

30 OTTOBRE 2026 • 16 MIN DI LETTURA • DANILO GIUDICE

Furto Binance da 6,3 miliardi: cosa è successo e cosa fare ora

Cinquanta firme autentiche, un contratto che obbedisce a un solo indirizzo e dieci blockchain svuotate in una sera. Il furto più grande della storia delle crypto spiegato passo per passo, con i comunicati di Binance e quello che devi fare tu.



PERCHÉ TI RIGUARDA

- Se hai fondi su Binance: **l'exchange ha dichiarato che coprirà tutte le perdite** con il fondo SAFU e con fondi propri. I prelievi sono sospesi e la ripresa è attesa **entro 48 ore**.
- Nei prossimi giorni il rischio più concreto per te non è il furto, sono **le truffe che lo sfruttano**: falsi rimborsi, finti operatori, “servizi di recupero fondi”.
- Binance dice di non aver trovato prove di una fuga di chiavi private: i dati mostrano **firme valide ottenute dai suoi sistemi**. È la lezione che vale anche per il tuo wallet.
- Tutto quello che leggi qui è verificabile: ogni passaggio rimanda alla **transazione originale** sulla blockchain.

SE HAI FRETTA: COSA FARE ADESSO

1. **Informati solo dai canali ufficiali** di Binance: il sito, l'app e l'account X verificato. Nessun rimborso passa da un messaggio privato.
2. **Non rispondere** a chi ti offre compensazioni, airdrop di risarcimento o il recupero dei fondi: sono truffe, sempre.
3. **Non spostare nulla di corsa**: quando i prelievi riaprono, usa solo indirizzi della tua rubrica e prova prima con un importo piccolo.
4. **Salva una schermata dei saldi** di oggi: ti servirà se qualcosa non torna, e per la dichiarazione.

Il dettaglio è in [che cosa devi fare adesso](#). Puoi anche [scaricare questo articolo in PDF](#), per leggerlo con calma o girarlo a chi ti ha chiesto spiegazioni.

La sera del 29 ottobre 2026 dai wallet di Binance sono usciti circa **6,36 miliardi di dollari** su dieci blockchain diverse: quasi tutto in meno di mezz'ora, il resto in una seconda ondata alcune ore dopo. Nessuno ha forzato una cassaforte: ogni singola transazione era firmata in modo perfettamente valido dall'infrastruttura di Binance stessa. È come se qualcuno, entrato nell'ufficio giusto, avesse usato il **timbro autentico** della banca su moduli preparati da lui. Tienilo a mente, quel timbro: ci servirà ancora, perché spiega sia come è avvenuto il furto sia perché nessuno ha potuto annullarlo.

In questa analisi di **MoneyViz** ricostruiamo i fatti dalla fonte più affidabile che esista per un evento del genere: la blockchain. Abbiamo letto una per una le transazioni su Ethereum e Avalanche, le abbiamo confrontate con i comunicati ufficiali di Binance e con il rapporto di TRM Labs, la società di analisi che ha tracciato tutti i trasferimenti. Dove un dato viene da una sola fonte, lo diciamo.

Ecco che cosa è successo, minuto per minuto, dove sono finiti i soldi, quanto è stato bloccato e, soprattutto, che cosa conviene fare a te.

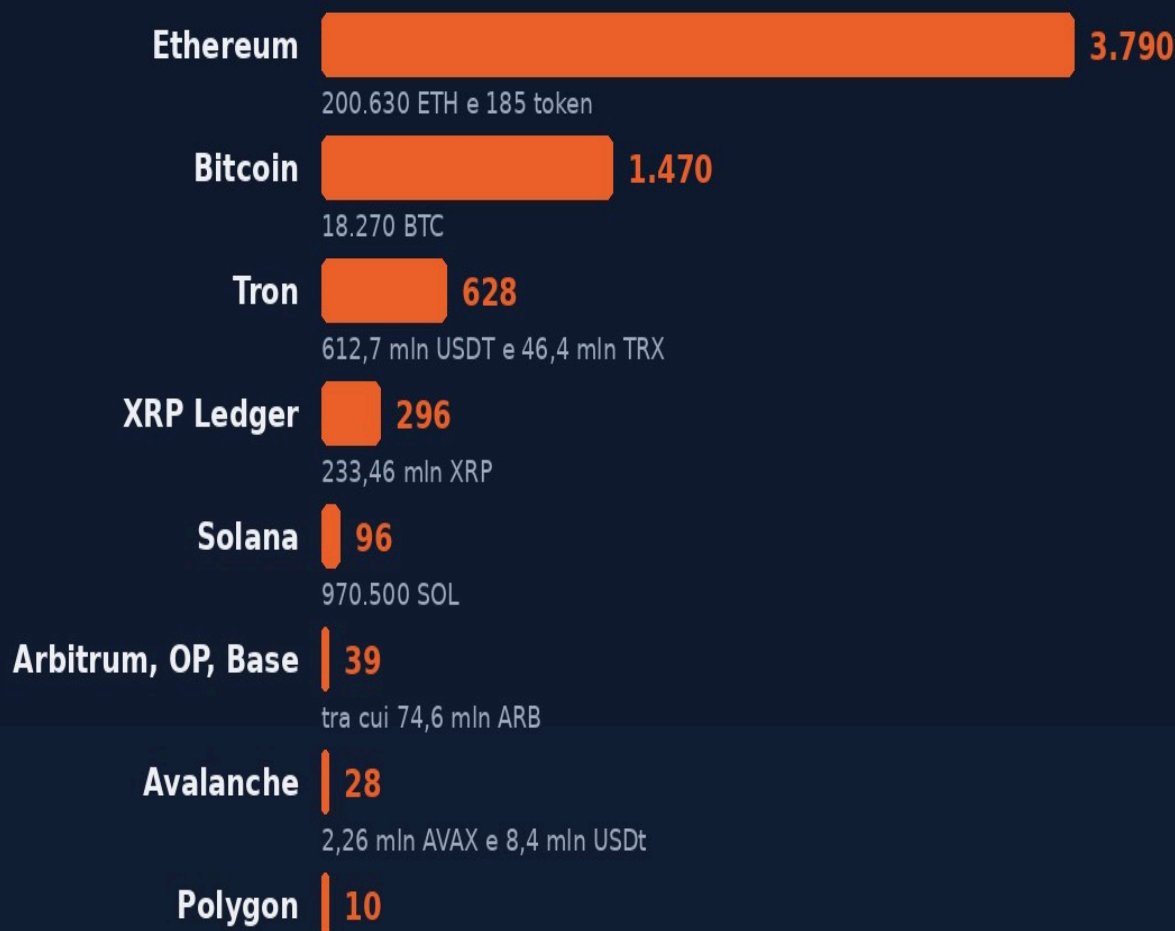
Che cosa è successo a Binance la sera del 29 ottobre?

