IL POTERE CHE SOPRAVVIVE ALLA MACCHINA

La lezione nascosta del caso Binance per la sicurezza dell’impresa agentica

Francesco Marinuzzi

Agentic engineer - Cybersecurity specialist

Saggio tecnico | 5 novembre 2026 | Versione 1.0

Executive summary

L’incidente di sicurezza che ha colpito Binance il 29 ottobre 2026 offre una lezione che supera la finanza decentralizzata. Secondo la relazione preliminare pubblicata da Binance il 3 novembre, circa 6,34 miliardi di dollari in asset digitali sono stati coinvolti e circa 2,85 miliardi risultavano congelati o intercettati al momento della comunicazione. Questi importi non devono essere confusi con una perdita netta definitiva, ancora soggetta a riconciliazione e indagine. [1]

Il dettaglio architetturalmente decisivo riguarda Ethereum EIP-7702: l’attaccante ha indotto un servizio interno di firma a produrre autorizzazioni capaci di delegare l’esecuzione dell’account a codice esterno. Spegnere i servizi di hot wallet non ha annullato l’autorità già registrata nello stato della blockchain. Per neutralizzarla è servita una nuova operazione valida on-chain, effettuata alle 00:10 UTC del 30 ottobre. [1][2]

> **La cessazione della macchina che conferisce un potere non comporta necessariamente la cessazione del potere conferito.**

La tesi di questo saggio è che la cybersecurity debba governare non soltanto identità, credenziali e processi, ma anche le **autorità esternalizzate**: deleghe, consensi, token, ruoli e permessi che possono sopravvivere all’arresto del componente originario. È un problema critico per gli agenti AI, la cui capacità operativa si esercita attraverso API, strumenti e servizi terzi.

Si propone pertanto un principio di progettazione: ogni capacità di conferire autorità esterna deve accompagnarsi a un inventario verificabile, a un percorso di revoca indipendente, a limiti di durata

e privilegio e a una misura esplicita del tempo di esposizione residua dopo il contenimento.

1. Dall’incidente al principio generale

Un’organizzazione può bloccare il proprio software compromesso e continuare a subire gli effetti di poteri già trasferiti. Ciò accade quando l’autorizzazione non vive soltanto nell’infrastruttura locale, ma viene accettata e mantenuta da un sistema esterno autonomo: una blockchain, un identity provider, un cloud, un servizio SaaS o un sistema di automazione.

Nel caso Binance, il rapporto preliminare indica un attacco multistadio che ha combinato tecniche di social engineering, compromissione di endpoint e strumenti AI interni, sottrazione di capacità operative e abuso di un servizio di firma per i wallet. La relazione attribuisce agli attaccanti l’uso di 50 transazioni di firma finalizzate a manipolare il nonce e stabilire deleghe EIP-7702 malevole. L’inchiesta era ancora in corso al 3 novembre: per questo non ogni passaggio può essere considerato definitivamente accertato. [1]

Il titolo della vicenda è il denaro coinvolto; il cuore della lezione tecnica è la **persistenza dell’autorità al di fuori del perimetro di contenimento**.

2. EIP-7702: autorizzazione, delega e codice sono tre oggetti diversi

EIP-7702 è una proposta Ethereum che introduce una transazione con un elenco di autorizzazioni firmate. Per ogni autorizzazione valida, il protocollo imposta nel codice dell’account autorizzante un indicatore di delega formato dal prefisso **0xef0100** e da un indirizzo di destinazione. L’account conserva indirizzo e saldo, ma le chiamate che ne attivano l’esecuzione possono utilizzare il codice presente all’indirizzo delegato, nel contesto dell’account autorizzante. [2]

Elemento	Significato tecnico
Autorizzazione firmata	Dichiarazione crittografica che contiene, fra gli altri dati, chain ID, indirizzo delegato e nonce.
Indicatore di delega	Valore 0xef0100 + indirizzo, scritto nello stato del codice dell’account autorizzante.
Codice delegato	Logica eseguibile ospitata nell’account di destinazione; le sue capacità e i controlli dipendono dall’implementazione.
Revoca	Nuova autorizzazione valida che imposta come destinazione l’indirizzo nullo e rimuove l’indicatore corrente.

