Conio x PoliTO

25 maggio 2023

CONIO

Conio Profile

2015

NASCITA e FONDAZIONE

Conio nasce con un finanziamento iniziale di Poste Italiane. Conio ha collaborato con Poste Italiane in vari progetti di ricerca e sviluppo per applicazioni blockchain.

Posteitaliane

2018

SEED ROUND

Round di finanziamento Seed.
Conio sviluppa ulteriormente la sua offerta B2B

Q1 2020

PRIMA PARTNERSHIP BANCARIA

HYPE, prima banca in Europa a lanciare il servizio di custodia e trading di Bitcoin.

HYPE

Q4 2020

GARTNER COOL VENDOR IN BANKING.

Gartner: "Conio consente alle banche di offrire asset digitali."

Gartner COOL VENDOR 2020

ROUND SERIE A

Banca Generali guida un round di investimenti Serie A

Q4 2021

SECONDA PARTNERSHIP BANCARIA

Banca Generali integra il servizio di custodia e trading di Bitcoin.

BANCA GENERALI

Q1 2022

TERZA PARTNERSHIP BANCARIA

Avvio di una partnership tecnologica con un'importante istituzione finanziaria italiana.

GARTNER "HYPE CYCLE VENDOR"

Gartner HYPE CYCLE VENDOR 2021-2022

Conio è stata nominata Hype Cycle Vendor da Gartner.

Conio - Digital Assets Solution

Custodia

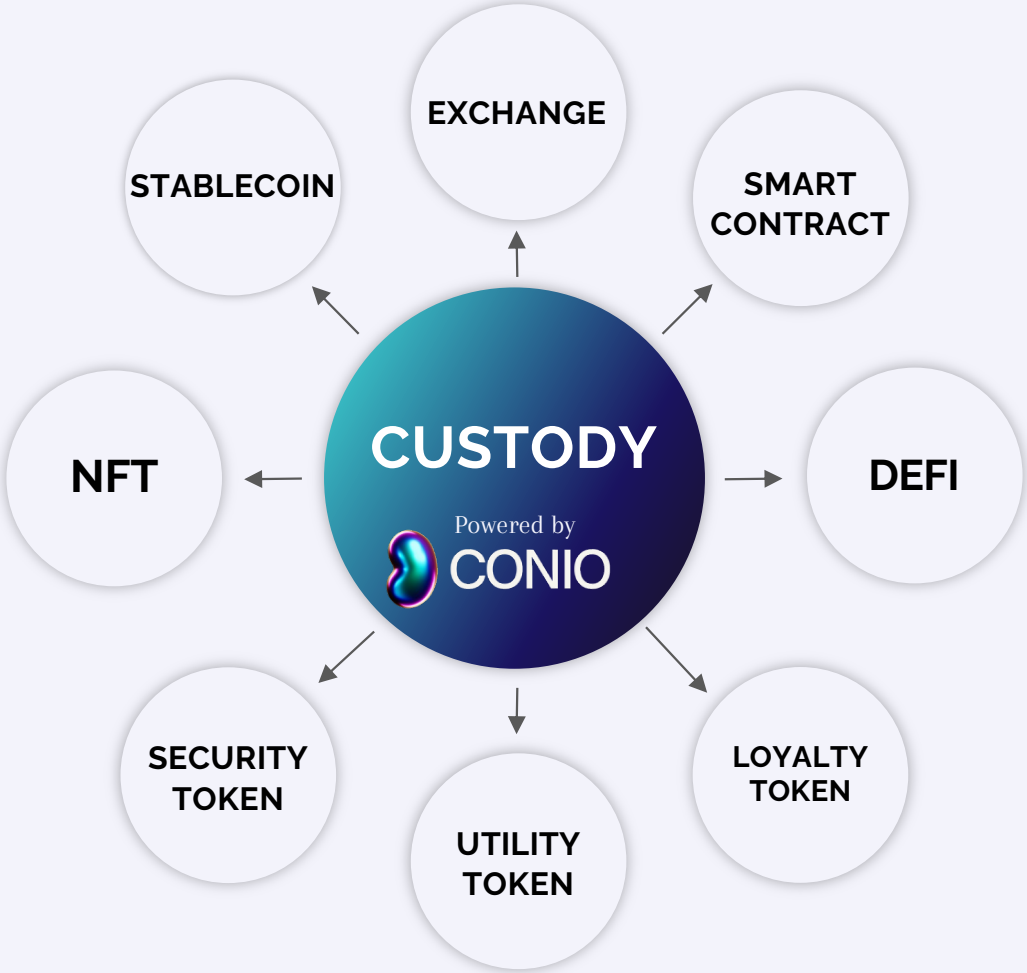
Offriamo una **soluzione di custodia** per banche e utenti finali unica nel suo genere, grazie a un sistema brevettato basato sui wallet Multi-Sig.

