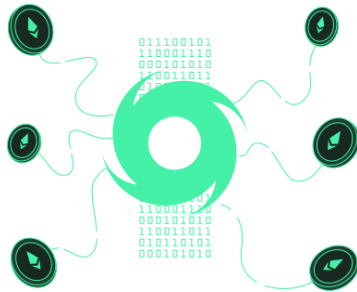
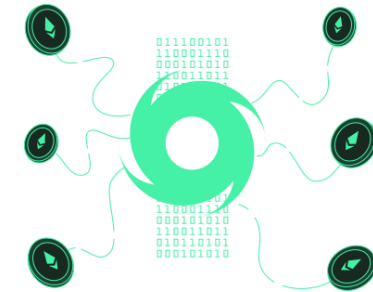


Strategie avanzate di demixing per



TORNADO.CASH



Analisi comportamentale e data-clustering nelle indagini su blockchain

10° Convegno Nazionale ONIF - Osservatorio Nazionale Informatica Forense

"Informatica forense: Il prossimo capitolo è già iniziato."

Genova - 16 Ottobre 2026

Umberto BUONORA

Contacts

- > umberto.buonora@recoveris.io
- > <https://t.me/misterserious>
- > <https://it.linkedin.com/in/umberto-buonora-158569197>

Working for

- > Recoveris - Head of Investigations

<https://recoveris.io>

- > Former Italian LE

<https://gdf.gov.it>



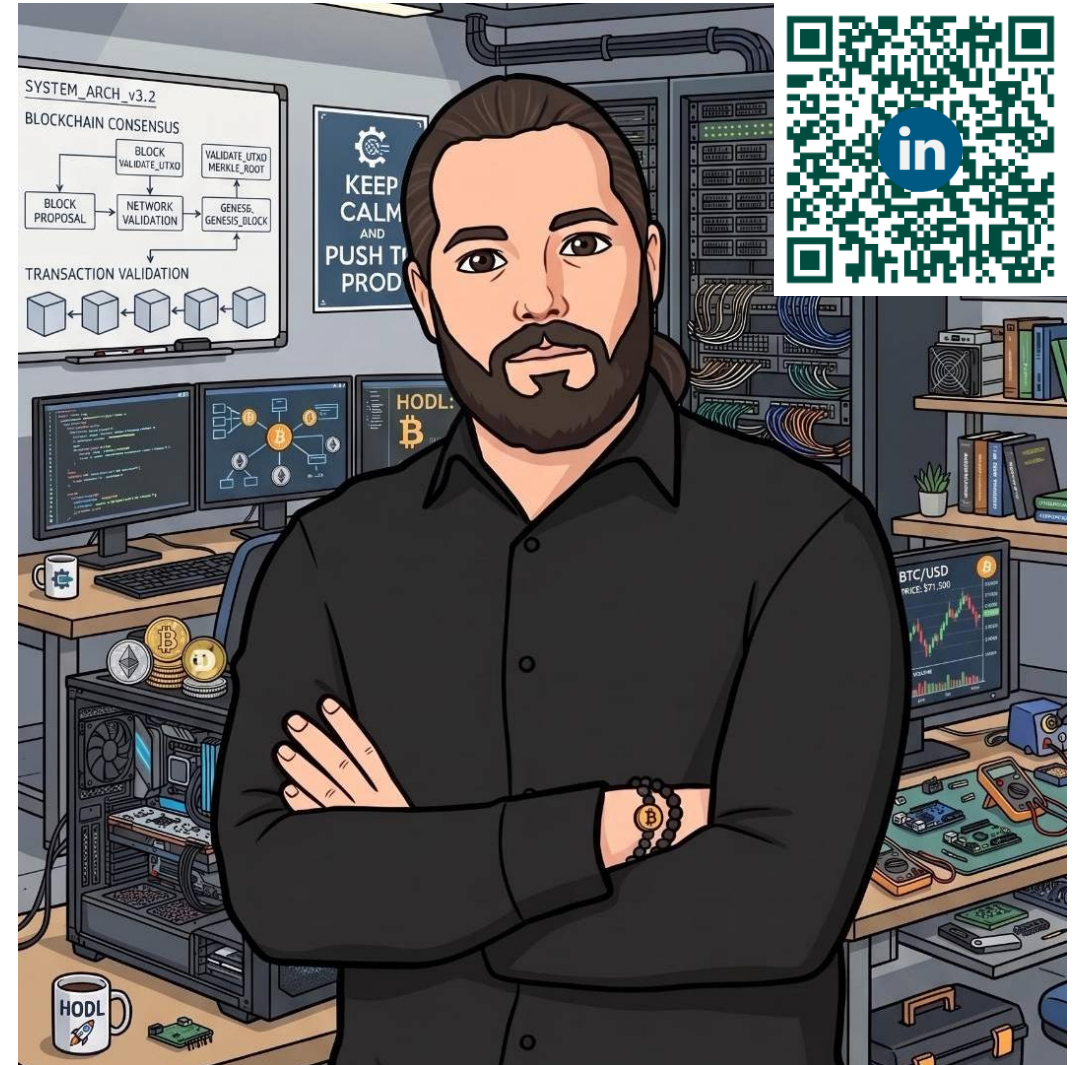
Free-time projects

- > Anubitux - Distro for cryptos

<https://anubitux.org>

- > OsintOps - knowledge sharing

<https://osintops.com>



Alessandro RELLA

Contacts

- > alessandro.rella@recoveris.io
- > https://t.me/stanley_k
- > <https://www.linkedin.com/in/alessandrorella/>

