SALA TECHNOLOGY & OPERATIONS

Gestione sicura dei digital asset: tra custodia e cybersecurity

Mattia Coffetti
Chief Information Security Officer, CheckSig

Matteo Sciolla
Head of Custody, CheckSig

CLEAR SUMMIT 2026

CHECKSIG CLEAR

Chi siamo

Mattia Coffetti
Chief Information Security Officer

- Background CIO/CISO in ambienti mission-critical
- Top 10 mondiale in gare di Incident Response e Cyber Intelligence
- Focus: sicurezza applicata ai digital asset
- https://www.linkedin.com/in/mcoffetti

Matteo Sciolla
Head of Custody

- Computer Engineering, University of Pennsylvania
- In CheckSig dal 2023: ha guidato lo sviluppo della Client Area
- Architettura software per la custody: TypeScript, AWS
- https://www.linkedin.com/in/m-sciolla

Unione tra cybersecurity e custody: il controllo sui digital asset nasce qui

CHECKSIG CLEAR

Cybersecurity e digital asset

La sicurezza la conoscete già. Qui cambia il controllo.

Mattia Coffetti | Chief Information Security Officer

Digital Asset

Sicurezza controllo e modello operativo

Le crypto non sono “solo un nuovo asset”

sono un nuovo modello di controllo

La sicurezza non si improvvisa

servono competenze e processi specifici

Il modello vincente non è il fai-da-te

è l’integrazione con partner specializzati

CHECKSIG

Perché parla a tutti voi

Tre prospettive, una stessa decisione operativa

1. **Sicurezza e infrastruttura**
   Le competenze che già usate restano valide. Cambia come va progettato il controllo.

2. **Governance, rischio e compliance**
   Non è una solo scelta tecnologica. È una scelta di modello operativo.

3. **Distribuzione e cliente finale**
   La domanda è già sulla scrivania. Servono criteri per la risposta.

Stessi principi, nuovo controllo

Quello che conoscete già

- gestione del rischio
- segregazione dei ruoli
- controlli operativi e compliance

Quello che cambia

- controllo più diretto degli asset
- transazioni irreversibili
- minore tolleranza all'errore operativo
- nuovi rischi legati a operatori statali

Non cambia il principio della sicurezza. Cambia come va progettato il controllo.

Il cambio di paradigma nella security

Velocità

Il tempo per reagire si riduce significativamente

Le difese pensate per tempi lunghi non bastano più

Evoluzione degli scenari

Non difendi più solo da minacce note

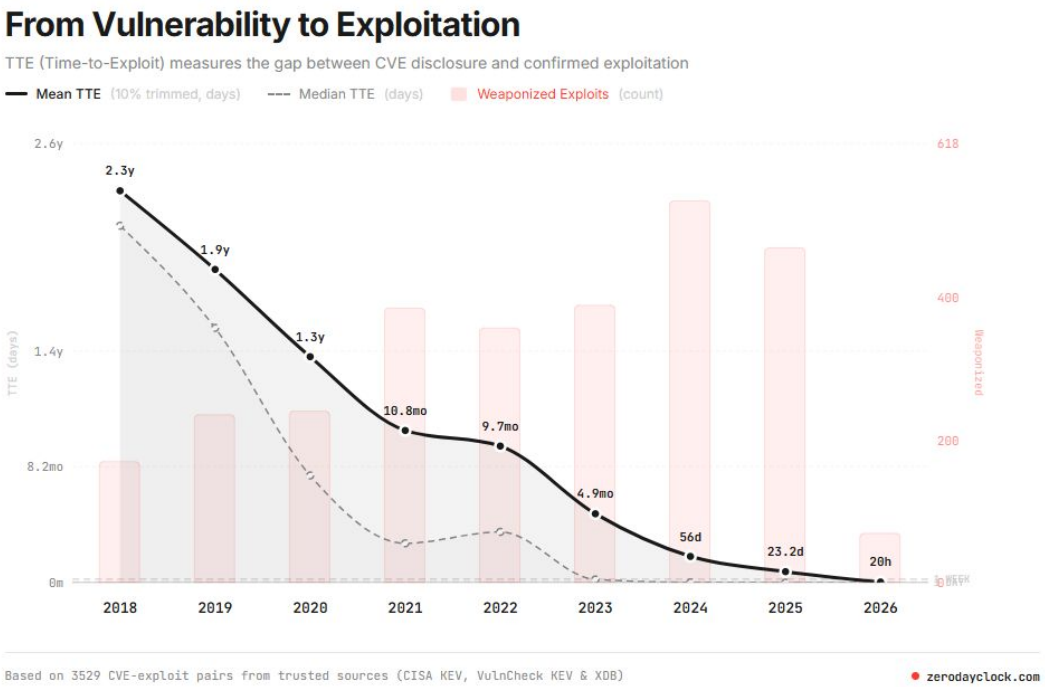
Anche da falle ignote al produttore stesso (zero-day) e da componenti di terze parti compromesse

