OK COMPUTER

OK Computer, Radiohead

Please could you stop the noise? I'm trying to get some rest
From all the unborn chicken voices in my head

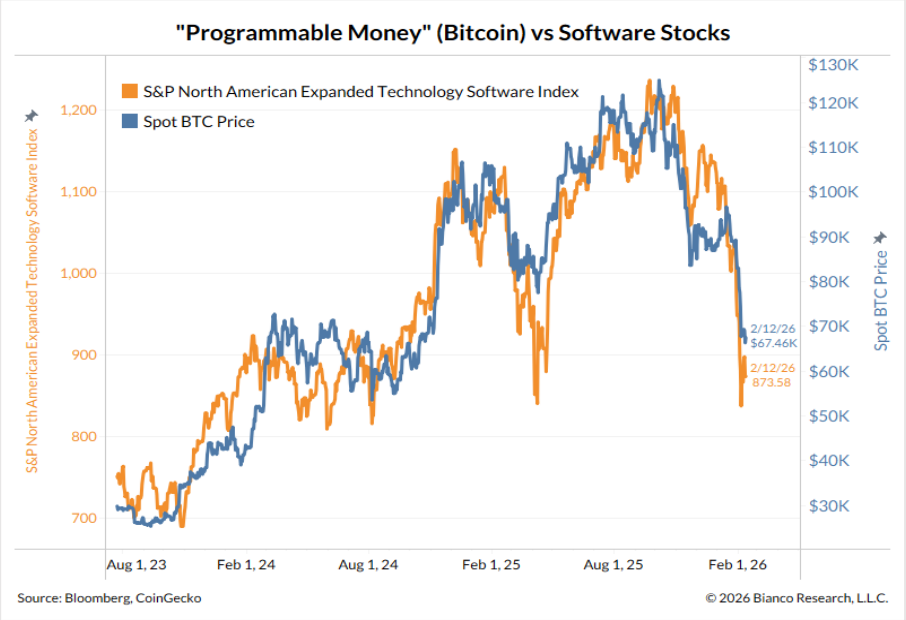
What's that? (I may be paranoid, but not an android)
What's that? (I may be paranoid, but not an android)

Paranoid Android - OK Computer - Radiohead, 1997

Nel 1997 i Radiohead pubblicavano *OK Computer*, un album che catturava l'ansia di un mondo in cui la tecnologia avanza più velocemente della nostra capacità di controllarla. Quasi trent'anni dopo, il titolo suona come una domanda rivolta direttamente a Bitcoin: sarà il computer - quello quantistico - a mettere in crisi il sistema? **Per oltre quindici anni, il rischio che i computer quantistici potessero violare la sicurezza di Bitcoin è stato liquidato come fantascienza: oggi non è più così.**

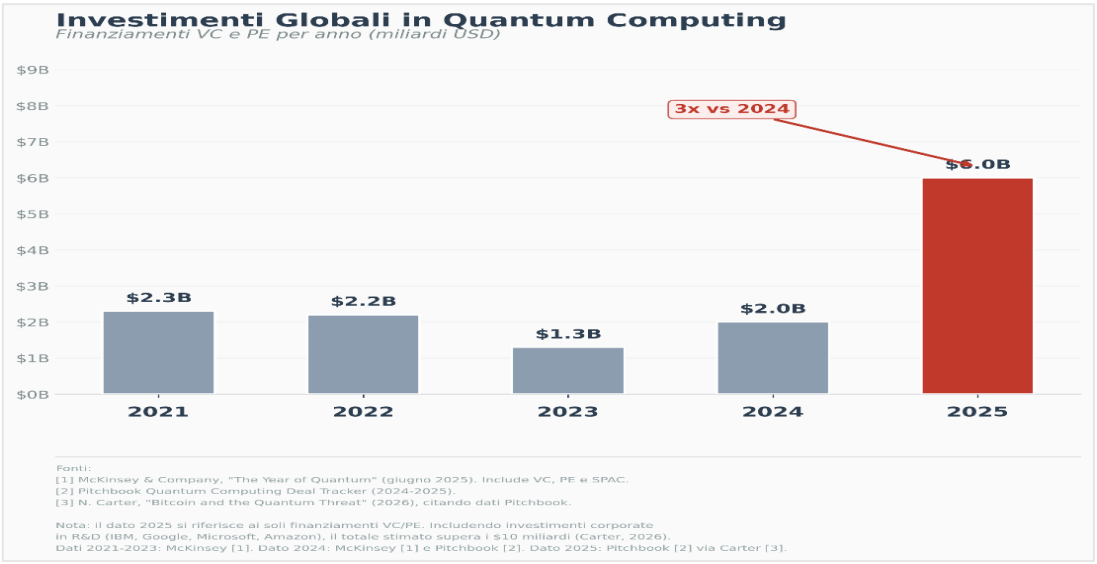
Bitcoin, nel corso della sua storia, ha mostrato correlazioni variabili con asset diversi - dall'oro ai titoli tecnologici, dalla liquidità globale alle materie prime. Un dato recente, da interpretare con cautela ma da non ignorare, merita attenzione: negli ultimi due anni Bitcoin ha mostrato una correlazione particolarmente marcata con i titoli del settore

