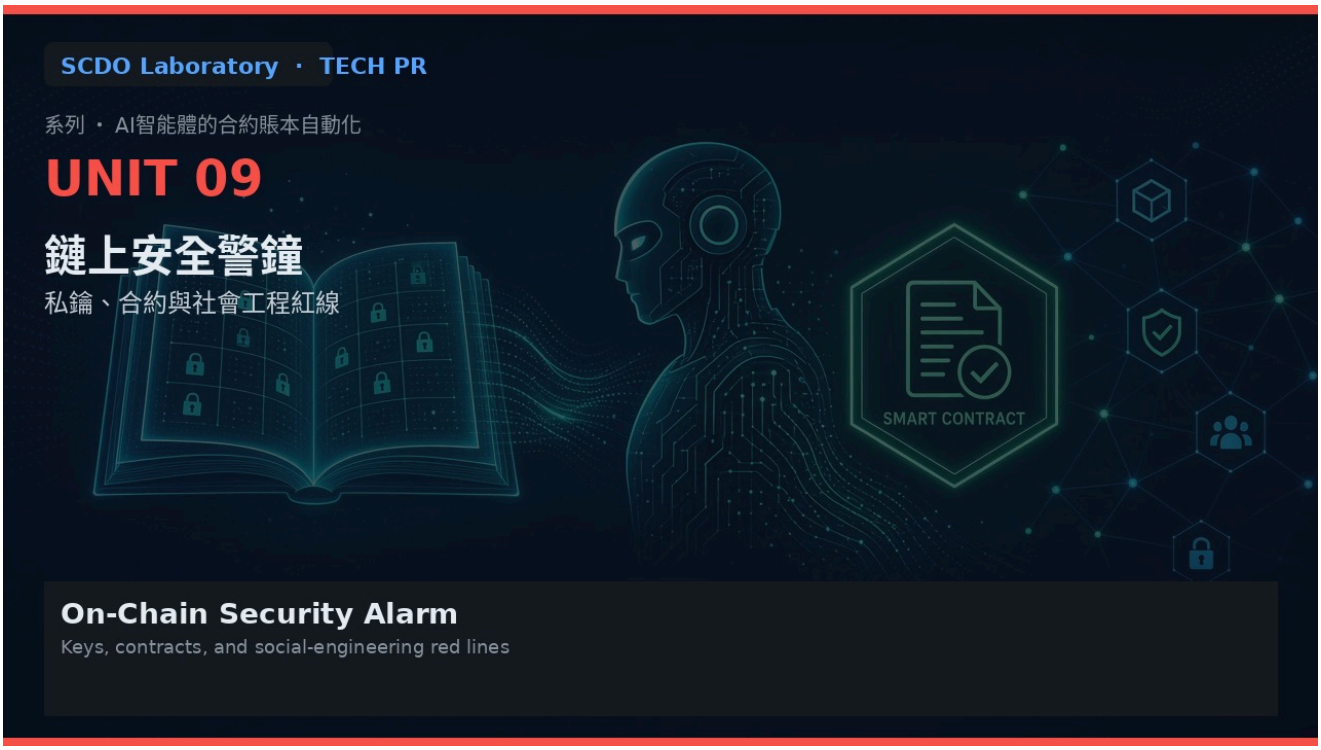


SCDO Laboratory · TECH PR · UNIT 09

AI智能體的合約賬本自動化 · 下一代智能支付系統

鏈上安全警鐘

私鑰、合約與社會工程紅線 · 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。

