

# Blockchain, Crypto Economy & NFTs

FS 2026

## After this mini-lecture you will be able to:

- Explain hot, warm, cold, MPC, and HSM custody architectures
- Describe prime brokerage services for institutional crypto
- Analyse the BUIDL (\$2.9B) and Kinexys (\$1B+/day) case studies
- Evaluate institutional digital-asset strategies under Swiss law (FINMA/BVV2)

## The core question

How do institutions hold, trade, and generate yield from digital assets *without* taking on the operational risks that destroyed FTX?

Full 45-min lecture available: [20260508.0900.institutional.crypto.pdf](#)

## Hot

Online. Instant. Highest risk.  
Exchange float only.

## Warm

Semi-offline. Hours to access.  
Multi-sig. Day-to-day institutional  
flows.

## Cold

Air-gapped. Maximum security. >90%  
of assets. Insurable.

## MPC (Multi-Party Computation):

- Key split into shares across parties; no single party reconstructs full key
- Threshold signing: 2-of-3 parties sign without assembling key
- Used by: Fireblocks, Coinbase, BitGo Prime

## HSM (Hardware Security Module):

- FIPS 140-2/3 certified tamper-proof physical device
- Key generated and used inside device; never exported in plaintext
- Used by: Anchorage Digital, Fidelity Digital Assets, SIX SDX

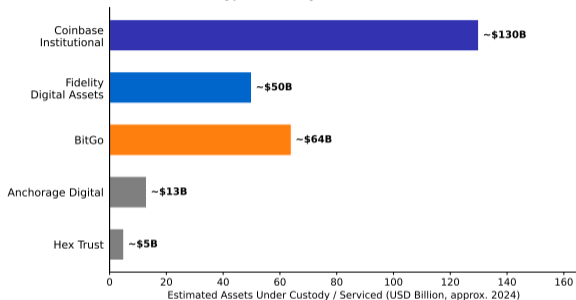
**Best practice:** HSM for root key generation + MPC for operational signing.

---

FTX had no proper custody segregation; customer assets commingled with Alameda trading capital. This is what institutional custody prevents.

# Custody Market & Product Stack

### Institutional Crypto Custody: Estimated Market Positions (2024)



Note: Figures are approximate estimates from public disclosures and press reports. Fireblocks (not shown) reports \$1T+ in transaction volume, not AUM.

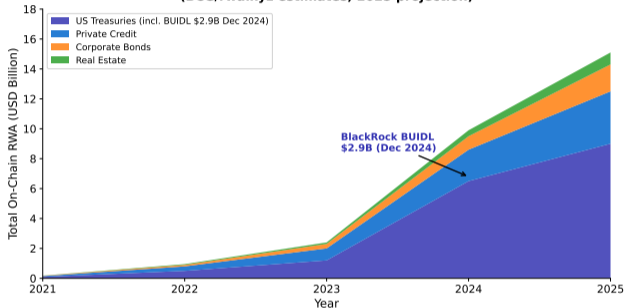
### Institutional Product Stack: Who Offers What?

	Custody	OTC Trading	Margin Lending	Derivatives	Staking Services	Reporting & Tax
Full-Service Platform (Galaxy)	Yes	Yes	Yes	Yes	Yes	Yes
Digital Asset Custodian (BitGo)	Yes	No	No	No	Yes	Yes
Crypto Prime Broker (e.g. Coinbase)	Yes	Yes	Yes	Yes	Yes	Yes
Traditional Bank (e.g. JPMorgan)	Yes	Yes	No	Yes	No	Yes

Legend:   
  Service offered   
  Not offered / limited

Coinbase Institutional leads with ~\$130B AUC. Full-service platforms (Coinbase, Galaxy) approach TradFi prime broker capability.

**Real-World Assets On-Chain: Market Growth 2021-2025**  
(BCG/rwa.xyz estimates; 2025 projection)



Note: Total on-chain RWA market estimated 4T – 16T addressable (BCG 2022 / Citi 2023 range).  
On-chain actual: ~\$15B deployed as of early 2025 per rwa.xyz.

## Why tokenise real-world assets?

- T+0 settlement (vs. T+2 traditional)
- Programmable compliance (KYC embedded in token)
- 24/7 markets for illiquid assets
- DeFi composability (yield-bearing collateral)

## Market (2025):

- Total deployed: ~\$15B (as of 2025; rwa.xyz)
- Addressable: \$4T–\$16T (BCG/Citi estimate)
- Largest fund: **BlackRock BUIDL \$2.9B** (as of 2024)

US Treasuries dominate on-chain RWA (~\$9B). BlackRock BUIDL reached \$2.9B December 2024, surpassing Franklin FOBXX as largest tokenised fund.

