The Custody Protocol

The Case for Custody

Bitcoin investing

- Bitcoins are **easy to buy** on exchanges, but to leave them there has proved to be unsafe (multiple hacks and incidents)
- If you **do not own** your bitcoins' **private key**, then those bitcoins **are not yours**
- Bitcoin financial sovereignty: "be your own bank!" but unfortunately **bitcoin safe storage is quite technical**

In need of custody solutions

- **Institutional investors**: safe custody is not their core business. Traditional financial custody practices are for assets that cannot be stolen and are ill-suited for crypto-assets with irreversible transactions
- **High-net-worth individuals**: threat model (coercion, violence, ransom, etc.)
- **Non-technical individuals**: needs reliable intermediaries

The need for crypto assets' custodians and digital vaults is exploding

Available Custody Solutions

Some companies have developed custody solutions, in particular:

Coinbase Custody

Market leader.
In 2019 Coinbase acquired Xapo institutional business.

Bakkt

Custody service for Bakkt's physically delivered futures.
It is available even to all institutions.

Fidelity Digital Asset

Institutional solution for crypto currencies custody. Available even to European institutions

Gemini Custody

Institutional-grade crypto storage. Pilot Project with State Street.

They practice (to varying degrees) "*security by obscurity*"

Our Solution: An Open Standard For Custody

1. Define a **public protocol**

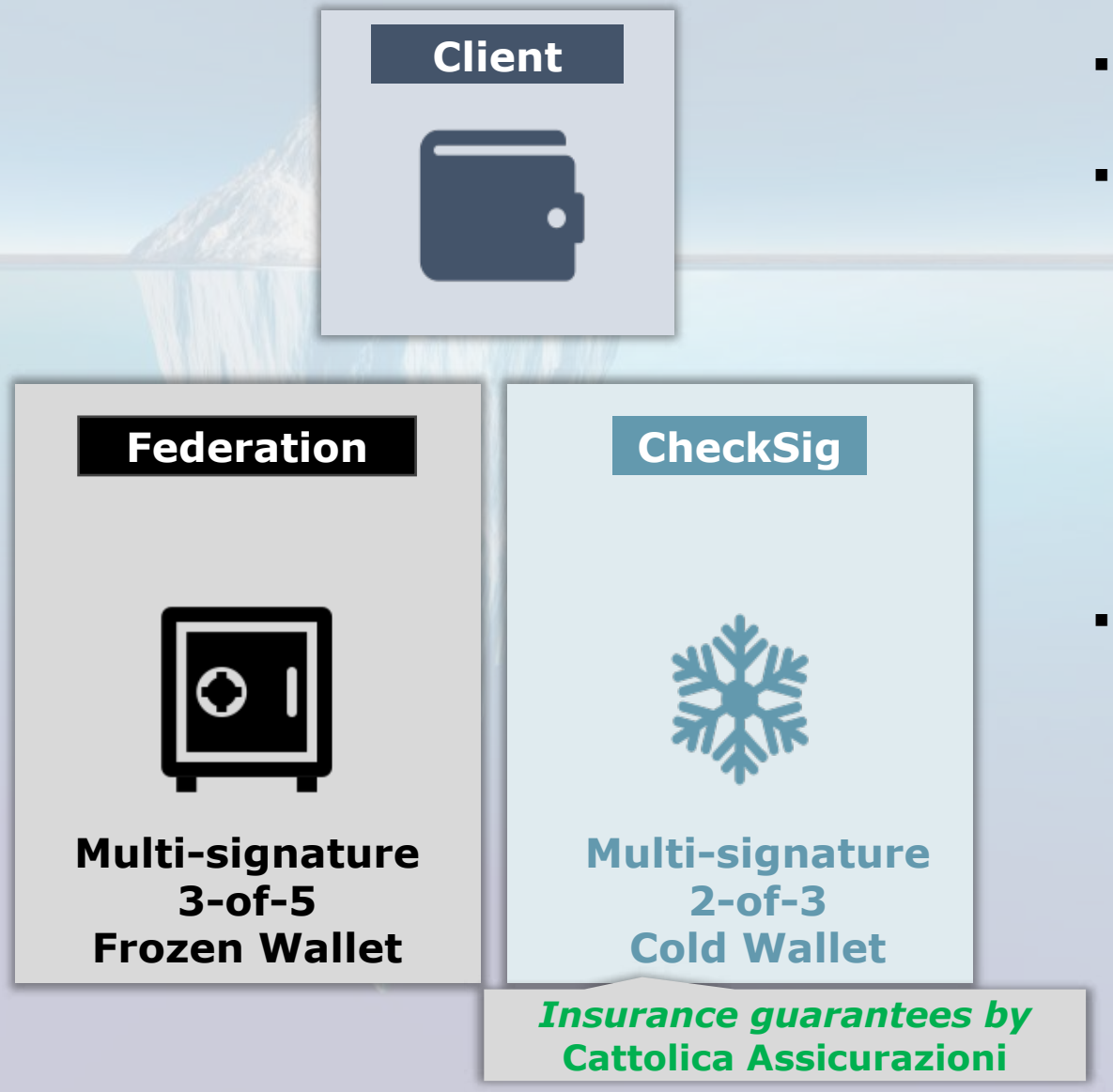
- Open standard
- Fully auditable
- Peer reviewed