Exchange

Garantiamo l'**acquisto e la vendita** di digital asset direttamente dal proprio wallet, offrendo la best execution dell'ordine e diminuendo i rischi di cambio per il cliente.

Tokenization

Grazie alle soluzioni tecnologiche sviluppate in-house, siamo in grado di offrire diverse soluzioni di tokenizzazione per svariate tipologie di risorse e asset.



Conio Products - Custody

Sono richieste **2 su 3 chiavi** per firmare una transazione.

Standard transaction

Recovery Transaction

Customers Key

Online - Client App.

One key is internal in the storage of the device with an **encrypted system** of the customer to sign and **approve transactions** with **2FA**

Conio's Key

Online - Conio Infrastructure.

Secure Conio Custody to confirm and countersign transaction of the customers to guarantee daily operations

Bank's Key

Offline - Bank n-of-m

Recovery key to provide back the Tokens to the customer with a **quorum n-of-m** with the **highest safety** from internal and external possible attack vectors

Emergency Recovery Transaction

The **assets are always owned by the customers** so the bank and Conio doesn't have on their balance sheet any volatility of the tokens.

Conio Products - Wallet Security

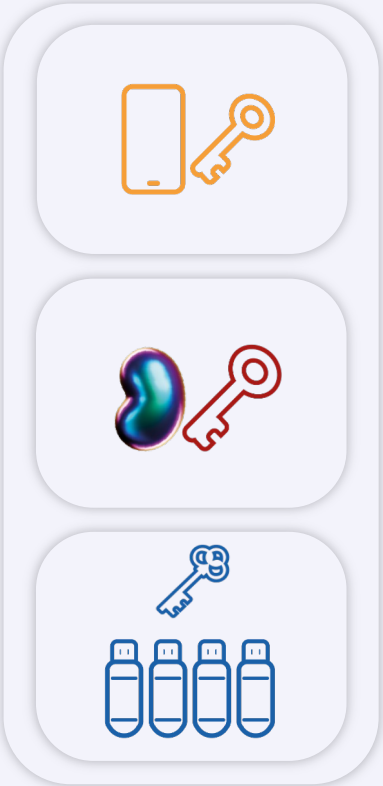
Generazione delle chiavi private

- le chiavi private generate dal wallet devono essere sicure
  - come si generano chiavi sicure?

Archiviazione delle chiavi private

- le chiavi private devono essere archiviate in modo sicuro
  - bisogna evitare che un attaccante possa recuperarle

