

2026 國泰金控技術年會 #Agentic AI #IT現代化 #數位資產

一天，八場，447 分鐘

Cathay Technology Conference | 第七屆 | 現場 400 人、線上 1,500 人

121,935 字逐字稿 8 份摘要 447 分鐘錄影

2026 年的國泰金控技術年會是第七屆，也是國泰推動數位轉型的第十年。現場 400 人、線上 1,500 人，歷屆累計參與近兩萬人次。全天議程圍繞三個主軸編排，而八場內容彼此互相引用的密度相當高——下午講者引用上午的論點，最後一場的結語回頭呼應開場。

/ 三個主軸

Agentic AI 與數位同事（場次 03、05、08）國泰把 AI Agent 進化成「數位同事」：有員工編號、有辦公室（受控執行環境）、有員工守則（[Agent.md](#)）、有工時（任務排程）、有薪水（Token 額度）、有直屬主管。三位數位同事 Vanessa、Sherlock、Lawrence 現場實機演示。

AI 驅動 IT 現代化（場次 06、07、08）從 Google Cloud 的 Agentic Enterprise Framework，到國泰自己的 AI SDLC 與 6+1 Squad Team，再到用 BMad Framework 把需求管理交給 Agent。

數位資產與 Web3（場次 09）虛擬資產服務法今年通過後，金融機構與 VASP 的合作路徑、機構級保管技術，以及 Agentic Payment 帶來的 KYA（Know Your Agent）責任歸屬難題。

/ 貫穿全場的四句話

- 「科技會改變金融，但真正改變金融的是勇於改變的人。」 — 科技進程影片
- 「AI 是一個放大器，它放大的是已經存在的東西。」 — 顏勝豪 Otto，場次 07
- 「大家不是在 deploy 一個 agent，你是在 onboarding 一個 agent。」 — 李倩 Maggie，場次 05
- 「AI strategies generally die in the middle.」 — Oliver Jay，場次 03

/ 幾個值得單獨記住的數字

數字	出處
90%+ adoption、70%+ weekly active	國泰導入 OpenAI Codex 給集團所有總部同仁的實際使用率（場次 01）
15 個月 → 6 週	OpenAI 推出新世代模型的節奏變化（場次 03）
10,000 個 agent	OpenAI 研究團隊協作解開一個世界級數學難題的規模（場次 03）
4,500 題	政大為 20 家銀行打造金融大語言模型的評測題數（場次 05）
98%	Security Agent 在第一層 Alarm Triage 可達到的 reduction（場次 06）

數字	出處
150+ 套系統	國泰集團已完成上雲的系統數（場次 01、07）
8.45 兆美元	穩定幣今年的月均交易量，較去年成長約七成（場次 09）
25.5 億美元	2024–2025 年中心化交易所 20 起攻擊的總損失（場次 09）

/ 關於這份摘要

八場錄影共 447 分鐘，以 openai-whisper large-v3 轉寫後人工校閱、整理成摘要。逐字稿全文共 121,935 字。

三件在整理過程中發現、需要知道的事：

- **場次編號沒有 04。** 原始檔案中標示為「Oliver Jay」的檔案，經位元組比對與場次 03 的檔案完全相同。Oliver Jay 的演講並未遺失，它就在場次 03 的 36:20 之後——該檔實為 10:25–11:15 的連續錄影，涵蓋兩場。
- **場次 05 的錄影長 80.6 分鐘，但真實發言在 50:20 結束。** 主持人在該處宣布午休，其後 30 分鐘是午休的環境音。
- **場次 01 與 02 內容重疊。** 場次 01 的後半段就是完整的爐邊對談。

摘要中的人名、數字與專有名詞建議對照原始影片核實；場次 09 的台大法律系教授姓名，機器轉寫為「楊若平」，已標註待核實。

2026 國泰金控技術年會・會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。

開場致詞 Opening Remarks

開場致詞 Opening Remarks

國泰金控科技長 | 姚旭杰 Marcus Yao

09:40–09:45 有效內容 47.4 分鐘 逐字稿 13,478 字

⚠ 本檔涵蓋範圍大於標題：包含開場、科技進程影片、Marcus 致詞，以及後續完整的爐邊對談（與場次 02 內容重疊）。爐邊對談的摘要請見 02。

/ 一、年會定位

2026 年為國泰技術年會**第七屆**，也是國泰推動數位轉型的**第十年**。現場 400 人、線上 1,500 人，歷屆累計參與近 2 萬人次。

今年聚焦三大主軸，全天議程即依此編排：

1. Agentic AI 與數位同事
2. AI 驅動 IT 現代化
3. 數位資產與 Web3

/ 二、科技進程影片：十年轉型的自我敘事

- 轉型範圍從金控、銀行延伸到人壽、產險、證券，跨子公司、跨業種協作
- 「數據的下水道工程」——地基打得夠，AI 才能真正起飛
- 核心系統翻新的難度：「像一邊開火車一邊換引擎，一刻都不能停」
- 上雲不只是把資料搬到雲端，而是徹底翻新運作體制
- VASP、虛擬資產、RWA、穩定幣，表面是新技術，**核心其實還是信任**

「科技會改變金融，但真正改變金融的是勇於改變的人。」

/ 三、科技長 Marcus 致詞：核心競爭力是 Trust

全場論述收斂到單一命題——**國泰的核心競爭力就是信任**，而科技的價值是讓信任可以持續被建立、被驗證、被放大。

規模化的信任（關鍵數據）

指標	數字
Cube App 月活躍客戶	500 萬，逾 1,500 萬筆交易／月
Cube 信用卡月刷卡人數	500 萬
人壽／產險／證券／數位平台	各至少 100 萬 MAU
智能助手「阿發」	每月服務 100 萬客戶
上雲系統	超過 150 套
國泰世華三大中台	承載數百隻自核心移轉的微服務

Trust Infrastructure 的兩層意涵

Marcus 以太太不會問「今天 Cloud Migration 做得怎麼樣」、只會說「明天 Cube 卡友優先搶票，你們最好不要當機」為例，定義客戶信任 = 服務可靠 + 系統穩定 + 資料受保護。

因此上雲與中台不只是 IT strategy，而是 Cathay's Trust Infrastructure；而這個基礎建設不只含硬體網路系統，也包含人與工作方式。

最具體的一項揭露

今年已導入 OpenAI Codex 給集團所有總部同仁，短短幾個月達到超過 90% 的 Adoption、超過 70% 的 Weekly Active Usage。

（此數字在下午 Oliver Jay 的演講中被引為「給 AI 廣泛存取權」的正面案例。）

提早佈局而非等候發生

- 2017 年成立 Blockchain 團隊，研究區塊鏈、加密貨幣、虛擬資產
- 幾年前成立 Quantum Computing 團隊——因為今天所信任的加密與資安，未來都可能被重新定義

「Innovation takes us forward. Trust makes sure we move in the right direction.」

/ 可行動要點

- Codex 90% adoption／70% WAU 是集團級 AI 導入的可對標基準線
- 「信任基礎設施」的框架可直接複用於向管理層說明上雲與中台投資的理由
- 提早佈局的兩個標的（區塊鏈 2017、量子運算）顯示國泰對「技術風險窗口」的判斷節奏約為 5-8 年

爐邊對談

國泰下一個十年：從數位轉型到持續進化

主談人 國泰金控副董事長 | 蔡宗翰 Joseph Tsai / 主持人 國泰金控副總經理 | 施君蘭 Lana Shih

09:45-10:15 有效內容 34.2 分鐘 逐字稿 9,725 字

/ 核心命題

這場對談最值得記下的不是成功經驗，而是**兩次公開承認的失敗**，以及從中提煉出的判準：數位轉型的出發點必須是業務痛點與客戶，不能是 IT 本身。

/ 一、起點不是「數位轉型」

蔡宗翰 2005 年回台、2016 年展開轉型，但當初的起心動念與數位無關：

- 在國泰人壽，**業務前線總覺得總公司不懂客戶、沒聽過客戶的聲音**
- 銀行也一樣，理專與分行經理認為總行不知道前線要什麼，「往往都是擋我們而已」

「當初是想要解決這個問題，不是為了數位而數位。」

當時國泰的網站由 IT 部門管理，業務團隊根本不把它當通路，只視為一個諮詢網站。

/ 二、失敗案例一：以 IT 為出發點的大型轉型

- 邏輯是「要數位化 → 需要很強的 IT → 找最好的專家顧問 → 規劃一個很大的 IT 轉型」
- 規劃規模約 **90 幾億**
- **走不到一年半就開始出問題，整個計畫最後收回**

失敗原因（蔡宗翰自述）：

「出發點只是純粹想要去整頓 IT 而已。還是沒有理解說我們到底需要什麼，前線需要什麼，BU 需要什麼，客戶需要什麼。**我覺得這個出發點是錯的。**」

/ 三、失敗案例二：KOKO 品牌

- 品牌 Logo 選了很久、討論第一個產品是什麼、甚至開了門市
- 結果發現：**客戶不想要再一個 App**——功能沒有厲害到足以打動他們再下載一個 App
- 更根本的原因是「下水道的工作沒有做好」，系統沒整理好之前，想推新的客戶體驗與 UI/UX 非常困難