Attori evoluti

**Non sono attacchi opportunistici.
Sono operazioni.**

Gruppi legati a stati/nazioni e organizzazioni criminali strutturate

Da 2,3 anni a 20 ore



Time-to-Exploit Milestones

When mean time-to-exploit crosses each threshold

1 Year — REACHED — ~2021	1 Month — REACHED — ~2025
1 Week — REACHED — ~2026	1 Day — REACHED — ~2026
1 Hour — PROJECTED — ~2026	1 Minute — PROJECTED — ~2028

Fonte: zerodayclock.com

CHECKSIG CLEAR

Dove nasce davvero il rischio operativo

Modelli tradizionali di custodia

Software di orchestrazione di terze parti

Codice non controllato direttamente

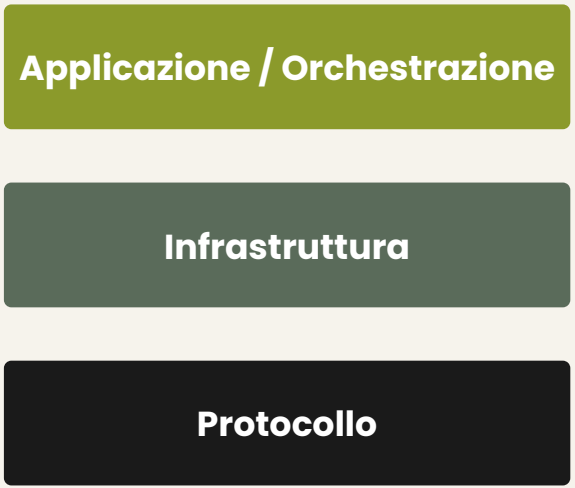
Dipendenze nella supply chain

Librerie, container, build pipeline

Astrazione dal protocollo

Logica di firma delegata a layer esterni

Stack tipico



Ogni layer aggiuntivo introduce una nuova superficie di attacco.

Ridurre la superficie di attacco: controllo end-to-end

Approccio CheckSig

CheckSig — controllo end-to-end

- Protocollo di gestione progettato internamente
- Nessuna dipendenza da orchestrazione esterna
- Controllo diretto su sviluppo, infrastruttura, logica di firma
- Formazione ad hoc al personale e devops

Meno layer → meno dipendenze → meno superficie di attacco

Non aggiungiamo controlli sopra il sistema. Riduciamo il sistema stesso.

CHECKSIG CLEAR

La domanda non è se entrare nei digital asset. È con quale modello operativo farlo.

Perché non è un tema solo tecnologico.
È un tema di controllo, processi e responsabilità.

Ed è esattamente qui che la custody diventa il modo per rendere questo controllo concreto.

Casi reali

Cosa succede quando i controlli non funzionano

Matteo Sciolla | Head of Custody

1 Bybit, febbraio 2025, $1.5 mld

Scenario

- Bybit usa Safe{Wallet} come vendor per gestire il cold wallet
- Il vendor viene compromesso (uno sviluppatore Safe è target di social engineering)
- Il codice del vendor viene modificato per mostrare ai firmatari una transazione fittizia

Impatto

- >400k ETH (e altri) drenati dal cold wallet
- Record assoluto: il più grande furto crypto di sempre
- Attribuzione FBI a Corea del Nord (TraderTraitor / Lazarus)

19 febbraio 2025
app.safe.global compromesso

20 febbraio 2025
Lazarus aspetta la firma giusta

21 febbraio 2025
Bybit firma. 401.347 ETH spariti.

Il perimetro non era Bybit. Era anche Safe.

CHECKSIG CLEAR

2 Drift Protocol, aprile 2026, $285M

Scenario

- Lazarus si finge società di quant trading per 6 mesi
- Costruisce relazioni con i firmatari abilitati a cambiare il protocollo
- Il 1 aprile 2026 le autorizzazioni vengono usate per drenare il protocollo

Impatto

- $285M drenati in meno di 15 minuti
- Più grande hack DeFi del 2026
- Attribuzione a Corea del Nord (Lazarus) confermata da Drift e da Chainalysis

