SALA AML

AML 2.0: il ruolo della forensica on-chain

Francesco Codega
Operations Lead, CheckSig

CLEAR SUMMIT 2026

CHECKSIG CLEAR

Agenda

AML & Asset Digitali: dal Problema alla Soluzione
Il problema, i rischi per le istituzioni finanziarie, perché la forensica on-chain è fondamentale

Demo
Scenari simulati: tracciamento fondi, identificazione controparti, risk scoring

Conclusione & Q&A
Sintesi e punti forti, domande

01

AML & Asset Digitali: dal Problema alla Soluzione

Il Mercato Crypto: Una Realtà in Rapida Espansione

$2,5T+

Capitalizzazione di mercato globale

560M+

Utenti crypto attivi nel mondo

€3B+

Asset detenuti da italiani su exchange

Insight chiave

- Le criptovalute non sono più una nicchia speculativa
- Istituti finanziari esposti in modo crescente
- I clienti con grandi patrimoni detengono asset crypto significativi

Necessità urgente di strumenti di controllo adeguati

I Rischi per le Istituzioni Finanziarie

AML / CFT

Riciclaggio di denaro e finanziamento al terrorismo attraverso asset digitali — **esposizione regolatoria diretta**

Frode e Truffa

Scam, phishing e schemi Ponzi che coinvolgono **fondi già introdotti nel circuito bancario tradizionale**

Compliance

DORA, MiCAR, normativa EBA: **obblighi di due diligence su controparti che operano con asset digitali**

Reputazione

Associazione involontaria a wallet sanzionati (OFAC, UE) o ad attività criminali — **danno reputazionale immediato**

La Blockchain: Trasparenza Pubblica e Pseudonimato

Trasparenza

- Ogni transazione è registrata in modo permanente e pubblico
- L'intera storia di ogni address è visibile on-chain
- Impossibile cancellare o alterare i dati storici
- Verificabile da chiunque in qualsiasi momento

Pseudonimato vs Anonimato

- Gli indirizzi non contengono dati identificativi reali
- Chiunque può creare wallet multipli senza registrazione
- Le identità reali non sono visibili direttamente
- Senza strumenti avanzati, il tracciamento è impossibile

Travel Rule: Passi avanti ma...

- La Travel Rule obbliga gli Exchange a trasmettere le informazioni su ordinante e beneficiario per ogni trasferimento crypto sopra i 1.000€, esattamente come avviene nei bonifici bancari
- Se l'Exchange riceve da un indirizzo provato non c'è però modo di ottenere informazioni sull'origine legittima dei fondi: si rende necessario avere strumenti per approfondire

Perché gli Strumenti Tradizionali Non Bastano

Limiti Strumenti Tradizionali

- Sistemi AML progettati per flussi bancari, non per blockchain
- KYC non applicabile direttamente a indirizzi
- Impossibile tracciare la provenienza reale dei fondi e nessuna visibilità sulle controparti dietro un indirizzo
- Ritardi nell'aggiornamento delle blacklist e sanction list
- Audit trail frammentato: dati on-chain non integrati

Sfide Specifiche Crypto

- Pseudonimato: nessun nome associato agli indirizzi
- Complessità intrinseche dell'ecosistema:
  - Transazioni senza intermediari verificati (DeFi e DEX)
  - Tecniche di oscuramento volontario dell'origine (Mixer)
  - Scambio asset tra blockchain diverse (Bridge)
  - Coin con crittografia avanzata (Monero, Zcash):
- Velocità: transazioni irreversibili in pochi minuti

Processo End-to-End: dal Cliente al Regolatore

01
Richiesta Onboarding
Il cliente fornisce i propri dati

02
KYC & Screening
Verifica identità, screening LSEG World-Check, AML policy

03
Forensica On-Chain
Know Your Transaction (KYT), Tracciamento fondi, Risk scoring

04
Valutazione Rischio
Esposizione diretta, Controparti, Alert automatici

05
Decisione
Basso / Medio o Alto rischio

Rischio Basso / Medio

✓ ACCETTAZIONE

- Onboarding completato, fondi accettati nel circuito
- Se rischio medio:
  - richiesta di documentazione aggiuntiva sull'origine dei fondi
  - intervista diretta al cliente per giustificare le controparti rischiose
  - monitoraggio più frequente delle transazioni successive