Working for

- > Recoveris - Blockchain Investigations Manager

<https://recoveris.io>



- > Former Italian LE
- <https://gdf.gov.it>

Free-time projects

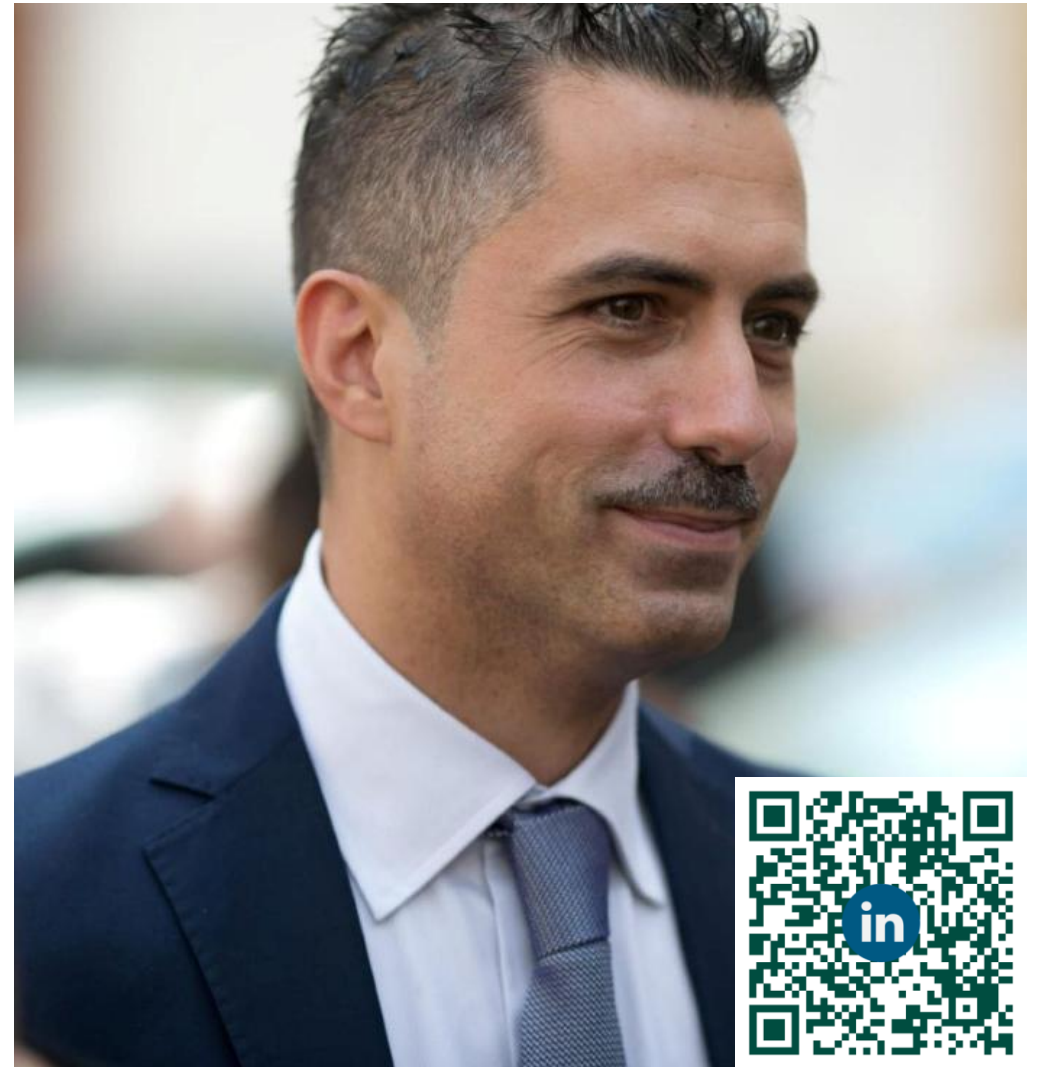
- > Anubix - Distro for cryptos

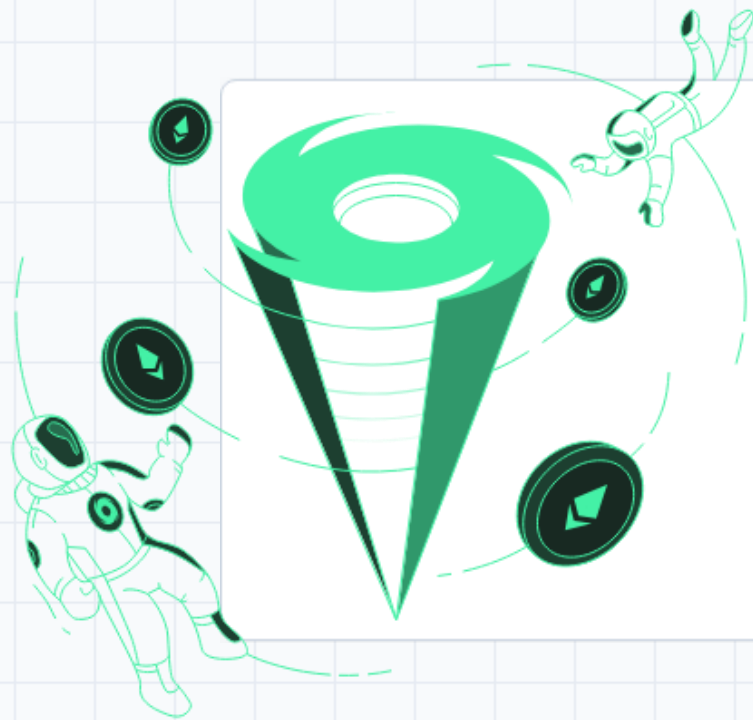
<https://anubix.org>



- > OsintOps - knowledge sharing

<https://osintops.com>





CONOSCERE TORNADO.CASH

Operazioni pratiche e meccanismi *on-chain*

COSA FA TORNADO.CASH?

Tornado Cash è una soluzione non-custodial decentralizzata per la tutela della privacy, basata sulla blockchain Ethereum.

- > Migliora la riservatezza delle transazioni interrompendo il collegamento on-chain tra gli indirizzi di origine e di destinazione.
- > Poiché le transazioni su Ethereum sono pubbliche per impostazione predefinita, gli autori delle minacce utilizzano i “coin mixer” per occultare il flusso di fondi illeciti.
- > Il protocollo utilizza gli smart-contract per accettare depositi da un indirizzo e consentire prelievi da un indirizzo completamente diverso.
- > Si basa in larga misura sulla crittografia avanzata piuttosto che su un sistema di fiducia centralizzato.



LA FASE DI DEPOSITO

Generazione dei *Secrets* e inserimento nei *Pool*

STEP 1: GENERAZIONE DELLA NOTA CRITTOGRAFICA

Prima che qualsiasi importo venga trasferito sulla blockchain, il browser (o lo script) dell'utente genera localmente i componenti crittografici necessari per la transazione.

1. Generato in locale

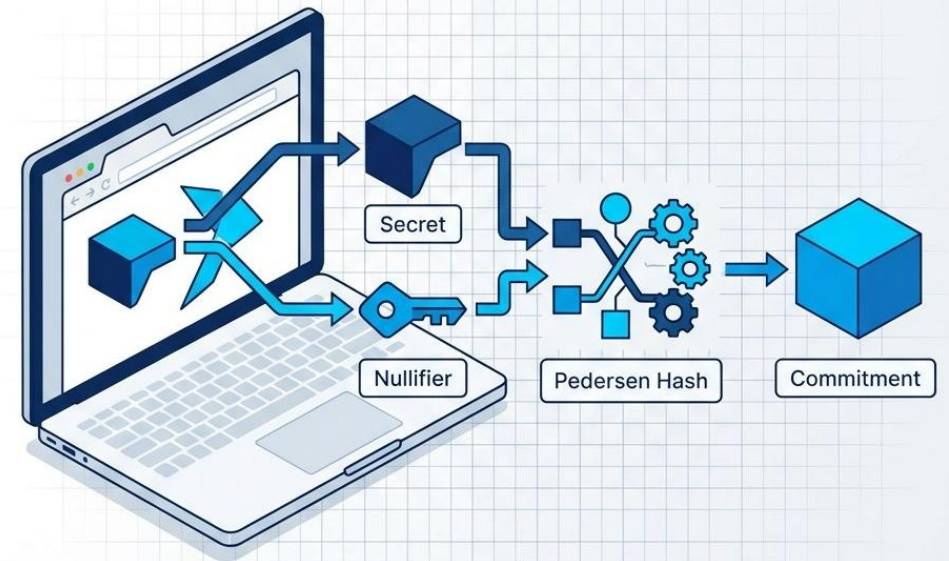
Il client genera due enormi numeri casuali:

- > **Secret:** verrà utilizzato in seguito per dimostrare la titolarità.
- > **Nullifier:** viene utilizzato in seguito per impedire la doppia spesa.