## BlackRock USD Institutional Digital Liquidity (BUIDL)

- Launched: March 2024, Ethereum (Securitize)
- Structure: tokenised money-market fund (US Treasuries)
- AUM: **\$2.9B by December 2024**
- Min. investment: \$5M (institutional only)
- Settlement: T+0 via USDC stablecoin swap

### Why it matters

- World's largest asset manager (\$10T+ AUM) validates on-chain funds
- DeFi protocols can use BUIDL as yield-bearing safe-asset collateral
- Franklin FOBXX (2021) was first; BUIDL proved institutional scale

**Key AC:** BUIDL AUM at launch = \$0. By Dec 2024 = \$2.9B. Not \$500M.

---

Franklin FOBXX (2021) was the first US-registered mutual fund on blockchain. BUIDL is the first at institutional scale with DeFi integration.

## Kinexys (formerly JPMorgan Onyx, rebranded 2024):

- Core: intraday US dollar repo settlement on private Ethereum
- **Volume: \$1B+ daily repo settlement** (2024) (Source: JPMorgan Kinexys reports, 2024)
- Counterparties: BlackRock, Barclays, BNY Mellon, Siemens
- Also: tokenised collateral mobility (tri-party repo), multi-currency payments

## ROI mechanism:

Traditional repo closes 3pm. Kinexys settles 24/7. Frees trapped intraday collateral. Estimated \$1M+/day client collateral savings (press reports).

## Why Kinexys works

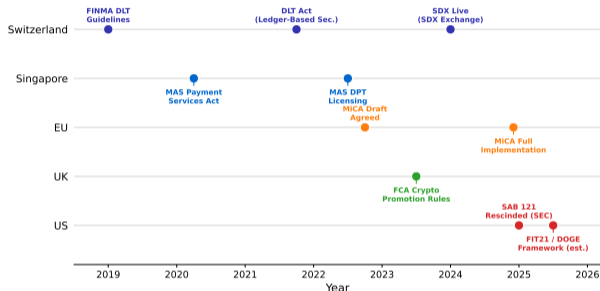
Satisfies all 5 blockchain criteria:

- Multiple parties: yes
- Shared truth: yes
- Intermediary removal: yes
- Immutability: yes
- Tokenisation: yes

---

Kinexys is the largest-volume enterprise blockchain use case globally by daily settlement value. The rebranding from "Onyx" signals product maturity.

## Crypto Regulatory Milestones by Jurisdiction (2019-2025)



Note: Switzerland DLT Act (2021) enabled ledger-based securities. EU MiCA fully in force Dec 30, 2024. US framework remains fragmented; SAB 121 rescinded Feb 2025.

## Swiss context for pension funds:

- **FINMA**: supervises Pensionskassen and crypto custodians
- **BVV2 / OAK BV**: governs pension investment categories (Art. 55 “other investments”  $\leq 15\%$ )
- Swiss DLT Act (2021): created ledger-based securities as legal asset class
- **MiCA is EU law**: does *not* apply to Swiss pension funds

**Recommended path** for most Swiss Pensionskassen (2024-2025): SIX-listed crypto ETP (FINMA-regulated, clean BVV2 fit).

Switzerland DLT Act (Feb 2021) is the key legal enabler for institutional on-chain assets in Switzerland (Source: Swiss Federal Council, 2021). EU MiCA (Dec 2024) applies to EU-domiciled entities only (Source: MiCA Official Journal, 2023).

## How institutions access crypto:

- **Spot ETFs:** iShares IBIT, Fidelity FBTC; pensionable via BVV2/OAK BV test
- **Tokenised funds:** BUIDL (\$2.9B), FOBXX; daily NAV, T+0 liquidity
- **Regulated derivatives:** CME futures, cash-settled, no custody needed
- **Direct custody:** maximum exposure, maximum compliance burden

## Key barriers (falling, not gone):

- Basel III: 1250% risk weight on Group 2 crypto
- SAB 121 (US, 2022–2025): forced on-balance-sheet treatment; rescinded Feb 2025
- FATF Travel Rule: >CHF 1000 transfers require originator data
- Tax uncertainty across jurisdictions

**Direction:** barriers falling; 2025–2027 expected to see significant institutional acceleration.

---

Bitcoin ETF approval (Jan 2024) was the inflection point: crypto became accessible via Bloomberg terminal without custody complexity.

