比特幣與量子時代的對決：您的資產還安全嗎？

莊允心 [1†]
[1] 國立成功大學工學院工程管理碩士在職專班
yhchuang@gs.ncku.edu.tw

摘要

比特幣於 2009 年問世，作為全球首個去中心化的加密貨幣 (Cryptocurrency)，如今已成為規模最大的加密貨幣，並帶動了其他各種加密貨幣的發展。比特幣系統的安全性植基於公開金鑰密碼學 (Public-Key Cryptography)，然而，隨著量子運算技術的快速發展，比特幣系統所採用的橢圓曲線數位簽章演算法 (ECDSA) 與安全雜湊演算法 (SHA-256) 面臨著被破解的風險，使得比特幣及其他區塊鏈 (Blockchain) 系統處於風雨欲來的安全威脅。本研究將剖析比特幣的運作原理與交易機制，探討其資產安全性與投資風險。也將分析量子電腦的發展趨勢與量子運算技術的最新進展，評估其對比特幣系統的潛在威脅，進一步討論可行的因應方案，以確保比特幣在量子時代的穩定性與安全性。

關鍵詞：比特幣、區塊鏈、量子運算、後量子密碼學

† 通訊作者 (Corresponding author.)

Bitcoin Security in the Quantum Era: Risks, Challenges, and Solutions

Yun-Hsin Chuang[1]
[1]College of Engineering, National Cheng Kung University
yhchuang@gs.ncku.edu.tw

Abstract

Bitcoin was introduced in 2009 as the world's first decentralized cryptocurrency. Today, it is the largest cryptocurrency by market capitalization and has driven the development of various other cryptocurrencies. The security of the Bitcoin system is based on public-key cryptography. However, with the rapid advancement of quantum computing technology, the elliptic curve digital signature algorithm (ECDSA) and the secure hash algorithm (SHA-256) used by Bitcoin are at risk of being compromised, putting Bitcoin and other blockchain systems under imminent security threats. This study will analyze the operation and transaction mechanisms of Bitcoin, explore its asset security and investment risks, and assess the development trends of quantum computing and the latest advancements in quantum computing technology. It will also evaluate the potential threats to the Bitcoin system and further discuss possible solutions to ensure Bitcoin's stability and security in the quantum era.

Keywords: Bitcoin, Blockchain, Quantum Computing, and Post-Quantum Cryptography

壹、前言

比特幣 (Bitcoin) 是全球最具影響力的加密貨幣 (Cryptocurrency)，它推動著區塊鏈技術的發展。比特幣的核心安全機制依賴於公開金鑰密碼學 (Public-Key Cryptography)與工作量證明 (Proof of Work, PoW)，確保交易的完整性與不可篡改性。然而，隨著量子計算技術的快速進步，現行的簽章機制可能面臨挑戰。量子電腦的發展雖尚未達到足以威脅比特幣的程度，但各國政府與科技巨頭正積極研發更強大的量子計算技術，一旦突破 2000 個以上的量子位元 (Qubits)，現有的簽章演算法將難以抵禦量子攻擊。本研究將深入探討比特幣在量子時代下的安全性與發展前景，分析量子運算對其核心密碼學機制的潛在影響，並評估可能的應對措施。同時，我們也將探討比特幣市場的波動性，為投資者提供建設性的建議，以確保數位資產在未來仍能保持安全性與穩定性。

貳、比特幣的運作原理與交易

2008 年中本聰 (Satoshi Nakamoto) 以化名發佈了比特幣白皮書[13][14]，並於 2009 年推出了比特幣網路，開創了去中心化數位貨幣 (Digital Currency) 的時代。比特幣的核心技術——區塊鏈 (Blockchain)，則是它的支撐基礎，提供了分散式的記錄和驗證機制。至今，中本聰的真實身份仍然是謎。比特幣不僅是最早推出的加密貨幣，亦已成為目前市值最大的加密貨幣。比特幣相較於傳統貨幣的最大特色在於其「去中心化」與「匿名性」。任何人皆可匿名創建帳戶，且用戶的轉帳記錄與系統中新發行的比特幣均由區塊鏈上的分散式帳本來維護與管理。系統透過去中心化的點對點 (peer-to-peer, P2P) 網路來處理轉帳需求及管理。因此，比特幣的運作不會受到任何個人、團體、企業，甚至國家機構的第三方控制。在比特幣問世前，已有許多相關的數位貨幣概念，如 David Chaum 的 ecash [3][4]、Adam Back 的 Hashcash [1]、Wei Dai 的 b-money [16]、 Nick Szabo 的 Bit Gold [11] 以及 Hal Finney 的 Reusable Proof-of-Work (RPOW) 等，透過將這些概念整合，最終促成了比特幣的誕生。

2009 年 1 月 3 日，中本聰在位於芬蘭赫爾辛基的一個小型伺服器上，創建出史上第一個比特幣區塊—創世區塊 (Genesis Block)，並獲得 50 枚比特幣的獎勵，這也是比特幣系統中第一批比特幣。2010 年 5 月 22 日，一位名叫 Laszlo Hanyecz 的工程師以一萬枚比特幣購買了兩片 Pizza，當時一枚比特幣的價值只有 0.003 美元，若以現在的比特幣價格換算，如今那兩片 Pizza 已價值約 8.25 億美元。這筆交易被認為是比特幣在現實世界中的第一筆交易，也是在比特幣歷史上最為著名的一筆，不僅展示了比特幣作為一種支付工具的潛力，也讓比特幣的價值開始被更多人認識，奠定了未來的重要基礎，幣圈的人甚至把每年的 5 月 22 日訂為比特幣披薩日 (Bitcoin Pizza Day) 來紀念。

