

8 OTTOBRE 2026 • 14 MIN DI LETTURA • DANILO GIUDICE

Bunker mode e AI: wallet a rischio?

Justin Drake e Vitalik Buterin avvertono che la matematica accelerata dall'intelligenza artificiale potrebbe indebolire la sicurezza di Bitcoin ed Ethereum prima del computer quantistico. In questa analisi MoneyViz spiega che cosa temono, che cosa propongono e perché la parola chiave è «calma». Gli interventi discussi non dimostrano una violazione della crittografia: ragionano su un rischio futuro e sulle possibili precauzioni.



PERCHÉ TI RIGUARDA

- Se tieni le cripto su un indirizzo che **non ha mai inviato nulla**, sei già nella posizione che Drake e Buterin consigliano: **questa settimana non devi fare niente**. Fanno eccezione gli indirizzi Bitcoin Taproot (iniziano con bc1p) e i vecchissimi P2PK, che mostrano la chiave pubblica anche se non hai mai speso
- Se hai somme importanti su indirizzi da cui hai già speso, conviene **pianificare con calma** lo spostamento su un indirizzo nuovo, anche generato dalla stessa seed
- Nessuno ha mostrato un attacco: è uno **scenario da prendere sul serio**, non un'emergenza in corso. Chi ti scrive di «migrare subito» è con ogni probabilità un truffatore
- Il rischio più concreto resta l'errore umano: Buterin dice di aver perso **più soldi in migrazioni sbagliate che in tutti gli attacchi messi insieme**

Valutare con calma se intervenire, in base al tipo di custodia e di indirizzo.

Preferisci leggerlo con calma, o passarlo a chi in famiglia custodisce le cripto? Puoi [scaricare l'articolo in PDF](#).

Durante la Guerra fredda, in Svizzera e non solo, molte famiglie si costruivano un bunker. Non perché fossero sicure che la bomba sarebbe caduta l'indomani, ma perché costruirlo con calma costava poco, e costruirlo all'ultimo momento era impossibile. E nessuno, alla prima sirena di prova, si precipitava giù per le scale al buio.

Il punto di partenza è la minaccia quantistica, ovvero il giorno in cui un computer quantistico sarà abbastanza potente da scardinare la crittografia di Bitcoin ed Ethereum. Drake ha suggerito che, nello scenario peggiore, il problema potrebbe presentarsi prima, e da un'altra parte: non da un laboratorio di fisica, ma dalla matematica accelerata dall'intelligenza artificiale.

Il 7 ottobre 2026 Justin Drake, ricercatore della Ethereum Foundation, ha chiesto al settore di iniziare a preparare, con calma, una «bunker mode». Poche ore dopo Vitalik Buterin, cofondatore di Ethereum, ha risposto aggiungendo dubbi e frenando la fretta. In questa analisi di **MoneyViz** traduciamo i due interventi in parole semplici: che cosa temono, che cosa propongono, che cosa *non* dicono, e che cosa conviene fare a te, a seconda di quanto hai e di come lo custodisci.

Che cosa hanno detto Drake e Buterin il 7 ottobre?

Drake chiede di preparare un piano di difesa senza panico; Buterin concorda sul rischio ma invita a non correre. Nel suo [post su X](#) Drake scrive di chiedere all'industria blockchain di «iniziare con calma a pianificare la bunker mode». Il motivo è che, nel caso peggiore, una rottura pratica della firma digitale usata da Bitcoin ed Ethereum potrebbe arrivare «in mesi, non anni», grazie a un salto nella matematica trovato o accelerato dall'AI.

Lo spunto è recente. Il 6 ottobre OpenAI ha pubblicato una raccolta di centinaia di nuovi risultati matematici prodotti da un suo modello interno. Per Drake è il segnale che la «superintelligenza matematica» è arrivata: settimane in cui accadono secoli di progresso.

Buterin ha risposto in [due interventi](#). Il primo messaggio è una frenata: non raccomanda a nessuno di precipitarsi a spostare i fondi oggi. Il secondo è un allargamento: il rischio, secondo lui, non riguarda solo la crittografia di oggi, ma anche parte di quella pensata per sostituirla.