Conio Products - Wallet Security

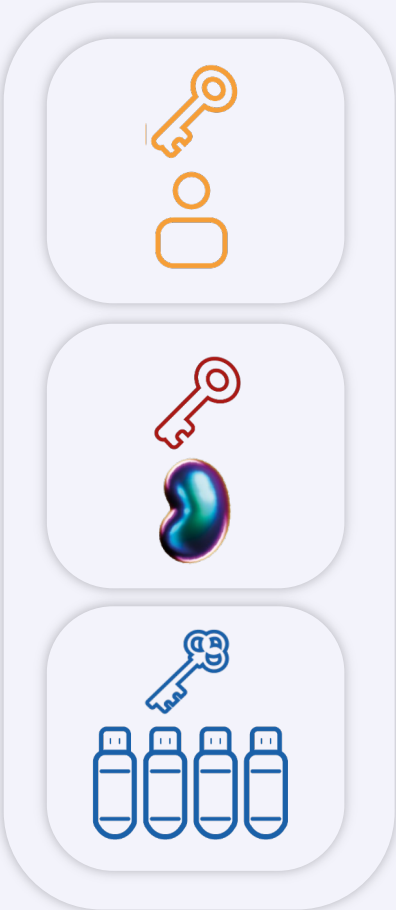


Difese Preventive Conio

- **N chiavi indipendenti**
  - in caso di compromissione di una parte le altre parti restano sicure
- generate su **N parti diverse**
  - per evitare generazione di chiavi centralizzata
- generate con **N tecnologie diverse** (generatori random Android/iOS, python, go)
  - qualora una libreria random fosse vulnerabile le altre sarebbero diverse

Conio Products - Wallet Security

Conio Multisig Wallet 2-di-3



- **Chiave 1 - Chiave Cliente**
  in possesso dell'utente
- **Chiave 2 - Chiave Conio (Hot)**
  archiviata cifrata nel Trusted Execution Environment (TEE) di Conio
- **Chiave 3 - Chiave Banca (Cold)**
  composta da N shard (MPC)

Conio Custody - Overview

TECNOLOGIA PROPRIETARIA

Sistema di custodia interamente sviluppato in-house (Italia)

SUCCESSIONI

In caso di successione, con Conio è facile movimentare i fondi verso i legittimi eredi

SECURITY BY DESIGN

La tecnologia di Conio è stata progettata per eliminare qualsiasi rischio di sicurezza (modello zero trust)

NO RISCHIO CONTROPARTE

In caso di fallimento di Conio, i fondi rimangono disponibili al cliente grazie alla chiave della banca e del cliente stesso

NO PERDITA FONDI

In caso di perdita della chiave del cliente, grazie al sistema di recovery di Conio, i fondi possono sempre essere recuperati

BILANCIO BANCA

Le cripto detenute dai clienti non devono essere iscritte nel bilancio della Banca

Conio Research

List of Patents (5) and Publications (7):

[1] Conio Inc., Method and Apparatus for a Blockchain-Agnostic Safe Multi-Signature Digital Asset Management (patent, 2022)
[2] Conio Inc., Methods and systems for safe creation, custody, recovery, and management of a digital asset (patent #11164182 - 2021)
[3] Conio Inc., Method and apparatus for restoring access to digital assets (patent #10547441 - 2020)
[4] Conio Inc., Display screen with animated graphical user interface (patent #D824404 - 2018)
[5] Conio Inc., Display screen with animated graphical user interface (patent #D834043 - 2018)
[6] Di Nicola, V., Longo, R., Mazzone, F., & Russo, G. (2020). Resilient Custody of Crypto-Assets, and Threshold Multisignatures. Mathematics, 8(10), 1773
[7] Battagliola, Michele, et al. "Threshold ECDSA with an Offline Recovery Party." Mediterranean Journal of Mathematics 19.1 (2022): 1-29
[8] Battagliola, Michele, et al. "A Provably-Unforgeable Threshold EdDSA with an Offline Recovery Party." arXiv preprint arXiv:2009.01631 (2020)
[9] Mazzoni, M., Corradi, A., & Di Nicola, V. (2021). Performance evaluation of permissioned blockchains for financial applications: The ConsenSys Quorum case study. Blockchain: Research and Applications, 100026
[10] De Angelis, S., Zanfino, G., Aniello, L., Lombardi, F., & Sassone, V. (2022). Evaluating Blockchain Systems: A Comprehensive Study of Security and Dependability Attributes. 4th Distributed Ledger Technology Workshop (DLT 2022)
[11] Lombardi F. & Fanton, A. (2022). Is DevSecOps Enough? (ITASEC 2022)
[12] Lombardi F. & Fanton, A. (2022) From DevOps to DevSecOps is not Enough. CyberDevOps: an Extreme Shifting-Left Architecture to Bring Cybersecurity within Software Security Lifecycle Pipeline. Software Quality Journal (under revision)

Grazie

gabriele.pascuzzi@conio.com

CONIO