UNBOUND

Safeguarding Digital Assets

With an Enterprise Grade Security Platform

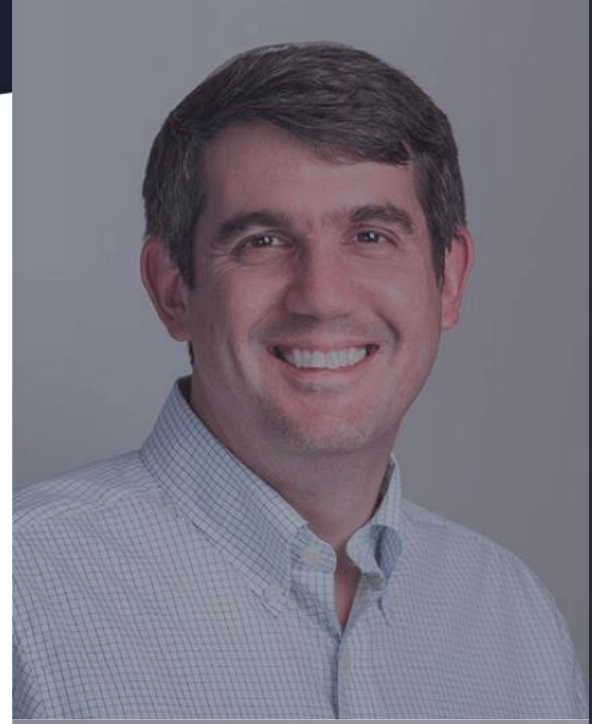
Rebecca Aspler
Director, product Management

WHO WE ARE

Unbound delivers secure, scalable and agile **cryptography designed for the digital business**.

Developed by **world-renowned scientists** in the field of Multiparty Computation.

Built on **100 person-years** of cryptographic research and development experience.



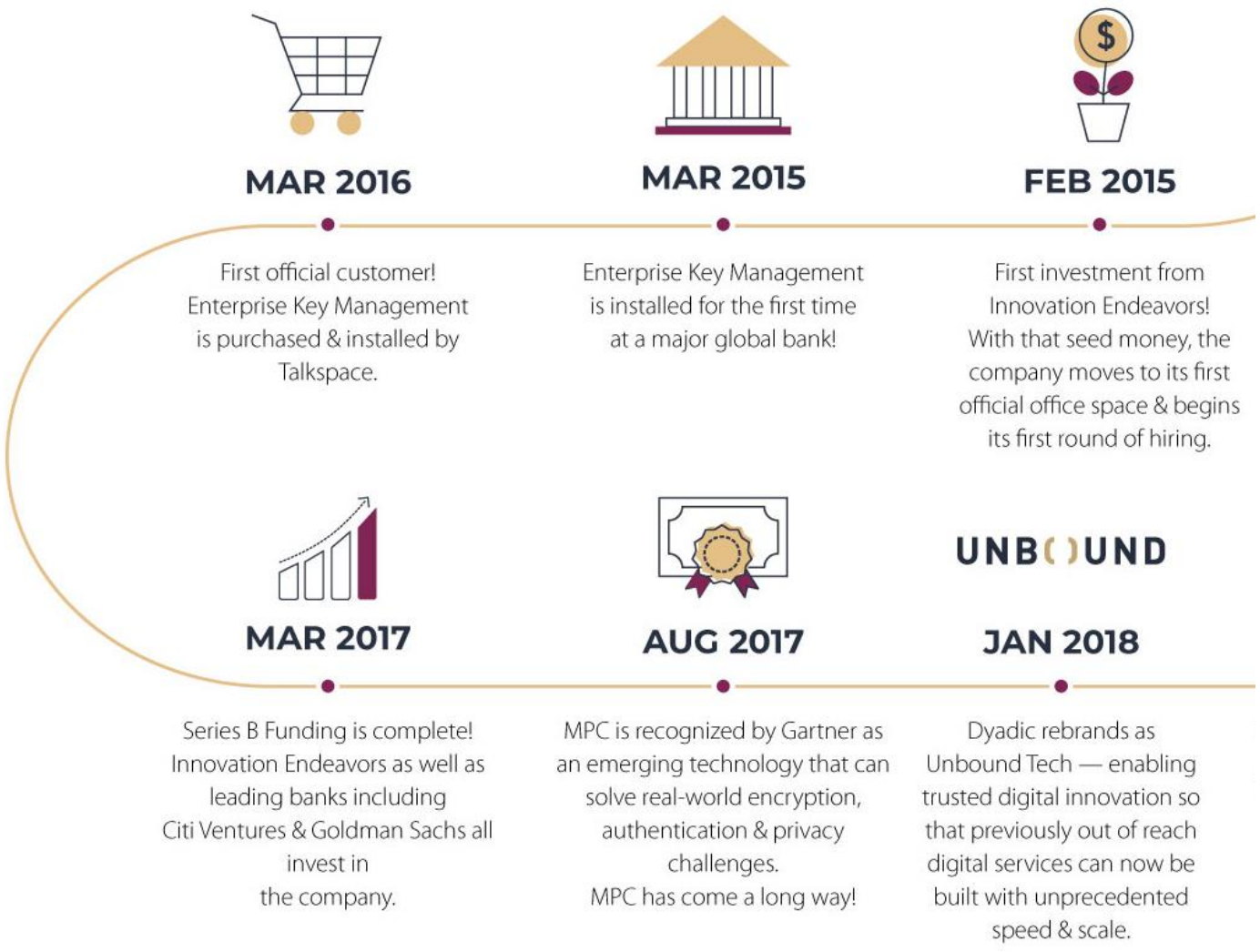
Prof. Yehuda Lindell
CEO, Co-founder

Wikipedia

Prof. Nigel Smart
Co-founder

Wikipedia

Unbound Timeline



- Established in 2015
- Our business is safeguarding Digital secrets – we are eliminating risks.
- Our solutions are based on revolutionary breakthroughs in cryptography – Multi-Party Computing (MPC)
- Working with Fortune 500 enterprises and top global exchanges

UNBOUND

Market State

- Investors want digital assets in their portfolio.
- The regulator has been catching up.

Institutional interest Grows

TYPES OF ASSET CLASSES

Below are various financial products which show similar characterisitcs and behaviour

www.jagoinvestor.com

CASH	EQUITY	FIXED INCOME	REAL ESTATE	COMMODITIES
Liquid Funds	Startup Funding	Endowment Policies	REIT	Corn
Saving Account	Index Funds	Debt Mutual Funds	Commercial Property	Wheat
Online Wallets	ETF's	Debentures	Bunglow	Crude Oil
Hard Cash	Equity Mutual Funds	EPF/ PPF / NSC	Plots	Copper
	Stocks	Bonds	Flats	Silver
		Post Office Products		Gold
		Recurring Deposits		
		Fixed Deposits		
Represents	Represents	Represents	Represents	Represents
Liquidity and Power to buy Anything	Ownership into a business	Lending money to someone	Ownership of Physical space	Ownership of goods which has an end use

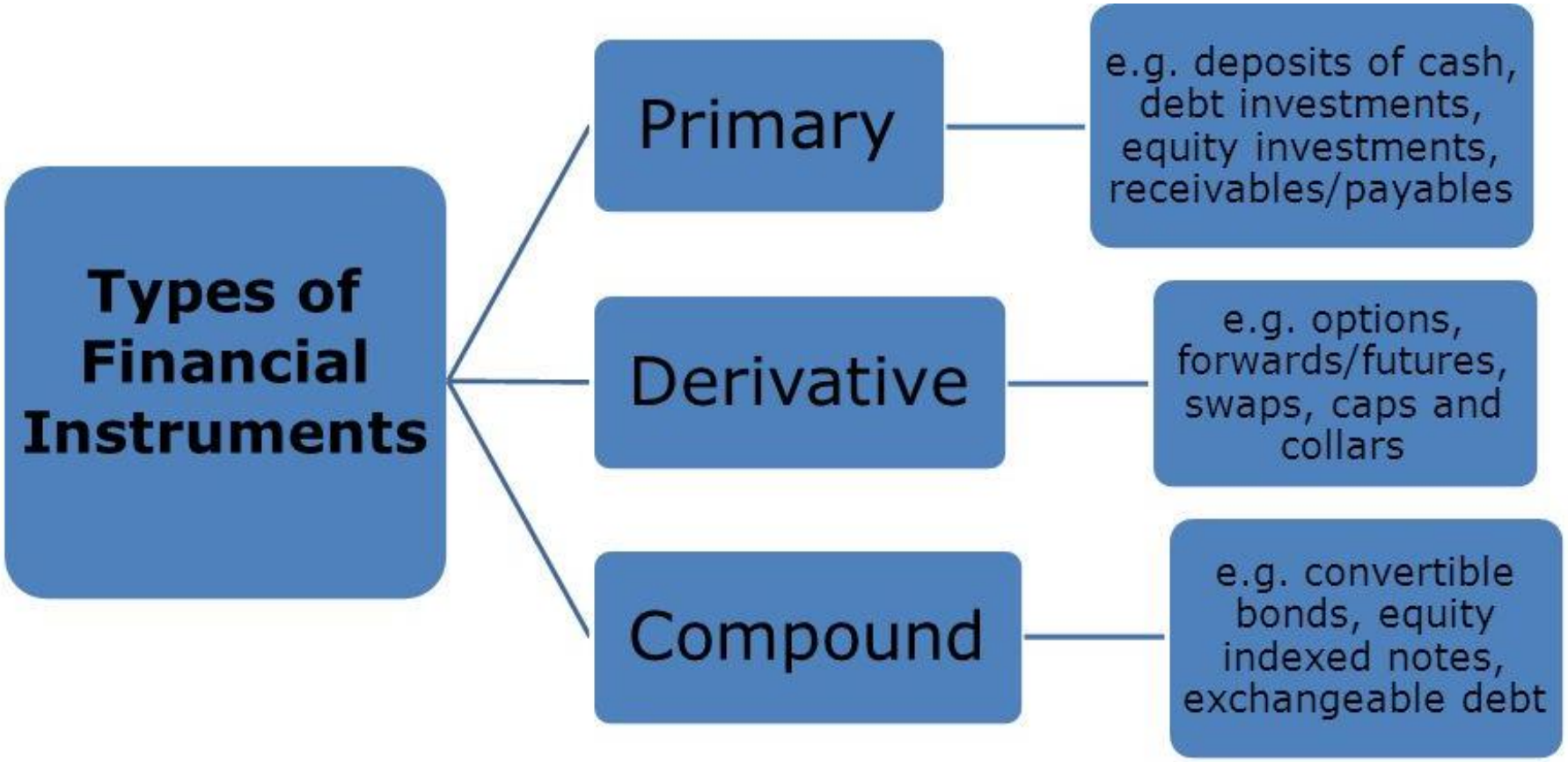
- Cryptocurrencies
- Security Tokens
- Utility Tokens
- Stable coins
- Smart Contracts

