HashKey肖風：須賦AI Agent數字身份 提升可信度

專訪

AI與區塊鏈之間有着「一體兩面」的關係，直至AI Agent（代理人工智能）OpenClaw的爆紅出圈，AI能自主為人類工作並取代部分工序，但同時凸顯AI Agent的安全問題，由區塊鏈賦予其數字身份是其中一種有效管理AI Agent的方法。HashKey董事長兼首席執行官肖風日前在接受《經「滬」論》專訪時表示，自己並非人工智能技術專家，但從區塊鏈與數字金融基礎設施的角度觀察，AI與加密技術正在逐步走向深度融合。隨着OpenClaw等前沿AI智能體的快速崛起，未來AI Agent很可能不再只是工具，而是需要具備獨立「身份」與「原生錢包賬戶」的經濟主體，而區塊鏈技術正好成為與AI agent綁定數字身份的關鍵工具。

●肖風（左）日前接受《經「滬」論》主持陳滬銘專訪。 香港文匯報記者萬霜靈 攝

談及AI智能體的身份體系，肖風認為未來所有AI Agent都將擁有獨立的「身份」，但這個「身份」並非沿用現實世界的身份證體系，而透過基於區塊鏈的地址和靈魂綁定代幣（Soulbound Token）形式來實現是一個技術上適配的解決方案。他指出，讓人工智慧體沿用現實世界的人類身份證體系顯然不切實際，並提到以太坊創始人7年前就提出「靈魂綁定代幣」概念，也是「非同質化代幣(Non-Fungible Token, NFT)」剛出來時的延伸概念。因為每一枚NFT都是獨一無二的， 透過NFT與區塊鏈技術，即可為每個AI agent綁定一個數字身份。

「如果AI Agent開始獨立於人並創造經濟價值，它一定需要一個賬戶，目前看唯一適配的形式是數字錢包，而不是透過銀行為該Agent開的賬戶。」肖風稱。他解釋道，在AI大模型階段，用戶透過傳統銀行賬戶購買的token，可以被消耗用於調用中國開發的大模型服務，但當進入Agent與Agent之間自由支付場景時，傳統銀行賬戶體系就無法支撐了，因其受制於多個智能體的開戶數量限制、責任歸屬不清、支付成本過高以及運轉效率低下等根本問題。據悉，HashKey Group已加入由Google發起的Agent Payment Protocol（AP2）技術聯盟，與PayPal、Circle、UnionPay International等機構共同探索AI Agent支付體系，並研究穩定幣支付、鏈上身份及AI Agent鏈上結算等應用。

未來每個人或擁50個AI Agent

肖風指出，在近年與人工智慧界專家學者交流中，大家普遍形成的共識是AI與加密技術（區塊鏈/加密貨幣）是一體兩面，兩者最終將深度融合，相互賦能，相輔相成。他進一步援引AI專家的觀點指出，未來每個人可能擁有達50個AI Agent，這些智能體將無縫滲透至我們生活的各個面向，從日常瑣事到複雜決策，全面提升個人效率與生活品質。

香港有條件成為數字金融「華爾街」

面對全球AI熱潮下的競爭，肖風認為香港擁有「背靠祖國」的得天獨厚優勢，只要善加利用，就能在全球數字經濟版圖中佔據中心位置。他指出，從互聯網、區塊鏈再到人工智慧，這三大領域基本是中美兩強稱雄的態勢。而香港作為中國的一部分，能夠充分借力內地龐大的人才資源、資產資源與技術資源，這是世界上其他地區難以複製的獨特優勢。憑藉「超級聯繫人」的定位，結合「一國兩制」下普通法的制度優勢，香港完全有能力實現特區政府提出建成「全球數字資產中心」的目標，甚至有望推動全球金融格局從過去的「紐倫港」格局，逐步升級為「紐港倫」，令香港在全球金融體系中的地位進一步躍升。

●香港文匯報記者 陳鍵行

(《經「滬」論》專訪肖風的完整版將於稍後時間推出)

掃碼睇片

OpenClaw被揭安全隱患兼「食錢」風口來時匆匆去也匆匆

「養龍蝦熱」急變「放生潮」

市場瞬息萬變，令人慨嘆風口來時匆匆去也匆匆。最近開源人工智能代理（AI Agent）OpenClaw（俗稱「龍蝦」）爆紅，一些內地互聯網龍頭如騰訊（0700）、百度（9888）等，早前也推出一鍵式雲端部署服務，「上門安裝龍蝦」成了內地熱門話題；然而，隨着OpenClaw被揭發有嚴重的網絡安全隱患，其實還是個「食錢怪」，一句簡單指令也會偷偷跑掉幾萬個流量單位（Tokens），有人開啟該AI才幾小時，賬單使用費便過千元（人民幣，下同）。有見及此，首批下載龍蝦AI的「養蝦人」已開始連夜尋求卸載該程式，催生了「上門徹底卸載」服務，而龍蝦AI的卸載指南也開始在網上廣泛流傳。 ●香港文匯報記者 周紹基