Alle 20:05 UTC, le 21:05 in Italia, i wallet operativi di Binance hanno cominciato a svuotarsi uno dopo l'altro, su dieci reti diverse. Il primo è stato il XRP Ledger: fra le 20:05 e le 20:09 cinque wallet di Binance hanno mandato 233,46 milioni di XRP a un unico indirizzo, secondo la ricostruzione di [TRM Labs](#). Poi Solana e Optimism, alle 20:20 Bitcoin con 18.270 BTC in un colpo solo, quindi Tron con 612,7 milioni di USDT.

Su Ethereum, dove c'era la parte più grande, l'operazione è stata più raffinata: lo vediamo fra poco. Due ore e mezza dopo è arrivata una seconda ondata, sui wallet di Binance su Avalanche e Polygon. In totale, ai prezzi del momento, TRM conta circa 6,36 miliardi di dollari: **il furto più grande mai registrato nel settore**, circa quattro volte quello subito da Bybit nel febbraio 2025.

DIECI BLOCKCHAIN IN UNA SERA

Quanto è uscito da ogni rete, in milioni di dollari



Totale ai prezzi del momento del furto: circa 6,36 miliardi di dollari

Congelati: circa 2,7 miliardi secondo TRM, circa 3 miliardi secondo Binance

MoneyViz · Fonte: TRM Labs, valori al momento del trasferimento, dati al 30/10/2026 00:30 UTC

Dieci blockchain in una sera: Ethereum da sola vale quasi il 60% del totale. Fonte: TRM Labs, valori al momento del trasferimento.

CHE COS'È UN HOT WALLET

Un exchange tiene la gran parte dei fondi dei clienti in *cold wallet*, scollegati da internet, e una parte più piccola in **hot wallet**, collegati e sempre pronti a pagare i prelievi. È come la cassa di uno sportello rispetto al caveau: serve a lavorare, e per questo è la parte più esposta. Tutti i fondi usciti il 29 ottobre provengono da hot wallet.

Perché si parla di “ottobre nero”?

Perché il furto a Binance chiude un mese in cui l'intelligenza artificiale ha cambiato il ritmo degli attacchi al software di base di internet. Il 21 ottobre il progetto PHP, il linguaggio su cui gira circa il 70% dei siti web, ha pubblicato correzioni d'emergenza per due falle battezzate **PHP2Shell** (CVE-2026-109618 e CVE-2026-109619, gravità 9,2 su 10): permettevano a chiunque, senza credenziali, di eseguire codice sui server e di leggerne la memoria, password e chiavi comprese.

Il dettaglio che fa di questo episodio uno spartiacque è *come* sono state trovate. Il difetto era noto in forma embrionale dal 2024, ma trasformarlo in un attacco funzionante richiedeva una catena di passaggi “al limite di ciò che un ricercatore umano può fare in pratica”, scrive Wiz, che ci è riuscita con l'aiuto di modelli di intelligenza artificiale. Secondo KuppingerCole, Amazon ha registrato un tentativo di sfruttamento quattro giorni prima della correzione, e le agenzie di sicurezza di Stati Uniti e Regno Unito hanno consigliato di **spegnere i sistemi che non si potevano aggiornare subito**. Lo stesso giorno una libreria molto usata per collegare le app all'intelligenza artificiale, LiteLLM, è stata pubblicata con dentro un programma che rubava password e chiavi.

Nessun elemento collega queste falle al furto a Binance, che l'exchange attribuisce a un portatile compromesso. Ma il quadro del mese è questo, e sul fronte crypto ottobre si chiude nel modo peggiore: **forse il mese più nero di sempre per i furti di criptovalute**. Il solo caso Binance vale circa quattro volte il furto a Bybit del febbraio 2025, fino al 29 ottobre il più grande della storia.