Blockchain Digital Assets

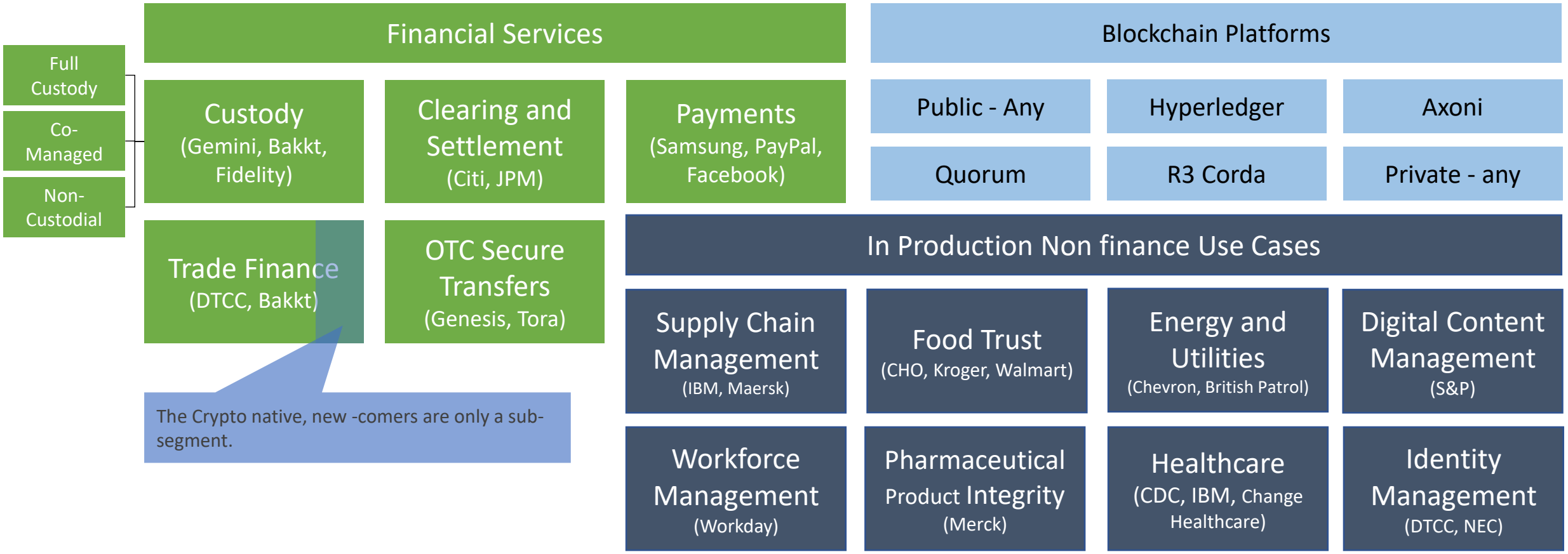
A New Financial Asset Class

UNBOUND

Financial Instruments



In Production – Blockchain Use Cases



UNBOUND

Front office	**Asset management** - Investment research - Portfolio and risk management - Sales and client relationship management - Product development	**Trade execution** - Financial Information eXchange (FIX) connectivity - Trade order management and execution	
Middle office	**Investment operations** - Billing - Cash administration - Client data warehouse - Client reporting	- Corporate actions processing - Data management - OTC derivatives processing	- Performance and analytics - Portfolio recordkeeping and accounting - Reconciliation processing - Transaction management
Back office	**Fund accounting** - Daily, monthly, and ad-hoc reporting - General ledger - NAV calculation - Reconciliation - Security pricing	**Global custody** - Assets safekeeping - Cash availability - Failed trade reporting - Income/tax reclaims - Reconciliation - Trade settlement	**Transfer agency** - Shareholder servicing

Financial Handling of Orders
A Multi Layered Approach

UNBOUND

Challenge
The Key is the Asset

Capital Markets

Every Transaction Requires Key Based Authentication and Authorization

UNBOUND

Key = Asset

Lose the key → lose the asset

Key Usage = Steal

Just one private key operation stands between the fraudster and the asset

No Do-Overs

The blockchain is decentralized and transactions are

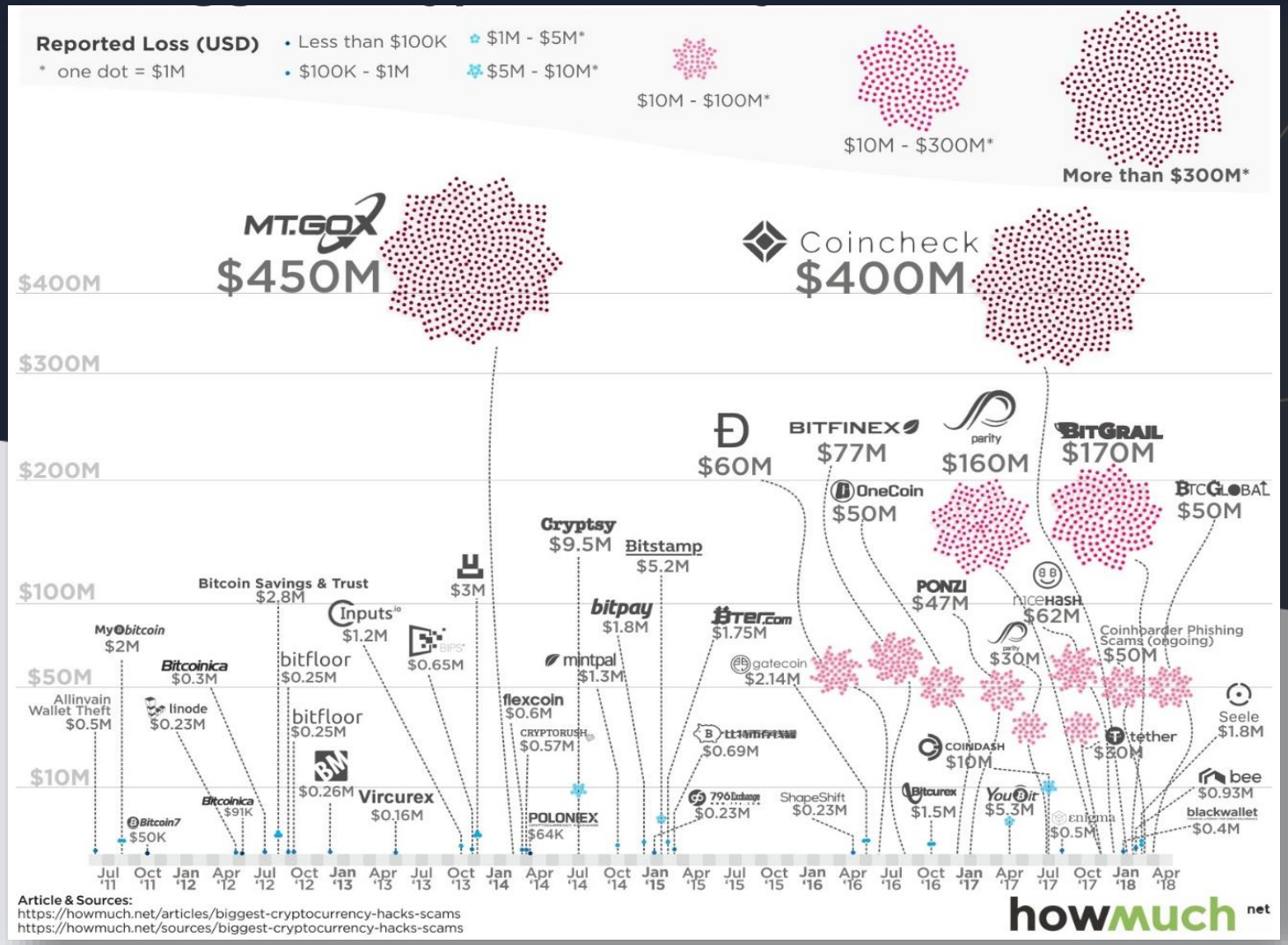
non-reversible

Capital Markets - Various Threats and Challenges

UNBOUND

1. The key is the asset
2. Outside Attacks
3. Insider Threats
4. Operational Errors
5. Regulator Requirements
6. Insurers Requirements
7. Market Agility
8. Customers' Trust
9. Liquidity