Che cosa protegge, oggi, le tue criptovalute?

Una firma digitale che si basa su un problema matematico considerato, finora, impossibile da risolvere in tempi utili. Ogni volta che invii bitcoin o ether, il tuo wallet produce una firma che dimostra che possiedi la chiave privata, senza mostrarla. Chiunque può verificare la firma usando la tua chiave pubblica. La sicurezza sta tutta in un'asimmetria: dalla chiave privata si ricava la pubblica in un istante, dalla pubblica alla privata no.

CHIAVE PRIVATA, CHIAVE PUBBLICA, INDIRIZZO

Pensa a un timbro e alla sua impronta. La **chiave privata** è il timbro: chi lo ha può firmare, e deve restare solo tuo. La **chiave pubblica** è l'impronta lasciata sulla carta: tutti la vedono e possono controllare che la firma sia autentica. L'**indirizzo** è una sorta di impronta dell'impronta, ottenuta passando la chiave pubblica in una funzione di hash.

Il sistema di firma di Bitcoin ed Ethereum si chiama **ECDSA** (*Elliptic Curve Digital Signature Algorithm*) e si basa su oggetti matematici chiamati **curve ellittiche**. Risalire dall'impronta al timbro, cioè dalla chiave pubblica a quella privata, richiederebbe con i metodi noti più tempo dell'età dell'universo.

«Con i metodi noti» è l'inciso su cui si regge tutta la discussione. Nessuno ha mai dimostrato che un metodo più rapido non esista: semplicemente, decenni di matematici non lo hanno trovato.

Perché l'intelligenza artificiale potrebbe arrivare prima del computer quantistico?

Perché il computer quantistico è un problema di ingegneria con tempi leggibili, mentre una scoperta matematica può arrivare all'improvviso, su computer che esistono già. Il pericolo quantistico è noto: un computer quantistico abbastanza grande potrebbe eseguire l'algoritmo di Shor e ricavare le chiavi private da quelle pubbliche. Per farlo servono però macchine che ancora non esistono, e la loro costruzione segue una traiettoria che, pur discussa nei tempi, si può osservare.

Drake parla di un'altra cosa. Per lui una «rottura» è recuperare una chiave privata in tempi pratici, il suo esempio è una settimana, usando hardware già disponibile, come un grande insieme di schede grafiche. In quel mondo non serve aspettare i fisici: basta un algoritmo nuovo, abbastanza migliore di quelli conosciuti.

La ragione per cui lo ritiene plausibile non è un attacco dimostrato, che non c'è. È un cambio di passo nella ricerca matematica. Drake cita risultati recenti che hanno messo in crisi ipotesi considerate solide per anni: tra questi, un algoritmo che sulla carta supera il limite ritenuto insuperabile per la moltiplicazione di grandi numeri, e la smentita, annunciata a maggio da OpenAI, di una celebre congettura di Paul Erdős sulle distanze tra punti, formulata nel 1946.

PER CHI VUOLE APPROFONDIRE: IL PRECEDENTE DELLA FATTORIZZAZIONE

Buterin usa un esempio storico. La crittografia RSA, diffusa su internet, si basa sulla difficoltà di scomporre un numero enorme nei suoi fattori primi. Il metodo ingenuo richiede un tempo dell'ordine di $2^{n/2}$ per un numero di n bit. Decenni di lavoro umano hanno prodotto il **number field sieve**, che riduce quel costo a qualcosa come $2^{n^{1/3}}$. È il motivo per cui una firma RSA oggi pesa centinaia di byte e non 64.

La domanda di Buterin è se esistano scorciatoie simili, per le curve ellittiche e per altri schemi, che gli esseri umani non hanno trovato e che un sistema automatico potrebbe trovare. Non serve che l'AI «capisca» la crittografia: basta che comprima cinquant'anni di progresso matematico in due.

Drake aggiunge un precedente metodologico: nel 2018 la ricercatrice Ewin Tang mostrò che un problema per cui si pensava servisse un computer quantistico si poteva risolvere in modo efficiente anche con un computer classico. Da qui la sua ipotesi, dichiaratamente non dimostrata, di uno «Shor classico».

