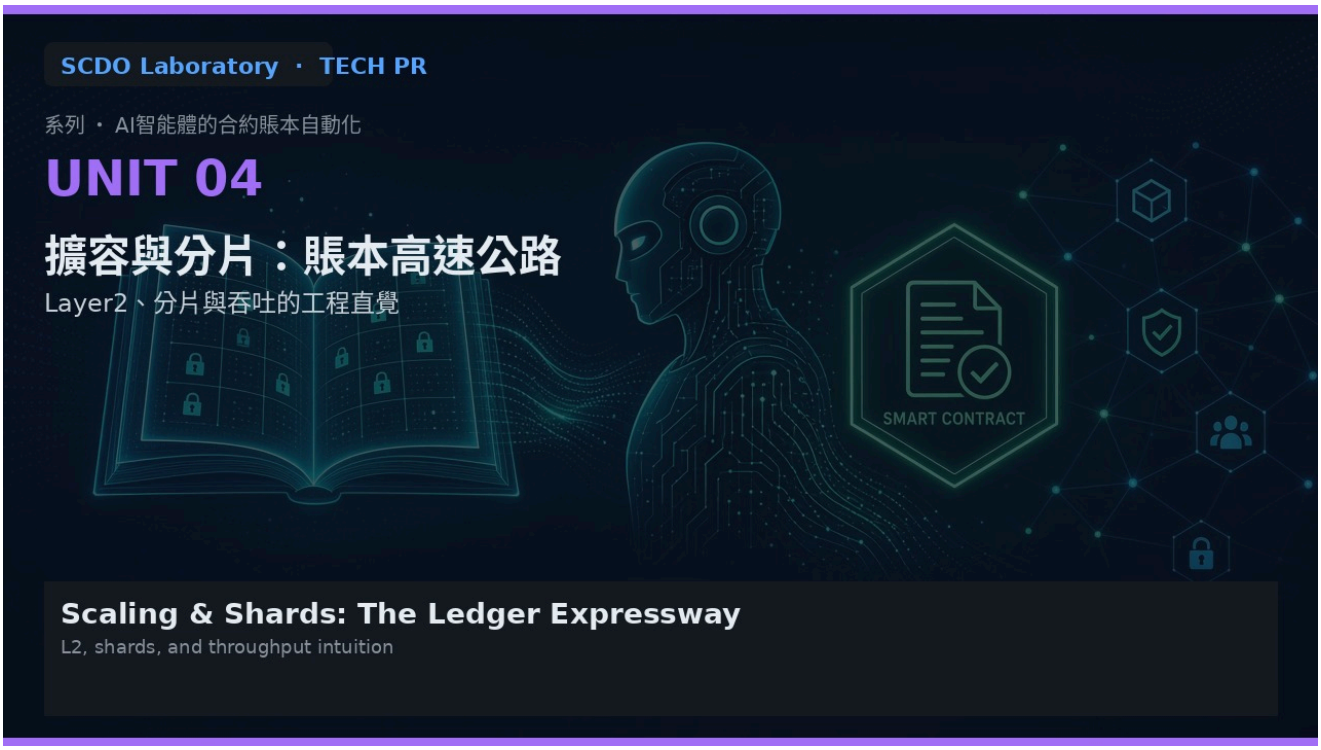


SCDO Laboratory · TECH PR · UNIT 04

AI智能體的合約賬本自動化 · 下一代智能支付系統

擴容與分片：賬本高速公路

Layer2、分片與吞吐的工程直覺 · 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。

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：

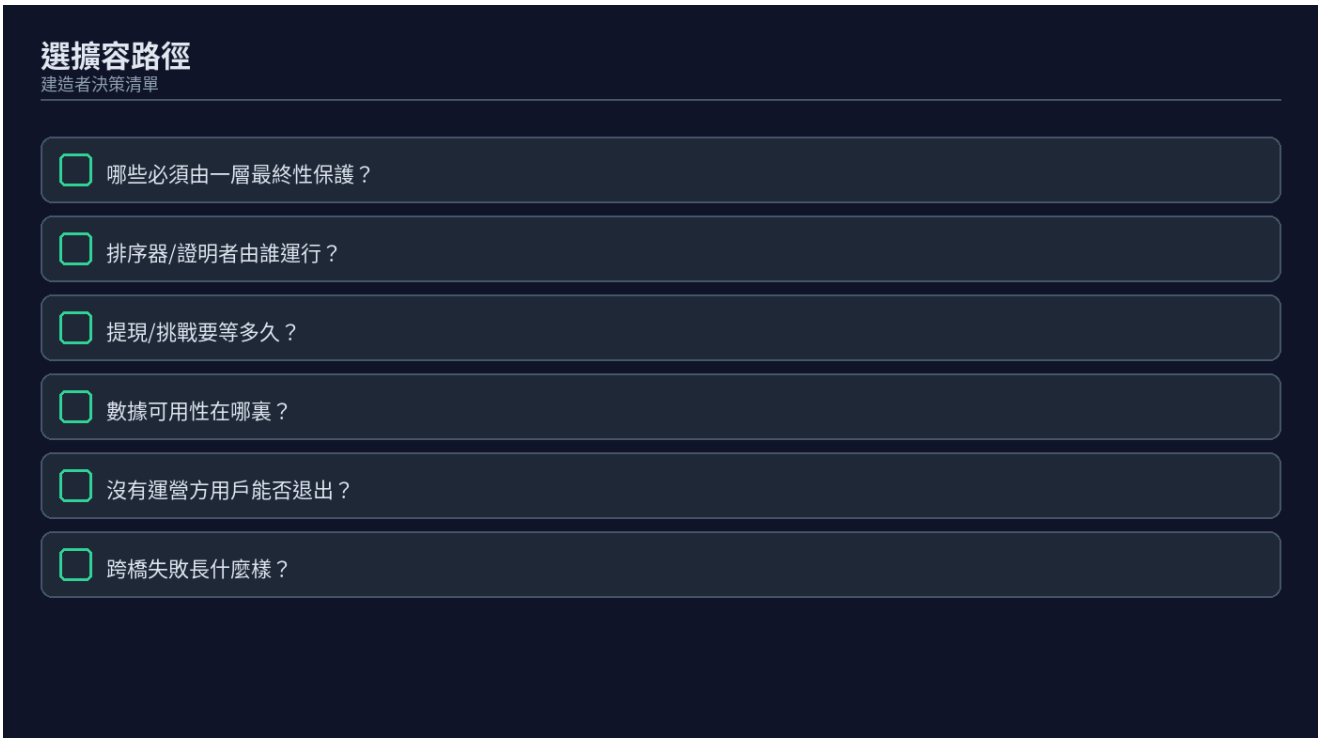
1. 在 L2 执行一堆交易；
2. 把压缩后的数据（或承诺）发到 L1；
3. 用一种机制保证“二层没乱记账”——要么靠欺诈证明，要么靠有效性证明。

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）