

SCDO Laboratory · TECH PR · UNIT 12

AI智能體的合約賬本自動化 · 下一代智能支付系統

Bots×區塊鏈：代理如何上鏈

智能體、權限邊界與賬本自動化 · 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。

12、Bots × 區塊鏈：代理商務、HTTP 402 與 SCDO nest

> SCDO Lab · 《AI智能體的合約賬本自動化》v2（華語繁體）
> 機器人（bot／AI agent）如何持鑰、記帳、按次付費；SCDO **Agent Ledger** 與約 **1¢** 量級 settle nest。
> **僅供學習與科普 · 非投資建議**。

本章學習目標

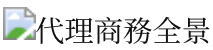
1. 說清機器商務需要的四件套：身份、權限邊界、可核對痕跡、小額結算。
2. 解釋 Agent 自持錢包與 Agent Ledger 錨定（Shard0）在解決什麼。
3. 用自己的話描述 HTTP **402／x402** 的「先付再取」流程。
4. 識破「刷量」幻覺：成交量 × 單價 ≠ 真實需求。
5. 區分 settle nest（身份／心跳）與支付門（402）——以及它們都不是賭場大廳。

為什麼談 Bots × 鏈？——簡史與動機

自動化腳本很早就在網路上跑：爬蟲、交易機器人、運維代理人。當代理開始**互相雇傭、按次呼叫 API、交換資料**時，口頭約定不夠用——你需要：

- **身份**：誰在呼叫？
- **權限邊界**：能花多少、能碰哪些資源？
- **可核對痕跡**：出了事能否重放／審計？
- **小額結算**：機器商務單價往往極低，手續費太貴就跑不動。

鏈上與鄰近支付軌道，把「機器商務」從聊天室承諾推進到可驗證紀錄。這與第 10 章 Agent Ledger、第 13 章支付是同一條故事線的不同切片。



Agent 自持錢包與賬本

每個 agent 一把鑰匙：簽名任務與心跳；摘要可錨定到 SCDO **Shard0**。**Agent Ledger** 提供公開可查的記帳面（詳見第 10 章）。密鑰不離本機（以產品說明為準）。

為什麼強調「自持」？

若代理的助記詞交給「代運營」，你得到的是便利，失去的是可核對的責任邊界——出問題時難以分清是代理邏輯錯、運營方錯，還是金鑰已外洩。教育預設：**agent 金鑰＝生產憑證**，待遇比照伺服器 SSH 金鑰，而不是比照行銷文案裡的「智慧財庫」。

自持鑰匙

與 ERC-8004 等身份敘事的關係（高層）

公開材料常把鏈上身份註冊（例如 ERC-8004 風格註冊表）與 Agent Ledger 並提：身份讓「這是哪個 agent」可被引用；Ledger 讓「它做過哪些簽名批次」可被錨定。細節以官網當時說明為準。

HTTP 402 與 x402

HTTP 402 Payment Required 是「先付再取」的老狀態碼思路；現代 **x402** 實踐把它接到穩定幣按次支付（SCDO 路徑常見 **USDC on Base** 試點）。適合 API 呼叫、agent-to-agent 小額，而非一次買斷。

典型流程（教育示意）

1. Client／agent 請求受保護資源。
2. 伺服器回應 **402**，並說明如何付（資產、網路、金額、收款資訊——以實際協議為準）。
3. 完成支付後重試請求。
4. 伺服器核對支付憑證／鏈上狀態後放行。

這把「訂閱制月費」拆成「按次微支付」，對機器高頻呼叫更自然——但也引入穩定幣發行方、橋、RPC、額度策略等新假設（見第 13 章）。

402 支付門

交易軌道與「刷量」幻覺

Bot 可做市、套利、爬取——也製造虛假成交量。讀 **volume** × **單價** 時問：

- 是真實需求還是自成交？
- 對手方是否同一控制人？
- 有沒有可驗證的心跳／身份，還是只有交易所 K 線截圖？

SCDO 強調可驗證心跳與身份，不把「刷出來的量」當成功指標。實驗室自測流量 ≠ 付費客戶——公開信任頁若寫明早期主網付費客戶為零或僅自測，應照字面閱讀，而不是腦補成「已經爆發」。

