

●香港對數字資產「強監管 強合規」路線，令傳統金融機構安心開展相關業務。 香港文匯報AI製圖

近期加密市場接連發生中心化交易所資產被盜事件，最矚目莫過於幣安被黑客攻擊並盜走逾63億美元，即折合高達約494億港元，打破被盜加密資產金額的歷史紀錄，事件凸顯中心化交易所（CEX）的安全及風控問題，市場開始思考在監管和合規中尋找更安全的資產託管出路。香港數字資產市場正逐步由「有沒有牌照」的起步階段，邁入構建機構級風控體系的新階段。BlockSec聯合創始人、香港中文大學信息工程學系副教授周亞金近日接受香港文匯報專訪時表示，銀行及大型金融機構高度重視風險及合規，香港的監管要求雖然帶來額外成本，但亦為主流金融機構的參與帶來更廣闊的出路，長期發展會「更穩，後勁更大」。 ●香港文匯報記者 陳鍵行

港「強監管 強合規」路線 數字資產發展走得更遠更穩

BlockSec周亞金：為主流金融機構開關出路



●BlockSec聯合創始人周亞金認為，香港的監管要求雖然帶來額外成本，但亦為主流金融機構的參與帶來更廣闊的出路。 受訪者供圖

周亞金接受訪問時表示，香港選擇「強監管、強合規」路線，雖提高虛擬資產交易平台及穩定幣發行商的經營成本，但亦促使市場由過去依賴散戶及代幣交易的模式，轉向資產管理、代幣化資產及其他更接近傳統金融的業務。香港最初提出發展去中心化互聯網（Web3）時，去中心化金融（DeFi）社區一度非常興奮，市場曾預期各類去中心化金融協議可以在香港落地。但隨着政策逐步展開，可以看到香港實際走的並不是將離岸加密貨幣市場模式搬入香港，而是一條以合規為前提、希望與傳統金融接軌的數字資產發展道路。

數字資產管理 港發展潛力大

「如果你的Web3或者數字貨幣不能接入主流金融基礎設施，市場就很難真正做大。」周亞金指出，銀行及大型金融機構高度重視風險及合規，在缺乏合規框架下，金融機構不敢大規模採用區塊鏈作為金融基礎設施；隨穩定幣、代幣化資產逐步納入合規框架，主流金融機構才有條件參與。

他認為，香港監管要求帶來的成本，同時亦在重塑持牌平台的商業模式。離岸交易所可以面向散戶提供大量代幣交易，依靠交易量快速擴張，但香港的合規平台不能完全複製這套模式，需要在合規場景中重新尋找增長空間。周亞金舉例，香港可以發展數字資產管理、股票及其他資產上鏈，以及代幣化美國國債等業務。「短期來看，它可能沒有像離岸交易所那種爆發性的增長，但長期來看會更穩，後勁更大。」

監管邏輯與鏈上技術磨合需時

不過，香港現階段亦面對傳統金融監管邏輯與鏈上技術之間的磨合問題。周亞金以非託管錢包（unhosted wallet）為例，指傳統銀行賬戶背後有金融機構負責客戶身份識別（KYC），但區塊鏈地址可以由用戶自行建立，並沒有金融機構替每一個地址完成KYC。因此，如果把傳統金融的轉賬規則等制度完整搬到所有鏈上交易，便會遇到一個很實際的問題：「這些賬戶誰來做KYC？」他表示，這並不代表香港監管方向有問題，而是數字資產仍屬新領域，監管機構亦需要在市場發展過程中理解技術結構，尋找傳統金融監管目標與區塊鏈實際運作之間的平衡。

AI助篩查反洗錢 仍需人工把關

談及香港穩定幣的監管科技，周亞金表示，從技術角度看，穩定幣可透過智能合約監察交易及限制相關地址的資產移動，但真正困難之處並非「能不能凍結」，而是如何判斷哪一個地址具有風險。「技術上是可以做的，難點是你怎麼知道這筆資金是非法還是合法。」他指出，要識別風險地址，需要結合區塊鏈數據分析、鏈上行為分析及鏈上情報，對交易進行風險評級，而相關技術目前仍可能出現誤報或漏報。周亞金也認為，人工智能可協助處理大量反洗錢告警。AI Agent可先處理及篩選報告，再交由人員作最後確認；涉及大額資產時，仍應保留人工判斷，實際應用需要按風險及金額作分級、分層管理。