The Biggest Cryptocurrency Hacks and Scams

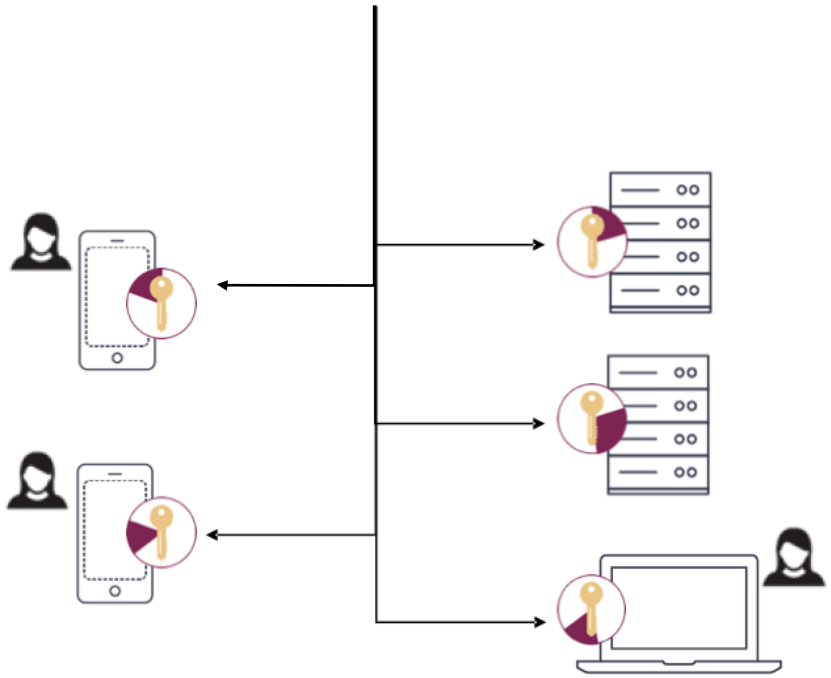


UNBOUND

How Unbound MPC Security Platform is Addressing Capital Markets Needs

UNBOUND

Sign transaction



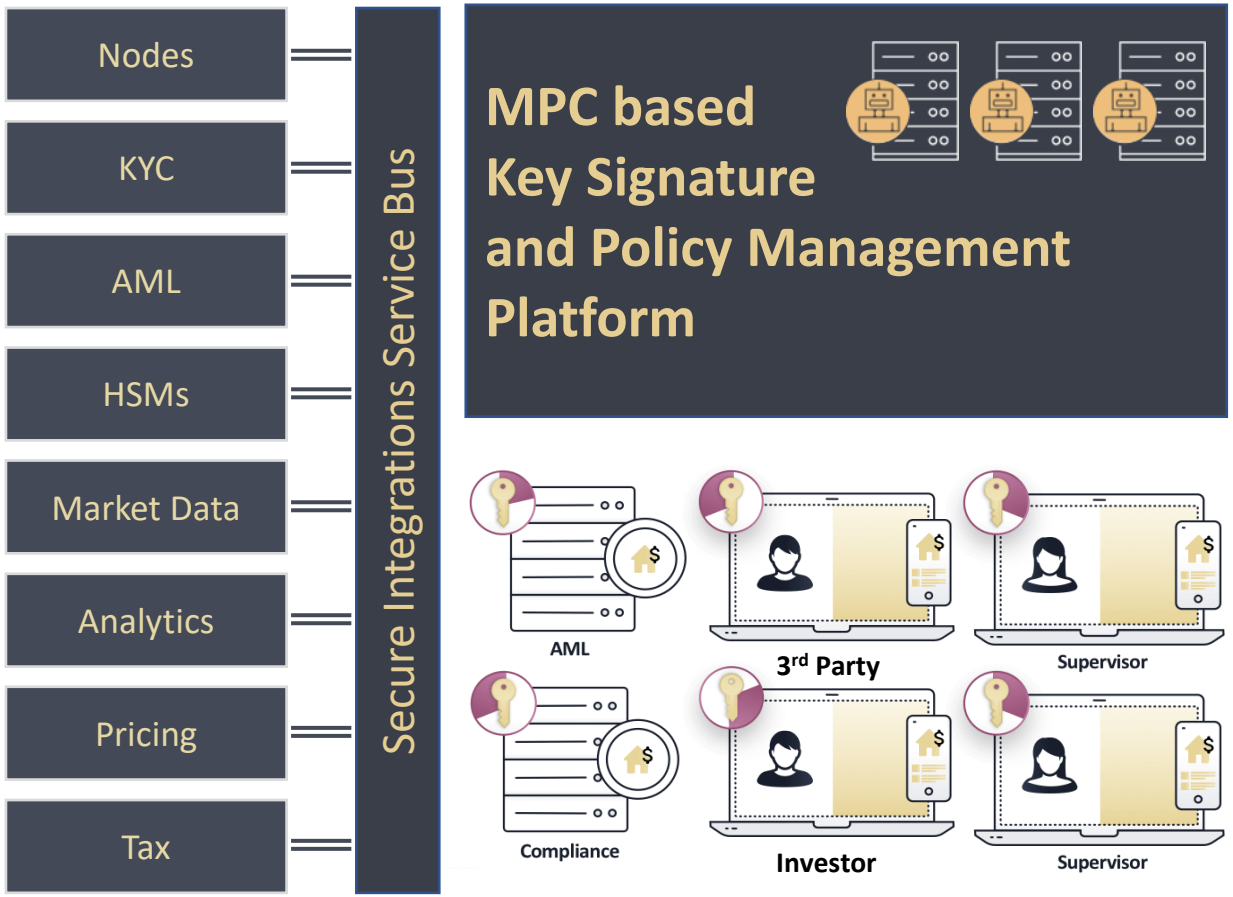
Pure software approach

- Split the key into different random shares
- Place the random shares in different, highly segregated places (any hardware)
- Perform all cryptographic operations using key shares without ever bringing them together
- Shares are refreshed continuously

How does it work?

- MPC – sub-field of cryptography since 1980s
- Allows multiple machines to jointly compute a function while keeping their inputs private
- Security guarantee – mathematically proven
- Recent protocol optimizations enable commercial use

UNBOUND



Robust Cryptographic Platform

- Based on FIPS 140 L2 validated vHSM
- MPC Based - Approvers hold only key shares
- Easy incorporation of any asset
- Distributed policy validation

Institutional-grade policy controls

- Cryptographically validated
- Multiple approvers enforce policies
- A group of admins
- Whitelists

Built in Integrations streamline your business

- Node management
- KYC and AML
- Market data and pricing
- Analytics and Reporting

UNBOUND

"By 2022, at least 50% of major cryptocurrency exchanges will use **multiparty computation (MPC)** to support multiparty signoff and protect user private keys, up from less than 1% today."

Gartner®

Cool Vendors in Blockchain Security and Privacy, 2019

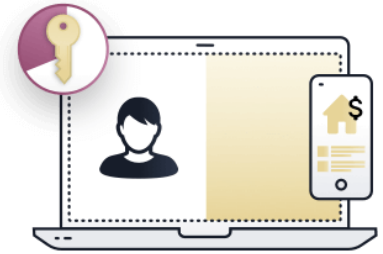
UNBOUND

Challenge
Enterprise Grade Policy Controls

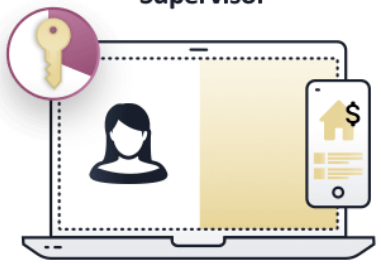
Proactive Compliance – Segregation of Authorities

UNBOUND

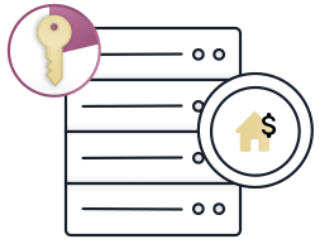
Customer (1-of-2) AND **Service Provider (3 of-5)** AND **Trustee (1-of-2)**