/ 四、Cube 的設計哲學：把選擇還給客戶

- 當時信用卡部門有 **18-19 張卡** 在推給消費者，客戶皮夾裡十幾張卡，誰用得完
- 核心念頭是「**Empower 客戶**」——讓客戶拿一張卡就能自己決定回饋方式，而不是由公司幫他訂定或再推一張新卡
- 第一版做出來發現系統做不到即時更換優惠，**退回去整理系統整整一年**，直到能做到「每天可以更換想要的優惠」才推出

「一年給你換一次，那就沒有意義了。」

/ 五、下水道工程：四五年沒有 return 的投資

- 系統多導致資料庫多、規格不一，不整理就在運作與彈性上受限
- 與數據團隊花了**整整四五年**，帳面上完全沒有 return
- 但今天 Cube 平台的彈性與開發機會都建立在此之上

「Everybody invests the penthouse, but nobody invests the basement.」（主持人引述）

/ 六、文化改變：從上對下到多溝通

蔡宗翰認為十年來最大的文化改變是溝通，而非技術：

「20 年前回來的時候，我不懂公司開會的方式——走進去，一個主管站起來，把投影機上的資料唸給你聽。會議就結束了，也沒有結論。叫了 20 個人來開這個會，我就不懂意義是什麼。」

現在會議多半時間在討論，而且刻意要聽基層同仁看到的問題。

/ 七、對 AI 的判斷

- 現在整個產業處於「**AI drunk**」階段（喝了、醉了），情緒兩極——什麼都可行，或什麼都好可怕
- 但它終究是 incredibly powerful 的工具：**不是讓工作消失，而是工作機會會轉變，說不定更多**
- 對團隊的明確要求：「**我們不要做一些 window dressing，做給你看看而已**」——要實際挑戰現在的運作方式、流程、思考方式，甚至從產品設計端就開始調整
- 競爭格局：金融業高度監管，彎道超車有挑戰；但其他產業裡，**幾個人的小公司真的有可能挑戰大型競爭者**

/ 八、未來三到五年：兩件既興奮又睡不著的事

1. **從客群分眾走向真正的 Personalization**——針對個人需求與喜好服務，而非用客群分類
2. **工作場景的意義感**——集團 5 萬多名員工，希望每天做的事是有意義有價值的；對報表、核對、填奇怪小東西這類日常雜務正是 AI 能改善的
3. 附帶觀察：台灣今年經濟成長約 13-14%，財富創造帶來面對社會挑戰的機會

/ 可行動要點

- 判斷任何轉型專案的第一個問題應該是「客戶會覺得有什麼不一樣」，而非「IT 要怎麼強化」——這是 90 億專案失敗換來的教訓
- 基礎建設投資要有「四五年無 return」的心理準備與管理層共識
- 導入 AI 時明確禁止 window dressing 型專案，要求動到實際流程

2026 國泰金控技術年會，會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。

專題演講 #Agentic AI #數位同事 #人機協作 #ChatGPT #Agentic Enterprise

從 Agentic AI 到 Digital Colleague / From GPT to the Agentic Enterprise

梁明喬 Joe Liang • 劉浩翔 Jeremy Liu / OpenAI International, Managing Director | Oliver Jay

10:25-11:15 有效內容 70.4 分鐘 逐字稿 35,419 字

本檔為連續錄影，涵蓋官方議程的兩場：10:25 的中文專題演講，與 10:55 起 Oliver Jay 的英文演講。

⚠ 原始檔案清單中另有一個標示為「1055-1115 Oliver Jay」的檔案，經位元組比對與本檔完全相同。Oliver Jay 的演講並未遺失，就在本檔 36:20 之後。

上半場：數位同事 (Digital Colleague)

/ 一、技術脈絡

國泰連續三年以 AI 為技術年會主題：2024 年發表 Gaia、去年發表 Gaia 2.0。

Gaia 2.0 四大模組：

1. Orchestration 協調層
2. Runtime 執行環境
3. Protocol 協定層 (MCP、A2A)
4. Agent Marketplace

過去一年已把國泰內部運行 AI Agent 的基礎框架搭建完成。

/ 二、「數位同事」與一般 AI Agent 的三個關鍵差異

	一般 AI Agent	數位同事
記憶	活在單一 session 裡	跨 session 長期記憶，可共事數月仍記得你是誰
主動性	人說一動做一動	自主推進長程任務，會自己喚醒自己推進下一步
對象	面對單一使用者	識別組織中不同人事時地物，對不同角色做出不同回應

/ 三、與真人員工的鏡像設計

真人員工	數位同事
員工編號	系統獨立帳號與編號
辦公室	受控邊界的運行環境
員工守則	<code>Agent.md</code> 行為邊界
打卡工時	任務排程（可設 7×24，且不違反勞基法）
薪水	Token 額度——依職等與能力分配不同 Token 數量與可呼叫模型
姓名、email	名字加 <code>.ai</code> 後綴、有自己的 email
直屬主管	設定 reporting line，知道誰是 mentor、老闆、同事

Agent Profile 層 包含：`Agent.md`（行為準則）、`Identity`（身份角色）、`Soul.md`（人格與風格，甚至可寫 MBTI）、Skills（技能庫）、Memory。

/ 四、管理機制四大模組

1. 獨立且可識別的身份
2. 人機協作模式與**責任邊界**的釐清
3. 資源與成本管理
4. Performance 衡量

/ 五、三位數位同事的實機 Demo

Vanessa — 數位 TPM（Mentor：昌宏）

展示三項能力：- **業務世界觀**：知道「智能平台專案」指的是什麼，每天主動撈取與自己相關的任務 - **主動性**：在專案看板發現兩個長期逾期且無人處理的任務，主動提出「找工程師 Carson 支援」的建議解法（不只回報問題，還給可裁決的方案） - **跨通路存取**：橫跨 Teams、Outlook、OneDrive、專案看板——查看板找出逾期任務 → 確認 Carson 工項已完成 → 從 OneDrive 取出 API Spec 附件 → 在 Outlook 找三人共同空檔 → 自動發出交接會議邀請

Sherlock — 審查委員會（Mentor：Ann）

- 記得 10/7 委員會有一案因換模型需重做風險評估，不必重問「委員會是什麼時候」
- 已自主以 email 通知專案團隊補件並設定回覆期限
- Mentor 要求「之後這類重新送審的專案都要附上前一次審查結果」→ **Sherlock 透過調整自己的 `skill.md` 學會新的做事方式**
- **記憶寫入有審核機制**：不是無腦寫入長程記憶，Mentor 所說的必須記下，其餘節點由科技審查專員判定哪些該進長程記憶

Lawrence — 法務 (Mentor : Fanny)

- 收到業務單位急件 email 後，**主動建議把該合約從工作清單第 4 順位調整到第 2 順位**，並請 Mentor 確認
- 直接在 Word 內編修合約初稿：缺件以備註提醒、商業條件以螢光筆標示
- **主動補齊缺漏的次承攬條款**，並提醒承辦單位確認該業務是否適合承攬給第三方
- 完成後存檔、寄給法務同事與對應金管轄區的複核同事、附重點摘要與自己的署名，再透過 Teams 回報今日完成與明日待辦

專業能力來源：技術團隊與法務室緊密合作，梳理日常流程與 Domain know-how 寫成 skill，再持續測試迭代。

/ 六、數位同事的三階段職等藍圖

階段	能力
Level 1	特定單一任務；一對一面對 Mentor
Level 2	主動喚醒、主動追蹤、舉一反三、自我學習；跨任務型態的記憶學習；可與同部門多位同事協作
Level 3	完整企業世界觀、成熟自我學習機制；可對跨單位不同組織與角色做出相對應回應

「就像 Spider-Man 一樣，能力越大責任越大，**那當然 Token 也會越來越大。**」
「Human and AI Better Together.」

下半場：Oliver Jay (OpenAI) — From GPT to the Agentic Enterprise

Oliver Jay 以三個最常被問到的問題組織整場演講。

/ 問題一：What has changed?

AI 的四段演進

1. ChatGPT 剛推出時**只是 chatbot**，甚至不是很聰明的 chatbot
2. 2024 年發明 **reasoning** 新典範，模型開始會思考（從國中、高中程度一路躍進）
3. 去年是 **agents** 元年——不只回答問題，而是**完成任務**
4. **現在的主題是 agents 如何協同工作**——ChatGPT 或 Codex 處理複雜任務時會自行 spawn 子 agent 去搜尋網頁、另一個 agent 做資料分析、再有一個 agent 統籌編排

上週的新聞：研究團隊用 **10,000 個 agent 協作**、花一到兩週解開了一個世界級數學難題。

其他關鍵變化

- **模態**：今年是語音崛起的一年。GPT Live 是第一個真正對話式的語音模型。**舊金山辦公室的開發者已經不打字了，他們用講的，由 agent 寫程式。**
- **給台灣的具體建議**：許多人回饋「用中文與 agent 互動更 token-efficient」——「讓你的 CFO 開心一點，用中文跟你的 agent 互動。」
- **專門模型**：今年推出資安模型 **Daybreak Red / Blue** 與生醫模型 **Rosalind**。「如果你是銀行、如果你管理關鍵基礎設施，現在正是利用這些模型的窗口。」
- **成本**：策略是在任何智能水準上都提供最低成本的模型；企業部署已從用單一模型改為**用一整個 family of models**，因為不是每個任務都需要最高智能
- **研發節奏**：從加入時的 **15 個月**推出一個新世代模型，縮短到現在的 **6 週**（5.6 → GPT-6 Astra，10 天前發表）
- **GPT-6 Astra**：意外解鎖的用例是 **3D rendering**；指令遵循能力極強（例如產出符合企業品牌調性的簡報）