「龍蝦」OpenClaw剛推出時，曾出現深圳上千人排隊「免費領養」龍蝦AI的壯觀場面，甚至不少用戶當時不惜付費請人代勞安裝。惟不足一周後，近日「養龍蝦熱」演變成龍蝦「移除潮」。因為龍蝦AI不單存在驚人的運作成本，也令用戶資料安全面臨巨大風險，外電消息指促使內地官方私下向國企、政府機關、金融機構等發出風險提示，警告龍蝦AI可能導致資料外洩、支付賬戶等被竊取，對金融等行業可能造成毀滅性打擊，故嚴禁未經許可在辦公網絡或業務系統安裝使用OpenClaw。

自動載入龐大資料 消耗大量Tokens

目前不少首批下載龍蝦AI的用家，已紛紛急着花數百元，請專人「上門卸載」，形成一場科技鬧劇。有科技界人士指出，很多用家在使用OpenClaw時，忽略了背後的API Token消耗。龍蝦AI在執行自動化任務時，會持續與大型語言模型互動，即使用戶只跟它說句「你好」，該AI也會使用大量Tokens。

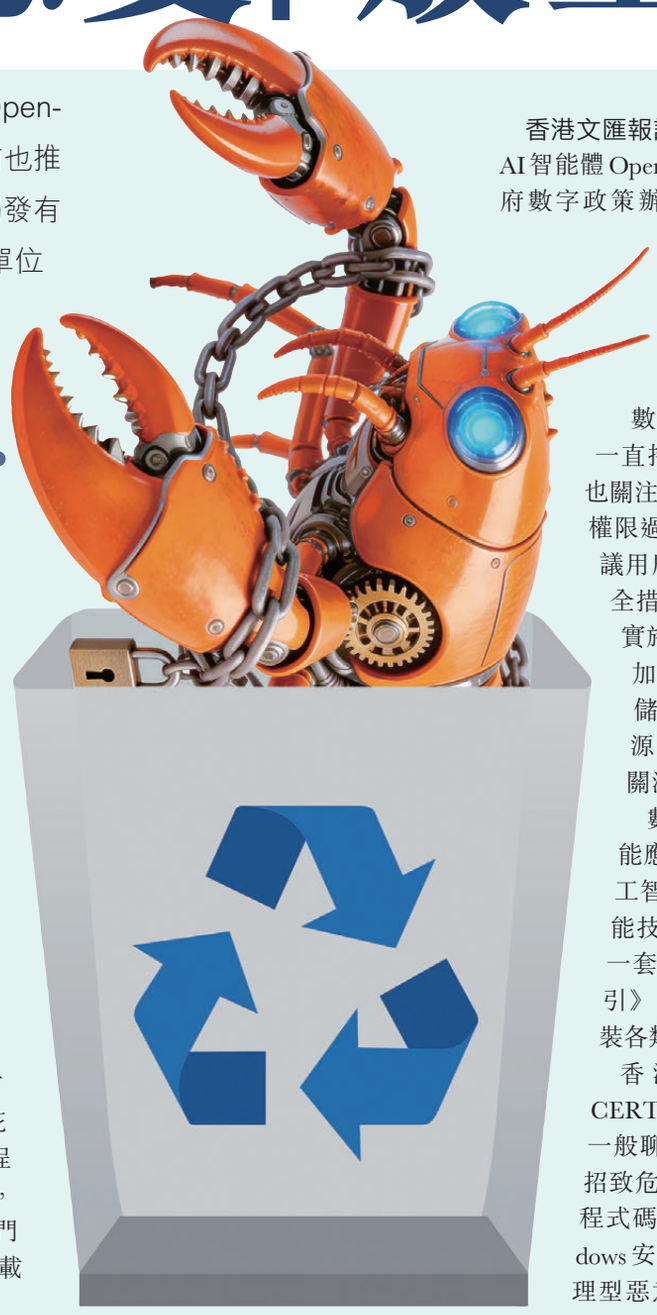
有用戶開着該AI數小時，便需支付大量流量費用，動輒上千元，這是因為龍蝦AI在每次講話前，都會強行載入大堆複雜背景資料和設定檔，導致成本飆升。若用戶沒有預設費用上限，費用便會急劇上升。故此，大量內地用戶都在四處詢問如何限制這「食錢」AI的流量。

