

SCDO Laboratory · TECH PR · UNIT 03

AI智能體的合約賬本自動化 · 下一代智能支付系統

公鏈地圖：智能體落哪條鏈

讀懂主網、共識與生態取捨 · Ying Willam Zhang · 2026

免責聲明：本書內容僅供學習與科普，不構成投資、法律或稅務建議。

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**

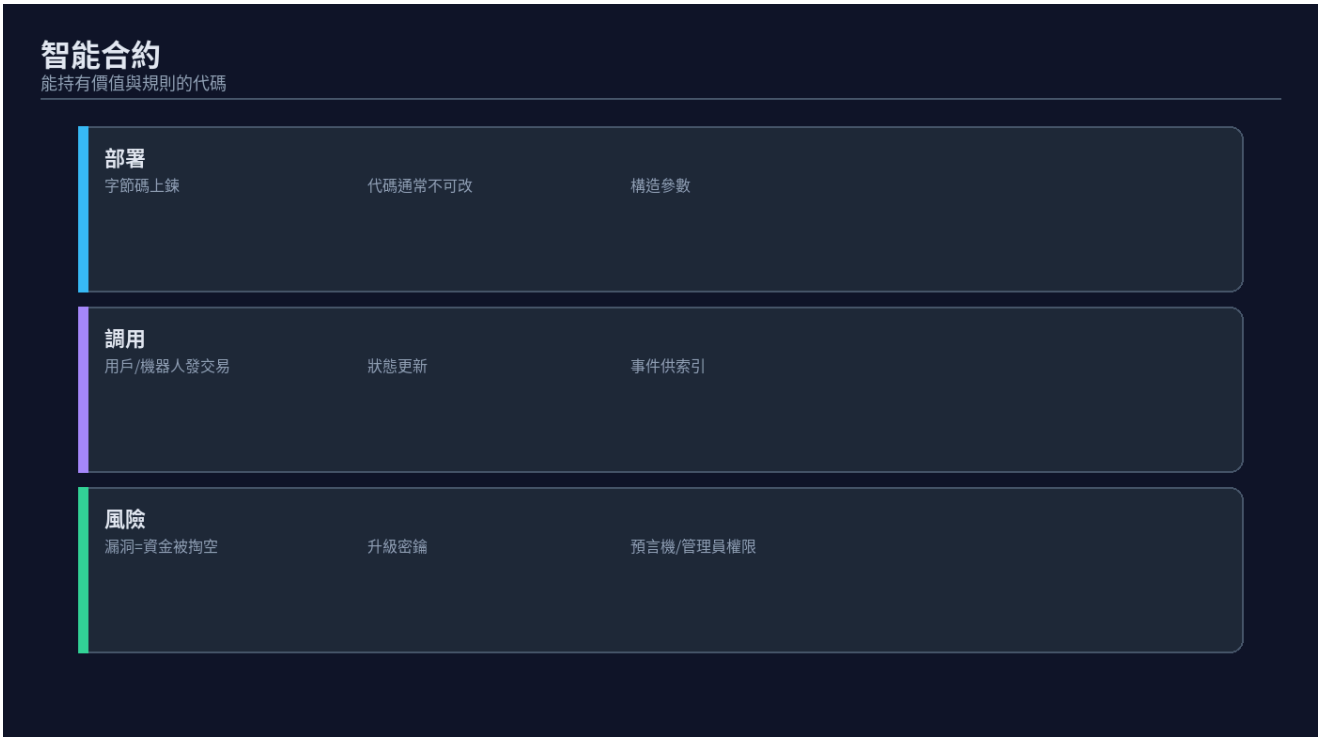
	比特币	以太坊（2026）
编程	脚本有限	EVM 智能合约（图灵完备，有 Gas 限制）
账户模型	UTXO	账户余额 + 合约账户
费用	BTC 手续费	ETH Gas（可很贵；许多用户改走 L2）
升级节奏	极保守	有路线图，但仍需广泛共识

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。

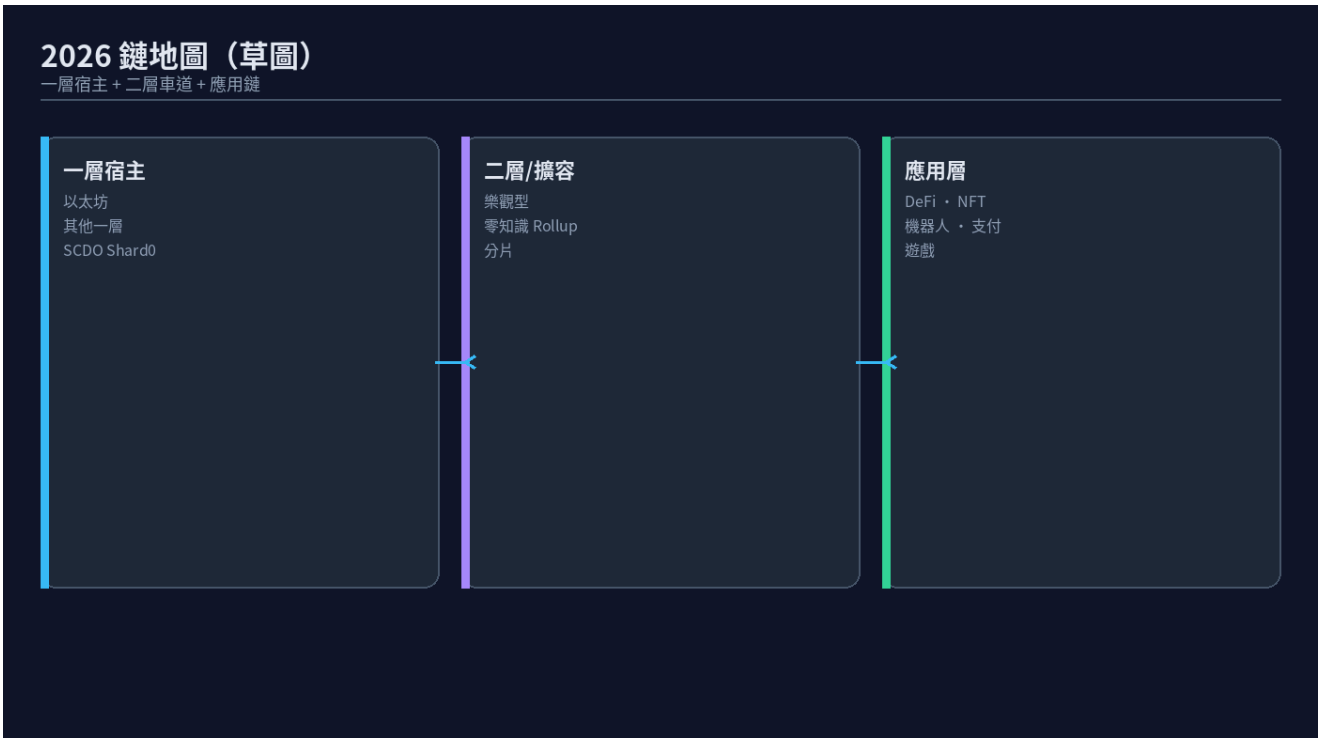
实际演进中，炸弹被多次**推迟**，以配合路线图；社区用硬分叉调整参数是常态，而不是“引爆炸弹毁灭网络”的科幻片。

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）