Supervisor



Supervisor

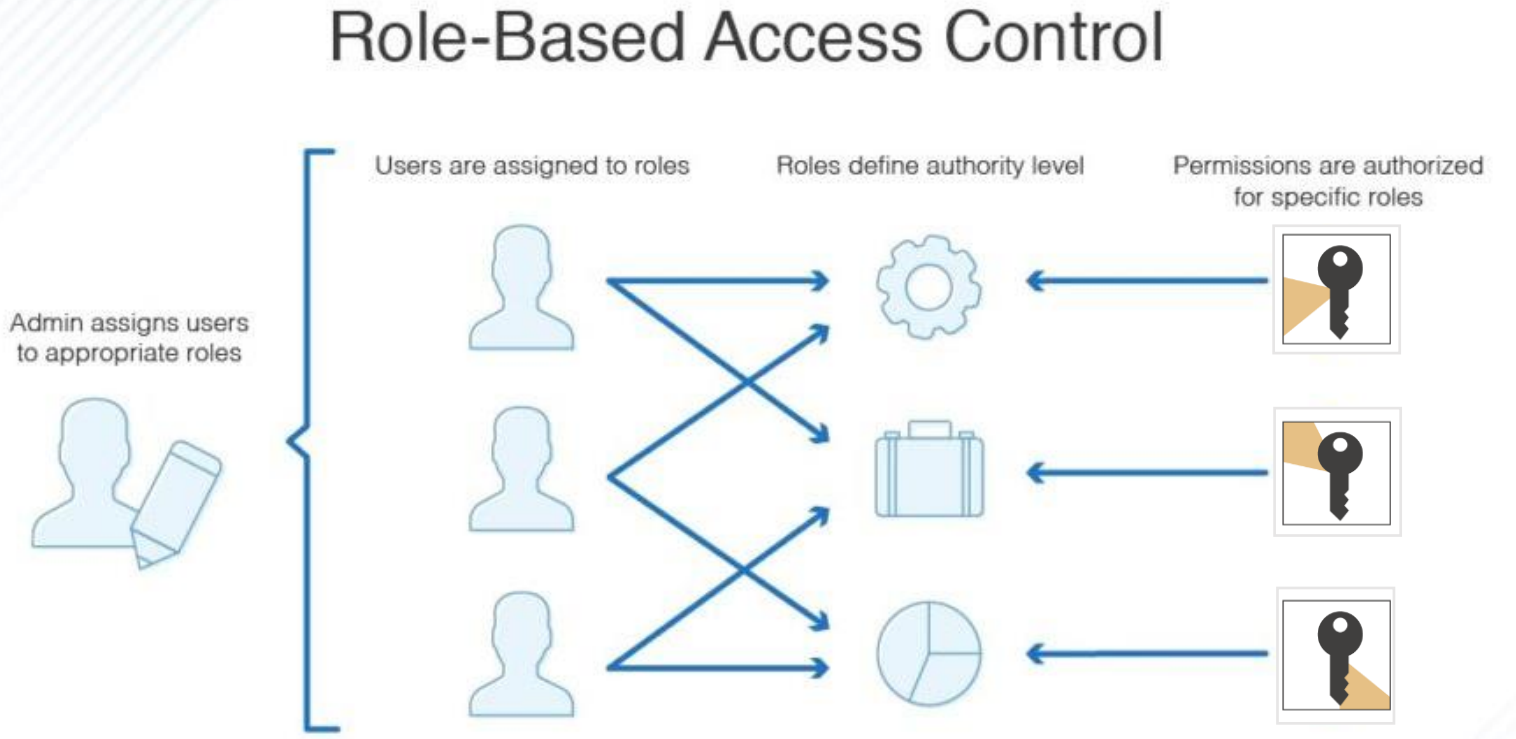


AML

Compliance

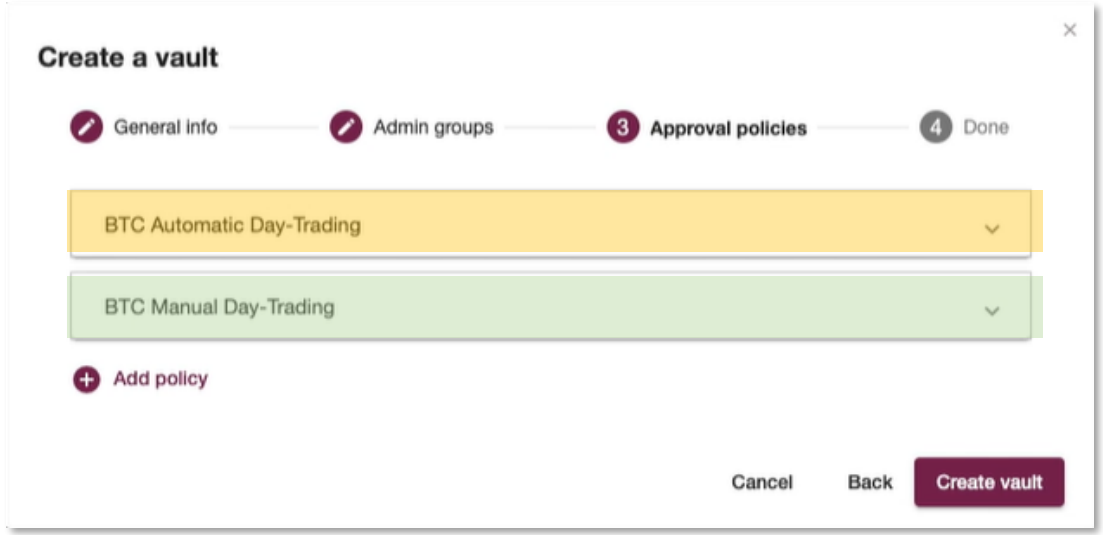
Anti Fraud

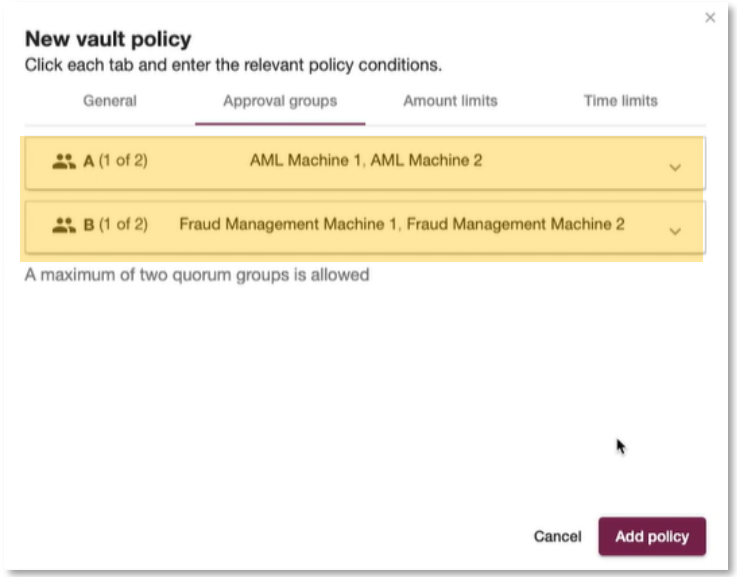
Roles Based Access

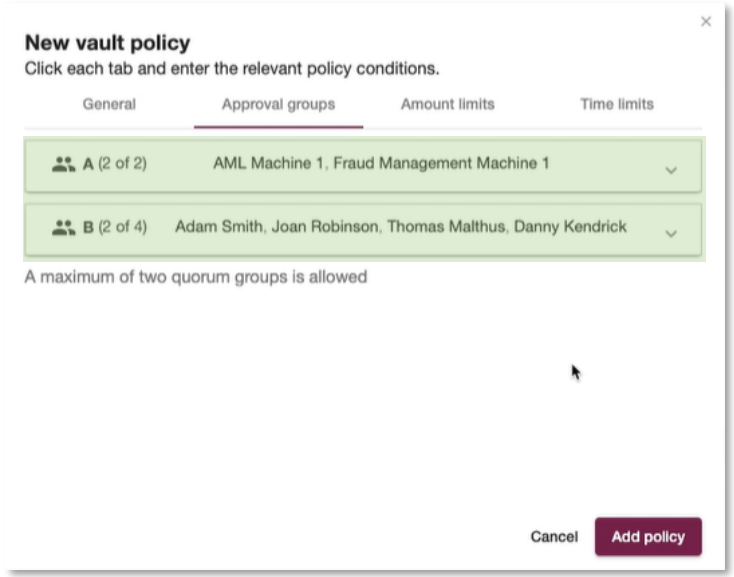


- A role:
  - Consists of one or more users.
  - Defines rights and authority level.
- Users
  - Hold only a key share.
  - Referred to as Participants.
- Approval Policy
  - Per type of action (transaction, change of policy, etc.)
  - Always a group of users.

