Lesson 08 — Regulation & Future Trends

Study Notes

Cryptoeconomics — BSc Level

Joerg Osterrieder

2025

Contents

Learning Objectives

By the end of this lesson, students should be able to:

1. **Describe** the global regulatory landscape for crypto assets and identify the major regulatory bodies and their respective jurisdictions.
2. **Apply** the Howey Test to determine whether a crypto asset is likely to be classified as a security under US law.
3. **Explain** the key provisions of the EU MiCA regulation and its implications for crypto service providers and stablecoin issuers.
4. **Analyse** the regulatory challenges posed by DeFi, including the absence of a clear intermediary and the legal status of DAOs.
5. **Compare** CBDC design choices and evaluate the privacy and monetary-policy trade-offs they entail.
6. **Identify** the major future trends shaping the cryptoeconomics landscape, including institutional adoption, Layer-2 scaling, and AI integration.

Regulatory Landscape Overview

Fragmented Global Approach

Regulatory Fragmentation

Crypto assets operate globally and around the clock, but regulation remains *jurisdictional* and fragmented. No single international authority governs crypto markets. Countries range from comprehensive frameworks (EU MiCA) through sector-by-sector enforcement (USA) to outright bans (China).

The diversity of approaches creates **regulatory arbitrage**: firms and activity migrate to favourable jurisdictions, which in turn pressures stricter regimes to refine their rules. Key tensions include:

- **Consumer protection vs. innovation**: over-regulation stifles domestic development; under-regulation exposes retail investors to fraud.
- **Transparency vs. privacy**: AML rules require identity disclosure, clashing with crypto's pseudonymous ethos.
- **National sovereignty vs. global interoperability**: unilateral rules applied to borderless protocols create enforcement gaps.

Key Regulatory Bodies

Body	Jurisdiction	Role in Crypto
SEC	USA	Securities enforcement; jurisdiction over crypto deemed investment contracts
CFTC	USA	Commodities jurisdiction; covers Bitcoin and Ether futures/spot
FinCEN	USA	Anti-money-laundering; exchanges as money service businesses
ESMA / NCAs	EU	Implementation of MiCA; licencing of CASPs
FCA	UK	Authorisation of crypto asset firms post-Brexit
MAS	Singapore	Licencing under Payment Services Act; innovation sandbox
FSA	Japan	Crypto exchange registration; strict AML requirements
FATF	International	Sets global AML/CFT standards; Travel Rule for VASPs

US Regulatory Framework

SEC Jurisdiction and the Howey Test

The US Securities and Exchange Commission asserts jurisdiction over crypto assets that qualify as *investment contracts* under the 1946 Supreme Court ruling *SEC v. W. J. Howey Co.*

The Howey Test

A transaction is an investment contract (and therefore a security) if it involves:

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

All four prongs must be satisfied.

Applying the Howey Test to crypto assets:

- **ICO tokens**: Most initial coin offerings satisfy all four prongs — investors contribute ETH/BTC expecting profits from the founding team's development work.

- **Bitcoin**: Generally fails prong 4; no identifiable promoter whose efforts determine returns. The SEC has repeatedly declined to classify BTC as a security.
- **Ether**: Status contested; the SEC acknowledged in 2024 that spot Ether ETF approval implies treating ETH as a non-security commodity.
- **XRP (Ripple)**: Partially ruled a security when sold to institutional investors (July 2023 ruling), not when sold on open market.

CFTC for Commodities

The Commodity Futures Trading Commission has jurisdiction over *commodity* derivatives and spot markets involving fraud. Bitcoin and Ether are generally treated as commodities. The CFTC:

- Regulates Bitcoin and Ether futures traded on CME and Cboe.
- Brought enforcement actions against unregistered crypto derivatives exchanges (BitMEX, FTX).
- Has argued for expanded spot-market authority over crypto commodities.

The SEC–CFTC jurisdictional boundary is unresolved pending Congressional legislation (e.g., the proposed FIT21 Act).

Common Pitfall

Misconception: "The SEC and CFTC have agreed on which agency regulates crypto."
Correction: The boundary is actively contested. Bitcoin futures (CFTC) vs. ICO tokens (SEC) is relatively clear; the status of many altcoins remains litigated. Both agencies have brought enforcement actions against the same entities.