2. Creazione dell'hash del *Commitment*

Questi due numeri vengono sottoposti ad hash (utilizzando la funzione di hash di **Pedersen**) per creare il Commitment.

```
Commitment = Hash(Secret + Nullifier)
```



STEP 2: INVIARE IL DEPOSITO

 [Voting](#) [Compliance](#) [Docs](#)

 **Ethereum**   **Settings**

Deposit **Withdraw**

Token

ETH

Amount 

0.1 ETH 1 ETH 10 ETH 100 ETH

Connect

Statistics **100 ETH**

Anonymity set 

47677 equal user deposits

Latest deposits

47677. a day ago	47672. 3 days ago
47676. a day ago	47671. 3 days ago
47675. 2 days ago	47670. 3 days ago
47674. 3 days ago	47669. 3 days ago
47673. 3 days ago	47668. 3 days ago

STEP 2: INVIARE IL DEPOSITO



INVIARE LA TRANSAZIONE

L'utente invia una transazione Ethereum standard allo smart contract specifico di Tornado Cash (ad esempio, il pool da 10 ETH).

Payload: 10 ETH + il *Commitment* hash generato precedentemente.



UPDATE DEL MERKLE TREE

Lo smart contract riceve i fondi e inserisce il *Commitment* nel proprio Merkle tree interno (una struttura dati che registra tutti i depositi).



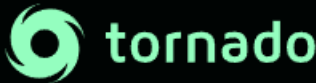
LA NOTA DI BACKUP

L'utente deve conservare in modo sicuro il *Secret* e il *Nullifier* originali (spesso rappresentati da una lunga stringa che inizia con `tornado-eth-10-`).
La loro perdita comporta la perdita definitiva dei fondi.

LA FASE DEL PRELIEVO

Prove con *zero-knowledge* e uscita dei fondi dal mixer

LA FASE DEL PRELIEVO

 [Voting](#) [Compliance](#) [Docs](#)

 **Ethereum**   [Settings](#)

Deposit

Withdraw

Note 

Recipient Address [Donate](#)

Withdraw

Statistics

100 ETH

Anonymity set 
47677 equal user deposits

Latest deposits

47677. a day ago	47672. 3 days ago
47676. a day ago	47671. 3 days ago
47675. 2 days ago	47670. 3 days ago
47674. 3 days ago	47669. 3 days ago
47673. 3 days ago	47668. 3 days ago

STEP 3: ELABORAZIONE DELLA PROVA (OFF-CHAIN)

Per effettuare un prelievo, l'utente deve fornire un indirizzo Ethereum nuovo di zecca e vuoto. Ma come fa a pagare la commissione *gas* necessaria per avviare la transazione di prelievo senza collegarsi a un vecchio wallet?

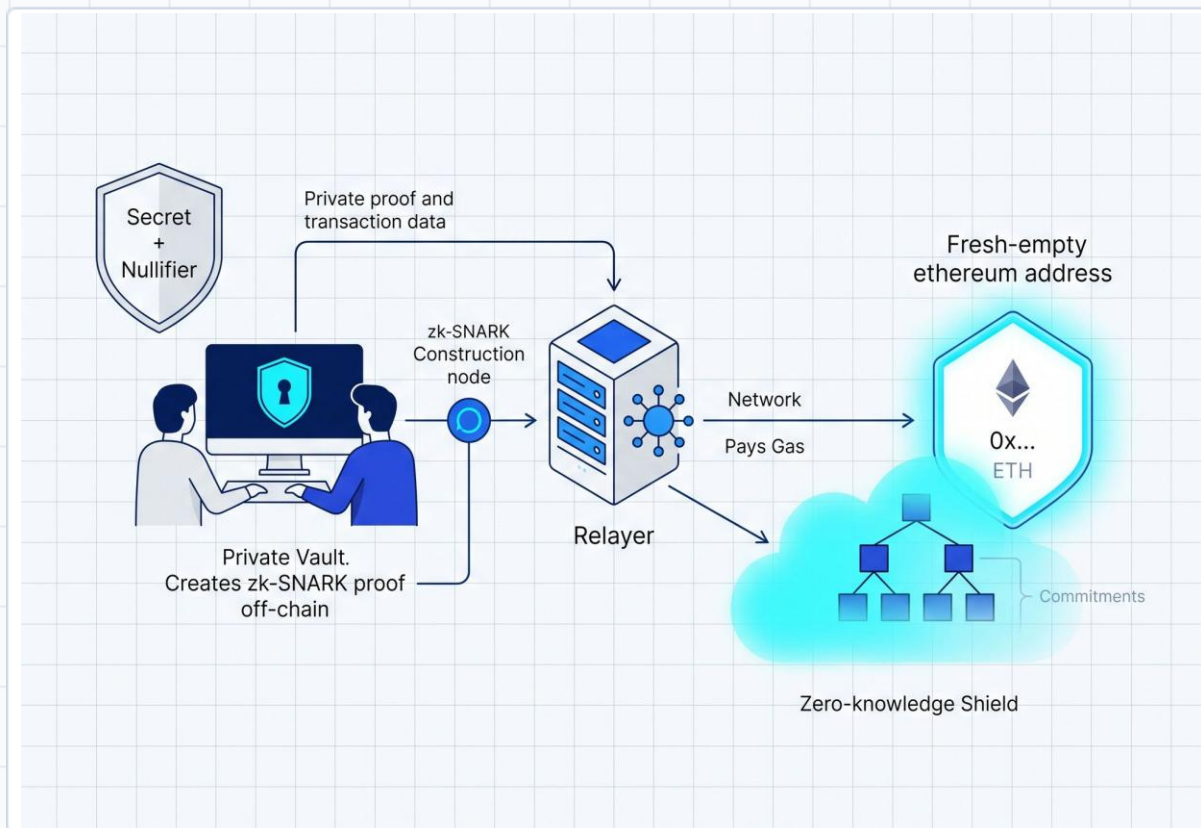
Il Relayer Network

Gli utenti utilizzano solitamente un “Relayer” decentralizzato. Il Relayer paga la commissione *gas* per la transazione su Ethereum e, in cambio, trattiene una piccola percentuale dei fondi prelevati.

Generazione dello *zk-SNARK*

Il client dell'utente utilizza la Nota salvata in precedenza (composta da *Secret + Nullifier*) per generare una *Prova* crittografica. Tale prova afferma sostanzialmente quanto segue:

"Possiedo il Secret e il Nullifier corrispondenti a uno dei Commitments attualmente presenti nel tuo Merkle tree, ma non ti dirò quale."



