

SCDO Laboratory · TECH PR · UNIT 02

AI智能體的合約賬本自動化 · 下一代智能支付系統

Web3入門：智能體的互聯網

從帳號到錢包，下一代應用座標 · 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。

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**。

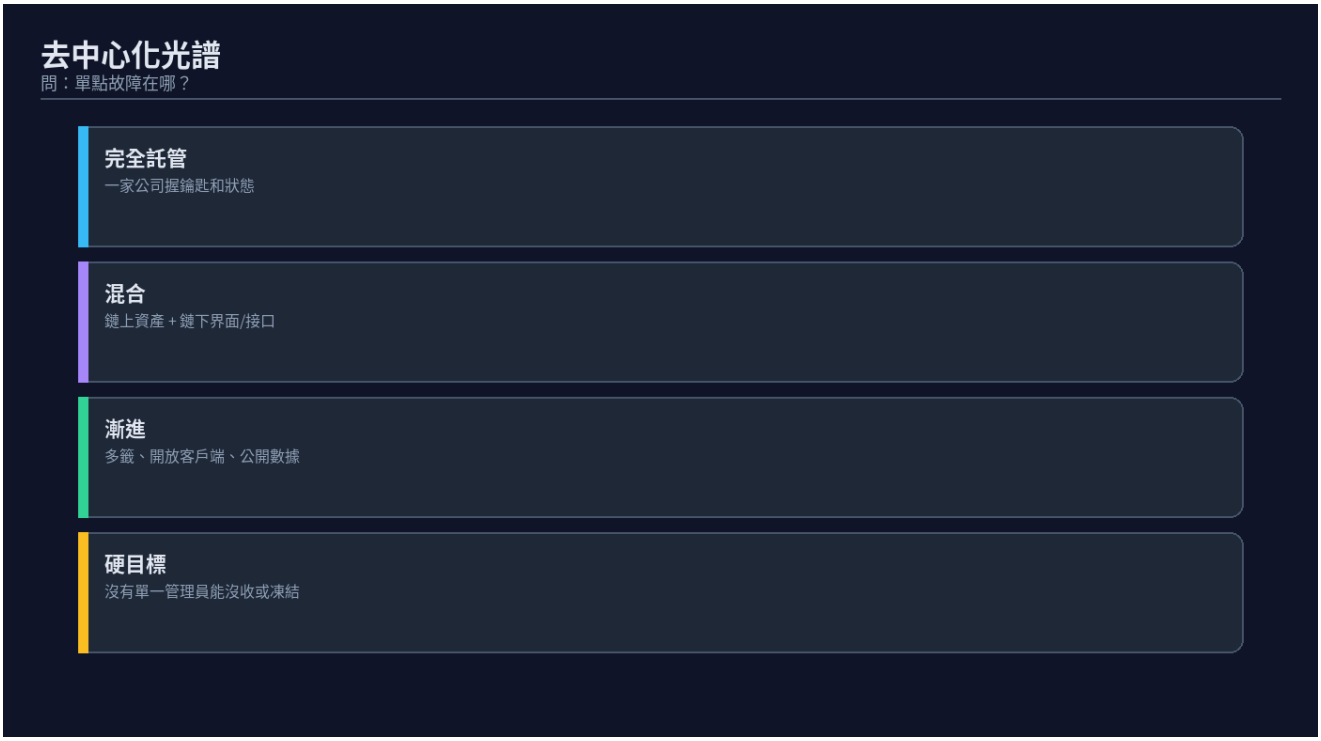
- 密码学让普通人也能加密通信、自持资产——巨头不容易单方面抹掉你链上的币（司法与托管场景另说）。
- 但流量、法币出入金、手机应用商店、合规牌照，仍高度中心化。
- 许多“Web3 应用”前端还是普通网站，域名被掐、接口被关，体验照样挂。

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：

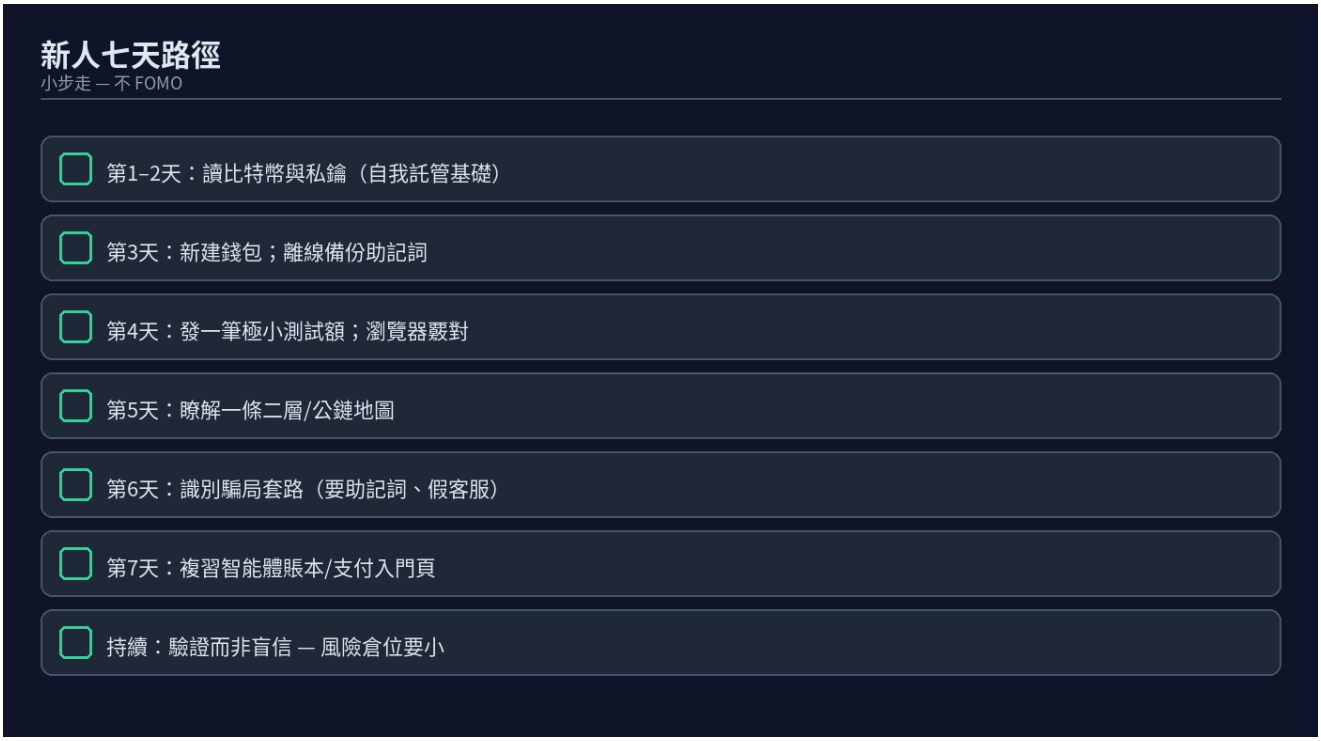
- **可编程支付与金融积木（DeFi）**：兑换、借贷、抵押——好用，也有清算与合约风险。
- **公开可查的凭证（NFT 等）**：票务、徽章、会员、道具证明“你持有过/持有着”。
- **跨境价值传输的另一条轨道**：在合规允许的前提下，作为补充通道存在。

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）