Drake segnala anche un indizio di altro tipo: tra le centinaia di risultati pubblicati da OpenAI, quelli sulla crittografia sono pochissimi. Nel suo ragionamento, se scoperte di questo genere venissero tenute riservate, il pubblico lo saprebbe in ritardo. È un'ipotesi sua, non un fatto accertato, e va letta come tale.

Perché le curve ellittiche e i reticoli preoccupano più delle hash?

Perché hanno una struttura matematica ricca, e la struttura è proprio ciò su cui un matematico, umano o artificiale, può costruire scorciatoie. Le curve ellittiche hanno proprietà regolari ed eleganti, studiate da più di un secolo. Le funzioni di hash, al contrario, sono progettate per non averne: rimescolano i dati in modo che non resti alcun appiglio.

Qui Buterin allarga il discorso. La crittografia «post-quantum», quella che si sta standardizzando per resistere ai computer quantistici, si basa in buona parte sui **reticoli**. Lo schema di firma ML-DSA, approvato dal NIST statunitense nel 2024, è uno di questi. Secondo Buterin la convinzione diffusa, «curve rotte, hash salve, reticoli salvi», non regge più: la sicurezza concreta dei reticoli potrebbe subire colpi seri dai prossimi due anni di matematica assistita dall'AI.

Più struttura, più appigli

Molta struttura matematica

Pochissima struttura



Drake: solo hash, niente curve né reticoli

Buterin: hash dove si può, reticoli con chiavi dieci volte più grandi

MoneyViz | Fonte: Justin Drake, Vitalik Buterin, 7 ottobre 2026

Più struttura matematica significa più appigli per chi cerca una scorciatoia. Elaborazione MoneyViz sui post di Justin Drake e Vitalik Buterin del 7 ottobre 2026.

CHE COS'È UNA FUNZIONE DI HASH

Una **funzione di hash** trasforma qualsiasi dato in una stringa di lunghezza fissa, una specie di impronta digitale. Cambia una virgola nel dato e l'impronta cambia completamente. Soprattutto, dall'impronta non si torna indietro. Bitcoin usa hash della famiglia SHA, Ethereum Keccak; esistono anche schemi di firma costruiti solo con hash, come SPHINCS+ (standardizzato dal NIST come SLH-DSA) e WOTS.

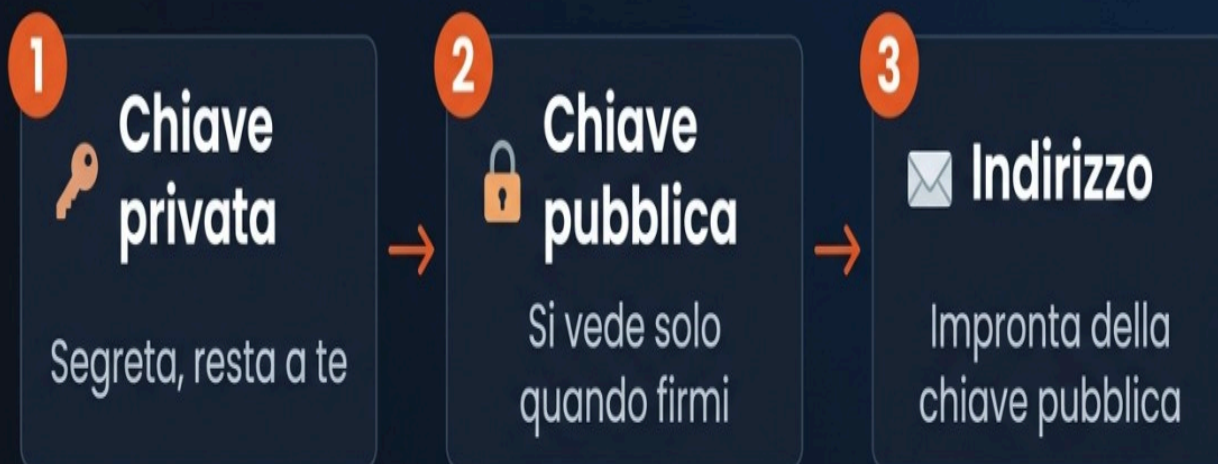
Nemmeno le hash sono garantite per sempre. Una singola funzione può essere indebolita da un attacco specifico, com'è successo in passato a MD5 e SHA-1, e per questo si usano funzioni studiate a lungo. Buterin cita anche una via teorica più radicale: se si dimostrasse che $P = NP$, cadrebbero tutte insieme, ma lui lo considera molto improbabile. Ed è più plausibile che un oggetto progettato per non avere struttura non ne abbia davvero, piuttosto che uno con tre scorciatoie note non ne nasconda una quarta.