Avoid *"security by obscurity"*

2. Develop a **proprietary implementation** of the protocol with:

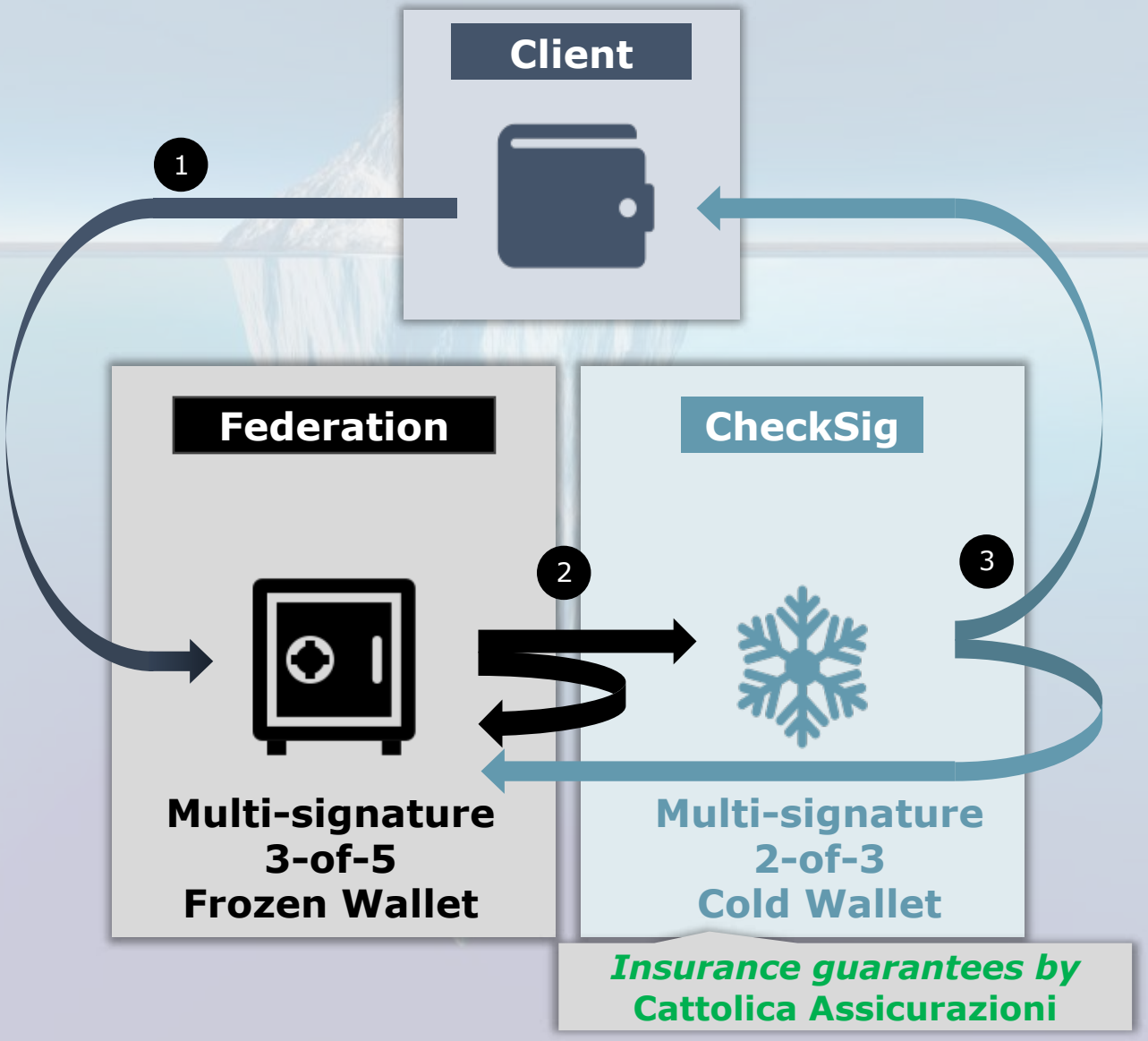
- Periodic proof-of-reserve
- Insurance guarantee scheme
- Canary alert to detect distress
- Multi-location worldwide operations
- Multi-signature
- Secure Hardware Device to sign transactions
- Multi Secure Hardware vendor for risk mitigation
- **Two-level solution**