鏈上資金看得見 卻未必攔得住

香港文匯報訊（記者 陳鍵行）香港發展穩定幣，鏈上交易公開透明是否意味可疑資金可以被即時發現及截停？周亞金認為，數字資產可以追蹤，但「可追蹤」並不代表追蹤後一定能立即採取行動，真正的難點在於地址背後「究竟是誰」，以及能否在資金迅速轉移前完成風險判斷。他認為，香港應聚焦如何結合區塊鏈數據、交易行為及鏈上情報，快速且精準地識別真正的高風險地址。

周亞金指出，區塊鏈交易紀錄公開，資金由一個地址流向另一個地址可以被追蹤，但地址本身只是一串字符。若不知道地址背後的實際控制者，即使清楚看到資金流向，亦未必可以立即判斷交易是否涉及非法活動。

移動速度遠快於傳統執法程序

另一問題是數字資產移動速度遠快於傳統執法程序。周亞金表示，數字貨幣可以在數秒之內跨越不同地址及司法管轄區，而且建立新地址的成本極低，資金持有人可以透過大量地址分散資產，市場亦存在混幣器等工具增加追蹤難度。

即使執法部門最終識別到相關地址，凍結資產亦存在時間差。周亞金指出，司法機構要扣押或凍結資產，需要取得充分證據及完成相關法律程序，「等你把所有證據都蒐集好，向法庭要求凍結的時候，資產可能已經走了。」跨境資金則進一步增加難度。若資產流入其他交易平台、跨鏈橋或穩定幣，企業及執法機構需要與不同司法管轄區及相關服務提供者協作，而跨境司法合作本身亦需要時間。

結合鏈上數據 識別高風險地址

周亞金表示，因此交易平台一旦發生安全事故，第一時間最重要的並非完全查清攻擊方法，而是立即追蹤資金，同時聯絡執法機構、資金流入的交易所或跨鏈橋，以及相關穩定幣發行商，爭取先截停資產，再補充後續調查及法律程序。對香港穩定幣而言，他認為技術上能否監控及限制地址並非最大的瓶頸，更關鍵的是如何結合區塊鏈數據、交易行為及鏈上情報，足夠快及準確地識別真正的高風險地址。

今年加密市場安全事件頻發（部分）

發生日期	受害平台或項目	估算損失金額	主要攻擊手法與原因	備註或後續發展
2026年10月29日	幣安 (Binance)	63 億美元	工程師手提電腦遭入侵，黑客藉此存取服務容器並提交未經授權的提現	史上最大盜幣案，當中約30億美元資產已成功凍結，幣安承諾全額補償受影響用戶
2026年9月	Bitget	3.51 億美元	中心化交易所熱錢包 / 基礎設施漏洞遭惡意利用	官方事後與多家機構展開追截及安全升級
2026年4月	KelpDAO	2.92 億美元	黑客入侵 LayerZero 相關基礎設施並偽造跨鏈消息，無底層資產下憑空鑄造代幣	屬於嚴重的 DeFi 協議基礎設施漏洞利用
2026年4月	Drift Protocol	2.85 億美元	「社會工程學」（即利用人性弱點的攻擊）攻擊，黑客取得安全委員會管理權限，將無價值代幣設為抵押品並借走資產	針對 DeFi 治理與多重簽名權限的漏洞利用

風控職能趨融合 複合型人才需求增

香港文匯報訊（記者 陳鍵行）隨着香港數字資產市場朝合規化、機構化發展，企業對人才及風險管理能力的要求亦正在改變。周亞金表示，數字資產令安全、風控及合規三個傳統上分開運作的職能逐步融合，亦令香港對複合型人才的需求增加。

周亞金指出，在傳統體系中，安全團隊主要負責程式碼及伺服器安全，合規部門處理反洗錢，風控團隊則處理業務風險，三者分工相對清晰。但數字資產進入企業業務體系後，這些界線開始變得模糊。例如數字資產一旦被盜，企業除了處理技術漏洞，亦要即時追蹤資金、與執法機構及律師合作；由資產保管、存入、提取至支付，亦需要持續判斷是否涉及非法資金。

「數字貨幣進入業務體系後，由保管、存入、提取到支付，中間是否涉及非法資金，所有環節其實一下子串在一起了。」他認為，未來涉及數字資產的企業，很難再把安全、風控及合規完全割裂。