software americano (evidenza di seguito). Alcuni operatori di mercato ne danno una lettura suggestiva: Bitcoin come *programmable money*, un asset il cui valore è inseparabile dall'integrità del suo codice. Senza sposare necessariamente questa tesi, vale la pena esaminare cosa accadrebbe se una minaccia credibile a quel codice si materializzasse.



E la minaccia si sta concretizzando, perlomeno a giudicare dalla dimensione degli investimenti nel settore. Nel solo 2025, i finanziamenti privati nel settore dei computer quantistici hanno superato i 6 miliardi di dollari - il triplo rispetto all'anno prima e più di quanto investito nei quattro anni precedenti messi insieme.

Con lo scritto odierno ci proponiamo di analizzare il rischio che il quantum computing rappresenta per Bitcoin, presentando le ragioni di chi lo ritiene imminente e di chi lo considera gestibile e lontano e, infine, riportando un framework quantitativo per valutarne l'impatto sul prezzo.



Il lucchetto di Bitcoin

Per comprendere il rischio quantum, è necessario partire da un concetto fondamentale: Bitcoin funziona grazie a un meccanismo crittografico che possiamo pensare come un lucchetto matematico. Ogni wallet di Bitcoin è protetto da una coppia di chiavi: una chiave pubblica (l'indirizzo a cui si ricevono fondi, visibile a tutti) e una chiave privata (la "combinazione" segreta che permette di spendere quei fondi).

La sicurezza dell'intero sistema si basa su un'asimmetria: dalla chiave privata si può facilmente ricavare la chiave pubblica, ma il percorso inverso - risalire dalla chiave pubblica a quella privata - è ritenuto impossibile con i computer attuali. Anche il più potente supercomputer del mondo impiegherebbe miliardi di anni per tentare tutte le combinazioni possibili.

Nic Carter, partner di Castle Island Ventures e una delle voci più autorevoli nel settore che ha approfondito estensivamente il tema quantum, usa un'analogia efficace: immaginate un'auto su una pista circolare. Il guidatore preme l'acceleratore un certo numero di volte, compiendo numerosi giri, e parcheggia l'auto in un punto preciso. Guardando dove è parcheggiata l'auto, risulta praticamente impossibile capire quante volte ha premuto l'acceleratore. L'unico modo sarebbe rimettersi alla guida e ripetere il processo dall'inizio, provando ogni possibilità - un'operazione che richiederebbe un tempo inimmaginabile.

I computer quantistici potrebbero cambiare questa equazione. A differenza dei computer tradizionali, che elaborano un calcolo alla volta, i computer quantistici sfruttano le proprietà della meccanica quantistica per esplorare un numero enorme di possibilità simultaneamente. In termini pratici, un computer quantistico sufficientemente potente potrebbe essere in grado di "aprire il lucchetto" di Bitcoin -

COSA SONO I COMPUTER QUANTISTICI?

