证正确	新人直觉
Optimistic Rollup	默认诚实，有人发现作恶可在挑战窗内开撕（欺诈证明）	提款回 L1 常要等挑战期
ZK Rollup	每批状态用零知识证明（有效性证明）说明计算正确	证明生成复杂；提款逻辑与 OP 不同

状态通道、支付通道（如比特币闪电网络思路）也是“链下扩容亲戚”：适合高频小额、参与方相对固定；和通用智能合约 Rollup 不是同一产品形态。原稿年表式长文此处不复述。

怎么选路：一张决策草图



问自己四句：

1. 我要的是**便宜交互**，还是**最大程度继承以太坊安全**?
2. 我能不能接受提款延迟（常见于部分 Optimistic 路径）？
3. 桥和官方入口是不是我认准的域名？（钓鱼重灾区）
4. 应用是否真的部署在该 L2，还是只是“宣称支持”？

跨 L2 / 跨链桥默认高风险：锁资产、铸映射资产、多签或验证者集——历史上巨额被盗多次。能少桥就少桥；大额分批、先小额试。

代表方案短卡片（2026，不排名荐买）

以下只帮你建立地图，**不构成推荐**。名称与产品线会变，以官方文档为准。

Arbitrum（Optimistic 系）

- **是什么**：以太坊上成熟的 Optimistic Rollup 生态之一，EVM 兼容较好。
- **新人会碰到**：许多 DeFi / 应用同时部署；Gas 相对主网便宜。
- **注意**：仍要分清主网与 Arbitrum 网络；官方桥与假桥；挑战期相关的提款预期。

Optimism（Optimistic 系）与超级链叙事

- **是什么**：另一大 Optimistic Rollup 阵营；强调开源栈与“多条 OP 栈链”的生态扩展。
- **新人会碰到**：部分应用、治理与跨链体验和 Arb 类似但不相同。
- **注意**：不要把“同一套技术栈”理解成“同一条链、同一桥、同一风险”。

Starknet（ZK / STARK 系）

- **是什么**：用 STARK 证明的 ZK 路线；合约语言与工具链曾与纯 Solidity 世界不同（生态在持续 EVM/开发者体验改进）。
- **新人会碰到**：学习曲线、钱包与工具可能和 Arb/OP 不完全一样。
- **注意**：先搞清账户模型与官方入口，再大额进入。

zkSync（ZK 系；修正旧称）

- **命名**：原稿「zkSync2.0」「zkSnyc」等写法过时或笔误。对外请用项目**当前官方产品名**（及其文档中的网络名称），以区块浏览器与钱包网络列表为准。
- **是什么**：面向以太坊的 ZK 扩容路线之一，追求有效性证明与更好费用体验。
- **注意**：主网 / 测试网 / 不同产品线不要混；空投传闻区钓鱼极多。

其他你会刷到的词

- **Base 等应用链 / OP 栈链**：常与某一生态或分发渠道绑定，仍要核对是否继承何种安全。
- **Validium / 数据可用性折中**：把数据放链下以更便宜，安全假设变化——进阶话题，新人先知道“更便宜往往换了假设”。
- **共享排序器、去中心化排序**：关系到审查抵抗与单点；2026 仍在演进。

使用 L2 的日常习惯（比追叙事有用）

1. **钱包切对网络**：转错链、资产“消失”多半是人看错网络。
2. **只从官网/已验证入口进桥与 DApp**；搜索广告可能是假站。

3. **小额试通**再加大；记下自己的地址与交易哈希。
4. **授权管理**：L2 上一样会被恶意 `approve`。
5. **提回 L1 前读清规则**：时间、费用、官方桥路径。
6. **不要把侧链、Rollup、托管兑换“一键跨链”混为一谈**——底层信任方不同。

和 SCDO Lab 视角的一句衔接

扩容让自动化代理（AI agent）更买得起链上动作，但也让**错误与盗刷更快发生**。二层再便宜，仍需要：额度限制、可审计记录、可撤销的权限——这是我们谈 Agent Ledger 时强调的：速度服务业务，痕迹服务责任。

深入一点：数据放哪、谁排序、钱怎么回 L1

数据可用性（Data Availability）

Rollup 要让别人能检查二层有没有作恶，通常需要把足够的数据放到人们能拿到的地方。数据放在以太坊上更“继承安全”，费用也更高；放到别处更便宜，但安全假设变了。新人不必背所有缩写，记住权衡：**越便宜，往往越多依赖额外诚实假设**。

排序器（Sequencer）

多数 L2 今天仍有**中心化或半中心化排序器**负责排交易顺序、给快速确认。它带来丝滑体验，也带来：

- 宕机 → 暂时不好用；
- 审查 → 某些交易迟迟进不去；
- MEV → 顺序本身有价值。

长期路线多在讨论去中心化排序与共享排序；2026 年仍是“产品体验先行、去中心化补课”的阶段。用 L2 时，把排序器当成**可见的单点**，而不是假装不存在。

退出与桥

- **官方桥**：规则相对清晰，Optimistic 系提款可能有挑战等待。
- **第三方桥 / 流动性桥**：快，但多一层信任与合约风险。
- **中心化交易所充提**：方便，本质是托管账户记账。

选择取决于金额、时间敏感度与你愿意相信谁。没有“又快又零信任又零学习成本”的免费午餐。

比特币旁路与“别的二层”

以太坊 L2 最热闹，但扩容思想不独属于它。比特币有闪电网络等通道思路；其他 L1 也有自己的二层或应用链。跨生态时名称混乱——有人把一切侧链都叫 L2。**以安全继承关系为准，不以营销名为准**。

案例阅读法（避免当粉丝）

读任何 L2 新闻，强制问：

1. 证据系统是 Optimistic 还是 ZK，还是根本没有？
2. 交易数据发布到哪？
3. 升级钥匙在谁手里，有没有时间锁？
4. 用户资产被卡住时的社会与技术退出路径是什么？
5. 假官网最近有没有在钓鱼？

把这五问当肌肉记忆，比记住 TVL 排行有用。

费用直觉

L2 降低的是**执行与拥堵成本**，不是魔法免单。网络拥堵、复杂合约、代币授权、跨桥，仍可能突然变贵。养成习惯：发送前看估算；大动作拆成小步骤。

与开发者相关的一句（非教程）

若你将来做应用：优先考虑用户从哪条 L2 进来、官方桥路径如何写进文档、错误网络如何提示。很多“丢币”其实是 UX 没防呆。教育用户切网络，是产品责任的一部分。

新手上路的一天（故事化串讲）

假设你在以太坊主网有一点 ETH，想用某 DeFi，却被 Gas 劝退。你打开钱包，添加一条 L2 网络（或钱包已内置），从官方文档复制桥地址——先核对域名每一个字母。你先桥 5 美元等值资产做实验：几分钟后（或更久），浏览器显示 L2 到账。然后你在 L2 上做一笔小兑换，Gas 明显便宜。你记下：主网地址与 L2 地址通常相同，但**余额分网络记账**；看错网络会以为“币丢了”。玩够后，你决定是否把资产桥回主网，并预留等待时间与费用。这一天没有让你致富，但完成了比听十场 AMA 更有用的肌肉记忆。

若中途弹出未知签名，你拒绝；若有人私信“你的桥接失败，点此修复”，你当作骗子。若官方桥拥堵，你宁可等，也不要第一次就改走陌生快桥。把这种偏执留下——L2 让交易变便宜，也让诈骗的边际成本更低。

再进阶：同一生态可能有多条链、多个版本名称；测试网与主网名字相似。养成“先看 chainId / 浏览器网址，再签名”的强迫症，是成人礼。

常见问题（L2）

问：L2 上的币和主网是同一个吗?
答：余额按网络分开记账；地址常常相同，网络不同就不是同一条账本视图。

问：为什么提币有时要等很久?
答：某些 Optimistic 路径有挑战窗；第三方桥用流动性换时间，但换信任假设。

问：侧链是 L2 吗?
答：不一定。看安全是否依赖母链的数据/证明，而不是看广告词。

问：我该选哪条 L2?
答：看你的应用部署在哪、桥是否官方、社区与客户端成熟度，不看单一 TVL 截图。

问：Gas 为 0 的活动安全吗?
答：代付 Gas 可以是账户抽象特性，也可以是钓鱼包装；仍要读签名。

扩容争论里的价值观

社区争 L2 时，表面争吞吐，深层争价值观：谁有权排序？谁能升级合约？用户能否在排序器作恶时仍靠 L1 强制退出？不同答卷产生不同产品。有人愿用一点中心化换丝滑支付；有人宁肯贵一点也要最大程度不依赖单一公司。没有唯一正确答案，但有错误答案——那就是把营销口号当成安全证明。

回顾以太坊扩容史，你会看到状态通道、Plasma、侧链、Optimistic Rollup、ZK Rollup 轮流占据讨论 C 位。被淘汰的不一定是“骗子技术”，常常是工程与体验没跟上，或安全模型不被主流接受。今天的赢家叙事三年后也可能改写。因此本书故意用卡片而不是“终极排名”。你会换手机，也会换默认 L2；迁移成本来自资产与习惯，不来自忠诚。

对机构用户，托管方可能提供“账户抽象 + 代付 Gas + 白名单合约”的一揽子。那是另一套信任模型：方便，且把你拉回部分 Web2。教育的目标不是禁止这种便利，而是让你**叫得出自己信任了谁**。说不清信任对象时，就不要存入超过失眠阈值的金额。

最后提醒开发者与运营：文档里用截图标明“选对网络”，在错误网络上禁用危险按钮，比发十篇线程有用。L2 降低的是链上费用，降低不了沟通费用——而沟通费用才是大多数用户资产事故的真正 Gas。

分片（Shard）：扩容的另一条亲戚线



Layer2 是“上面再盖一层”。**分片（sharding）**是把一条大链切成多条并行的“车道”，账户与交易按规则分到不同分片，跨分片用专门的记账（如 Classic 上的 Debt）对齐。

概念	一句话
本地区块	分片内部打包、出块、确认
跨分片	发送分片先记账，接收分片确认后再入账（不同链实现细节不同）
和 Rollup 的差别	分片常是同族多链并行；Rollup 多把结果锚定回一条 L1

SCDO 的实际布局（2026，教育向）： Classic **Shard1–4** 用 **ZPoW** 做原分片核心；另有并列的 **Shard0 EVM（Ethash，chainId 5680）** 承接合约与 Agent Ledger。细节见第 10 章 SCDO、第 11 章挖矿——本章只建立“分片 ≠ 侧链 ≠ Rollup”的地图。

本章收束

1. L1 挤，才需要 L2；2026 以太坊用户大量活动在二层。
2. 侧链 ≠ Rollup；安全是否继承 L1，是灵魂问题。
3. Optimistic 靠挑战，ZK 靠有效性证明——体验与提款逻辑不同。
4. 记卡片不背百科；桥与假网站比“选错叙事”更致命。
5. 下一章进入 **DeFi**：在这些 L1/L2 上，兑换、借贷、做市到底怎么运转，风险在哪。

（第 4 章完 · v2 原创重写 · SCDO Lab）

5、DeFi

SCDO Lab · Web3 新人必读指南 v2
DeFi = 去中心化金融：用智能合约拼出兑换、借贷、做市等积木。好用，也可怕。
不贴协议白皮书长文；不把 TVL 当信仰。**不是投资建议，更不是赚币教程**。

什么是 DeFi?



DeFi（Decentralized Finance）：在公链（及 L2）上，用开源或可验证的智能合约，提供传统金融里常见的部分服务——兑换、借出借入、提供流动性赚费、衍生品等——尽量减少“必须开户信某家券商后台”的环节。

你通常需要：

- 一个自托管钱包（或你清楚风险的托管入口）；
- 一点原生币付 Gas；
- 读懂签名在授权什么。

它从哪来?

比特币证明了链上资产；以太坊智能合约让“钱的规则”可编程。2010 年代末到 2020 年“DeFi Summer”，自动做市商、借贷协议爆发；之后经历泡沫、黑客、稳定币风暴、监管压力。到 **2026**，DeFi 仍在，更冷静：机构与 RWA（真实世界资产上链）叙事增多，但**合约风险与用户操作风险从未消失**。

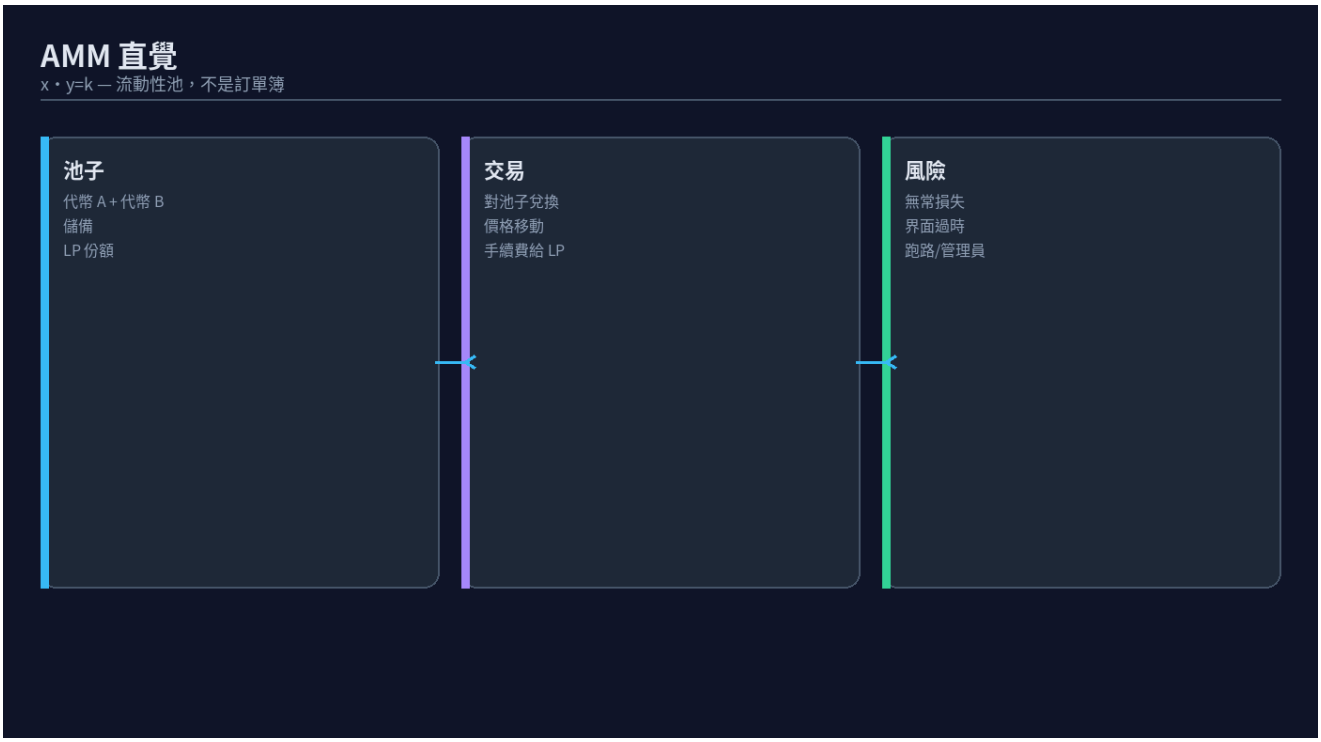
特点和优点（也是双刃剑）

特点	好处	代价
无许可接入	有钱包就能试	骗子也能部署假合约
可组合	协议像乐高互调	风险传染；一个坑拖垮一串
透明	参数与仓位可查	透明≠你看得懂；MEV 会夹你
全球 24/7	不停市	无客服回滚；签错就错

主流采用还卡在哪?

体验（Gas、桥、助记词）、合规（稳定币与出入金）、安全（黑客与钓鱼）、教育（无常损失、清算听不懂）。别信“DeFi 已经取代银行”的句子。

Uniswap：自动做市商入门



它是什么?

Uniswap 是以太坊生态里最具代表性的**去中心化交易所（DEX）**协议之一：不靠中心化订单簿撮合买卖双方，而靠**流动性池** + **公式定价**（自动做市商，AMM）。

人话：

- 有人往池子里存入两种代币（成为 LP，流动性提供者）；
- 交易者用 A 换 B，池子按算法调整价格；

- LP 承担价格变动带来的**无常损失**风险，同时可能赚取交易手续费。

和中心化交易所差在哪?



- 你常可自持钥匙交易（具体前端仍要防钓鱼）；
- 没有传统“充币到交易所账户”这一层（若你本就在交易所则另说）；
- 价格由池子与套利者共同形成，极端行情可能滑点巨大。

使用时心智模型

1. 选对网络（以太坊 L1 或某 L2 上的部署）。
2. 看清交易对、滑点、手续费层级。
3. 第一次授权代币给路由合约要谨慎；额度能少则少。
4. 小额试换；大额拆单或换更优路径。
5. 版本与费用档位会变——以你当时界面与区块浏览器为准，不背死数字。

借贷：以 Aave 一类协议为例（含风险）



它在干什么?

像“链上当铺 + 货币市场”:

- **存款人**提供资产，赚利息;
- **借款人**抵押某些资产，借出另一些;
- 价格波动导致抵押率不足时，**清算**卖抵押物保系统偿付。

Aave 是长期存在的头部借贷协议之一（还有同类竞品）。GHO 等稳定币实验属于其生态延伸——新人先懂抵押借还，再碰稳定币发行细节。

你必须懂的风险

1. **清算风险**：抵押品跌、债务涨，仓位被清算还要付罚金。
2. **智能合约风险**：代码漏洞、预言机操纵。
3. **利率与利用率**：钱荒时利率飙升。
4. **关联资产风险**：抵押物本身是另一种 DeFi 凭证时，风险叠罗汉。
5. **操作风险**：还错网、授错权、看错健康因子。

闪电贷：同一笔交易内借还、用于套利或清算的高级工具；不是“无抵押永久借款”的大众产品。听到“无风险闪电贷稳赚”多半是骗局或把复杂风险藏起来了。

Curve 与稳定币池（精简）

Curve 一类协议擅长**相似资产**（如各种稳定币、同类衍生）之间的低滑点兑换，并围绕奖励、治理、贿赂市场（历史上 Convex 等）形成复杂生态。

新人只需记住：

- 稳定币之间也可能脱锚，池子会亏；
- “稳定”是设计目标，不是物理定律；
- 高收益往往来自代币激励——激励结束，APY 会塌。

不必背完整 bribe 战争史；进阶者再读机制。

LP 与 Token 逻辑

提供流动性（LP） 不是“存银行吃利息”那么简单：

1. 你存入资产，换得 LP 凭证（常是另一种 Token）。
2. 交易者付费，你按份额分费。
3. 两种资产相对价格大变时，你撤出的组合可能不如单纯持有——**无常损失（IL）**。
4. 若再叠加农场奖励，要把奖励代币的抛压算进真实收益。

心法：先问“没有奖励币时，这池子是否仍合理”，再问“奖励能发多久”。

TVL 怎么读?

TVL（Total Value Locked）：锁在某协议合约里的资产估值总和。媒体爱排行。

读法：

- **能参考**：规模、相对热度；
- **不能迷信**：可被循环抵押夸大、价格暴涨暴跌扭曲、同质竞争刷数；
- **要拆开看**：锁的是什么资产？能否自由退出？审计与多签情况如何?

一句话：**TVL 是体温计之一，不是体检报告全文**。

合成资产（原则级）

合成资产：用抵押与预言机，在链上追踪某种价格（股票、外汇、加密指数等）的代币化敞口。

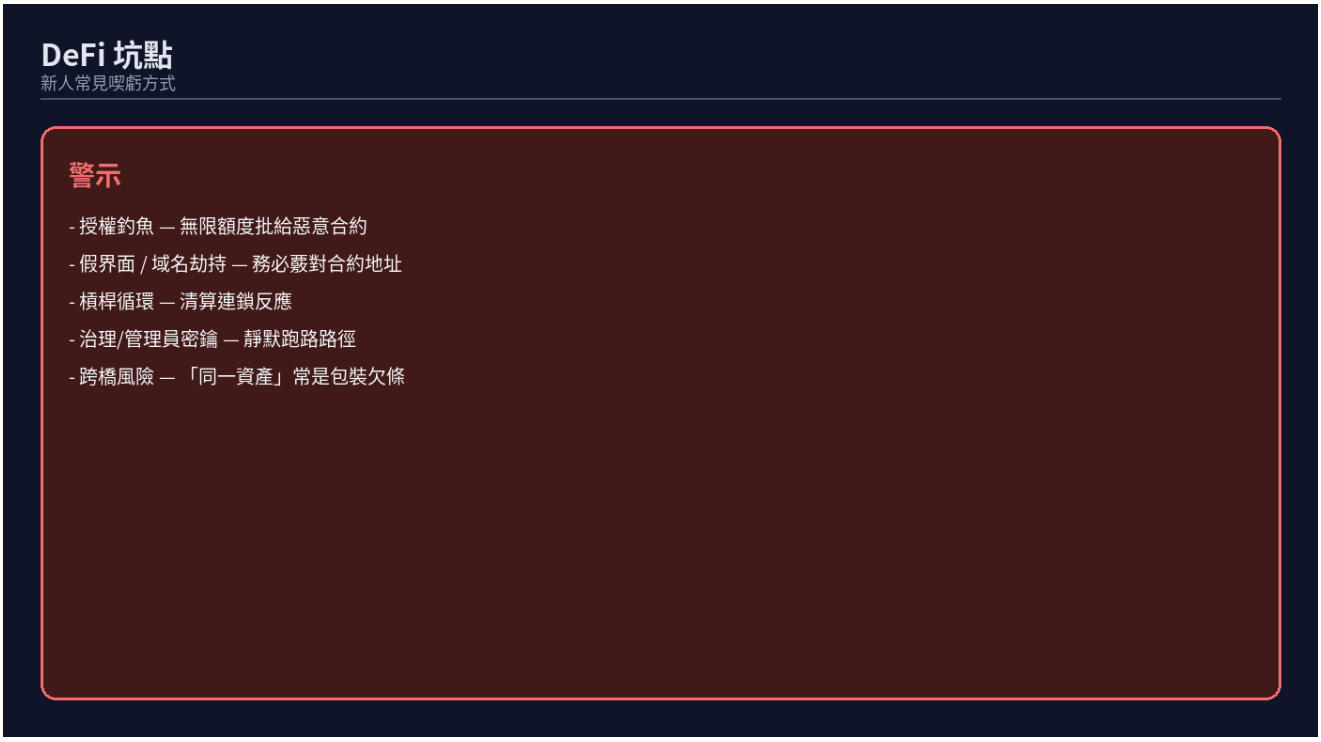
核心零件通常是：

1. 抵押品；
2. 债务/合成头寸；
3. 价格喂价（预言机）；
4. 清算与稳定机制。

难点永远在**信息输入**：链上不知道现实世界股价，除非有人喂。喂错或被操纵，合成物就会离谱。
Dai、sUSD 等各有机制权衡——评价时比“谁更去中心化、谁更抗审查、谁更依赖现实托管”，不要只