Che cosa ha detto Binance, parola per parola?

Binance ha confermato l'incidente, ha indicato come possibile origine il computer di un tecnico e ha promesso di coprire tutte le perdite. Il comunicato più dettagliato, pubblicato sul suo account ufficiale su X la notte del 30 ottobre, dice:

“Binance’s initial investigation suggests that the security incident may involve a compromised DevOps engineer’s laptop, which allowed an attacker to gain access to a service container and submit unauthorized withdrawal transactions. We have found no evidence of any wallet private key leak. [...] The estimated total impact sits at around \$6.3B. We have worked with blockchain partners to freeze affected assets, with ~\$3 billion frozen onchain so far. Binance will cover all losses from the SAFU fund and the company’s funds. User funds are safe.”

In italiano: secondo l'indagine preliminare, l'incidente potrebbe partire dal **portatile compromesso di un ingegnere DevOps**, attraverso il quale l'autore dell'attacco è entrato in un componente del sistema e ha inviato prelievi non autorizzati. Binance **non ha trovato prove di una fuga di chiavi private**, stima l'impatto in circa 6,3 miliardi, dice di

avere congelato con i suoi partner circa 3 miliardi e annuncia che **coprirà tutte le perdite** con il fondo SAFU e con fondi propri. Fra le misure prese: sospensione temporanea di depositi e prelievi, **revoca dell'autorizzazione dell'indirizzo coinvolto**, coinvolgimento delle forze dell'ordine.

Un aggiornamento successivo ha corretto il quadro operativo:

“Deposits remain unaffected and continue to operate as normal. Withdrawals remain paused while our team completes a security revamp of the withdrawal service and its related addresses. We expect to resume within 48 hours [...] The incident stems from multiple factors.”

Quindi: **i depositi funzionano**, i prelievi restano sospesi mentre Binance ricostruisce il servizio che li gestisce, con ripresa attesa entro 48 ore. Un rapporto completo sulla causa è stato promesso ma non è ancora uscito.

La mattina del 30 ottobre il co-CEO di Binance, Richard Teng, ha aggiunto un chiarimento in un [messaggio rivolto agli utenti](#):

“To be clear: the attacker did not simply use one engineer’s permissions, and this was not a single “one-click” action. It involved a more complex attack process. Our investigation has not attributed responsibility to any individual.”

In italiano: non sono bastati i permessi di un singolo ingegnere e non è stata un’azione “con un clic”, ma un attacco più complesso; l’indagine non attribuisce colpe a nessuna persona. È coerente con quello che si vede sulla blockchain: giorni di preparazione e firme ottenute su reti diverse.

COSA DICE BINANCE	COSA MOSTRANO I DATI	ESITO
Prelievi non autorizzati inviati da un componente interno, nessuna prova di una fuga di chiavi private	Le firme sono valide e prodotte dai wallet di Binance, su reti e schemi di firma diversi nel giro di mezz’ora	Coerente
Revocata l'autorizzazione dell'indirizzo coinvolto	La delega dell'hot wallet Binance 14 verso il contratto del responsabile oggi non c'è più	Coerente
Circa 3 miliardi congelati	TRM ne conta circa 2,7 miliardi, ZachXBT oltre 2,83 miliardi	Ordine di grandezza coerente, cifra non ancora consolidata
Impatto di circa 6,3 miliardi	TRM: 6,36 miliardi ai prezzi del momento	Coerente

Le dichiarazioni di Binance alla prova dei dati onchain

Come sono usciti i fondi, minuto per minuto?

La preparazione è cominciata 36 ore prima, il grosso dell’esecuzione è durato mezz’ora. Il primo movimento riconducibile al responsabile è del **28 ottobre alle 07:39 UTC**: un prelievo di 0,1 ETH da Tornado Cash, il servizio che rende anonima la provenienza delle cripto, verso il wallet che poi ha guidato tutta l’operazione ([transazione](#)). Altri

piccoli prelievi da Tornado Cash hanno finanziato il resto: in tutto l'operazione è costata circa 1,5 ETH di commissioni.

Il 29 ottobre, fra le 13:51 e le 16:47, quel wallet ha fatto delle prove su wallet di test, comprando piccole quantità di USDT e USDC per verificare che il meccanismo funzionasse anche sui token. Alle 15:59 ha pubblicato il contratto che avrebbe svuotato Binance. Poi, alle 20:05, è cominciato tutto.

LA NOTTE DEL 29 OTTOBRE 2026

Come sono usciti 6,36 miliardi, ora per ora (UTC)

● PREPARAZIONE ● FURTO ● BLOCCO

- 28/10 07:39 ● Primo prelievo da Tornado Cash verso il wallet operativo: 0,1 ETH
- 29/10 15:59 ● Pubblicato il contratto che svuoterà il wallet (0x63e8...6fAe)
- 20:05 ● XRP Ledger: 233,46 milioni di XRP escono da cinque wallet Binance
- 20:20 ● Bitcoin: 18.270 BTC in un colpo, subito spezzati in pezzi da 1.000 e da 100
- 20:20:59 ● Ethereum: una transazione porta 50 deleghe EIP-7702 firmate da Binance 14
- 20:24:23 ● Una sola transazione: 167.464 ETH, 1,615 miliardi di USDT e altri 62 token
- 20:41 ● 823 milioni di USDC escono dallo smart account Binance 34
- 21:01 ● Tether congela il collettore principale: oggi 1,175 miliardi di USDT bloccati
- 21:02:35 ● 23.314 ETH (19.763 presi in prestito su Aave) escono 12 secondi prima del blocco
- 21:04 ● Circle congela 823 milioni di USDC
- 21:47 ● 122.310 ETH ottenuti vendendo 325 milioni di USDT ai market maker
- 22:01 - 22:10 ● Ripple congela 40,5 milioni di RLUSD, World Liberty 27,8 milioni di USD1
- 23:04 ● Seconda ondata: escono i wallet Binance su Avalanche e Polygon
- 30/10 00:08 ● Il Security Council di Arbitrum sottrae circa 30 milioni di dollari al responsabile