從 Intelligence Era 到 Effectiveness Era

ChatGPT Work（Codex 與 ChatGPT 的合併，7/9 推出）**已突破 2,500 萬週活躍用戶。**

Oliver Jay 特別點名的兩個用例：- **自建網站**：他自己 15 分鐘內用自然語言（手機上）做出原本需要資料科學家排隊取數、工程師開發的儀表板；他 8 歲的兒子用語音為媽媽做了一個安排全家行程的網站 - **Computer Use**：讓 agent 像人一樣操作電腦。「事實證明，很多任務上電腦操作電腦比我強——更快、不會漏看、閱讀網頁的速度遠超過我。」典型場景是報帳（拍收據 → agent 自行判斷要登入 NetSuite → 提示你登入 → 擷取非結構化資訊填入結構化系統 → 需要授權才執行的動作會先問你）。「**如果你是 CFO、想壓縮結帳天數，computer use 是你最好的朋友。**」

台灣數據

- **Codex 使用量是全球前 10 的國家**——「台灣的人口絕對不是前 10。」
- ChatGPT 上**每三則訊息就有一則與工作相關，且成長了 35 倍**

/ 問題二：領先企業有何不同？

1. 心態：從 Scarcity 到 Expansive

- 過去經營公司是 **scarcity mindset**——看有多少預算、多少人，算出最多能做什麼。這是 productivity。
- 領先企業的心态是：「**如果我們不受限制，我們完整的野心是什麼？**」先問這個問題，再用 AI 填補落差。

「這是個微妙的差別，但我真的認為這個心態轉變非常關鍵。」

2. 使用強度的 escape velocity

前 10% 使用者的 output token 相對於其他人：**年初不到 3 倍 → 6 月已達 8 倍。**

3. AI 不只屬於開發者

OpenAI 內部 agentic 任務佔比：工程從去年中就快速爬升，但 ChatGPT Work 推出後，財務、招募、法務全面跟上——最新一張圖顯示 sales 的使用率已超越 engineering，工程師們有點受傷。

4. ROI 的正確衡量方式

重點不是 cost per token，而是 cost to complete a successful task。

低成本模型的單位 token 便宜，但可能要試更多次、花更久才能完成任務，反而燒掉更多 token。「如果低成本模型能準確、安全地完成工作，太好了——但真正重要的是完成工作的總成本。」

/ 問題三：領導者如何把 AI 變成成長？四件事

1. 給 AI 廣泛存取權——「你會非常驚訝創新來自哪裡。管理層往往看不到第一線的日常。」（明確點名國泰把 ChatGPT 與 Codex 給了所有人是好例子）
2. 從 business outcome 出發，不是從技術出發——否則你會花一兩年建一個永遠不夠完美的 data lake，都還沒開始產生價值
3. 由上而下以身作則——AI 會重新佈線很多工作方式，領導層若沒有完全買單並持續談論 AI，變革管理做不起來
4. 要求主管當責——「AI strategies generally die in the middle.」中層是摩擦最大、風險最高、恐懼最多的地方。最簡單的起手式：要求每位 VP、每位總監回答「這一季你要用 AI 改造哪一個 workflow、產出什麼結果」

/ 可行動要點

- 數位同事的「鏡像設計」（編號／辦公室／守則／工時／薪水／主管）是一套可直接照抄的治理清單
- 記憶寫入的審核機制、skill.md 的自我調整，是把「學習」變成可稽核流程的具體做法
- Oliver Jay 的 **cost to complete a successful task** 應取代 cost per token 成為 AI 專案的 ROI 指標
- 「每位主管本季一個 workflow」是可立即落地的當責機制

2026 國泰金控技術年會，會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。

高峰對談 #人才轉型 #數位勞動力

當 AI 成為企業新同事：數位勞動力與治理新秩序

主持人 施君蘭 Lana Shih／陳冠學 Quincy Chen・劉浩翔 Jeremy Liu・李倩 Maggie Lee・王儷玲 Jennifer Wang

11:35-12:15 有效內容 50.2 分鐘 逐字稿 16,623 字

/ 一、Quincy：不做漸進式，直接建一個與 AI 合作的團隊

面對「如何讓 AI 能力真正滲透進龐大的金融組織」，國泰世華選擇的不是漸進調整：

- 直接 build 一個與 AI 一起合作的 Team，規模約原 Scrum Team 的 **三分之一**
- **不做實驗室專案**——接的是其他 Scrum Team 同樣會接的真實需求
- 用「拓荒者」快速撞到能力天花板，再從成功經驗做快速輸出

「與其讓大家漸進式地調整，我們要直接去 Build 一個跟 AI 一起合作的 Team。」

目前已有成功範例並進入**擴大輸出期**，最近上線的部分 Cube App 功能已是由這個 AI Scrum Team 產出。

撞到天花板之後的真正瓶頸

「我有一段高速公路可以開到 200、300 都沒問題的時候，你馬上就知道哪個地方會塞車。」

塞車點依序是：1. **數位化根本不完整**——很多人說要 AI 做這些事，「你連數位化都沒做到，你連 API 都沒有」
2. **知識 Silo**——即便企業體內有知識，仍散落各處，必須全部打通 3. **80 分等於零**——「很多東西你做 80 分就會 Zero Adoption，你要做到 100 分 Adoption 才會起來。因為他會說，如果這東西只能幫我完成 50% 的工作，那我不如全部自己來。」 4. **組織與角色的重新定義**——工具都有了但人不願跨出去，「主力可能是在心態，還不見得是在 skill」

引用 Oliver Jay 的關鍵提問

「大部分人用 AI 的時候只想到前半句 *Is AI completing work?*，但真正的重點在 **matters**。我不是要 create 一大堆 Agent 去做那些 work that doesn't matter。」

/ 二、Maggie（微軟）：從 AI 助手到 Workflow，再到 Enterprise IQ

導入路徑

金融業起手多半是先給員工 AI 助手（Copilot）——撰寫文件、整理 email、RM 出門前快速備妥資料。看似簡單，但這是建立「員工該怎麼使用 AI」的最佳起點。

下一步是把 AI 放進 **workflow**：「在金融業通常不會有一個工作是由單一個人完成的，它要跨組織、跨系統、跨角色。」

兩個國際案例

- **AD Financial (美國)**：客服接線後的大量手打整理工作交給 AI，人類專注處理客戶敏感問題與同理回應
- **Rabobank (荷蘭)**：用 Copilot Studio 建 Customer Self Service Agent，**同時支援文字與語音**；能辨識客戶來電意圖，**能回答就回答，不能回答也不會胡思亂想**，而是導引到正確單位；信用卡掛失、重發等較複雜工作也能完成

企業的兩個能力缺口

1. **人的缺口**——不是不會用 AI 工具，而是「不知道**什麼流程**該用 AI、什麼叫 matterful、什麼產出必須 double verify」
2. **Intelligence Layer 缺口**——AI 模型負責推理，但它不知道你公司的核保規則、從屬關係、客戶過去 claim 過什麼。要在 Microsoft IQ 之上建立你自己的 **Enterprise IQ**

最鮮明的一句話

「大家不是在 **deploy** 一個 agent，你是在 **onboarding** 一個 agent。」員工走進公司你會給他識別證，你的數位員工也要有。你給他什麼 access control、什麼 data protection、怎麼 monitor 他看過哪些資料——**要像管理真實員工一樣管理數位員工**。而且要在 build 之前就想，不是 build 完才想。

對 PM 與主管的提醒

- PM 過去擅長設計系統與 workflow，未來要跨 Business User／IT／法遵去判斷：哪些題目交給 AI、哪些要人來 escalation、哪些要人做最後判讀
- 主管更辛苦——過去只管真實員工，未來要管數位員工，成為 **Hybrid Workplace**；對真實員工訂 KPI，對數位員工也要訂
- 治理建議：**中央設定標準，但由部門設計場景**

/ 三、王儷玲（政大）：金融大語言模型與評測標準

為什麼需要金融專屬模型

金融業大量知識庫跨公司甚至跨產業不能分享，又有法規限制，因此由產業聯盟主導**金融代言模型**，目前正在為 **20 家銀行** 打造銀行大語言模型。

訓練與評測方法

- **不是 RAG 的 open book 往外找答案**，而是先讓模型讀完該讀的知識庫，再測驗是否真的讀懂
- 重視**邏輯思考能力**：「我們讓 AI 去上大學讀理論基礎、讀 paper，最後考的**不是是非題選擇題，而是申論題**」
- 在訓練前先把每一題的解題思維鏈寫出來，讀完豐富知識庫後再考

- 規模：4,500 題的評測
- 四大 Domain：金融知識、法規合規、授信、財富管理（未來延伸至保險、投資）
- 必須是繁體中文版——外商已開發的 AI 能不能在台灣用，涉及台灣法規與消費者情境的差異，評測是關鍵門檻