比口号。

新人防坑十条



1. 官网与合约地址多方核对。
2. 授权额度最小化；定期撤销。
3. 不懂健康因子别杠杆到满。
4. 稳定币看储备与发行人风险，不只看名字带 USD。
5. 高 APR 先假设不可持续。
6. 合约升级权限、多签、时间锁要有人解释得清。
7. 分清：本金亏损、无常损失、清算罚金、代币归零，是不同坑。
8. 不要把交易所客服、Telegram 私信当官方。
9. 税务与当地合规自己负责。
10. 可以用模拟/小额当学费；不要用生活费当学费。

稳定币：DeFi 的血，也是风险源

没有相对稳定的计价单位，借贷与交易都会抖。稳定币大致分：

- **法币抵押 / 托管型**：有公司与银行账户叙事，看储备透明度与冻结政策。
- **加密抵押型**：链上抵押更多，市场机制复杂，极端行情可能脱锚。
- **算法/混合型**：历史炸过；看见“算法保证永远 $1”请提高警报。

在 DeFi 里你换到的“USD 字样代币”并不等于银行美元。阅读时间：谁能冻结？储备在哪？预言机怎么取价？

MEV 与你的成交价

矿工/验证者/搜寻者会抢跑、夹杀、重排交易。你在钱包里看到的“预期成交”不一定是最终结果。保护动作包括：合理滑点、私有交易通道（进阶）、避免在极薄池子大额扫单。不必成为 MEV 研究员，但要知道**公开内存池不是慈善晚会**。

治理代币与“投票权幻觉”

许多协议发治理币。持有 ≠ 你能单独决定金库。真正要看：法定人数、委托、多签、紧急开关。把治理币当“分红股票”很容易失望；把它当**协调工具 + 投机品**更诚实。

实操流程示例（抽象，不指向特定前端）

1. 准备专用浏览器配置文件与钱包。
2. 确认网络与合约地址（多来源交叉）。
3. 小额兑换，确认到账。
4. 若提供流动性：计算无常损失情景（价格 ±30%/±50%）。
5. 若借贷：设定强制平仓预警，不要顶格。
6. 操作结束检查授权；不需要的撤销。
7. 记账（税务以后会感谢你）。

监管与地缘（原则）

不同国家对 DEX 前端、稳定币、质押广告态度不同。有的地区访问前端会变；有的要求 KYC 入口。本书不教你“翻墙用法币入金”，只提醒：**技术全球，法律本地**。

当我们说“聪明钱”

链上能看到巨鲸地址，不等于你该跟单。假充值、骗局盘、内部对倒都能演戏。数据分析是工具；没有情景意识就会变成反向指标。

组合风险：乐高倒塌时

DeFi 的可组合性意味着：你的收益来源可能嵌了四层——存款凭证再拿去抵押，再挖矿，再把奖励卖成另一种债。每一层都有合约风险与预言机风险。牛市里这叫“高效资本”；熊市里这叫“多米诺”。

实操建议：画一张自己的仓位依赖图。若看不清依赖，就降杠杆、减层数。协议自己的“安全模块”“保险基金”能缓冲一部分，不是无限保单。跨协议的“一键策略金库”把复杂性外包给策略人——你要额外相信策略人与其合约。

另一个隐形风险是**流动性幻觉**：账面 TVL 高，但同质资产循环质押；真要退出时滑点巨大。大额退出前用模拟或小额探测深度。

把 DeFi 当工具箱：需要兑换就兑换，需要借贷就借贷，完成目标就减少暴露。整天追求最高 APY，通常是在卖波动性与尾部风险给你自己。

常见问题（DeFi）

问：无常损失是损失本金吗?
答：是相对“只持有”的机会差，撤出时两种资产数量会变；极端行情很痛。

问：审计过就安全吗?
答：审计降风险，不消风险；还看权限模型与依赖。

问：高 APY 哪里来?
答：多半是代币补贴或高风险；补贴停就没。

问：能只持稳定币吃利息吗?
答：仍有合约、发行方、脱锚风险；利率也会变。

问：钱包显示假代币怎么办?
答：忽略；不要点假“领取”页面。

流动性、价格发现与普通人的位置

自动做市商让任何人都能提供流动性，也把做市风险从专业柜面转移到了散户 LP。你赚的是手续费与可能的奖励，付的是逆向选择：知情交易者更可能在对你不利时成交。池子越薄，大单冲击越大；池子越深，单笔手续费分成可能越薄。选择费档与区间（若协议支持集中流动性）是专业活，新手应从全区间小额或干脆只做兑换开始。

借贷市场则把利率交给供需算法。利用率高时存款利率升、借款变贵，这是特征。危险在于你同时做多某个抵押品又借出另一种资产，价格闪崩时清算机器人比你的手指快。把健康因子当作安全带，而不是挑战极限的游戏分数。

还有一类“收益聚合”帮你自动复投。它们节省时间，也放大合约与策略风险。问自己：若策略人消失，合约是否仍允许你退出？有没有时间锁？有没有管理员铸币权限？把这些问题写在笔记里，比把 APY 截图发朋友圈更负责任。

DeFi 让全球资本市场的一部分变成 24/7 的许可式积木。它没有消灭风险，只是重新分配了风险与信息。你能看见链上数据，对手也能看见你的仓位。透明是双刃剑：既便于审计，也便于猎杀。

本章收束

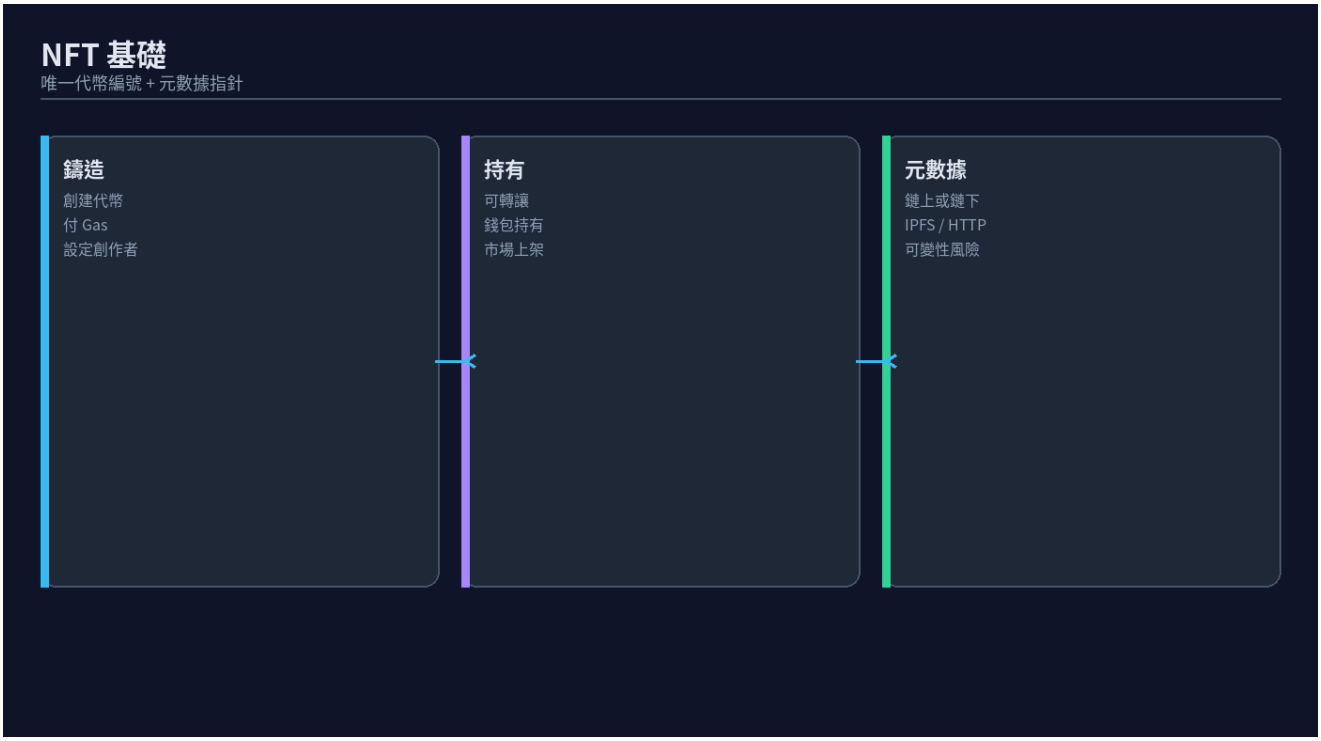
1. DeFi 是链上金融积木，核心是合约与抵押清算，不是魔法印钞机。
2. Uniswap 教你 AMM；借贷教你清算；Curve 教你“稳定也不稳定”。
3. LP 有无常损失；TVL 会骗人。
4. 合成资产的灵魂是预言机与抵押，不是名字好听。
5. 下一章 **NFT 与元宇宙**：把“独特凭证”从金融积木里拎出来，并给 2021 泡沫降降温。

（第 5 章完 · v2 原创重写 · SCDO Lab）

6、NFT 和元宇宙

SCDO Lab · Web3 新人必读指南 v2
NFT 本质是**链上非同质凭证**；元宇宙是更大、更模糊的叙事筐。
降调 2021–22 炒作；Sandbox / Decentraland 当**案例**不是“龙头必买”。**不是投资建议**。

NFT 是什么?



NFT（Non-Fungible Token，非同质化代币）：每个代币有唯一 ID，不能像 ERC-20 那样 1:1 无差别互换。常见标准是以太坊 **ERC-721**，也有 **ERC-1155** 等。

人话：NFT 更像**链上的产权编号/徽章编号**，证明“某个合约里的某个 ID 现在归这个地址”。它**不自动**等于：

- 你拥有图片文件的版权（多数时候版权另说）；
- 项目方永续运营；
- 地板价只会涨。

基础设施（你实际会碰到的）

- **发行合约**：mint（铸造）规则、版税接口、是否可升级。
- **元数据**：名字、图片链接；有的在链上，有的在 IPFS/中心服务器——服务器挂了图可能裂。
- **市场**：展示与成交的前端；同样有假站。

- **钱包**：显示 NFT、签名上架与授权。

真正说得通的用途（按靠谱程度）

1. **票务与门禁**：链上票，减少假票；仍要防黄牛与假 mint。
2. **会员与权限**：持有某 NFT 才能进社区/用功能。
3. **游戏道具与妆扮**：可交易、可携带（理想状态）；经济设计差仍会崩。
4. **证书与成就**：课程、贡献、出席证明——关键是发行方信誉。
5. **数字藏品/艺术**：文化与投机并存；多数会归零，这是市场常态。

比特币生态上的铭文等扩展，思想也是“把独特数据刻在/关联到链上资产”——标准与风险模型和以太坊 NFT 不同，另开专题更合适，此处点到为止。

泡沫教会我们什么？



2021 前后，头像小图、天价地板、名人站台、人人 mint。回撤之后剩下几条教训：

- **流动性单向**：牛市好卖，熊市无人接盘。
- **版税与平台规则可变**：创作者分成不是物理定律。
- **洗交易**可刷地板价与成交量。
- **钓鱼 mint**、假客服、盗授权，比“看错项目基本面”更快让你归零。
- **知识产权混乱**：有人卖你根本没权利卖的东西。

2026 年看 NFT，更健康的问题是：**这个凭证解决谁的什么问题？离了炒作成交，它还存在吗？**

元宇宙：概念降调版



概念

元宇宙没有统一定义。营销含义常是：持久的共享虚拟空间 + 身份 + 经济 + 可交互内容。技术拼图可能包括：游戏引擎、社交、创作者工具、支付、有时还有区块链道具与土地。

常被列举的特征（别当承诺）

- 持续在线的世界感；
- 可编辑、可创造；
- 数字身份与社交；
- 经济系统（可含链上资产）；
- 与现实场景连接（活动、品牌、远程协作）。

区块链不是元宇宙的充分条件：大量虚拟世界可以完全中心化运营。链上部分主要贡献**可验证的数字所有权与互通可能**——“可能”二字很重要，跨世界通用仍很难。

与 NFT 的关系

NFT 常被当作元宇宙里的地契、服装、门票。没有良好的世界与玩家，地契只是冷清的 JSON。反之，好游戏也可以先不上链；上链要问清：防欺诈、交易市场、开放经济是否真需要。

现实应用更 remembre 的方向

品牌虚拟发布会、远程演唱会、教育实训、工业数字孪生——这些常常**不需要**你先买一块“链上土地”。把元宇宙等同于“买地暴富”，是最误导新人的简化。

案例：The Sandbox 与 Decentraland（不是龙头安利）

二者都是较早把**可交易虚拟土地/体验**和加密钱包结合起来的项目，曾在舆论上被称作“元宇宙代表”。

应该怎么读案例：

维度	观察点
产品	是否还有人在里面创作与活动?
资产	LAND 等 NFT 的用途是游戏内生产还是纯炒?
公司/基金会	规则谁定？地图谁扩？
周期	热度随大盘与叙事起伏——回落不奇怪
教训	虚拟地产估值模型极脆弱；流量获取成本高

v2 **明确**：它们是学习样本，不是“2026 必买二元组”。同类世界还有很多，有的更偏链游，有的更偏 UGC 平台。选世界看内容与社区，不看谁上过最多头条。

新人实操清单

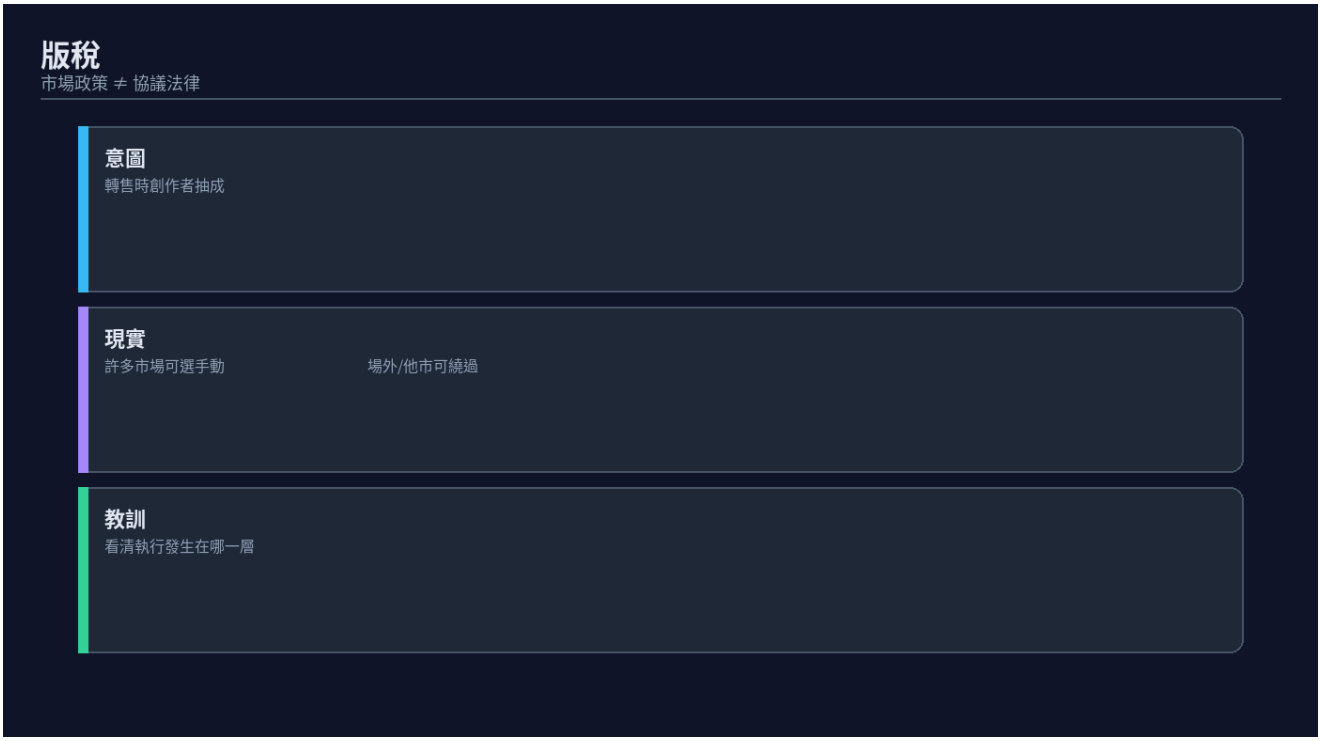
1. 分清：**收藏偏好** vs **投机**；后者按归零准备心态。
2. mint 前查合约、供应量、是否免费 mint 陷阱（授权盗币）。
3. 图片要问托管：IPFS？中心化 URL?
4. 勿信“地板价机器人稳赚”。
5. 元宇宙地产：先问你会不会用，再问会不会涨。
6. AI 生成图 + NFT：确权与原创争议更大，买前读许可。

元数据与“图裂了”问题

买 NFT 时你常买到的是：合约里的 tokenId + 指向元数据的链接。若图片存在项目方服务器，服务器关机图就裂。IPFS / 链上数据更耐审查，但不是无限免费硬盘。问卖家/文档：**元数据冻结了吗？备份策略是什么?**

版税（创作者分成）曾被市场当作默认，后来部分市场变成可选——创作者与平台博弈仍在继续。别把“永远收版税”写进你的财务幻想。

版税、许可证与版权



链上转移 ≠ 版权自动给你商业使用权。要看项目的许可证（能否二创、能否商用）。AI 生成的图铸造后，版权归属更混乱——诉讼与平台政策都在演化。收藏与商业使用前读条款。

身份类 NFT 与“灵魂绑定”

有些凭证设计成不可转让（或难转让），用于声誉、资格、出席。好处是减少纯炒；坏处是隐私与歧视风险（灵魂绑到地址上可能被追踪）。好的设计会考虑：**最小披露、可撤销、可刷新**。

元宇宙落地检查表

如果你的团队真要做“世界”而不是讲故事：

1. 帧率与操作手感是否达标?
2. 创作者工具是否让普通人能做内容?
3. 经济是否离开代币补贴还能转?
4. 身份是否跨场景有用，还是只有地皮 JPG?
5. 审核、儿童保护、骚扰处理有没有方案?

答不上来，就还是营销元宇宙。

与品牌 / 票务的务实结合

2026 年更常见的成功像是：演唱会票防伪、会员年证、数字藏品作为活动纪念品——**小而清晰的权利**，而不是“买地成为数字房东”。SCDO 视角同样：凭证要服务可验证事件，不做空泛地产神话。

社区、身份与“头像文化”之后

头像 NFT 曾是社交货币：进群、拿白名单、互相识别。热潮退后，留下的是更朴素的问题——**数字身份如何低成本验证**而不必每次 KYC。票务、会员、活动徽章、课程结业，都可以用 NFT 或可验证凭证表达。成功标准变成：核销流畅、造假困难、用户不必懂私钥也能在托管或智能钱包辅助下完成（同时理解托管代价）。

对艺术家：链上拍卖降低地理门槛，也带来平台分成与抄袭。保护自己需要水印策略、原创存证、法律顾问，而不只是“先 mint 再说”。对品牌：小规模凭证实验优于空投几十万张无人使用的图。

元宇宙话语若还要沿用，请改口为“持久多人在线世界 + 可选链上资产”。用词诚实，能过滤掉一半融资话术。

常见问题（NFT）

问：地板价上涨说明优质吗?
答：不一定；可能洗交易或流动性瞬态。

问：图在 OpenSea 上就是我的版权吗?
答：通常不是自动版权转让。

问：免费 mint 一定亏吗?
答：不一定，但常是授权钓鱼；看钱包提示。

问：元宇宙地热能买吗?
答：先当娱乐/实验预算；别当刚需房产。

问：怎样送 NFT 给朋友?
答：确认网络与地址；小额测试。

市场结构与创作者谈判权

NFT 市场的竞争一度围绕费用与版税开关。创作者希望二次销售分成；交易者希望摩擦低；平台希望占份额。结果是政策反复。对创作者，更稳的收入来自一级销售、委托创作、品牌合作，而不是假设永续版税。对收藏者，要分清你买的是：社群门票、艺术偏好、还是接盘投机券。三者可以重叠，但亏损时的心理账户不同——叠在一起最容易自我欺骗。

博物馆与机构开始尝试链上典藏编号时，重点往往是溯源与教育，不是地板价。这种用例值得关注：它把 NFT 拉回“凭证”本意。游戏与票务同理。一旦离开交易屏的多巴胺，NFT 的长期价值取决于线下/线上权利能否兑现：能否入场、能否兑换、能否升级。买之前把权利说明书读完；没有说明书就当成纯装饰。

关于元宇宙地产：可建造性、访问量、互操作标准决定了地皮是舞台还是荒地。把地皮切成大量 NFT 便于炒作，却不自动产生观众。观众来自内容与社交，内容来自工具与激励，激励若只有通胀代币，观众来了还会走。把预算花在关卡与活动运营上，通常比花在“多买两块虚拟街角”更接近正经生意。

从投机屏回到使用权

当成交量下降，真正留下来的 NFT 用法几乎都跟**使用权**绑定：门禁扫描成功、票根核销、会员权益解锁、游戏内装备可用。把这当成设计北极星，比盯着稀有度表格健康。发行方应公布权益期限、转让后权益是否迁移、失败退款规则；收藏者应把这些条款当购前必读，而不是事后维权口号。

技术上，动态 NFT（元数据可更新）适合游戏状态与会员等级，但也引入中心化开关：谁有权更新？更新是否留下链上痕迹？静态 NFT 更简单，却难表达成长。选择取决于场景，不存在一律正确。

跨链 NFT 与“包装桥接”增加了映射错误与假桥风险。能在一条你理解的网络上用完权益，就不要为了炫耀多链而频繁桥接。教育用户时，用“票在哪座城市的剧院”类比网络选择，往往比讲底层跨链消息传递更有效。

对 SCDO 一类强调可验证记录的团队，NFT/凭证应优先服务**事件发生过的证明**（参赛、结算、成就），而不是制造新的地产幻觉。证明要可验证、可过期、可隐私保护——三者常需权衡，写进产品说明比写进口号重要。

合规展陈与未成年人保护

当 NFT 进入校园、美术馆或面向未成年人的活动时，内容分级、隐私同意、监护人授权会比链上技术更先碰到墙。教育向凭证应避免强制公开地址与现实身份的硬绑定；能做选择性披露更好。商业活动则要处理发票、消费者撤回权与虚假宣传——“永久升值”一类用语是雷区。把法律顾问请进设计阶段，比事后删推特便宜。

国际展览跨司法辖区借展数字作品时，授权链与铸造权要事先厘清，以免出现“同一个 tokenId 两套权利叙事”。标准化还在路上；在此之前，合同仍是主语言，链是附件。