Proactive Compliance – Risk Based Policies







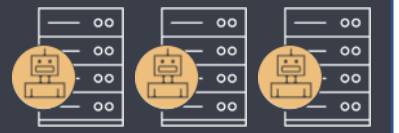
- N risk-level policies in one vault
  - BY asset type
  - By transaction amount
  - By time of day
  - By day of week
  - Custom Policies
- Only a group of users can edit a policy
- Distributed policy validation

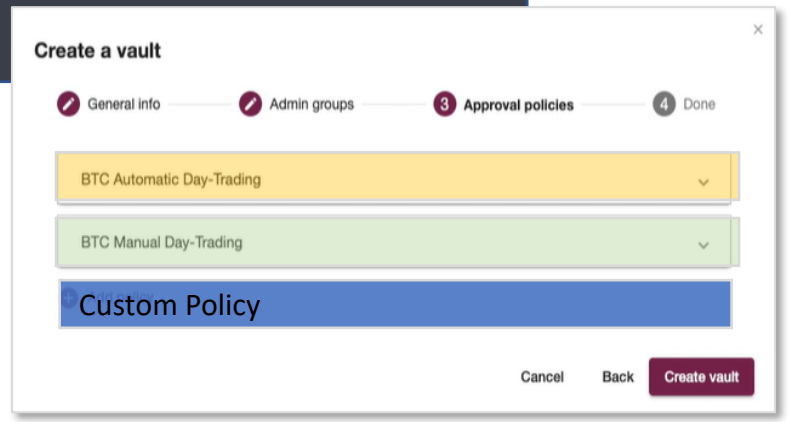
Proactive Compliance – Custom Policies - AML Example

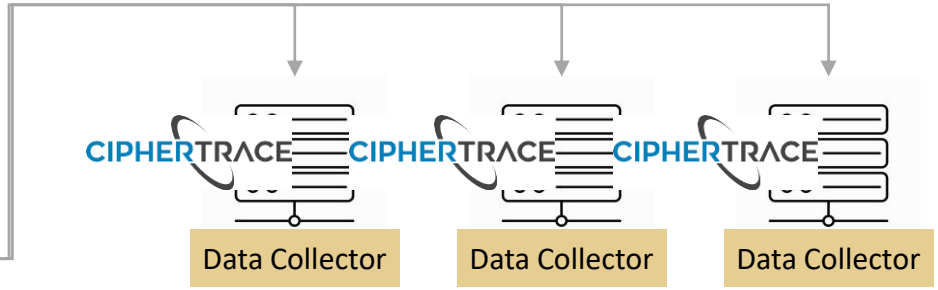
UNBOUND

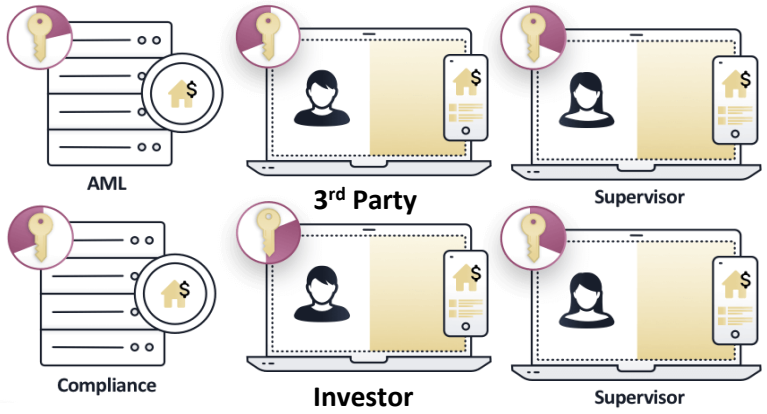
CASP

MPC based Key Signature and Policy Management Platform







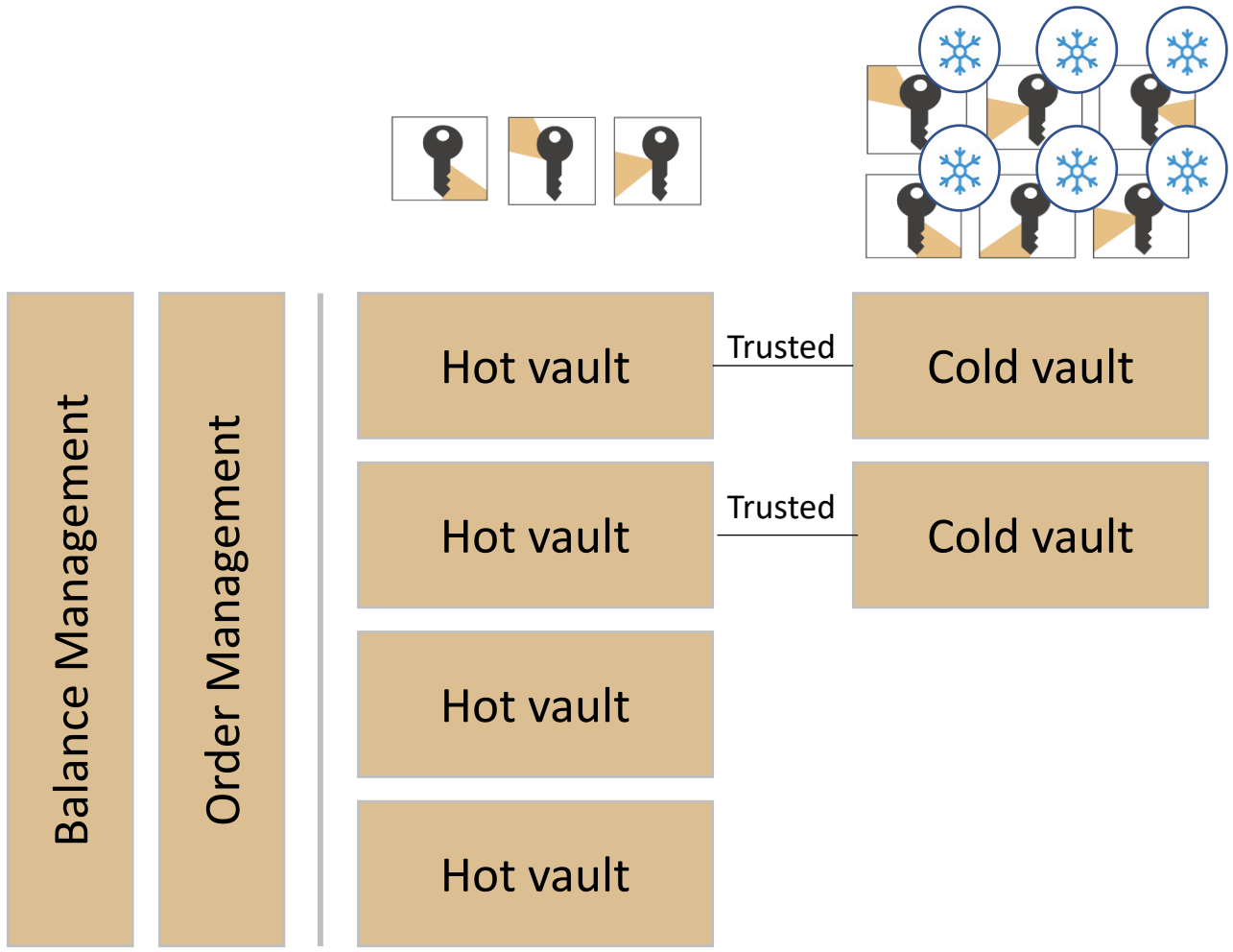


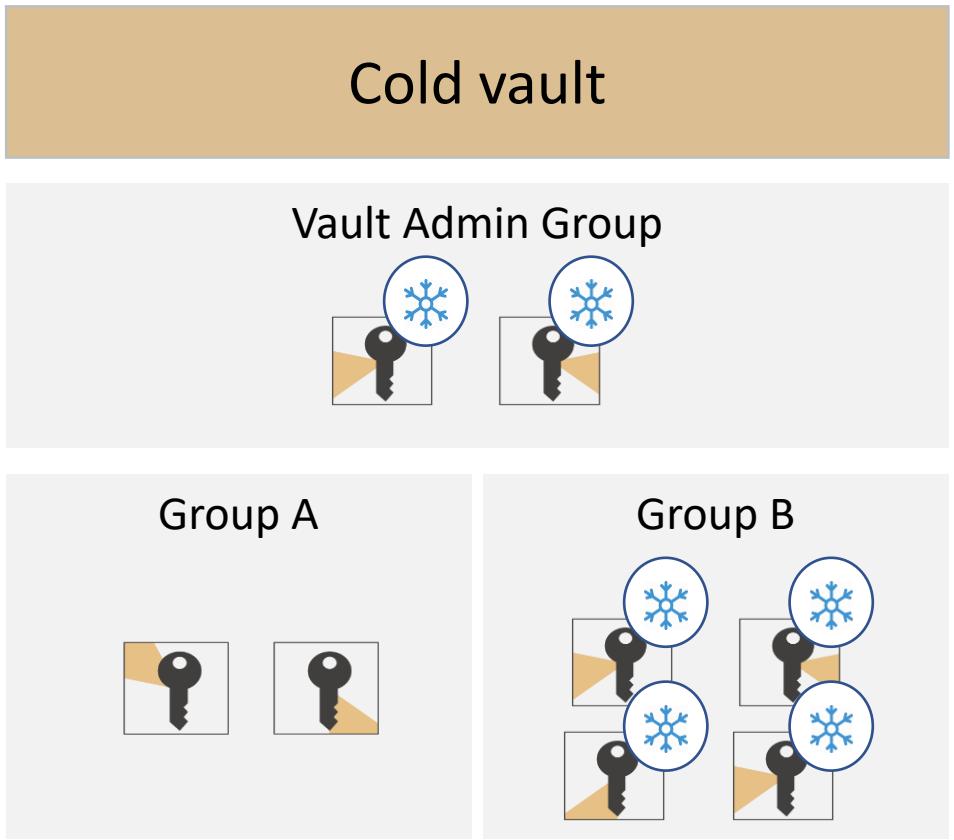
Configurable attributes:
When an address is graded 8+, decline the transaction and when the address is graded 4-7, require human approval and when an address is graded 0-3, approve.