2.1 運作原理

比特幣是一種基於點對點網路的加密貨幣，並利用區塊鏈技術作為底層架構的電子現金系統。它使得線上支付能夠直接由一方發起並支付給另一方，而無需依賴任何金融機構作為中介。這樣的設計解決了在沒有中心機構的情況下如何發行和流通貨幣的問題，並創建了一個匿名且去中心化的電子記帳系統。比特幣採用「分散式帳本」，這些帳本被同步儲存在系統中所有的全節點 (Full Node) 中。每個全節點都完整儲存並驗證比特幣區塊鏈中的資料，以確保交易的有效性，並協助維護系統的共識。這種架構不僅增強了比特幣系統的透明性與安全性，還使得整個網路無需依賴任何單一的第三方機構或中央控制，進一步確保其去中心化的特性。比特幣透過區塊鏈和全節點的分佈式結構，實現了去中心化且透明的交易和資金管理，讓用戶能夠安全地進行點對點交易並且保持高度隱私性。

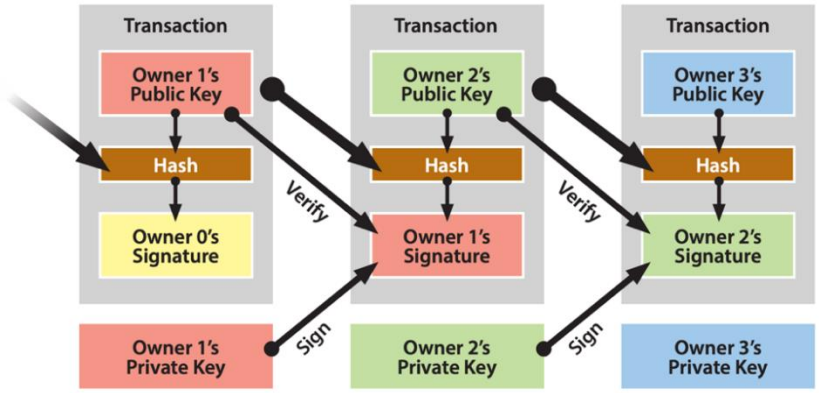
比特幣帳戶其實就是公開金鑰密碼系統中的一組公鑰 (Public key) 與私鑰 (Private key)，它們構成了你的比特幣錢包 (Bitcoin Wallet)。任何人都可以隨機生成私鑰，然後由私鑰算出公鑰，再由公鑰經過雜湊等步驟生成比特幣地址 (Address)。每枚比特幣本身並沒有唯一的編號，但是可以透過帳本來追蹤每一筆比特幣的來源和去向。這是因為比特幣是基於區塊鏈技術運行的，所有比特幣的移轉都會被記錄在區塊鏈上。這些帳本紀錄了每筆轉帳的細節，例如：發送者、接收者、轉帳金額以及時間戳記 (Timetamp)…等，讓比特幣具有可追蹤性。對於每個比特幣帳戶而言，地址是公開的，用於接收和傳送比特幣；而私密金鑰則需要妥善保管，它是用來簽署轉帳的關鍵。公鑰在一開始是保密的，但一旦需要從該地址進行轉帳，就必須公開公鑰，以便讓其他人驗證簽章的合法性。可以在相關網站[24]查詢比特幣的交易紀錄。

以下是當 Owner 1 要轉帳給 Owner 2 時的運作流程：

(1) Owner 1 準備轉帳的內容：發送方 (Owner 1) 和接收方 (Owner 2) 的比特幣地址，以及要轉帳多少比特幣。

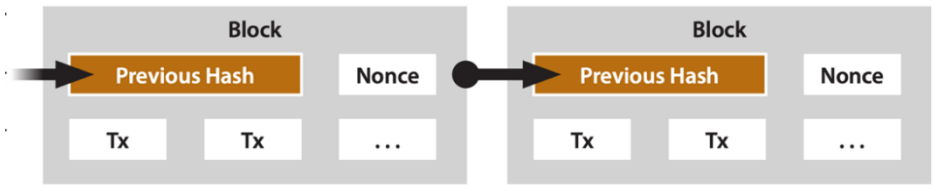
(2) Owner 1 使用自己的私鑰簽署這筆轉帳，以確保轉帳的合法性和證明此為 Owner 1 本人發起的轉帳，因為只有 Owner 1 的私鑰才能生成有效的簽章 (Signature)。一旦簽名完成，Owner 1 會將這筆已簽署的轉帳（包含轉帳內容、簽章及 Owner 1 的公鑰）發布到比特幣的點對點網路中，並將該轉帳廣播給其他比特幣節點。

(3) 當比特幣系統中的全節點收到這筆轉帳時，全節點會進行驗證。驗證的過程包含： 確認轉帳格式是否正確、確認 Owner 1 的帳戶有足夠的未使用交易輸出 (Unspent Transaction Outputs, UTXO，類似帳戶餘額的概念）來進行這筆轉帳、用「轉帳內容、簽章、Owner 1 的公鑰」來驗證簽章的合法性，確保這是由 Owner 1 所簽署的轉帳。驗證無誤後，這筆轉帳會被放入記錄池 (Mempool) 中，等待礦工進行下一步處理。（如圖一所示）