本章收束

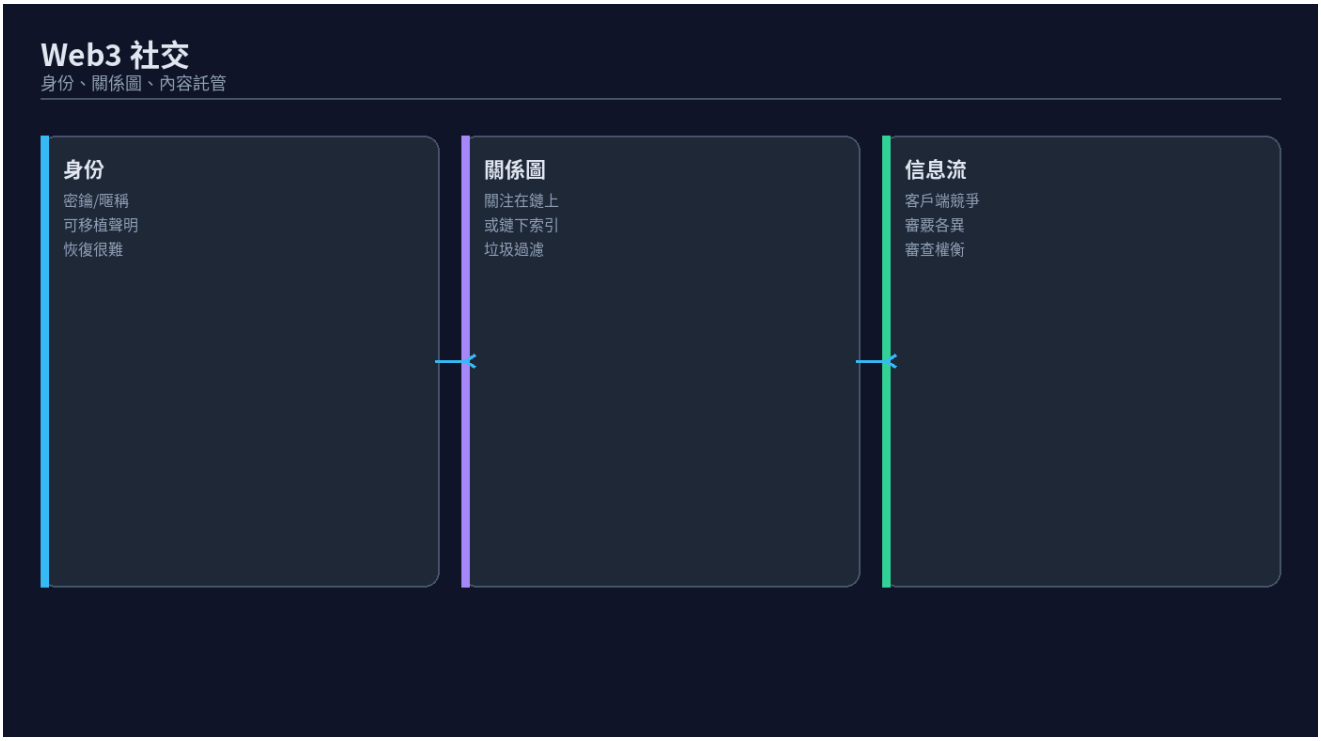
1. NFT = 独特链上凭证；用途大于头像投机。
2. 泡沫证明：无用需求的高估值不可持续。
3. 元宇宙是筐，区块链只是可选零件。
4. Sandbox / Decentraland 可作案例，不作必买名单。
5. 下一章 **去中心化社交**：当帖子与关注关系也想上协议时，联邦、Lens、Nostr 各自妥协什么。

（第 6 章完 · v2 原创重写 · SCDO Lab）

7、去中心化社交

SCDO Lab · Web3 新人必读指南 v2
社交想“上协议”时，争的不是多一个 App，而是：**关系与内容是否可携带、谁能封你、数据存在哪**。
压缩原稿上下两篇长文；讲清 **联邦 ≠ 完全去中心化**。**不是投资建议**。

Web3 社交是什么?



Web2 社交：账号在平台，粉丝与帖子基本锁在平台，规则由公司改。
Web3 社交尝试把一部分身份、关注关系、内容索引放到**开放协议或用户可控存储**上，让应用变成可替换的“客户端”。

理想画面：换前端不失社交图谱。
现实画面：体验、审核、发现、反垃圾仍很难；很多产品仍是“钱包登录的 Web2”。

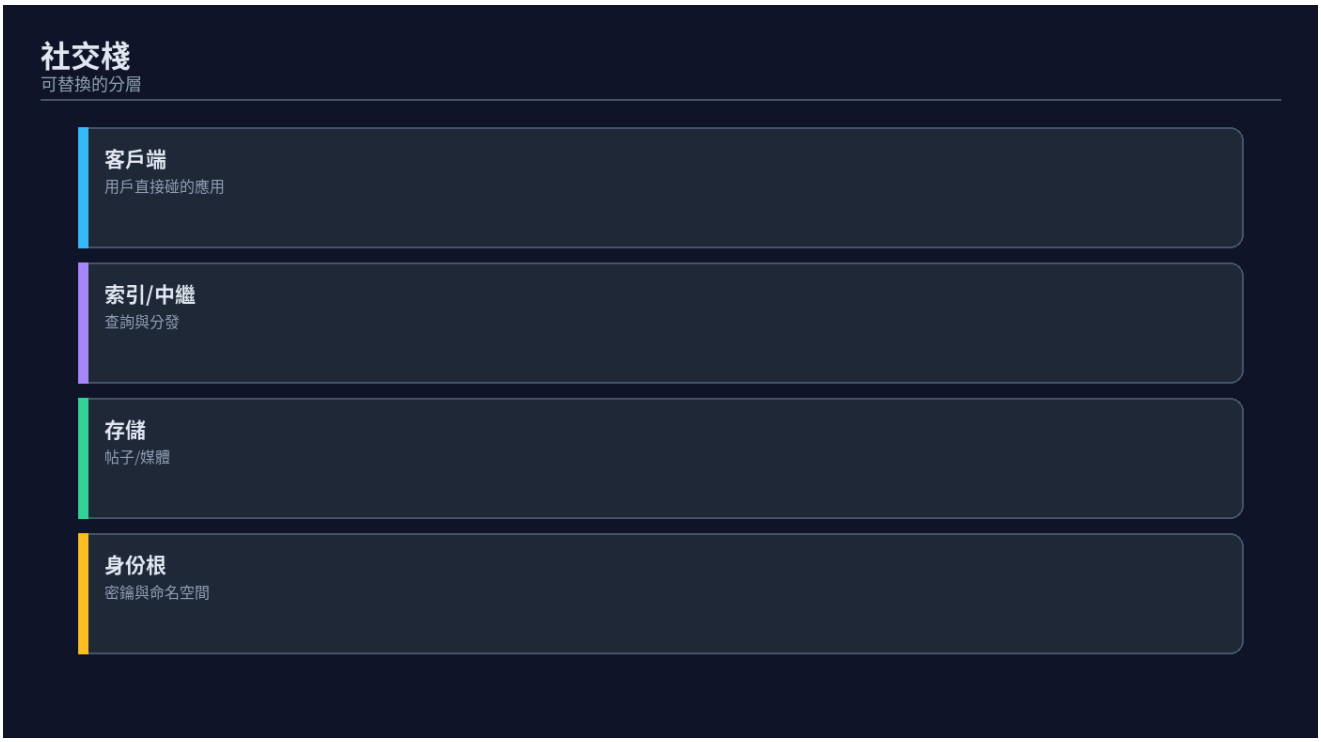
简史（极简）

从论坛、博客到巨头信息流，中心化带来增长也带来锁定与审查争议。区块链火了之后，出现“链上社交”实验：把关注关系上链、用 NFT 当门票、用代币激励发帖——有的做出产品，有的只做出行情。2026 年更冷静：协议层（图谱、中继）与应用层分开看。

如何进入（低风险）

1. 先当读者：弄清某产品用的是哪套协议。
2. 用小额或空账号试验；别一上来绑定主钱包大资产。
3. 分清：**链上写入**（贵、慢、永久）vs **链下存储 + 链上指针**。
4. 预设：跑路、停服、协议迁移都可能发生——可携带程度要实测。

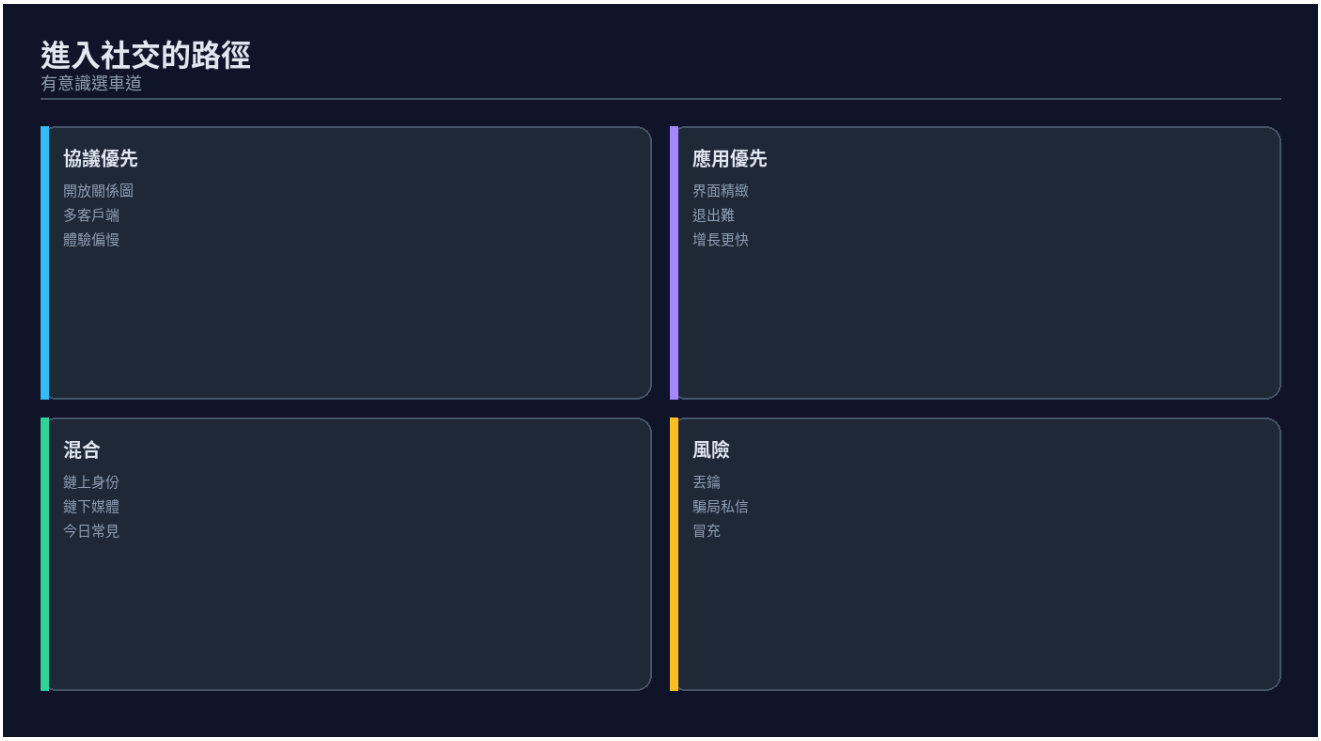
生态分层：基础设施 / 中间件 / 应用 / 工具



层	干什么	新人怎么碰
基础设施	公链/L2、身份、存储、可用性	一般间接使用
中间件	社交图谱协议、索引、通知、权限	决定“能不能搬家”
应用	你刷的客户端、创作者工作室	每天打开的那个
工具	分析、反钓鱼、跨前端导入	安全与迁移用

选产品时倒着问：应用好看吗？→ 中间件开不开？→ 基础设施贵不贵、审查点在哪？

三条路线对比（Lens / Mastodon / Nostr）



Lens 一类：链上社交图谱协议

- **想法**：关注、发帖等关系尽量协议化，多个客户端可共用图谱。
- **体感**：常要钱包签名；链上/近链操作影响费用与节奏。
- **注意**：协议开放 ≠ 某一前端去中心化；NFT/代币激励可能引入投机噪音。

Mastodon：联邦宇宙（Fediverse）

- **想法**：很多独立服务器（instance）用共同协议互通，像电子邮件域名。
- **关键澄清**：**联邦 ≠ 无管理员**。每个服务器仍有人管规则、封禁、存你的数据。你是“换邮局”，不是“没有邮局”。
- **适合**：反感单一全球公司审核、愿选社区服务器的人。
- **代价**：发现内容更碎；服务器寄宿风险（管理员作恶或关停）。

Nostr：密钥身份 + 中继

- **想法**：身份≈密钥对；消息发到多个中继（relay）；客户端各异。
- **体感**：更“密码学原生”；垃圾信息与发现依赖客户端与中继质量。
- **注意**：私钥丢了≈身份丢了；中继可拒绝服务——抗审查是程度问题。

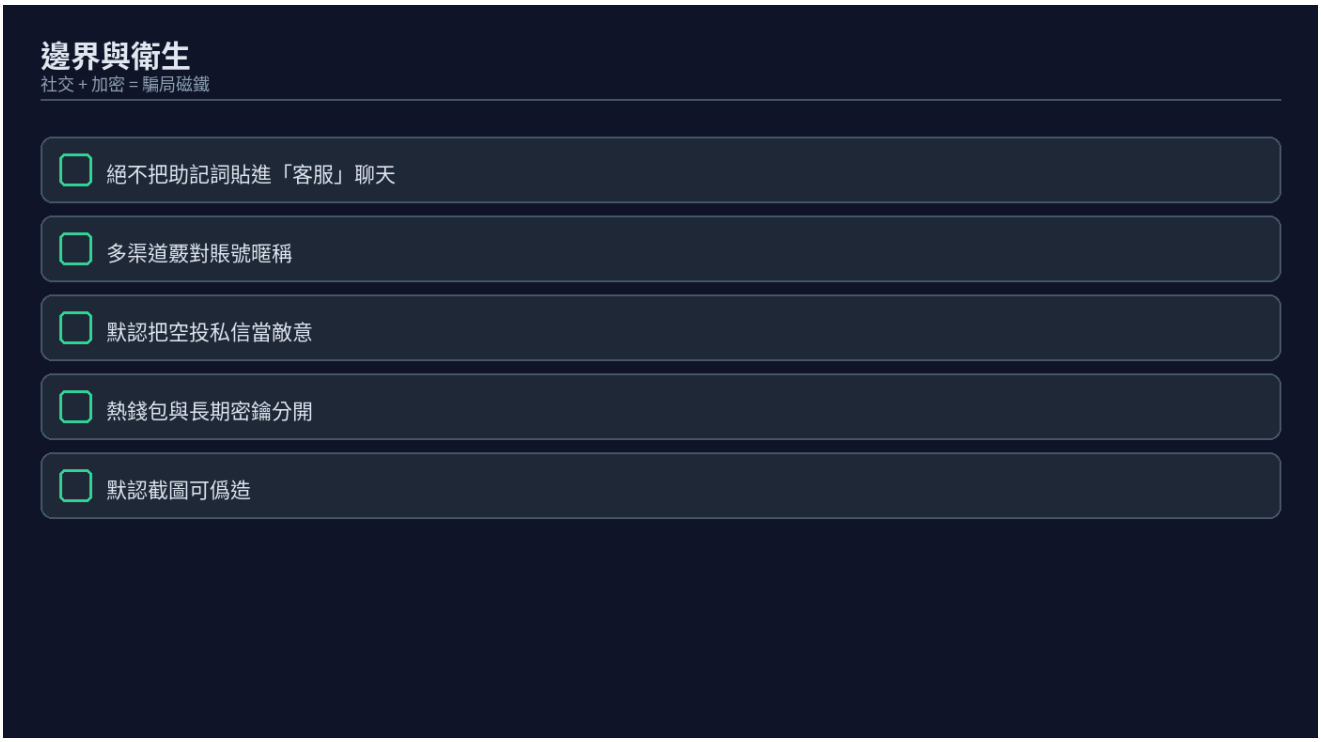
一张对照

	Lens 类协议	Mastodon 联邦	Nostr
身份	常绑钱包/剖面 NFT	服务器账号	公私钥
搬家	看协议与客户端	看服务器导出/互通	换客户端较易，中继列表要自己维护
去中心化要点	链与治理假设	多服务器，非零管理	多中继，非自动永续

	Lens 类协议	Mastodon 联邦	Nostr
主要摩擦	签名与费用/复杂	选服与碎片	垃圾与密钥安全

还有 Farcaster 等“足够去中心化 + 强产品”路线：混合链上身份与链下消息——读白皮书时抓**数据可用性与审查点**即可。

趋势与边界（2026）



值得期待的： 可验证凭证进社交（出席、贡献、抗女巫的弱信号）；客户端竞争；钱包签名 UX 改善。
别幻想的： 明年就全面替代超级 App；无审核的高质量广场自动出现；代币激励单独能养出健康公共讨论。

安全： 私信“客服”、签名授权、假空投在社交场景极密——第 9 章通用。
SCDO 轻提： 社交图谱若服务真实社区，需要可审计的权限与反滥用，而不是只发积分。Agent 自动发帖更要额度与日志。

反垃圾与女巫：开放协议的税

开放写入后，垃圾与刷量会来。Web2 用中心算法与人力；Web3 社交常用：质押、邀请、人机验证、客户端过滤、信誉分数。每种都引入新的中心或新的歧视。**完全无审核的全球广场**与**高质量对话**很难兼得——产品必须显式选择。

内容存储策略

- 全文上链：贵、永久、难删（某些场景是特性）。
- 链下存储 + 链上哈希：便宜，依赖存储网络或公司。
- 仅中继互传：更快，持久性看中继政策。

做创作者时要想：哪份副本是你在意的“正本”？

创作者经济的诚实账

代币打赏、粉丝币、内容 NFT 都能讲故事。可持续的创作者收入仍多来自：赞助、会员、广告、现场——链上工具是增益，不是自动财务自由。把粉丝关系锁在单一投机币上，币价崩时社群一起崩。

隐私

假名地址仍可能被聚类分析。社交图谱上链会让关注关系更透明，也可能更易被盯梢。需要隐私时：分开身份地址、减少链上社交绑定、了解ZK与混合网络等进阶工具（有学习成本）。

产品选择流程

1. 我要的是“反巨头”还是“更好玩的信息流”？
2. 能否导出或在第二客户端再现我的关系?
3. 私钥丢了有没有社会恢复?
4. 审核争议时我站哪边——选服务器/协议要符合价值观。
5. 我是否用主钱包登录了高风险实验客户端?

与新闻/治理的交叉

DAO 投票、论坛、快照类工具常和社交身份联动。警惕：**买票、刷量、委托集中**。链上治理不是自动民主，只是换了一套可统计的规则。

审核、价值观与“协议中立”神话

协议宣称中立，客户端仍可过滤；中继仍可拒绝；服务器仍可封禁。用户要的其实是**可预期的规则**与**可迁移的出口**，不是抽象绝对中立。当你加入某个联邦服务器或使用某个客户端默认屏蔽列表，你已经站队。这很正常——关键是规则是否公开、是否滥权、你能否带着关系离开。

另一个现实：名人与机构仍可能选择入驻更中心化、更好审核的产品，因为品牌安全。Web3 社交不会自动成为唯一公共领域；它会是多元中的一元。能接受这一点，讨论才不会变成宗教战争。

对建设者：先做小社区的高质量工具，再谈全球取代。对用户：用小号实验，主身份谨慎绑定。

常见问题（社交）

问：钱包登录等于去中心化?
答：只是登录方式；内容与审核可能仍中心化。

问：服务器没了怎么办?
答：联邦场景看你有无备份/迁移；选服要谨慎。

问：Nostr 私钥丢了?
答：身份难找回；提前多设备策略与社交恢复思路（若客户端支持）。

问：该不该把主钱包连社交 DApp?
答：建议专用地址。

问：链上发帖太贵?
答：多数方案把内容放链下或 L2。

协议社交的产品度量

衡量 Web3 社交，别只用代币价格。更有信息量的指标包括：日活地址里有多少是真人交互、客户端切换率、迁移成功率、被滥用率、创作者重复发布率、用户是否愿意把该身份用于现实活动验票。难测并不等于可以忽略——测不了就不要吹“已经取代”。

治理型社群把论坛与投票结合时，要设计反贿选与反冷漠：委托、乐观治理、一址一票与一人一票的折中，各有坑。社交身份与投票权绑太紧，会导致买号；绑太松，又难抗女巫。没有完美公式，只有不断修订的规则与公开的修订记录。

对普通人，最实用的策略也许是：**主社交仍在你已熟悉的网络，实验社交用小号与专用钱包**。等某协议证明迁移与审核都可接受，再逐步提高绑定。把所有社会网络迁到实验协议，像把所有存款放进实验合约，勇气可嘉，风险不对等。

客户端竞争与开放图谱的未来

若图谱真在开放协议上，客户端理应像电子邮件客户端一样竞争：更好的通知、更好的反垃圾、更好的创作工具。现实中流动性仍可能集中在一两个前端，因为网络效应对“发现内容”极强。开放协议降低了锁定的法律与技术上限，但不消灭锁定的经济诱因。作为用户，偶尔试用第二客户端，是保持退出权的健身动作。

开发者则为索引成本与写入成本发愁：全链索引贵，自建索引又变成新的中心。社区公共索引、可验证同步、轻客户端证明，都是正在进行的工程题。你可以不会写这些组件，但要能听懂：当你的时间线“读不到最新”，到底是中继问题、索引问题还是审查问题。把故障归对类，才不会乱换助记词或乱授权。

最后，社交与金钱刺激混装时，关系会被金融化：关注变成投资，回复变成市场动作。适当的分隔——例如专用“金融身份”与“闲聊身份”——能减少人格被价格侵蚀。这不是道德说教，是心理健康的风

险管理。

模块化身份：从单一巨头档案到可拼装证明

未来更可能出现的不是“一个去中心化脸书通吃”，而是可拼装的身份模块：登录器、信誉证明、可验证凭证、加密收件箱各由不同协议提供，前端负责编排。用户体验的胜负仍在编排质量。SCDO 强调的可验证记录，适合嵌在“信誉/成就”模块，而不是妄想重做整个信息流。建设者应选择窄切口做深，用户应避免把所有模块绑死在同一热钱包。

危机沟通与谣言

去中心化社交在危机时既快也乱：官方声明与假冒声明并行，截图脱离上下文传播。项目方应预置多通道验真（链上留言、已知密钥签名的通告、多个镜像站）。用户应等待可验证声明，而不是第一时间转发刺激性截图。训练这种习惯，比任何反钓鱼插件更能保护社群资产。

小结补丁

协议社交的胜负手是迁移成本与反滥用，不是口号。先小号，后绑定；先第二客户端，后全迁。

本章收束

1. Web3 社交争的是可携带与少单点，不是多一个皮肤。
2. 分层看：应用漂亮，不等于协议开放。
3. 联邦有管理员；Nostr 靠密钥与中继；链上图谱有费用与治理假设。
4. 2026 仍是实验场；先小号试验。
5. 下一章 **GameFi**：游戏经济上链的动机、失败模式与产业图——去掉“热度飙升”。

（第 7 章完 · v2 原创重写 · SCDO Lab）

8、GameFi

SCDO Lab · Web3 新人必读指南 v2
GameFi ≈ 游戏 + 金融激励（代币/NFT 经济）。好玩与好赚经常打架。
去掉“热度飙升/爆发式增长”口气。
不是投资建议。

GameFi 与 DeFi 有什么关系?