三重安全部署的評分設計

- 總分之下再分項（法遵、消費者權益、金額大小等）並給予不同權重
- zero tolerance 項目：只要錯一題就必須重新回去訓練

AI 治理框架

呼應上午 Demo 提出的五要素：身份、職權、權限、主管、工作紀錄——這些在真人世界本來就有，AI 治理只是 attach 到數位員工身上。

關鍵設計判斷：

「Human in the loop 不是每一個點都要，而是放在一個不可逆的點，或是那個點本身會對消費者保護、風險產生重大影響的地方。」

法遵風控不能最後才出現，必須在設計 end-to-end domain 的邏輯思考階段就放進工作流程。

數位員工的 KPI 三個 Domain

1. 風險（守門員）——在 human in the loop 的斷點擋掉風險
2. 價值創造——金融業需要有溫度的加值
3. 優化——end-to-end 流程與效率的整體提升

引述 McKinsey：用 AI Agent 時 use case 不是最重要的，重要的是怎麼創造那個例外的管理機制。

工作底稿與紀錄「就像飛機的黑盒子」，用來回饋成正向循環；把人的經驗用思維鏈的方式寫清楚，放回 Agent 的工作流程，才是經驗傳承。

/ 四、Jeremy：實作踩過的坑

設計階段一定要先想好的三件事

1. 獨立身份——要能識別這個行動是人做的還是 Agent 做的。（特別強調：數位同事的責任最後還是人類負責，不能什麼事都推給 Agent）
2. 能力邊界——依職責與任務明確畫出可操作範圍，並用統一的 Gateway 管理可存取權限
3. 可視化軌跡——「總不可能 Vanessa 昨天晚上默默在後台做了什麼你不知道，這其實是蠻危險的一件事情。」

運行階段最常踩的兩個雷

雷一：記憶汙染（Memory Pollution）

記憶儲存必須有非常精密的設計——什麼時候該記、該記什麼、記下來怎麼分門別類儲存。否則「他記了太多事情之後，反而把自己所有的記憶全部汙染了，到最後產出不好的效果」。

雷二：Over-skill

公司 skill 越來越多時會有重複。「有些時候他身上背了太多 skill，他會不知道自己到底要做什麼，**他會做一大堆你感覺起來很忙、但事實上是在繞圈圈的事情。**」

/ 五、一句話結語

與談人 結語

Maggie 不要等到所有事情都有完美答案才開始；但也不要再在流程邊界還不清楚時貿然冒進。找**高價值、低風險**且能讓 Agent work 的部分，並重視 continued learning loop

Jeremy 先畫好安全邊界，然後**選一條垂直應用的賽道直接實操實作**，在實作中自然學會如何在企業環境做好 Agent Adoption

Quincy AI 要上車，但不要為了 AI 而 AI。**問價值至少要問五層**——對你的 Team、對股東、對客戶各有什麼價值？「你如果只能說做了 AI 以後茶水間可以多聊天、看盤時間可以多一點，那只是第一層價值。」

王儷玲 勇敢嘗試，但**評測控管標準要先做好**，再逐步擴大許可權與最佳化流程。已進入**雙重 Agent (teamwork)** 階段，AI 員工之間可互相 call each other，希望五年內實現

/ 可行動要點

- 「**onboarding 而非 deploy**」應作為所有 Agent 專案的預設心智模型，且治理要在 build 之前設計
- **Human in the loop 放在不可逆的點**——這是可直接寫進設計規範的判準，避免每步都卡人工審核
- 記憶汙染與 over-skill 是兩個已被驗證的失敗模式，設計 Agent 時應列入檢查項
- Quincy 的「價值問五層」可作為 AI 專案立案時的過濾器

2026 國泰金控技術年會，會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。

專題演講 #Agentic AI #Multi-Agent治理

讓 Agent 安全上工：金融產業多雲環境 Multi-Agent 的治理與國際標準合規實踐

Google Cloud 台灣技術總經理 | 林書平 Harry Lin

13:30-13:50 有效內容 26.1 分鐘 逐字稿 11,110 字

/ 核心框架

這場不談產品細節，而是給出一套 **Agentic Enterprise Framework**——企業要開發、管理、治理 Agent 時，由下而上該看哪些層：

Agent Service (最上層)
Agent Management / Operation
Security
Data
Infra

/ Agent 時代的三大支柱

- 1. **Tokenomics (Token 經濟學)** —— Agent 不再只做單一件事，而是整合一整條流程，Token 消耗自然大增。關鍵問題是：流程的每一個 phase 都一定要用最貴的 Frontier Model 嗎？
- 2. **Business Process 與 Value 的整合** —— 必須整合進業務流程與價值，才看得到 Agent 的價值
- 3. **Security** —— 任何新技術採用時永遠最重要

/ 一、Infra 層：Inferencing 不是 Training

Harry 用武俠小說比喻兩者的差別：

Training		Inferencing
比喻	練功	戰場上即時回應
特性	大量吸取資訊、成千上萬 GPU/TPU 串連、運算數百億參數	需要低 latency 與充足 context

Agent 大部分工作是 inferencing，且互動模式是**來來回回的**——你問、它答、你補 context、它給更多資訊。這意味著 Agent 要即時且正確回應，靠的是 **Context**（也就是 Agent Session／Agent Memory）。

硬體的具體回應：Google 自研 TPU 第八代把 Training 與 Inferencing 分開，**Inferencing 的 Memory 是第六代的 3 倍**；NVIDIA GPU 也為 agent inferencing 做了對應調整。

/ 二、Data 層：AI Ready Data

問題的根源

企業既有資料**不是 design for agent，而是 design for human**——Database schema 是從人的角度、按 business process 設計，再由人寫程式下 query。

三個因此產生的落差：

1. **Scalability**——Google CEO Sundar 的 vision 是內部未來至少有**幾萬個 agent** 執行所有 operation。當 agent 數量以萬計、處理速度極快時，後端 database 與 storage 撐不撐得住？
2. **Context**——過往很多 context 存在人的大腦裡。做供應鏈的人知道整條供應鏈的業務脈絡，但 agent 看到資料時沒有這個脈絡
3. **Security Control**——過往是給人或程式一個 authority。但**同一個 agent 會被經理、處長、副總同時使用**，這個 authority 該怎麼做資料控管？

Context 的三個層次

層次	內容	例子
Technical Metadata	Schema、欄位、型別與意義	這個欄位是 Integer，代表信用卡消費金額
Business Semantics	這些技術欄位背後的業務意涵	這個 Campaign 打的是什麼族群、什麼地區
Personalization	不同角色與同一 agent 互動時要的資料不同	副總看全台灣，區域經理只看自己區域的消費族群特性

Multi-modality 帶來的新資料來源

Agent 不只看得懂文字——影片、聲音、圖片都能解析出意義。以行銷活動為例，除了活動數量、參與人數等文字資料，**Campaign 的影片與宣傳圖本身也是 Context**，agent 可以把它們轉化成 Business Context。

/ 三、Security 層：用魔法打敗魔法

「現在的 Hacker 也用 AI 來 create 他的 Attack Campaign……這相當於人家在用魔法，我不可能拿著木棍木槍去跟槍砲打戰。」

攻擊面的變化：AI 生成的釣魚 email 與連結、**多模態讓對方甚至能打通 deepfake 語音電話**給你做驗證。

為什麼 Security 特別適合用 Agent

三個特性：資料量非常龐大、有一定 pattern、流程可以自動化。

實際成效：第一層 Alarm Triage 至少可達 98% 的 reduction。

Security 人員的兩種痛苦：- **False Positive（誤判）**——不是攻擊卻被判成攻擊，要花大量時間確認 - **False Negative（漏判）**——更可怕，「只要漏判一個，你就被 Penetrate 進去」

Triage 之後的完整自動化鏈：收集對應 Log 與資料 → Analyze → 對應到 CVE 編號 → 決定該 Tag 什麼 Action → Post Action。

另一個角度是 Development 階段的安全：應用服務部署上線後，從 Container Runtime、Application、Agent 到 Model 各層都可能 Vulnerability，可用 Agent 掃描整個環境。

/ 四、Agent Management 層：生態系與新的攻擊面

Agent 生態系的主要元件：**Agent 本身、Model（大腦）、Tool（MCP、Skill）、API（整合 SaaS）**；元件之間透過 A2A 或 HTTP/RESTful API 溝通。

這些溝通衍生出兩個治理議題：

Agent Supply Chain

概念與 Software Supply Chain 完全相同——過去攻擊者 hack 你用的 Library，就能從中擷取你 Application 的資產。**現在 Agent 就像 Application，你呼叫的 API、你用的 MCP、甚至你 Skill 裡的 Context 都可能被 Poison。**

Data Access Control

Memory / Context Poisoning——如何透過這種方式引導你的 Agent 或 LLM 洩漏不該揭露的資料。

OWASP 已推出 Agentic Application 的 Top 10（過去是 Application Layer 與 Data 的 Top 10 攻擊），這是金融業合規可直接對照的國際標準。

/ 五、Enterprise Agent Platform 的四個治理角度

階段	要處理的事
Build	不同 Model、Agent Framework、Agent Development Kit（如 ADK 與各種 Open Source）
Scale	成千上萬個 Agent 的 Runtime； Long-term Context 與 Short-term Session 的管理 ——讓 Agent 記得你幾個月幾年來的習性，同時區分這個 session 在談 Travel、那個在談 Development
Governance	Agent Registry （每個 Agent 有 ID，ID associate 到被賦予的 authority 與可存取資料）、Identity、Policy、Agent Gateway 的 Input/Output 控管
Optimize	持續監控 Agent 的使用與 Response Quality，據以分析流程該拆成哪些 phase、每個 phase 該呼叫哪個模型