STEP 4: ESECUZIONE DEL PRELIEVO (ON-CHAIN)

L'utente invia la richiesta di prelievo allo smart contract tramite il **Relayer**. Il **payload** includerà:

- 1 La Prova:** il valore dello *zk-SNARK* generato in locale.
- 2 L'hash del Nullifier:** L'hash relativo esclusivamente al *Nullifier* della nota segreta generata precedentemente.
- 3 Il wallet di Destinazione:** Il nuovo wallet Ethereum.
- 4 Relayer Info:** L'indirizzo del Relayer e la sua commissione.

CONVALIDA E LIQUIDAZIONE DEL CONTRATTO

1. VERIFICA DELLA PROVA

Lo smart contract di Tornado Cash esegue complessi calcoli matematici on-chain per verificare la prova *zk-SNARK*.

- > Se i conti tornano, il contratto sa che l'utente ha effettivamente depositato dei fondi in precedenza.
- > Grazie alla crittografia Zero-Knowledge, il contratto non è in grado di sapere quale specifico deposito storico appartenga all'utente.

2. PREVENZIONE DEL *DOUBLE SPENDING*

Il contratto verifica l'hash del *Nullifier* inviato, confrontandolo con un elenco pubblico.

- > Se l'operazione è già stata registrata, viene rifiutata (qualcuno sta cercando di effettuare un prelievo due volte).
- > Se è nuovo, viene aggiunto all'elenco "spesi".
- > Il contratto provvede quindi a trasferire i fondi (al netto della commissione) al nuovo indirizzo di destinazione.

TRADE-OFF DEGLI UTENTI TORNADO.CASH

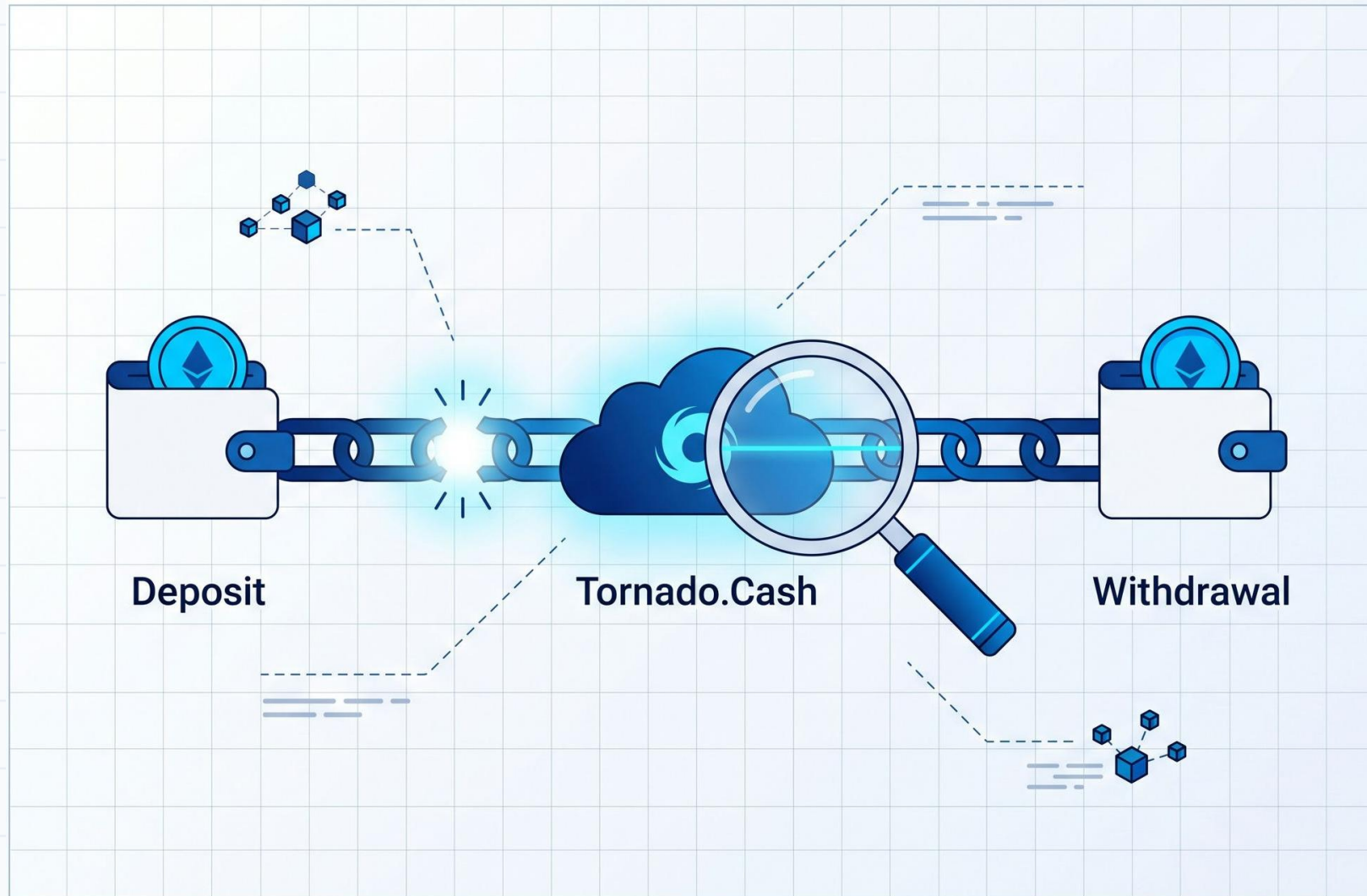


IN SINTESI: COSA È VISIBILE SULLA BLOCKCHAIN?

Elemento della transazione	Visibile sulla blockchain?	Implicazioni per gli Investigatori
Indirizzo di origine (mittente)	SI	Si conosce CHI ha inviato fondi al Mixer, QUANDO, e la DIMENSIONE della POOL selezionata.
L'hash "Commitment"	SI	È contenuto nel Merkle tree pubblico, ma sembra un insieme di dati casuali.
La Secret Note (Dati)	No	Memorizzato localmente dall'utente. Solo l'hash è pubblico.
Indirizzo di destinazione (beneficiario)	SI	Si può vedere chi ha ricevuto i fondi, ma il collegamento con il mittente è crittograficamente interrotto.
Indirizzo e commissione del Relayer	SI	I Relayers sono enti pubblici che facilitano il prelievo.

IN SINTESI: COSA NON È VISIBILE ON-CHAIN?