- **DeFi**：金融积木本身（兑换、借贷、做市）。
- **GameFi**：用游戏循环（任务、对战、养成、地产）驱动人来持有、消耗、交易代币与 NFT；底层常复用 DeFi 的池子、市场与桥。

人话：DeFi 是交易所与当铺；GameFi 想做“边玩边参与经济”。失败时，看起来像游戏，内核却是高通胀庞氏——分得清很重要。

由来（极简）

链游早年从收藏品与简易玩法起步；某阶段“打金”模式吸来大量劳务型玩家，也吸来崩盘。之后行业更多谈 **Play-and-earn / Play-to-own**、链下结算 + 链上资产、以及“先好玩再谈代币”。

游戏为什么要上链?



说得通的理由：

1. **资产可携带**：道具/角色不以单一服数据库为唯一真相（理想状态）。
2. **交易透明**：二级市场规则更公开（仍有假货与钓鱼）。
3. **开放经济**：第三方可做工具与市场（也带来机器人与剥削）。
4. **可验证随机/结算**：部分玩法需要公开可查的结果。

说不通的理由：

- “上链就会更好玩”；
- “发币就能冷启动永久通胀繁荣”；
- “元宇宙地产必然升值”。

常见类型

类型	特征	风险摘要
打金劳务型	时间换代币	代币跌、新人群不够就塌
收藏竞技型	NFT 角色/皮肤 + 对战	地板价泡沫、匹配质量
UGC 沙盒型	用户造内容/地皮	流量与工具门槛
链下游玩+链上结算	体验在传统客户端	桥接与托管复杂度
赌场换皮	高赔率“游戏”	监管与公平性质疑

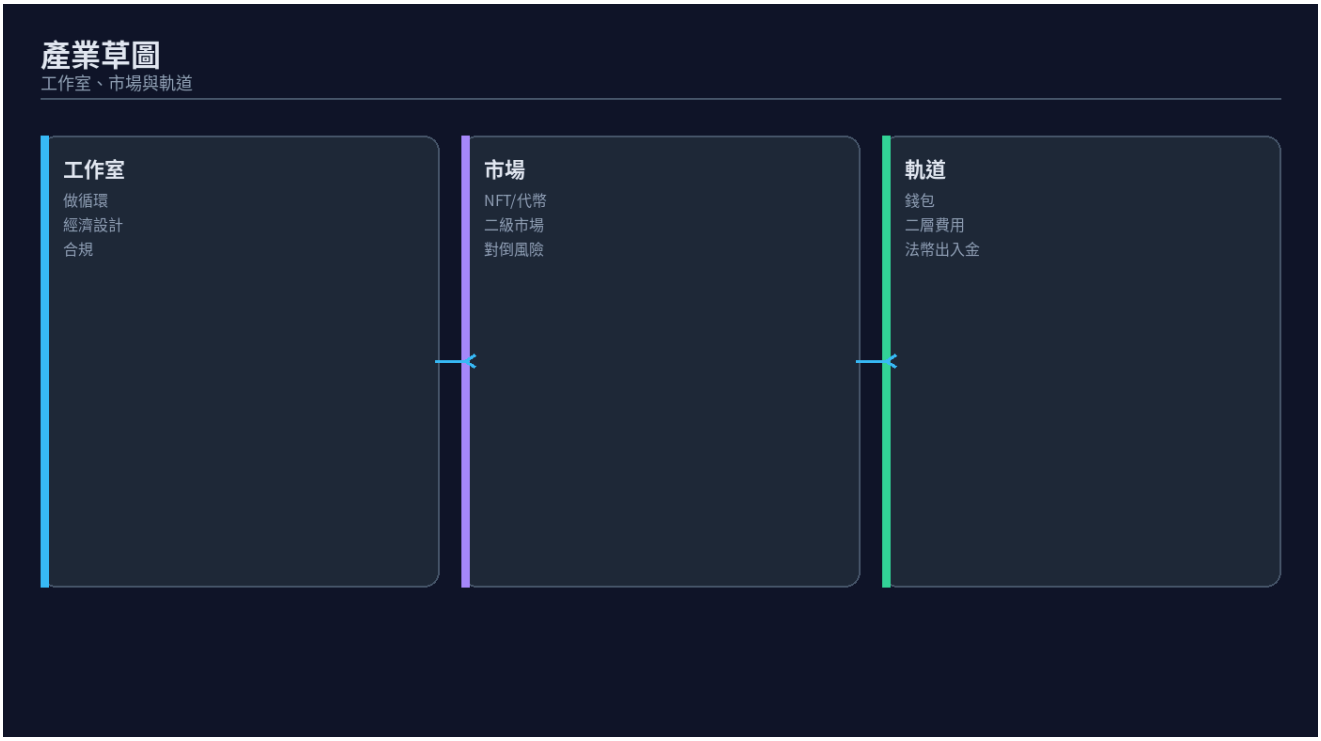
可持续性：先看死亡螺旋

健康游戏：乐趣 → 自愿付费/交易 → 经济平衡。
脆弱 GameFi：奖励代币 → 卖盘 → 物价崩 → 玩家撤离 → 只剩图表。

设计问题时问：

1. 没有代币奖励，还有人玩吗?
2. 消耗（sink）是否跟得上产出（source）？
3. 公会/工作室是否垄断产能?
4. 资产是效用还是纯投机券?

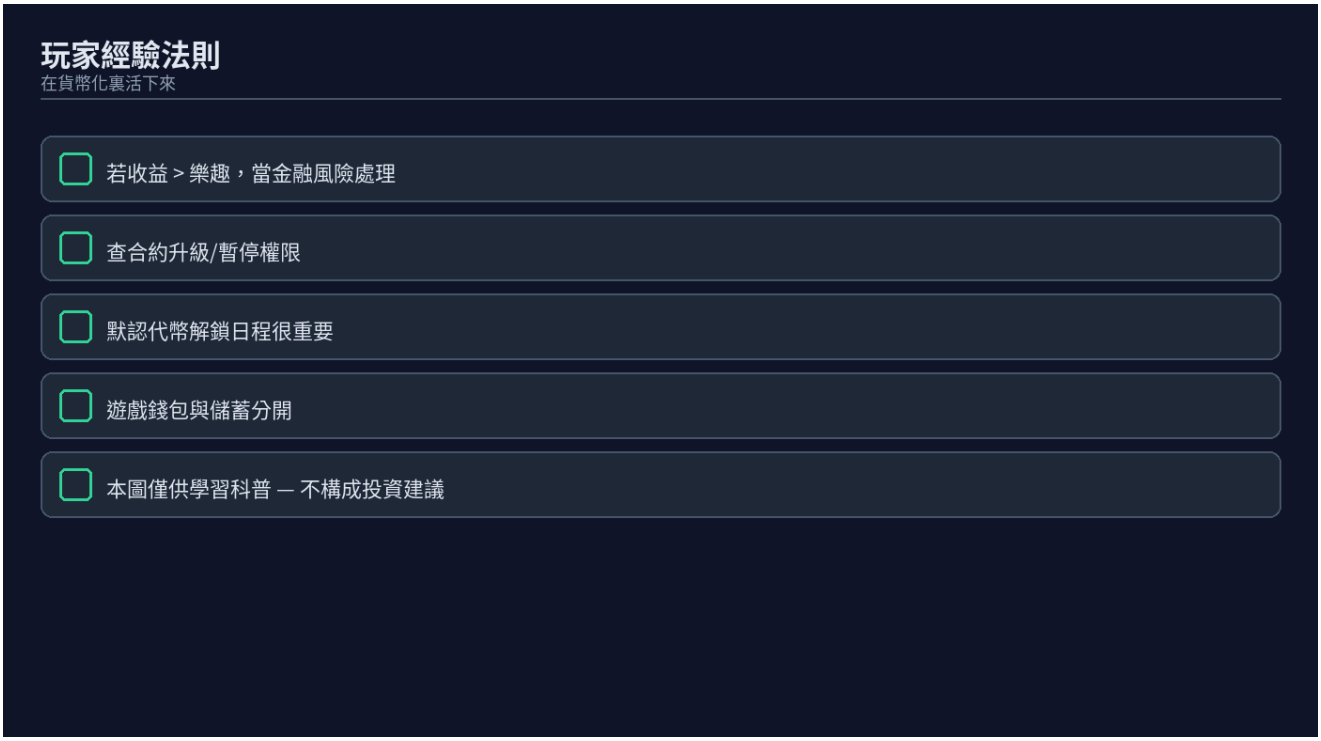
2026 生态产业图（示意，不点名安利）



玩家 / 公会
↓
游戏客户端与引擎 ← 发行商 / 工作室
↓
链上资产（NFT/代币）← 市场、桥、钱包
↓
公链 / L2 / 专用应用链
↓
流动性与金融服务（兑换、借贷—慎用杠杆打金）

外围还有：数据分析、反作弊、安全审计、合规咨询、创作者工具。
名单会过时；看角色不看去年的“必玩榜”。

新人守则



1. 先试玩再谈赚。
2. 打金收益按“归零”做压力测试。
3. 批准游戏合约权限要极省；专用小号钱包。
4. 警惕“稳赚日化”“内部号开盲盒”。
5. 注意当地对博彩与代币游戏的监管。

经济设计入门词

- **产出（Source）**：任务奖励、打怪掉落、挖矿。
- **消耗（Sink）**：修理、合成、门票、销毁。
- **软顶/硬顶**：通胀是否有上限。
- **赛季制**：定期重置减轻永久通胀。
- **双币/多币**：治理币与游戏币分离——复杂，也可能让玩家更糊涂。

好设计像城市交通：有来有回；坏设计像发传单式印钞。

公会、工作室与劳动

打金时代公会组织劳动力、分割设备与账号。这能提高效率，也会让个人玩家变成金字塔底。进入任何“团队带练”前看清合同：谁持有私钥、收益怎么分、退出谁负责安全。

技术架构常见选择

1. **全上链**：透明但贵、慢，适合强结算弱操作。
2. **连环大世界 + 资产上链**：手感好，信任服务器 + 桥。
3. **应用链**：自定义性能，安全与流动性自建。

没有银弹。问用户被盗或停服时，资产申索路径是什么。

监管雷达

部分玩法接近博彩或证券发行。不同国家定义不同。做发行或大规模拉新前要有法律意见——本书只做教育警示，不提供结构规避。

健康参与清单

- 预算：娱乐预算，不是房租。
- 钱包：专用。
- 时间：防沉迷，打金极易异化成打工。
- 信息：官方渠道，防Discord盗号。
- 退出：预设“跌掉多少就停”。

从玩家到建设者的边界

若你是工作室：先做 30 分钟好玩的垂直切片，再设计代币。经济顾问与玩法设计师要同桌，而不是代币先上线玩法后补。若你是公会：把安全培训写进制度，禁止要求成员上交种子。若你是投资者（高风险）：把 GameFi 代币当早期创业股权的高波动替代品，而不是工资。

链游的内容生产管道（美术、关卡、活动运营）成本不会因为上链而消失。区块链只替换了部分资产与结算假设。忽略内容成本的项目，最终只剩浏览器里的价格图。

与 SCDO 相关的产品实验若存在，应以公平竞赛、可验证成绩与娱乐本身为卖点，而不是“保证赚”。

常见问题（GameFi）

问：打金还能做吗?
答：当作高风险短工，默认收益曲线向下。

问：游戏 NFT 地板崩了?
答：先问还有没有人玩；没玩法支撑的价格难回。

问：公会要收我助记词?
答：拒绝；那是红线。

问：链游一定要代币?
答：不必；可先 Web2 账户 + 可选链上资产。

问：如何看工作室是否认真?
答：看更新频率、可玩版本、经济透明，不看路线图形容词。

内容管道、反作弊与直播时代

链游若依赖直播与网红获客，经济系统会被“曝光脉冲”冲击：来一波，砸盘一波。设计赛季与区域服，可以平滑脉冲，但也分割流动性。反作弊在有赏金的游戏里更难：自动化脚本、多开、工作室工作室化，会逼你做设备指纹或 KYC——那又与“无许可”叙事冲突。团队必须提前决定：你更怕工作室，还是更怕 KYC 流失的意识形态用户？两边都讨好通常两边都失望。

美术与音乐资产的版权、模组生态、UGC 分成，决定沙盒能否活。链上版税自动分账听起来美，实际要对接法币税务与未成年人保护。游戏行业老问题不会因为 Solidity 而消失。区块链擅长的是硬结算与开放市场；不擅长的是让关卡自动变有趣。

给你一个写作与评审时的口令：看见白皮书先翻“乐趣循环图”，没有就离远点；先翻代币分配图而没有乐趣循环的，多半是金融产品穿了游戏皮。

赛季、地区服与经济实验伦理

赛季制允许设计师重置通胀，却可能打击长期收藏者；解决方案包括跨赛季化妆品、成就灵魂绑定、或可继承的战绩凭证。地区服降低延迟与合规复杂度，却切割流动性与公会版图。公布经济实验时，应像药品试验：假设、样本、失败标准、是否回滚。把玩家当小白鼠却不告知，是伦理与商业的双重减分。

电竞化链游还要处理奖金托管与作弊争议：奖金放在多签还是合约？裁判是否中心化？录像与随机种子如何公示？这些题解不好，代币再漂亮也只是周边。

对打金劳动者密集的地区，外部分析常忽略汇率、电力与设备折旧。若你的经济模型依赖某地廉价劳动力永续，模型本身就脆弱。更可持续的方向是：本地玩家为乐趣付费，劳务型产出只是边缘——而不是反过来。

数据、匹配与观赛体验

匹配不公会摧毁竞技链游；随机种子可验证能减少“暗箱爆率”疑虑，却解决不了匹配分算法本身。观赛侧需要延迟、解说权限、精彩回放版权——这些几乎都在链下。把“可验证成绩单”铸成凭证发给选手与观众，是链能加分的地方；强行把每一帧操作上链，则是性能灾难。选对上链边界，是成熟团队的标志。

从 Demo 到长线运营的里程碑

建议内部里程碑：可玩 Demo（无币）→ 小规模测试网经济 → 主网限量资产 → 开放经济。每一步设失败即停条件：留存低于阈值、通货膨胀超阈值、重大安全事故。公开里程碑能过滤只想要“一键发币”的合作方。长线运营还要客服、反作弊轮班、活动日历——这些编制写进预算，才会少一点“突然停更”。链上金库透明度可做月报：收入、销毁、金库余额，用浏览器可核。透明不保证成功，但不透明几乎保证失信。

补强：代币分配与解锁日历

读 GameFi 项目先读分配：团队、投资人、生态、玩赚预算各占多少，解锁是否与内容里程碑挂钩。前线解锁砸盘是常态风险。没有日历的“公平发射”叙事也要看流动性与做市。把分配表当作可能伤害玩家体验的武器库——设计者慎用，玩家慎入。

本章收束

1. GameFi 嫁接游戏与金融；好玩与好赚常冲突。
2. 上链服务资产与透明，不自动提高乐趣。
3. 盯通胀与消耗，勿信永恒打金。
4. 2026 看产业角色，不背过时榜单；遵守合规与教育边界。
5. 下一章 **安全**：黑暗森林的防盗、钓鱼与授权——比追空投更救命。

（第 8 章完 · v2 原创重写 · SCDO Lab）

9、安全警钟长鸣

SCDO Lab · Web3 新人必读指南 v2
链上世界常被称作“黑暗森林”：默认有人想骗你签名、骗你授权、骗你导出助记词。**不贴第三方安全厂商长文**；不固化“11 款插件安装量榜”。讲原则与习惯。**不是投资建议**。

为什么特别危险?



1. **交易难撤销**：错了常常就是错了。
2. **签名权限极大**：一次盲签可能等于把钱包倒空。
3. **假网站成本低**：广告、抄袭 UI、仿造域名。
4. **社会工程升级**：假客服、假招聘、假恋爱、假 AI 助手。
5. **组合风险**：桥 + 授权 + 恶意代币 + 钓鱼环环相扣。

目标不是吓退你，而是让你建立**肌肉记忆**。

攻击者常见手法（地图）



类型	样子	防御要点
钓鱼网站	搜索广告/假链接超像真的	手输官网、书签、核对证书与域名
假空投/假 mint	“免费领”但要 approve	看清授权额度与合约
盗版扩展/钱包	山寨钱包应用	只从官方渠道，核对发布者
假客服	私信“帮你退款/解冻”	官方不会先要助记词
地址投毒	转账记录里混进相似地址	每次核对前后几位，用地址簿
恶意 RPC/Wi-Fi	网络劫持	敏感操作避免陌生网络；硬件钱包
合约后门	项目方或依赖库作恶	限额、分钱包、看审计仍不迷信
NFT 诈骗	盗图、假地板、索要报价签名	不乱签；懂 listing 签名含义

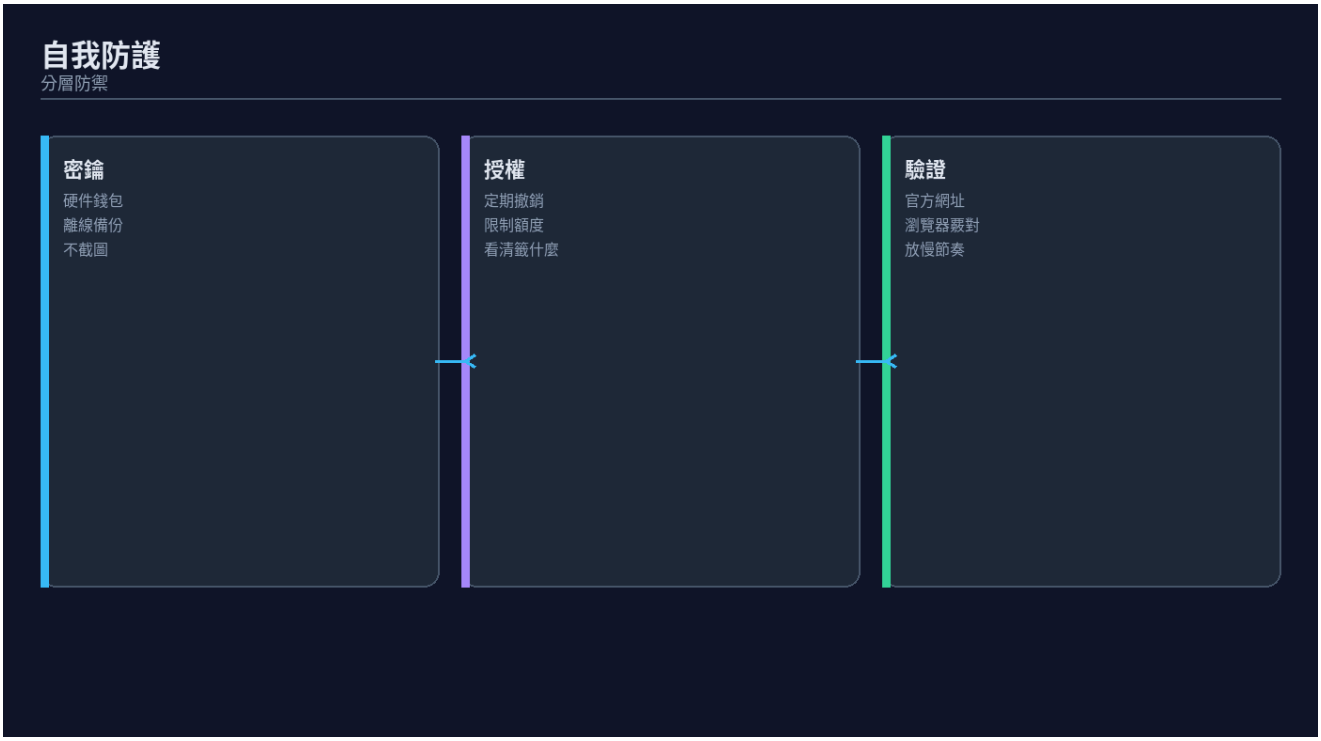
NFT 场景特供坑

- 看起来像“报价”的签名其实是授权转移；
- 免费 mint 要求无限额授权主流稳定币；
- Discord 一夜之间全是盗号链接。

钓鱼案的共性

急、怕、贪——三张牌。任何“倒计时必须签”都先冷处理。

防护原则（比插件列表重要）



1. **助记词 / 私钥永不联网输入**，永不发给任何人，不做云相册截图。
2. **大额冷、小额热**；游戏/实验用消耗型地址。
3. **授权最小化**；定期用可信工具撤销（自己核对网址）。
4. **一书签官网**；不点搜索第一条广告。
5. **硬件钱包**处理储蓄级资产。
6. **交易前模拟/预览**（若钱包支持）；看不清就拒绝。
7. **分仓**：不要一个地址打天下。
8. **假设私信全假**：尤其“支持人员”。
9. **升级与备份演练**：换设备前先恢复测试小额。
10. **法律与平台规则**：被盗报案与平台流程因地区而异，提前有心理预期。

怎么选防钓鱼工具？（原则，不发安装量榜）

- 是否开源或至少说明检测逻辑?
- 权限是否过大（能读一切页面？）？
- 更新是否勤、社区是否报过误报/漏报?
- 会不会要你提交种子？**要则直接丢弃**。
- 官网域名是否与文档、Git 仓库交叉验证?