圖一 轉帳流程 [14]

(4) 挖礦的核心是工作量證明，全節點礦工 (Full Node Miner) 需要不斷嘗試選取一個區塊內的隨機數 (Nonce)，直到找出一個符合當前的挖礦難度 (Mining Difficulty) 要求的區塊雜湊值 (Hash Value) ，也就是說其雜湊值前段包含足夠多的零。比特幣的挖礦難度會根據區塊產生的速度來調整，目的是保持每大約 10 分鐘產生一個新的區塊。因此，難度越高其雜湊值前段零的數量就會越多，這意味著礦工需要不斷嘗試更多次的隨機數，直到碰巧得到一個滿足要求的雜湊值。當礦工開始挖礦時，他會從記錄池中選擇多筆尚未確認的轉帳，並將這些轉帳打包到一個候選區塊中，這個區塊包含了轉帳資料、前一個區塊的雜湊值以及一些其他資訊。接著，礦工會生成一個隨機數 (Nonce)，然後將這個隨機數、候選區塊的轉帳資料、前一個區塊的雜湊值、以及礦工的地址獲得挖礦獎勵金 (Block Reward)…等資訊組合起來產生一個雜湊值，如果這個雜湊值的前段有足夠多的零來滿足系統要求的挖礦難度，那麼我們就說他挖到礦了，他將有機會獲得產生新區塊的資格，接著他會將他挖到礦的消息發布到比特幣的點對點網路中。(如圖二所示)



圖二 區塊鏈 [14]

(5) 當其他節點接收到這個新的區塊後，他們會驗證區塊的合法性，以確保這個區塊的所有轉帳都是有效的。如果驗證通過，這個區塊就會被添加到區塊鏈上，並且這些轉帳

會被視為已經確認。當某筆轉帳進入新的區塊並被確認時，這筆轉帳便完成了，此礦工當初寫進新區塊的獎勵金就成為比特幣系統新發行的比特幣。

2.2 比特幣的發行

比特幣是透過挖礦（找到特定的隨機數）過程生成的，系統每產生一個新的區塊，發給礦工的獎勵金就是新發行的比特幣。在最初始的時候（2009 年）礦工的獎勵金為 50 枚比特幣，也就是說比特幣系統每 10 分鐘會產生一個新的區塊及發行 50 枚比特幣。然而，貨幣如果無止盡發行的話會造成貨幣的貶值，故礦工獎勵金每四年會減半一次，這樣的設計使得比特幣逐漸變得稀缺，從而提高其價值。礦工獎勵金減半到最後會趨近於 0，改成支付礦工手續費，當比特幣總量趨於恆定時，比特幣的總數大約為 2100 萬枚。如果礦工數量過少或礦工不再有足夠的激勵來參與，比特幣網路可能會變得不穩定，進而影響到交易的處理速度和安全性。因此，確保有足夠的礦工在系統中運行是比特幣長期運行和發展的重要關鍵。

2.3 比特幣錢包

隨著比特幣的普及，如何安全存放比特幣資產成為每位投資者關心的問題。比特幣不像傳統銀行帳戶，它的存取依賴於「錢包」，比特幣並非真的保存在比特幣錢包內，所有的轉帳行為都被記錄在區塊鏈中，用戶透過錢包的「私鑰」，證明交易紀錄上的虛擬幣屬於自己。比特幣錢包更像是一個「鑰匙圈」，保存著錢包的地址與私鑰，提供一個直觀的介面供用戶來追蹤他們的交易紀錄，用戶可以透過錢包的地址來進行接收比特幣，也可用私鑰把比特幣轉帳到其他錢包。

錢包的種類與特性，直接影響著比特幣資產的安全性與使用便利性。根據儲存方式的不同，比特幣錢包可以大致分為以下三種：

(1) 熱錢包 (Hot Wallet)：隨時可用，但風險較高，僅適用於需要頻繁交易或小額支付的用戶。熱錢包指的是連接網路的比特幣錢包，隨時可以存取與交易，因此特別適合日常使用。無論是手機、電腦還是網頁瀏覽器，都可以執行熱錢包軟體，讓用戶輕鬆進行比特幣支付或轉帳。然而，由於這些錢包與網路相連，它們容易成為駭客攻擊的目標，如果設備感染惡意軟體，或駭客獲得存取權限，可能導致資金被盜，因此不建議存放大量比特幣。

(2) 冷錢包 (Cold Wallet)：離線儲存，適合長期及大量持有。冷錢包又稱離線錢包， 它不與網路連接，因此能有效防範駭客攻擊。這類錢包適合長期持有大量比特幣的投資者，雖然存取時稍嫌不便，但安全性極高。冷錢包的核心概念是離線儲存私鑰，確保駭客無法遠端存取資金。常見的冷錢包有硬體錢包 (Hardware Wallet) 和紙錢包

(Paper Wallet)。硬體錢包透過 USB 連接電腦交易，但私鑰仍然保持離線。紙錢包和實體錢包是指將比特幣的私鑰印在紙張或實體物品上，其使用實體方式離線儲存私鑰，當有需求時才進行授權交易，以降低遭駭客盜取私鑰的風險。然而，硬體錢包則需保管好裝置與備份密碼，紙錢包和實體錢包可能被週遭之人看到私鑰或是可能因物理損壞或遺失而無法取回資產。