MoneyViz · Fonti: onchain via Routerscan (ETH, AVAX), TRM Labs (BTC, XRP, Arbitrum) · 30/10/2026

La notte del 29 ottobre in quattordici passaggi, in orario UTC (in Italia un'ora in più). In arancione i furti, in verde i blocchi. Fonti: dati onchain letti con Routerscan per Ethereum e Avalanche, TRM Labs per Bitcoin, XRP e Arbitrum.

Come ha fatto un wallet di Binance a svuotarsi da solo?

Gli è stato fatto firmare in anticipo il permesso di obbedire a un programma scritto dal responsabile. Il wallet in questione è uno dei più noti di Binance, conosciuto come *Binance 14* (0x28C6...1d60). Lo strumento usato si chiama **EIP-7702** ed è una funzione di Ethereum attiva da maggio 2025.

EIP-7702 E GLI “SMART CONTRACT”, IN PAROLE SEMPLICI

Uno “**smart contract**” è un programma che vive sulla blockchain e si esegue da solo quando qualcuno lo chiama: Roberto Garavaglia, in *Tutto su Blockchain* (Hoepli), lo descrive come un *codice auto-esecutivo*, un protocollo transazionale automatizzato. Di solito un wallet normale e uno smart contract sono due cose distinte. Con EIP-7702, invece, un wallet può firmare un’autorizzazione che dice: “da ora in poi, quando qualcuno mi chiama, esegui il codice di questo contratto”. È una funzione pensata per rendere i wallet più comodi. Chi controlla quel contratto, però, controlla il wallet.

Alle **20:20:59 UTC** il wallet operativo del responsabile ha inviato una sola transazione con dentro **cinquanta autorizzazioni**, tutte firmate da Binance 14 e tutte rivolte allo stesso contratto. Perché cinquanta? Ogni wallet numera le proprie operazioni in ordine progressivo, il cosiddetto *nonce*, e un’autorizzazione vale soltanto per il numero a cui il wallet è arrivato in quel preciso istante. Pensa al numero di protocollo di un ufficio: un modulo timbrato per la pratica numero 100 non vale per la 101.

Binance 14 paga prelievi in continuazione, quindi il suo contatore corre. Il responsabile ha fatto timbrare cinquanta moduli, uno per ciascun numero dal 18.914.775 al 18.914.824, sicuro che almeno uno fosse ancora quello giusto al momento dell’esecuzione. Uno lo era, ed è bastato. Ecco di nuovo il **timbro autentico** dell’introduzione: le firme non erano falsificate, erano vere, prodotte dall’infrastruttura di Binance su richiesta di chi ne aveva preso il controllo.

Delega dell'hot wallet a un contratto sweeper controllato da terzi

1 · WALLET OPERATIVO (authorizedCaller)

0x7C86...5CA0

Finanziato da prelievi Tornado Cash dal 28/10, 07:39 UTC.

type-4 · 50 autorizzazioni · blocco 26.300.753

2 · BINANCE 14, HOT WALLET

0x28C6...1d60

Tuple firmate dalla chiave dell'EOA su nonce consecutivi 18.914.775-18.914.824.
Code dopo l'esecuzione: 0xef0100 || 0x63e8...6fAe.

esecuzione del codice delegato

3 · CONTRATTO SWEEPER

0x63e8...6fAe

sweep · withdrawETH · withdrawToken · callExecute, riservate all'authorizedCaller.

sweep() · blocco 26.300.770 · 64 trasferimenti

4 · COLLETTORE

0x5227...2f8c

167.464 ETH, 1,615 miliardi di USDT e altri 62 token alle 20:24:23 UTC.

PROPAGAZIONE

Binance 34: smart account (proxy ERC-1967, SingleOwnerMSCA) con Binance 14 come owner. callExecute → execute() dall'EOA delegato.

823 mln USDC

usciti alle 20:41 e alle 20:59

Tutte le firme sono valide e prodotte dall'infrastruttura di Binance: nessun controllo a livello di protocollo poteva respingerle.

MoneyViz · Fonte: transazioni 0xad99264d... e 0x53bd38b8... su Ethereum, verificate via Routerscan

Il meccanismo, passo per passo. Il contratto accettava ordini da un solo indirizzo, quello del responsabile. Fonte: transazioni 0xad99264d... e 0x53bd38b8... su Ethereum.

Tre minuti e ventiquattro secondi dopo, alle **20:24:23**, è partito l'ordine: una transazione con 64 trasferimenti verso un indirizzo collettore (0x5227...2f8c), con dentro **167.464 ETH, 1,615 miliardi di USDT**, 62,6 milioni di RLUSD, 29.934 wBETH, 11.372 XAUt (oro tokenizzato) e decine di altri token.