Context Engineering 的必要性

Agent 互動累積的 Context 會越來越長，導致執行效率問題，且幾年前的 Context 可能被擠掉。因此需要在 Session/Memory 中 Summarize——「有點像是精華記憶萃取，你不會保留一些無關緊要的東西。」

Optimize 與 Tokenomics 的連結

最簡單的方式當然是把所有 task 都交給最先進的 Frontier Model——「這一定是可行的方式，**但從 Cost 的角度這是你願意做的方式嗎？**」唯有監控 Agent 的產出品質與 Log，才有辦法判斷哪些 phase 可以用 Flash 這類

CP 值高的模型，哪些真的需要高階 Reasoning。

/ 可行動要點

- **OWASP Agentic Application Top 10** 可直接作為金融業 Agent 平台的資安檢核基準
- AI Ready Data 的三層 Context 模型（Technical / Business / Personalization）可用來盤點現有資料缺口
- Agent Registry + ID + Authority 的設計，與場次 03、05 提到的「數位同事獨立身份」是同一件事的不同說法
- Security Agent 的 98% alarm reduction 是可對標的量化預期

2026 國泰金控技術年會·會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。

專題演講 #IT現代化 #集團布局

AI in IT：驅動國泰集團 IT 全面升級的策略與布局

國泰金控數發中心雲端策略發展部協理 | 顏勝豪 Otto Yen

13:50-14:10 有效內容 24.0 分鐘 逐字稿 6,707 字

/ 開場：一支「失控的 Agent」悔過書影片

Otto 以同仁 Terry 製作的影片開場——Terry 在使用 Agent 時創造出一個失控的 Agent，主管要他寫悔過書，他很有創意地做成影片。事件發生在雲端 LAB 環境，雲端本來就適合建立隔離環境，所以雖然失控但未造成重大危害。

「Terry 這個影片做得很好，可是下次不要再這樣做了。」

影片中的關鍵論述（也是全場的治理基調）：

- AI knows common answers. **It does not know your company.**
- It learned recurring patterns, the average cases it had seen. **Your private context is not part of that average.**
- **So the control point must come before the action.**
- Give it only the permission this task needs. Test somewhere that cannot hurt the real project. Review exactly what it plans to change. For an irreversible action, a human presses the button.
- **Never let a reasonable guess become an irreversible action.**

/ 一、技術路線的三個取捨

1. 算力用雲端——不在第一天就蓋 GPU 機房，因為當時對自己的需求還不確定
2. 模型以三大開源模型為主——底層算力層與模型不是 focus 重點
3. 專注應用層與交互層——Agent 的使用與互動介面

交互層的觀察：IT 人員習慣對話框、CLI、IDE；但一般使用者不太可能透過 CLI 或 IDE 與 AI 互動——這正是強調安全與安全應用重要性的原因。

/ 二、Agent 的定義：Model + Harness

引用軟工大師 Martin Fowler（提出重構、Code Smell 的那位）網站上的定義：

AI Agent = Model + Harness

- **Model 是 stateless**——本身不記錄任何狀態
- **所有狀態操作都在 Harness**——harness 負責 handle state
- **所有控制手段、讓它更聰明的機制、護欄，講的其實都是 harness**

Otto 以今年初爆紅的 Agent 工具為例：**大家覺得它好用，其實是它的 Harness 做得很好**——像真人、能記錄東西、能使用工具、甚至能操控電腦。

個人級 Harness（Codex、Claude Code）vs **企業級 Harness**（Google／AWS／Azure 平台）：架構同樣是 Model + Harness，**差別在控制機制、治理能力與處理規模，完全是不同量級。**

企業級 Agent 依賴的既有 IT 核心能力

驗證授權、知識庫、API Gateway、工作流、CI/CD、觀測性、Security、Audit、SDLC 設計。

「這些東西其實你本來就應該做好。**如果沒有做好，即便有這樣的平台還是沒有用。**」

/ 三、上雲的意外紅利

- **2021 年啟動集團上雲計畫**
- **今年 4 月成果展達成「5 年 100 套系統上雲」，現已超過 150 套**
- 最終階段是 **Cloud First**：未來所有新系統開發建置以上雲為優先

關鍵觀察：

「發展上雲的時候並沒有想到今天 AI 發展的狀況。可是走到今年我們覺得，**我們本來以為整個上雲是為了系統現代化做準備，實際上它同時也是在為 AI 的發展做準備。**」

因為 AI 需要大量數據作為燃料，而雲端是很好的承載環境。

/ 四、AI & IT 藍圖

兩大核心

- **開發**：軟體工程、IT 知識管理
- **運維**：IT 的 AI 應用、治理維運（今年看到很多雲端資安事件，AI 在這塊可做不少貢獻）

下含 17 個子領域。

三階段，且總期間控制在兩年以內

「因為 AI 的發展速度太快，**你的計畫如果拉太長期它沒有意義。**」

階段	內容
一	100 天 pilot——模型都在雲端上，啟動實驗專案很快
二	找到好案例做 scale；同時設計 AI Budget 概念
三	AI Scale，把好案例擴散到全集團

AI Budget 的設計動機：AI 工具太多，很難約束同仁「只能用 A 不能用 B」。因此改為**給每位 IT 人員一個可使用的 AI 額度，在符合預算控制的前提下自己組合工具。**

/ 五、AI SDLC：用工程的確定性消弭 AI 的不確定性

這是全場最核心的一句話。Otto 對「幻覺」的定義極為犀利：

「AI 給我們的答案我們覺得很酷，我們會說它是**湧現**；如果它回的答案我們覺得怪怪的，我們會覺得它是**幻覺**。所以湧現跟幻覺其實是在做一樣的事情，只是我們最後得到的那個答案是不是符合我們的需求。可是 IT 在用 AI 的時候不應該出現這麼多幻覺，因為我們還是以工程的手段在做整個流程。」

三個發展重點：測試流程並形成工具與方法論 → 培養懂這些工程手段的人才與團隊 → 最終建一個 IDP 平台，讓開發與工具使用統一在單一平台操作。

/ 六、AI Squad Team：6 + 1

項目	設計
團隊規模	原本 12 人 → 壓縮到 6 人
配備	足夠的 AI 工具、一台獨立電腦、獨立帳號、個人化 agent
「+1」	就是 AI Agent
組成彈性	PM/UI/UX/RD/QA 各要幾人由團隊自己決定
佈署	銀行 4 個團隊（數銀 2、資訊板塊 2）

Otto 的一段自嘲：

「我一直提到我要設計一個 **6+1** 的團隊。可是我在跟 AI 的對話過程中，他**一直問我為什麼加 1 不是 1+6**——他覺得應該是由 AI 去帶領 6 個人去開發。然後我就覺得還蠻不錯的思考，我以後可以想一下。」

四個驗證目標（前兩項已達成不錯效果）

1. 交付量放大——「都已經給 AI 工具了，你不可能說開發速度跟以前一樣」 ✓
2. 協作路徑縮短 ✓
3. 每個角色做的事情可 Agent 化

4. 測試出的流程能變成企業可複製的能力

AI member 實際承擔的工作

會議記錄、程式碼監控、產生日報週報、需求整理、ticket 阻塞分析。

/ 七、SDLC 流程本身的重構

傳統 SDLC 的問題：一關一關走（BU 提需求 → UI/UX → SA/DE → Coding → QA → 上線），只要有一關卡住，下一關就進入 Waiting 狀態，也沒辦法提前做。

新的分類方式：把團隊角色重新分成兩種人——

- **Design Owner**：決定要做什麼、做功能設計
- **Deliver Owner**：負責交付與最終品質

最關鍵的變化：BU 團隊寫出 PRD/BRD 之後，就能直接產出會動的 HTML Prototype。有了會動的網頁，後續需求確認與開發的需求確定性大幅提高。

人機投入的微笑曲線：整個 SDLC 中，前段與後段人的投入較高，中段（開發、測試）AI 可承擔較多——這與過去整條線都要人力投入差異極大。

/ 八、明年的規劃

- **集團 SDD Hackathon**：因為集團內用 SDD 開發方法的團隊太多（有用 BMAD、有用 SpecKit、也有不走框架的），希望透過活動交流。三種場景：既有系統重構、開發新系統、既有系統新需求。會找三位外部評審
- **AI Apps（運維）是明年重點**：先建立 **AI Ready Data**（呼應 Harry 的論述），再讓運維達到更智能的境界。基礎是 INFRA 事實、可觀測性、Log，以及運維同仁累積的 SOP、Runbook、故障文件

/ 九、結語：AI 是放大器

引自 AI Con 的一句話，Otto 認為說得極好：

「AI 是一個放大器，它放大的是已經存在的東西。如果你的團隊本來就很混亂很散漫，加 AI 只是增加了這些混亂跟焦慮。你本來的開發工程體系、流程就沒做好的話，加入 AI 只會讓 AI 產生更多的技術債。所以最終還是要把底層的工具、方法、工程事件的方法做好，在這樣的情況下導入 AI 才能發揮更大的效果。」