(3) 交易所錢包 (Exchange Wallet)：方便但風險集中。許多新手投資者將比特幣存放在交易所，這是一種最直觀、最方便的方式，因為交易所錢包不需要管理私鑰，用戶只需登入帳戶即可交易。然而，這種方式的風險在於交易所擁有私鑰，而非用戶本身，如果交易所發生駭客攻擊、內部倒閉或資金挪用，用戶的資產可能瞬間消失。萬一交易所遭駭或倒閉，資金可能無法取回。投資界流行一句話：Not your keys, not your coins.，意思是如果你沒有掌握私鑰，那麼這些比特幣並不真正屬於你。因此，不建議長期將大額比特幣存放在交易所，而應該將之移轉到冷錢包中。

2.4 比特幣的交易

比特幣交易所的主要功能是買賣比特幣，它提供了一個市場，讓用戶可以用法定貨幣或其他加密貨幣來交易比特幣。當用戶從交易所購買比特幣後，可以選擇將其存放在交易所內的錢包，或是轉帳到自己的個人錢包。同樣地，如果用戶要在交易所出售比特幣，通常需要先將比特幣從個人錢包轉帳至交易所的錢包，才能進行交易。

比特幣小額付款 App 提供用戶以更方便快速的方式使用比特幣進行日常支付。比特幣小額付款 App 使用的閃電網路 (Lightning Network, LN) 是一種比特幣的第二層擴展技術，它的主要目的是加快交易速度並降低手續費，讓比特幣可以用於日常小額支付，例如：買咖啡、支付線上服務等。比特幣區塊鏈的設計雖然安全，但交易速度較慢（您結帳時願意在櫃檯前枯等 10 分鐘嗎？），因為每個區塊大約 10 分鐘產生一次，處理的交易數量有限，而且手續費會因為區塊空間有限而上升，小額交易成本太高。閃電網路解決了這些問題，讓比特幣支付幾乎即時完成，並且手續費極低。兩個用戶開設一個「支付通道」，事先將比特幣存入這個通道的智能合約，這筆存款類似於「押金」，以確保未來的交易可以在這個通道內進行，此後這兩個用戶可以不限次數地互相轉帳，這些交易不需要立即上鏈，因此沒有手續費或確認時間的問題。每次交易時，雙方更新各自的餘額，並簽署新的交易狀態。當用戶不再需要交易時，他們可以選擇關閉支付通道，最終的餘額會被提交到比特幣區塊鏈，正式記錄在鏈上。閃電網路不僅允許兩個用戶直接交易，也允許透過「多跳 (Multi-hop) 」的方式，讓不直接連接的用戶之間轉帳。交易幾乎是即時完成，不需要等待 10 分鐘的區塊確認時間。因為大部分交易都發生在「鏈下 (Off-chain) 」，只有開啟和關閉通道時才需要上鏈，所以手續費極低，適合小額支付。在支付通道內的交易不會被公開記錄在區塊鏈上，因此更難被追蹤，可以提供更好的隱私性。

然而，在使用比特幣小額付款 App 時需注意 App 運營商的信任風險，一些比特幣支付 App 是由小型企業或初創公司運營，若營運商因資金問題倒閉，用戶的比特幣可能無法取回。在選擇上應謹慎，並避免在不信任的 App 存放大量資金。

2.5 幣值波動

就貨幣發行量而言，物以稀為貴，由於礦工獎勵每四年減半，新比特幣的產出速度將逐漸降低，比特幣的總供應量被嚴格限制在約 2,100 萬枚。此外，一部分比特幣因私鑰遺失而無法流通，進一步減少市場上的可用供應，這種稀缺性使比特幣具備長期保值的潛力。

量子電腦的發展會不會造成比特幣幣值的波動？請試想:「如果您能藉由量子運算來取得某地址的私鑰，您會怎麼做呢？」大肆張揚以顯示自己很厲害，角逐諾貝爾獎？盜取大部分的比特幣，將之轉帳到您帳戶成為世界首富？或是安安靜靜地偷偷轉帳某些大戶的部分資產到您帳戶？前兩者皆會造成幣圈恐慌導致比特幣幣值跳水狂墜，好不容易盜來的比特幣將變得一文不值；後者，被盜者通常會懷疑自己電腦遭駭或是實體錢包被親密之人盜用，不會懷疑比特幣系統已被量子電腦攻破。

比特幣屬於高風險資產，其價格受政策、金融環境與全球經濟形勢多重影響，波動性高（如圖三所示），長期價值受到市場供需、技術發展與投資信心所左右。各國政府對加密貨幣的政策及監管態度會直接影響市場信心，例如：中國在 2021 年嚴厲打壓比特幣挖礦及加密貨幣交易、美國總統川普於 2025 年 3 月簽署了一份行政命令[26]，美國政府會集中保管透過刑事與民事沒收所得的所有比特幣，作為不出售的儲備資產，類似於政府儲備黃金或石油的方式。戰爭、制裁或國際關係緊張可能促使資金流向比特幣作為避險資產，例如俄烏戰爭期間，部分資金流入加密貨幣市場。美國聯邦準備理事會 (Federal Reserve System, Fed) 等央行的利率決策與量化寬鬆政策會影響比特幣市場流動性，例如：當利率上升，傳統投資回報增加，資金可能從高風險資產撤離。比特幣指數股票型基金 (Exchange-Traded Funds, ETF) 等金融產品的推出也會短暫提升比特幣的需求與價格。當法定貨幣通膨嚴重時，比特幣常被視為抗通膨資產，需求上升會推高其幣值。全球經濟不景氣時，投資人可能減少對高風險資產的持有，導致比特幣價格下跌；反之，若市場預期經濟恢復，比特幣可能隨高風險資產上漲。比特幣幣值的波動大，投資人應充分理解並承擔投資風險。