Perché un indirizzo mai usato è più protetto?

Perché finché non firmi, la tua chiave pubblica non è visibile a nessuno, e senza chiave pubblica non c'è niente su cui lavorare. È un fatto noto da anni nel dibattito sul quantum, e Drake e Buterin lo riprendono perché vale anche contro un attacco matematico classico dello stesso tipo. Un indirizzo che ha solo ricevuto fondi mostra soltanto l'impronta della chiave pubblica. La chiave stessa compare sulla blockchain la prima volta che spendi, e da lì resta pubblica per sempre.

Torna al bunker dell'inizio. Un bunker di cui nessuno ha mai visto la porta è molto più difficile da forzare di uno con l'ingresso in bella vista, perché per studiare una serratura bisogna prima trovarla. Un indirizzo mai usato è un bunker con la porta ancora interrata. Ogni firma la porta in superficie.

Perché un indirizzo mai usato è più protetto



A  **Indirizzo mai usato:** la chiave pubblica resta nascosta

B  **Indirizzo che ha già firmato:** la chiave pubblica è pubblica per sempre

MoneyViz | Fonte: Justin Drake, Vitalik Buterin, 7 ottobre 2026

La chiave pubblica resta nascosta finché non firmi la prima volta. Elaborazione MoneyViz.

Il vantaggio pratico è enorme: per proteggersi così non servono wallet nuovi, né nuova crittografia, né modifiche alle regole della rete. Basta spostare i fondi su un indirizzo che non ha mai firmato, che si può generare dalla stessa seed che già usi.

DUE ECCEZIONI DA CONOSCERE

Non tutti gli indirizzi Bitcoin nascondono la chiave. I formati più antichi (P2PK, quelli dei primi anni, compresi molti attribuiti a Satoshi Nakamoto) e quelli **Taproot** (indirizzi che iniziano con `bc1p`) mostrano la chiave pubblica già nell'indirizzo. Secondo il [tracker «Risq List»](#) di Project Eleven, società che vende soluzioni post-quantum, i bitcoin con chiave pubblica già esposta sono nell'ordine di 6-7 milioni.

Su Ethereum il conto è uno solo. Su Ethereum l'indirizzo resta lo stesso dopo ogni operazione: se da quel conto hai inviato anche una sola transazione, la chiave pubblica è già nota. In quel caso «spostare il resto» significa spostare tutto su un indirizzo nuovo.

Che cosa propone Justin Drake con la bunker mode?

Una migrazione di massa controllata verso indirizzi freschi, cominciando da chi ha di più, senza fretta e senza panico. La sua raccomandazione personale è che i grandi detentori, e gli utenti più esperti, spostino il grosso dei fondi su indirizzi che non hanno mai firmato. E che, quando poi spendono, spostino anche il resto su un indirizzo nuovo. Ripete due volte di non avere fretta: una migrazione precipitosa, scrive, farebbe più danni del rischio che vuole ridurre.

Sul piano delle aziende fa nomi precisi: Binance, Bitbank, Robinhood, Bitfinex e Tether avrebbero l'occasione di rafforzare il loro *cold storage*, cioè le riserve custodite offline. Per chi possiede meno di 50 bitcoin indica una protezione parziale che chiama «scudo di Satoshi»: circa ventimila indirizzi dei primi anni contengono 50 bitcoin ciascuno con la chiave pubblica già visibile, e chi disponesse di un metodo per sfruttarli avrebbe ogni interesse a svuotare prima quelli. È un ragionamento sulle convenienze, non una garanzia.