C'è un secondo passaggio, meno visibile e altrettanto istruttivo. Binance 14 era anche il **proprietario di uno smart account**, un wallet-programma chiamato *Binance 34*. Il contratto del responsabile aveva una funzione apposta per dare ordini a quel conto in nome del suo proprietario. Alle 20:41 e alle 20:59 sono usciti così **823 milioni di USDC** (transazione). Chi aveva in mano Binance 14 aveva in mano anche tutto ciò che si fidava di Binance 14.

Perché le altre blockchain sono state svuotate senza nessun trucco?

Perché sulle altre reti non serviva: i wallet di Binance hanno firmato normali trasferimenti verso il responsabile. Un secondo hot wallet su Ethereum, *Binance 16*, alle 20:24:47 ha mandato 28.006 ETH, 55,7 milioni di USDT e 25,9 milioni di RLUSD con una transazione ordinaria, senza nessuna delega. Su Avalanche, cinque wallet di Binance hanno mandato in tutto 2,26 milioni di AVAX e 8,4 milioni di USDt allo stesso indirizzo usato su Ethereum.

Reti diverse usano chiavi e sistemi di firma diversi: se tutte hanno prodotto firme valide per la stessa persona nel giro di mezz'ora, il problema non era una singola chiave. Era il **sistema che decide che cosa firmare**. TRM arriva alla stessa conclusione, ed è coerente con la versione di Binance. È l'ufficio del timbro, non il timbro.

PERCHÉ LA BLOCKCHAIN NON POTEVA DIRE DI NO

Una blockchain controlla una cosa sola: che la firma sia valida. Non sa chi ha premuto il pulsante, né perché. Una transazione firmata correttamente è definitiva, e non esiste un servizio clienti della rete che possa annullarla. Per questo le difese di un exchange stanno *prima* della firma, nei controlli interni su chi può chiederla: è lì che il 29 ottobre qualcosa ha ceduto.

Dove sono finiti i soldi?

Una parte è stata bloccata in poche decine di minuti, il resto è stato trasformato in ETH e parcheggiato in pochi indirizzi. Il responsabile sapeva che stablecoin come USDT e USDC possono essere congelate da chi le emette, e ha corso contro il tempo per convertirle in asset che nessuno può bloccare.

Alle 20:30, 500 milioni di USDT sono stati spostati su un wallet separato. Da lì **325 milioni sono stati venduti a operatori professionali** in cambio di circa 122.300 ETH, a un prezzo più alto di oltre il 10% rispetto al mercato, secondo TRM: pur di uscire in fretta, il responsabile ha accettato di perdere decine di milioni. Gli altri 175 milioni non hanno fatto in tempo: sono stati congelati.

Un secondo wallet ha usato 60 milioni di USDT come garanzia sul protocollo di prestiti Aave e ha preso in prestito circa 19.763 ETH. Funziona come un banco dei pegni: lasci un oggetto di valore e porti via contanti, ma il responsabile non ha alcuna intenzione di riscattare il pegno. Gli ETH sono usciti alle 21:02:35 (transazione): **dodici secondi prima** che Tether congelasse quel wallet. Nelle ore successive, decine di wallet secondari hanno venduto su Uniswap le altre criptovalute rubate, e il ricavato è confluito anch'esso in ETH.

DOVE SONO FINITI I SOLDI (ETHEREUM E AVALANCHE)

Dal collettore ai depositi: cosa è bloccato e cosa no

Le cifre sono quantità esatte lette sulla blockchain al 30 ottobre, ore 08:30 UTC. Nessuno dei depositi A-F ha mai inviato una transazione.

1,175 mld USDT · 823 mln USDC · 27,8 mln USD1 · 12.574 XAUT

CONGELATO

→ restano nel collettore

197.460 ETH (alle 20:38 e alle 01:14)

NON CONGELABILE

→ Deposito A · 0x8532...43D4

500 mln USDT: 325 venduti tramite UniswapX, 175 bloccati

NON CONGELABILE

→ Deposito E · 0xc887...286a · 137.602 ETH

200 mln USDT: 60 su Aave in garanzia di 19.763 ETH presi in prestito, il resto scambiato

NON CONGELABILE

→ Deposito B · 0x897C...8DF3 · 78.415 ETH

Centinaia di altcoin vendute su Uniswap da wallet secondari

NON CONGELABILE

→ Deposito D · 0x79e7...544a · 34.279 ETH

17.260 ETH (30/10 alle 05:15)

NON CONGELABILE

→ Deposito C · 0x03b0...20ea

88,5 mln RLUSD: 48 venduti in ETH, poi il blocco

CONGELATO

→ 40,5 mln RLUSD congelati da Ripple

ETH dalla vendita di RLUSD, wallet secondari e secondo collettore

NON CONGELABILE

→ Deposito F · 0x5440...c942 · 40.600 ETH

200.000 AVAX → 1,56 mln USDC → bridge di Circle verso Ethereum

CONGELATO

→ congelati da Circle all'arrivo

Totale non congelabile: circa 505.600 ETH, oltre 1,1 miliardi di dollari ai prezzi del 30 ottobre

MoneyViz · Fonti: dati onchain (Routescan), TRM Labs, Binance · 30 ottobre 2026

Dal collettore ai depositi. In verde ciò che è bloccato, in arancione ciò che nessun emittente può congelare. Quantità lette sulla blockchain il 30 ottobre mattina.