Non è corretto sostenere che lo smart contract delegato diventi automaticamente proprietario dei fondi, né che qualunque EIP-7702 dia controllo illimitato a terzi. La capacità effettiva dipende dal codice delegato, dai suoi controlli e dalle condizioni di esecuzione. In un attacco, però, una delega a codice malevolo può produrre un percorso operativo indipendente dal sistema aziendale che aveva

firmato l’autorizzazione.

Il problema della permanenza

La storia delle transazioni della blockchain resta registrata, ma questo non significa che i permessi siano per definizione irrevocabili. EIP-7702 permette esplicitamente di cancellare l’indicatore di delega, firmando una nuova autorizzazione indirizzata a **0x0000000000000000000000000000000000000000**. Ciò aggiorna lo stato corrente dell’account; non elimina dalla storia la transazione originaria e non annulla retroattivamente i trasferimenti già eseguiti. [2]

> **Immutabilità del registro e revocabilità dello stato autorizzativo sono proprietà differenti.**

3. Che cosa è successo durante il contenimento

Secondo Binance, i primi trasferimenti XRP non autorizzati documentati sono avvenuti il 29 ottobre fra le 20:05 e le 20:09 UTC. Altri trasferimenti hanno interessato più reti, compresi BTC, SOL, OP ed ETH. Le misure di contenimento hanno incluso la sospensione dei prelievi e il coordinamento per congelare asset. Ma la sospensione dei prelievi non disabilitava automaticamente le autorizzazioni Ethereum già efficaci. [1]

Il rapporto aggiunge che i wallet coinvolti utilizzavano **Multi-Party Computation (MPC)**: non esisteva una singola chiave privata da usare immediatamente per la revoca. Binance ha dovuto predisporre una procedura specifica di firma per rimuovere la delega. Il trasferimento non autorizzato finale, di 2.961,9 ETH, è stato confermato alle 23:56 UTC del 29 ottobre; la transazione era stata trasmessa in precedenza ed era rimasta pendente. Alle 00:10 UTC del 30 ottobre una nuova autorizzazione da Binance14 all’indirizzo nullo ha cancellato la delega. [1]

Momento (UTC)	Evento e rilievo
29 ott., 20:05–20:09	Trasferimenti XRP non autorizzati da cinque hot wallet.
29 ott., durante l’attacco	Abuso del servizio di firma e stabilimento delle autorizzazioni EIP-7702.
29 ott., 23:56	Conferma on-chain dell’ultimo trasferimento non autorizzato documentato.
30 ott., 00:10	Nuova autorizzazione a zero address; rimozione dell’indicatore di delega.

Non va dedotta dai soli orari della tabella una durata esatta fra spegnimento dei servizi e revoca: l’istante preciso di completamento del contenimento infrastrutturale non è riportato nella relazione con granularità sufficiente. La finestra di esposizione residua esiste sul piano concettuale, ma la sua misura esatta per questa vicenda non è ricostruibile dalla sola fonte aziendale.

4. Il paradosso della risposta agli incidenti

La risposta classica a un incidente privilegia isolamento dell'host, sospensione degli account, rotazione delle credenziali, disattivazione dei servizi e ricostruzione degli ambienti compromessi. Sono passaggi indispensabili ma non esaustivi nei sistemi in cui l'infrastruttura locale può aver esercitato il potere di creare autorità fuori dal perimetro.

La distinzione è tra **potere di conferimento** e **potere di revoca**. Il primo può essere esercitato durante una finestra di compromissione, il secondo può richiedere un percorso separato, nuovi consensi, la disponibilità di quorum MPC o una transazione validata da infrastrutture esterne. Il secondo percorso può essere più lento del primo.

Per una progettazione robusta occorre chiedersi: chi può firmare la delega? Dove resta efficace? Chi può revocarla? Il percorso di revoca resta praticabile quando il sistema originario è indisponibile o sospetto? La revoca interrompe soltanto effetti futuri o è necessaria un'ulteriore bonifica delle autorizzazioni derivate?