Two-level Frozen Wallet/Cold Wallet



- The client wants to put his bitcoin in CheckSig Custody
- The **Federation** is a set of **different** (e.g. five) **legal entities,** managing the Frozen Wallet. Each entity has a customized (**locked-down) secure hardware device** that can move coins only if:
  - authorized by CheckSig
  - coins go to the Cold Wallet and/or back to Frozen Wallet
  - **m-of-n** legal entities approve it (e.g. 3-of-5)
- The **Cold Wallet** is managed by CheckSig. It can move coins only if **2-of-3** CheckSig agents sign the transaction, usually moving coins to:
  - the client, upon his/her withdrawal request
  - the Frozen Wallet (if, for whatever reason, the withdrawal request turns out to be illegitimate)

The Transactions Flows



1. The client moves his/her coins to the Federation Frozen Wallet
2. At regular intervals, Federation agents sign an *unlock and redeposit transaction* that:
   - move the coins requested for withdrawal by the client from the Frozen Wallet to an address controlled by the Cold Wallet
   - moves all remaining coins under custody in the Frozen Wallet to another new address controlled by the Frozen Wallet itself: this serves as public verifiable *proof-of-reserve*
3. CheckSig has up to 7 days for security checks. Then:
   - if everything is in order, it forwards the coins to the client (*withdrawal transaction*)
   - in the event of a problem, it moves the coins back to the Frozen Wallet (*redeposit transaction*)

The Recovery Process

Client

Federation

Multi-signature
3-of-5
Frozen Wallet

CheckSig

Multi-signature
2-of-3
Cold Wallet

CheckSig

Multi-signature
2-of-3
Recovery Process

Insurance guarantees by
Cattolica Assicurazioni

The Recovery Process is a **2-of-3** multi-signature setup managed by CheckSig, only used in **disaster recovery scenarios**: if the coins under custody do not move for a long inactivity period, they can be moved (i.e. recovered) using the Recovery Process