Il 30 ottobre mattina la fotografia su Ethereum è questa: **sei depositi con circa 505.600 ETH**, più di 1,1 miliardi di dollari, che non hanno mai inviato una transazione. Uno di questi è stato riempito con gli ETH ricavati vendendo in

fretta gli RLUSD rubati, prima che Ripple li bloccasse. Fuori da Ethereum restano i **18.270 BTC**, che vengono spezzati in pezzi più piccoli per renderne più difficile il tracciamento.

DEPOSITO	INDIRIZZO	ETH	DA DOVE ARRIVANO
A	0x8532...43D4	197.460	ETH rubati direttamente agli hot wallet
E	0xc887...286a	137.602	Vendita di 325 milioni di USDT
B	0x897C...8DF3	78.415	Prestito su Aave e scambi di USDT
D	0x79e7...544a	34.279	Vendita di altre criptovalute su Uniswap
C	0x03b0...20ea	17.260	ETH dal collettore, il 30 ottobre alle 05:15 UTC
F	0x5440...c942	40.600	Vendita degli RLUSD rubati e altri wallet del responsabile

I depositi di ETH non congelabili, saldo al 30 ottobre 2026

GLI INDIRIZZI SOSIA INTORNO AL RESPONSABILE

Chi controlla questi indirizzi su un block explorer troverà centinaia di movimenti strani: token chiamati “ETH” o “USDT” con caratteri che sembrano uguali ma non lo sono, e indirizzi quasi identici a quelli veri, uguali nei primi e negli ultimi caratteri. È **address poisoning**, la stessa tecnica che si usa contro i normali utenti. Morale per te: **un trasferimento che compare nella tua cronologia non è una prova che quel token esista o abbia valore**. Ne abbiamo parlato nella puntata sull'[approval phishing](#).

Quanto è stato congelato, e da chi?

Circa 2,7 miliardi di dollari, quasi tutti in stablecoin, bloccati dalle società che le emettono. Qui il timbro autentico mostra il suo rovescio: se la rete accetta ogni firma valida, l'unico modo per fermare i soldi è che intervenga chi ha il potere di bloccare un token. Le stablecoin ce l'hanno, ETH e BTC no.

Il primo blocco è arrivato alle 21:01 UTC, 37 minuti dopo lo svuotamento principale, quando Tether ha congelato il collettore ([transazione](#)). Alle 22:06 Tether ha congelato anche lo stesso **Binance 14**, perché il wallet era ancora sotto controllo del responsabile e continuava a ricevere fondi.

CHI	QUANDO (UTC)	COSA
Tether	dalle 21:01	Circa 1,77 miliardi di USDT, di cui 1,175 miliardi nel collettore
Circle	dalle 21:04	823 milioni di USDC, poi 1,56 milioni arrivati da Avalanche
Tether Gold	21:11	12.574 XAUt, circa 50 milioni di dollari in oro tokenizzato
Ripple	22:01	40,5 milioni di RLUSD, dopo che 48 milioni erano già stati venduti
World Liberty Financial	22:10	27,8 milioni di USD1
Security Council di Arbitrum	00:08 del 30/10	Circa 30 milioni di dollari in ETH e ARB

Chi ha congelato che cosa (fonte: dati onchain e TRM Labs)

PERCHÉ UNA STABLECOIN SI PUÒ CONGELARE E ETH NO

USDT, USDC, RLUSD e USD1 sono emessi da società che hanno previsto una funzione di blocco: possono impedire a un indirizzo di muovere i propri token. ETH e BTC non hanno un emittente, e nessuno ha quel pulsante. È un compromesso: una stablecoin è più recuperabile in un caso come questo, ma anche più esposta a decisioni di terzi. Su Arbitrum, invece, un gruppo con poteri di emergenza sulla rete ha spostato d'autorità i fondi del responsabile, come [ha segnalato l'investigatore ZachXBT](#): una decisione eccezionale e discussa.

Chi c'è dietro il furto?

TRM Labs lo attribuisce con “alta confidenza” a **TraderTraitor, un'unità legata alla Corea del Nord**. È la stessa unità che l'FBI ha indicato come responsabile del furto a Bybit del febbraio 2025. TRM cita elementi ricorrenti: piccoli prelievi da Tornado Cash per finanziare il wallet operativo, una preparazione iniziata con largo anticipo, firme ottenute prima e usate tutte insieme. Sono esattamente i passaggi che si vedono sulla blockchain.

ZachXBT ha aggiunto un tassello: fondi del furto a Binance e di quello subito da Bitget sono finiti sullo **stesso indirizzo**. Secondo lui, è lo stesso attore. Va detto con chiarezza: sono attribuzioni di società di analisi e investigatori indipendenti, molto solide nel metodo ma non ancora confermate da un'autorità.

I fondi dei clienti di Binance sono al sicuro?

Binance dice di sì e si è impegnata pubblicamente a coprire tutte le perdite; i segnali da seguire arriveranno dai numeri. I fondi sono usciti dai wallet operativi dell'exchange, non dai conti dei singoli clienti: il tuo saldo su Binance è un debito di Binance verso di te, e Binance ha detto che lo onorerà con il fondo **SAFU** (*Secure Asset Fund for Users*, la riserva di emergenza creata nel 2018) e con i propri fondi.