工具是辅助，**不能替代阅读签名**。

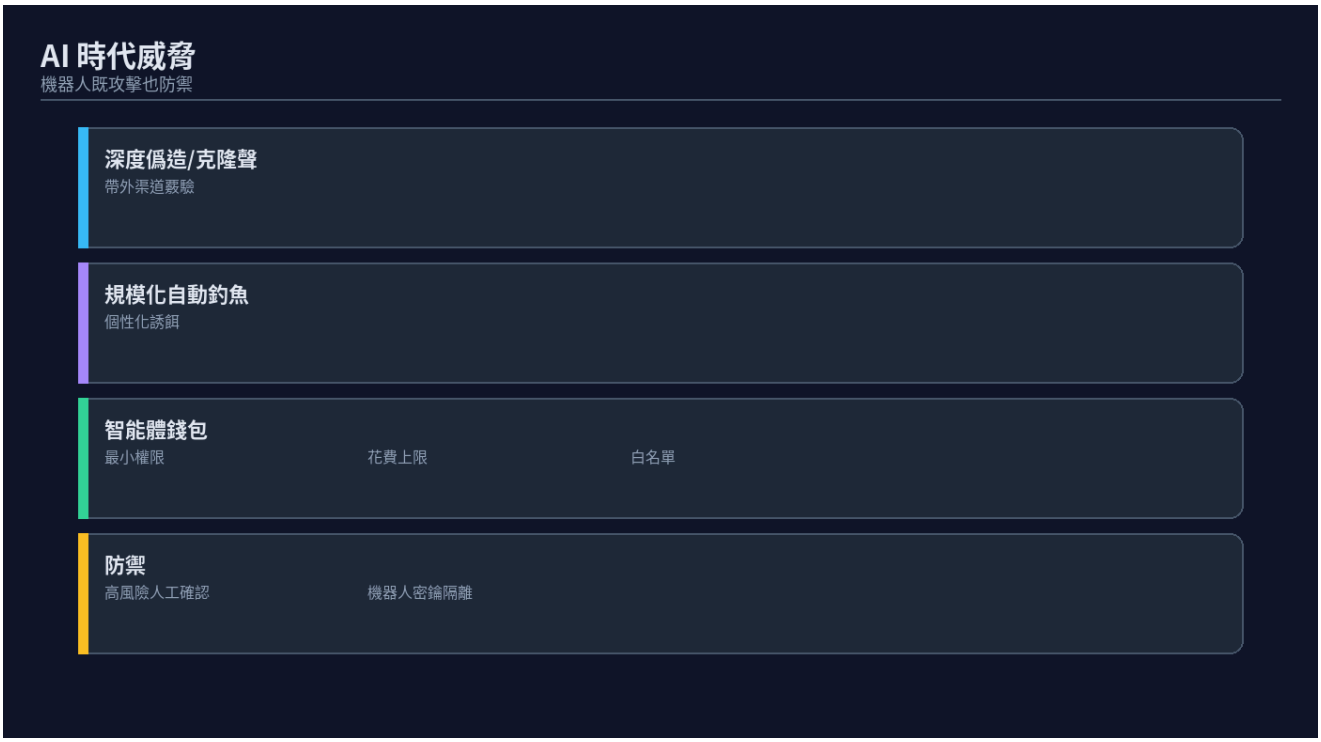
风险分类速查（原则转述）

链与合约层：漏洞、预言机、桥、升级密钥。
客户端层：假钱包、恶意扩展、剪贴板木马。

人层：贪婪、恐惧、盲目信任 KOL。
运营层：项目方跑路、多签内鬼、假审计。

应对：限额、分权、时间锁、多签、监控、保险（有限）、以及最重要的——**不参与看不懂的东西**。

AI 时代加一行



自动代理可以替你签名路径上的步骤。给 agent 的权限应像给实习生：额度、白名单合约、可撤销、全日志。这与 SCDO 强调的可审计记录一致——**速度不能牺牲追溯**。

事件发生后怎么办（原则）

1. **马上**：断网相关设备；撤销授权（从干净设备）；转移剩余资金到新种子钱包。
2. **取证**：交易哈希、钓鱼域名、聊天记录截图。
3. **报案/平台**：按当地警察与平台流程；别指望一定追回。
4. **复盘**：哪一步盲签？哪一步点了搜索广告？
5. **不要**再去点“找回资产”的连环骗局。

家庭与团队场景

多人金库用多签与角色分离：发起、审批、执行分开。一人兼任所有角色等于单点。培训成员：客服话术识别、硬件钱包操作、紧急联络树。

开发者最小安全集（给会写合约的读者）

- 检查表与同行评审；
- 测试网与不变式 fuzz；
- 限制升级权限与时间锁；
- 预言机双源；
- 应急暂停与披露渠道；
- 不要抄不明来源的“发财合约”。

审计报告不是免死金牌：范围、版本、是否修复要看清楚。

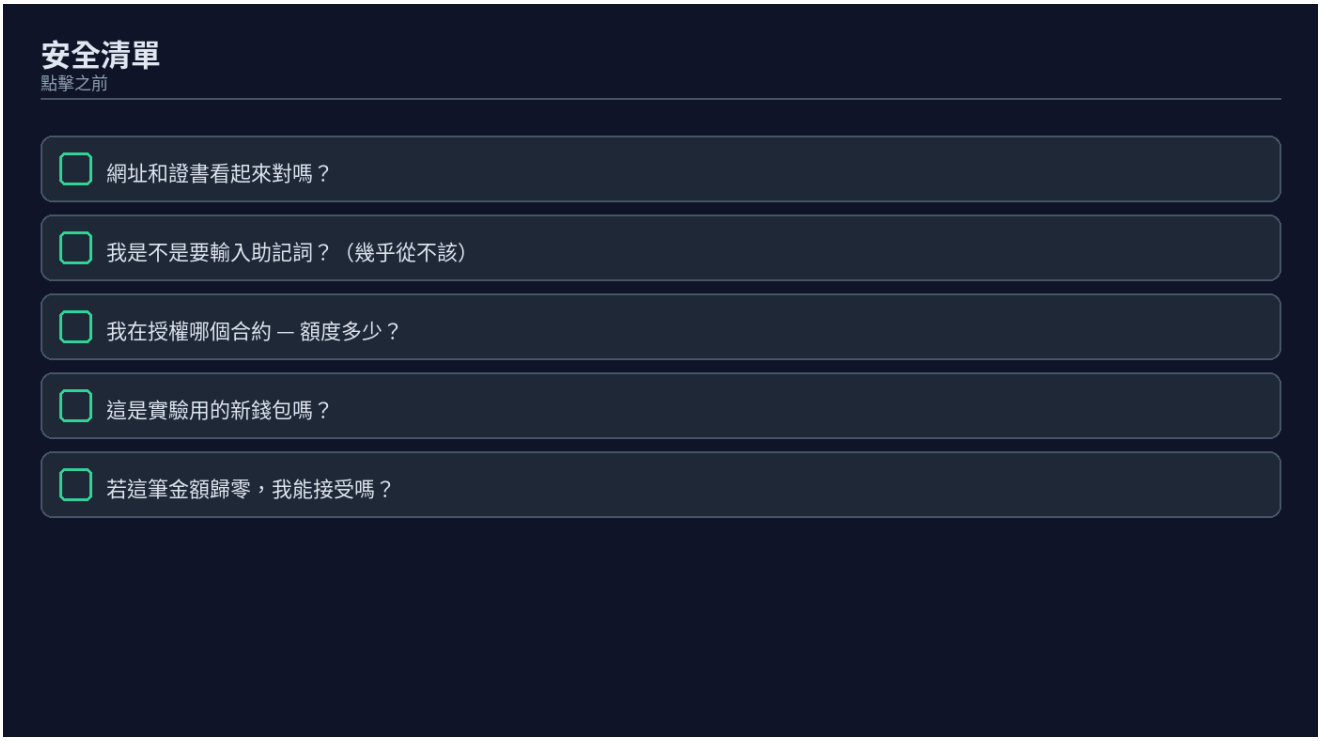
物理与供应链

假硬件钱包、二手设备预植后门、维修留后门——大额用户从官方渠道买，验包装，初始化自己生成种子。手机 root/越狱降低热钱包安全假设。

心理安全

羞耻感让受害者不敢声张，骗子更易得手。建立“被骗可讨论”的朋友圈文化，比再装五个插件有用。

日常检查清单（可打印）



每周：

- [ ] 浏览授权列表，撤销不再使用的；
- [ ] 确认书签仍指向真域名；
- [ ] 更新钱包与系统补丁；
- [ ] 检查备用硬件/纸备份是否可读；
- [ ] 复习一次“假客服”话术。

每月：

- [ ] 小额演练恢复钱包到干净设备；
- [ ] 盘点哪些地址装了哪些实验性合约；
- [ ] 阅读一条近期重大黑客复盘（学模式不学模仿）。

每年：

- [ ] 评估是否升级硬件钱包固件（官方渠道）；
- [ ] 家庭成员紧急情况是否知道如何联系与“不转账口令”。

把清单贴在书桌——比收藏一百篇安全长文有效。

常见问题（安全）

问：已经输入助记词到假站？
答：立刻视为泄露；转移资产到全新种子；旧地址放弃。

问：硬件钱包保百？
答：大幅降低热端风险，不防你自己签恶意交易。

问：公共 Wi-Fi 能用钱包吗？
答：尽量别；非要用则硬件确认+小额。

问：家人要我远程协助转账？
答：防诈骗口令；视频确认。

问：授权撤销交易太贵？
答：优先撤销高危无限额；择机低费用时段。

组织级威胁模型（小团队也能用）

即使只有三个人的工作室，也可以写一页威胁模型：资产种类（金库、热钱包、域名、社交账号、代码仓库）、对手（外部黑客、钓鱼、内部人员、供应商）、最坏影响、现有控制、缺口。域名与社交账号被盗造成的假公告，往往比合约漏洞更快收割粉丝。开多因素认证、权限最小化、硬件密钥存管理员账号，是低成本高回报。

代码仓库的依赖投毒、CI 泄露私钥、测试网助记词误用于主网，都是经典乌龙。清单：密钥用专用保管；CI 用短期令牌；测试与生产隔离；发布合约的机器专用。事故披露模板提前写好：何时发现、影

响范围、用户该做什么、补偿政策是否存在。沉默与装死会摧毁唯一比钱珍贵的东西——信任。

个人用户把“组织级”缩到家庭版：谁会继承钱包？有没有遗嘱式说明（小心写法别变成泄密）？紧急联络人是否知道你不会向其索要验证码？这些话题尴尬，但比链上遗产纠纷更可控。

模拟攻击演练（建议每年一次）

找一位懂行的朋友做“红队半日”：试图用钓鱼页、假签名、假客服话术骗你（约定禁止真转大额）。演练后只改流程不伤感情。企业可请外部公司，个人可用家庭会议形式。发现的问题写成清单：域名是否易混、书签是否齐全、硬件确认是否被忽略成盲签。

同时演练“丢失手机”：热钱包是否有生物识别二次关；交易所是否开提现白名单；社交账号是否能通过备用邮箱夺回。安全是过程，不是买一件硬件就毕业。

若你使用 AI 助手管理日程甚至草稿交易，永远不要把种子或无限权限交给云端对话。把助手当成互联网上的陌生人——可以很有用，也可以很危险——直到你能为其行为建审计日志与额度。

旅行与跨境场景

出境携带硬件钱包、纸备份拆分存放、避免托运行李放种子、公共充电口不直连（充电攻击）、酒店保险箱不等于安全。交易所提现白名单若绑定国内手机号，漫游时要确保仍能 2FA。提前演练比到机场才想起来可靠。涉及申报与外汇规则，遵守当地法律，本书不讨论规避。

合约交互的三秒法则

每次签名前强制三秒：1）这是哪个域名？2）合约要我的钱还是只要一个验签？3）我是否主动发起？任一答不上来就拒绝。把三秒法则教给团队新人，能挡下大量即时反应式被盗。配合钱包的模拟结果（若有）与硬件屏幕确认，形成纵深。记住：安全是减速带，不是刹车毁乐趣；减速是为了开得更远。

补强：剪贴板与二维码

手机恶意软件会替换你复制的地址；转账前务必核对屏幕前后几位。二维码可被贴假码；大额支付用地址簿白名单。桌面端同样可能有浏览器恶意扩展监听剪贴板——扩展权限审查要严。

本章收束

1. 默认有对手在钓鱼；撤销很难。
2. 种子保密、授权最小化、官网手输。
3. NFT 与空投是重灾区。
4. 插件按原则选，不按过气榜单。
5. 下一章 **最后**：学习路径、免责声明、SCDO 轻延伸与更新方式。

（第 9 章完 · v2 原创重写 · SCDO Lab）

10、SCDO：分片 PoW、站点与新人怎么试

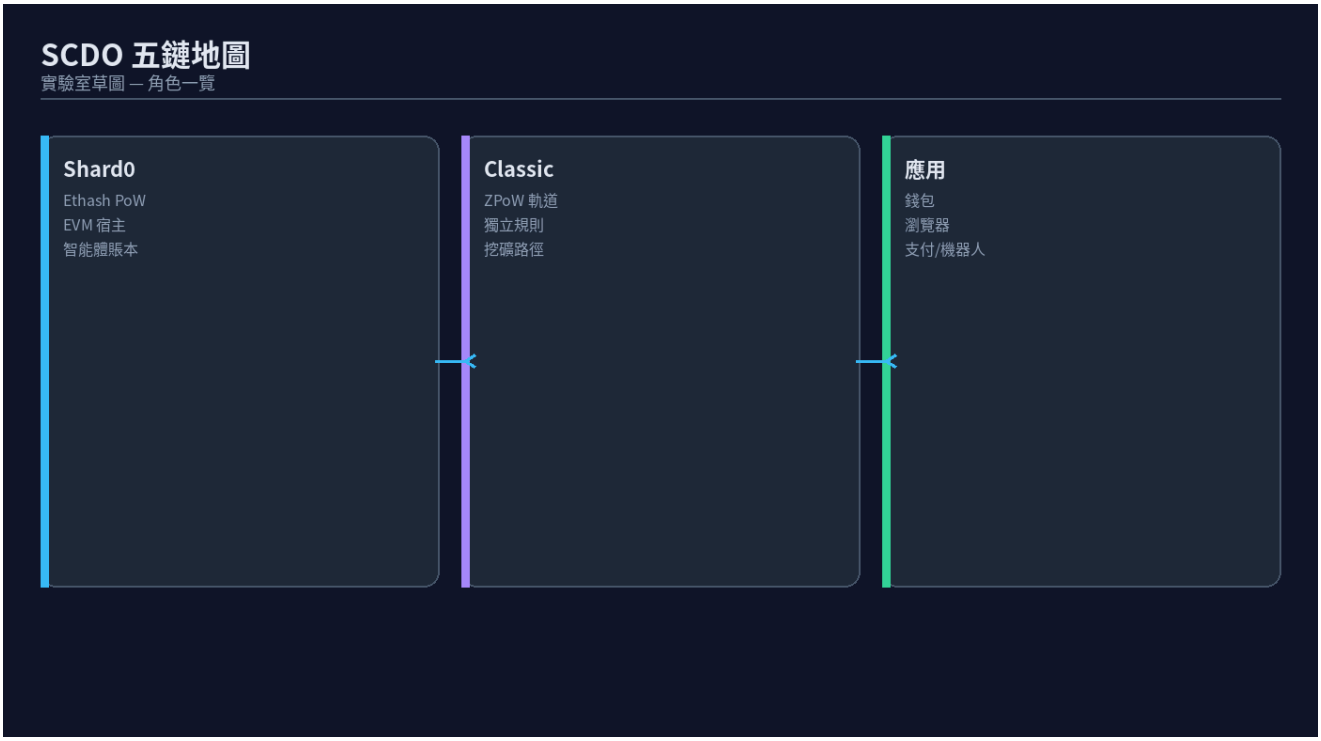
SCDO Lab · Web3 新人必读指南 v2
前九章给了通用地图；本章把镜头对准 **SCDO**：它是什么、五条链怎么分工、官网/浏览器/钱包/Agent Ledger 在哪、合规怎么读、新人如何小步试。
非投资建议。

SCDO 是什么?

SCDO 是面向去中心化价值转移的点对点公有区块链体系，由 **SCDO Laboratory**（运营主体 **9Y9 PTY LTD**）维护公开站点与工具。2026 年在线网络可理解为**五条并列地位的链**:

链	共识 / 客户端	角色（教育向）
Shard0 EVM	**Ethash** PoW · core-geth 谱系 · chainId **5680**	智能合约、Agent Ledger 锚定、类以太坊工具
Classic Shard1–4	**ZPoW** · go-scdo	原分片核心；地址常以 **1S…** 开头

一句话：**Classic 保留科学计算型 ZPoW 分片；Shard0 用 Ethash 接 EVM 与代理记账**。 二者是并列产品面，不是“主链 vs 废弃链”的简单故事。



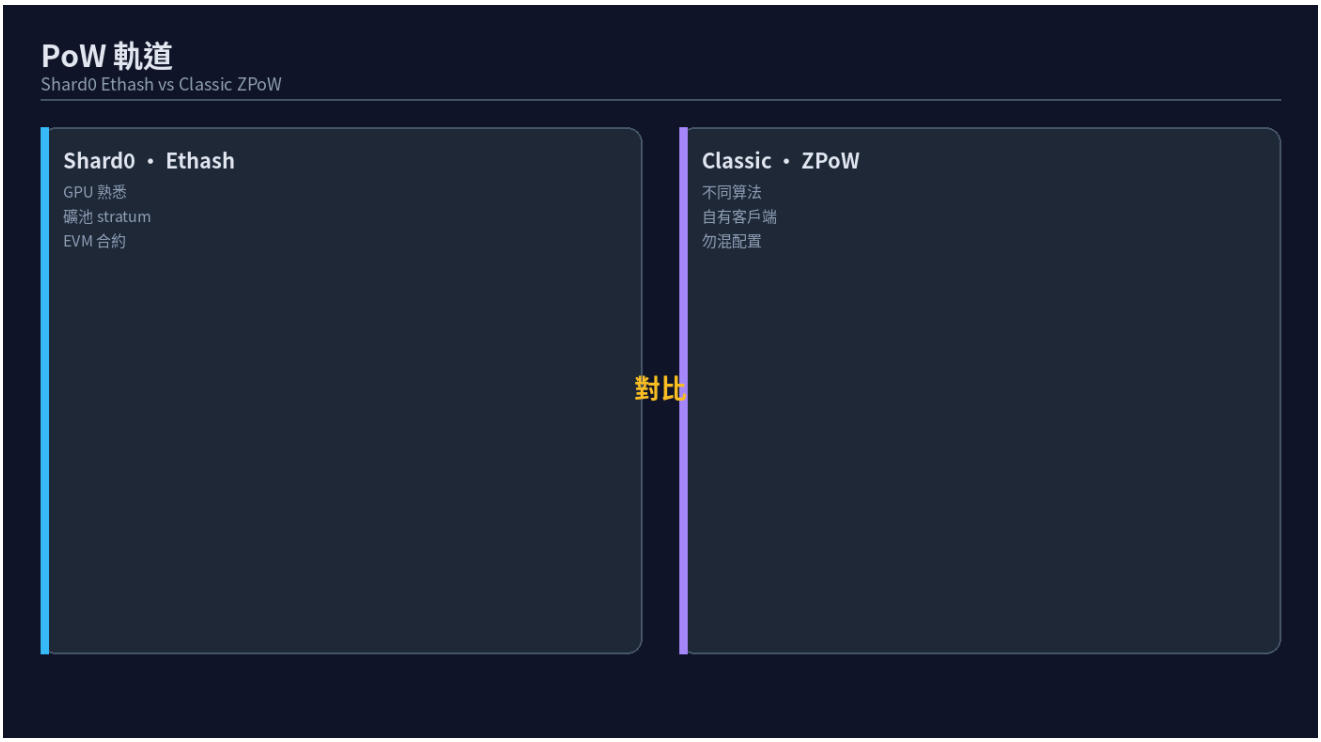
分片与 PoW：读懂两条轨道

Classic：分片 + ZPoW

- 账户与节点划分到 Shard1–4；同片交易本地确认，跨片用 **Debt** 等机制对齐。
- **ZPoW** 侧重可验证的科学计算风格工作量（相对纯哈希竞赛更偏 CPU 友好设计目标），实务上仍常见 GPU 记账。
- 详细挖矿见第 11 章。

Shard0：Ethash EVM

- 预合并以太坊风格 **Ethash** 纪元；公共 RPC / 浏览器以官网与 scdoscan.io 为准。
- 便于 MetaMask 类工具、ERC 合约与 Agent 身份（如 ERC-8004 注册表）。



官网、浏览器与透明度

入口	用途
scdo.com.au	官网：钱包、Agent Ledger、论文、合规、学习区
scdoscan.io	区块浏览器与透明度相关页面
`/papers/`	技术论文与白皮书更新（含 2026 架构说明）
`/learn/web3/`	本指南（你正在读）

读链上数据、核对软件哈希与公开说明时，优先一手来源；二手“稳了”截图不可替代浏览器与官方文档。

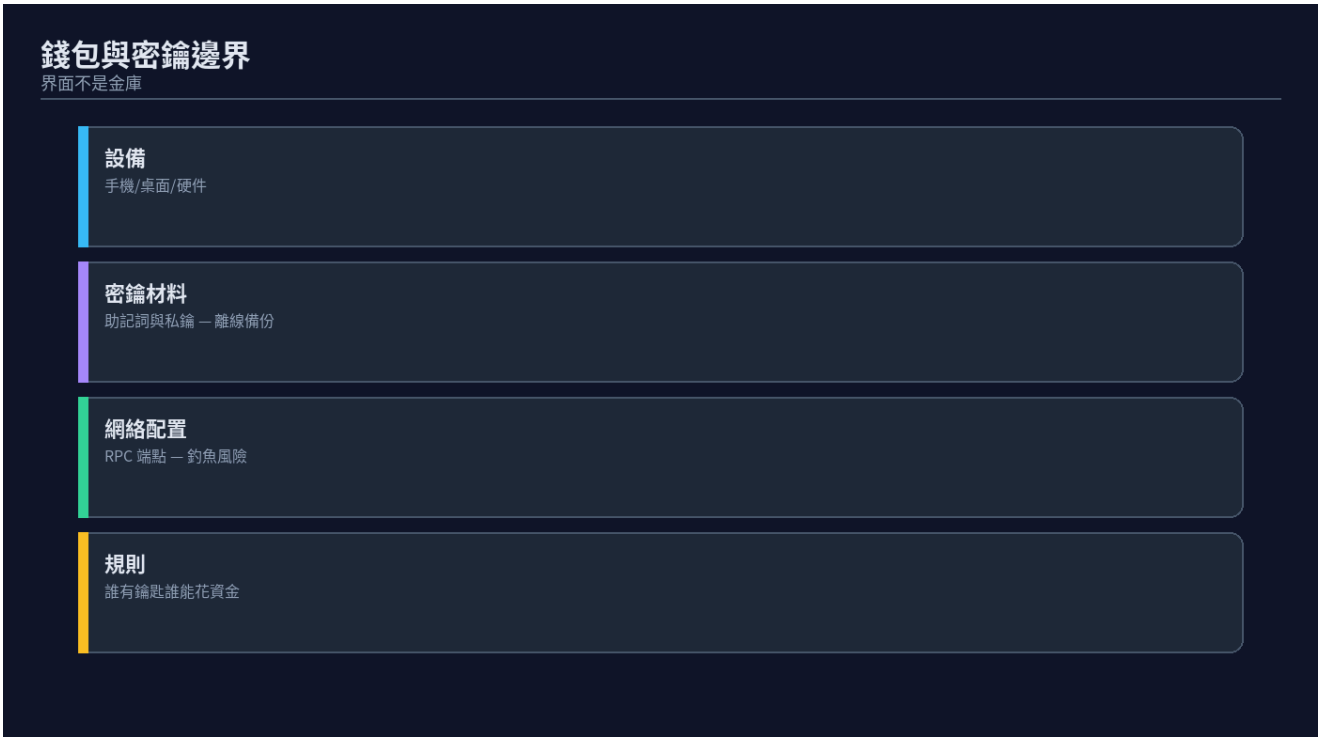


钱包（SCDO Wallet）

SCDO Wallet 面向五链 UI：Classic `1S…` 与 Shard0 `0x…`；密钥在本地（以产品当时说明为准）。另有无头 Linux agent 等形态供服务器记账。