EU MiCA Regulation

Markets in Crypto-Assets Overview

MiCA — Markets in Crypto-Assets Regulation

MiCA (Regulation (EU) 2023/1114) is the first comprehensive legal framework for crypto assets in a major jurisdiction. It entered into force on 29 June 2023, with phased application:

- **30 June 2024**: Provisions for asset-referenced tokens (ARTs) and e-money tokens (EMTs) — the stablecoin rules.
- **30 December 2024**: Full application to all crypto asset service providers (CASPs) and other token issuers.

MiCA covers three asset categories:

Category	Description	Key Rules
Asset-Referenced Tokens (ARTs)	Tokens referencing multiple assets (currencies, commodities)	Reserve requirements, independent audit, issuer authorisation
E-Money Tokens (EMTs)	Tokens referencing a single fiat currency	Must be backed 1:1 by fiat; issued only by credit institutions or e-money institutions
Utility Tokens	Access tokens for goods/services on a DLT platform	Whitepaper disclosure; lighter regime

Licensing Requirements for CASPs

Crypto Asset Service Providers (exchanges, custodians, advisers) must:

1. Obtain authorisation from the national competent authority (NCA) of their home EU member state.
2. Meet capital requirements (minimum €25,000 to €150,000 depending on service type).
3. Implement governance, conduct of business, and conflict-of-interest rules.
4. Comply with AML/CFT obligations (Travel Rule, KYC).
5. Disclose environmental impact of consensus mechanisms (proof-of-work).

Once authorised in one member state, a CASP benefits from a *passport* allowing it to operate across all 27 EU member states.

Stablecoin Rules under MiCA

Stablecoins above significance thresholds (1 million transactions or €200 million daily volume) face enhanced requirements:

- Reserve assets must be held in segregated, low-risk, liquid instruments.
- Independent audit of reserves required at least annually.
- Volume caps for significant EMTs to limit monetary-policy interference.
- Tether (USDT) was effectively delisted by several EU exchanges in H2 2024 pending MiCA compliance.

Asian Approaches

Singapore — MAS Licensing

The Monetary Authority of Singapore (MAS) has adopted a *progressive* framework under the Payment Services Act (PSA, 2019; amended 2021):

- Digital payment token (DPT) service providers must hold a Major Payment Institution (MPI) licence.
- Retail advertising of crypto is restricted; no point-of-sale promotions permitted.
- MAS operates a Fintech Regulatory Sandbox enabling firms to test innovative products with temporary relief from specific rules.
- Singapore positions itself as an institutional crypto hub while discouraging retail speculation.

Japan — FSA Registration

Japan was among the first countries to regulate crypto exchanges under the Payment Services Act (2017, following the Mt. Gox collapse):

- All crypto exchanges must register with the Financial Services Agency (FSA).
- Strict segregation of customer assets (cold-wallet requirements after the Coincheck hack, 2018).
- Japan recognises crypto assets as legal property, not legal tender.
- Stablecoins regulated under the revised PSA from June 2023.

China — Comprehensive Ban

China's approach represents the most restrictive stance among major economies:

- September 2021: People's Bank of China declared all crypto transactions illegal; banned all cryptocurrency mining.
- Rationale: capital outflow concerns, financial stability, energy consumption.
- Exception: the digital yuan (e-CNY) CBDC is actively promoted.

Example: Regulatory Arbitrage in Practice

After China's 2021 mining ban, Bitcoin's hash rate dropped approximately 50% over two months. Within six months, mining capacity had migrated to the USA, Kazakhstan, and Russia, and the hash rate recovered to pre-ban levels. This illustrates the limits of unilateral bans against permissionless, globally distributed protocols.

KYC/AML Requirements

Identity Verification

Know Your Customer (KYC) rules require crypto service providers to verify client identities before account opening:

- Collect government-issued ID and proof of address.
- Screen against sanctions lists (OFAC, EU, UN).

- Apply enhanced due diligence (EDD) for high-risk customers, Politically Exposed Persons (PEPs), and high-value transactions.
- Record-keeping for a minimum of five years.

The Travel Rule

FATF Travel Rule (Recommendation 16)

Virtual Asset Service Providers (VASPs) must **collect, verify, and transmit** originator and beneficiary information for transfers at or above USD/EUR 1,000. The rule mirrors the bank wire transfer rule and is designed to prevent money laundering through anonymous crypto transfers.

Implementation challenges:

- No centralised messaging network for VASPs (unlike SWIFT for banks).
- Multiple competing Travel Rule protocols: TRISA, TRP, OpenVASP, Sygna.
- Unhosted (self-custodied) wallets: many jurisdictions require verification of the counterparty wallet owner, but no technical standard exists to enforce this at the protocol level.
- Privacy coins (Monero, Zcash shielded) technically incompatible with Travel Rule requirements, leading to delistings.