> UN COLLEGAMENTO VISIBILE E TRACCIABILE TRA L'ETH DEPOSITATO E L'ETH PRELEVATO





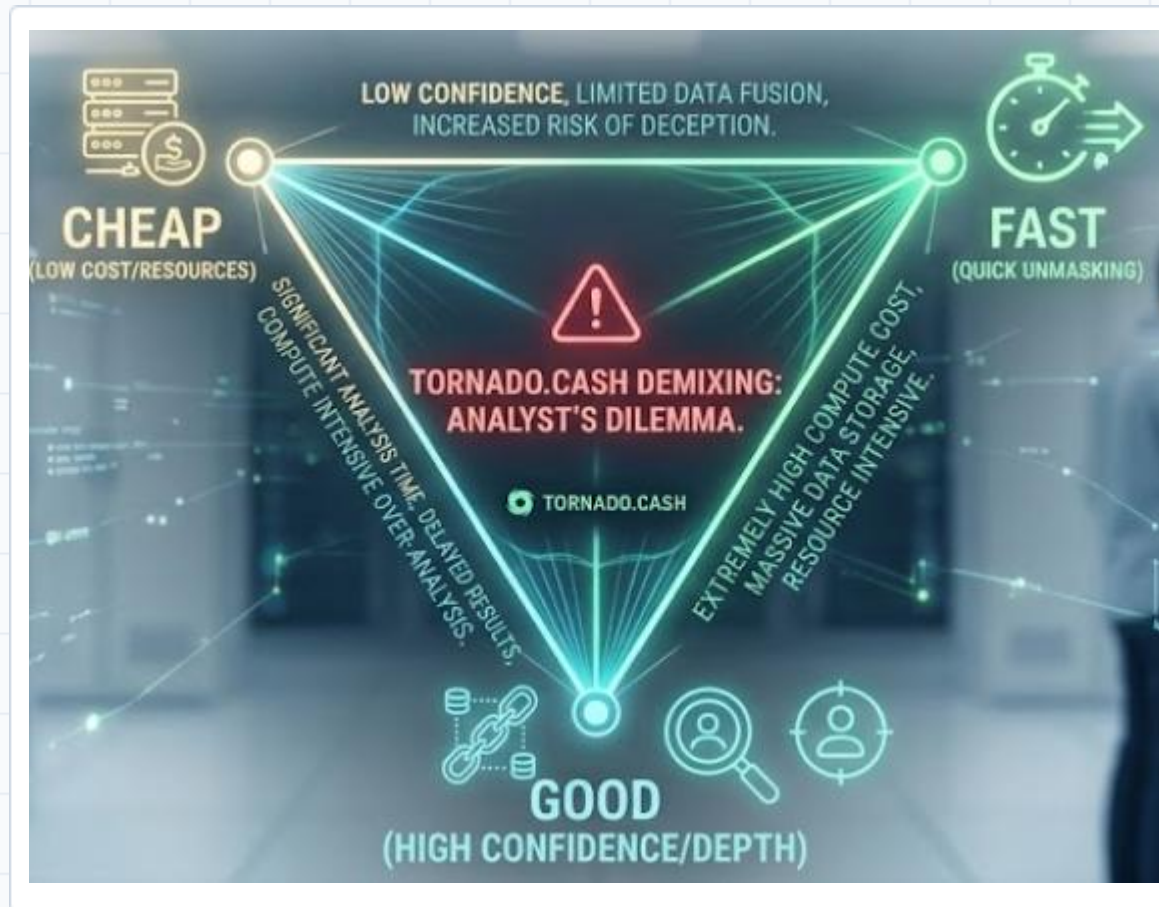
STRATEGIE DI DEMIXING

Come sfruttare le falle di OPSEC nelle indagini su crypto

IL FLUSSO DI LAVORO DI DEMIXING

Sebbene la crittografia alla base di Tornado Cash (zk-SNARKs) non sia stata violata, il **comportamento degli utenti** spesso compromette l'anonimato garantito dal protocollo.

- > Le forze dell'ordine e i professionisti della sicurezza si affidano a euristiche di “demixing”.
- > **Il Demixing non viola il protocollo**; analizza i metadati on-chain relativi ai depositi e ai prelievi.
- > Mettendo in correlazione i tempi delle transazioni, gli importi e le successive interazioni tra gli indirizzi, gli analisti possono collegare, in termini probabilistici, un mittente con il relativo destinatario.



ERRORI COMUNI DI OPSEC (EASY WINS)



Correlazioni temporali: se un utente deposita 100 ETH e ne preleva 100 ETH su un nuovo indirizzo esattamente 5 minuti dopo, l'intervallo di tempo così ristretto riduce notevolmente l'insieme di anonimato.



Raggruppamento in base alla dimensione dei blocchi: poiché TC utilizza pool fissi, chi ricicla denaro deve suddividere i fondi. Se vengono effettuati 10 depositi da 10 ETH ciascuno e un singolo nuovo indirizzo riceve 10 transazioni in entrata da 10 ETH ciascuna dal mixer, ciò costituisce una prova schiacciante della titolarità comune.



Riutilizzo degli indirizzi: a volte i criminali effettuano accidentalmente un prelievo verso un indirizzo precedentemente collegato a loro, oppure pagano le commissioni di gas per il prelievo utilizzando un portafoglio già noto, ripristinando così immediatamente la pista investigativa.



Interazione con un CEX: interazione con servizi identificabili nel breve termine. Prelevare dal mixer e depositare immediatamente su un exchange centralizzato (CEX) consente alle forze dell'ordine di richiedere i dati KYC tramite mandato.

INTEGRAZIONE DI ATTIVITÀ “UNMIXED”