新人原则（与第 9 章一致）：

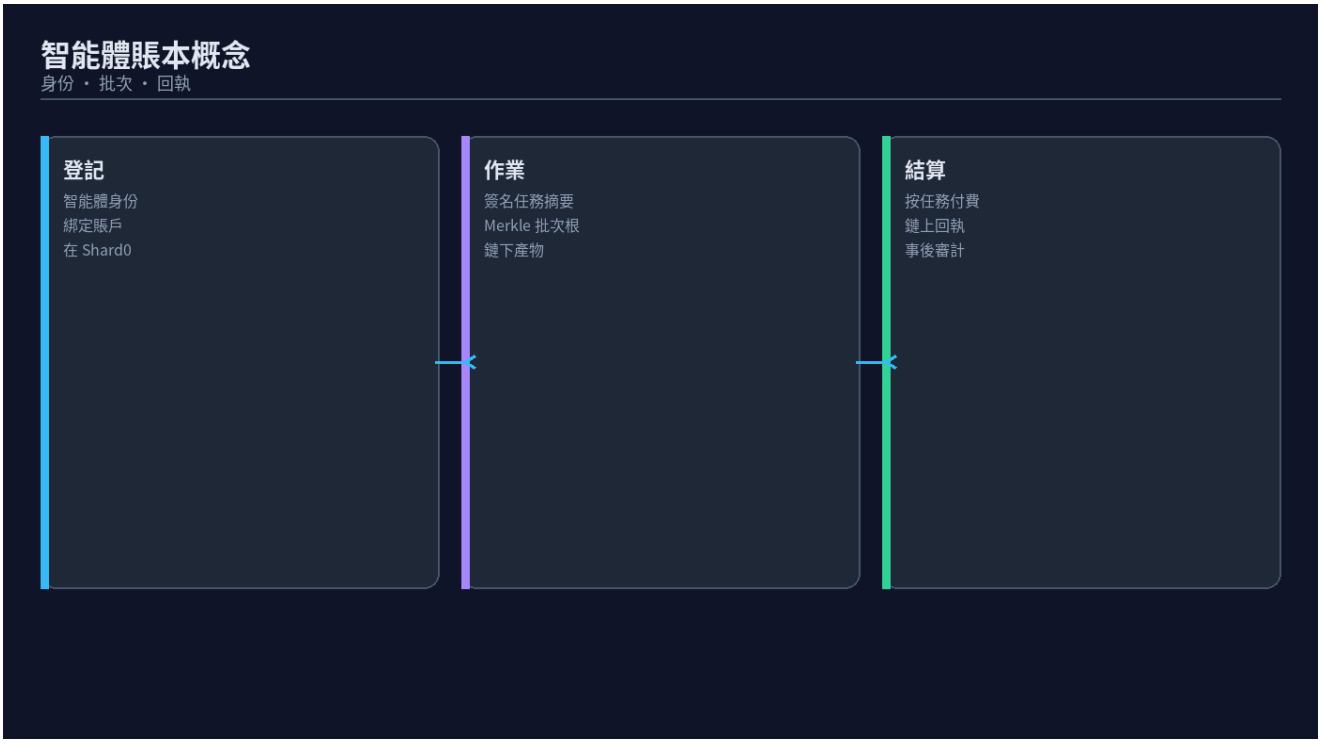
1. 先小额、先只读浏览器。
2. 种子词 / 私钥不进聊天、不进云笔记。
3. 下载只认官网路径与校验说明。



Agent Ledger：可验证的代理记账

Agent Ledger 让每个 AI agent 持有自管密钥，签名任务/心跳，并把摘要锚定到 **Shard0**；可选 ERC-8004 身份。站点入口：scdo.com.au/agent-ledger/。

它解决的是：**机器在做事时，谁签名、痕迹能否核对**——不是“自动印钞”。支付层（如 x402 / HTTP 402、约 1¢ 量级 settle nest）见第 12–13 章。

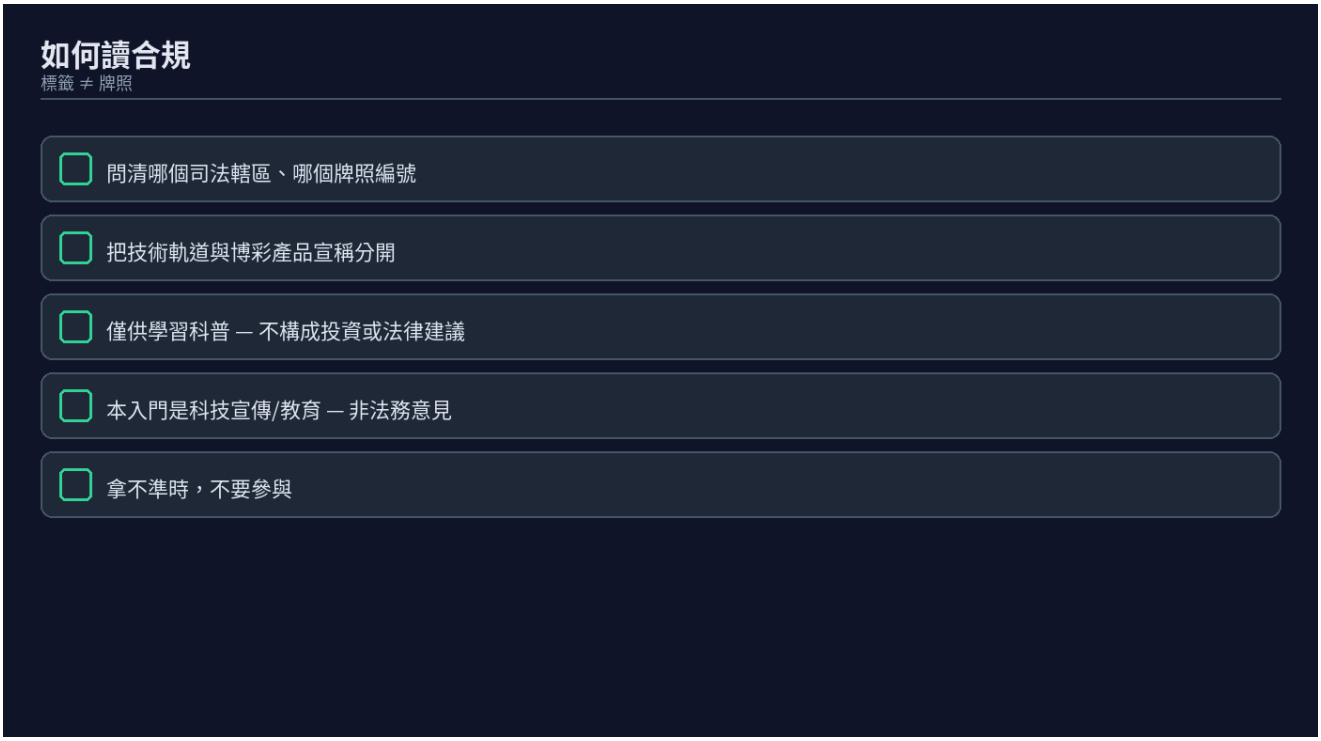


合规语境（高层，非法律意见）

运营相关主体 **9Y9 PTY LTD** 公开材料中可见：

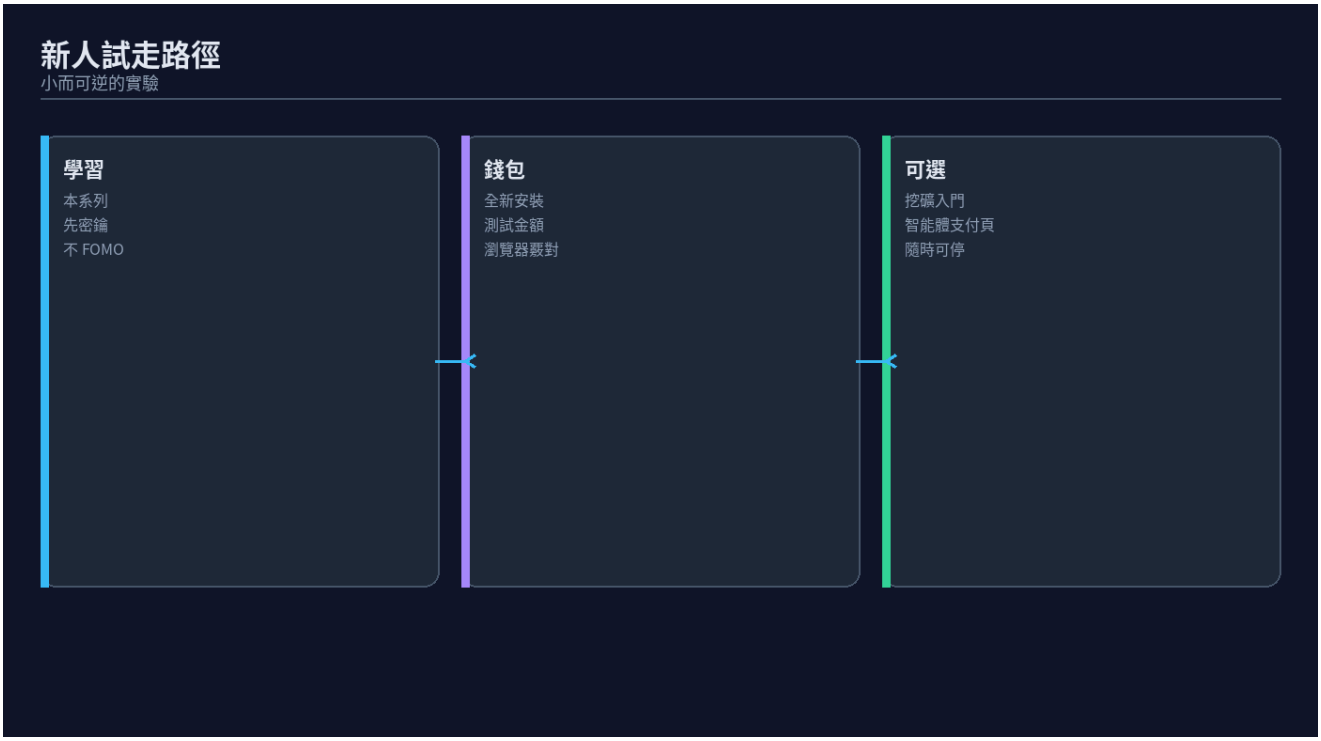
- **AUSTRAC** 数字货币兑换（DCE）登记号示意：**DCE100714503-001**（请在 AUSTRAC 公开名录自行核验；**登记 ≠ 背书或批准**）。
- **AFCA** 外部争议解决会员示意：**124589**（投诉先联系运营方，未满意可了解 AFCA 路径）。

细节以 scdo.com.au/compliance.html 与监管公开页为准。本书不解释如何规避法律。



新人怎么试 SCDO（不涉及大额）

1. 打开官网，只读 Wallet / Agent Ledger / Papers 说明。
2. 用浏览器查看 Shard0 或 Classic 公开信息（高度、交易形态）。
3. 若创建钱包：最小权限、最小余额、先转一笔“灰尘”级测试（若你所在地法律允许）。
4. 对 agent：先理解签名与心跳，再谈支付试点。
5. 重读第 9 章安全清单。



与前九章的衔接

1–9 章教你通用 Web3；本章教你 **SCDO 产品面怎么读**。挖矿、机器人商业、支付、博彩合规角度见后续章。

免责声明（本章强调）

- 教育向原创；非投资、法律、税务建议。
- 数字资产可归零。
- 遵守你所在地法律。
- 第三方名称为说明，非背书。
- 产品以官网**当时**说明与风险提示为准。

本章收束

SCDO = **分片 Classic（ZPoW）+ Shard0 EVM（Ethash）+ 官网工具链（钱包、浏览器、Agent Ledger）+ 可核验合规披露**。下一步：第 11 章挖矿，第 12 章 Bots×链，第 13 章支付，第 14 章博彩合规视角。

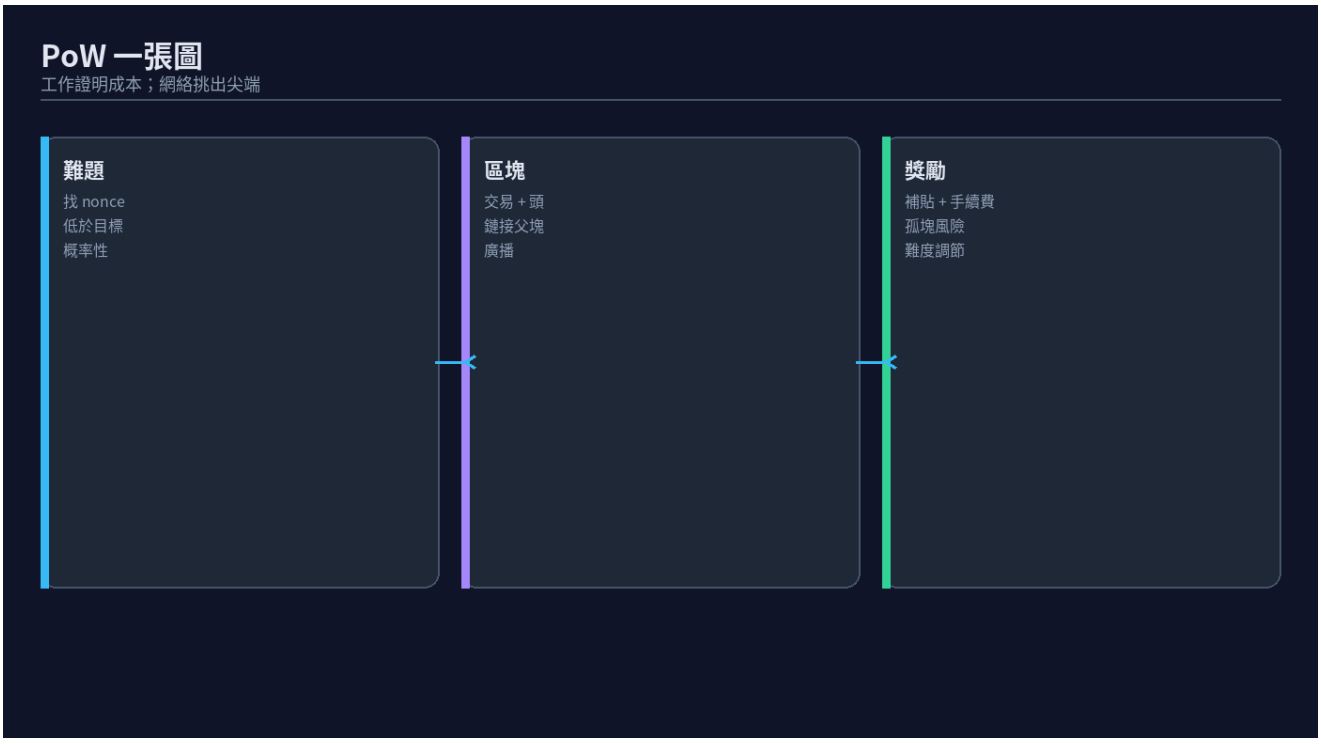
（第 10 章 · SCDO · SCDO Lab）

11、挖矿：PoW、矿工/矿池、GPU/ASIC 与 SCDO 记账

SCDO Lab · Web3 新人必读指南 v2
接第 4 章分片地图与第 10 章 SCDO：本章讲清工作量证明、矿工与矿池、硬件路线，以及 **SCDO 两条挖矿轨道**（Shard0 Ethash + Classic S1–4 ZPoW）。
非投资建议。

什么是挖矿（PoW）？

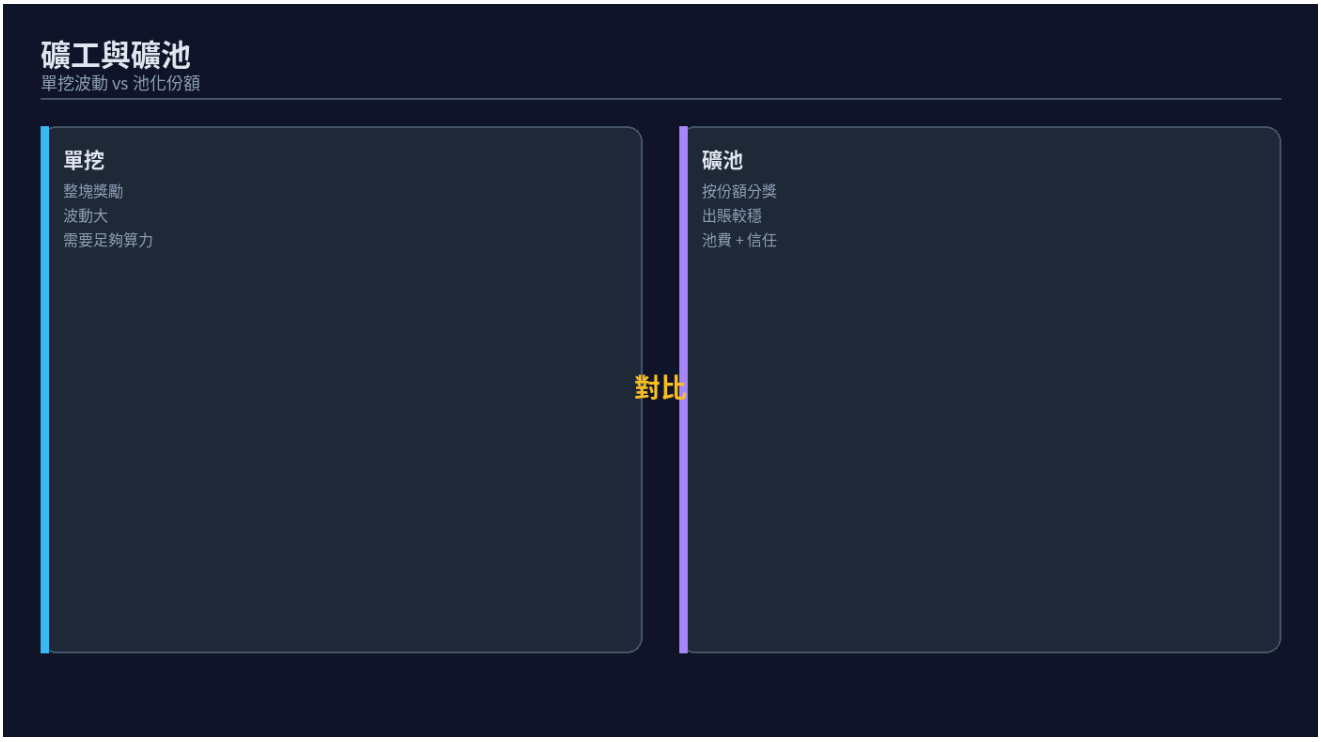
工作量证明（PoW）让节点竞争完成可验证的计算难题；赢家打包区块并获得区块奖励与手续费（具体规则因链而异）。挖矿本质是：**用能耗与硬件换取出块权与激励**，并让改历史变得昂贵。



矿工、全节点与矿池

角色	做什么
全节点 / 记账节点	存状态、验证、可出块
矿工	跑 PoW 搜索，提交满足难度的解
矿池	汇集算力，按贡献份额分配奖励（降低单人出块方差）

矿池降低“运气波动”，也引入**中心化与规则信任**：看清费用、支付地址、是否可切换、历史诚信。



GPU、CPU 与 ASIC

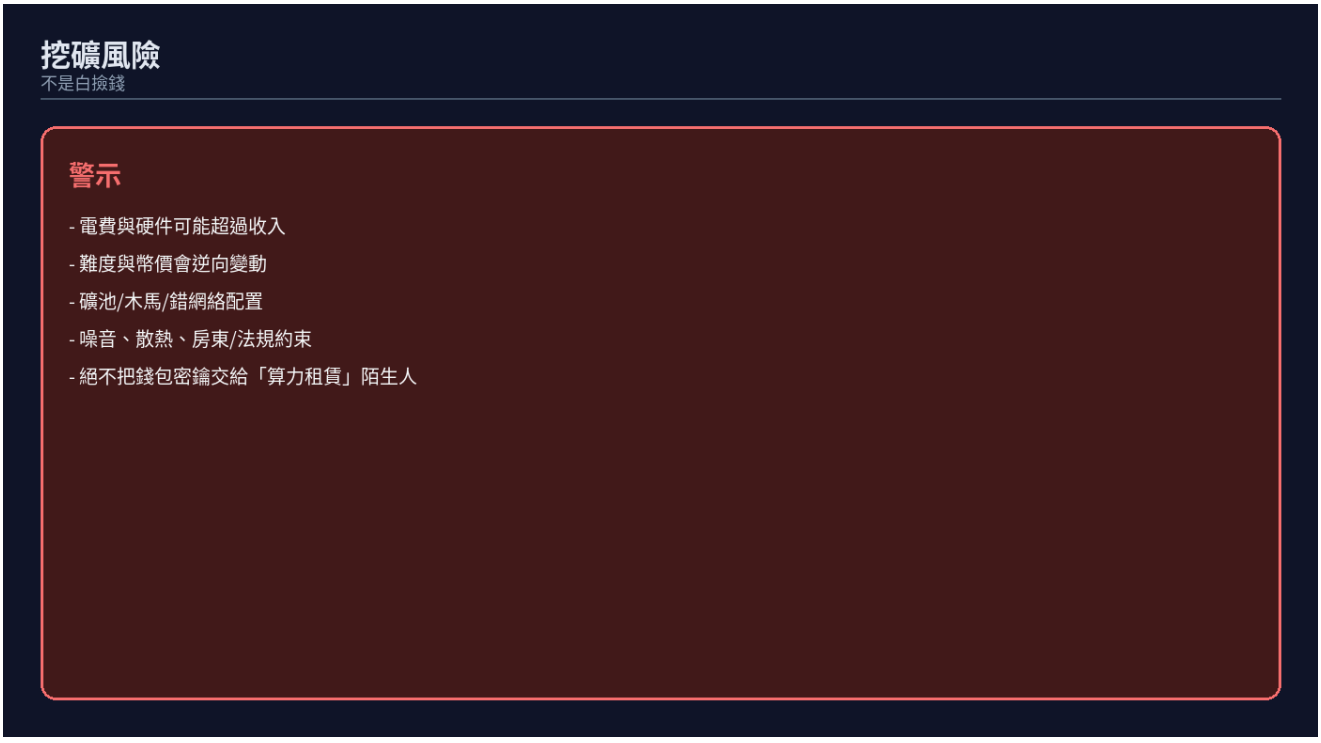
- **CPU：** 灵活，适合部分科学计算型算法；吞吐量常低于专用卡。
- **GPU：** 通用算力主力；Ethash 族与许多 PoW 仍常见。
- **ASIC：** 为特定哈希算法定制，效率极高，也让普通硬件更难竞争。

