

生成式AI在金融領域的技術演進與挑戰

東吳大學智能商業研究中心主任 李宜熹、國立高雄科技大學金融系教授 王友珊

近年來，生成式人工智慧（Generative AI / GenAI）在百工百業引發革命性的影響，金融業也不例外。生成式 AI 是指能夠產生新內容（如文本、圖像、語音、程式碼等）的AI系統，與傳統只分析資料的AI相比，其最大特點在於內容創造能力。特別是在2022年底OpenAI推出ChatGPT以後，生成式AI的應用熱潮迅速席捲金融領域。本文從技術演進角度出發，探討生成式AI在金融領域的發展方向。

生成式AI在金融領域的技術演進

早期金融AI與生成式技術的崛起

金融業應用人工智慧其實由來已久，但早期多著重在分析與預測，而非內容生成。在2010年代，金融機構已廣泛使用傳統機器學習技術（如分類、群集分析、時間序列預測等）來進行風險評估、市場預測與詐欺偵測等任務。但這些方法雖能從歷史數據中找出模式，卻無法主動產生新的文字報告、圖像或決策建議。

直到2014年左右，生成式模型開始興起。Ian Goodfellow等人提出生成對抗網絡（Generative Adversarial Networks, GAN）¹，證明AI可以在圖像等領域產生以假亂真的新內容。隨後，變分自編碼器（Variational Autoencoder, VAE）、強化學習等技術也逐步應用於生成性任務。然而，這些早期生成模型主要在圖像、多媒體等領域展露頭角，對金融領域的直接影響有限。真正讓金融業產生變革的是自然語言處理（NLP）方面的突破：從序列模型（如RNN、LSTM）逐漸發展到革命性的Transformer架構（Vaswani等人在2017年提出）²，使電腦對語言的理解與生成能力大幅提升。Transformer架構透過「自注意力機制」有效訓練

¹ 參見：<https://arxiv.org/abs/1406.2661>

² 參見：<https://arxiv.org/abs/1706.03762>

超大語言模型，為日後的GPT系列模型奠定基礎。

大語言模型與基礎模型時代

以Transformer做基礎，研究人員開始訓練大語言模型（Large Language Model, LLM）。2018年以來，相繼出現如BERT、GPT-2等模型，其中GPT-3（2020年問世）擁有1,750億參數³，展現出驚人的文字生成能力，能撰寫文章、回答問題甚至生成程式碼。相比傳統金融AI僅能執行特定任務，大語言模型透過建置基礎模型（Foundation Model），在巨量通用語料上預訓練，然後可針對不同類型的應用任務進行微調，因而具有高度的通用性和可遷移性。大語言模型的出現，讓金融機構看到嶄新應用的可能：單一模型即可應對從客服對答、報表摘要到程式碼開發等多種業務需求。

大語言模型在金融領域的應用初期，多半是將開源模型或透過商用API直接套用於金融任務。例如，一些金融機構嘗試使用GPT-3來分析財報或回答投資問題。然而，由於金融語言有其專業術語與知識背景，通用模型的表現不甚理想。為了解決這個問題，業界開始研發金融專屬的大語言模型。一個代表性成果是BloombergGPT。2023年，Bloomberg公司訓練一個專為金融領域設計的500億參數語言模型，使用Bloomberg自身數十年累積的金融數據（約3,630億詞彙）以及額外的通用語料作為訓練資料。研究顯示，BloombergGPT在金融相關任務上的表現遠勝一般模型，同時在一般語言任務上也維持不錯的水準⁴。這證實領域適應（Domain Adaptation）的重要性：透過在金融資料上的預訓練或微調，生成式模型更能掌握財經語境中的細微差異，提供更精確有用的結果。

生成式AI技術的成熟與關鍵進展

除了模型規模與資料的提升，近年生成式AI的品質飛躍還歸功於數項關鍵技術進展：

- 人類反饋強化學習（Reinforcement Learning from Human Feedback, RLHF）⁵：OpenAI在ChatGPT中引入RLHF，透過人類給予模型回饋來優化回答，使模型能產生更符合使用者期望的內容。這大幅提升生成式AI回應的可用性與安全性，降低出現無關或冒犯內容的機率。
- 提示工程與工具使用：使用者現在可以透過設計提示（Prompt）引導模型產生所需輸出；模型也能結合外部工具（如資料庫查詢、檢索引擎等）來輔助完成複雜任務，增強實用性。
- 多模態（Multimodal）生成：最新的生成式模型不再侷限於單一形態的資料。透過結