此外，安裝龍蝦AI的時候，也會潛藏嚴重的網絡安全風險，很多用戶在設定AI時未有配置適當的防火牆，導致電腦的通訊埠(Port)直接暴露，極容易招致駭客掃描並接管系統的權限，令用戶個人隱私有洩露風險。內地已出現駭客利用漏洞盜用信用卡，甚至轉走加密貨幣的案件。

偶發邏輯錯誤 失控無視指令

OpenClaw在執行指令時，亦偶爾會出現邏輯錯誤。根據內地媒體報道，有用戶發現其龍蝦AI在處理電郵時失控，無視停止指令，瘋狂刪除收件箱內數百封重要郵件，甚至誤將整個電腦的資料清空。這種「不聽使喚」的表現，讓原本追求效率的工具變成災難。

隨着龍蝦AI的問題陸續湧現，逼使不少用家寧願花錢請專業人士遠端連線，甚至上門徹底移除有關AI。據內地媒體指，有龍蝦用家在不久前才花500元請專人上門安裝，不足1個月便急急移除程式。深圳、上海、北京等地均有標榜「安全徹底，無殘留」、「零殘留，永絕後患」等為口號的上門卸載服務，上門卸載收費接近300元、遠端連線卸載也需約200元。



●「龍蝦」用戶這一星期以來很忙碌，排隊下載，然後又匆忙卸載。 設計圖片

香港文匯報訊 (記者 莊程敏) 俗稱「龍蝦」的開源AI智能體OpenClaw的安全風險續引起關注，特區政府數字政策辦公室及香港網絡安全事故協調中心（HKCERT）分別發出警示，提醒相關單位和個人用戶在部署及應用OpenClaw時，須採取充足安全措施。

對運行環境實施嚴格隔離

數字辦在回覆傳媒查詢指出，該辦公室一直持續監測人工智能(AI)最新發展趨勢，也關注到有關OpenClaw存在潛在風險，包括權限過高、數據洩露及系統安全等方面。建議用戶在應用OpenClaw時，要採取充足安全措施，包括強化網絡控制，對運行環境實施嚴格隔離，以降低權限過高的風險；加強憑證管理，避免將密鑰以明文形式儲存在環境變量中；嚴格管理插件來源，確保插件的可信性與安全性；持續關注官方發布的安全更新等。

數字辦表示，特區政府高度重視人工智能應用的治理和風險防範工作，制定《人工智能道德框架》及《香港生成式人工智能技術及應用指引》等文件。同時已制定一套全面的《政府資訊科技安全政策及指引》，供各部門遵守和使用。各部門在安裝各類軟件前，必須開展風險評估。

香港網絡安全事故協調中心（HKCERT）亦提醒，AI代理平台風險已遠超出一般聊天式AI 工具。OpenClaw強大功能卻招致危機，惡意攻擊者可利用偽造的GitHub程式碼庫及Bing AI，向搜尋OpenClaw Windows安裝程式的使用者，散播惡意軟體與代理型惡意軟體，竊取資訊。另有報告指出，OpenClaw曾有高風險漏洞，惡意網站能藉此挾持OpenClaw 代理程式。雖然漏洞已獲修復，但事件說明，若然缺乏充分的安全監管與控制措施，部署AI代理工具可能會招致風險暴露。

籲盡快更新OpenClaw版本

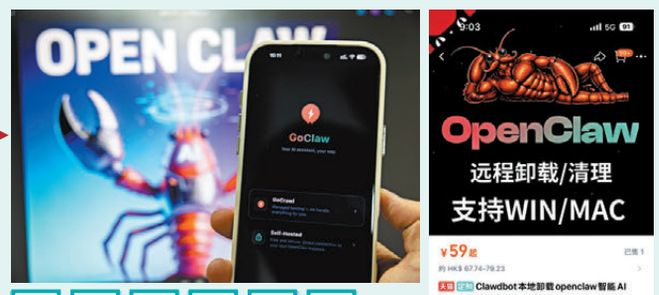
HKCERT 建議用戶應注意網絡安全，可採取的措施包括：核實下載來源與安裝指引；盡快更新OpenClaw版本；審慎安裝第三方「技能」腳本；當代理要求執行高風險操作時，保持警惕；把OpenClaw視為高權限自動化平台管理。