5. La metrica proposta: tempo di autorità residua

Si definiscano quattro eventi: **t0**, inizio della compromissione; **t1**, creazione di una delega esterna; **t2**, arresto o isolamento dell'infrastruttura compromessa; **t3**, revoca effettiva e verificata della delega. La finestra **t3 − t2**, quando positiva, rappresenta il tempo in cui l'autorità può sopravvivere al contenimento locale.

> **TAR = max(0, t3 − t2) | Tempo di Autorità Residua**

TAR è una metrica proposta in questa analisi, non uno standard normativo né una misura già validata per l'incidente Binance. Può essere calcolata per ciascuna autorizzazione e aggregata, per esempio con percentile 95, valore massimo e somma ponderata per criticità. L'obiettivo non è solo ridurre il tempo per spegnere una macchina, ma ridurre il tempo in cui un terzo conserva capacità operative dopo il contenimento.

La misura va accompagnata da una verifica dell'effettività della revoca: una API che restituisce "success" non prova necessariamente che ogni cache, replica, token già emesso o autorizzazione derivata sia stata neutralizzata.

6. Applicazione all'impresa agentica

Un agente AI non opera soltanto producendo testo. Può invocare tool, emettere richieste API, autorizzare servizi, programmare automazioni, creare account e modificare configurazioni. In un'architettura agentica il rischio non coincide con la durata del processo AI: i suoi effetti autorizzativi possono mantenersi attivi dopo la disattivazione del modello, dell'orchestratore o del tool originario.

Uno scenario esemplificativo è una prompt injection che induce un agente dotato di privilegi eccessivi a creare una deploy key su GitHub, concedere un consenso applicativo in Microsoft 365 o

emettere credenziali cloud a lunga durata. Anche se l'agente viene spento pochi secondi dopo, il soggetto che possiede la nuova credenziale potrebbe continuare a utilizzarla. Sono esempi architetturali, non azioni attribuite all'incidente Binance.

Ambiente	Autorità che può sopravvivere al processo
Repository e CI/CD	Deploy key, token di automazione, segreto di pipeline o webhook.
Identity provider	Consenso OAuth, applicazione con privilegi, credenziali di servizio.
Cloud	Ruoli, policy, access key e sessioni con durata residua.
SaaS / CRM	Token di integrazione e connessioni autorizzate.
Blockchain	Delega on-chain o altre approvazioni persistenti.

Le semantiche di questi meccanismi sono diverse: alcuni scadono, altri sono revocabili centralmente, altri dipendono da quorum o finalità distribuite. Non è la tecnologia a renderli equivalenti. È comune il rischio di **disaccoppiamento temporale e amministrativo** fra la fine dell'agente e la fine delle facoltà che ha generato.

7. Un modello di governance: Authority Lifecycle Management

La proposta operativa è introdurre un livello di **Authority Lifecycle Management (ALM)**, distinto dai tradizionali audit log delle chiamate. Il registro non deve limitarsi a descrivere quale API sia stata invocata: deve rappresentare quali poteri effettivi sono stati creati o modificati e dove essi possono essere esercitati.

Campo del registro	Domanda a cui rispondere
Delegante e attore	Quale identità, agente o servizio ha creato il potere?
Destinatario e sistema	Chi può ora esercitarlo e su quale infrastruttura?
Permessi e limiti	Quali operazioni, asset, importi o risorse sono inclusi?
Inizio e scadenza	Da quando è valido e quando decade automaticamente?
Procedura di revoca	Chi autorizza la revoca e con quali mezzi indipendenti?
Verifica dello stato	Quale evidenza prova l'avvenuta cessazione del potere?
Dipendenze derivate	Quali token, deleghe o effetti ulteriori sono stati creati?

Sette controlli da rendere progettuali

1. Minimo privilegio e limitazione temporale. Ridurre ambito, durata e valore delle autorità delegabili. Dove possibile imporre scadenza automatica, limiti di spesa e autorizzazioni singole per operazione.