FATF Guidelines

The Financial Action Task Force (FATF) sets global AML/CFT standards through its 40 Recommendations and periodic country evaluations:

- **Grey list**: Countries with strategic AML/CFT deficiencies under increased monitoring (e.g., UAE, previously).
- **Black list**: High-risk jurisdictions subject to enhanced due diligence (North Korea, Iran).
- FATF evaluates countries' implementation of crypto regulations in mutual evaluations; poor scores affect correspondent banking access.

Stablecoin Regulation

Systemic Risk Concerns

Stablecoins have attracted intense regulatory scrutiny for two reasons:

1. **De-peg risk**: The May 2022 collapse of TerraUSD (UST) and its algorithmic backing mechanism (LUNA) wiped out approximately $40 billion in market value within days, causing contagion across crypto markets.

2. **Systemic risk**: A stablecoin with significant adoption (e.g., Tether's $100B+ market cap) could, if it experienced a run, affect traditional money markets through fire sales of reserve assets.

Reserve Requirements

Regulators broadly require that stablecoins maintaining a peg be backed by *high-quality liquid assets* (HQLA):

- MiCA (EU): Reserves must include mostly bank deposits and short-dated sovereign bonds; no more than 30% in other assets.
- UK FCA proposal: "systemic" stablecoins regulated similarly to e-money; full backing required.
- US (proposed): Full reserve backing; issuers must be bank-like entities subject to prudential supervision.

Audit Obligations

- Independent third-party attestations of reserves (monthly under MiCA for significant stablecoins).
- Real-time on-chain proof-of-reserve systems (Chainlink PoR) emerging as a complement to traditional audits.
- Tether historically provided only quarterly attestations, not full audits — a persistent source of regulatory criticism.

Example: Terra/LUNA Collapse as Regulatory Catalyst

TerraUSD (UST) maintained its USD peg algorithmically: burning LUNA tokens minted UST and vice versa. When confidence broke in May 2022, a "death spiral" ensued — UST de-pegged, LUNA inflated hyperbolically, and the ecosystem collapsed from $60B to near zero in 72 hours. This event accelerated stablecoin legislation in the EU (MiCA), UK, and US, all of which moved to ban or strictly limit algorithmic stablecoins.

DeFi Regulatory Challenges

No Intermediary Problem

Traditional financial regulation targets *intermediaries*: banks, brokers, exchanges. DeFi deliberately removes intermediaries, replacing them with autonomous smart contracts. This creates three core regulatory challenges:

- **Who to license?** A Uniswap liquidity pool is a smart contract; there is no legal entity to hold a licence.
- **Who to fine?** When Tornado Cash (a privacy mixer) was sanctioned by the US OFAC

in August 2022, developers were arrested, but the smart contracts continued operating autonomously.

- **How to enforce KYC?** Permissionless protocols allow any wallet to interact; there is no account-opening step where identity can be verified.

Smart Contract Liability

- **Developer liability**: The Tornado Cash case (developer Alexey Pertsev convicted in the Netherlands, 2024) suggests courts may hold developers liable for foreseeable illicit use even of open-source code.
- **Front-end vs. protocol distinction**: Regulators increasingly target the web front-end (which has an operator) while the underlying protocol remains unregulated. Uniswap Labs received an SEC Wells notice in 2024.
- **"Sufficient decentralisation" test**: Some regulators consider whether a protocol is sufficiently decentralised to lack a responsible party. No clear legal threshold exists.

DAO Legal Status

Decentralised Autonomous Organisations present unresolved legal questions:

- A DAO governance token may constitute a security (SEC position for some tokens).
- The CFTC fined Ooki DAO in 2022, establishing that token holders who voted on governance could bear personal liability for DAO actions.
- **Legal wrappers**: Wyoming (USA) and the Marshall Islands recognise DAOs as legal entities (LLC or non-profit), providing limited liability to participants.
- Without a wrapper, DAO token holders may be treated as general partners with unlimited personal liability.

Common Pitfall

Misconception: "If a protocol is decentralised, regulators cannot touch it."
Correction: Regulators can and do target: (1) developers who deployed the code, (2) front-end operators, (3) liquidity providers in specific jurisdictions, and (4) governance token holders who voted on material decisions. Decentralisation reduces but does not eliminate regulatory risk.