Per chi non può smettere di firmare, come gli oracoli che portano i prezzi sulla blockchain o i comitati di sicurezza delle reti di secondo livello (*layer 2*), il consiglio è più stretto: cambiare chiave a ogni messaggio e affiancare uno schema basato sulle hash come SPHINCS+. Per uscire dalla bunker mode, conclude, servirà una crittografia «post-AI». La sua inclinazione è puntare tutto sulle hash, ed evitare curve, reticoli e simili. È la direzione già indicata dalla [bozza di roadmap di Ethereum](#) curata dai ricercatori della Ethereum Foundation, i cui tempi, secondo Drake, vanno accelerati.

Che cosa aggiunge Vitalik Buterin?

Una frenata sui tempi, un allargamento sui rischi e quattro indicazioni pratiche. Buterin non firma lo scenario peggiore di Drake. Dice che la firma attuale potrebbe cadere prima del previsto, e che questo è un motivo in più per usare indirizzi freschi. Ma sposta l'attenzione sui reticoli, e ne trae una conseguenza quantitativa: dove si vuole una sicurezza di lungo periodo con schemi a reticolo, conviene moltiplicare per dieci la dimensione delle chiavi. A quelle dimensioni, ammette, le soluzioni basate sulle hash diventano più efficienti in ogni caso in cui bastano.

È anche per questo che la roadmap «lean» di Ethereum, nell'ultimo anno, ha scelto firme solo basate su hash. Il problema più difficile, osserva Buterin, non riguarda le blockchain: è la cifratura a chiave pubblica che protegge messaggistica e siti web, per la quale le sole hash non bastano.

Le sue indicazioni per chi custodisce fondi sono le parti più utili:

1. **Indirizzi mai usati:** tenere i fondi su indirizzi che non hanno mai firmato è una buona idea, se non è difficile. Se è facile, va fatto.
2. **Migrazioni con prudenza:** le migrazioni vanno maneggiate con più paura degli attacchi. Buterin scrive di aver perso più denaro in migrazioni andate storte che in tutti gli attacchi messi insieme.
3. **Multisig con conferme fuori dalla catena:** nei conti che richiedono più firme, raccogliere le conferme *off-chain* evita di pubblicare le chiavi di tutti i firmatari. Se la firma attuale cadesse, il conto resterebbe in mano a chi raccoglie le firme, invece che a chiunque.
4. **Privacy senza dati cifrati sulla blockchain:** nei protocolli di privacy, meglio non scrivere note cifrate sulla catena, dove restano per sempre, e mandarle per altre vie.

Il secondo punto è quello che riporta al bunker. Nelle esercitazioni di protezione civile si insegna una cosa che sembra ovvia e non lo è: ci si fa più male correndo giù per le scale al buio che per la sirena. Buterin, in sostanza, dice lo stesso delle crypto.

Che cosa conviene fare, concretamente, a seconda di chi sei?

Ridurre l'esposizione della chiave pubblica, con calma e in proporzione a quanto hai. È l'unica misura che entrambi considerano sensata e che non richiede di credere allo scenario peggiore. Non è protezione post-quantum: è igiene.

CHI SEI	CHE COSA FARE	QUANDO
Piccole somme su un indirizzo mai usato per inviare (non Taproot bc1p, non P2PK)	Niente. Al prossimo invio, sposta il resto su un indirizzo nuovo	Nessuna urgenza
Somme importanti su indirizzi da cui hai già speso	Pianifica lo spostamento su un indirizzo fresco, anche dalla stessa seed; fai prima una prova con un importo piccolo	Con calma, senza una scadenza: dipende dal tipo di custodia e di indirizzo
Cripto lasciate su un exchange	Le chiavi le gestisce la piattaforma: informati su come protegge il suo cold storage	Quando l'exchange comunica un piano
Conti multisig, tesorerie, oracoli	Conferme off-chain, rotazione delle chiavi, valutare firme basate su hash	Da pianificare ora

La bunker mode tradotta per profilo: che cosa fare e con quale urgenza

Il perché della calma sta nel costo dell'errore. Una seed copiata male, un indirizzo di resto sbagliato, un sito falso travestito da «migrazione bunker», un messaggio che ti offre aiuto per spostare i fondi: sono pericoli già reali, molto più di un algoritmo che nessuno ha mostrato. Nessun exchange serio e nessun ricercatore ti chiederà mai la seed. Se qualcuno lo fa, è una truffa, come raccontiamo nell'[anatomia di una truffa con il finto supporto](#).

