

SCDO Laboratory · TECH PR · UNIT 05

AI智能體的合約賬本自動化 · 下一代智能支付系統

DeFi樂高：合約裡的金融積木

CEX/DEX、流動性與風險邊界 · 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。

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**。

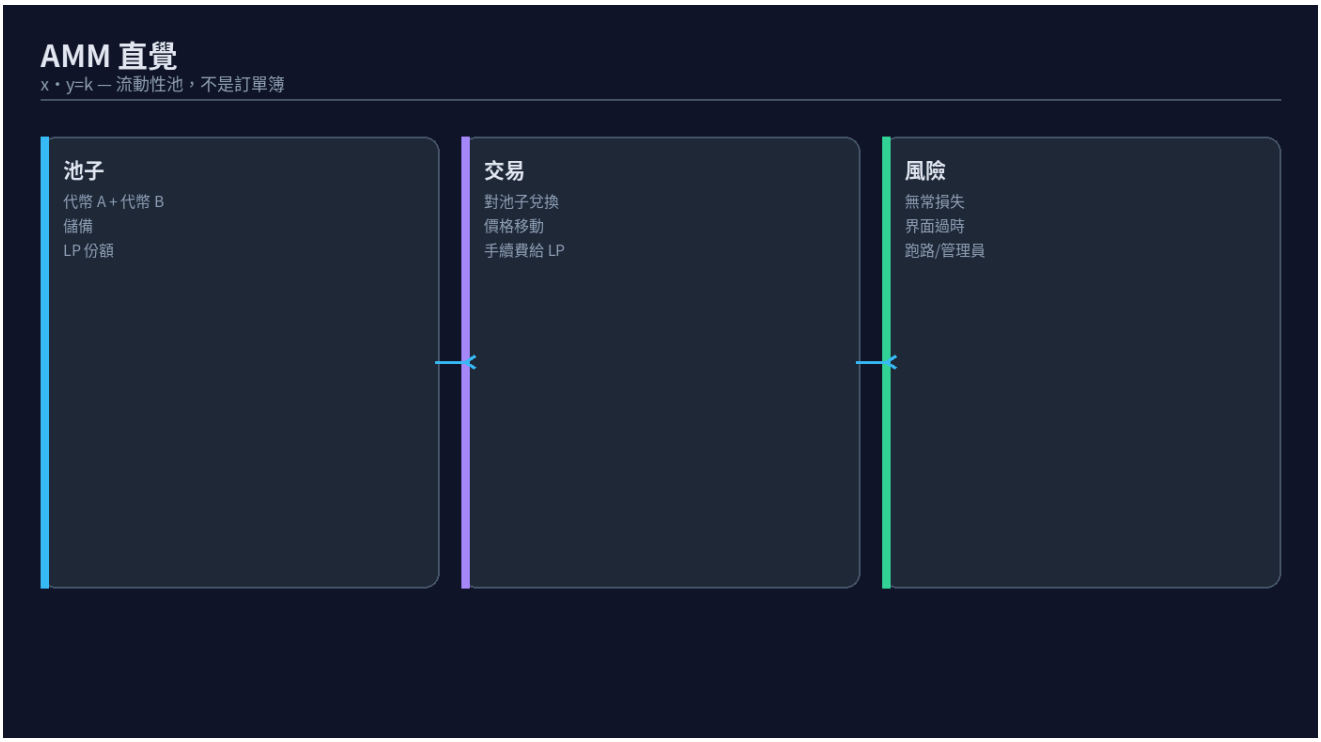
特点和优点（也是双刃剑）

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。

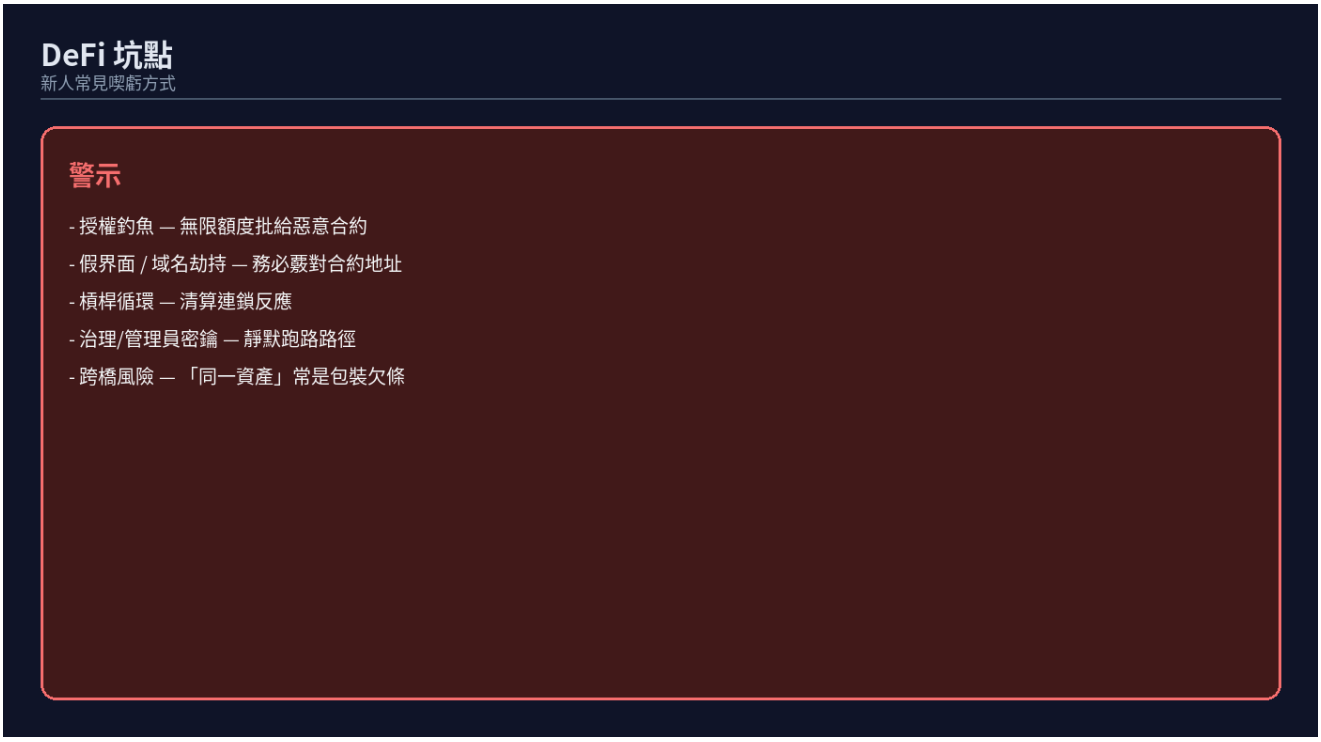
核心零件通常是：

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）