/ 可行動要點

- **Model + Harness** 是理解 Agent 產品差異的最佳框架——評估工具時該問的是 harness 的治理能力，而非模型
- **AI 計畫期間控制在兩年以內**，是應對技術變化速度的具體管理決策
- **AI Budget**（給額度而非指定工具）解決了「工具太多無法約束」的實務問題

- **Design Owner / Deliver Owner** 的角色重分類，是把 AI 導入 SDLC 的關鍵前置動作，比導入工具本身更重要
- 「AI 是放大器」可作為評估任何團隊是否該導入 AI 的第一道檢查

2026 國泰金控技術年會，會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。

專題演講 #軟體開發週期 #開發生產力

AI Agent 赋能 SDLC：以 BMad Framework 打造 Requirement Management Agent

國泰世華銀行業務中台部協理 | 鄭正略 Louis Cheng

14:10-14:30 有效內容 23.0 分鐘 逐字稿 8,891 字

/ 開場：一個下午把 15 年前的專案轉成微服務

Louis 把自己 15 年前寫的 Struts2 (Java 1.1) 專案放上 GitHub，用 SDD 方法一個下午就全部轉成微服務，而且 follow 團隊的 standard。

「我整個有點傻眼，我說怎麼那麼快就把它做完了。當然我 Token 燒很多。」

他的個人立場：

「新的東西其實帶來的不是改變，所以不用擔心 AI 會取代人。但是永遠都有一個議題，就是假設你不能跟上這個腳步的時候，你就会被淘汰。這跟 AI 沒有關，這是跟你自己個人、或者是你對工作的態度有關。」

/ 一、為什麼選 BMAD：框架比較

層級	框架	問題
工程師導向	LangGraph、AutoGen	特定工程師才能操作，來回一陣子，時間花比較長
No-code / Low-code	Flowise、n8n	方便，但仍需了解那個工具；工具演進快，也有資安議題
對話式引導	BMAD	用對話引導你建立 Agent、內建知識、全員可使用

BMAD 的差異化特點：

- 建立一個 Agent 在 30 分鐘內完成——「當時我一看到我蠻 Shock 的」
- 用腦力激盪的方式引導，而且有組織性、有架構性 → 在企業內部建的 10 個 Agent 都會是同樣的脈絡
- 去年 10 月就在討論 Markdown 而不是 RAG——在本機建立的東西可以累積在自己身上
- 一般員工或非技術主管都可操作（前提是你要有想法，完全沒 idea 是建不起來的）
- 最難上手的反而是安裝（要裝 Python、NPX 之類）

最核心的設計哲學

「最重要就是在**降低使用門檻**。大家都知道下 Prompt 是一件很難的事情，因為每個人 Prompt 都下不一樣。**我不希望我的部門、我的組織裡面的人下的 Prompt 不同，然後出現不同的結果**。它把**申論題變成選擇題**——你在寫考題的時候哪個比較好寫？選擇題當然比較好寫，因為可以猜嘛。而且它的選擇題還會給你一些指引。」

實際給 BU 端使用的回饋很好，因為「你教他 SOP，還不如跟他講 1、2、3、4、5，他比較好選擇，選擇錯了他也會跟你講」。

/ 二、BMAD 的兩種模式與版本建議

模式	說明
BMM (Agent AI Team)	丟一個 idea (例如「我要開發一個信用卡權益平台」)，會自動叫出 BA、SA、PM、開發、QA、Architect 等角色問你問題，整理出 BRD/PRD。另有「 大亂鬥 」功能——丟一個問題，每個 Agent 都發表意見
BMB (企業主)	Louis 去年就判斷企業會走 BMB，今年果然成為主軸

「BMM 我必須要講他 **Token 燒死我了**，我一開始用這個被他燒光光。後來我發現這樣不行啊，我又不是每次都要一個團隊做一件不是那麼難的事情。」

版本建議：用 V6 Alpha 就很夠力。**今年 7 月推出 Autonomous (自主 Agent)** ——建立 Agent 時可設定是對話式還是自動式，自動式就能整進 CI/CD 流程。

「它本身具備這兩個功能以後，我覺得它就已經蠻**殺手級**的了。大家可以從 V6.10 開始去走。」

/ 三、五個元件

元件	說明
Persona	先設定這個角色
Task	定義 AI 的邊界跟移交準則
Flow	引導式／對話式／自主式／混合
Output	固定的 Markdown 產出
Human in the Loop	每次問完一定會問你要不要繼續，所有 Agent 執行動作時都會詢問一遍

知識沉澱 (Sidecar 記憶設計)

「就像我們在帶新人，你要叫他記起來，不然他記不起來你會很麻煩。我們做了一個 ETL 的工具，第一次跟他講叫他修改，他修改錯掉。可是修改完有更正他說，請你修改完這個以後，下次同樣類似的 case 給他，他不會再有問題。這就叫做知識沉澱。」

Write Once, Run Anywhere

一次建立的 Agent 可跨工具運作：**Claude Code**、**Codex**、**GitHub Copilot**、**IBM Bob**——不用再做任何事情就能直接執行。

Louis 團隊實際使用約 40–50% 的工具：Kiro、Windsurf、Gemini、OpenCode、IBM BOB、GPT、Codex、Claude Code。

版本控管建議：BMAD 雖有版本控制，但**建議走自己內部的 Git**——「畢竟在企業內使用，不能一直仰賴在個人的 PC 上。」

架構順序提醒：以前會把企業層擺最上面，**不對，AI 要從企業層開始**，因為這是資安議題。企業層與資安議題先在最底層做好，未來只要改變企業層，各部門、各專案的 Agent 都可以跟著動，而不是一直 bottom-up。

/ 四、核心案例：Requirement Management Agent

問題定義

「其實在進行專案之前有提案的程序，**提案的程序都不納入成本，這是不合理的**。因為蠻多 BU 單位會找 IT 談，有可能花三個月去想一個 idea，一直要找 IT 確認等等。通常 IT 都會說，等到看到需求書，**你這個東西提得完全天馬行空，退掉**——它三個月時間就不見了。**我覺得這就是無效的溝通跟無效的會議**。」

做法

把權益平台系統的 know-how 放進 RM Agent，提供給 BU 單位使用，加速產出 BRD 與 PRD；後續陸續推廣給企金與中台人員。

「就節省掉他要找 IT——因為找 IT 都用開會的方式，每次訂好會議開得很長，花了好多時間，真的很浪費。那我們用這種方式，**你的 BU 就一直問他，你也不用擔心，因為有時候 IT 比較兇嘛，會罵你**。」

成效

1. 降低對資訊人員訪談的高度依賴
2. Time to Market 縮短
3. 與 BU 的衝突降低——「因為你去想嘛，它有它的 KPI，我有我的 KPI，我又不是只有做你的開發，我還有維運的議題。**所以溝通時間變短了，溝通頻次變少了，其實衝突就變少了**。」

推動方式（很誠實的一段）

「這是我們部門上半年建的 Agent（Security Agent、DevBridge、Code Review、SDD）。我是要求他們，其實不是他們很愛用，而是因為我剛剛講這是你們今年的 KPI，所以不好意思，所以他們就拼命用。但其實用下來他們就有感覺——你一定要先強迫人家用 AI，不然我覺得有些人會自己覺得技術很厲害，就一直用下去。」

/ 五、流程要先破壞，再加 AI

「我們在做 AI 的時候不是把原本的流程擺入 AI 的功能增加生產力，而是要把流程做調整。以前要做頁面，是 Figma 產生 Prototype 給 User 看，然後 HTML 再轉到 Angular。現在 Prototype 跟 HTML 不用產生了，我就不用前端程式，因為 Figma 可以直接透過 AI 轉成 Angular，甚至更狂一點，照片直接轉 Angular，做得到的。所以理論上來講，要想的是先把流程破壞掉，之後再加入 AI 的工具，其實會速度快很多。」

/ 六、SDD 實作與品質自動優化

三層目標：技術目標、業務目標、組織目標。

三種債的自動化處理：

債	做法
技術債	用 SonarQube 的 Metrics，「技術債假設這個專案裡面有 10 個小時，我就跟 AI 講請你依據 SonarQube 的技術債去修正——時數往下降表示技術債在解決」
資安債	原碼掃描接 NCP，做中低風險、中高風險的修復
升級債	比較麻煩，是相對複雜的議題

Code Review 的兩難（Louis 當場問全場）

「AI 寫的程式你要所有都看嗎？要不要所有都看？不看怪怪的，看了就覺得沒有用。所以有些人提到一件事就是——定出標準，只要超出例外的你再去看。不然你就要放手相信 AI，不然就不要用 AI，不然這樣就很怪。所以基本上前面的 standard 把它定出來（中高低風險、難易中等等），其實你走 AI 這件事情可能會比較 easy 一點。」

/ 七、兩個彩蛋工具

- Hedron——降低 Token 使用，跨多個 AI 工具平台，只要跑在本機、以 Gateway 方式運作，有動態 Dashboard。「因為我們一直在用 Codex、用 GitHub Copilot，Token 用得超兇的。實際上把上下文再做一些調整，其實可以降蠻多。」
- Harris——跨 Session 記憶，Claude Code、Codex 跑的 Session 會被記起來，可以切換使用。與 Hedron 搭配