算法设计会影响“谁更能挖”：偏科学计算的 ZPoW 与偏哈希的 Ethash，硬件生态不同。



费用、风险与诚实预期

挖矿是经营：电费、散热、宕机、难度上升、币价波动、池子规则变更。可能亏损。监管与电网政策因地而异。本书不提供“稳赚机型清单”。



SCDO 挖矿轨道 A：Shard0 Ethash

- 链：Shard0 EVM · Ethash · chainId 5680。
- 工具生态接近以太坊 PoW 时代 GPU 方案；以官网/浏览器公开指南与透明度为准。
- 项目方自有算力占比可能较高——独立记账者加入有助于去中心化（以公开披露为准）。



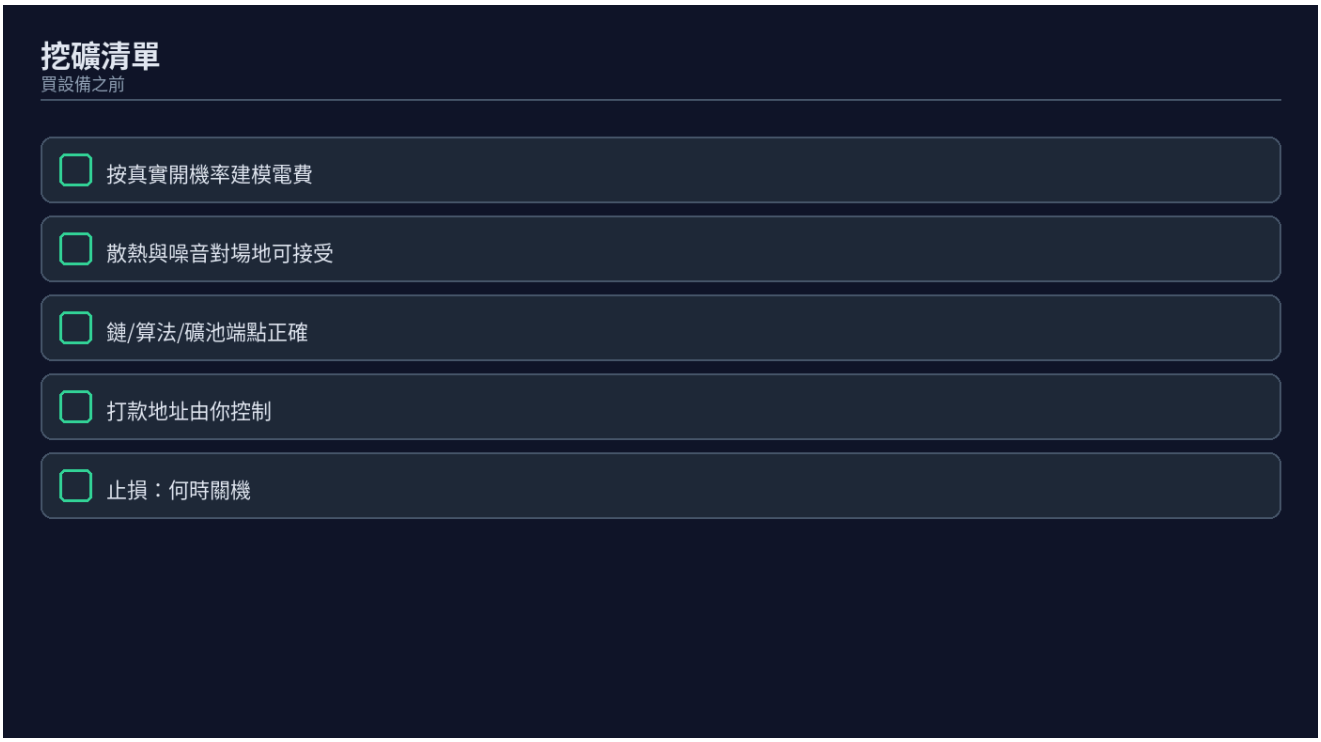
SCDO 挖矿轨道 B：Classic Shard1–4 ZPoW

- 四分片 Classic；共识 **ZPoW**。
- 地址与钱包路径与 Shard0 不同（`1S…` vs `0x…`）。
- 实务常见 GPU（如公开材料中的 zminer 路线）与钱包内 CPU 记账选项——以当时官方说明为准。



新人清单（挖矿）

1. 先读懂你挖的是哪条链、哪种算法。
2. 算清电费与噪音；不要只看“日收益截图”。
3. 钱包地址核对三遍；池子用官方或你信任的来源。
4. 固件/矿工软件验哈希，防捆绑木马。



本章收束

PoW = 可验证算力竞赛；矿池换稳定性也换信任点；硬件随算法分野。SCDO：**Shard0 Ethash vault 式 EVM 轨 + Classic S1–4 ZPoW 分片轨**。下一步：机器人商业与支付章。

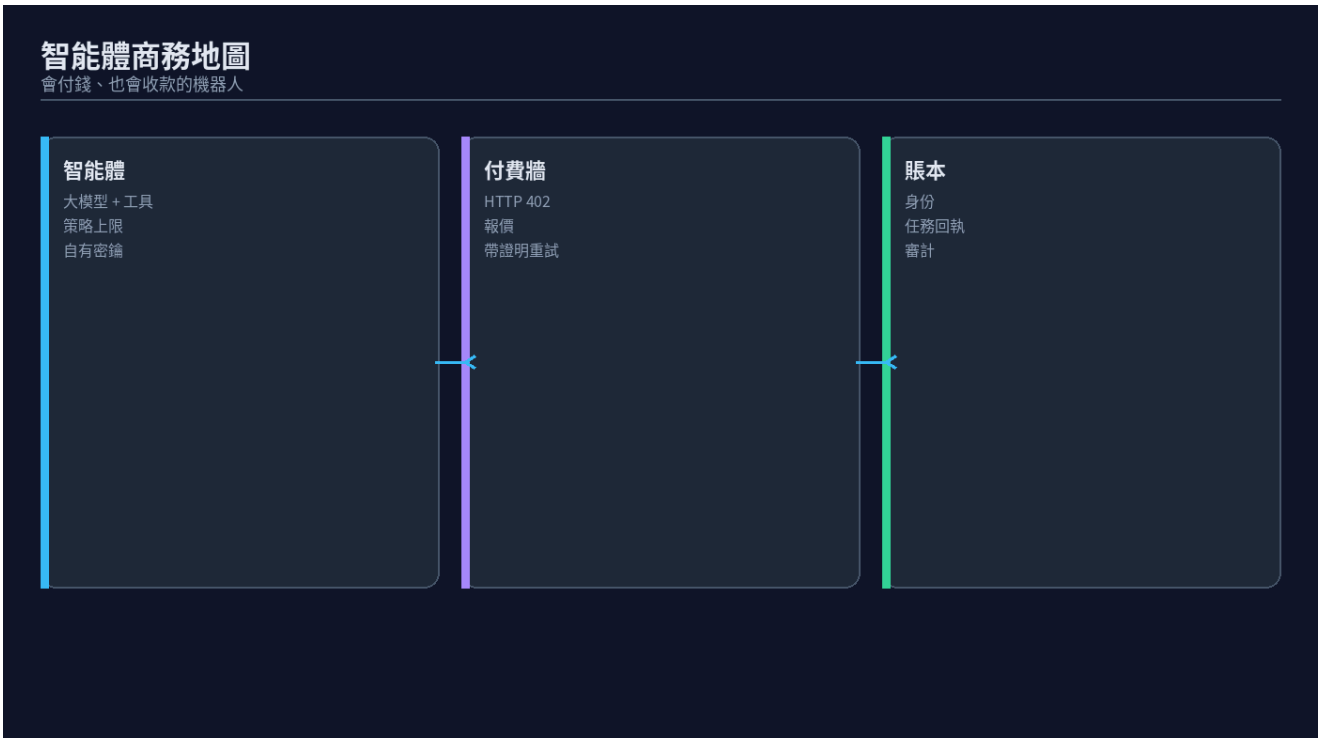
（第 11 章 · 挖矿 · SCDO Lab）

12、Bots × 区块链：代理商务、HTTP 402 与 SCDO nest

SCDO Lab · 《AI智能体的合约账本自动化》v2
机器人（bot / AI agent）如何持钥、记账、按次付费；SCDO Agent Ledger 与约 1¢ 量级 settle nest。
非投资建议。

为什么谈 Bots × 链?

自动化代理要调用 API、交换数据、雇其他代理——需要**身份、权限边界、可核对痕迹、小额结算**。链上与链下支付轨道把“机器商务”从口头约定变成可验证记录。



Agent 自持钱包与账本

每个 agent 一把钥匙：签名任务与心跳；摘要可锚定到 SCDO **Shard0**。**Agent Ledger** 提供公开可查的记账面（详见第 10 章）。密钥不离本机（以产品说明为准）。



HTTP 402 与 x402

HTTP 402 Payment Required 是“先付再取”的老状态码思路；现代 **x402** 实践把它接到稳定币按次支付（SCDO 路径常见 **USDC on Base** 试点）。适合 API 调用、agent-to-agent 小额，而非一次买断。



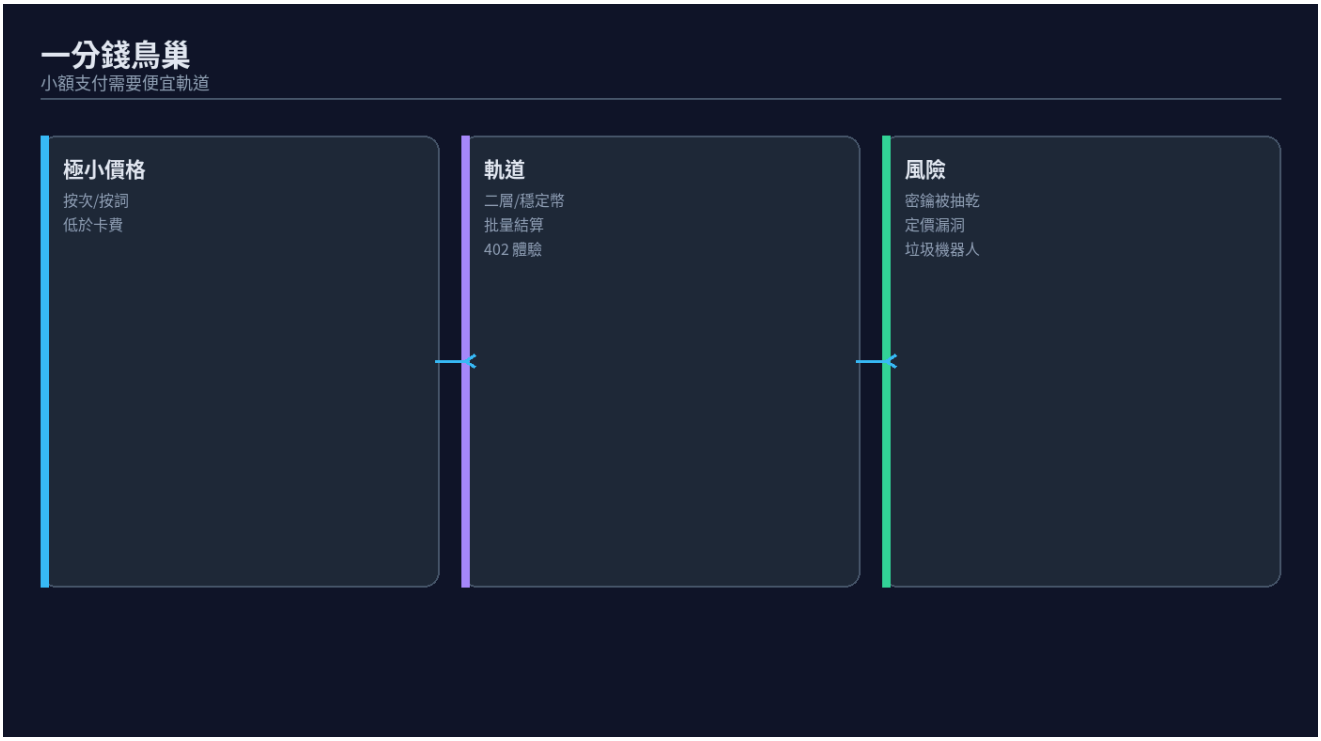
交易轨道与“刷量”幻觉

Bot 可做市、套利、爬取——也制造虚假成交量。读 **volume** × **单价** 时问：是真实需求还是自成交? SCDO 强调可验证心跳与身份，不把“刷出来的量”当成功指标。



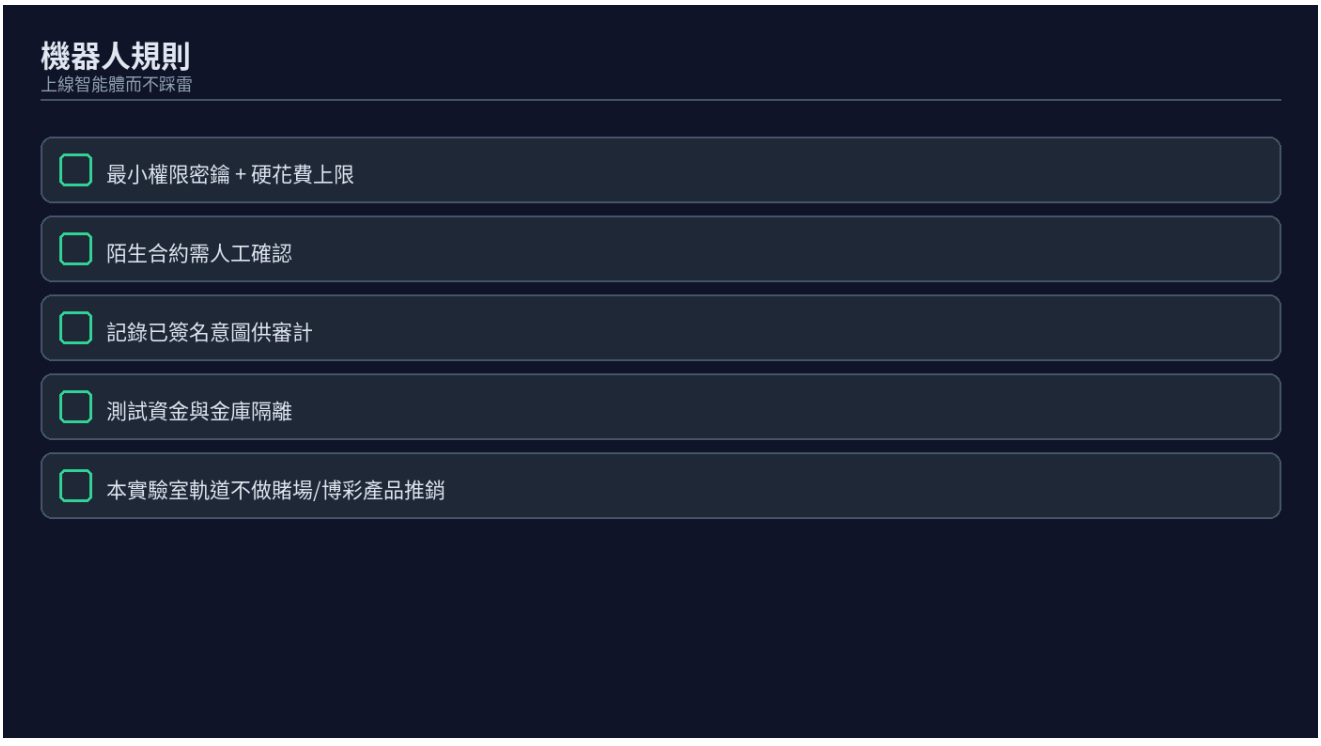
SCDO settle nest（约 1¢ 量级）

把高频、小额结算想象成**鸟巢式节点**：身份 + 签名心跳 + 可选支付路由。Merlin SoftCenter 等 `scdo_ledger` 包是**身份/心跳 settle-nest**，不是赌场大厅，也不是 x402 本身。约 **1¢** 量级用于直觉：机器商务要够便宜才跑得动。



新人守则

1. 先跑通签名与心跳，再开支付。
2. 限额、白名单、可撤销权限。
3. 分清测试网与主网。
4. 不把 agent 助记词交给第三方“代运营”。



本章收束

Bots × 链 = 自持钥 + 可验证账本 + 402/按次付费 + 诚实度量。下一章展开支付与稳定币。

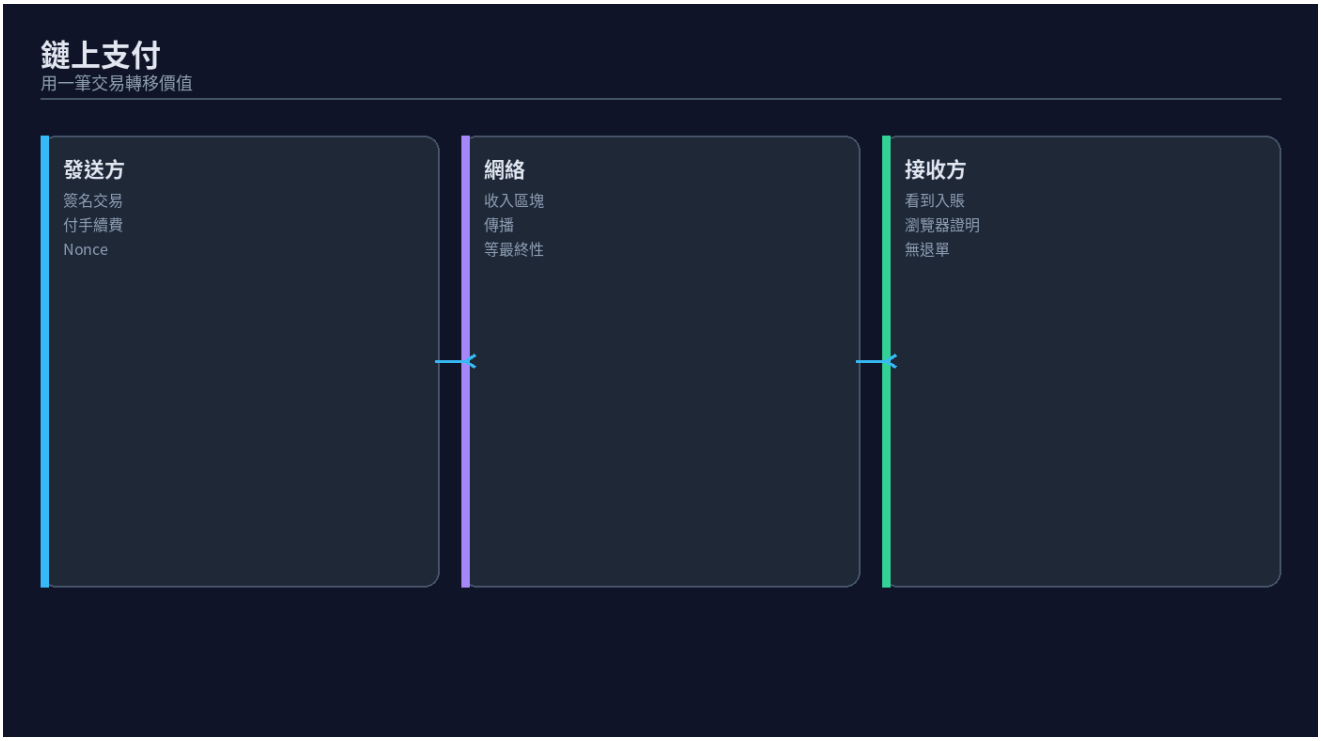
（第 12 章 · Bots · SCDO Lab）

13、支付：链上付款、稳定币、x402 与 SCDO settle shell

SCDO Lab · 《AI智能体的合约账本自动化》· 副标题：下一代智能支付系统
非投资建议。

链上支付在解决什么?