UNBOUND

Challenge
Insurers require the incorporation of cold vaults into the architecture

Hot and Cold Vaults

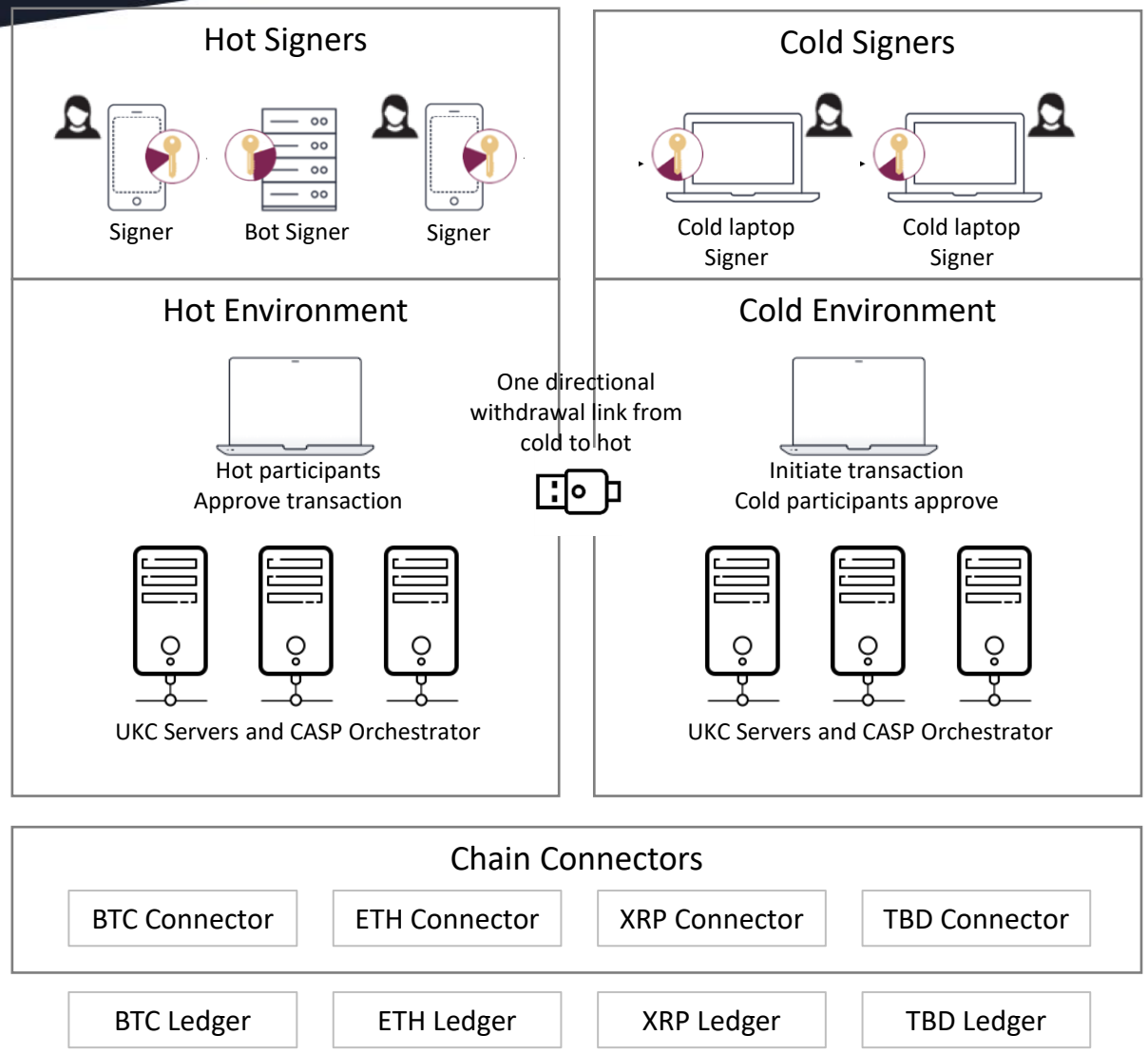




Cold Vault

> Fully cold admin group

➢ Fully cold approval groups



TRUSTED (COLD & HOT) SYSTEMS

- Combining the strength of a cold environment with the ultra-secure, MPC based solution offering.
- Withdrawal data flow is one-directional – from cold to hot only.
- Cold participants sign transactions, physically, in the secured environment.

IBM/Z LINUX ONE AND UNBOUND CASP - BUNDLED

UNBOUND

IBM

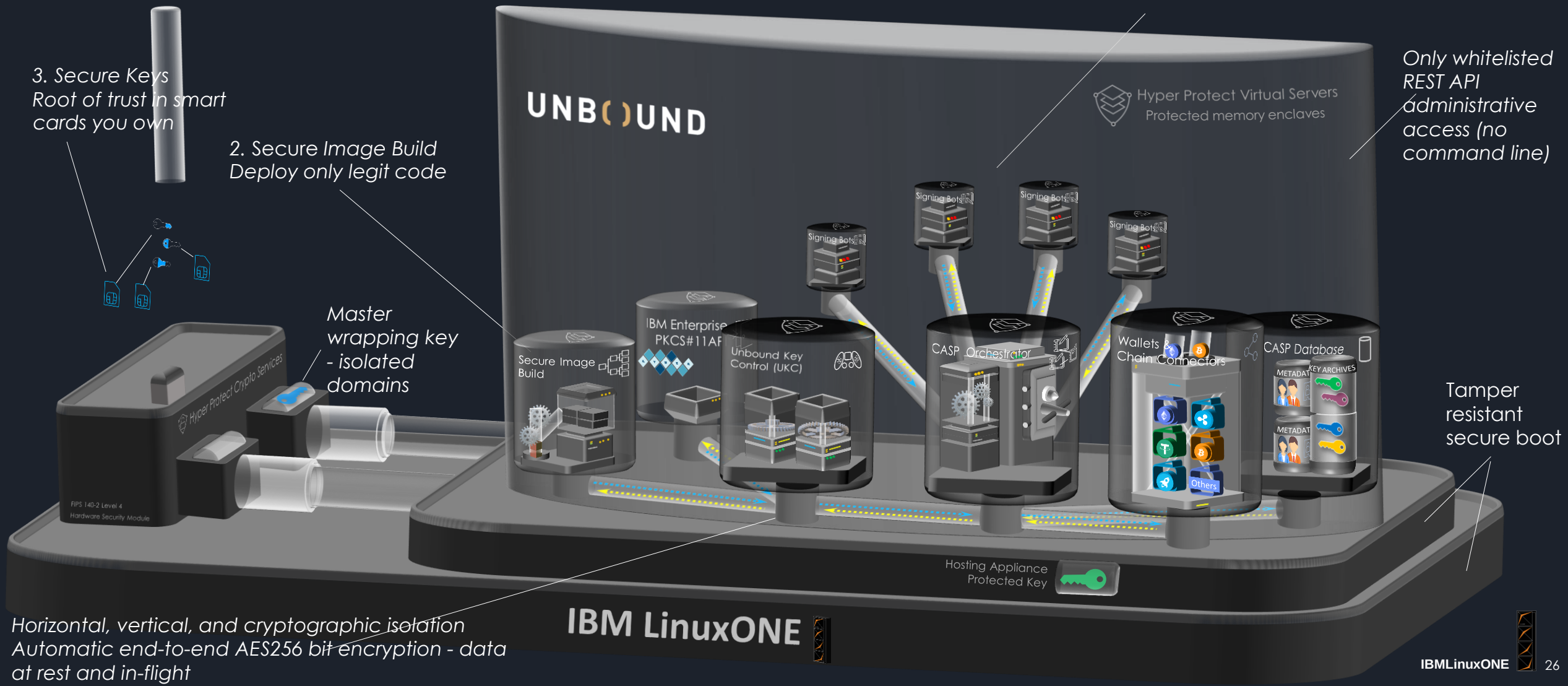
1. Secure Execution
Enclaves isolated from attack

Only whitelisted REST API administrative access (no command line)

3. Secure Keys
Root of trust in smart cards you own

2. Secure Image Build
Deploy only legit code

Master wrapping key - isolated domains



Tamper resistant secure boot

Horizontal, vertical, and cryptographic isolation
Automatic end-to-end AES256 bit encryption - data at rest and in-flight

UNBOUND

Challenge
Regulation Ready Security Platform

Germany - The Banking Act

UNBOUND

Regulation	Unbound Security Platform
The organizational requirements include: • A separate compliance function. • A risk control function and an independent internal audit function. • A relatively strict four-eye principle (that is, that two individuals approve the action) when granting loans or otherwise taking over credit risk.	• Have AML and compliance officers as members of the approval policy • Tamper proof Audit DB assures the validity of the data. • The custodian can utilize that to send out account statements.
• The managers of a bank have an independent obligation to secure compliance with regulatory requirements. Independent means that these responsibilities cannot be overridden by the bank's owners. In that regard, shareholder rights in a financial institution are restricted.	• Policies must not include custodian owners as part of the approval process. • Compliance officers should be part of the approval process of each transaction.
• Account balance and periodic notices	• Vault per customer
Strict auditing requirements and expertise - which can normally be found with one of the four leading accounting firms	• Tamper proof Audit log assures the validity of the data. • The custodian can utilize that to produce data reports to the independent public accountant.