Due impegni concreti permetteranno di verificarlo: la **ripresa dei prelievi**, attesa entro 48 ore dall'ultimo aggiornamento, e una Proof of Reserves aggiornata, cioè la dimostrazione pubblica delle riserve detenute per conto dei clienti. Attenzione al suo limite: mostra le riserve, ma da sola non certifica tutte le passività dell'exchange, quindi è un

indizio forte, non una garanzia completa. La promessa di Binance è credibile ma resta una promessa: è giusto saperlo, senza drammi e senza ingenuità.

Che cosa ha fatto il mercato?

ETH è sceso, ma attribuire tutto al furto sarebbe una scorciatoia. La mattina del 30 ottobre ETH quotava circa 2.237 dollari, in calo del 3,6% sulle 24 ore secondo i dati di Routescan; durante la notte, scrive TRM, oscillava fra 2.300 e 2.350 dollari. Un movimento di un giorno non dice nulla sulla tendenza dei prossimi mesi, e con i dati disponibili non è possibile separare l'effetto del furto da quello di altri fattori della stessa giornata.

Che cosa devi fare adesso?

Proteggerti dalle truffe che arrivano dopo un furto è più urgente che preoccuparti del furto stesso. Ogni grande incidente produce un'ondata di messaggi falsi che sfruttano la paura. Ecco cosa fare, in ordine:

1. **Usa solo i canali ufficiali.** Sito e app di Binance, digitati da te, e l'account X verificato [@binance](#). Nessun rimborso, nessuna "verifica dell'account" e nessuna compensazione passa da Telegram, WhatsApp, email non richieste o messaggi diretti.
2. **Diffida di chi promette di recuperare i fondi.** I "servizi di recupero" sono una truffa nella truffa: ti chiedono un anticipo o l'accesso al wallet. Il [finto supporto](#) funziona proprio così.
3. **Ignora token e airdrop di "risarcimento"** che compaiono nel tuo wallet. Non interagire, non provare a venderli: spesso servono a farti firmare un'autorizzazione che ti svuota il conto.
4. **Quando i prelievi riaprono, non avere fretta.** Il giorno della riapertura è quello con più traffico e più tentativi di frode. Usa indirizzi della tua rubrica, mai copiati dalla cronologia, e prova prima con un importo piccolo.
5. **Salva una schermata dei saldi** di questi giorni e scarica gli estratti conto appena possibile: se qualcosa non torna, è la tua prova.
6. **Se hai un wallet tuo su Ethereum**, controlla periodicamente le autorizzazioni concesse con uno strumento come [Revoke.cash](#), e rifiuta qualsiasi richiesta di firma "EIP-7702" o di "aggiornamento dell'account" che non hai avviato tu.
7. **Ripensa a quanto tieni in un solo posto.** Non è un invito a scappare da Binance: è la regola di sempre. Nessuna piattaforma, per quanto grande, dovrebbe custodire tutto ciò che possiedi.

E IL FISCO?

Se i tuoi saldi restano intatti, per te non succede nulla di fiscalmente rilevante: il furto ha colpito i wallet dell'exchange, non le tue crypto, e non c'è nessuna cessione a tuo nome. Le crypto che detieni su Binance restano da indicare nel [quadro RW](#) e le operazioni che fai nel [quadro RT](#), come sempre. Con **MoneyViz** colleghi il conto Binance e ritrovi tutti i movimenti già pronti per la dichiarazione, anche quelli dei giorni di blocco.

Torniamo al timbro. Secondo Binance, il 29 ottobre non è stata rubata la chiave della cassaforte: qualcuno è entrato nell'ufficio dove si timbrano i moduli, e ogni modulo uscito quella sera era autentico. Per questo la rete lo ha accettato, e per questo l'unico rimedio è arrivato da chi aveva il potere di bloccare i propri token. Vale anche per te, in piccolo: **il tuo timbro è la tua firma, e la tua chiave è la frase di recupero.** Molti truffatori te la chiederanno apertamente: non

condividerla mai, con nessuno, per nessun motivo. I più insidiosi invece ti chiederanno solo di firmare qualcosa, con fretta e con un buon motivo. Quella firma non darla mai a chi te la chiede per primo.

Scarica questo articolo in PDF, con tutte le infografiche, per leggerlo con calma o girarlo a chi ti ha chiesto spiegazioni.

COME ABBIAMO RICOSTRUITO I FATTI

Le transazioni su Ethereum e Avalanche le abbiamo lette direttamente sulla blockchain con [Routescan](#) e altri strumenti di analisi onchain: i movimenti indirizzo per indirizzo, i blocchi decisi da Tether, Circle e dagli altri emittenti, la delega usata per svuotare Binance 14. Ogni transazione citata si può controllare su [Etherscan](#). I dati su Bitcoin, Tron, XRP Ledger e Solana vengono dal rapporto di TRM Labs. Abbiamo seguito i soldi passaggio per passaggio, scartando i token falsi creati per confondere le tracce: i movimenti più piccoli, sotto circa 100.000 dollari, possono non comparire. I depositi restano sotto monitoraggio.