I computer tradizionali elaborano informazioni usando "**bit**" che possono essere solo 0 oppure 1 - una "semplificazione" della realtà. Il mondo in cui viviamo, però, è intrinsecamente più complesso: a livello subatomico, le particelle non si comportano in modo binario. I computer quantistici utilizzano "**qubit**" che, sfruttando queste proprietà della fisica, possono trovarsi in entrambi gli stati contemporaneamente. In un certo senso, sono computer che usano le regole dell'universo così come sono davvero, anziché' semplificarle. Questa proprietà li rende radicalmente diversi - non più "veloci" in senso generico, ma capaci di risolvere certi tipi di problemi matematici estremamente complessi in tempi drasticamente inferiori.

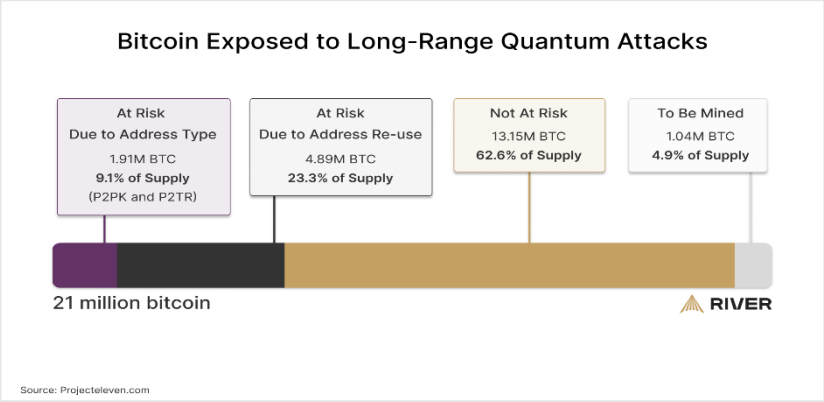
cioè risalire dalla chiave pubblica a quella privata - in un tempo ragionevole.

Quantificare il rischio

Non tutti i bitcoin sono ugualmente esposti alla minaccia quantum. La vulnerabilità dipende dal tipo di portafoglio (wallet) utilizzato e da come è stato gestito nel tempo. **Il punto chiave è la visibilità della chiave pubblica**. Come abbiamo discusso, un computer quantistico potrebbe teoricamente ricavare la chiave privata partendo da quella pubblica. Ma non tutti i wallet espongono la chiave pubblica allo stesso modo. I portafogli più a rischio sono quelli che rendono la chiave pubblica direttamente visibile sulla blockchain. Si tratta principalmente di tre categorie:

- **Wallet dei primi anni di Bitcoin**: nei primi anni di vita della rete, l'indirizzo stesso era la chiave pubblica. Circa 1.7 milioni di BTC si trovano in questi portafogli.
- **Wallet riutilizzati**: ogni volta che si effettua una transazione da un portafoglio, la chiave pubblica viene esposta. Chi ha riutilizzato lo stesso indirizzo più volte ha involontariamente reso visibile la propria chiave pubblica. Circa 4.8 milioni di BTC si trovano in questa condizione.
- **Wallet "Taproot"**: introdotti con un aggiornamento della rete nel 2021, utilizzano un formato che, per ragioni tecniche, espone anch'esso la chiave pubblica. Rappresentano una quota minore ma in crescita (circa 185,000 BTC).

In totale, si stima che circa il 20-30% dell'intera offerta di Bitcoin - tra i 6 e i 7 milioni di BTC - abbia la chiave pubblica esposta e sia potenzialmente vulnerabile ad un attacco quantistico. I wallet più moderni, che utilizzano formati dove la chiave pubblica è nascosta dietro un ulteriore livello di protezione (un "*hash*"), non sono a rischio da questo tipo di attacco - almeno finché non vengono utilizzati per effettuare una transazione. **Un elemento particolarmente delicato riguarda i bitcoin considerati "persi"**: portafogli i cui proprietari hanno smarrito le chiavi di accesso, o che appartengono a persone decedute. River stima che circa 1.6 milioni di Bitcoin rientrino in questa categoria, a cui si



aggiungono i circa 968,000 BTC attribuiti a Satoshi Nakamoto. Questi fondi non potranno mai essere migrati verso portafogli più sicuri, rappresentando una vulnerabilita' permanente del sistema.