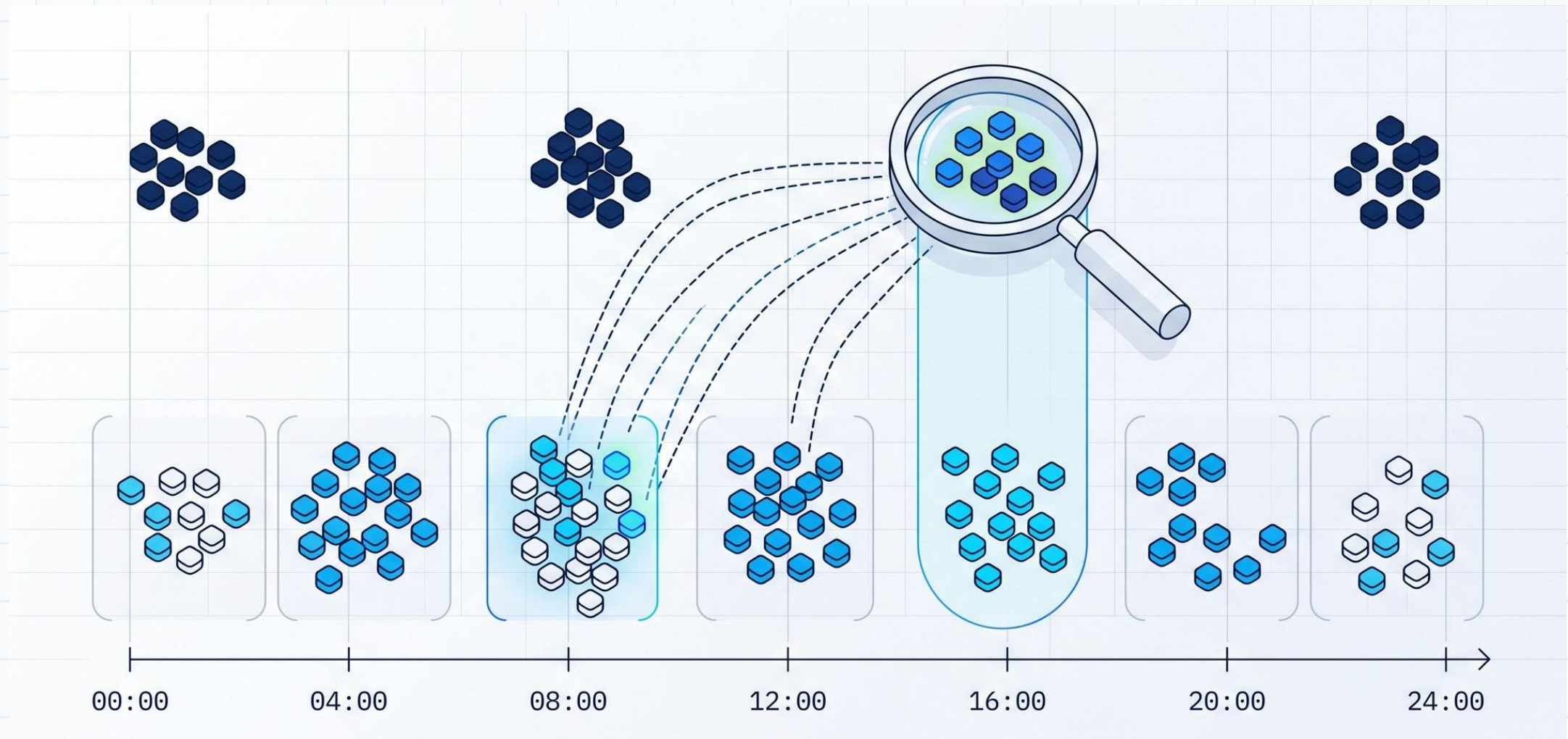
CONSOLIDAMENTO DI QUANTITÀ ESATTE DI ETH



CONSOLIDAMENTO DI QUANTITÀ ESATTE DI ETH DOPO ALCUNI “HOP”



PRELIEVI RAGGRUPPATI PER “ORARI”



ANALISI DEL COMPORTAMENTO DI TUTTI I PRELIEVI



CASE SCENARIO

- Servizio DeFi vittima di un attacco hacker nel Dicembre 2024
- Asset rubati da molteplici EVMs
- Asset confluiti in Ethereum e convertiti in ETH
- Asset inviati a Tornado.Cash (vari importi, con priorità sui più grandi disponibili)
- 545 ETH depositati (5x100 ETH, 4x10ETH, 5x10 ETH)



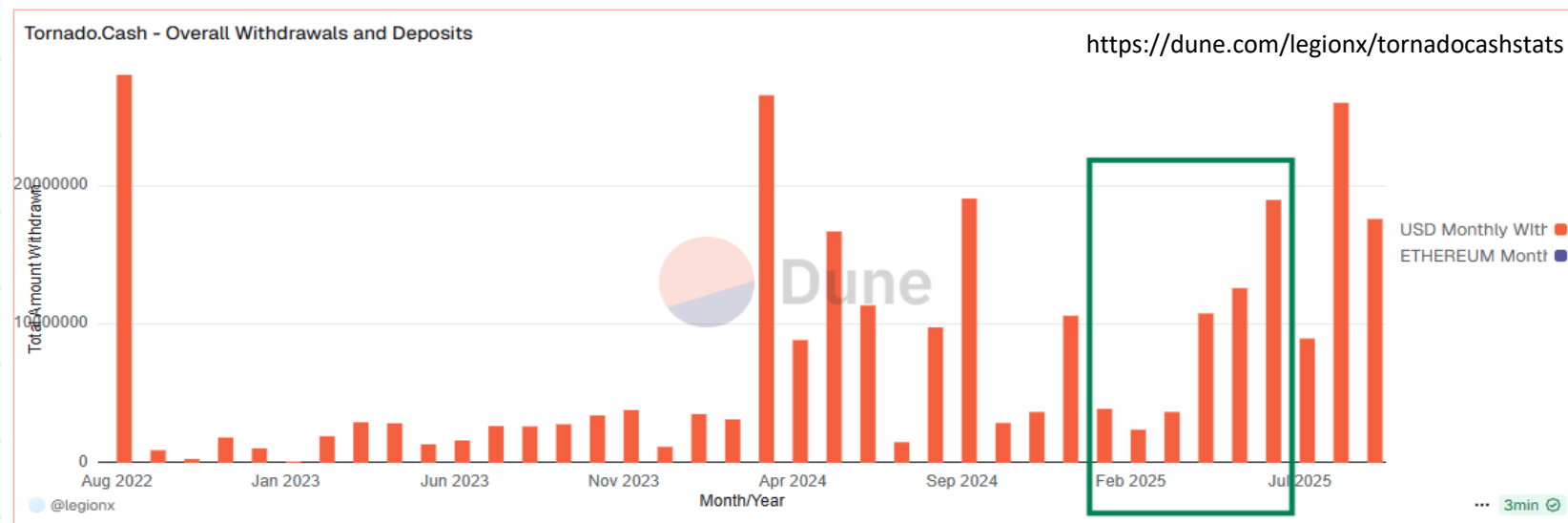
CASE SCENARIO: SFIDE

- Gli approcci “facili” non funzionano
- Ma accade qualcosa...

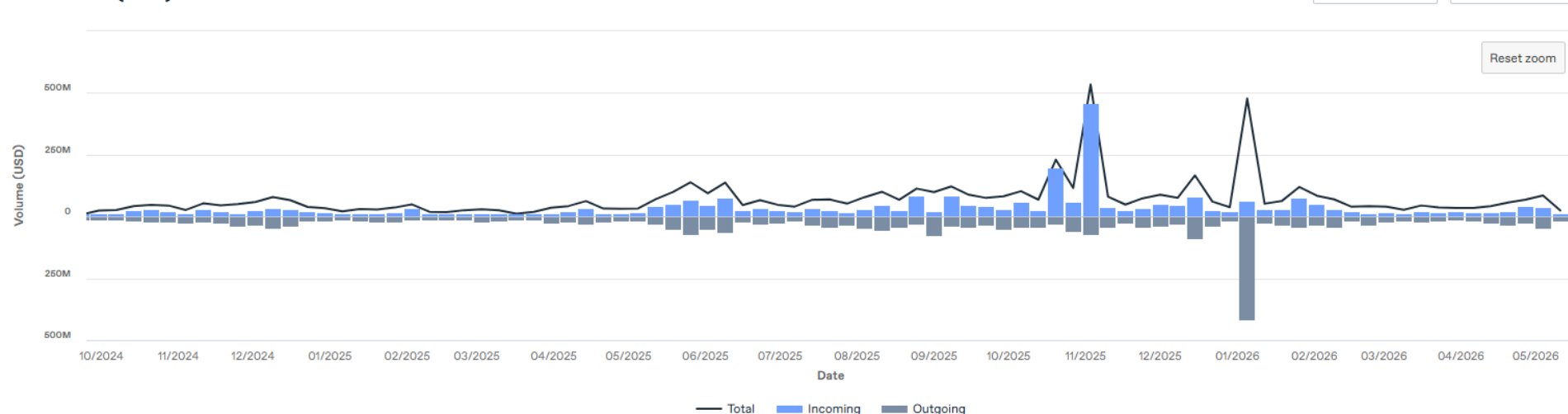


CASE SCENARIO: SFIDE

Il 21 febbraio 2025 sono stati sottratti a ByBit 1,5 miliardi di dollari in ETH, aumentando notevolmente la mole di dati da analizzare a causa dei fondi riciclati tramite il servizio Tornado.Cash.