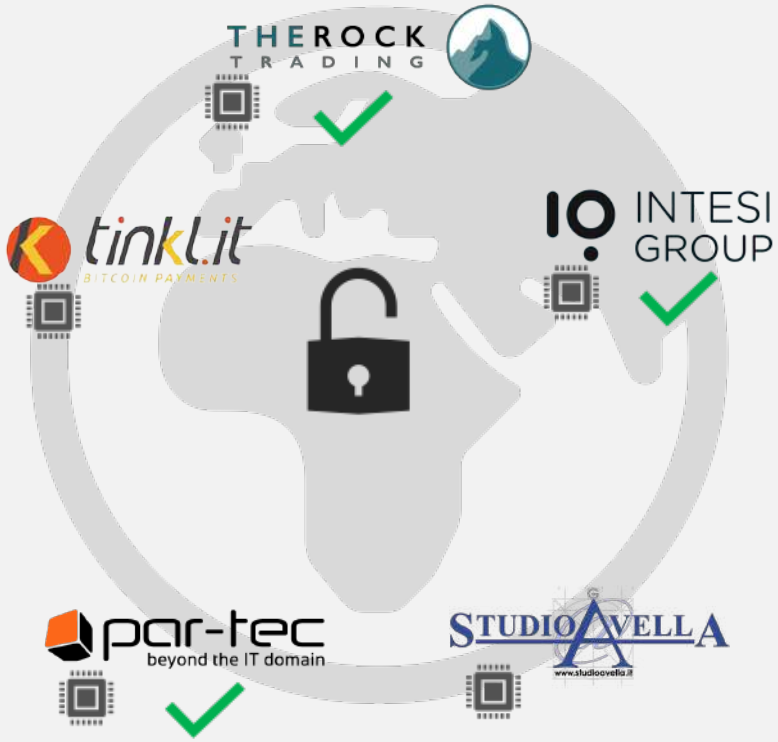
Frozen Wallet: Federation Level

Federation

Coins can be moved only:
1. if authorized by CheckSig
2. to Frozen Wallet and/or Cold Wallet addresses
3. if signed by m-of-n Federation agents

Multi-signature 3-of-5 Frozen Wallet

Multi-entities Federation



- A set of **different** (five) **legal entities**
- Each entity has a **customized** (**locked-down) secure hardware device** that can only move coins to Cold Wallet (*unlock*) or back to Frozen Wallet itself (*redeposit*)
- To move the coins, **3-of-5 signatures** are required
- Legal entities / secure hardware devices are **geographically distributed**
- *Unlock and redeposit* happens on a **periodic** (e.g. monthly) **base**

The Federation Agents

Federation

Multi-signature
3-of-5
Frozen Wallet

- **Studio Avella**: Accounting Company
- **Intesi Group**: Certification Authority
- **ParTec**: Tech Consultancy Company
- **Tinkl.it**: Bitcoin Payment System
- **The Rock Trading**: Crypto Exchange

Cold Wallet: CheckSig Level

CheckSig

Coins can be moved only:
1. after 7 days since receiving them
2. if signed by 2-of-3 CheckSig agents

Multi-signature 2-of-3 Cold Wallet

Multi-signature CheckSig

- **Managed by CheckSig**
- **Off-the-shelf** secure hardware devices with **no limitation**; it will usually move coins to client wallets or back to the Frozen Wallet
- To move the coins, **2-of-3 signatures** are required
- The hardware devices are **geographically distributed and is safe locations**

Disaster Recovery Process

CheckSig

- Frozen Wallet coins can be moved only:
  1. if not moved for a long period
  2. if signed by 2-of-3 CheckSig agents
- Cold Wallet coins can be moved only:
  1. if signed by 2-of-3 CheckSig agents

Multi-signature 2-of-3 Recovery Process

CheckSig Recovery Process

- **Managed by CheckSig**
- **Off-the-shelf** secure hardware devices with **no limitation**, but **coins can only be moved after a long inactivity period**
- To move the coins, **2-of-3 signatures** are required
- The hardware devices are **geographically distributed and is safe locations**
- Used to recover coins if the Frozen Wallet loses its 4-of-7 quorum or the Cold Wallet loses its 2-of-3 quorum

Insurance, Compliance, and Certifications

Insurance:

- Insurance guarantees by SATEC Underwriting (Cattolica Assicurazioni)
- **First and only** italian insurance contract in the crypto-currency world

Compliance:

- Compliant with best standards of KYC/AML/CFT

Attestation:

- Agreement with Service Auditor to start SOC 1 and SOC 2 attestation procedure
- SOC reports are auditing procedures that provide objective reports on the security of the company internal organization and clients data management