Aggiornamento: questo articolo riflette i dati disponibili il 30 ottobre 2026 mattina. Saldi e totali congelati possono cambiare: li stiamo monitorando e aggiorneremo il testo se ci saranno movimenti rilevanti o quando Binance pubblicherà il rapporto sulle cause.

Fonti

- [Binance su X](#) — comunicato sull'indagine preliminare: portatile compromesso, nessuna fuga di chiavi private, impatto di circa 6,3 miliardi, copertura delle perdite
- [Richard Teng \(co-CEO di Binance\) su X](#) — “non un'azione con un clic”, nessuna responsabilità individuale
- [TRM Labs](#) — ricostruzione completa: 6,36 miliardi su dieci blockchain, delega EIP-7702, blocchi, attribuzione
- [ZachXBT su X](#) — blocco su Arbitrum, totale congelato e collegamento con il caso Bitget
- [Wiz](#) — PHP2Shell: come l'intelligenza artificiale ha trasformato una falla nota in un attacco funzionante
- [KuppingerCole](#) — PHP2Shell: cronologia e raccomandazioni delle agenzie di sicurezza
- [Ethereum Improvement Proposals](#) — la specifica di EIP-7702
- [Etherscan](#) — la transazione con le 50 deleghe firmate da Binance 14
- [Etherscan](#) — lo svuotamento principale: 167.464 ETH e 63 token in una transazione
- [Binance](#) — pagina della Proof of Reserves
- [MoneyViz](#) — quadro RW crypto 2026: guida completa alla compilazione

Co-autore: [Filippo Chiricozzi](#)

Domande frequenti

Quanto è stato rubato a Binance il 29 ottobre 2026?

Binance stima un impatto di circa 6,3 miliardi di dollari. TRM Labs, che ha tracciato ogni trasferimento sulle dieci blockchain coinvolte, arriva a circa 6,36 miliardi ai prezzi del momento del furto: 3,79 miliardi su Ethereum, 1,47 miliardi in 18.270 BTC, 628 milioni su Tron, 296 milioni in XRP e il resto su Solana, Arbitrum, Optimism, Base, Avalanche e Polygon. È il furto più grande mai registrato nel settore.

I soldi dei clienti di Binance sono al sicuro?

Binance ha dichiarato che coprirà tutte le perdite con il fondo SAFU e con fondi propri, che i fondi degli utenti sono al sicuro e che pubblicherà una Proof of Reserves aggiornata. I fondi sono usciti dai wallet operativi dell'exchange, non dai conti dei singoli clienti. Due segnali concreti da seguire sono il ritorno dei prelievi, previsto entro 48 ore dall'ultimo aggiornamento, e la nuova Proof of Reserves: mostra le riserve detenute, ma da sola non certifica tutte le passività dell'exchange, quindi è un indizio forte, non una garanzia completa.

Come hanno fatto a svuotare un wallet di Binance?

Hanno fatto firmare al wallet Binance 14, in anticipo, cinquanta autorizzazioni che gli ordinavano di obbedire a un programma scritto dal responsabile, usando una funzione di Ethereum chiamata EIP-7702. Una delle cinquanta è risultata valida e da quel momento il wallet ha eseguito gli ordini del programma: alle 20:24 UTC ha mandato in una sola transazione 167.464 ETH, 1,615 miliardi di USDT e altri 62 token.

Quanto dei fondi rubati è stato bloccato?

Circa 2,7 miliardi di dollari secondo TRM, circa 3 miliardi secondo Binance. Tether ha bloccato circa 1,77 miliardi di USDT, Circle circa 825 milioni di USDC, Ripple 40,5 milioni di RLUSD, World Liberty Financial 27,8 milioni di USD1, e il Security Council di Arbitrum circa 30 milioni. Restano fuori portata circa 505.600 ETH e 18.270 BTC: sono criptovalute che nessuno può bloccare con un comando.

Ho fondi su Binance: che cosa devo fare adesso?

Niente di affrettato. Segui solo i canali ufficiali di Binance, non rispondere a messaggi che promettono rimborsi, compensazioni o recupero fondi, non cliccare link ricevuti in privato e non spostare nulla verso indirizzi che non sono già nella tua rubrica. Quando i prelievi riaprono, prova prima con un importo piccolo. Conserva una schermata dei saldi di questi giorni.

Se Binance copre le perdite, il furto ha effetti fiscali per me?

Se i tuoi saldi restano intatti, per te non succede niente di fiscalmente rilevante: il furto ha colpito i wallet dell'exchange, non le tue crypto, e non c'è nessuna cessione a tuo nome. Le crypto che detieni su Binance continuano a stare nel quadro RW e le operazioni che fai nel quadro RT, come sempre.

Gli autori



AUTORE

Danilo Giudice

Content Strategist, MoneyViz

Content Strategist MoneyViz, CMO Routescan, CMO 0Var, co-founder Bitcoin Sicilia, co-founder ETHNA.

Costruisce narrative che traducono la complessità blockchain in contenuti accessibili per investitori e community.

[LinkedIn](#) · [Bitcoin Sicilia](#)



CO-AUTORE

Filippo Chiricozzi

Digital assets e fintech, Banca Sella

Dal food tech al fintech fino al web3: ex COO di Moovenda, oggi in Banca Sella con focus sui digital assets. Autore della newsletter Deky Daily e di analisi onchain sugli attacchi agli exchange, fra cui la ricostruzione del caso Bitget.

[LinkedIn](#)

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