Rischio Alto

✕ RIFIUTO & SEGNALAZIONE UIF

- Blocco immediato dei fondi ricevuti
- Segnalazione all'Unità di Informazione Finanziaria (UIF)
- Dossier forense completo allegato alla segnalazione

CHECKSIG CLEAR

Blockchain Intelligence: Il Ruolo di Chainalysis

Cos'è Chainalysis

- Leader mondiale nell'analisi forense blockchain
- gestisce il più vasto database del settore che associa indirizzi blockchain anonimi a entità del mondo reale
- Usato da FBI, Europol e oltre 700 istituzioni tra cui CheckSig

Nel 2025 i fondi ricevuti da indirizzi considerati illeciti ammontavano a 154 mld di dollari, nella maggior parte (84%) in stablecoin; questa fetta risulterebbe invisibile senza l'utilizzo di strumenti dedicati all'analisi on-chain. (Fonte: Chainalysis Crypto Crime Report 2026)

Funzionalità Principali

Reactor

Cardine dell'investigazione forense che permette di mappare i flussi collegando indirizzi anonimi a entità reali (exchange, darknet market, truffatori, ...)

KYT (Know Your Transaction)

Automatizza lo screening delle transazioni in tempo reale, segnalando attività sospette o fondi provenienti da fonti illecite

Il Valore della Forensica On-Chain per le Istituzioni Finanziarie

Compliance Rafforzata

Dimostrare alle autorità di vigilanza la piena conformità AML/CFT in ogni relazione con controparti crypto

Riduzione del Rischio

Identificare proattivamente wallet ad alto rischio prima che i fondi entrino nel circuito bancario

Audit & Reportistica

Generare evidenze documentali complete per audit interni, revisori e organi di controllo

02

Demo

Scenario simulato — Chainalysis Reactor in azione

Prima di Iniziare: Concetti Essenziali per la Forensica

Indirizzo o Address

Identificatore alfanumerico univoco (es. 1A2B3C...). Come un IBAN, ma senza nome associato.

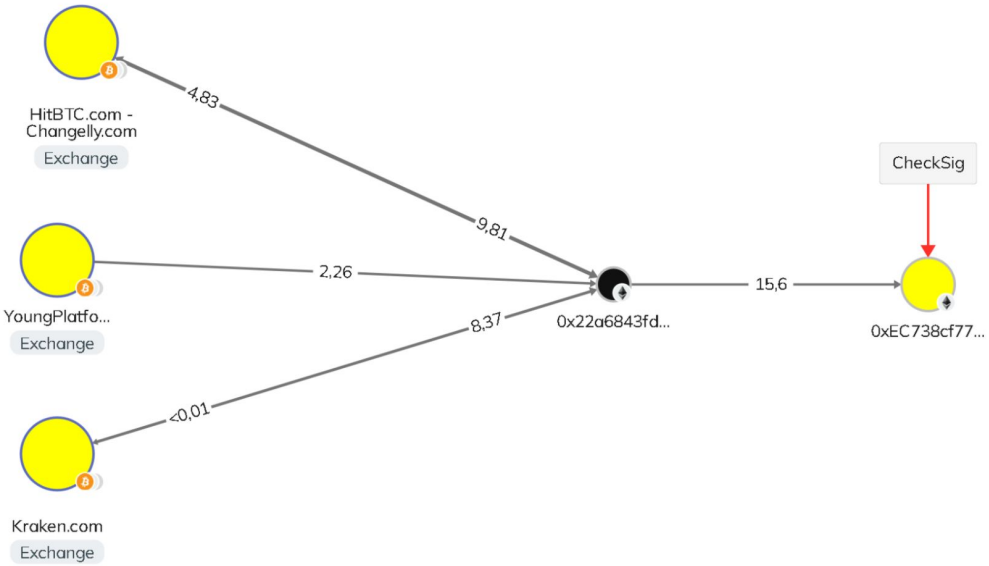
Transazione (Tx)

Trasferimento di valore tra indirizzi, registrato in modo permanente e pubblico nella blockchain.