香港數字辦：應用OpenClaw時要採取安全措施

「龍蝦」科技鬧劇經過

排隊下載龍蝦

專家警示風險



用戶匆忙卸載

科企趕風口 投入「養蝦熱」

香港文匯報訊（記者 陳鍵行）隨着電腦端「養龍蝦」熱潮不止，有更多公司投入「養蝦業」，手機端的「龍蝦」應用亦橫空出世。百度（9888）昨日在安卓應用商店正式上線「紅手指Operator」，號稱全球首款手機龍蝦應用程式。用戶透過下載App並註冊，即可實現手機「養蝦」，而蘋果iOS端預計本月內上線。App上線後即收穫「龍蝦之父」的回應，表示願與百度共同開發龍蝦。

百度手機版「龍蝦」上線

在百度版手機版「龍蝦」上線後，OpenClaw創始人Peter Steinberger在海外社媒上連發兩條帖文回應，稱中國AI創新速度「Amazing」，並表示願與百度共同開發龍蝦。

據內媒消息，「紅手指Operator」由百度智能雲團隊打造，使用App無需更換設備，亦無需本地安裝複雜環境，下載並註冊後即可指揮百度版「龍蝦」執行任務，iOS端預計本月內上線。

在這一能力基礎上，「紅手指Operator」進一步將原生OpenClaw預置部署至雲端虛擬手機中，OpenClaw負責處理複雜任務，自動化指令將在電腦與網頁端環境中被執行，例如全網收集熱點並生成日報、跨網頁尋找資源並自動下載、執行深度數據抓取等任務。Operator則側重負責原生App環境中任務的執行。它能夠完成跨App、多線程的交互操作，比如打車、外賣訂餐、手機遊戲掛機、社交軟件交互等。

透過兩者協同，無論是在開會間隙還是通勤路上，用戶的一句指令就能使AI完成信息搜集、定時推送、跨平台操作等複雜流程。例如，用戶只需輸入「幫我搜索3月18日北京到長沙價格最低的機票」，系統即可在雲端自動完成搜索與下單步驟，僅需用戶確認即可。

App推出就引發下載熱潮，大量用戶的湧入，一度「撐爆」伺服器，系統後台資源出現緊缺提示。百度智能雲回覆，正全速調配資源擴容，全力保障用戶體驗。

商湯AI智能助力接入OpenClaw

商湯科技（0020）昨日亦宣布將旗下AI智能辦公助手「辦公小浣熊」的核心能力封裝為名為「Raccoon Skills」的功能插件，具備Excel數據分析、文檔處理、報告生成等能力，並全面接入OpenClaw生態，這意味任何正在「養龍蝦」的個人及開發者，都可以直接為自己的AI智能體安裝這個技能包，提升OpenClaw的辦公能力，猶如為「龍蝦」加上專門處理日常辦公問題的「工作鉗」。

除了軟件層面的合作，商湯攜手趨境科技推出「本地部署 + 雲端擴展」的AI Box，將OpenClaw、小浣熊能力與優化硬件整合，打造一台AI辦公專用機。方案以OpenClaw作為智能體執行層，支援多入口接入、任務執行和自動化調度，依託辦公小浣熊提供辦公能力與雲端擴展服務，並以趨境AI Box承接本地推理、設備部署與遠程運作及維護支持。

龍蝦概念股續回吐

香港文匯報訊 (記者 周紹基) 油價波動及中東局勢繼續影響港股，油價昨午曾一度急升近一成，高見每桶94.6美元，拖累恒指跌377點。臨近收市，隨着油價升幅回順，港股全日跌幅收窄至182點，收報25,716點。科指及國指一同低收，科指跌0.5%，國指微跌4點。成交續減，全日僅得2,422億元。油價偏強，使石油股向好，但近日爆火、俗稱「龍蝦」的OpenClaw被揭發有資訊安全及流量超支的風險，導致龍蝦概念股繼續回吐。

商湯智譜跌逾8%

焦點板塊方面，油價推升石油股，中海油(0883)升3.7%，中石油(0857)升1.1%。連煤炭股都有支持，兗礦能源(1171)升8.3%，兗煤澳大利亞(3668)升5.1%。油服股方面，山東墨龍(0568)再升2.4%，惟百勤油服(2178)先升後倒跌逾8%。另外，OpenClaw引發資訊安全風險，相關概念股反覆下跌，騰訊(0700)跌1%，阿里巴巴(9988)跌1.2%，商湯(0020)跌8.3%，Minimax(0100)及智譜(2513)各跌5%及8.9%。

輝立證券董事黃瑋傑昨表示，西方國家宣布動用戰略石油儲備，以緩解油價供應，油價昨午得以掉頭下降。但油價的跌幅並不大，是股市受壓的主因之一，主要因為今次並非是單純油價事件，市場都希望伊朗戰事盡快得到解決，以掃除不明朗因素。他表示，若港股失守10天線，可能恒指要再回調，並考驗25,610點這個支持位，更低的底部更下移至25,440點。