圖三 近五年比特幣兌新台幣之變化 （資料來源：Google）

參、量子電腦對比特幣的威脅

本章將探討量子運算及量子電腦的發展現況，分析其對比特幣網路所造成的威脅程度，並探討防禦及應對方案。

3.1 量子運算的發展與潛在威脅

近年來，量子運算技術的快速發展讓學術界與產業界豎起警戒雷達。有別於傳統電腦，量子電腦利用量子位元 (Qubit) 進行運算，透過量子疊加 (Superposition) 與量子糾纏 (Entanglement) 來大幅提升運算能力，在某些特定問題上能夠實現指數級加速，如：大質因數分解、解離散對數、以及某些組合的最佳化問題...等。這項技術的突破對現今許多系統的加解密機制、簽章機制、身份認證機制以及金鑰協定等構成嚴重威脅，使目前廣泛應用於網路傳輸、金融交易和區塊鏈技術的安全機制曝險。

量子運算的理論基礎可以追溯至 1980 年代，由 David Deutsch [5][6] 和 Richard Feynman[7]等人提出。隨後，Peter Shor 於 1994 年提出了量子因數分解演算法 (Shor's Algorithm) [15]，證明量子電腦能夠在多項式時間 (Polynomial Time) 內完成大質因數分解與離散對數求解，這威脅到了目前廣泛應用的 RSA、ECC（橢圓曲線密碼學）等公鑰加密機制。這意味著，透過量子運算，公開金鑰可被逆推出私密金鑰，從而威脅到基於離散對數與大數因數分解難題的現行密碼系統，包括比特幣在內，一旦攻擊者成功計算出某個地址的私密金鑰，便能竊取該地址內的資產。另一方面，Lov Grover 於 1996 年提出的 Grover 演算法[8]可針對非結構化資料的窮舉搜尋問題提供平方加速，使得如 SHA-256 這類的雜湊函數安全性受到一定程度的影響，顯示出量子電腦在破解雜湊函數方面的潛在威脅。雖然相較於 Shor 演算法[15]，其對比特幣系統的影響較小，但仍可能

削弱比特幣挖礦的安全性，進一步改變其經濟與安全機制。根據現有研究，當量子運算能力達到約 2000 個以上的量子位元 (qubits) 且具備高容錯能力時，比特幣所採用的 ECDSA 簽章將不再安全。Proos 和 Zalka [12] 於 2003 年分析指出，在量子電腦上，約 1000 個量子位元即可破解 160 位元的 ECDSA，而分解安全性相當於 1024 位元 RSA 模數的加密系統則需約 2000 個量子位元。

在硬體發展方面，Google 公司於 2019 年宣布實現了量子霸權 (Quantum Supremacy) [2]，其 53 量子位元的 「Sycamore」處理器在 200 秒內完成了一個傳統超級電腦需耗時約一萬年的運算任務。Google 的量子人工智慧實驗室 (Google Quantum AI) 於 2024 年 12 月宣布[17] 其擁有 105 量子位元的「Willow」處理器，在計算能力上取得了顯著突破，它在不到五分鐘的時間內完成了一項超級電腦需要花 10^{25} 年才能完成的計算。IBM 公司於 2021 推出了擁有 127 量子位元的「Eagle」處理器，於 2022 年推出了具有 433 量子位元的「Osprey」處理器，於 2023 年發表首款擁有 1,121 個超導量子位元，呈蜂窩狀排列的「Condor」處理器，並預計於 2025 年推出擁有 1,386 量子位元的多晶片處理器「Kookaburra」[25]。Rigetti Computing 公司於 2024 年 12 月推出其 84 量子位元「Ankaa-3 系統」[21] ，其提供雲端量子運算服務，並預計於 2025 年第一季於 Amazon Braket 和 Microsoft Azure 上架。IonQ 公司於 2022 年推出了 36 量子位元的單核心量子處理器「Forte」，量子位元和閘的配置可以根據使用者需求進行定制 [22]。Quantinuum 公司於 2024 年 6 月推出了具有 56 量子位元的量子電腦。美國麻省理工學院 (MIT) 等機構也在光學量子運算與超導量子運算方面取得突破，2024 年麻省理工學院的研究人員開發了一種在超導量子處理器上產生合成電磁場的技術，該團隊在一個包含 16 個量子位元的處理器上展示了這項技術 [23]。全球量子運算競賽進入白熱化階段。雖然目前的量子電腦仍然受到量子位元數量不足、量子錯誤率高、量子糾錯技術尚未成熟等問題的限制，但未來數十年內，量子運算能力的提升極可能會對傳統密碼學帶來實質性的衝擊。