CBDCs (Central Bank Digital Currencies)

Design Choices

CBDC Definition

A **Central Bank Digital Currency (CBDC)** is a digital form of *central bank money* — a liability of the central bank, denominated in the national unit of account, and available for use by the general public (retail CBDC) or financial institutions (wholesale CBDC).

Key design dimensions:

Dimension	Option A	Option B
Architecture	Account-based (central bank holds all accounts)	Token-based (bearer instrument, validated by credentials)
Intermediation	Direct (central bank–citizen)	Two-tier (commercial banks distribute)
Programmability	Non-programmable (like cash)	Programmable (smart contracts, spending restrictions)
Anonymity	Fully traceable	Privacy-preserving (zero-knowledge)
Bearing	Non-interest-bearing	Interest-bearing

Privacy Trade-offs

The programmability and traceability of CBDCs raise fundamental civil-liberties concerns:

- A programmable CBDC could carry expiry dates, geographic restrictions, or categorical spending limits — features impossible with cash.
- Full transaction visibility gives the central bank and government unprecedented surveillance capability.
- Most central banks (ECB, Bank of England) have publicly committed to *not* designing CBDCs with programmable restrictions and to including privacy protections; independent verification remains unclear.
- Academic proposals (e.g., MIT Digital Currency Initiative) explore zero-knowledge-proof-based CBDC designs that preserve user privacy while preventing double-spending.

Pilot Programmes

Country	Status (as of 2025)	Notes
Bahamas	Launched (Sand Dollar, 2020)	First retail CBDC; limited adoption
Nigeria	Launched (eNaira, 2021)	Compulsory merchant acceptance; low uptake
China	Large-scale pilot (e-CNY)	Billions in transactions; integrated with Alipay/WeChat Pay
EU	Design phase (Digital Euro)	ECB aims for 2027–2028; two-tier model
USA	Research (Project Hamilton)	MIT + Boston Fed; CBDC legislation stalled in Congress
India	Pilot (e-Rupee, 2022)	Wholesale and retail pilots; gradual rollout

Future Trends

Institutional Adoption

The approval of spot Bitcoin ETFs by the US SEC in January 2024 marks a watershed moment for institutional adoption:

- **Spot Bitcoin ETFs**: 11 products approved on 10 January 2024. BlackRock's IBIT became the fastest-growing ETF in history, surpassing $10B AUM in 49 days. Combined AUM exceeded $120B by early 2026.
- **Access expansion**: Pension funds, registered investment advisers (RIAs), and 401(k) retirement accounts can now access Bitcoin exposure without self-custody.
- **Corporate treasuries**: MicroStrategy and others hold Bitcoin as a treasury reserve asset; accounting standards (ASC 350 update, FASB 2023) now allow fair-value accounting for crypto holdings.

ETF Expansion

Beyond Bitcoin ETFs, the institutional pipeline includes:

- Spot Ether ETFs (approved USA, May 2024).
- Multi-asset crypto index ETFs (pending regulatory approval in several jurisdictions).
- Options on Bitcoin ETFs (approved October 2024), enabling sophisticated institutional hedging strategies.

Layer-2 Scaling

Base-layer blockchains (Bitcoin, Ethereum) process 7–30 transactions per second — insufficient for mass-market payment applications. Layer-2 solutions move computation off-chain while inheriting the base layer's security:

- **Optimistic Rollups** (Arbitrum, Optimism, Base): Assume transaction validity; allow a 7-day fraud-proof window. Throughput: ∼2,000–4,000 TPS.
- **ZK Rollups** (zkSync Era, StarkNet, Polygon zkEVM): Generate a cryptographic validity proof for each batch. No withdrawal delay; higher computational cost to prove.
- **State Channels** (Lightning Network): Bilateral or multi-party payment channels settled off-chain; ideal for high-frequency micropayments.

Combined L2 TVL exceeded Ethereum mainnet TVL for many metrics by 2025, signalling genuine scaling traction.

Interoperability

The multi-chain landscape (Ethereum, Solana, Bitcoin, Cosmos, Polkadot) requires bridges and cross-chain protocols:

- Cross-chain bridges have been the largest attack surface in DeFi (Ronin $625M, Wormhole $320M, Nomad $190M).
- **Native interoperability**: IBC (Inter-Blockchain Communication) protocol in the Cosmos ecosystem provides trust-minimised cross-chain messaging without lock-and-mint bridges.
- **Intent-based architectures**: Users express desired outcomes ("I want 100 USDC on Arbitrum"); solvers compete to route the trade optimally across chains.

