LA FORT KNOX DELLE VALUTE DIGITALI.

INNALZATI GLI STANDARD DI SICUREZZA GRAZIE ALLA NUOVA TECNOLOGIA DI CONIO: LA SOLUZIONE IDEATA PER GLI INVESTITORI ISTITUZIONALI

Milano, 15 Gennaio 2020 - **Conio**, la società italiana specializzata in tecnologie per la custodia di criptovalute, in collaborazione con il Dipartimento di Matematica dell'Università di Trento, ha ideato e **sviluppato la tecnologia Multi-Signature Virtualization**: la prima soluzione che **aumenta lo standard di sicurezza** del wallet **per qualsiasi valuta digitale** e consente di coniugare il livello di sicurezza tipico di una gestione offline delle chiavi, all'efficienza dei wallet online. Conio ha già realizzato un primo wallet Ethereum su cui ha implementato lo schema della Multi-Signature Virtualization. L'applicazione sviluppata è ancora una volta una prova della capacità pionieristica di Conio nelle tecnologie di frontiera e nel saper fornire soluzioni affidabili per la custodia di tutte le criptovalute esistenti.

Le soluzioni di custodia attuali hanno dei limiti

Nel mondo delle criptovalute, per svolgere qualsiasi operazione è necessario utilizzare la propria chiave privata. Chiunque entri in possesso di questa chiave, può disporre dei fondi. Ciò rende il sistema di **custodia della chiave il fattore più importante** da considerare per chiunque, in particolare per gli investitori istituzionali. Qualsiasi attività l'istituzione voglia svolgere, che si tratti di un acquisto, una vendita o un trasferimento di denaro, dovrà interfacciarsi con il sistema di custodia. E' per questo fondamentale, per un'istituzione, adottare un sistema di custodia che, oltre che essere sicuro, renda semplice e veloce gestire le chiavi.

Oggi, le istituzioni tendono ad adottare soluzioni di custodia basate sul Cold Storage, che consente di conservare e **gestire offline la propria chiave** privata.

Tale soluzione ha però dei punti deboli. In particolare rischia di vincolare e limitare l'operatività dell'istituzione. Il Cold Storage infatti **rende più lenta l'esecuzione** di qualsiasi tipo di operazione, elemento che **rischia di minare la capacità di servire tempestivamente i clienti**. Inoltre, per le criptovalute basate sull'algoritmo Proof of Stake (PoS), il Cold Storage impedisce la piena partecipazione alla rete, dato che, per esercitare i propri diritti, è necessario esporre online il proprio stake. Sintetizzando, spesso le istituzioni si trovano a dover affrontare un **trade-off tra sicurezza ed**

efficienza operativa. La soluzione ideata da Conio, consente però di aumentare lo standard di sicurezza e superare il problema.

Conio: più chiavi, meno rischio

Fra **i vantaggi più importanti** della soluzione di Conio, emerge la possibilità di disporre sempre online delle criptovalute, mantenendo però il livello di sicurezza tipicamente garantito solo dallo storage offline delle chiavi. Questo ha due prime implicazioni:

1. Possibilità di **movimentare tempestivamente** le criptovalute
2. Possibilità di **partecipare pienamente alla rete** e di esercitare i propri diritti quando si utilizzano valute basate sull'algoritmo Proof of Stake

La tecnologia ideata, inoltre, presenta altri due grandi vantaggi, particolarmente importanti per gli investitori istituzionali:

3. Possibilità di adottare un **Sistema di Custodia unico**, adatto a tutte le criptovalute
4. Possibilità di **recuperare sempre i fondi**, qualora vengano smarrite le credenziali, **anche nel caso di valute** basate sul modello **Single Signature**

La soluzione di Conio, infatti, ha il merito di **innalzare lo standard di** sicurezza e di poterlo applicare a **tutte le valute, indipendentemente dalle loro caratteristiche** di base: alcune valute, come Bitcoin, supportano sistemi di sicurezza considerati più sicuri rispetto ad altri. Bitcoin, infatti, supporta il modello Multi-Signature: un meccanismo grazie al quale viene generata più di una chiave, ed è possibile scegliere quante di queste chiavi siano necessarie per autorizzare una transazione, così da avere sempre almeno una chiave di scorta. Invece, Ethereum, seconda solo a Bitcoin nell'ecosistema delle criptovalute, e persino Libra, ideata nel 2019 da Facebook con il proposito di divenire un sistema di pagamento mondiale, sono basate sul modello Single Signature. Questo espone chi le gestisce a rischi concreti. Il modello Single Signature, infatti, è un meccanismo che prevede un'unica chiave per autorizzare le transazioni. Pertanto **perdere la chiave, significa perdere i propri soldi per sempre**. Queste valute andrebbero quindi gestite in modo diverso. **Per la prima volta,** però, la tecnologia ideata da Conio rende possibile estendere a tutte le valute digitali e stablecoin **un Sistema di Custodia unico e decisamente sicuro**.