Volume (USD)



FINGERPRINT / COMPORTAMENTO – CHE COSA SIGNIFICA?



RACCOLTA DI DATI COMPORTAMENTALI

1	Receiver Address	Receiver address occurrence	Receive	Receive	Relayer occur	Value	Value U	Graph		Automatic exposure	Exclude?	Behavior label	Consolidatio
								tracing ID	Tracing notes				
2336	dbf0909100574e7ead16afce26abec227d7db81d27c	2				10	26928.21		Arbitrum Foundation	YES			
2337	dbf0909100574e7ead16afce26abec227d7db81d27c	2				10	26928.21		Arbitrum Foundation	YES			
2338	dbf0x56684b5776f07f82782b30581b3fc9b6ef28240f	1				967	9.9549	26478.98	Mayan Finance	YES			
2339	9360xad2ddc34a00c8ebaec818bb7ad9029647aa62ee1	1				649	0.9936	2643.01	Mixin - ChangeNOW - CoinSpot - Coinbase - unknown smart contract - Bitrefill - Cryptomus - Mimic.fi	YES			
2340	dbf0xdc0ddca33bde1af82302bf285eba0d02a9e13f0a	4				967	9.9549	26478.96	Across Protocol	YES			
2341	dbf0xdc0ddca33bde1af82302bf285eba0d02a9e13f0a	4				967	9.9549	26478.93	Across Protocol	YES			
2342	dbf0xdc0ddca33bde1af82302bf285eba0d02a9e13f0a	4				967	9.9549	26478.98	Across Protocol	YES			
2343	dbf0xdc0ddca33bde1af82302bf285eba0d02a9e13f0a	4				967	9.9549	26478.97	Across Protocol	YES			
2344	9360x6c2ad65371c40d74c10881cc43c01ee8be95759c	1				413	0.9935	2642.68	deBridge	YES			
2345	9360x6340bf08cc3f37b4e1a7a0b963a323db7897c20	1				194	0.9935	2642.57	deBridge	YES			
2346	9360x6938c61cbab9f4c6842b542bb7f4f3b09199155b	1				456	0.9936	2643	deBridge	YES			
2347	2910x1fad1ef99b0f02f23b3a15c16d132007236a496f	1				280	99.5976	264919.7	h6Bridged to Arbitrum (same address), then 1 ETH transfers with LayerSwap, back to Ether on 0x86d9ca0c0554ef4cb1e9d36ccbcd6385e813d96 then split to multiple addresses, amounts about 10 ETH each	NO	YES	Arbitrum same address + LayerSwap 1 ETH + 10 ETH split and some fee collector	YES
2348	2910xc6135478883d14fbd3d77a791a0bb5860ddbbf39	1				270	99.5978	264920.32	h6Bridged to Arbitrum (same address), then 1 ETH transfers with LayerSwap, back to Ether on 0x9333a0a470d98655a92685a940ec56759603b1ba then split to multiple addresses, amounts about 10 ETH each	NO	YES	Arbitrum same address + LayerSwap 1 ETH + 10 ETH split and some fee collector	YES
2349	9360xed7a14ab80caadeb81758c21dba560eedccfd3a	1				232	0.9941	2644.26		YES			
2350	2910xf08b5b21df2028751431790a8e6d786c2669194	1				270	99.5979	264920.51	h6Bridged to Arbitrum (same address), then 1 ETH transfers with LayerSwap, back to Ether on 0xb649f1c9c097ee3ed2c2526f659b7f81a9fc5909 then split to multiple addresses, amounts about 10 ETH each	NO	YES	Arbitrum same address + LayerSwap 1 ETH + 10 ETH split and some fee collector	YES
2351	2910xdb7c4d74121cbd66cc6eb6f686875b6fc435d6f3	1				649	99.5677	264840.41	h6Bridged to Base with Across. Part bridged back to Ethereum with Stargate and sent to Railgun, part wrapped for Zerolend wrapped Ether, unwrapped to another address on Base, sent back to Ethereum with Stargate and Rhino brige. Rhino wd sent to Railgun. Stargate wd bridged with ChainFlip to Solana GSK8fKWCM3foFDfVv34qgJjHm5v7s3LkhrFaQfARpBE, forwarded to B1EYVLR2bP4a1QcR1HPJvghwoSkXmRF3fTmDmWcQEy2, pretty big address	NO	YES	Solana B1EYVLR2bP4a1QcR1HPJvghwoSkXmRF3fTmDmWcQEy2	
2352	9360x007f60147cf299b0cac409536d9caf69cab37f51	1				456	0.9933	2642.21		YES		Unspent	
2353	9360xad7d0a06f059ebc641da05f4f296da236547cb7e	2				160	0.993	2641.17		YES			
2354	9360xad7d0a06f059ebc641da05f4f296da236547cb7e	2				160	0.9929	2640.92		YES			
2355	9360x3162502b501e55e07b371ddc1aa48e635fd278e0	1				232	0.9938	2643.47		YES			
2356	dbf0x726932303fefb4ecd3fe592019ed45de9077cb9	1				270	9.9579	27303.72		YES			

L'IMPORTANZA DEI TAG

Total Workspace Withdrawals (Inc. Excluded)

79785.8518 ETH

Amounts by Combined Behavior Tags

Combined Tags	Occurrences	Total Received (ETH)
UNSPENT	80	6680.9987
LAYERZERO, TRON BLACKLISTED	67	4297.4859
OPTIMISM ARBITRUM HYPERLIQUID WAGYU	32	3187.2278
ZCASH	10	906.3138
LIFI, ONE, UNISWAP POOL	8	617.3181
UNSPENT, WASTEFEЕ, YELLOWCARD	5	500.0000
TC AGAIN, ZCASH	5	497.8916
LIFI, MOONSHOT, UNISWAP POOL	5	497.8377
FRANKLIN, LIFI, UNISWAP POOL	22	487.8468
WRAP USDT LIFI UNIDENTIFIED	13	444.0978
STETH, SUSD	5	310.1000
USDT LIFI BSC UNIDENTIFIED	6	302.0980
ASTER, HIFISWAP	5	300.7932
INK LAYERZERO	9	240.2714