2. Inventario continuo. Confrontare il registro interno delle autorizzazioni con lo stato osservabile nei sistemi terzi; individuare le deleghe sconosciute, anomale o non più giustificate.

3. Percorso di revoca indipendente. Prevedere un meccanismo di emergenza che non dipenda dall'host compromesso o dall'unico workflow ordinario; proteggere tale capacità con controlli specifici e test ricorrenti.

4. Policy sulle azioni autorizzative. Distinguere le normali operazioni di business da quelle che generano nuovi poteri: queste ultime richiedono controlli di firma, approvazione e validazione più stringenti.

5. Contenimento esteso. Una procedura di incident response deve comprendere l'enumerazione delle capacità esterne conferite, e non soltanto l'isolamento dei sistemi locali.

6. Verifica della bonifica. Revocare non equivale a riparare: vanno individuati accessi derivati, modifiche già apportate e asset eventualmente trasferiti.

7. Esercitazioni e metriche. Misurare TAR con drill periodici, distinguendo tempo di rilevamento, tempo di isolamento, tempo di revoca e tempo di verifica.

8. Implicazioni per ingegneria e responsabilità organizzativa

La questione riguarda contemporaneamente architettura, cybersecurity, gestione delle identità, compliance e continuità operativa. In un'impresa agentica, il disegno dei poteri conferibili dagli agenti è un problema di governance prima ancora che di prompt engineering. Una decisione apparentemente tecnica — consentire a un agente di creare un token o una delega — può introdurre un rischio operativo che sopravvive al software che l'ha prodotta.

Il criterio da aggiungere agli assessment dei sistemi agentici è semplice: **per ogni azione che produce autorità durevole, esiste un piano di cessazione testato e indipendente?** Se la risposta è negativa, l'architettura mantiene un debito di revocabilità. Questo debito non emerge necessariamente nei tradizionali test di penetrazione centrati sulla macchina o sull'applicazione.

9. Conclusione: governare ciò che resta possibile

Il caso Binance mostra una separazione fondamentale: l'organizzazione può arrestare i servizi compromessi e tuttavia dover ancora interrompere un potere valido presso un'infrastruttura esterna. Ethereum EIP-7702 rende la separazione particolarmente visibile perché la delega è iscritta nello stato dell'account e la sua revoca deve transitare attraverso le regole del protocollo.

Nell'impresa agentica questa dinamica non è un'eccezione legata alle criptovalute. Ogni agente capace di modificare i permessi di sistemi terzi può lasciare in eredità capacità operative

autonome. La cybersecurity deve quindi estendere il suo perimetro dal controllo del processo al controllo delle autorità che il processo ha generato.

> **La sicurezza non può più limitarsi a governare ciò che i sistemi possono fare. Deve governare anche ciò che hanno reso possibile ad altri di continuare a fare.**

Fonti e nota metodologica

[1] Binance, “29 October 2026 Binance Security Incident: Initial Findings and Response Update”, 3 novembre 2026. https://www.binance.com/en/blog/community/3229153443759566763

[2] Ethereum Improvement Proposals, “EIP-7702: Set Code for EOAs”, testo della specifica tecnica. https://eips.ethereum.org/EIPS/eip-7702

[3] GCSA, “Independent Forensic Investigation and EIP-7702 Attack Link Analysis”, 30 ottobre 2026. https://media.gcsa.com/en-US/news-3730400

[4] Elliptic, “The largest theft in history: North Korea likely behind the $6.4 billion Binance hack”, 30 ottobre 2026. https://www.elliptic.co/insights/binance-largest-hack-in-history/

Nota: la ricostruzione dell’incidente si fonda principalmente sul rapporto preliminare Binance del 3 novembre e sulla specifica EIP-7702. Le ipotesi di governance, il termine “Authority Lifecycle Management” e la metrica TAR sono proposte analitiche dell’autore. Cifre, attribuzioni e sequenze investigative possono evolvere con le verifiche indipendenti.