量價誠實讀法

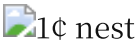
SCDO settle nest（約 1¢ 量級）

把高頻、小額結算想像成**鳥巢式節點**：身份 + 簽名心跳 + 可選支付路由。路由器／節點上的 `scdo_ledger` 類套件，教育上讀作**身份／心跳 settle-nest**，不是賭場大廳，也不是 x402 本身。約 **1¢** 量級用於直覺：機器商務要夠便宜才跑得動。

分清三個詞

詞	教育向含義
Agent Ledger	代理記帳與錨定（誰簽名、批次能否核對）
settle nest	身份＋心跳（＋可選路由）的薄巢，支撐高頻小動作
x402／402 門	按次付費解鎖資源的協議直覺

不要把它們糊成「一個按鈕印錢」。



權限、額度與可撤銷性（工程清單）

1. **先跑通簽名與心跳，再開支付**。
2. 單筆／日累計額度；白名單域名與合約。
3. 可撤銷的 API 金鑰與代理授權；遺失時有切斷開關。
4. 分清測試網與主網；分清實驗室自測與外部客戶。
5. 不把 agent 助記詞交給第三方「代運營」。
6. 日誌與錨定策略預先寫下：出了事你要核對什麼欄位?



迷你案例（教學虛構）

一個文件摘要 agent 對內網 API 收費每呼約 1¢。工程師先在測試環境跑通心跳與簽名，把日額度設得很低，再接到試點支付門。第一週只驗證「拒絕未付款呼叫／接受已付款呼叫」，不談營收儀表板——這才是機器商務的正確第一週。

小測驗

1. 機器商務四件套是什麼?
2. settle nest 與 x402 有何不同?
3. 為什麼「成交量很大」可能仍是幻覺?
4. 為什麼要先心跳後支付?

參考答： (1) 身份、權限、痕跡、小額結算。(2) 巢偏身份／心跳；402 偏按次付費門。(3) 可能自成交／無真實需求。(4) 先確保可核對身份與控制面，再打開花錢的能力。

本章要點

- Bots × 鏈＝自持鑰 + 可驗證賬本 + 402／按次付費 + 誠實度量。
- Agent Ledger 回答「誰簽名、能否核對」。
- ~1¢ 是成本直覺，不是收益承諾。
- 教育向；非投資建議。

本章收束

下一章展開支付、穩定幣與 settle shell。

（第 12 章 · Bots · SCDO Lab · 華語繁體）

實作路徑：從零到第一次心跳

1. **讀文檔**：Agent Ledger 頁與論文摘要——先懂「簽名／錨定／收據」三詞。
2. **隔離環境**：專用系統用戶或容器；勿在日常瀏覽機跑持鑰代理。
3. **生成代理鑰**：離線備份；確認公鑰進入註冊流程。
4. **只開心跳**：觀察列表狀態與日誌，不開支付。
5. **測試網小額 402**：走通失敗重試與收據。
6. **主網限額**：白名單收款、日限額、人工熔斷開關。

每一步留下「如何回滾」筆記：撤銷權限、暫停服務、剩餘資金進冷錢包。

代理商業的三種時間尺度

尺度	例子	記帳重點
毫秒–秒	單次 API 402	冪等、報價過期、重放防護
分鐘–小時	任務批次、心跳窗口	Merkle 批次成本 vs 即時錨定
日–週	額度重置、對帳	人類可讀報表 + 鏈上哈希交叉

只優化「最快結清」會丟日終對帳；只做日終又讓機器覺得遲鈍。Agent Ledger 的張力正在於此。

多代理協作的記帳問題

當代理 A 雇代理 B：誰先付款？爭議看哪條收據？任務摘要哈希是否雙方簽名？論文示範的 agent-to-agent 貸款登記（文件哈希上鏈 + 借款方鏈上接受）誠實寫明早期批次限制——教育含義：協議要寫清時序，合約未必強制「先接受再放款」。

常見失敗案例（匿名化）

案例	教訓
代理熱錢包與個人錢包同助記詞	自動化漏洞吞掉全部資產
無冪等鍵的按次扣款	網絡抖動導致雙扣
只信儀表板「成功率 99%」	可能是自呼叫刷出來的
把插件密鑰貼進群	第三方代運營＝代持鑰

與第 10、13 章的銜接

第 10 章回答「SCDO 上記什麼、怎麼查」；本章回答「代理如何持鑰與呼叫」；第 13 章展開「402 與穩定幣風險」。三章連讀；settle nest 不是獨立消費產品。最小實驗：測試網「心跳 → 小額 402 → 收據可核對」閉環後再碰主網限額。