Bear case: perché il rischio è serio

Prima di tutto, un chiarimento importante: la minaccia dei computer quantistici non riguarda solo Bitcoin. La crittografia che protegge BTC è della "stessa famiglia" di quella che protegge le comunicazioni su WhatsApp, le transazioni bancarie online, le cartelle cliniche digitali, i sistemi di difesa militare, le e-mail aziendali ecc. In un mondo in cui un computer quantistico sufficientemente potente diventasse realtà, tutto ciò che oggi consideriamo "sicuro" perché' crittografato sarebbe potenzialmente a rischio. Bitcoin, però, ha una vulnerabilità aggiuntiva rispetto a questi sistemi. Se le banche possono aggiornare i propri server in settimane, **Bitcoin no: è un sistema**

LO SCONTRO USA-CINA E LE TENSIONI IN CORSO

La tecnologia non è uno strumento della competizione geopolitica: è la competizione. Il quantum computing ne è il caso limite. Chi arriva primo ottiene la capacità di rompere ogni crittografia esistente, dalle transazioni bancarie alle comunicazioni militari. La Cina ha dimostrato la supremazia quantistica con lo Zuchongzhi 3.0 (105 qubit), che esegue calcoli un milione di miliardi di volte più velocemente del supercomputer più potente al mondo. Pechino ha investito oltre 15 miliardi di dollari nel settore, il quadruplo degli USA, e il 15° Piano Quinquennale lo include tra le priorità strategiche. Gli Stati Uniti mantengono il vantaggio sulla correzione degli errori (Google, IBM, Quantinuum) e sui brevetti chiave, ma la supply chain è fragile e dipendente dall'estero.

Il Q-Day, ovvero il momento in cui un computer quantistico romperà la crittografia RSA, è atteso negli anni 2030, ma l'algoritmo ibrido JVG (annunciato il 2 marzo 2026 dall'AQTI) potrebbe comprimere drasticamente la timeline. Il rischio immediato è l' ***harvest now, decrypt later***: attori statali raccolgono comunicazioni crittografate oggi per decifrarle domani. Citibank stima che un singolo attacco quantistico al sistema Fedwire metterebbe a rischio circa 2-3,3 trilioni di PIL americano. Solo il 5% delle organizzazioni ha implementato protezioni post-quantistiche (DigiCert, 2025).

Le tensioni attuali confermano il paradosso del decoupling documentato dagli autori: le sanzioni non frenano la Cina, la accelerano. Trump ha sanzionato quasi 20 entità cinesi per AI e quantum nel gennaio 2026, ma l'effetto, come per i chip Nvidia e per DeepSeek, sarà un nuovo "momento Sputnik" che spingerà Pechino verso l'autonomia completa. Intanto, il conflitto iraniano è una miniera d'oro per il "harvest now": ogni comunicazione militare e diplomatica trasmessa in queste settimane con crittografia classica è potenzialmente immagazzinata per la decrittazione futura. Il decoupling tecnologico è irreversibile e reciproco e nel quantum, chi perde il passo perde tutto.

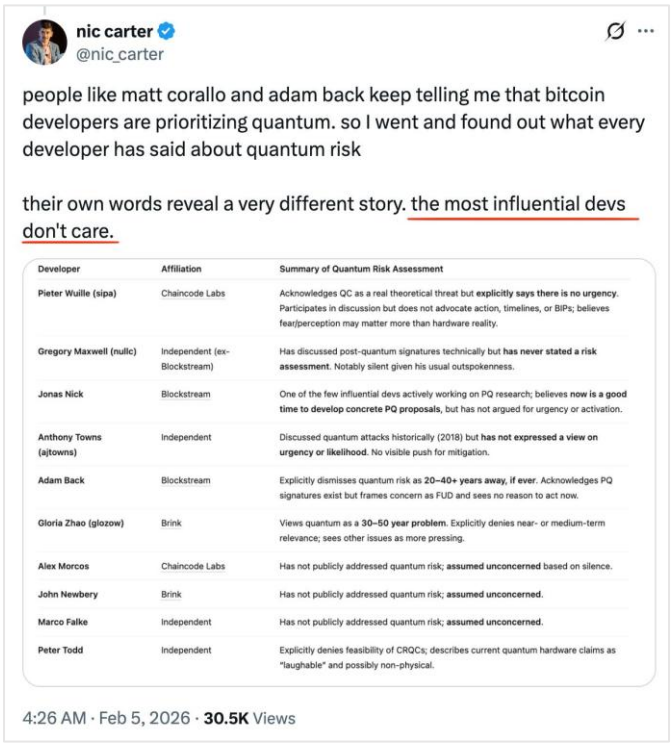
(Cfr. Balestrieri, F. e Balestrieri, L., *Tecnologie dell'impero*, Luiss, 2024)