/ 可行動要點

- **「把申論題變成選擇題」**——這是降低組織 AI 使用門檻最具體的設計原則，直接解決「每個人 Prompt 不同導致結果不同」的一致性問題
- **RM Agent 的真正價值不是產文件，而是降低 IT 與 BU 的組織衝突**——這是少見且可量化的軟性效益
- **流程先破壞再加 AI**，與 Otto 的「AI 是放大器」互為表裡
- Code Review 的「定出標準、只看例外」是可立即採用的實務判準
- 用 SonarQube 技術債時數作為 AI 修復成效的客觀指標，可直接複製

2026 國泰金控技術年會·會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。

專題演講 + 高峰對談 #虛擬資產 #穩定幣 #虛擬資產專法 #VASP

金融級虛擬資產與穩定幣技術布局／數位資產如何邁向主流？金融機構與 VASP 的合作路徑

林政憲 Eric Lin／主持人 施君蘭 Lana Shih／吳建興 James Wu・鄭光泰 Titan Cheng・楊岳平 Alex Yang・賴偉晏 Wayne Lai

14:50-15:50 有效內容 70.9 分鐘 逐字稿 19,982 字

本檔為連續錄影，涵蓋官方議程的兩場：14:50 林政憲的專題演講，與 15:10 起的高峰對談。

第一段：Eric — 數位資產技術佈局

／ 一、市場規模（換個角度看區塊鏈）

Eric 刻意不從「比特幣現在多少錢」切入，而是問**金融服務在鏈上的發展程度**：

指標	數字
穩定幣今年月均交易量	約 8.45 兆美元（較去年月均成長約 7 成）
加密貨幣持有人數（2025）	約 7 億人，約全球人口的 1/10
RWA	資產規模成長且多元化——大宗商品、黃金、公開市場證券陸續上鏈

大型機構的參與軌跡

貝萊德／富達的比特幣與以太幣現貨 ETF → 星展、匯豐、JPMorgan 的存款代幣 → BlackRock／Franklin 基金上鏈、星展數位債券 STO → 國泰證券發行台灣第一檔債務型 STO → DTCC、Clearstream 等保管結算機構納入區塊鏈 → 今年 7 月 JPMorgan 把部分 ETF 透過 DTCC 上鏈，再把代幣抵押到交易所做保證金使用

／ 二、保管：為什麼機構級保管是必要的

兩個安全神話的破除

交易所不安全：2024-2025 年中心化交易所發生 20 起攻擊事件，總損失約 25.5 億美元，其中 Bybit 一家就約 15 億美元。

冷錢包也不一定安全——今年 7 月的 Coldcard 事件：

改版時把原本**硬體的隨機性**不小心改成**軟體的隨機性**。軟體偽隨機產生的私鑰組合非常少，駭客根本不需要碰到你的冷錢包，只要用電腦花幾天算出私鑰，就能盜取你鏈上的資產。

國泰的機構級保管（今年 5 月取得主管機關許可，服務 VIP 客戶的比特幣與以太幣）

四大技術支柱：

1. **HSM 硬體安全模組**——私鑰的產生、保存、簽章交易全在硬體環境執行，私鑰永不脫離硬體；硬體遭人為破壞會自動清除內部資料。**關鍵在硬體隨機性**，不會有 Coldcard 那種軟體偽隨機的破綻
2. **Air Gap 離線隔離**——私鑰保管系統完全斷網，駭客沒有從外部攻擊竊取的機會
3. **幣流追蹤**——引入外部系統辨識可疑交易與風險帳號
4. **多層多簽**——出入金需多角色多人員審核達門檻才放行，**沒有任何一個人可以做完所有事情**，且每一步都留下紀錄

「機構級的保管，它不再只是我們把私鑰藏好這麼簡單，我們還要把整個交易流程都保護好。」

/ 三、穩定幣的四大場景

1. **數位資產交易市場**——未來 RWA 也可用穩定幣交易，做到**原子交割（DvP）**：「一手拿證據、一手交付款項」，提高資金運用效率、降低信用風險
2. **高通膨國家的日常支付**——存款越放越薄、習慣使用美元，但換匯有管制額度；穩定幣是比較好取得的「數位美元」
3. **跨境支付**——傳統支付的**金流與資訊流是分開的**（Visa/Mastercard/SWIFT 制定資訊流標準，金流仍需經銀行體系層層結算，每多一間銀行就多一些成本與時間）。**穩定幣天生結合資訊流與金流——資訊收到的同時價值已經移轉**，可實現點對點移轉
4. **Agentic Commerce**

/ 四、Agentic Payment：支付主體的根本改變

台灣民眾使用 AI 的調查（國際卡組織）

- 近 **7 成**每週至少使用 AI 一次
- 近 **4 成**購物時參考 AI 建議
- **6 成以上**願意讓 AI 規劃旅遊行程**並完成相關支付**

「我們對 AI 的期待，正從『AI 可以提出建議』變成『**AI 可以幫我完成**』。而 AI 要能幫你完成，**支付就是非常關鍵的能力**。」

最根本的變化：交易主體

過去不管哪種支付方式都以人為主體——人決定買什麼，再付款。未來「AI 買什麼、跟誰買、買多少錢，**這些都是 AI 自主決定的**」；人只專注在目標與預算。

Agentic Commerce 五個價值層



Eric 的主張：銀行結合自己擅長的身份驗證、授權與資金移轉能力，再結合 VASP 的鏈上服務能力，共同發展 Agentic Payment。

兩大協定的關係

	x402	MPP
主導機構	x402 Foundation（Google、AWS、Visa、Mastercard、Coinbase、Circle 等加入）	Stripe
支付軌道	聚焦加密貨幣／穩定幣	加密貨幣 + 法幣、信用卡
關係	底層協議	向下相容 x402，堆疊其上，額外擴出其他支付軌道

另有 Amazon + Ripple + Coinbase 的 Agent Core Payments。

兩大核心挑戰

- 1. 使用者安全性——要不要把信用卡、虛擬資產錢包私鑰交給 Agent？怎麼知道 AI 不會亂付款、不會把私鑰交給其他人？
- 2. 商家整合——AI 想付錢，商家也要能支援 Agentic Payment 收款

最值得記下的開放問題：KYA（Know Your Agent）

「過去人去買、人去決策，所以人來負責，沒有什麼問題。但未來如果交給 AI 來做，會是 Agent 負責嗎？不知道。還是 Agent 背後的那個人來負責？這個也不知道。所以我覺得未來 KYA 這樣的議題，是需要被拿出來探討的。」

/ 一、James（國泰資訊長）：從客戶需求看合作

三類客戶需求：

客戶類型	需求
高資產客戶	數位資產只是資產配置多一個項目； 要的是安心 ，不求高報酬，希望有值得信賴的人幫他保管
企業客戶	買方想用穩定幣付貨款（尤其跨境）；要交易成本低、速度快，甚至能做穩定幣與法幣整合的資金調度
一般客戶	一站式服務—— 能不能在同一個平台做兩種資產的配置與管理

具體合作模式構想（複委託概念）：銀行 App 提供入口 → 對接 VASP 尋價 → 客戶決定是否買單 → 下 order → VASP 撮合、清算、交割 → **產品回到銀行做保管** → 客戶看到的是**整合性財管報表**（傳統法幣＋數位資產）

「各取各的專長，在法規上或實際上也沒有什麼衝突。這樣的合作可以當作**起手式**。」

/ 二、楊岳平教授：虛擬資產監理的三階段邏輯

這段是全場最有解釋力的分析——為什麼現階段大家都覺得痛苦。

第一階段：出發點是犯罪防治

「七八年前大家就意識到虛擬資產跟洗錢犯罪之間的關係。所以非常一大部分監理的出發點其實來自**犯罪防治的需求**。我每次在公開場合也會講，除了金管會以外，另一個虛擬資產法制的推手是**法務部**——因為他們真的快要受不了了。在第一線被虛擬資產相關犯罪折騰的，真的快受不了了。**我們永遠不要忘記這件事情。**」

第二階段：管理者心態的轉變

「一開始大家沒有動力去管的時候，各部會是互相推脫的。一旦有個人進來要管——比如金管會要負責管這件事的時候，**人的思維就會改變，從『不做不錯』變成『既然我要負責了，我就什麼都要確保不要出事，因為只要一出事都是算我的』。**」

於是金融監理、消費者保護、客戶資產安全等議題開始浮上檯面。

第三階段：必須伴隨業務開放

「主管機關想的事情不能都只是管理。如果光是管理，**政治上頭是得不到支持的**——你一直在管，大家一定會說你在扼殺產業。所以開始要有產業扶植的想法，也必須要有一定程度的業務開放。」

為什麼現階段特別痛苦

1. 還沒走到大方向的業務拓展，所以**感覺管理大過於發展、成本大過於效益**

2. **金融機構是 Latecomer**——從 2014 年金管會新聞稿禁止，到 2024 年登記制出來才鬆口，**整整十年的禁止**。而 VASP 業者在這部分累積了 **12-13 年的作戰經驗**

國際對照的反直覺觀察

「德國其實在 **2019 年** 法律就允許銀行做虛擬資產保管，但你也沒看到有什麼具體的德國銀行開始把市場拿走。事實上現在國際上主要在做虛擬資產保管服務的，還是那些會被歸類為金融科技業者的——只是這些業者越做越大，比如 Coinbase，你恐怕不能只說它是個金融科技業者，因為**該拿的牌好像也都拿得差不多了，信託業牌也拿了。**」