3.2 比特幣系統的安全性現狀

目前比特幣的安全性依賴於兩大核心密碼學技術：橢圓曲線數位簽章演算法 (ECDSA) 與 SHA-256 安全雜湊函數。在當前的傳統運算環境下，攻擊者要想從公開的比特幣公鑰推導出對應的私鑰，幾乎是不可能的，但這兩種技術在量子運算環境下可能面臨威脅。本小節從比特幣系統「簽章機制的瓦解」與「Proof-of-Work (PoW) 難度的下降」來探討比特幣系統的安全性現狀。

3.2.1 簽章機制的瓦解

若量子運算能由公開的公鑰推導出私鑰，那簽章機制將被瓦解，就好比銀行存摺的

私章被盜取或複製，帳戶內的資產隨時可被盜領。目前的比特幣交易模式要求用戶在發送資金時，必須使用私鑰對交易簽章，這使得交易驗證依賴於 ECDSA 的安全性。ECDSA 的安全性植基於橢圓曲線離散對數問題 (ECDLP) 的計算困難度，目前在傳統電腦上需要指數時間才能求解，這使得比特幣地址的私鑰幾乎不可能被暴力破解。然而，Shor 演算法[15]可以在多項式時間內解決 ECDLP，一旦足夠強大的量子電腦問世，攻擊者便能直接從公開的比特幣公鑰推導出私鑰，從而竊取資產。這對於早期比特幣交易使用的 P2PK (Pay-to-Public-Key) 地址特別危險，因為這類地址的公鑰在交易時會直接暴露，一旦量子電腦能力足夠強大，這些資金將面臨極大的風險。

智能合約與去中心化金融 (DeFi) 也是比特幣安全性的重要考量點。雖然比特幣的智能合約功能相對以太坊等區塊鏈較為有限，但其 Bitcoin Script 機制仍允許多重簽章與時間鎖定交易等高級功能。如果量子電腦能夠破解這些智能合約的密碼學基礎，那麼比特幣上的複雜交易將面臨更大的風險。

3.2.2 PoW 難度的下降

比特幣的 PoW 挖礦機制依賴於 SHA-256 進行雜湊運算，以確保區塊鏈的不可篡改性。理論上，SHA-256 具有 2^{256} 的計算複雜度會使得對其進行暴力破解是極為困難的。然而，Grover [8] 演算法能對 SHA-256 進行平方根加速攻擊，將雜湊函數的搜尋空間從 2^{256} 降至 2^{128}，雖然這仍然需要極為龐大的運算資源，但若未來量子運算技術持續突破，挖礦難度可能會大幅降低，導致比特幣區塊鏈的安全性受影響。此外，量子電腦的出現可能會顛覆目前的挖礦競爭模式，導致網路算力過度集中於擁有量子技術的實體，破壞比特幣的去中心化特性。

3.2.3 51%攻擊

比特幣的安全挑戰不僅來自於密碼學技術本身，還包括挖礦過程的中心化問題。在比特幣網路的初期，任何個人都可以透過 CPU 或 GPU 進行挖礦並參與區塊驗證，但隨著挖礦設備的普及，挖礦的算力已逐漸集中在少數大型礦池手中。當前，全球前幾大礦池已掌握了比特幣網路超過 50%的算力，這使得比特幣網路可能面臨 51%攻擊的風險，即若單一實體或聯盟掌握超過 50%的算力，則可對區塊鏈進行重組，甚至雙重支付攻擊。雖然這種攻擊的成本極高，並且短期內不太可能發生，但其存在性仍然對比特幣的去中心化特性構成威脅。

51% 攻擊是指當某個個人或組織獲得超過 51% 的算力控制權時，他們可以影響區塊鏈的交易驗證與出塊機制，從而破壞工作量證明 (Proof-of-Work, PoW) 區塊鏈的安全性。攻擊者可以修改交易歷史，使已發出的交易變成「未發送」，進而進行雙重支付，等

於「用同一筆錢花兩次」；可以選擇不將某些交易納入區塊，造成交易延遲甚至完全無法執行；也可以強制讓區塊鏈重組 (Reorg)，創建更長的「惡意鏈」，使先前的合法交易無效，影響交易最終性 (Finality)；也可以排擠其他礦工，使自己成為唯一的出塊者，獲取所有區塊獎勵。

3.3 防禦與挑戰

3.3.1 Post-Quantum Cryptography

為了應對量子運算的威脅，全球密碼學界和資訊安全專家積極投入研究能夠抵抗量子攻擊的後量子密碼學 (Post-Quantum Cryptography, PQC)。美國國家標準暨技術研究院 (National Institute of Standards and Technology, NIST) 於 2016 年啟動了「後量子密碼學標準化計畫」，廣徵英雄帖[19]，當時收到來自 25 個國家所提交的 82 個演算法，之後陸續進行了 3 輪淘汰賽，直到 2022 年才選出 4 個候選演算法來進行標準化作業，包含：CRYSTALS-Kyber（公鑰加密與密鑰交換）、CRYSTALS-Dilithium（數位簽章）、FALCON（數位簽章）、SPHINCS+（基於雜湊函數的數位簽章）。NIST 於 2024 年 8 月公佈了 3 個標準 [20]，包含：FIPS-203 (Module-Lattice-Based Key-Encapsulation Mechanism Standard, ML-KEM，植基於 CRYSTALS-Kyber)、FIPS 204 (Module-Lattice-Based Digital Signature Standard, ML-DSA，植基於 CRYSTALS-Dilithium)、FIPS 205 (Stateless Hash-Based Digital Signature Standard, SLH-DSA，植基於 SPHINCS+)，並預計近期內會推出植基於 FALCON 的 FIPS 206。這些演算法被設計為能夠抵擋量子電腦的計算能力，確保未來的加密通訊與數位簽章仍然安全。