decentralizzato, senza un'autorità centrale che può decidere e implementare un cambiamento rapidamente. È proprio questa caratteristica - che in condizioni normali rappresenta un elemento di resilienza - a diventare il punto debole quando "il tempo stringe".

Il Quantum accelera

La potenza dei computer quantistici sta crescendo a un ritmo superiore alle attese. Un'analisi di Capriole Investments (gestore attivo nel mondo degli asset digitali con strategie sistematiche), basata sulle stime di fisici quantistici, organismi di sicurezza informatica e delle principali aziende del settore, stima che la probabilità che un computer quantistico sia in grado di violare la crittografia di Bitcoin (il cosiddetto "*Q-Day*") sarà del 60% entro il 2030 e dell'80% entro il 2031.

Nic Carter, che ritiene il rischio concreto e abbastanza imminente, osserva che uno dei segnali più eloquenti di questo fenomeno e dei rischi ad esso connessi non proviene dalle aziende, ma dai governi. Gli Stati Uniti, il Regno Unito, l'Unione Europea e la Cina sono giunti in maniera indipendente ad una timeline simile: abbandonare gli attuali standard crittografici entro il 2030 e completare la transizione verso nuovi sistemi entro il 2035. Il National Institute of Standards and Technology (NIST) statunitense ha pubblicato le prime specifiche per algoritmi crittografici resistenti al quantum, suggerendo appunto la dismissione degli algoritmi attuali entro il 2030.



Bitcoin è troppo lento per aggiornarsi

Sempre Carter nota che il problema non è solo la velocità con cui avanza il quantum computing - è la lentezza con cui Bitcoin può adattarsi. I precedenti non sono incoraggianti: in dieci anni, Bitcoin ha completato solo due aggiornamenti significativi. Il primo, proposto nel 2015, è stato adottato solo nel 2017. Il secondo, concepito nel 2018, è stato attivato alla fine

del 2021. Capriole stima che il tempo necessario per aggiornare il codice di Bitcoin e migrare la maggioranza degli utenti attivi verso portafogli sicuri sia di circa 2 anni in uno scenario realistico - con possibilità che si estenda a 3 anni o più. È un'operazione di una complessità rilevante per una rete decentralizzata, dove ogni modifica al protocollo deve passare attraverso un processo di proposta, dibattito, raggiungimento del consenso tra sviluppatori, test, deployment e infine adozione da parte di minatori, nodi e utenti.

Un aspetto particolarmente preoccupante, evidenziato sia da Carter che da Capriole, è **l'atteggiamento di parte della comunità degli sviluppatori**. Molti developer influenti di Bitcoin non considerano ancora il rischio quantum come una priorità. Carter propone un esercizio utile per capire l'urgenza: ragionare a ritroso. Se Q-Day fosse nel 2033 - una stima conservativa, secondo lui - quanto tempo servirebbe per prepararsi? Almeno cinque anni per migrare tutti gli utenti verso portafogli sicuri. Tre anni per raggiungere il consenso della comunità su come procedere. Un anno per testare il nuovo codice. Totale di nove anni: la community è già in ritardo.