把“我付了”变成**可验证的状态变更**：金额、资产、收款方、时间与交易哈希。适合程序化结算；不适合假装“绝对匿名”或“绝对无监管”。



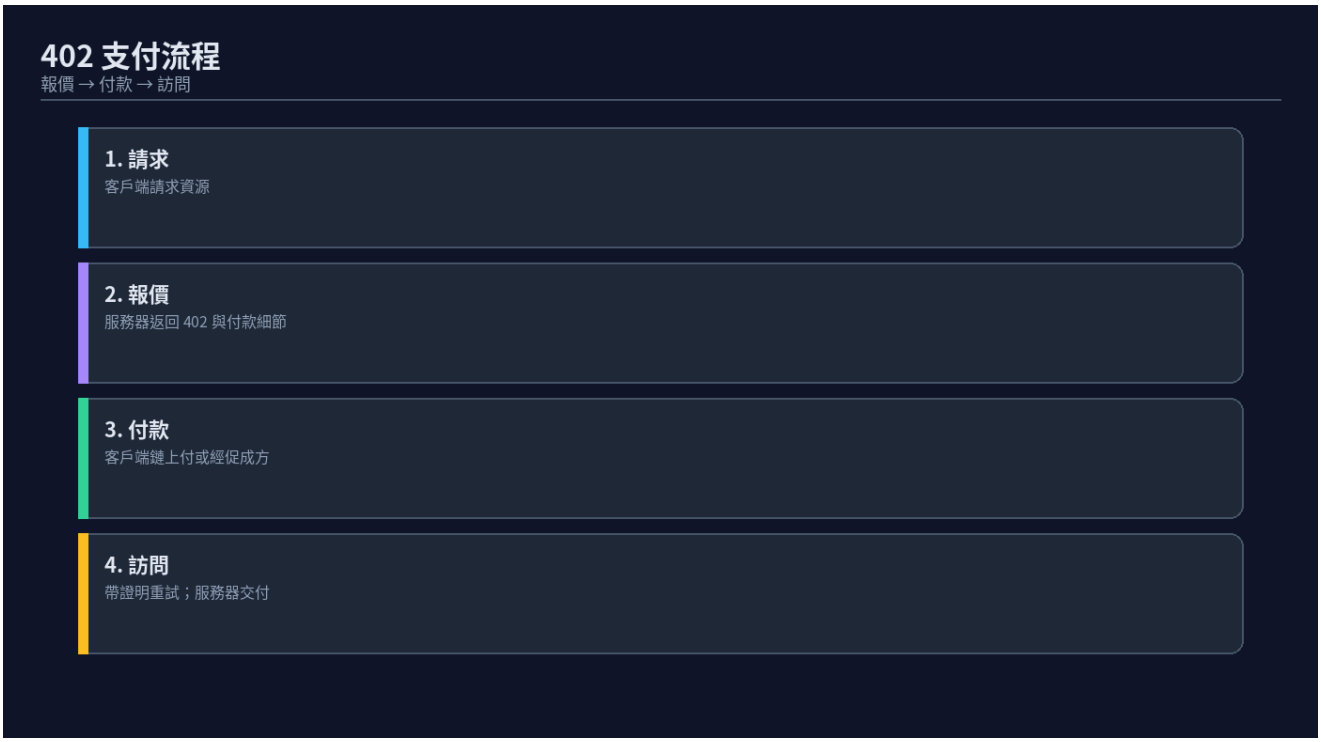
稳定币：计价单位与风险

稳定币让机器用近似法币单位计价。风险包括：储备与脱锚、冻结名单、合约漏洞、发行方政策。教学上把它当**工具**，不当“无风险现金”。



x402 / HTTP 402 支付壳

按次解锁资源：请求 → 402 → 支付 → 重试成功。SCDO 相关实践把小额 **USDC** 接到 agent 调用路径；以官网试点说明为准，早期阶段可能变化。



SCDO settle shell 与 ~1¢ nest

Settle shell = 围绕账本与支付路由的薄壳：限额、收据、锚定。**~1¢ nest** 描述成本直觉——智能支付要支撑高频低额，而不是只服务巨额转账。



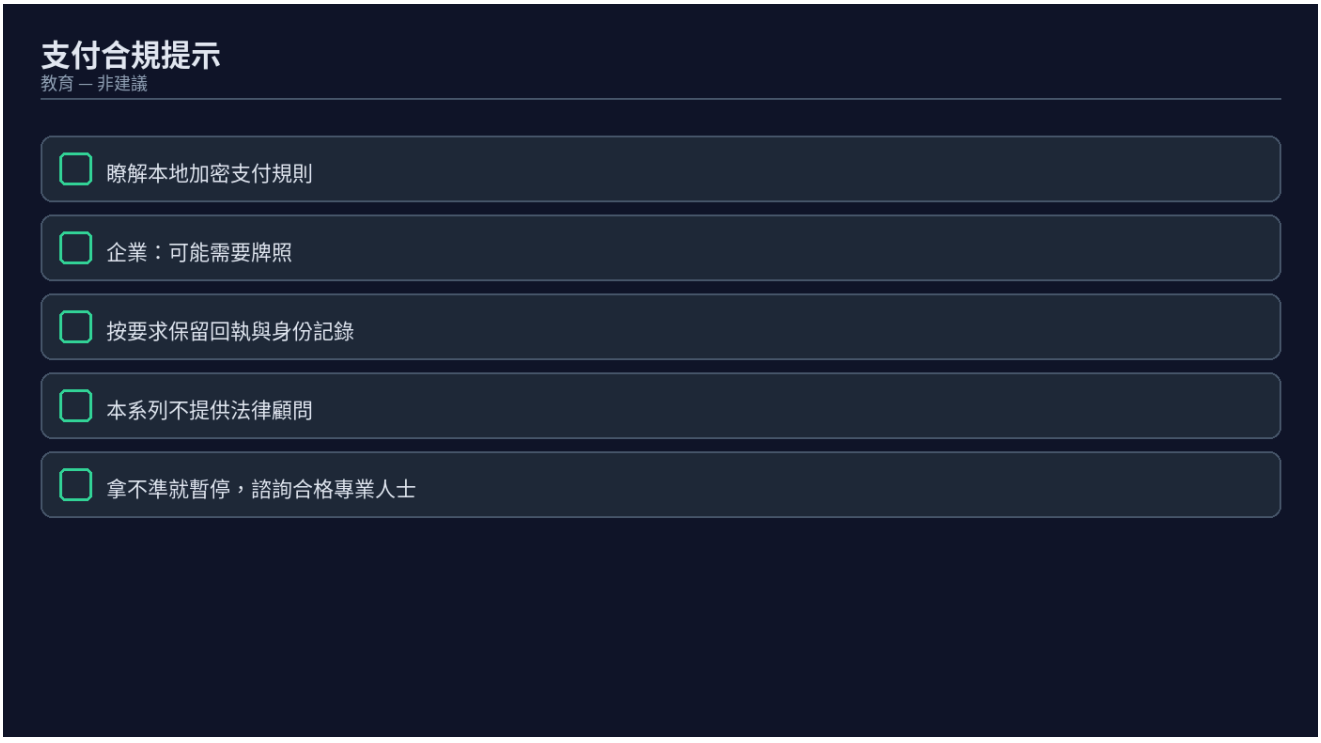
与 CEX / DEX 的关系

入金/出金常经 **CEX**；链上兑换经 **DEX/AMM**（第 5 章）。Agent 支付层尽量减少人为点选，但仍可能依赖稳定币发行与桥——每多一跳多一个信任假设。



合规与用户保护（高层）

跨境支付、兑换、汇款可能触发本地牌照与报告义务。澳语境下可阅读运营方 AUSTRAC DCE / AFCA 披露（第 10 章）——**登记≠背书**。



本章收束

下一代智能支付 = 稳定币计价 + 402 按次门 + 可验证账本壳 + 诚实风险披露。下一章：博彩/公平性与合规视角。

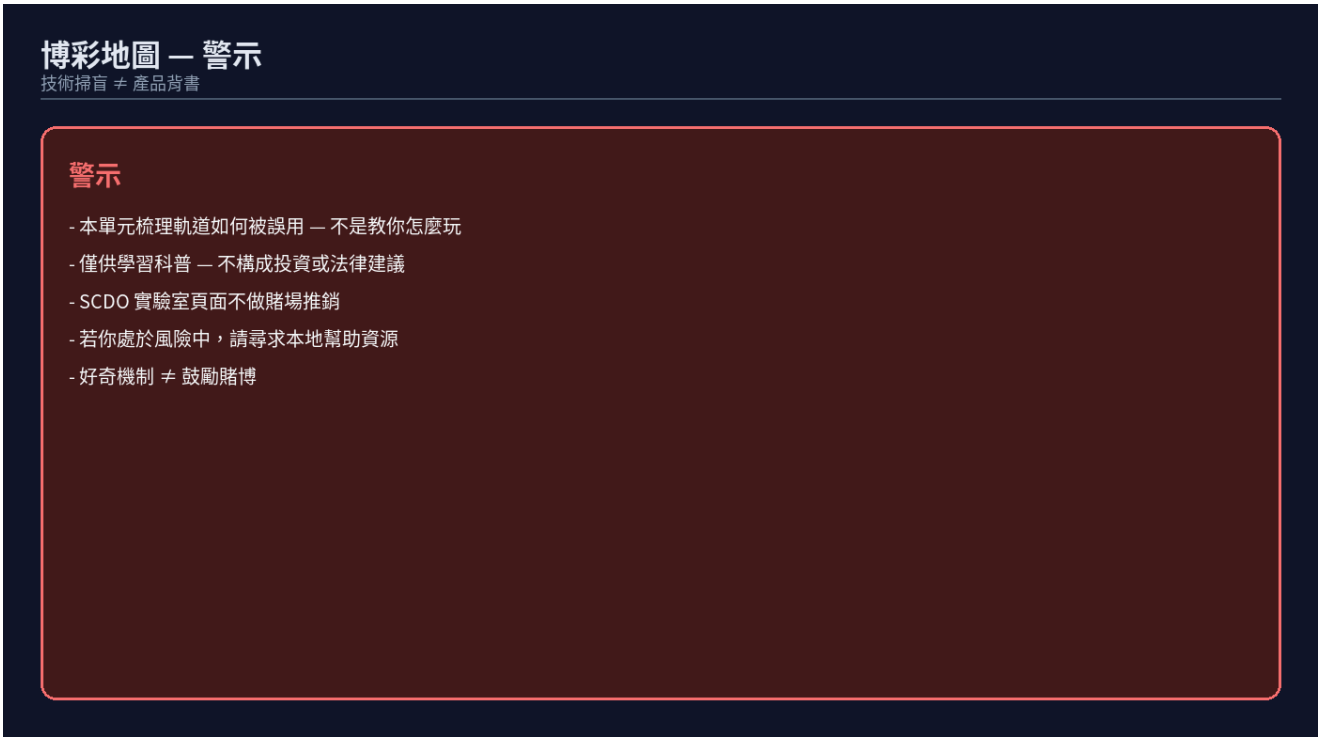
（第 13 章 · 支付 · SCDO Lab）

14、博彩视角：链上公平、结算轨道与合规（高层）

SCDO Lab · 教育章。说明可验证随机与结算概念，**不提供赌博教程，不引流赌场**。

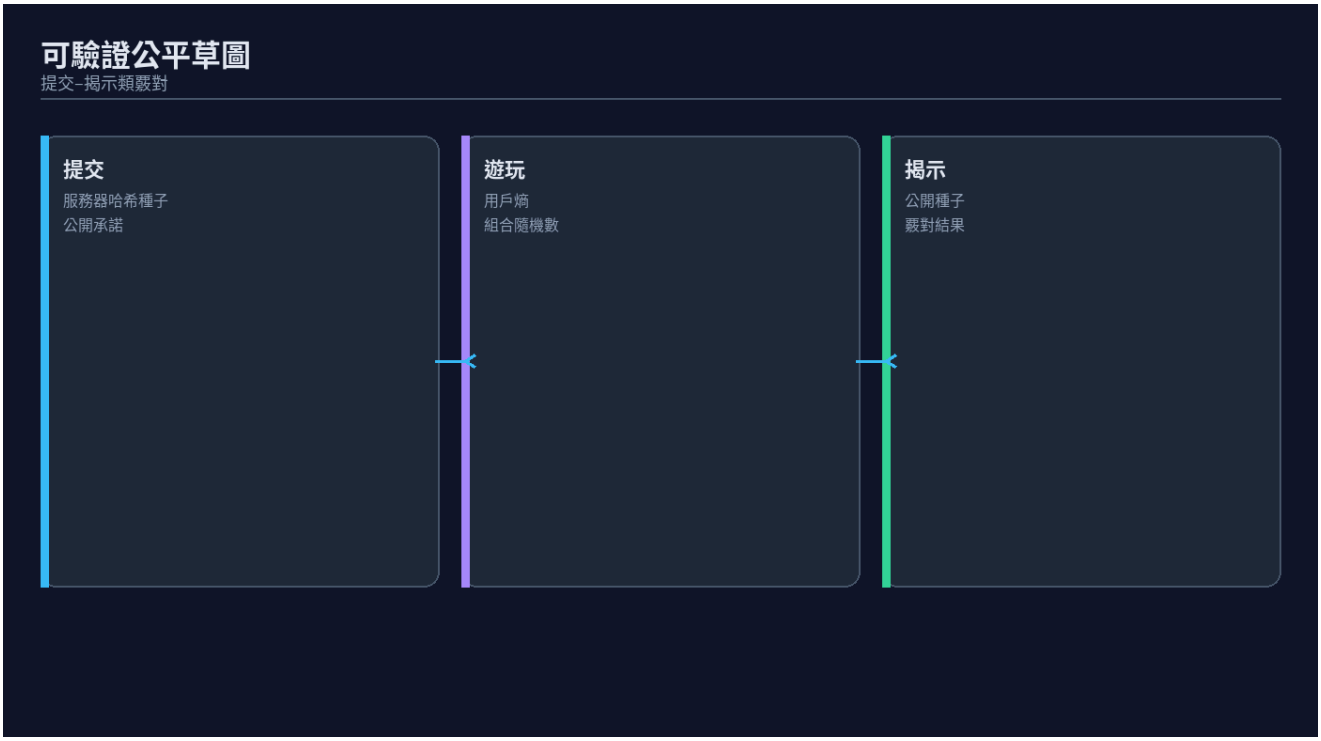
为什么单独一章?

链上常出现“可证明公平”话术。新人需要分清：**数学承诺 ≠ 合法可玩 ≠ 庄家诚信**。本章给地图与红线，不给投注策略。



链上公平性在说什么?

常见模式：提交哈希承诺 → 开奖揭示 → 可核对随机或结果。它减少“事后改结果”，但**不消除**合约后门、预言机操纵、前端篡改、出金拒绝与法律风险。



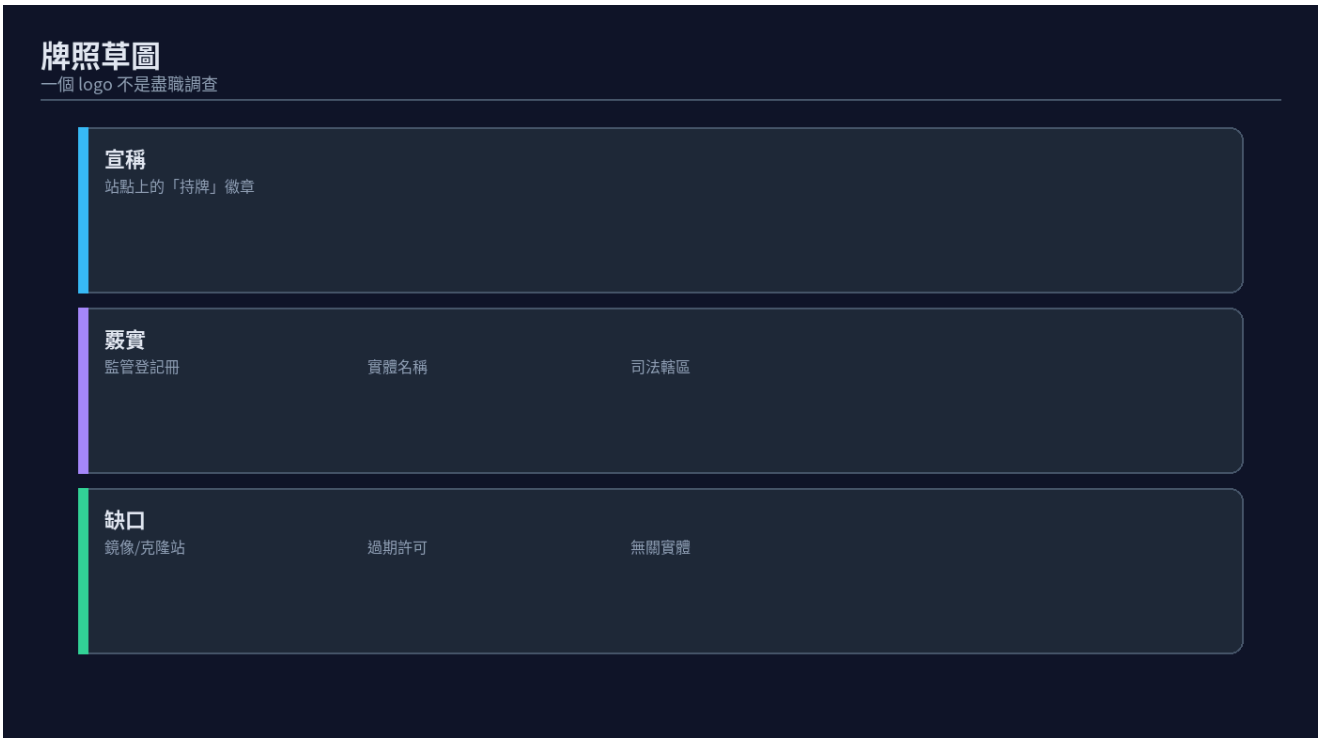
结算轨道

投注、派彩、托管合约、跨链桥都会引入对手方。教育上把它当作**高风险结算**，与第 13 章支付壳同类阅读：限额、审计、是否可暂停、资金是否托管。



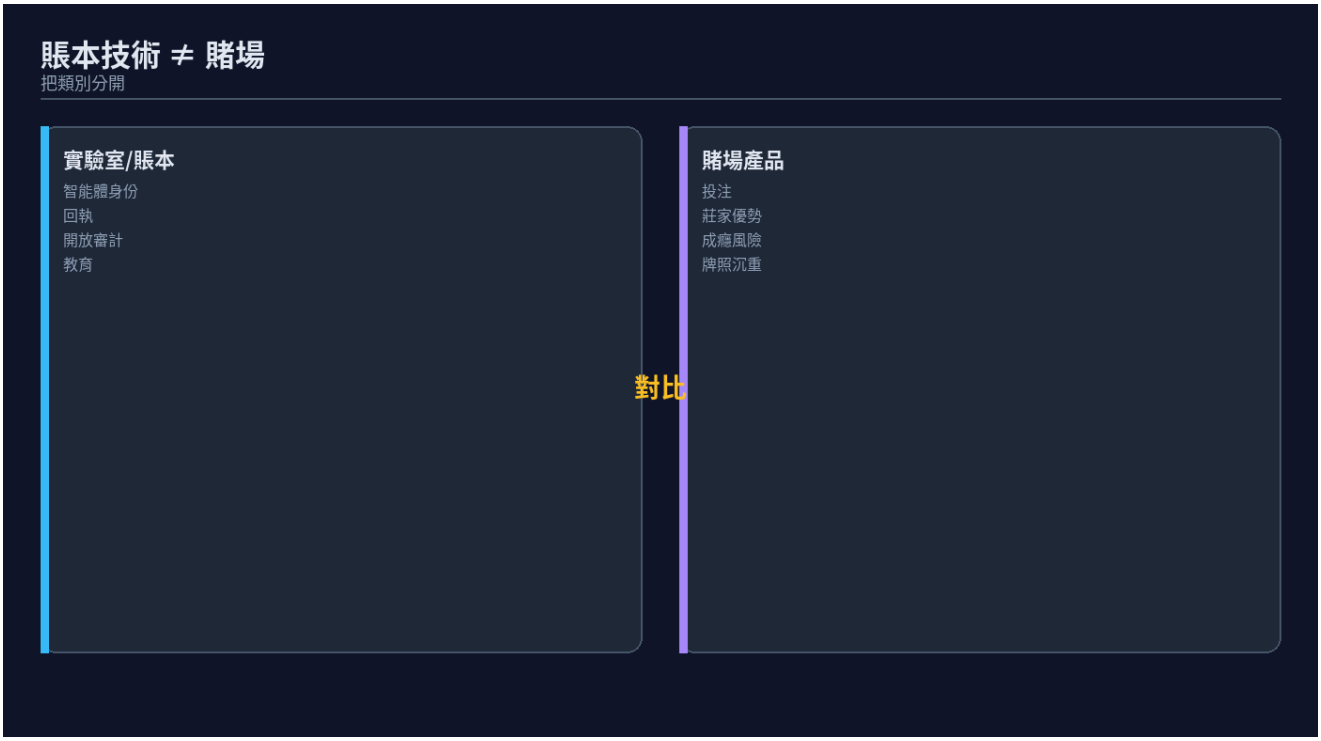
牌照与投诉（AU 高层示意）

数字资产兑换与博彩可能分属不同制度。SCDO 公开材料中的 **AUSTRAC DCE / AFCA** 是运营兑换相关披露语境，**不是**“已获赌场牌照、可以放心赌”的意思。各地博彩牌照、广告与年龄限制极严——以当地法律为准。



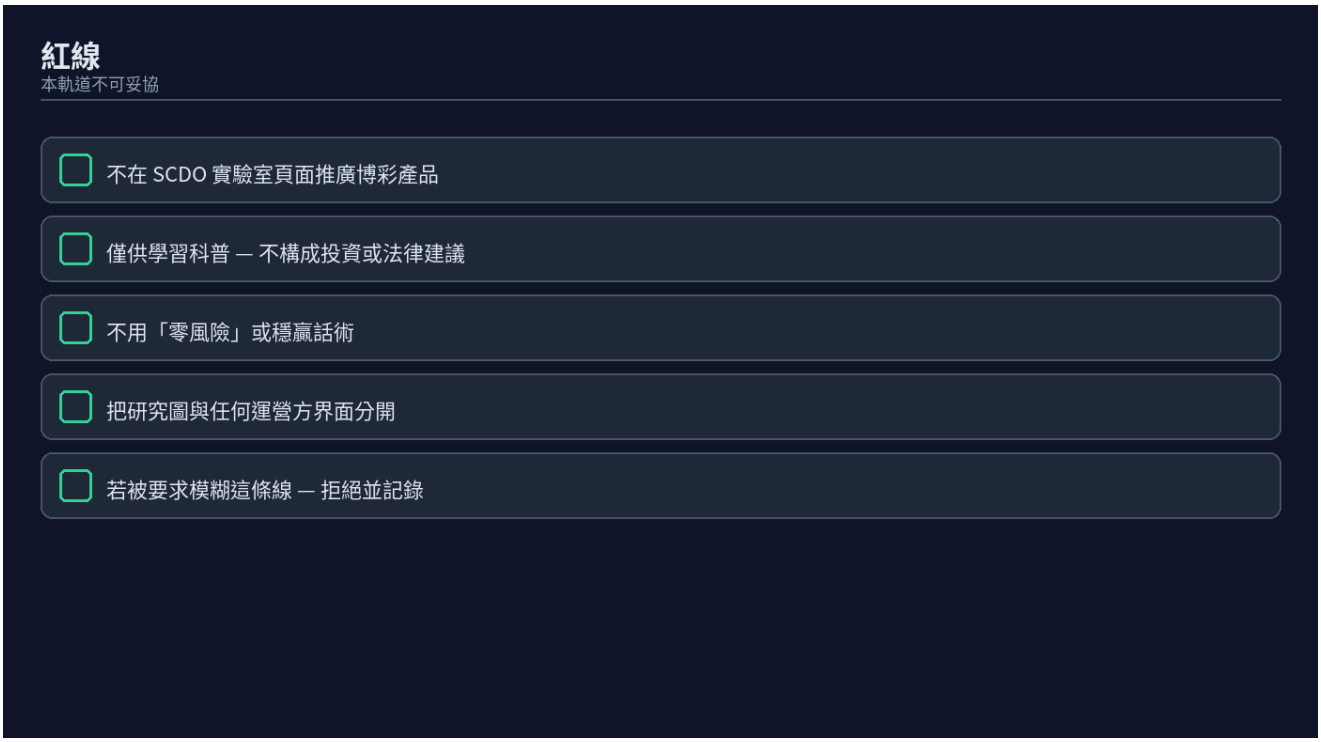
SCDO games / ledger 角度（克制）

若官网出现游戏向实验或账本能力，应读作：**可验证记录与权限边界的技术演示**，并遵守当地法律。Agent Ledger 用于代理记账，不是赌场后台。



红线清单

1. 不提供赌博教程，不引流赌场。
2. 不把技术演示写成可玩合作方。
3. 不教翻墙入金、不教规避 KYC。
4. 未成年人与禁赌地区：直接离开。



本章收束

博彩章的任务是**降噪**：公平性话术要拆解，结算要当高风险，合规要本地化，SCDO 相关能力不当赌场广告。全书回到可验证与安全习惯。

（第 14 章 · 博彩视角 · SCDO Lab）