比特幣網路的簽章機制可陸續轉換為後量子數位簽章機制，在過渡時期可採用傳統密碼學與後量子密碼學混合的簽章機制，確保在量子電腦尚未成熟時仍保有較高的兼容性與安全性。目前比特幣地址是基於公鑰的雜湊值（例如 P2PKH、P2SH)，可升級為能抵擋量子攻擊的地址格式，確保比特幣資產不受量子電腦攻擊影響。若比特幣網路能在量子電腦變得足夠強大之前完成後量子密碼學的轉換，那麼比特幣的安全性將得以延續，並能應對量子時代的挑戰。

3.3.2 保護公鑰的比特幣地址形式

中本聰在 2009 年 1 月 3 日挖出創世區塊後，於 1 月 12 日向比特幣開發者 Hal Finney 以 P2PK (Pay to PubKey) 的方式轉帳 10 枚比特幣 [18]。然而，值得注意的是，P2PK 在交易過程中會直接暴露公鑰，這使得它們在量子時代將面臨極高的風險。其後，比特幣的地址類型經歷了多次演進，目前主要有四種：Legacy (P2PKH)、Nested SegWit (P2SH)、

Native SegWit (Bech32 / P2WPKH)、Taproot (Bech32m / P2TR)。

Legacy (Pay to PubKey Hash，縮寫為 P2PKH) 是格式為 1 開頭的地址，以公鑰的雜湊值加入版本前綴再經過 Base58 編碼處理後當作接收地址，是最傳統的地址格式，自比特幣建立之初就存在。P2PKH 地址透過 SHA-256 和 RIPEMD-160 雜湊函數對公鑰進行加密，公鑰並沒有對外公開，直到要花費未使用交易輸出 (UTXO) 時才會公開公鑰讓別人驗證簽章的有效性。和 P2PK 相比，P2PKH 大大提高了安全性。然而，一旦花費 UTXO 的轉帳被廣播並記錄到區塊鏈，其公鑰就會暴露，這使得曾經轉帳出去但仍存在尚未轉移資金的地址仍然面臨潛在風險。

支付到腳本雜湊 (Pay-to-Script-Hash，縮寫為 P2SH) 是格式為 3 開頭的地址，它是比特幣改進提案 BIP 16 於 2012 年引入的一種比特幣交易方式，允許多重簽章和更複雜的智能合約，提供更靈活的支付條件，類似信託的概念，先支付給信託，當條件滿足時可以把錢領出。它把複雜的交易腳本寫入地址中，與傳統的 P2PKH 地址相比，P2SH 是鎖定一個「腳本的雜湊值」，而不是具體的公鑰。當要花費 P2SH 鎖定的資金時，花費必須提供解鎖腳本和滿足腳本條件的簽章。

原先比特幣區塊的容量上限為 1MB，能容納的交易數量有限，外加大約每 10 分鐘才產生一個新的區塊，容易導致交易壅塞、交易速度緩慢。SegWit (隔離見證，Segregated Witness) 是比特幣在 2017 年 8 月 (BIP 141) 實施的一項重大協議升級，主要目標是提升交易速度、降低交易手續費。Segwit 可將比特幣區塊中的所有簽章資料移至末端，將所有交易的簽章集中在一起，這樣可以在相同的區塊容量中容納更多筆交易，同時保有比特幣區塊鏈的安全。而且每個區塊能提供的交易數量增加後，能夠降低每筆交易的交易成本。當 SegWit 被引入時，有了新的比特幣地址格式：格式為 bc1q 開頭 Native SegWit (P2WPKH)。為了確保能兼容舊版錢包，比特幣社群使用 P2SH 來封裝 SegWit 交易，稱為 Nested SegWit (P2SH-P2WPKH)，格式和 P2SH 一樣為 3 開頭，使 SegWit 地址可以與不支援 SegWit 的舊版錢包兼容。

Taproot (Pay-to-Taproot, P2TR) 引入於 2021 年比特幣的 BIP 341 改進提案，P2TR 交易支付的對象和 P2SH 一樣是一個腳本雜湊 (Script Hash)，但它使用 Merklized Abstract Syntax Trees (MASTs) [9]，MASTs 結合了 Merkle Trees [10] 和 Abstract Syntax Trees (ASTs) 的特性，將複雜腳本隱藏在根腳本中，只有當支付條件觸發時，才會公開腳本，否則外部無法得知具體腳本內容。此外，P2TR 引入了 Schnorr 簽章，並且能夠將多重簽章和複雜條件聚合成單一簽章。

以上幾種現行的比特幣地址皆能保護公鑰不被暴露。然而，比特幣區塊鏈上儲存著大量未使用交易輸出，這些 UTXO 可能對應於早期使用 P2PK 地址的比特幣，一旦量子電腦足夠強大，這些 UTXO 可能成為攻擊者的首要目標。