US - Custody Rule – Applied to Funds and Securities

UNBOUND

Regulation	Unbound Security Platform
Qualified custodian. A qualified custodian maintains those funds and securities: i) In a separate account for each client under that client's name; or ii) In accounts that contain only your clients' funds and securities, under your name as agent or trustee for the clients.	• Vault (key) per customer • Tamper proof audit log assures the integrity of the data. • Customer based periodic reports • Insurable platform
Account statements to clients.	
An independent public accountant verifies all of those funds and securities by actual examination at least once during each calendar year at a time that is chosen by the accountant without prior notice or announcement to you and that is irregular from year to year, and files a certificate on Form ADV-E [17 CFR 279.8] with the Commission	

Japan FSA

UNBOUND

Regulation	Unbound Security Platform
Exchanges must go through a rigorous FSA vetting process, particularly focused on cyber security, anti-money laundering, terrorist financing, user protection and data security.	• Have AML and compliance officers as members of the approval policy
In the guidelines and laws related to the Payment Services Act, which was passed in April 2017, the FSA recommends "split management" of assets with a clear classification between the company's cryptocurrency and customer cryptocurrency, as well as management of assets through "cold wallets," or wallets that are managed offline, to the "greatest extent possible."	• Integrate offline signers or fully offline vaults into the architecture
Don’t leave all the funds with one person on one wallet.	• Define multi-party approval policies. • Define a vault per asset and/or per customer
Keep the wallet changing hands consistently.	• Replace signers in an approval policy on a periodic basis

UNBOUND

Challenge
Crypto Agility - The Ability to Support New Assets Quickly

UNBOUND

Secure any asset

- Integrate easily and quickly to protect new ledgers using CASP chain connector framework
- Multi-party approval mechanism applies automatically
- **No need to develop asset-specific code**

UNBOUND

Challenge
Speed to (1) finalize a trade, (2) clear and settle a transaction

UNBOUND

High-Frequency Trading (HFT) requires:

1. Liquidity
2. Efficiency (speed)
3. Trust

CASE STUDY: LIQUID

High Trading Velocity with High Security

UNBOUND

Liquid by Quoine

Need – Assure Customers Trust

- By speeding up trade efficiency.
- By maintaining institution-grade security.

Why Unbound

- Enterprise grade security platform
- Risk based policies
- Operational simplicity

Process and Results

- Increasing liquidity by moving more assets into online MPC-based wallets
- Clearing withdrawals in minutes

UNBOUND

Challenging the (Security) Status Quo

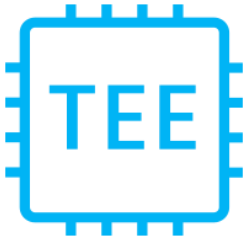
Securing Capital Markets Use Cases - Technologies

UNBOUND

HSM
A hardware security module (HSM) is a physical computing device that (1) safeguards and (2) manages digital keys for strong authentication and provides crypto-processing.

Multi-sig
Multi-signature refers to more than one key to authorize a digital asset transaction.

- Usually 2of3.
- Ledger Specific.



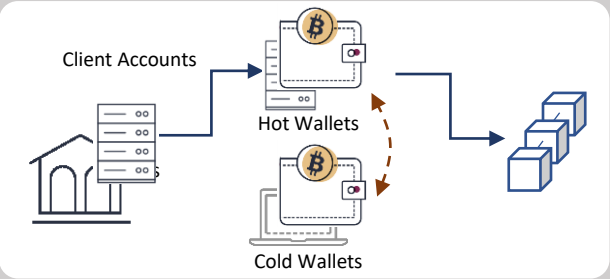
TEE (Mostly SGX)
A TEE as an isolated execution environment on the main processor. Since these are vulnerable to key extraction via software **side-channel attacks,** we will not cover this option today.

MPC
Machines jointly working while keeping inputs private (Zero Knowledge Proof) The key never exists as one entity. It is created and maintained as N random shares

Securing Capital Markets Use Cases - Solutions

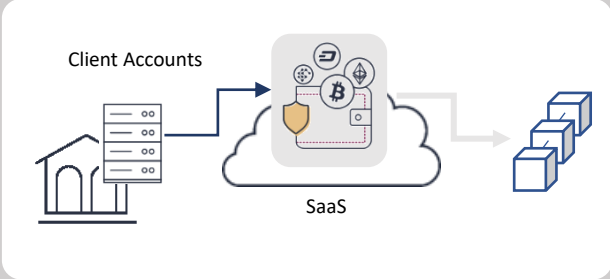
UNBOUND

Home Grown / DIY



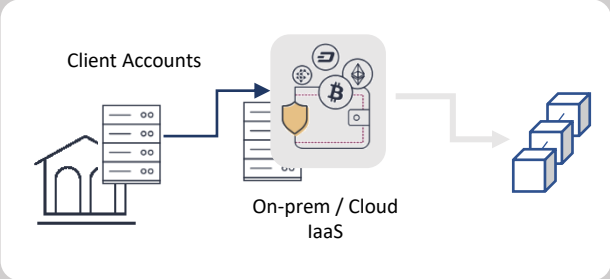
- High TCO.
- Hard to maintain and upgrade
- Key protection (HSM, multi-sig) may be used for added security, but have flexibility and usability limitations

SaaS



- Cloud-hosted secure systems
- Liability is split between the vendor and the customer.
- Dependent on the SaaS provider to add assets and features.

Security Platform



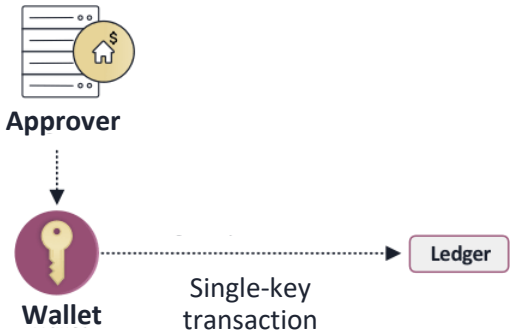
- Security software.
- Integrate with the institution's infrastructure and systems
- Full control over security and key management

MPC = Next Gen Multi-Sig

UNBOUND

Single-key Signatures

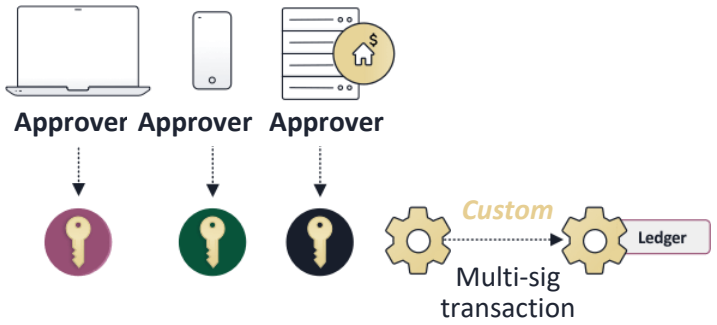
Risky & inflexible



- Key = single point of failure
- Complicated for multiple Tx approvers
- Slow to transact if stored offline
- Vulnerable if used online

Multi-signature

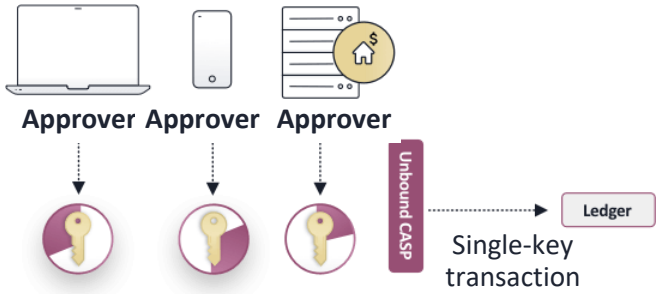
Added security, limited flexibility



- Cryptographic multiparty approval
- Not supported by all ledgers
- Limited quorum group structure
- Hard to change approvers

Multiparty Computation (MPC)

Best-in-class security, flexibility and speed



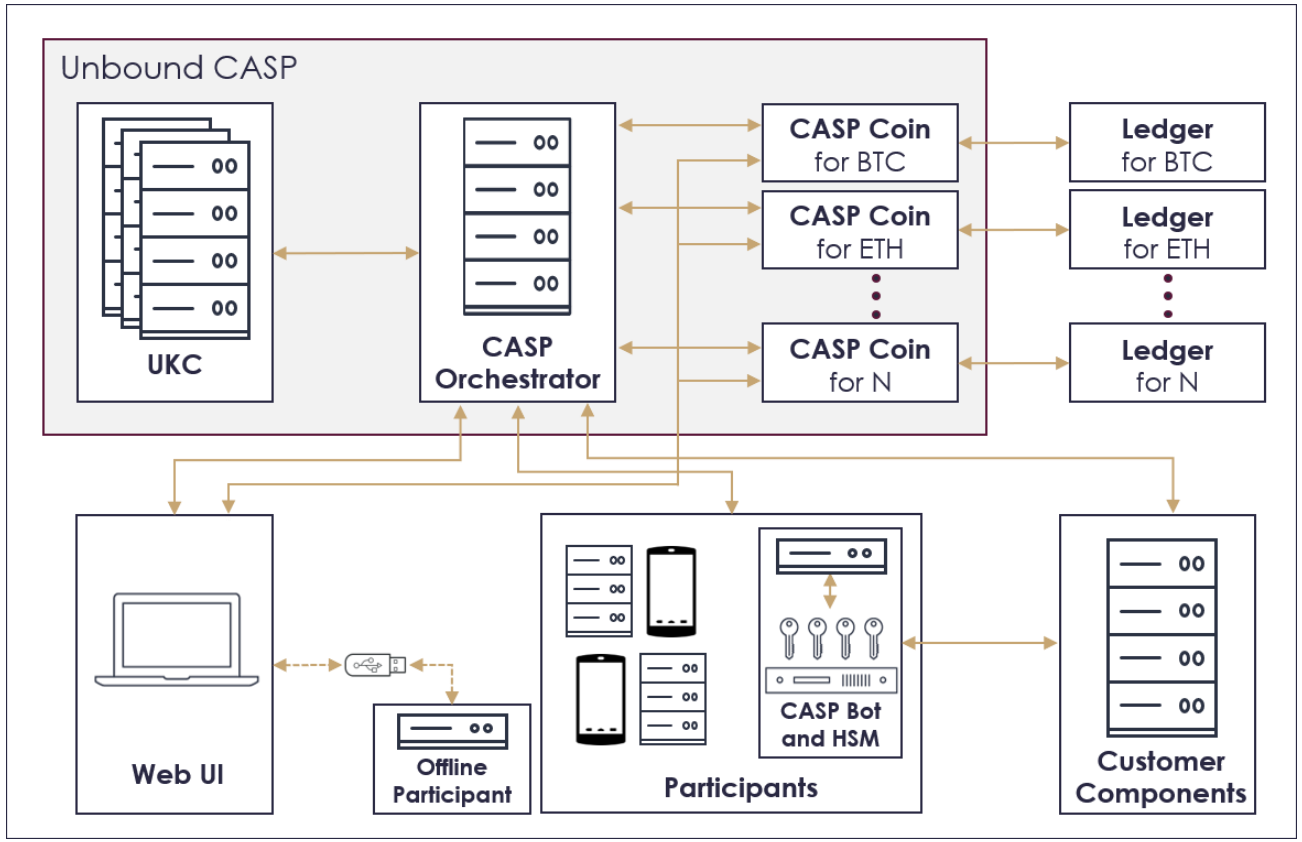
- Cryptographic multiparty approval
- Distributed policy enforcement
- Supports any ledger
- Any quorum size & structure
- Update approvers easily
- Offline approvals
- Optional hardware integration