³ 參見：<https://zh.wikipedia.org/zh-tw/GPT-3>

⁴ 參見：<https://arxiv.org/abs/2303.17564>

⁵ <https://huggingface.co/blog/rlhf>

合圖像、文字、語音等模態，AI可以從多源資料中學習。例如，有研究發現將金融文本與相關圖表、影像結合，讓模型同時理解公司財報中的文字說明和財務圖表。這種多模態能力未來可望應用於投資研究（如分析企業年報的文字與圖像）或保險理賠（如分析照片與說明文字）等場景，讓模型理解力更接近人類的綜合推理。

- **輕量化與隱私保護**：由於大型模型參數動輒數百億，推動模型壓縮和高效微調技術（如參數高效微調、知識蒸餾、量化等）發展。這讓金融機構可以在本地部署稍小的模型，保護敏感數據不離開內網的同時，享受生成式AI帶來的功能⁶。事實上，不少銀行因資料安全考量，限制員工直接使用外部的ChatGPT，而選擇自行訓練或採購內部版的模型⁷。

ChatGPT引爆後的產業變革

ChatGPT 3.5在2022年底驚艷出世，使生成式AI的應用場景之想像空間大增，因此，2023年也被譽為生成式AI元年。ChatGPT僅用兩個月就累積一億用戶⁸，成為當時用戶增長最快的應用⁹。這一現象也激發金融業對生成式AI的重視。2023年可以說是金融業生成式AI「試驗→採用→擴散」的關鍵轉折點（Singularity）。年初時，許多機構還在觀望、僅進行小型概念性驗證（Proof-of-Concept, PoC）；但隨著技術成熟和初步效果顯現，許多領先金融機構迅速轉向規模化部署。同年5月的一項銀行產業高管圓桌調查中，有高達60%的受訪者表示生成式AI已成為「董事會層級」的策略重點，並推動全行更廣泛的採用¹⁰。

在技術面，OpenAI又在2023年與2024年陸續推出更大參數的模型GPT-4、GPT-4o¹¹，以及具推理模式（Reasoning）的o1與o3模型，使LLM在推理、編碼、專業問答等方面的能力全面提升¹²。同時，各科技大廠也同步推出各種開源大語言模型（如Meta的Llama系列）

⁶ 參見：<https://arxiv.org/abs/2410.15653v4>

⁷ 參見：<https://www.imf.org/en/Publications/fintech-notes/Issues/2023/08/18/Generative-Artificial-Intelligence-in-Finance-Risk-Considerations-537570>

⁸ 此紀錄在2025年1月被深度求索（DeepSeek）刷新。

⁹ 參見：<https://www.imf.org/en/Publications/fandd/issues/2023/12/AI-reverberations-across-finance-Kearns>

¹⁰ 參見：<https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/one-year-in-lessons-learned-in-scaling-up-generative-ai-for-financial-services>

¹¹ Open AI執行長Sam Altman於2025/02/13更在其X平台帳號上宣布，該公司即將釋出GPT-5模型。參見：<https://x.com/sama/status/1889755723078443244>

¹² 參考Open AI對於AGI（Artificial General Intelligence）的五階段發展里程碑。Level 1：對話型AI（Conversational AI）：專注於模擬人類對話；Level 2：理性思考者（Reasoners）：不僅能對話，還具備解決複雜問題的能力；Level 3：自主代理人（Agents）：不僅理解與推理，還可以自主執行任務。這意味著AI能夠長期管理並完成一系列的工作；Level 4：創新者（Innovators）：打破單純的問題解決，能夠獨立提出新點子、設計全新方案，甚至發明新的產品或流程；Level 5：組織型AI

與特定領域模型，給金融機構更多元的選擇。2025年初DeepSeek R1¹³ 創新技術的開源引發各界廣泛的關注，讓受制法規拘束與缺乏運算資源的金融業，看到生成式AI加速落地與進階開展的想像空間。許多機構選擇與大型科技公司合作，使用雲端上的專屬大模型服務；也有機構組建內部團隊，自行研發調校模型，以便對模型風險有更高的掌控度。例如，摩根大通（JPMorgan Chase）在禁止員工使用公共版ChatGPT的同時，積極開發自有的大模型應用，並於2024年中推出內部版的ChatGPT風格聊天機器人「LLM Suite」，定位為AI助手，支援員工進行研究分析等工作。這種「自主可控」的趨勢，反映出大型金融機構在擁抱創新與管控風險之間取得平衡的策略考量。

綜言之，生成式AI技術演進的軌跡是：模型更強大→更貼合金融場景→更易用可靠。伴隨技術成熟，金融業的應用從零星試點走向廣泛開展。下一步，隨著模型能力持續提升及產業實踐累積，生成式AI在金融業的影響勢必更為深遠。

