

L08 — Regulation & Future Trends

Cheatsheet

Regulatory Landscape

Three US Regulators

SEC (Securities and Exchange Commission) — enforces securities law; claims jurisdiction over tokens deemed securities.

CFTC (Commodity Futures Trading Commission) — jurisdiction over Bitcoin and commodity-like tokens; regulates derivatives.

FinCEN (Financial Crimes Enforcement Network) — enforces AML/KYC via Bank Secrecy Act; treats exchanges as money-service businesses.

EU: MiCA (Markets in Crypto-Assets) — first comprehensive crypto regulation; effective Jun 2024 (stablecoins) / Dec 2024 (full). Requires licensing for crypto-asset service providers (CASPs), stablecoin reserve disclosures, consumer protections, and PoW environmental disclosures.

Global divergence:

- Crypto-friendly: Singapore, Switzerland, UAE
- Restrictive: China (full ban), India (heavy taxation)
- El Salvador: Bitcoin legal tender (2021)

FATF Travel Rule — VASPs must share originator and beneficiary information for transfers above \$1,000; challenges privacy coins and decentralised protocols.

Securities Law: The Howey Test

Howey Test (US Supreme Court 1946)

A transaction is an *investment contract* (security) if ALL four prongs are met:

1. Investment of *money*
2. In a *common enterprise*
3. With an *expectation of profits*
4. Derived from the *efforts of others*

Application to tokens: If a token meets all four prongs it is a security subject to SEC registration requirements.

Most utility tokens sold in ICOs have been argued to satisfy all four.

“Sufficient decentralisation” test — Ether deemed not a security by SEC (2018) because no central team drives profit expectations. Provides partial defence for mature, community-run networks.

Stablecoin Regulation

Key concerns:

- **Reserve requirements** — fiat-backed stablecoins must hold 1:1 high-quality liquid assets (MiCA imposes this for EMTs).
- **Transparency** — regular audits and public reserve disclosures.
- **Systemic risk** — large stablecoins (>\$10B) face stricter MiCA rules; concern over bank-run dynamics.
- **Algorithmic stablecoins** — effectively banned under MiCA after Terra/LUNA collapse (May 2022).

Terra/LUNA collapse: algorithmic stablecoin lost peg; \$40B wiped out in 72 hours; accelerated stablecoin regulation globally.

CBDC — Central Bank Digital Currency

Definition

Digital form of central bank money, issued and controlled by a central bank. Not a cryptocurrency — no mining, no decentralisation.

Type	Description
Retail CBDC	For general public; replaces/supplements cash
Wholesale CBDC	For interbank settlement; faster cross-border payments

Design choices: account-based vs. token-based;

interest-bearing vs. non-interest-bearing; programmable (spending restrictions) vs. passive.

Concerns: financial surveillance, bank disintermediation, programmable restrictions on spending.

Examples: Bahamas (Sand Dollar), Nigeria (eNaira), China (e-CNY, largest pilot with billions in transactions), EU Digital Euro (testing phase).

KYC / AML

KYC (Know Your Customer) — identity verification before onboarding a user: government ID, proof of address, source of funds for large amounts.

AML (Anti-Money Laundering) — ongoing transaction monitoring, suspicious activity reports (SARs), sanctions screening (OFAC list).

Travel Rule (FATF Rec. 16) — exchanges must transmit originator and beneficiary data alongside transfers ≥\$1,000; technically challenging for blockchain because public keys are pseudonymous.

Non-custodial wallets — remain outside traditional KYC perimeter; FATF recommends risk-based approach for unhosted wallets.

DeFi Regulatory Challenges

Core Problems

No intermediary: no legal entity to regulate or sanction.

Pseudonymous: user identity unknown; KYC technically impossible at protocol layer.

Cross-border: smart contracts have no physical jurisdiction.

Regulatory actions (2023–2024):

- Tornado Cash developer arrested (OFAC sanctions, Aug 2022)
- Uniswap Labs received SEC Wells notice
- CFTC fined Ooki DAO (sets DAO liability precedent)

Emerging frameworks: “sufficient decentralisation”

defence; front-end vs. protocol distinction; DAO legal wrappers (Wyoming LLC, Marshall Islands DAO Act).

NFT Regulation

IP rights: NFT ownership \neq copyright. Default: buyer gets licence to display; commercial rights require explicit grant. Many projects use CC0 (public domain) or bespoke licences.

Securities classification: Fractional NFTs and NFTs with profit-share or royalty rights may satisfy Howey; “collectible” NFTs less likely to be securities.

Tax treatment (US IRS): NFTs are property; sale triggers capital gains. Royalties are ordinary income for creators. Receipt of NFT airdrop is ordinary income at fair market value.

AML concerns: art market historically low-AML; NFTs raised FATF flags for potential money-laundering through wash trading and inflated sales.

Exchange Regulation

Licensing: US exchanges typically registered with FinCEN + state money-transmitter licences; EU under

MiCA requires CASP authorisation.

Custody requirements: Segregation of client assets from exchange assets; post-FTX push for mandatory proof-of-reserves audits.

Proof of Reserves

Cryptographic attestation that exchange holds assets \geq liabilities. Uses Merkle-tree inclusion proofs so users can verify their balance is included without exposing all user data. Became industry norm post-FTX (Nov 2022).

Future Trends

Institutional adoption: Bitcoin spot ETFs approved (US, Jan 2024); BlackRock IBIT fastest-growing ETF ever; $>$ \$120B AUM by early 2026; pension funds and RIAs can now access Bitcoin without custody complexity.

ETF expansion: Ethereum spot ETFs approved (US, May 2024); other asset ETFs expected; tokenised fund structures.

Layer-2 scaling: Optimistic rollups (Optimism, Arbitrum) and ZK rollups (zkSync, StarkNet) provide 100–1000 \times throughput; account abstraction simplifies UX (social recovery, gas sponsorship).

Account abstraction (ERC-4337): wallets become smart contracts; enables seedphrase-free onboarding, gasless transactions, and multi-factor authentication — critical for mass adoption.

Real-world asset tokenisation: bonds, real estate, commodities on chain; 24/7 settlement, fractional ownership, programmable compliance.

Regulatory Comparison: US vs EU vs Asia

	US	EU	Asia
Framework	No unified law; SEC/CFTC war	MiCA (2024) — comprehensive	Singapore (MAS); China (PBOC); Japan (FSA)
Stablecoins	No federal law; state rules	MiCA Title III/IV; 1:1 reserves	MAS licence; Japan (coin law 2020)
DeFi	Enforcement-first approach	“Sufficient decentralisation” carve-out under review	SG: risk-based self-regulation
CBDCs	Fed exploring FedNow; no CBDC yet	Digital Euro pilot (ECB)	e-CNY live; Japan pilot
Stance	Uncertain, litigious	Clear but strict	Mixed; Singapore most open