AI Integration

The intersection of AI and blockchain is nascent but rapidly developing:

- **AI agents and on-chain execution**: Autonomous AI agents that hold wallets, sign transactions, and interact with smart contracts (e.g., Fetch.ai, Autonolas).
- **Verifiable computation**: ZK proofs can verify that an AI model ran correctly on specific inputs without revealing the model weights ("zkML").
- **Decentralised AI inference**: Networks like Bittensor incentivise miners to provide AI compute and model training using tokenised rewards.
- **MEV and AI**: Machine learning increasingly used to predict and capture Miner Extractable Value in DeFi order flows.

Practice Problems

1. **(Howey Test Application)** A startup issues "PROJ tokens" via an ICO. Token holders receive 20% of the startup's future revenue. Tokens are transferable on secondary markets. Apply each of the four Howey prongs and conclude whether PROJ tokens are likely to be classified as securities under US law.
2. **(MiCA Categorisation)** Classify each of the following under MiCA and state the main compliance obligation:
   (a) A token pegged to the USD and backed 1:1 by bank deposits.
   (b) A governance token that provides voting rights in a DAO but no financial claim.
   (c) A token pegged to a basket of gold and EUR.
3. **(Travel Rule)** Exchange A (EU, MiCA-licenced) sends 5,000 USDC to Exchange B (Singapore, MPI-licenced) on behalf of customer Alice. What information must Exchange A transmit to Exchange B under the FATF Travel Rule? What if the destination is an unhosted wallet?
4. **(CBDC Design)** A central bank is designing a retail CBDC and must choose between (i) full traceability or (ii) a privacy-preserving design using zero-knowledge proofs. Outline two advantages and two disadvantages of each option from the perspectives of monetary policy, financial crime prevention, and civil liberties.
5. **(DeFi Regulation)** A DeFi protocol operates via immutable smart contracts on Ethereum. It has no company, no front-end operator, and governance is conducted via a DAO. A regulator claims the protocol facilitates unlicensed securities trading. What legal arguments does the protocol's community have? What are the weaknesses of those arguments?
6. **(Regulatory Scenario)** You are advising a crypto exchange based in the EU (MiCA jurisdiction) that wants to offer trading in a new token. The token grants holders a share of protocol revenue. List the regulatory questions you would ask to determine the token's classification and the required disclosures.

Key Takeaways

1. **Global fragmentation**: Crypto regulation is a patchwork. The EU (MiCA) leads with a comprehensive framework; the US applies existing securities and commodities law; Asia varies from permissive (Singapore, Japan) to prohibitive (China).
2. **The Howey Test** remains the primary US tool for distinguishing securities from commodities. The key prong is whether profits derive from the efforts of a common enterprise's promoters.
3. **MiCA** is the most significant regulatory development: a single licence valid across 27 EU states, with strict rules for stablecoin issuers and crypto service providers.
4. **KYC/AML**: The Travel Rule extends traditional bank AML obligations to VASPs. Implementation is technically challenging, especially for privacy coins and unhosted wallets.

5. **Stablecoins** face the most urgent regulatory pressure because of systemic risk (Terra/LUNA) and potential monetary-policy interference (large-scale issuance).
6. **DeFi** is the hardest regulatory problem: no intermediary means no obvious licence holder. Developer liability, front-end targeting, and DAO legal wrappers are the current battlegrounds.
7. **CBDCs** represent the central-bank response to private stablecoins. Design choices — programmability, anonymity, intermediation model — have profound implications for privacy and monetary sovereignty.
8. **Future trends**: Institutional adoption (ETFs), L2 scaling (rollups), interoperability (IBC, intent architectures), and AI integration are reshaping the crypto landscape faster than regulation can track.

Further Reading

- European Parliament (2023). *Regulation (EU) 2023/1114 on Markets in Crypto-Assets (MiCA)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1114
- FATF (2021). *Updated Guidance for a Risk-Based Approach: Virtual Assets and VASPs*. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf
- Hinman, W. (2018). *Digital Asset Transactions: When Howey Met Gary (Plastic)*, SEC Speech. https://www.sec.gov/news/speech/speech-hinman-061418
- Auer, R., Cornelli, G., & Frost, J. (2020). "Rise of the Central Bank Digital Currencies". *BIS Working Paper 880*. https://www.bis.org/publ/work880.htm
- Ante, L. (2023). "The Impact of DeFi Regulations on Protocol Activity." *Journal of Alternative Investments*.
- Buterin, V. (2023). "The Promise and Challenges of Crypto + AI Applications." https://vitalik.eth.limo/general/2024/01/30/cryptoai.html