SCHEDA TECNICA

Il sistema di custodia adatto a tutti gli asset digitali

La soluzione, creata dalla società nel corso degli anni, è basata su un'architettura Multi-Signature 2-di-3 che si innesta su vari livelli: due chiavi online; una chiave offline, suddivisa in multiple Shamir shares salvate su dispositivi HSM. Finora questo sistema è stato usato dalla società per gestire i Bitcoin in questo modo:

1. SISTEMA DI CUSTODIA MULTISIGNATURE A 3 CHIAVI

   Conio ha implementato sui suoi wallet un modello Multi-Signature che prevede **3 chiavi**. Per spostare i fondi, sono sempre necessarie almeno 2 di queste chiavi. **Conio è in possesso solo di una** di queste due chiavi, mentre **un'altra è in possesso del cliente.**

2. SISTEMA DI GESTIONE OFFLINE DELLA 3° CHIAVE

   La **terza chiave** è custodita **offline**, grazie a una combinazione di dispositivi Hardware Security Modules (HSMs) e ad un software specializzato basato sull'algoritmo Shamir's Secret Sharing (SSS). La chiave è inoltre **suddivisa in più parti,** distribuite su più dispositivi HSM, assegnati a loro volta ad operatori diversi. Questo consente di proteggere la chiave da eventuali attacchi interni o esterni e di utilizzarla **per recuperare i fondi nel caso** in cui la prima o la seconda **vengano smarrite o rubate**.

Ora, con la nuova tecnologia di Conio, queste misure di sicurezza possono essere estese anche alle valute che non supportano il modello Multi-Signature:

3. MULTI-SIGNATURE VIRTUALIZATION

   Grazie allo sviluppo della tecnologia Multi-Signature Virtualization, basata sul concetto di threshold signatures, Conio rende possibile l'utilizzo di un modello "2-di-3" in maniera agnostica rispetto alla blockchain sottostante. In questo modo, Conio permette l'utilizzo di un modello **Multi-Signature anche per criptovalute che non lo supportano nativamente**.

Con l'ideazione e sviluppo di questa soluzione, **Conio** è la **prima compagnia al mondo** a offrire competenze tecnologiche e crittografiche in grado di garantire uno **standard di sicurezza avanzato per qualsiasi valuta** digitale a prescindere dai limiti nativi della stessa.

GLOSSARIO

- **HSM (Hardware Security Module)**: dispositivi fisici specializzati nello storage sicuro di dati e nel loro utilizzo.
- **Multi-Signature**: meccanismo grazie al quale viene generata più di una chiave, ed è possibile scegliere quante di queste chiavi siano necessarie per autorizzare una transazione.
- **Proof of Stake (PoS)**: algoritmo di consenso basato sull'ammontare di criptovalute messe in gioco dall'utente.
- **Single-Signature**: meccanismo che prevede un'unica chiave per autorizzare le transazioni.

APPENDICE

Conio

Start up fondata nel 2015 da Christian Miccoli e Vincenzo Di Nicola, ha realizzato il primo portafoglio mobile italiano per la compravendita di Bitcoin, basato sulle più innovative tecnologie proprietarie di sicurezza a livello internazionale. Grazie alle sue competenze nella gestione della tecnologia del futuro, Conio apre la strada a nuove applicazioni e dà vita a nuove opportunità in tutti i settori.

Il **Portafoglio Bitcoin Conio** è pensato per ogni tipologia di utente e permette di comprare, vendere, custodire, inviare e ricevere Bitcoin direttamente dal proprio smartphone. Al wallet è possibile accedere attraverso un'app per smartphone progettata e realizzata con l'obiettivo di semplificare un mondo molte volte ancora troppo complesso per il grande pubblico. Per iniziare ad usare il Portafoglio Bitcoin Conio basta scaricare l'app sul proprio smartphone (disponibile per Android e iOS). Immediatamente consente di visualizzare in tempo reale il valore di cambio della criptomoneta e l'ammontare del proprio portafoglio.

Ufficio Stampa Conio

Francesca Donelli, Matteo Miccoli

Email: francesca@conio.com, matteo@conio.com

Tel: +39 3935443926 - + 39 3420202315