Amounts by Individual Behavior Tags

Individual Tag	Occurrences	Total Received (ETH)
UNSPENT	87	7290.5316
LAYERZERO	73	4300.7627
TRON BLACKLISTED	67	4297.4859
OPTIMISM ARBITRUM HYPERLIQUID WAGYU	32	3187.2278
LIFI	37	1803.0025
UNISWAP POOL	53	1793.8008
ZCASH	16	1405.1991
TC AGAIN	126	787.1761
ONE	8	617.3181
YELLOWCARD	7	610.0000
MAYA	23	515.8870
WASTEFEЕ	5	500.0000
MOONSHOT	5	497.8377
FRANKLIN	22	487.8468

RICERCA DEI DATI

E	F	G	
Receiver address occurrence	Receiver	Receiver	Relayer
1			0x03392600086874456e
10			
3			
8			0x000000cd6521ed1a65
10			
10			
1			0x0e9d9a828247f5eed7
1			0x03392600086874456e
6			0xc7c3c87603c5595510
1			0xc49415493eb3ec64a0
1			0x4750bcfcc340aa4b31f
3			0x3a1d526d09b7e59fd8
5			0xc7c3c87603c5595510
5			0xc7c3c87603c5595510
5			0xc7c3c87603c5595510
5			0xc7c3c87603c5595510
1			0x4750bcfcc340aa4b31f
1			0xc49415493eb3ec64a0
1			0xc49415493eb3ec64a0
13			0x4af043aca08bbe1fa2a
13			0x4af043aca08bbe1fa2a
13			0x4af043aca08bbe1fa2a
1			0xf0bf3c1d67afa6c48b9f
1			0xf0bf3c1d67afa6c48b9f
1			0x0e9d9a828247f5eed7
4			0x3a1d526d09b7e59fd8
4			0x3a1d526d09b7e59fd8
4			0x3a1d526d09b7e59fd8
4			0x3a1d526d09b7e59fd8
2			0x3a1d526d09b7e59fd8

is there a behavior or similar behaviors that were encountered for a total of about 555 ETH (more or less)?



Referenced: A1:T6464

Analysis steps

There are several behaviors with a total value of approximately 555 ETH (more or less).

Here are the behaviors and their total values:

- **Symbiosis OTC Tron:** 539.7271 ETH
- **UniSwap pool:** 560.0000 ETH

Other behaviors that fall within a 10% range of 555 ETH include:

- **Arbitrum Base Optimism unspent:** 500.0000 ETH
- **Zoomex:** 500.0000 ETH
- **unspent wBTC:** 599.1305 ETH
- **LiFi + Binance Kraken:** 600.0000 ETH
- **Unspent Arbitrum and Optimism:** 600.0000 ETH
- **Lido AAVE:** 603.0000 ETH
- **USDT to Binance:** 603.0000 ETH

Please note that this analysis assumes the 'Value' column directly represents the amount in ETH. If the 'Value' column contains different cryptocurrencies, this interpretation would be inaccurate.

Insert Copy

RICERCA DEI DATI

I dati devono essere raccolti (quasi) manualmente

Potrebbe essere necessaria un'analisi complessa

Il tracciamento automatico non supporta alcuni servizi

È molto probabile che siano coinvolte più blockchain

Potrebbero essere necessari dati off-chain

VANTAGGI

Si possono “*porre domande*” ai dati

È possibile gestire enormi quantità di dati

Si possono analizzare dati provenienti da più fonti, se **opportunamente normalizzati**

Lo stesso set di dati può essere utilizzato in più casi

Risultati facili da aggiornare

LIMITAZIONI

È necessario analizzare tutti i prelievi, al fine di escluderli e soddisfare gli standard previsti dai vari ordinamenti giuridici

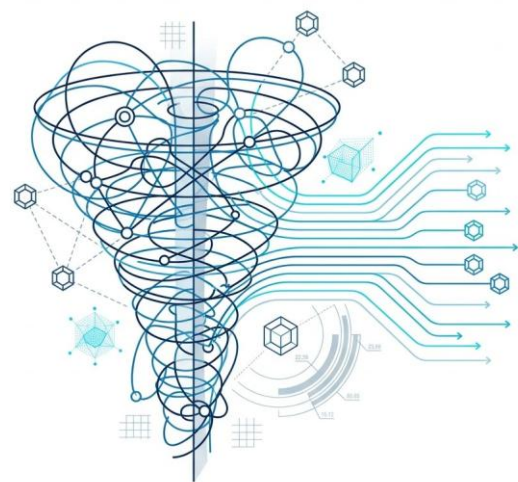
L'analisi può richiedere **molto** tempo

È possibile ottenere più di un candidato (potrebbero essere necessari dati off-chain per la convalida)

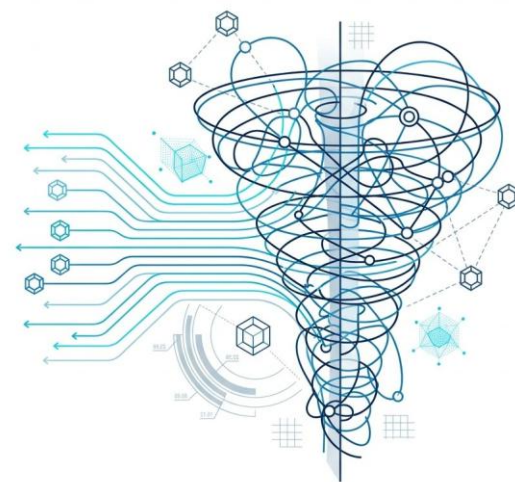
I dati possono subire variazioni (nuovi prelievi, movimenti di attività successivi all'analisi, nuove attribuzioni, ecc.)

MATRICE DEL LIVELLO DI AFFIDABILITÀ NEL TRACCIAMENTO

TIPO DI INDICATORE	MODELLO COMPORTAMENTALE OSSERVATO	LIVELLO DI AFFIDABILITÀ
Corrispondenza esatta	Combinazione specifica di importi frazionati irregolari depositati e prelevati contemporaneamente.	Alta (Quasi Certa)
Riutilizzo degli indirizzi	L'indirizzo di prelievo condivide la cronologia delle transazioni (o la fonte di approvvigionamento del gas) con l'indirizzo di deposito.	Alta (Link determinante)
Basato sul tempo	Fondi prelevati pochi minuti o poche ore dopo un attacco hacker che ha avuto grande risonanza mediatica.	Media (Forte Connessione)
Consolidamento	Diversi indirizzi di uscita del mixer finiscono per inviare fondi a un unico indirizzo di deposito di un exchange centralizzato.	Media - Alta
Comportamento	Stesso comportamento on-chain utilizzato per trasferire un importo in ETH corrispondente ai depositi	A seconda dei risultati



DOMANDE?





recoveris
GRAZIE



umberto.buonora@recoveris.io alessandro.rella@recoveris.io