這亦改變了香港的人才需求。周亞金表示，數字資產從業人員一方面需要技術思維，理解智能合約；另一方面亦要具備商業及金融思維，掌握基本金融衍生品知識，同時了解一定程度的法律及監管要求。

高校與監管增互動 課程緊貼需求

他指出，目前香港部分高校已有區塊鏈相關課程及學位，但培養的人才仍較偏向單一技術方向，同時具備技術、金融及監管知識的複合型人才仍較稀缺。

他認為，香港既然選擇走合規數字資產發展道路，產業界、高校及監管機構之間亦需要增加互動，讓高校更了解業界實際需求，同時讓監管機構更深入掌握技術及商業模式的變化。

CEX失竊衝擊信心 託管風控需升級

香港文匯報訊（記者 黎梓田）上月底幣安被黑客攻擊並盜走逾63億美元，已成為加密行業歷史上規模最大的安全事件之一。HashKey Group高級研究員孫偉向香港文匯報表示，從過去的經驗來看，大型交易平台遭遇安全事件，對市場的影響並不僅僅在於被盜資產本身，更在於其可能廣泛削弱市場風險偏好，並引發投資者對中心化交易所（CEX）資產安全、償付能力及流動性風險的重新評估，亦將對機構的權限管理、交易驗證和安全審計提出更高要求。



●幣安被黑客攻擊盜款，引起市場關注加密資產風險。 資料圖片

孫偉指出，當前比特幣本身正面臨調整壓力，美國實際利率持續處於高位，抬高了投資者持有比特幣的機會成本，而現貨ETF資金需求減弱、長期持有者上方積累較大沽壓，限制了比特幣反彈空間。在這背景下，買盤更加謹慎。

令資產價格波動放大

此次事件可能帶來的流動性影響亦值得關注。孫偉認為，幣安作為全球最大的數字資產交易平台，其充提業務暫停不僅影響自身用戶，也可能影響做市商的跨平台資金調配和市場流動性。尤其是在市場風險偏好已經下降的背景下，一旦投資者集中轉移資產、做市商主動收縮風險敞口，就可能進一步放大價格波動，並向市場傳導。

從長期來看，此次事件也可能進一步推動監管機構提高對數字資產託管和交易平台風險管理的要求，包括獨立第三方託管、客戶資產隔離、冷熱錢包管理及簽名權限控制等，對機構的權限管理、交易驗證和安全審計也提出更高要求。

港可設「提款熔斷機制」防幣安事件重現

香港文匯報訊（記者 黎梓田）幣安近日遭黑客入侵並盜走巨額資產的事件，再次為全球虛擬資產產業敲響了技術安全的警鐘。有Web3業界人士建議，香港作為正大力發展Web3的國際金融中心，證監會與金管局可從中吸取多方面的風控與合規經驗。

在加強風控措施方面，香港必須繼續嚴格落實將至少98%客戶資產存放於線下冷錢包的規定，並針對其餘2%的熱錢包引入門檻簽名（MPC）與多重簽名機制，避免單一員工憑證遭劫持即引發系統性提款。同時，合規平台內部應全面貫徹零信任架構與雙人授權機制，強化DevOps工程師設備的端點安全監控，防範進階持續性威脅（APT）攻擊。

發行人需具鏈上快速凍結技術

在技術與應急防禦層面，香港應要求持牌交易所部署基於大數據與AI的動態提款熔斷機制。一旦偵測到異動或非典型合約呼叫，系統需能即時暫停交易，並與區塊鏈安全機構共享威脅情報。此外，鑑於事件中穩定幣發行人迅速協助凍結被盜資產，香港在落實法幣穩定幣發行人監管制度時，也應明確要求發行人具備配合執法部門進行鏈上快速凍結的技術能力與法定條款。

最後，為保障散戶投資者利益，香港應持續要求持牌平台提供足額的第三方商業保險與獨立補償基金，並貫徹客戶資產與平台營運資金的獨立託管。這場事件證明Web3的核心威脅已轉向高階網絡安全與技術漏洞，香港唯有堅持「風險為本、安全為先」的原則，以最高標準的技術審計與應急機制嚴格把關，才能在推動創新的同時打造出受國際信任的數字資產生態圈。