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

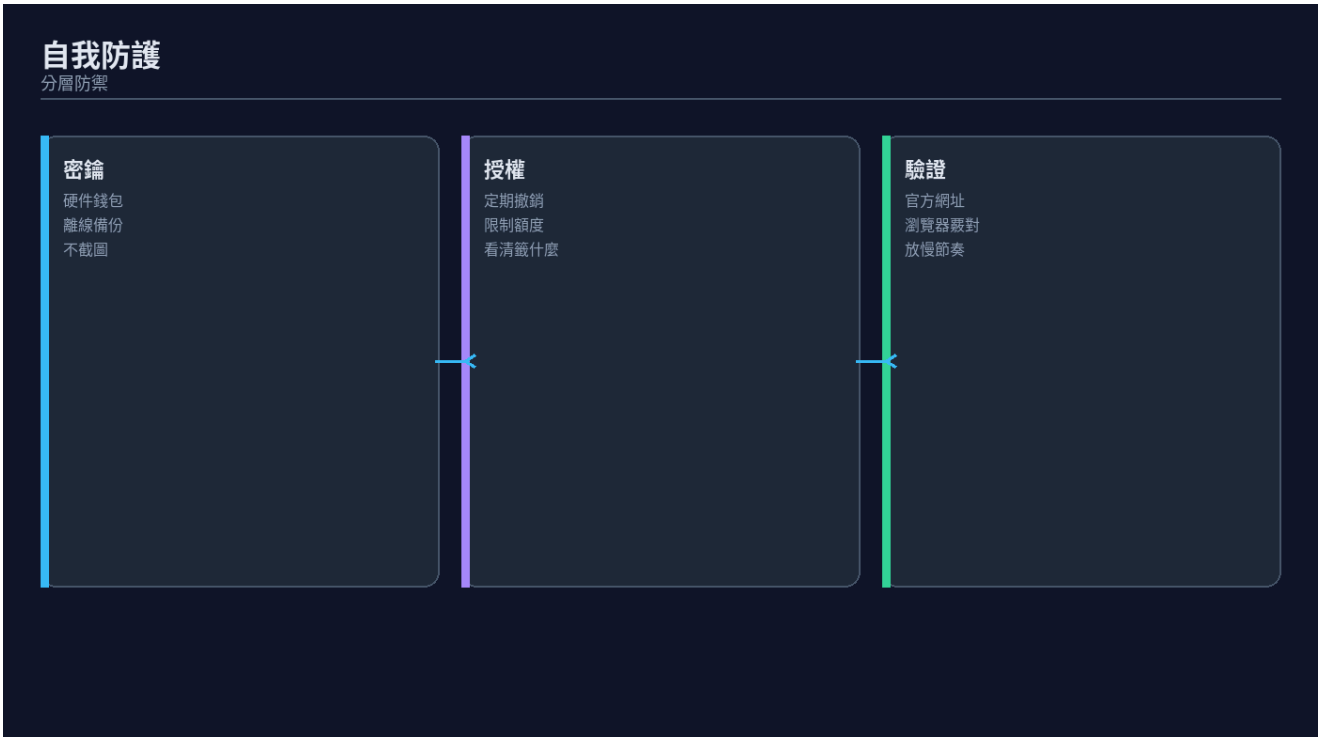
NFT 场景特供坑

- 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**。

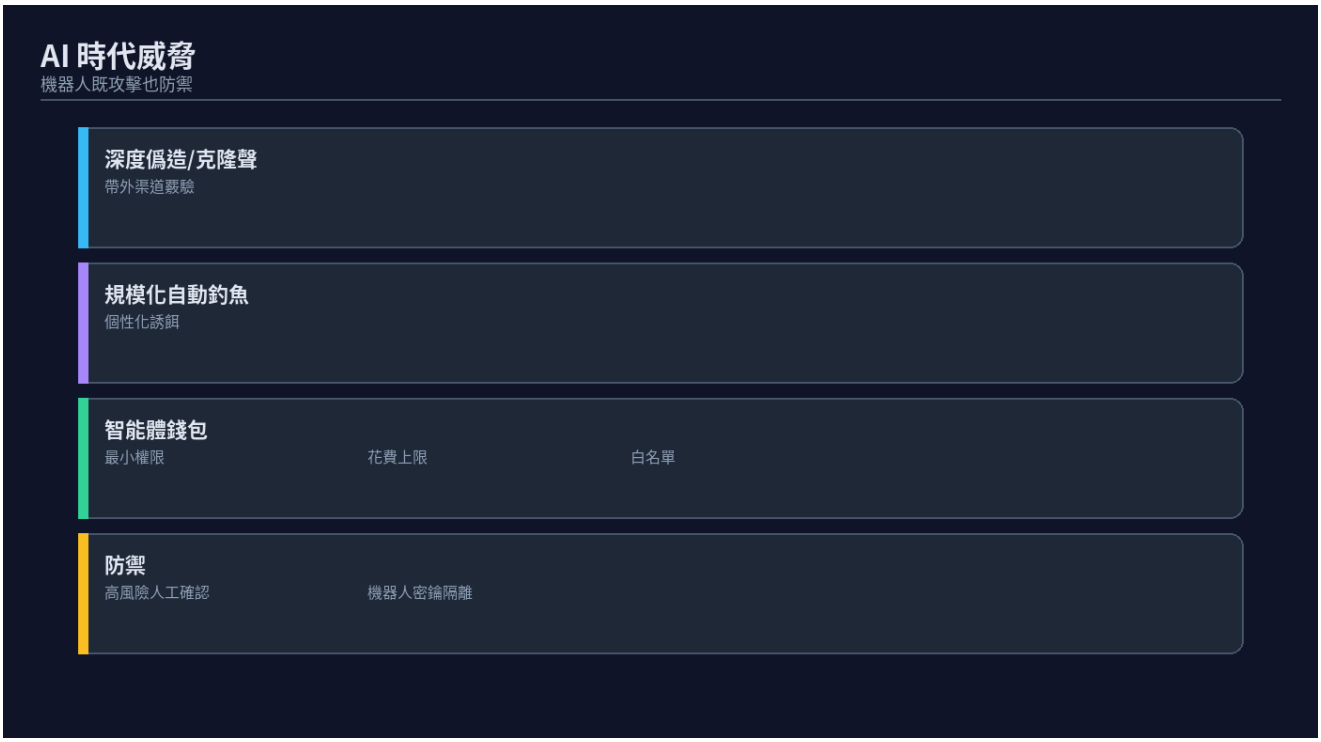