Se hai fondi sparsi su più wallet e indirizzi, il primo passo è sapere dove sono. **MoneyViz** ti permette di consultare saldi e movimenti di wallet ed exchange in un unico posto e di ricostruire gli spostamenti tra i tuoi indirizzi.

Che cosa NON dicono Drake e Buterin?

Non dicono che la crittografia di Bitcoin ed Ethereum sia già rotta, né che i tuoi fondi siano in pericolo oggi. Nessuno dei due mostra un algoritmo. Nessuno dei due afferma che i fondi su indirizzi mai usati siano a rischio. Lo scenario dei «mesi, non anni» è il caso peggiore di Drake, presentato come tale; Buterin non lo sottoscrive.

La minaccia è condizionale: se la matematica accelerata dall'AI trovasse sulle curve ellittiche, o sui reticoli, una scorciatoia simile a quella che il number field sieve trovò per la fattorizzazione, il margine di sicurezza si assottiglierebbe prima dell'arrivo dei computer quantistici. Prepararsi a questa possibilità, senza scambiarla per un'emergenza in corso, è tutto il contenuto della bunker mode.

Una nota anche sui prezzi: notizie di questo tipo possono muovere il mercato per qualche ora, ma una reazione di un giorno non dice nulla sulla tendenza, e nessuno dei due interventi parla di prezzi.

Spostare le crypto tra i propri indirizzi ha conseguenze fiscali?

Di per sé no: trasferire crypto tra indirizzi che appartengono tutti a te non è una vendita, quindi non genera plusvalenze. Restano però due cose da curare. La prima è la documentazione: dopo una migrazione devi poter dimostrare che il nuovo indirizzo è tuo e da dove arrivano i fondi, altrimenti in caso di controllo un trasferimento può sembrare un deposito di provenienza ignota. La seconda è il monitoraggio: tutti i wallet in tuo possesso vanno indicati nel quadro RW della dichiarazione, compresi quelli nuovi.

NOTA FISCALE: MIGRAZIONE SÌ, MA CON LE CARTE IN ORDINE

Prima di spostare i fondi, annota indirizzo di partenza, indirizzo di arrivo, data, importo e commissioni pagate, e conserva l'identificativo di ogni transazione. Con [MoneyViz](#) i trasferimenti tra wallet propri vengono riconosciuti come tali e non come vendite, e i quadri RW e RT si preparano dallo storico completo. Per approfondire leggi la [guida completa al quadro RW crypto 2026](#); per un dubbio veloce c'è [Fiscangelo](#), l'assistente fiscale gratuito di MoneyViz. Questo articolo non sostituisce una consulenza sul tuo caso. Se vuoi tenerlo a portata di mano, puoi [scaricare l'articolo in PDF](#).

Torniamo, per l'ultima volta, al bunker. Chi lo costruiva in giardino non viveva nel terrore: aveva semplicemente deciso che il momento giusto per prepararsi era quando non c'era fretta. E sapeva che il pericolo più probabile non era la bomba, ma inciampare sulle scale. La bunker mode di Drake e Buterin chiede la stessa cosa: un rifugio costruito con calma, una porta che resta interrata finché non serve aprirla, e nessuna corsa al buio. Valutare con calma se intervenire, in base al tipo di custodia e di indirizzo. Non precipitare. E ricordare che finora il modo più costoso di perdere crypto non è stato un matematico artificiale, ma una migrazione fatta male.