La risposta delle istituzioni

La pressione non è solo teorica. Nel corso degli ultimi mesi, diversi allocatori istituzionali di rilievo hanno iniziato a prendere posizione pubblica sul rischio quantum:

- **Jefferies** (gennaio 2026): Christopher Wood, responsabile globale della strategia azionaria della banca di investimento americana, ha rimosso l'allocazione del 10% a Bitcoin dal proprio portafoglio modello, riallocandone metà in oro fisico e metà in titoli minerari auriferi. Wood, che era stato tra i primi sostenitori istituzionali di Bitcoin nel 2020, ha definito il rischio quantum come "potenzialmente esistenziale" per la narrativa di Bitcoin come riserva di valore.
- **BlackRock** (maggio 2025): il più grande emittente di ETF crypto al mondo ha inserito il quantum computing tra i fattori di rischio nel prospetto del proprio ETF spot su Bitcoin
- **Van Eck** (novembre 2025): il CEO dell'asset manager, particolarmente attivo nel mondo degli asset digitali, ha dichiarato che la società "si allontanerà da Bitcoin se la tesi verrà *fondamentalmente compromessa*, citando esplicitamente le preoccupazioni sulla crittografia legate al quantum.

Bull case: perché il rischio è gestibile

Timeline più lunghe

Non tutti, nella comunità accademica e crittografica, concordano con le stime più pessimistiche. Justin Thaler, professore di informatica alla Georgetown University ed attivo nel campo della crittografia, offre un'analisi dettagliata del perché molti annunci nel settore quantum, a suo avviso, siano fuorvianti. Thaler osserva che le aziende del settore fanno un uso disinvolto di termini tecnici che possono ingannare anche osservatori sofisticati. Il numero di "qubit" annunciato nei comunicati stampa è spesso riferito a tecnologie che non sono in grado di eseguire il tipo di calcolo necessario per violare la crittografia di Bitcoin. In termini più semplici: il divario tra i computer quantistici disponibili oggi e quelli necessari per rappresentare una minaccia reale è ancora enorme. Attualmente i migliori sistemi dispongono di circa 1,000 qubit fisici e poche decine di qubit logici. **Per violare la crittografia di Bitcoin servirebbero diverse migliaia di qubit logici stabili, ciascuno dei quali richiede centinaia o migliaia di qubit fisici per funzionare correttamente**. Siamo ancora a diversi ordini di grandezza di distanza. Come riporta River, uno studio del 2022 dell'Universita' di Sussex ha stimato che sarebbero necessari tra i 13 e i 300 milioni di qubit per violare la crittografia di Bitcoin in un arco di 1-8 ore. Anche se stime piu' recenti hanno ridotto significativamente questi numeri, il consenso accademico - come emerge dal sondaggio del Global Risk Institute citato da Nic Carter - colloca la probabilita' di un computer quantistico in grado di rompere la crittografia intorno al 2035-2040, e non prima. Thaler sintetizza così: "*Affermare che un computer quantistico capace di violare la crittografia di Bitcoin sarà disponibile entro 5 anni non è supportato dai progressi pubblicamente noti. Anche 10 anni rimane una stima ambiziosa*."

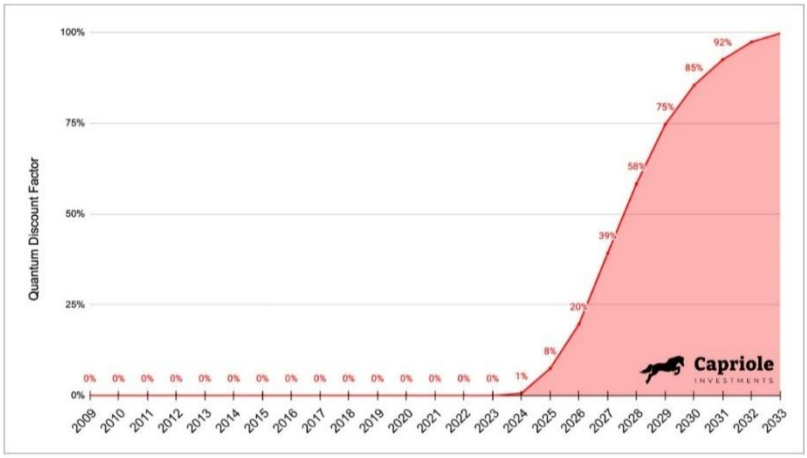
Pareri discordanti

Una voce particolarmente netta nel ridimensionare il rischio arriva dall'interno della comunità Bitcoin. Giacomo Zucco, tra i massimi esperti di Bitcoin in Italia e figura di riferimento nel panorama tecnico internazionale, in un recente podcast **sostiene che la percezione del rischio quantum sia radicalmente distorta rispetto alla realtà dello stato dell'arte.** La sua tesi parte da una distinzione fondamentale: il quantum computing non è un problema di ingegneria in fase di perfezionamento, come lo era la miniaturizzazione dei chip nel XX secolo. *È una scommessa su un percorso teorico che*