Finanza &Mercati

Fca-Psa, l'intesa b
La cassa extra pia

Bitcoin come l'oro, arriva la cassaforte assicurata

CRIPTOVALUTE

Accordo tra Satec (Cattolica) e la start up CheckSig per la copertura dei rischi

Pierangelo Soldavini

UniCredit, nuovi disagi per i servizi online

Bitcoin come l'oro, arriva la cassaforte assicurata

CRIPTOVALUTE

Accordo tra Satec (Cattolica) e la start up CheckSig per la copertura dei rischi

Pierangelo Soldavini

L'oro di Fort Knox non è assicurato, ma lo sono i trasporti da e per il deposito delle riserve auree americane. Lo stesso si sta realizzando per i bitcoin, che molti considerano come l'oro dell'era digitale. In un nuovo passo di riconoscimento del mondo delle criptovalute nasce la prima polizza specificamente dedicata. Satec Underwriting, società di Cattolica Assicurazioni, ha siglato un accordo per la copertura dei rischi di CheckSig nel servizio di custodia Bitcoin.

Esattamente come succede per le grandi riserve di oro fisico, la copertura non comprende l'asset in bitcoin, ma le operazioni di deposito e ritiro da parte dei soggetti interessati, quelle che avvengono online e che sono quindi più esposte al rischio di furto.

CheckSig è la startup italiana che offre un servizio di custodia Bitcoin per investitori istituzionali, banche comprese, e high-net-worth individuals risolvendo i problemi legati a sicurezza, complessità tecnologiche e conformità regolamentare per chi vuole investire in criptovalute. Nel rispetto della privacy del singolo cliente, il servizio della startup punta a essere del tutto trasparente, basato su una *proof of reserve*: una cassaforte di cristallo per Bitcoin, come fossero l'equivalente digitale di lingotti d'oro, il cui contenuto e le cui aperture sono osservabili da tutti.

In un mercato offuscato da paradigmi di sicurezza mai pubblici o documentati e proprio per questo tormentato da frodi e scandali, CheckSig si candida a garantire trasparenza: ogni mese la cassaforte virtuale potrà essere aperta solo su iniziativa di cinque entità legali esterne, preautorizzate dalla stessa CheckSig, che comunque non potrà aprirla autonomamente verificando la capacità di tutela, vale a dire l'esistenza effettiva del totale dell'asset depositato. A oggi molti operatori - tipicamente gli exchange, le piattaforme di scambio per criptovalute - forniscono il servizio di custodia ai clienti, che però non hanno alcuna visibilità sull'esistenza effettiva dei bitcoin. Non sono mancati episodi di scomparsa di bitcoin presso questi operatori.

Grazie al know-how tecnologico di Satec Underwriting e di Cattre, società di riassicurazione per rischi non tradizionali del Gruppo Cattolica, è stata messa a punto la prima polizza per il mercato italiano, che copre sia il vero e proprio furto durante le operazioni di prelievo dei bitcoin custoditi, sia i danni derivanti da intrusioni e violazioni della sicurezza e legati al ripristino dei dati.

Nata nell'ottobre 2019, CheckSig ha raccolto a oggi 950mila euro per il 19% del capitale - per una valutazione di 5 milioni - tra business angel e soci societari che si vanno ad affiancare ai tre fondatori: Ferdinando Ametrano, Paolo Mazzocchi ed Eric Ehlers. Tra i finanziatori figura anche The Rock Trading, l'exchange italiano che non fornisce servizio di custodia e che ha siglato con la startup un accordo per l'acquisto e la vendita delle criptovalute per i clienti CheckSig.

CATTOLICA ASSICURAZIONI
DAL 1896

CheckSig Custody: Hardware Security

Multi Secure Hardware vendor for risk mitigation:

- Signed support agreement with Ledger (the biggest and more secure hardware wallet vendor) and CryptoAdvance

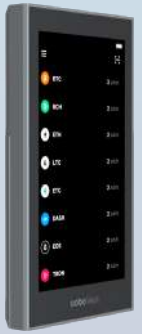
Ledger

crypto advance.

- Under consideration: Cold Card and/or Cobo Vault

COLDCARD

cobo



www.checksig.io

info@checksig.io