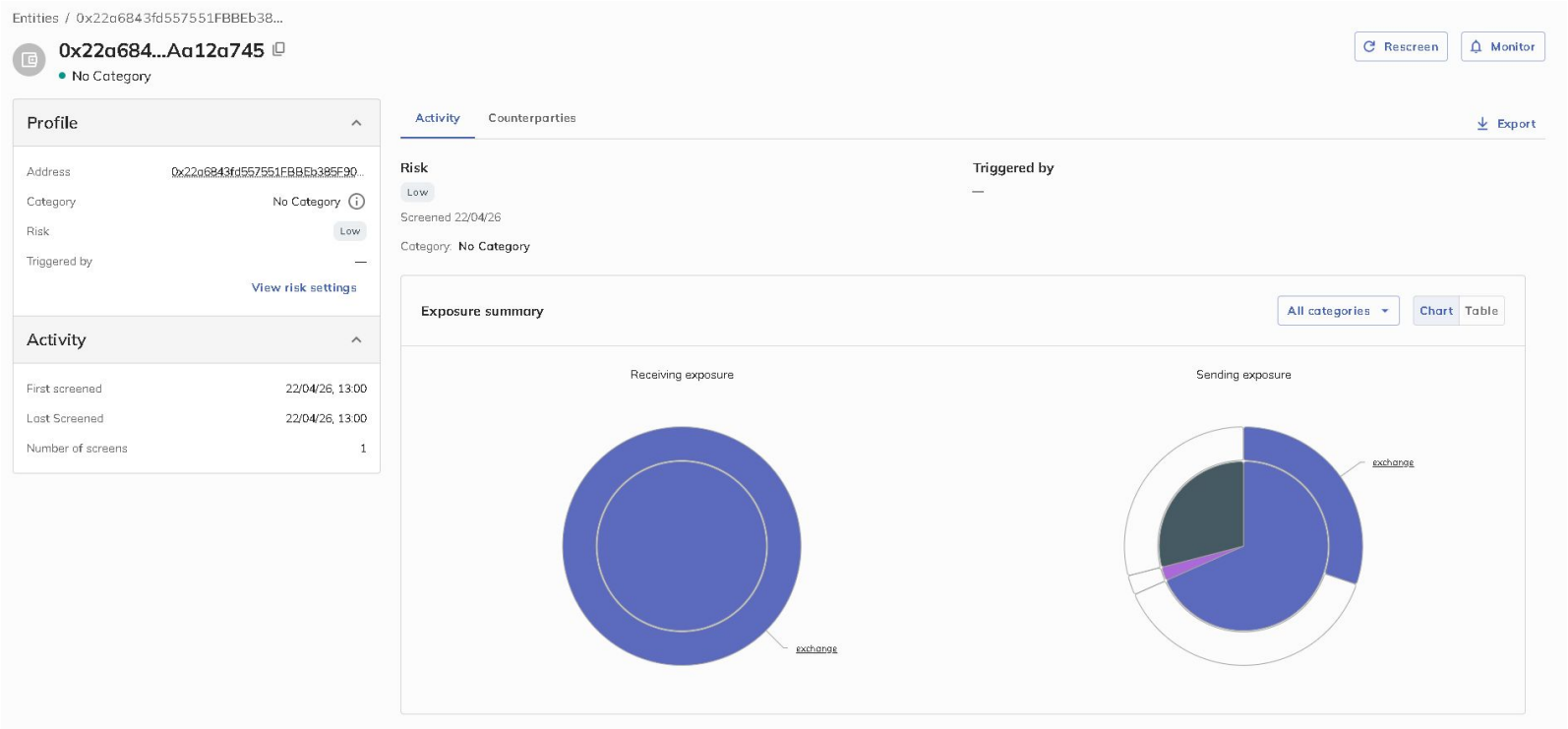
Cos'è il Transaction Tracing

- Ricostruzione del percorso dei fondi dalla sorgente alla destinazione finale
- Identifica se i fondi provengono da indirizzi noti come illeciti (darknet, hack, scam) o entità riconosciute (Exchange, Custodial, ...)