## Custody infrastructure:

- Hot/warm/cold: speed-security trade-off
- MPC: key never reconstructed in one place
- HSM: FIPS-certified tamper-proof hardware
- Market leaders: Coinbase (~\$130B), BitGo (~\$64B), Fidelity (~\$50B)

## Products:

- Prime brokers bundle custody + OTC + lending + derivatives + staking
- Bitcoin ETF (Jan 2024): opened pension/SWF access at scale
- Spot Bitcoin ETFs (IBIT / FBTC): pensionable via BVV2/OAK BV; tokenised funds for T+0 liquidity

## Real-world asset tokenisation:

- \$15B on-chain; \$4-16T addressable
- BUIDL: \$2.9B (Dec 2024), largest tokenised fund
- FOBXX: first SEC-registered blockchain fund (2021)
- Kinexys: \$1B+ daily repo, largest enterprise volume

## Swiss regulatory framework:

- FINMA + BVV2/OAK BV govern pension digital-asset decisions
- DLT Act (2021) enables ledger-based securities
- MiCA: EU only

---

BlackRock's \$2.9B on-chain fund in 2024 signals that institutional and crypto finance are converging, not competing.

## Quiz: Institutional Crypto (1/2)

**Q1.** Which custody architecture uses distributed key shares so the private key is never fully reconstructed?

- A) Hot wallet   B) HSM   C) MPC   D) Cold storage

## Quiz: Institutional Crypto (1/2)

**Q1.** Which custody architecture uses distributed key shares so the private key is never fully reconstructed?

A) Hot wallet   B) HSM   C) MPC   D) Cold storage

**Answer: C:** Multi-Party Computation splits the key; threshold signatures sign without assembly.

**Q2.** What was the AUM of BlackRock BUIDL as of December 2024?

A) \$500M   B) \$1.2B   C) \$2.9B   D) \$4.1B

## Quiz: Institutional Crypto (1/2)

**Q1.** Which custody architecture uses distributed key shares so the private key is never fully reconstructed?

- A) Hot wallet   B) HSM   C) MPC   D) Cold storage

**Answer: C:** Multi-Party Computation splits the key; threshold signatures sign without assembly.

**Q2.** What was the AUM of BlackRock BUIDL as of December 2024?

- A) \$500M   B) \$1.2B   C) \$2.9B   D) \$4.1B

**Answer: C:** BUIDL reached \$2.9B by December 2024, making it the largest tokenised fund.

**Q3.** What regulatory framework governs Swiss pension fund (Pensionskasse) investment categories?

- A) MiCA   B) BVV2/OAK BV   C) Basel III   D) AIFMD

## Quiz: Institutional Crypto (1/2)

**Q1.** Which custody architecture uses distributed key shares so the private key is never fully reconstructed?

- A) Hot wallet   B) HSM   C) MPC   D) Cold storage

**Answer: C:** Multi-Party Computation splits the key; threshold signatures sign without assembly.

**Q2.** What was the AUM of BlackRock BUIDL as of December 2024?

- A) \$500M   B) \$1.2B   C) \$2.9B   D) \$4.1B

**Answer: C:** BUIDL reached \$2.9B by December 2024, making it the largest tokenised fund.

**Q3.** What regulatory framework governs Swiss pension fund (Pensionskasse) investment categories?

- A) MiCA   B) BVV2/OAK BV   C) Basel III   D) AIFMD

**Answer: B:** BVV2 (Verordnung über die berufliche Vorsorge) governs Swiss pension investments. MiCA is EU-only.

**Q4.** JPMorgan Kinexys processes approximately how much in daily repo settlement (2024)?

- A) \$100M   B) \$500M   C) \$1B+   D) \$10B+

## Quiz: Institutional Crypto (1/2)

**Q1.** Which custody architecture uses distributed key shares so the private key is never fully reconstructed?

- A) Hot wallet   B) HSM   C) MPC   D) Cold storage

**Answer: C:** Multi-Party Computation splits the key; threshold signatures sign without assembly.

**Q2.** What was the AUM of BlackRock BUIDL as of December 2024?

- A) \$500M   B) \$1.2B   C) \$2.9B   D) \$4.1B

**Answer: C:** BUIDL reached \$2.9B by December 2024, making it the largest tokenised fund.

**Q3.** What regulatory framework governs Swiss pension fund (Pensionskasse) investment categories?

- A) MiCA   B) BVV2/OAK BV   C) Basel III   D) AIFMD