UNBOUND

Multi Layer Security Approach

UNBOUND

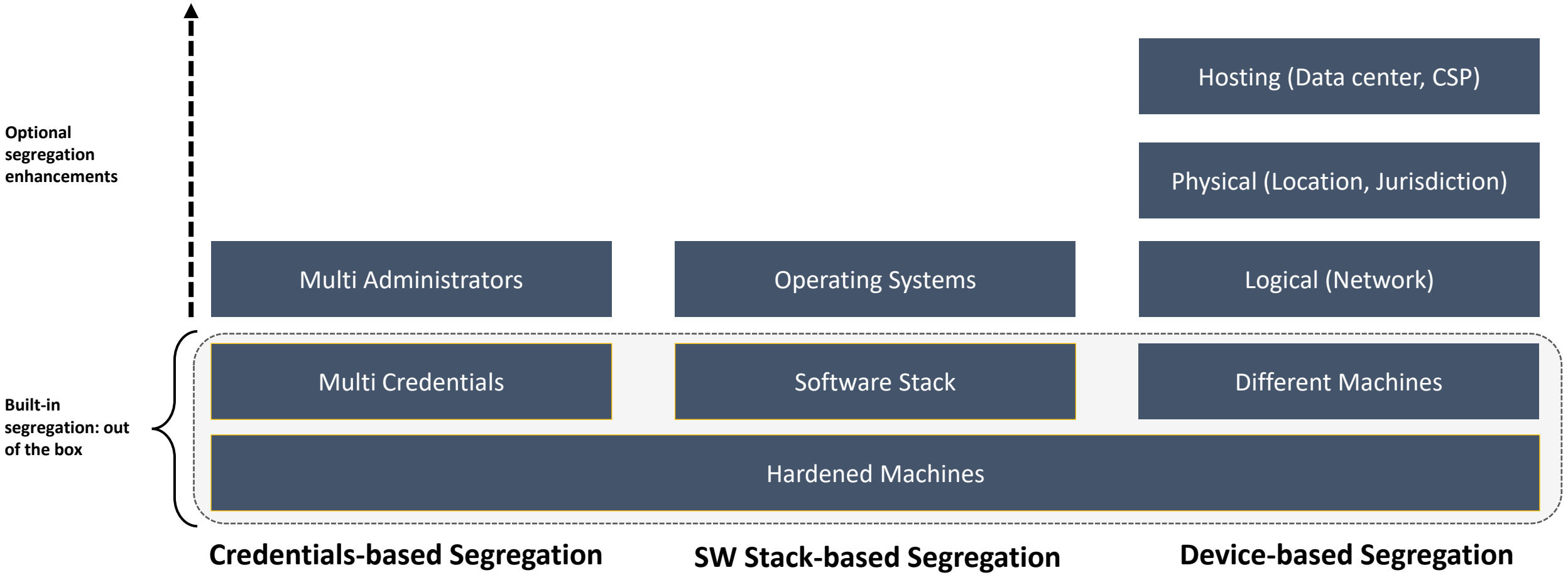
High Level Architecture



- A vault is a secure container for the cryptographic material used to protect a crypto asset, such as the seed or private key.
- CASP uses Multiparty Computation (MPC) to split the crypto material between the different participants in the vault. This ensures that the material never exists in a single place.
- Only the approved quorum of participants can complete a transaction based on the vault definition
- UKC Developers Guide
- CASP User Guide

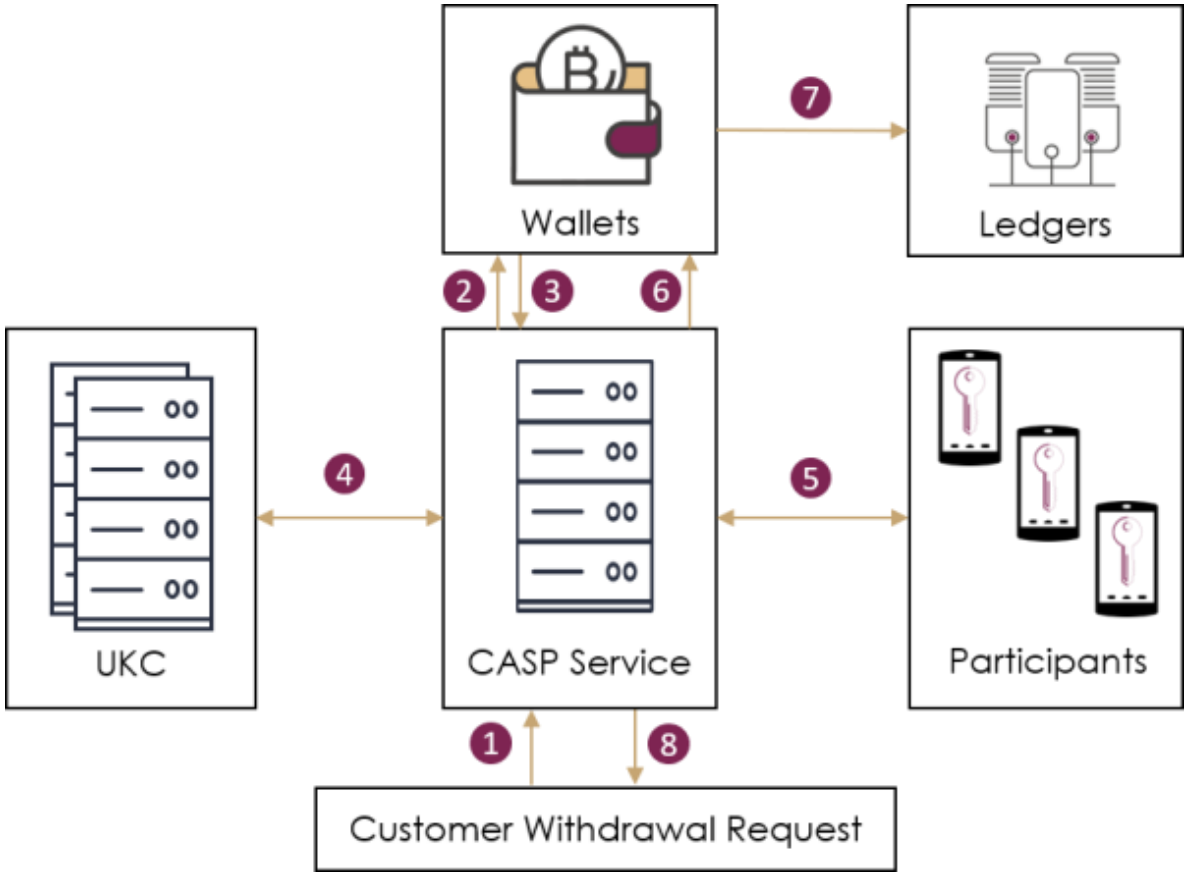
CASP Setup and Component Segregation

UNBOUND



UNBOUND

Transaction Flow



1. A client triggers a withdrawal request that is sent to CASP (web/API). The request includes the raw transaction details and the hash of the raw transaction based on the specific protocol.
2. The wallet computes the relevant transaction details after reading info from the ledger verifying balances, etc.
3. The wallet (chain connector) sends the transaction and hash to the CASP service for signing.
4. Partial work is done on CASP and UKC.
5. CASP sends the transaction details and the partial interim results to all participants. The participants execute their part and send their results back to the CASP server.
6. Once enough results are collected, the signature is computed and returned to the wallet (i.e. chain connector).
7. The wallet (chain connector) sends the signed transaction to the ledger.
8. The plain signature is returned to the customer as a confirmation of the withdrawal.

UNBOUND