Fonti

- [Justin Drake — post su X sulla «bunker mode», 7 ottobre 2026](#)
- [Vitalik Buterin — post su X sui rischi della matematica accelerata dall'AI, 7 ottobre 2026](#)
- [Vitalik Buterin — post su X sulle migrazioni, 7 ottobre 2026](#)

- [Decrypt — Ethereum Researcher Says AI May Break Encryption Before Quantum Does](#)
 - [The Block — Vitalik Buterin warns against hasty wallet migrations](#)
 - [OpenAI — raccolta di risultati matematici pubblicata il 6 ottobre 2026](#)
 - [Will Sawin — An explicit lower bound for the unit distance problem \(arXiv, 2026\)](#)
 - [Ewin Tang — A quantum-inspired classical algorithm for recommendation systems \(arXiv, 2018\)](#)
 - [NIST — FIPS 204, Module-Lattice-Based Digital Signature Standard \(ML-DSA\)](#)
 - [NIST — FIPS 205, Stateless Hash-Based Digital Signature Standard \(SLH-DSA, da SPHINCS+\)](#)
 - [strawmap.org — bozza di roadmap di Ethereum L1 della Ethereum Foundation](#)
 - [Project Eleven — la Bitcoin Risq List e i bitcoin con chiave pubblica esposta](#)
 - [ethereum.org — come funzionano gli account di Ethereum](#)
 - [MoneyViz — quadro RW crypto 2026: guida completa alla compilazione](#)
-

Domande frequenti

Che cos'è la bunker mode proposta da Justin Drake?

È un piano di difesa che Justin Drake, ricercatore della Ethereum Foundation, ha chiesto al settore di preparare con calma il 7 ottobre 2026. Prevede una migrazione controllata dei fondi verso indirizzi che non hanno mai firmato transazioni, cominciando dai grandi detentori, nel caso in cui la matematica accelerata dall'intelligenza artificiale indebolisca la firma digitale ECDSA usata da Bitcoin ed Ethereum.

L'intelligenza artificiale ha già rotto la crittografia di Bitcoin ed Ethereum?

No. Né Drake né Buterin mostrano un attacco o un algoritmo. Drake descrive uno scenario peggiore in cui una rottura potrebbe arrivare «in mesi, non anni»; Buterin non lo sottoscrive e scrive di non raccomandare a nessuno di spostare i fondi in fretta. È un rischio da prendere sul serio, non un'emergenza in corso.

Perché un indirizzo mai usato è più protetto?

Perché un indirizzo che ha solo ricevuto fondi mostra soltanto l'impronta (hash) della chiave pubblica. La chiave pubblica compare sulla blockchain la prima volta che si invia una transazione. Un attacco che cerca di ricavare la chiave privata da quella pubblica non ha nulla su cui lavorare finché la chiave resta nascosta. Fanno eccezione i vecchi indirizzi Bitcoin P2PK e quelli Taproot (bc1p), che mostrano la chiave già nell'indirizzo.

Devo spostare subito le mie criptovalute?

Se hai piccole somme su un indirizzo da cui non hai mai inviato nulla, non devi fare niente, a meno che sia un indirizzo Bitcoin Taproot (inizia con bc1p) o un vecchio P2PK, che mostrano già la chiave pubblica. Se hai somme importanti su indirizzi da cui hai già speso, conviene pianificare con calma lo spostamento su un indirizzo nuovo, anche generato dalla stessa seed, facendo prima una prova con un importo piccolo. Buterin ricorda che le migrazioni fatte di fretta gli sono costate più di tutti gli attacchi subiti, e nessuno serio ti chiederà mai la seed per «aiutarti» a migrare.

Perché Vitalik Buterin è preoccupato anche per la crittografia post-quantum?

Perché buona parte della crittografia post-quantum, come lo standard di firma ML-DSA approvato dal NIST, si basa sui reticoli, oggetti matematici con molta struttura. Secondo Buterin la sicurezza concreta dei reticoli potrebbe subire colpi seri dai prossimi due anni di matematica assistita dall'AI: per questo preferisce firme basate solo su funzioni di hash, come WOTS e SPHINCS+, e chiavi dieci volte più grandi dove i reticoli restano necessari.

Spostare le crypto tra i miei indirizzi è tassato?

Un trasferimento tra indirizzi che appartengono tutti a te non è una vendita e quindi, di per sé, non genera plusvalenze. Conviene però documentare ogni spostamento (indirizzi, data, importo, commissioni, identificativo della transazione) e ricordare che anche i nuovi wallet vanno indicati nel quadro RW della dichiarazione dei redditi.

Articolo pubblicato su moneyviz.it — Another Block In The Wallet. Le immagini sono in pubblico dominio, i crediti sono indicati nell'articolo.