展望未來

展望未來，生成式AI在金融領域的應用有幾個重大的發展方向：

首先是更無縫的人機協作。未來的AI將更深入地嵌入金融專業人員日常工作流，扮演貼身助理角色。銀行分行經理可能透過耳麥即時詢問AI以回答客戶疑問；在投資決策會議上，AI可以即席提供所需的數據和分析佐證。AI Copilot的概念將真正落地，每位理財專員、風控人員甚至程式開發人員旁都配有AI助手。而隨著使用的常態化，人們對AI的信任和駕馭能力也會提升，形成正向循環。

其次，多模態與主動性將是下一波重點。未來的生成式AI不僅能回應文字輸入，還能理解圖表、聲音，甚至主動發起動作（Agentic AI）。例如，在交易領域，AI代理可以監控市場即時數據與新聞，一旦觸發特定條件自動發出預警或建議操作（當然執行仍須人核准）。在客戶服務方面，AI能分析客戶表情聲調（若取得允許），主動調整溝通策略。自主智能體（Autonomous Agents）的興起，可能使AI從工具變成相對自主的「同事」。

再次，產業生態將隨AI發展而變化。預計大型科技公司、金融機構與新創將在金融AI領域展開更多合作與博弈。一方面，傳統金融機構可能組建聯盟，共享產業數據來訓練屬於金融業的產業大模型，降低對科技巨頭的依賴。另一方面，科技公司也會釋出更多符合金融合規要求的AI解決方案，例如，具備數據隔離、結果可解釋性的「客製化版本」模型服務。監管部門則可能推出產業指引或沙盒，鼓勵在可控環境下測試創新。

（Organizations）：最終目標，AI將能夠掌控整個組織的運作，從策略規劃到日常營運管理都能應對自如。目前各家AGI的發展大致上已經到了Level 2的中後階段，正在朝Level 3的前期階段積極邁進。

¹³ 參見：<https://arxiv.org/abs/2501.12948>

最後，從更宏觀角度看，生成式AI將推動金融服務的普惠化與個性化。AI助手降低專業理財知識的門檻，讓一般投資人也能獲得量身訂做的建議與資訊，大幅改善客戶體驗¹⁴。同時，銀行可透過AI更深入了解每位客戶的需求和行為模式，從而提供大規模客製化（Mass Customization）的產品組合。這是以往難以實現的。當然，前提是客戶對AI的產出保持適當懷疑，培養基本的媒體素養以辨別真偽。監管機構和媒體也需及時闢謠澄清，防止深度偽造資訊誤導投資公眾。

生成式AI在金融領域需正視之挑戰

儘管生成式AI在金融領域展現出誘人的前景，但仍有諸多挑戰需要正視：

- **可靠性與正確性**：金融業對精確度要求極高。AI「幻覺」（Hallucinations）出錯誤數據或不實資訊，在財務決策中可能釀成大錯。因此未來技術研發需著力於提升模型輸出的可信度，例如，引入事實校驗、強化模型對財經知識的掌握等。
- **倫理與合規**：AI可能隱含歧視性偏見，或產生誤導性的內容。金融機構必須確保AI決策符合公平對待客戶原則，並遵守監管對於自動化決策的要求（如不得在信貸審核中引入種族、性別偏見等）。各國國際金融監理機構所發布的文獻指出：「能辨別負責任和不負責任的創新」是監管新的AI技術時面臨的重大課題與挑戰。
- **資料隱私**：金融數據敏感且受監管保護。使用外部大模型服務可能有資料外洩風險，而內部訓練模型則面臨數據不足與成本問題。未來或許需要發展更完善的聯邦學習、隱私計算技術，讓AI在保護隱私前提下學習。
- **人才和文化**：將生成式AI真正落地，還需要金融從業人員信任並善用它。這涉及改變傳統的作業流程和思維模式。一些先行機構已開始為員工提供AI工具訓練，培養「AI素養」。組織層面也可能出現新職能，例如，專門負責AI模型管理與治理的團隊。企業文化是否能接納AI帶來的變革，將決定應用成效的上限。
- **系統性風險**：若整個金融系統都廣泛依賴類似的AI模型，當模型出現系統性錯誤時（例如，無法預測某黑天鵝事件，正如AI只學習歷史資料，對前所未見的事件可能無能為力），可能放大金融市場的波動。BIS年報警告，深度學習AI的廣泛採用「創造新的系統性風險」。這需要監管部門和業界共同研究應對之道，例如，加強壓力測試情境設計，納入AI集體失靈的假設等。



¹⁴ 參見：<https://micronotes.ai/ai-in-banking-balancing-innovation-and-regulation/>