肆、結論

比特幣與量子時代的對決：您的資產還安全嗎？答案是肯定的！比特幣目前仍是高度安全的數位資產，以下是主要原因：

(1) 量子電腦尚未足夠強大：量子電腦須達 2,000 個以上量子位元 (qubits) 且具備高容錯能力，才可能對現行加密機制構成威脅。目前量子電腦的技術尚未超過 1,400 個量子位元，且錯誤率仍高，量子糾錯技術尚未成熟。

(2) 後量子密碼學的發展與轉換：密碼學界已積極研究後量子加密技術 (PQC)，並由美國國家標準暨技術研究院 (NIST) 進行標準化，未來比特幣網路可逐步升級至後量子演算法，以抵禦量子電腦的攻擊。

(3) 現行的比特幣地址格式不會暴露公鑰：量子運算的主要威脅在於由公鑰推導出私鑰，目前的比特幣地址格式不會暴露公鑰，除非曾經轉帳出去。

如何保護您的比特幣資產？即使比特幣本身高度安全，仍建議採取適當的防護措施：

(1) 選擇正規交易所，避免詐騙：親自登入交易所官網進行交易，切勿透過社群、代買、投資群組等方式購買，以免遭詐騙。

(2) 將比特幣存放於冷錢包：交易所可能因駭客攻擊或經營問題倒閉，因此應在購買後立即轉移到個人冷錢包，避免資產受損。

(3) 使用「一次性」地址，降低風險：接收比特幣時無需公開公鑰，但轉帳時需公開公鑰進行簽章驗證，因此建議使用一次性地址（用過即棄），避免私鑰推導風險。

(4) 謹慎評估投資風險：比特幣價格波動劇烈，投資風險高，進場時間不同將影響投資績效，而且過去績效不代表未來收益，購買前請務必評估個人風險承受能力。

整體而言，比特幣依然是高度安全的數位資產，但量子運算發展仍需關注，投資人應搭配適當的安全措施，以確保資產穩定與安全。

[誌謝] 本研究由國家科學及技術委員會所支持，計畫編號：NSTC 113-2635-E-006-001 -。

參考文獻

[1] B. Adam. “Hashcash-a denial of service counter-measure,” (2002).

[2] F. Arute, et al. “Quantum supremacy using a programmable superconducting processor,“ *Nature* 574.7779 (2019): 505-510.

[3] D. Chaum, A. Fiat, and M. Naor. “Untraceable electronic cash,” *Advances in Cryptology—CRYPTO’88: Proceedings 8*. Springer New York, 1990.

[4] D. Chaum, and S. Brands. “'Minting'electronic cash,” *IEEE spectrum* 34.2 (1997): 30-34.

[5] D. Deutsch. “Quantum theory, the Church-Turing principle and the universal quantum computer,” *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences* 400.1818 (1985): 97-117.

[6] D. Deutsch, and R. Jozsa. “Rapid solution of problems by quantum computation,” *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (1992): 553-558.

[7] R. P. Feynman “Quantum mechanical computers,” *Found. Phys.* 16.6 (1986): 507-532.

[8] L. K. Grover “A fast quantum mechanical algorithm for database search,” *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*. 1996.

[9] R. Jeremy, M. Naik, and N. Subramanian. “Merkelized abstract syntax trees,” *XP055624837, Dec* 16.3 (2014).

[10] R. Merkle. “Protocols for public key cryptosystems.” *In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122–133. IEEE Computer Society*, 1980.

[11] S. Nick. ”Bit Gold,” *Recuperado de https://nakamotoinstitute.org/bit-gold/TVer página* (2005): 251-260.

[12] J. Proos, C. Zalka. “Shor's discrete logarithm quantum algorithm for elliptic curves." arXiv preprint quant-ph/0301141 (2003).

[13] N. Satoshi.“Bitcoin: A peer-to-peer electronic cash system,” (2008).

[14] N. Satoshi, and A. Bitcoin. “A peer-to-peer electronic cash system,” Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf 4.2 (2008): 15.

[15] P. W. Shor. “Algorithms for quantum computation: Discrete logarithms and factoring,” *Proceedings 35th annual symposium on foundations of computer science. IEEE*, 1994.

[16] D. Wei. “B-money,” Nov. 1998. https://bitcoinstan.io/prehistory/doc/1998_3.pdf

[17] https://blog.google/technology/research/google-willow-quantum-chip/

[18] https://blockstream.info/tx/f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16?expand

[19] https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals

[20] https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms

[21] https://investors.rigetti.com/news-releases/news-release-details/rigetti-computing-launches-84-qubit-ankaatm-3-system-achieves

[22] https://ionq.com/quantum-systems/forte

[23] https://news.mit.edu/2024/quantum-simulator-could-uncover-materials-high-performance-electronics-1030

[24] https://www.blockchain.com/explorer.
[25] https://www.ibm.com/quantum/technology
[26] https://www.whitehouse.gov/fact-sheets/2025/03/fact-sheet-president-donald-j-trump-establishes-the-strategic-bitcoin-reserve-and-u-s-digital-asset-stockpile/

[作者簡介]

畢業於國立臺灣大學電機工程學系博士班，目前服務於國立成功大學工學院工程管理碩士在職專班，為教育部資訊安全師資增聘計畫之專任教師，專注於資訊安全的教育及各項資訊安全相關研究計畫的推動。其研究專長包括應用密碼學、資訊安全與網路安全，涵蓋行動通訊、智慧電網、遠距醫療、智慧城市及物聯網等領域的傳輸安全、隱私保護與身份認證議題。