

陳志華 | 超級電腦未來可破解所有虛擬資產區塊鏈？

編輯：方靜蕙 責編：韓進珞

AI播報 

2026-10-06 09:27

AI摘要

- 量子電腦或威脅區塊鏈加密，但非即時危機。
- 後量子密碼學可助區塊鏈升級過渡。
- 香港應及早佈局金融科技與人才培訓。



社會不用對量子電腦過度恐慌，但亦不應忽視長遠影響。

文：陳志華

近日坊間流傳，指未來超級電腦可破解所有虛擬資產區塊鏈，甚至創造新鏈，因而有人認為不值得投入Web 3.0。筆者認為此說法忽略區塊鏈與密碼學本質，值得客觀釐清。

區塊鏈褪去包裝，本質是分散式記帳本加上密碼學。其防禦建基於數學密碼難題，並非牢不可破。理論上，只要有足夠算力及針對性算法，密碼確可能被破解。然而，以現時傳統超級電腦算力，若以暴力方式推算私鑰，所需時間可能比宇宙年齡更長。因此，坊間所指「超級電腦」，相信實際是量子電腦。

量子電腦並非單純提升算力，而是利用量子疊加與量子糾纏，配合秀爾演算法（Shor's Algorithm），對現有區塊鏈依賴的橢圓曲線加密（ECC）及RSA加密構成重大威脅，可謂降維打擊。業界將量子電腦真正威脅密碼學之日稱為Q-Day，近期有預測指可能於2030年來臨，但時間表仍不確定。

面對量子威脅，區塊鏈並非坐以待斃。分散式帳本技術與密碼學一直進步，底層加密演算法有升級至抗量子方案空間，例如透過硬分叉更新協議。美國已制訂抵抗量子電腦攻擊的新一代加密標準。學術界近年積極研究區塊鏈如何過渡至抗量子時代，後量子密碼學（Post-Quantum Cryptography, PQC）成為熱門課題。本人兩年前在香港曾參加後量子密碼學穩定幣發布會，可見相關項目逐步浮現。主流加密貨幣社群亦討論過渡至PQC算法，以對抗量子電腦泛用化攻擊。

量子技術與區塊鏈之間，並非單純破解與毀滅，而是一場密碼學矛與盾之爭，雙方你追我趕。關鍵在於量子電腦商用落地較快，還是後量子密碼學發展更快。若後者及時成熟，區塊鏈生態便可有序過渡，繼續發揮價值。

值得注意的是，密碼學應用不限於加密貨幣。銀行業長期大量應用密碼學，例如硬件安全模組（HSM），保障交易與數據安全。香港金融管理局在Fintech 2030策略宣言中亦納入量子抗性（quantum resilience），推動銀行業預備應對量子電腦攻擊，反映監管機構已正視風險。

精選文章



青聯策論 | 新時代創業：從「點起步」到「點連結世...」



寰宇前瞻 | 低碳轉型審慎風險 建立協調治理框架



姚志勝 | 美財長會否來港出席APEC財長會？——也談...



夏小嫻 | 中美關係新定位下的香港機遇與擔當



陳博智 | 凝聚愛國力量 堅定推進祖國統一大業

筆者認為，社會不用對量子電腦過度恐慌，但亦不應忽視長遠影響。**虛擬資產與Web 3.0發展，關鍵不在於是否被單一技術徹底摧毀，而在於業界能否及早準備、持續升級加密標準，並與監管機構保持溝通。香港作為國際金融中心，若能在後量子密碼學、金融科技及人才培訓方面及早佈局，既可提升金融系統韌性，亦可把握新一輪技術轉型機遇。**與其因傳聞卻步，不如以客觀務實態度認識風險，在密碼學矛與盾之間，尋找穩健發展之路。

作者為香港證券及期貨專業總會會長

本文為作者觀點，不代表本媒體立場

圖：IC photo

#陳志華

#超級電腦

#虛擬資產

#區塊鏈

#Web3.0

#金融科技

#香港證券及期貨專業總會



評論



寫下您的評論...

評論

編輯推薦



梁文廣 | 堅決打擊分裂干涉 善用「一國兩制」優勢共創復興前景

議事堂 | 2天前



卓偉 | 發布煽動假信息無關新聞自由 《紐約時報》罔顧事實顛倒是非

議事堂 | 3天前



周文港 | 順風揚帆，更上層樓

議事堂 | 4天前



李誦 | 香港亞運成績單背後的合作密碼

議事堂 | 4天前



劉暢 | 七十七載風華正茂 香港乘勢開創新局

議事堂 | 4天前



崔劍 | 國慶講話鼓勵香港積極融入國家發展大局

議事堂 | 4天前

橙TV

專訪

視頻專題

動畫圖解

資訊

港聞

國際

兩岸

區聞

評論

議事堂

有話直說

圍爐

投投是道

財經

財經專欄

產經

地產

搵錢呢啲嘢

文化

文化本事

書人書事

文化專欄

樓上戲院

親子教育

名人專訪

教養妙法

好書推薦

升學導航

生活

發緊夢

Mycookey

玩樂情報

飲食優惠

娛樂

即時娛樂

煲劇誌

電影快遞

娛樂專欄

公仔紙

備仔有心事

文地貓

腔叔

YO! s 生活漫畫式

HK Eye

The Reason I Liv...

Master Talks

ICH of HK

China Curiosity