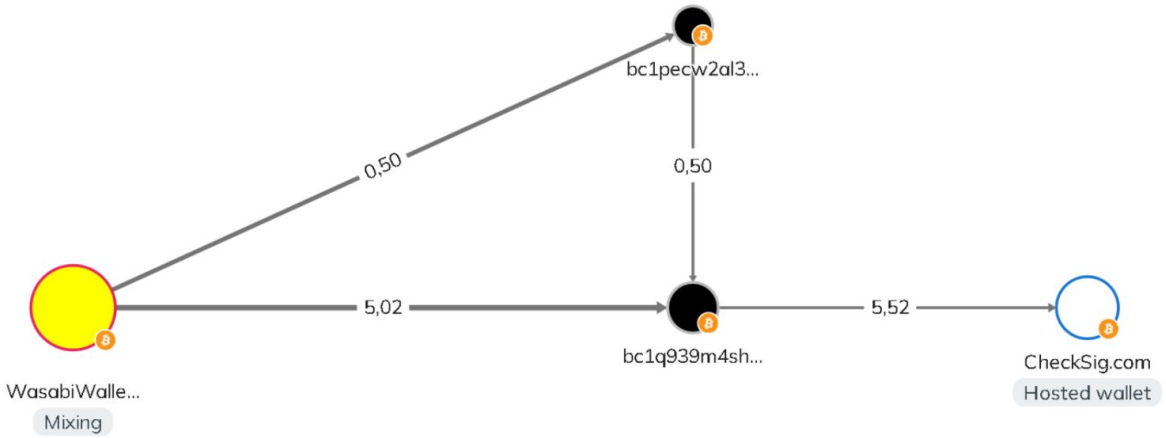
Caso 1: Rischio Basso – Reactor



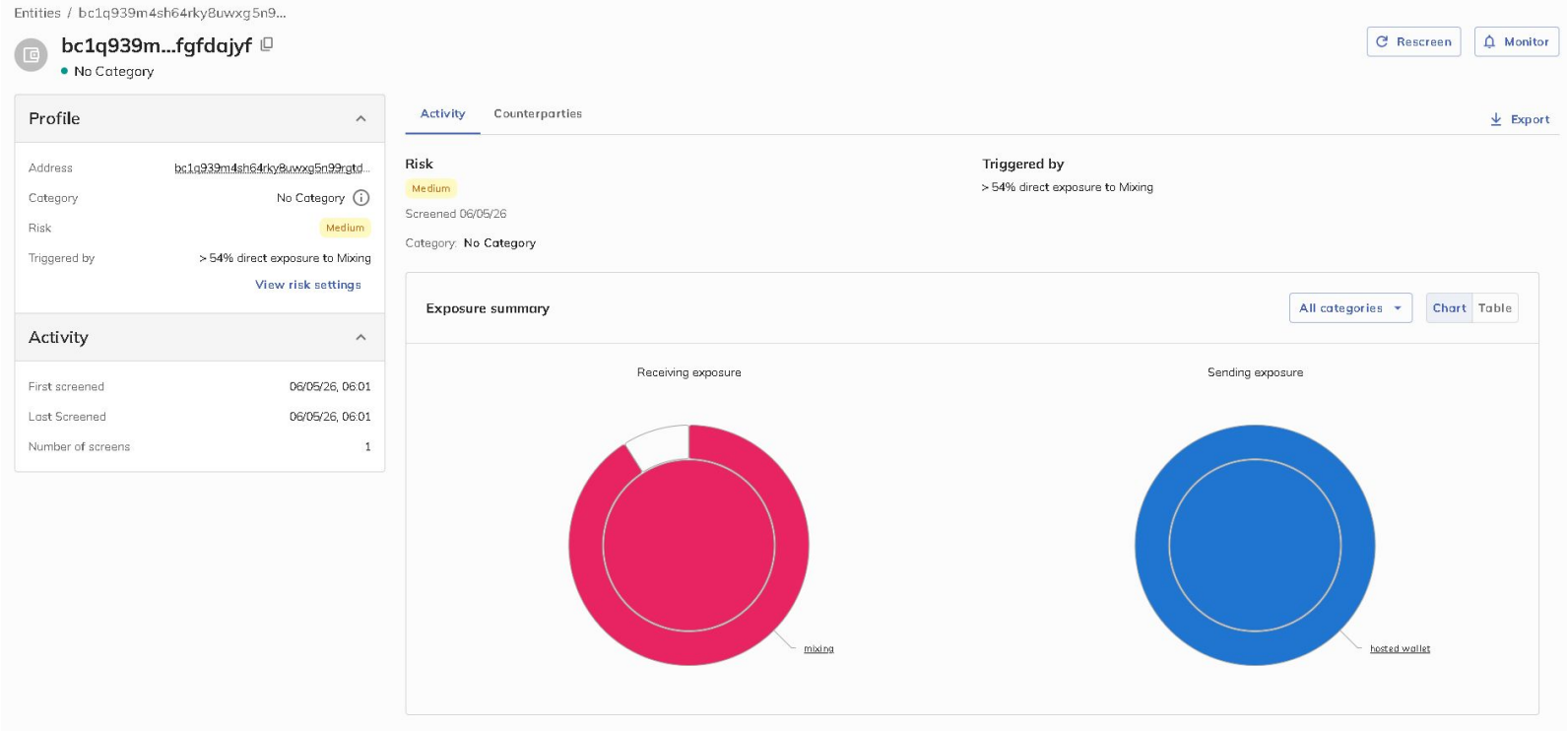
Caso 1: Rischio Basso – KYT



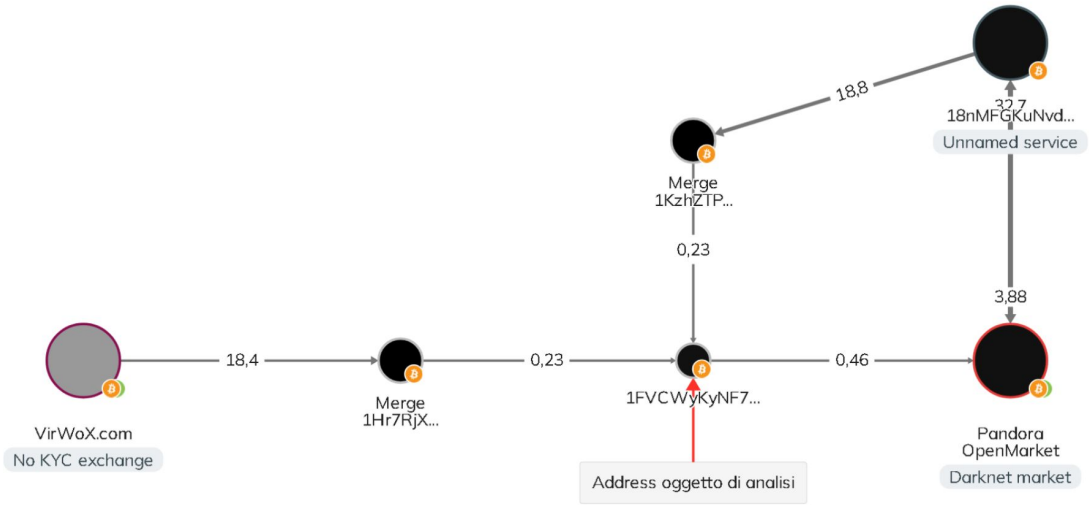
Caso 2: Rischio Medio – Reactor



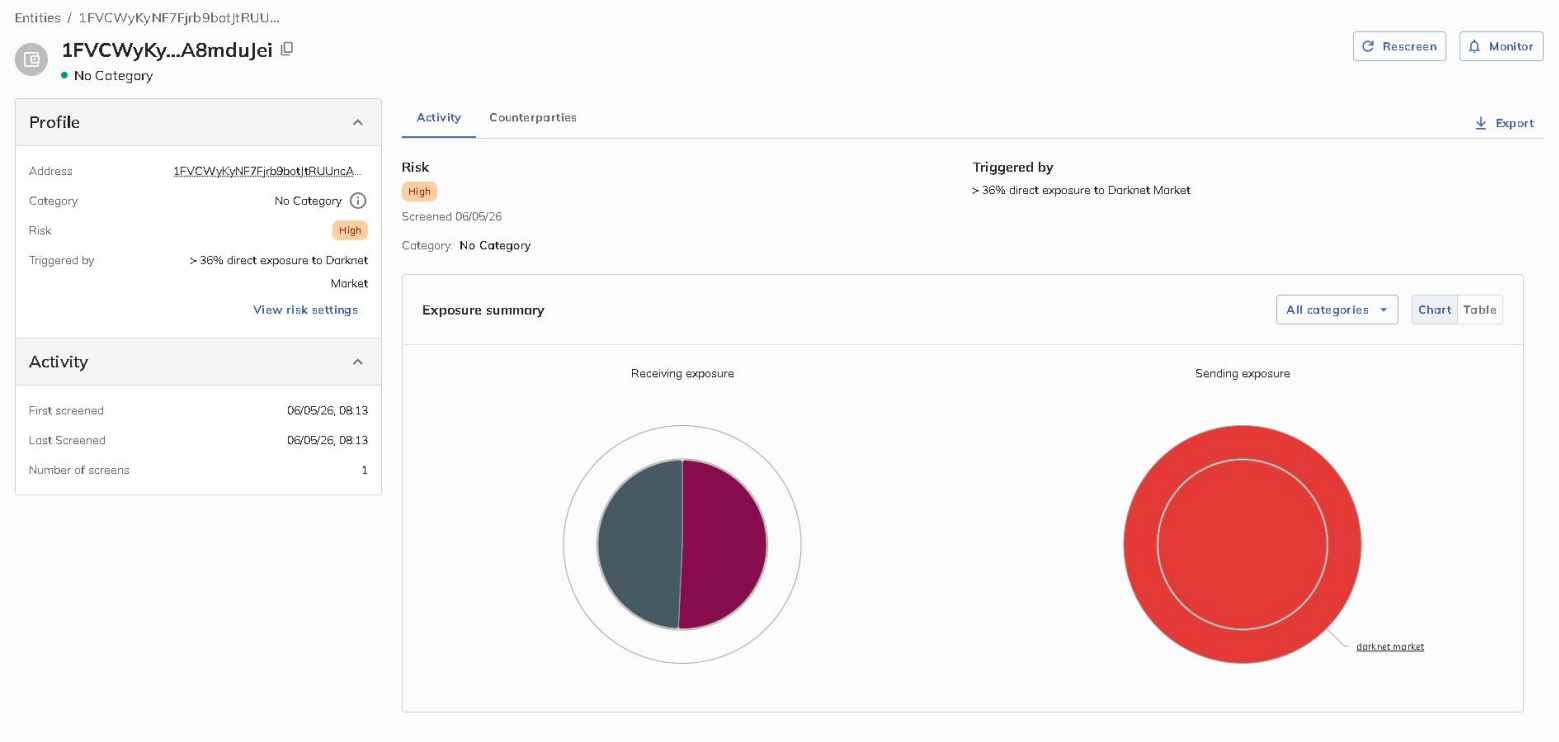
Caso 2: Rischio Medio – KYT



Caso 3: Rischio Alto - Reactor



Caso 3: Rischio Alto - KYT



03

Conclusione & Q&A

Punti Chiave: Cosa Abbiamo Imparato Oggi

01

Il rischio crypto è reale e rilevante per le istituzioni finanziarie

Oltre 560M di utenti crypto nel mondo: i vostri clienti già detengono asset digitali. Il rischio è già nella vostra base clienti.

02

Gli strumenti tradizionali non sono sufficienti

I sistemi AML e KYC standard non sono progettati per la blockchain: serve un layer aggiuntivo di blockchain intelligence.

03

La blockchain è trasparente, non opaca: si può investigare

Ogni transazione è pubblica e permanente. Con gli strumenti giusti, il tracciamento è possibile e affidabile.

04

CheckSig Clear: soluzione operativa completa per le istituzioni finanziarie

Due diligence, monitoring continuo, reportistica forense: un processo integrato e conforme alle normative vigenti.

SECONDO PIANO

Assisti alla plenaria di chiusura in auditorium

CLEAR SUMMIT 2026

CHECKSIG CLEAR