**Answer: B:** BVV2 (Verordnung über die berufliche Vorsorge) governs Swiss pension investments. MiCA is EU-only.

**Q4.** JPMorgan Kinexys processes approximately how much in daily repo settlement (2024)?

- A) \$100M   B) \$500M   C) \$1B+   D) \$10B+

**Answer: C:** Kinexys reported \$1B+ daily repo settlement volume in 2024.

## Quiz: Institutional Crypto (2/2)

**Q5.** FIPS 140-2/3 certification is associated with which custody technology?

- A) Cold storage   B) MPC   C) HSM   D) Multi-sig

## Quiz: Institutional Crypto (2/2)

**Q5.** FIPS 140-2/3 certification is associated with which custody technology?

A) Cold storage   B) MPC   C) HSM   D) Multi-sig

**Answer: C:** Hardware Security Modules (HSMs) are FIPS 140-2/3 certified tamper-proof devices.

**Q6.** Which institution launched the first US-registered mutual fund using blockchain for share record-keeping?

A) BlackRock   B) Fidelity   C) Franklin Templeton   D) Vanguard

## Quiz: Institutional Crypto (2/2)

**Q5.** FIPS 140-2/3 certification is associated with which custody technology?

- A) Cold storage   B) MPC   C) HSM   D) Multi-sig

**Answer: C:** Hardware Security Modules (HSMs) are FIPS 140-2/3 certified tamper-proof devices.

**Q6.** Which institution launched the first US-registered mutual fund using blockchain for share record-keeping?

- A) BlackRock   B) Fidelity   C) Franklin Templeton   D) Vanguard

**Answer: C:** Franklin FOBXX (2021) was the first SEC-registered mutual fund with blockchain as share registrar.

**Q7.** Which Swiss legislation created “ledger-based securities” as a legal asset class?

- A) FinSA (2020)   B) DLT Act (2021)   C) MiCA (2024)   D) BVG (1983)

## Quiz: Institutional Crypto (2/2)

**Q5.** FIPS 140-2/3 certification is associated with which custody technology?

- A) Cold storage   B) MPC   C) HSM   D) Multi-sig

**Answer: C:** Hardware Security Modules (HSMs) are FIPS 140-2/3 certified tamper-proof devices.

**Q6.** Which institution launched the first US-registered mutual fund using blockchain for share record-keeping?

- A) BlackRock   B) Fidelity   C) Franklin Templeton   D) Vanguard

**Answer: C:** Franklin FOBXX (2021) was the first SEC-registered mutual fund with blockchain as share registrar.

**Q7.** Which Swiss legislation created “ledger-based securities” as a legal asset class?

- A) FinSA (2020)   B) DLT Act (2021)   C) MiCA (2024)   D) BVG (1983)

**Answer: B:** The Swiss DLT Act (February 2021) created the legal category of ledger-based securities.

**Q8.** What is the estimated total addressable market for real-world asset tokenisation?

- A) \$15B   B) \$150B   C) \$4T–\$16T   D) \$100T+

## Quiz: Institutional Crypto (2/2)

**Q5.** FIPS 140-2/3 certification is associated with which custody technology?

- A) Cold storage   B) MPC   C) HSM   D) Multi-sig

**Answer: C:** Hardware Security Modules (HSMs) are FIPS 140-2/3 certified tamper-proof devices.

**Q6.** Which institution launched the first US-registered mutual fund using blockchain for share record-keeping?

- A) BlackRock   B) Fidelity   C) Franklin Templeton   D) Vanguard

**Answer: C:** Franklin FOBXX (2021) was the first SEC-registered mutual fund with blockchain as share registrar.

**Q7.** Which Swiss legislation created “ledger-based securities” as a legal asset class?

- A) FinSA (2020)   B) DLT Act (2021)   C) MiCA (2024)   D) BVG (1983)

**Answer: B:** The Swiss DLT Act (February 2021) created the legal category of ledger-based securities.

**Q8.** What is the estimated total addressable market for real-world asset tokenisation?

- A) \$15B   B) \$150B   C) \$4T–\$16T   D) \$100T+

**Answer: C:** BCG (2022) and Citi (2023) estimate \$4T–\$16T addressable; ~\$15B deployed (early 2025).