potrebbe non realizzarsi mai. La Legge di Moore - il raddoppio della potenza dei chip ogni due anni - si basava su un fatto ingegneristico osservato e replicabile: maggiori investimenti producevano effettivamente chip più potenti. Il quantum computing non funziona così. Sappiamo in teoria cosa dovrebbe fare un computer quantistico, ma costruire l'hardware necessario per farlo è un problema di natura completamente diversa. **Ma l'elemento forse piu' interessante dell'analisi di Zucco riguarda la capacità di Bitcoin di reagire. A chi obietta che il sistema decentralizzato sia troppo lento per aggiornarsi in tempo, Zucco ribalta l'argomento: la stessa teoria dei giochi che rende Bitcoin resistente ai cambiamenti arbitrari lo renderebbe straordinariamente veloce nell'adottare un aggiornamento quando il patrimonio di tutti verrebbe esposto a un rischio. Ogni singolo utente sarebbe individualmente incentivato ad accettare il cambiamento. In uno scenario di emergenza, Bitcoin potrebbe aggiornarsi addirittura piu' rapidamente di una struttura centralizzata, perché non serve il permesso di nessuno: basta che ciascuno agisca nel proprio interesse.** Zucco - che è laureato in fisica - è anche significativamente piu' critico verso chi ha alimentato il panico sul tema: a suo giudizio, parte del dibattito pubblico sul quantum è stato guidato da figure del mondo finanziario e del trading che ripetono narrazioni della stampa generalista senza una reale comprensione tecnica della materia - contribuendo a un allarme sproporzionato rispetto allo stato effettivo della tecnologia. Su una simile linea di pensiero si colloca **Lyn Alden**, analista macro di riferimento nel panorama Bitcoin, secondo cui il mercato sta prezzando un rischio superiore a quello effettivo. Il pericolo concreto, a suo giudizio, è affrettare l'upgrade: le firme quantum-resistant - le prove crittografiche che autorizzano ogni transazione - sono molto più pesanti in termini di dati, e adottare il metodo sbagliato sarebbe costoso. Meglio attendere che la crittografia post-quantum si stabilizzi.

Quantificare l'incertezza

Tra le analisi esaminate, quella di Capriole Investments **si distingue per il tentativo di tradurre questo rischio in un impatto quantitativo sul prezzo**. La logica del modello proprietario "*Quantum Discount Factor*" è semplice: se esiste una probabilità X% che un computer quantistico violi la crittografia di Bitcoin prima che il sistema venga aggiornato, allora il valore di Bitcoin dovrebbe essere scontato di X%. L'investitore razionale non aspetta la certezza - incorpora la probabilità nel prezzo.



Incrociando le stime di fisici, organismi di sicurezza e le principali aziende del settore, Capriole calcola che questo sconto si aggiri oggi intorno al 20%. Ma il dato più significativo è la traiettoria (evidenza a sinistra): per i primi 17 anni di vita di Bitcoin, il Quantum Discount Factor è stato pari a zero - il rischio che esistesse un computer quantistico in grado di violare la crittografia era nullo. Dal 2025, tutto è cambiato. La curva si è impennata, e senza progressi concreti nell'aggiornamento del protocollo, lo sconto sale al 39% nel 2027, al 58% nel 2028 e al 75% nel 2029. In poco più di un anno, senza azione, il valore di Bitcoin rischierebbe di venire dimezzato.

Ogni anno di inerzia ha un costo esponenziale. Il tempo è il vero asset in gioco.

Approfondimento a cura di **Andrea Accatino**

Lugano, 8 marzo 2026