Autunno 2025
Lazarus avvia il social engineering

23–30 marzo 2026
Pre-firma di transazioni con autorizzazioni nascoste

1 aprile 2026
$285M drenati

I firmatari erano la governance. Non era abbastanza

CHECKSIG CLEAR

3 Coinbase, maggio 2025, $400M

Scenario

- Cybercriminali corrompono customer support contractor esteri di Coinbase
- Per 5 mesi i contractor esfiltrano dati di clienti (nomi, SSN, dati bancari) col loro accesso legittimo
- Maggio 2025: richiesta di riscatto da $20M. Coinbase rifiuta e mette $20M di taglia

Impatto

- 69.461 clienti coinvolti
- $180–400M di impatto finanziario stimato (class action, remediation)
- Nessun fondo prelevato direttamente, ma social engineering downstream sui clienti

Dicembre 2024 — Inizio esfiltrazione dati

Maggio 2025 — Ricatto e disclosure pubblica

1 maggio 2025 — Rifiuto riscatto, $20M di taglia

Il badge era reale. L'intento no.

CHECKSIG CLEAR

Quale di questi tre scenari vi preoccupa di più?

Supply chain

Social engineering

Insider

Custody come risposta operativa

La custody non è conservazione passiva.
È controllo attivo.

Tre attacchi, tre presidi

Diversi tra loro, lo stesso disegno di controllo

SUPPLY CHAIN **Bybit** $1,5 mld	**VETTORE** Vendor della firma compromesso: i firmatari firmano una transazione diversa da quella mostrata.	→ **PRESIDIO MANCANTE** **Signing controllato:** si verifica e si firma il contenuto reale, non la rappresentazione di un'app esterna.
SOCIAL ENGINEERING **Drift** $285M	**VETTORE** Social engineering prolungato sui firmatari, indotti a pre-autorizzare clausole nascoste.	→ **PRESIDIO MANCANTE** **Multi-ruolo + signing controllato:** non eliminano il rischio, ma alzano significativamente la soglia.
INSIDER **Coinbase** $400M	**VETTORE** Insider con accesso legittimo a dati sensibili.	→ **PRESIDIO MANCANTE** **Segregazione ruoli + data governance:** zero fondi mossi ma è mancato il minimo privilegio sui dati

Una custody seria poggia su quattro pilastri

Dal protocollo alle assicurazioni.

PROTOCOLLO · *nuovo*

La sicurezza scritta nelle regole crittografiche
↳ multisig, timelock, layer frozen / cold / hot, smart contract, tutto verificabile on-chain in autonomia

APPLICATIVO · *nuovo*

Il software che firma e verifica
↳ Signing controllato (lezione Bybit), audit e penetration test sul codice e sulla supply chain

GOVERNANCE · *noto, su oggetti nuovi*

Chi può fare cosa, con quanti consensi
↳ multi-ruolo (Drift), minimo privilegio (Coinbase), audit di processo

RESILIENZA · *noto, su oggetti nuovi*

Continuità operativa quando qualcosa si rompe
↳ Disaster recovery dei fondi, distribuzione delle chiavi, coperture assicurative dedicate

Per garantire i quattro pilastri servono specialisti del settore.

Il flusso operativo in quattro passi

Un controllo attivo, una traccia verificabile.

1

Creazione transazione

Presidio: proposta strutturata da operatore identificato

Verifica: origine, identità e ruolo tracciati

2

Approvazione multi-ruolo

Presidio: approvazione multipla per ruolo

Verifica: log immutabili di approver e ruoli

3

Signing controllato

Presidio: firma multi-step sul protocollo

Verifica: hash della transazione su block explorer / nodo proprio

4

Audit e tracciabilità

Presidio: log immutabile di ogni operazione, audit interni periodici

Verifica: audit indipendenti certificati

Nel mondo crypto,
la sicurezza non è un layer aggiuntivo.

È il principio con cui si progetta
l'intero sistema.

Dalla tecnologia alle persone.
La custody rappresenta la sua esecuzione operativa.

Tre domande da portare a casa

Come scegliere un custodian. In tre domande.

1. **Cosa fate direttamente e cosa è di terzi?**

2. **Chi può muovere i miei asset, e con quanti consensi?**

3. **Cosa posso verificare in autonomia?**

Un custodian serio risponde a tutte e tre — in modo dimostrabile, non a parole.

CHECKSIG CLEAR

SALA TECHNOLOGY & OPERATIONS

Gestione sicura dei digital asset: tra custodia e cybersecurity

Mattia Coffetti
Chief Information Security Officer, CheckSig

Matteo Sciolla
Head of Custody, CheckSig

CLEAR SUMMIT 2026

CHECKSIG CLEAR

SECONDO PIANO

Assisti alla plenaria di chiusura in auditorium

CLEAR SUMMIT 2026

CHECKSIG CLEAR