法律該做與不該做的兩件事

原則一：盡可能維持中立

「法律最好什麼都不要規定、什麼都不要管。立法者或監理者**理論上是趕不上市場上頭的變化，也不會了解市場上頭的 niche**，不應該去預設虛擬資產市場裡頭誰該做什麼角色。讓不同的 player 處在動態的市場競爭狀況，**生意人有他的敏銳度，會自己找到擅長的地方，不擅長的去找合作對象。**」

原則二：合作不能讓預期的監理強度被妥協

「合作的背後其實是一種**分工**，是一個工變成兩個人做。而一個工變成兩個人做的時候，**最忌諱的就是這兩個人各自都突然有一個地方不負責了**——導致本來一個人負責時你找得到負責的人，切成兩個的時候找不到。這種情況是法律必須要介入的。」

傳統金融界最有名的對應規定就是**作業委外**——你不能因為把作業委外了就裝作沒你的事。

保管業務委外是重大突破：

「在傳統金融監理當中，**核心業務是不能委外的**。但我們立法時理解到保管業務的特殊性，**雖然保管業務可以委外，但受委託對象必須是一個有牌照的保管商。**」

這個設計的目的不是促成特定合作，而是**確保監理品質的一致**——但它有可能促成合作：「如果我今天是一個有保管商牌照的人，對自己的保管沒有信心，我可以找一個對自己有信心、但不一定找得到客戶的人來幫我保管。**這種合作機會有時候第一個人是金融機構、第二個是 VASP 業者，但有時候也可以是反過來。**」

破除英美法系 vs 大陸法系的迷思

「雖然大家常講英美法系跟大陸法系有根本差異，但來到**金融法的世界，不存在**。你去看美國的金融法規，那規定的**絕對比台灣細**，成文化的程度之高、之嚴謹、之細膩。真正的差異反而來自**美國跟英國之間**——美國規定得非常細、兼容並蓄；英國都是原則導向，講一大堆大原則，**在大陸法系的角度會覺得這個寫得等於沒寫**。台灣的共識是希望寫清楚一點。但清楚的規定**不能放在法律裡頭，因為萬一要修的時候要去立法院**，那會是一個很大的問題。**這就是虛擬資產服務法後來折衷的結果——你會感覺到大量的授權規定。**」

/ 三、Wayne (KPMG)：國際趨勢與三種可買的能力

轉折點

「真正讓我們這邊動得比較快，應該是去年美國天才法案通過之後，我認為它已經升高到所謂國安的等級。早期國內專家的文章真的比較偏 fraud、詐騙味比較多，但曾幾何時，目前所有的文章都已經開始正式認為這是一個蠻不錯的商模。簡單的說，如果台灣不做這一題就來不及了。」

自建 vs 合作的關鍵提問

「DBS、HSBC、JPMorgan——各位知道他們跟 VASP 相關的系統是自建還是委外嗎？我跟各位報告，大部分都是自建。但這是很久以前的事，也許在五年前、十年前就已經在做。HSBC 的平台叫 Orion，JPMorgan 甚至發行自己的存款代幣。此時此刻如果台灣的金融機構要全心自建這個系統，我覺得會有點慢。而且在這個慢的背後，如果你又土砲全都自己建，我們會產生的是另外一個 Security Hole。」

最刺的一句話

「早上也提到金融機構最重要的關鍵是 Trust。我們最怕什麼不見？是信任不見嗎？不是，是錢不見。那錢怎麼會不見？在區塊鏈的世界裡面有太多太多新的東西，which 是金融機構所不熟悉的。我隨便問大家一個名詞——區塊鏈分岔。我剛剛做了一個調查，他說只有頭髮會分岔吧，區塊鏈為什麼會分岔？除了分岔還有混幣器等等。如果不靠一些技術廠商來做支持的話，我認為會慢非常多。」

跟 VASP 合作可以買的三種能力

能力 說明

買客 兩邊客戶重疊性可以盤點。有重疊表示「你們的客戶早就已經往 VASP 這條路上了」，他們需要的是更好的 One Stop Shopping 服務

買技術 「最困難的倒不是新技術怎麼弄進來，而是去接傳統銀行的 legacy 系統」——銀行要不要結帳、要不要維持原本的財富管理、利息、NII fee 等業務，介接非常有挑戰

買人才 兩邊團隊必須做比較好的結合。「2022 年我們還在談 ChatGPT、談生成式 AI，曾幾何時我們已經開始很深入地在談跟 VASP 的介接，人才怎麼快速 Tune 上來是未來的挑戰」

7×24 的配套提問

紐約證交所、美國結算中心都在推 7×24，實時交易未來就是會發生。

「請問我們現在有到 7×24 嗎？有啦，客服中心可能有。可是客服中心我如果打進去問他，我的加密貨幣出了問題的時候，誰能夠回答呢？那回答完之後如果系統需要做一些因應，請問我的 IT 是不是也需要做一個 7×24 比較新型態的服務？」

台幣穩定幣的想像場景

美國的 buyer 買台灣供應鏈的東西 → 錢打進來 → 他再用這個錢去付薪水 → 領了薪水之後再用它來做投資。「**直接是 B2B2C 的場景，我覺得整個是會串通的。**」

/ 四、James：穩定幣只是開端

「現在大部分人都把穩定幣當作**支付工具**，但我認為支付工具應該只是一個開端。假設我今天跨境支付，穩定幣交易速度很快，**可是我拿到穩定幣之後萬一還是換成法幣，那對我來講真的有成本降、速度快嗎？比較好的應該是讓穩定幣繼續持有，將來付給 Supplier、甚至付員工薪水都可以用穩定幣。而如果穩定幣留在手上不需要馬上支付，可不可以有一個地方可以 park？所以 money market 的東西就會代幣化，你可以暫時 park 在那邊生一些利息。那將來你的資產、貨幣、合約都在同一個世界裡，是不是就變成一個生態圈，又多了這些資產可能變成另一種新型態資產的底層。所以初期是支付工具，但最後它會衍生成一個生態圈。**」

國泰的 Readiness (James 的誠實回答)

- 2018 年成立 Web3 研究團隊
- 2019 年做貿易文件共享（幾家銀行與海運公司共享貿易文件資料以防弊）
- 定位：**國泰當一個 bridger（橋接者）**，把傳統金融知識（產品設計、AML、法遵）與 Web3 的效率（碎片化、一手交錢一手交貨、24×7）串起來
- 但坦承：「將來我們現在可能只有客服人員是 24×7……**我們的工作模式、服務模式可能也要變成 24×7，我認為我們還有待努力。**」

主持人接話：「我想這個應該也是我們早上講的，**AI Agent 應該要出動了**——今天整個議程從頭到尾都是連結在一起的。」

/ 五、三年展望

與談人 期待

Wayne	「如果地上有一千塊掉在地上你會怎麼做？」希望三年後這件事 像喝水一樣如數家珍 ，每個人清楚知道可為與不可為——也就是 financial literacy 的普及化 。科技絕不會是 VASP 單點，一定會與 AI 等技術結合出新應用場景
楊岳平教授	「三年可能有點短。 我期待的境界是三年以後我們不用討論這些議題 ，它已經變成我們的一部分，大家都蠻熟悉也沒有太多問題，所以不需要討論—— 就像現在我們不會去討論網際網路的樣子。 」
Titan	效率與品質是人類一直追求的目標，「 但我認為其實很少人在聊保護這件事情 」。從聯防到專法通過，與金融機構合作可以取得足夠 Qualified 的用戶品質資料，這是未來品質與效率最重要的基石
James	「金融業經營的是信任。 我希望三年後，現在看似兩個世界的傳統金融與數位資產市場，在中華（監理）、資安、交易、透明等面向都已經得到一個互信的標準 。未來從使用者角度，我希望不是兩個平行空間，而是在一個平台上 可以做兩塊資產的配置與管理 ，而且是一個信任安全的環境。」

/ 主持人結語

呼應早上蔡宗翰的談話——台灣這幾年享受非常好的經濟成長，有很多資本正在流動。

「今天談的這個合作，應該並不是你有我沒有，而是有很多機會大家可以共同去 create，有更大的餅值得我們合作把它發掘出來。」

/ 可行動要點

- **Coldcard 軟體偽隨機事件**是說明「為什麼需要 HSM 硬體隨機性」最有力的實例，可直接用於內部教育訓練
- **KYA (Know Your Agent)** 是尚無答案的監理缺口，值得列為長期追蹤議題
- 楊岳平教授的**兩原則（監理中立 + 分工不得妥協監理強度）**，可作為評估任何金融科技合作架構的檢查點
- Wayne 的**三種能力（客戶／技術／人才）**提供了「自建 vs 合作」決策的具體拆解方式，其中「介接 legacy 系統才是最難的」是關鍵提醒
- **7×24 的配套盤點**（客服能否回答加密貨幣問題、IT 是否也要 7×24）是進入數位資產業務前必須先回答的營運問題

2026 國泰金控技術年會·會後整理的閱讀筆記，非官方發布內容。錄影以 openai-whisper large-v3 轉寫後校閱，講者姓名與職稱已對照官方議程核正。人名、數字與專有名詞建議對照影片核實。