风险分类速查（原则转述）

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。

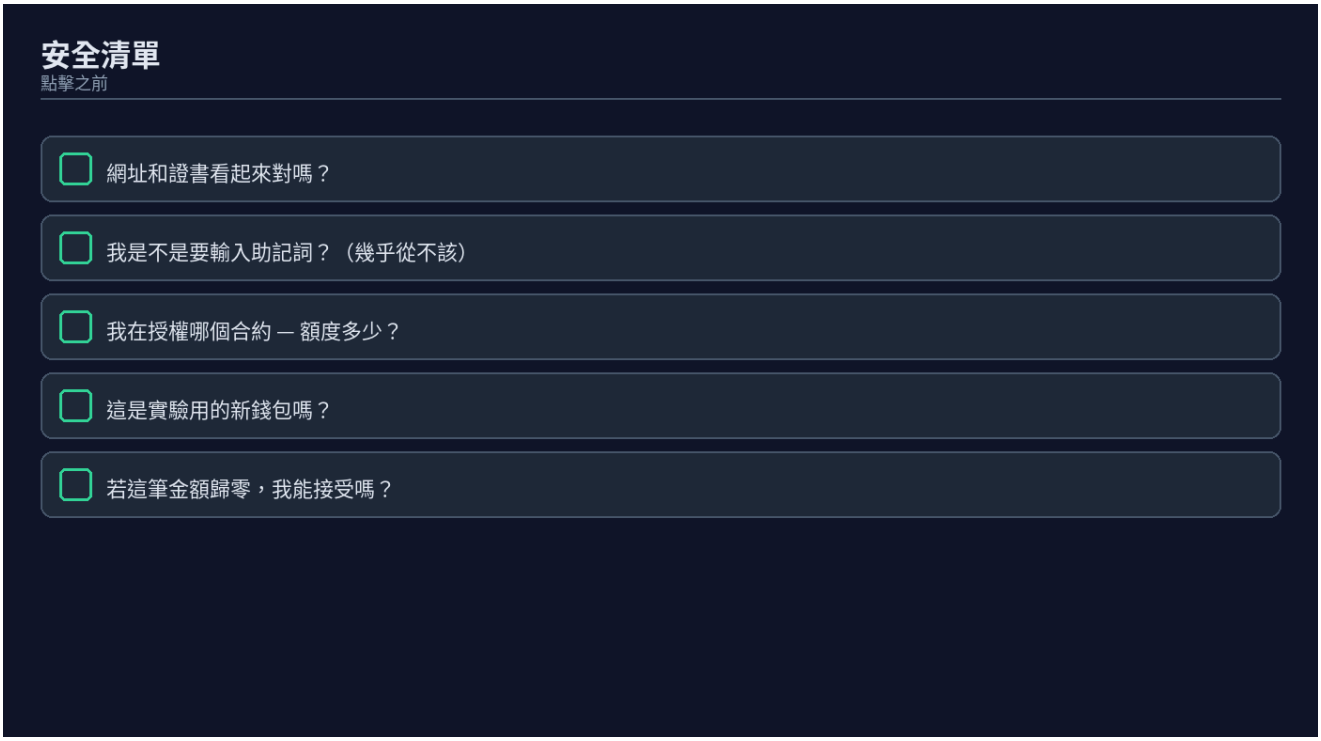
物理与供应链

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）