In-Class Exercise: Blockchain Business Models

Exercise 1: Structured Debate — "Is Chainalysis a Software Vendor or a Regulated Utility?"

Format: Split into two teams. Each team prepares its position, then presents. After both sides speak, the class votes — but first read the debrief questions. Use Chainalysis as the reference case, because its attribution-and-tracing graph is licensed to many parties under software terms, yet it functions like shared infrastructure for the sanctions-screening, investigations, and reporting activities of banks, regulators, and venues across the regulated stack.

Team A — "Chainalysis Is a Software Vendor"

Anchoring evidence: Chainalysis sells data and analytics products under licence terms. It does not custody assets, does not operate a venue, does not take counterparty risk, and is not itself a regulated financial institution. Its revenue mix, release cadence, and customer-relationship model read as a business-to-business analytics firm.

Team A: Chainalysis Is a Software Vendor	
Argument I	
Argument II	
Argument III	
Concession	*Strongest argument AGAINST your position:*
Closing	*How you address the concession:*

Team B — "Chainalysis Is a Regulated Utility"

Anchoring evidence: The Chainalysis attribution graph is the de facto reference dataset for sanctions screening across crypto venues and for many regulators. Once banks, venues, and regulators rely on the same graph, the firm functions as shared compliance infrastructure with utility-like dependence. The cost of replacing Chainalysis for any single customer is high, and the cost of the market collectively switching is much higher.

Team B: Chainalysis Is a Regulated Utility	
Argument I	
Argument II	
Argument III	
Concession	*Strongest argument AGAINST your position:*
Closing	*How you address the concession:*

Debrief Questions

© Joerg Osterrieder 2026

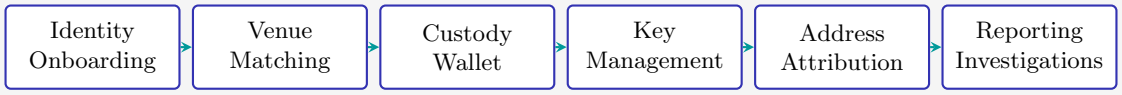
Q1: Does the answer — software vendor or regulated utility — matter for how supervisors should treat Chainalysis and the firms that depend on its outputs? Why or why not?

Q2: Could the answer genuinely be "both, at the same time"? If so, what does that imply for the usefulness of the classification?

Q3: Name another data-foundation firm in financial services that blurs the software-versus-utility boundary similarly. What tension does that create for its investors?

Exercise 2: Value Chain Mapping

Scenario: The crypto-services value chain has six links. For each link, identify which of the five firms on the reference slate (Coinbase, Kraken, Chainalysis, Fireblocks, Anchorage) most clearly owns the link, and describe what the firm is substituting for the legacy or absent service at that link. Firms rarely own every link outright — be explicit when the firm is renting a link via a partner custodian, oracle, or law firm.



Value Chain Link	**Firm Owning It**	**Friction Removed or Filled**	**Replaces or Improves?**	**Bank Loses or Adapts?**
Identity Onboarding				
Venue Matching				
Custody / Wallet				
Key Management				
Address Attribution				
Reporting / Investigations				

Synthesis Question

Q1: Which link in the chain is *most vulnerable* to a new crypto-native entrant? Which is *most resistant*? Defend your reasoning with reference to switching costs, regulatory barriers, and data advantages.

© Joerg Osterrieder 2026

Facilitator Solutions

Sample answers for instructor reference. These are illustrative; student reasoning may diverge and still be valid.

Exercise 1: Debate Sample Answers

Team A (Chainalysis Is a Software Vendor) — sample arguments

Argument I. Chainalysis sells products under licence terms with subscription pricing and standard software-vendor service-level agreements. It does not custody assets, does not operate a venue, does not take settlement risk, and is not itself an entity to which prudential or operational-resilience obligations apply. The legal form is squarely that of a business-to-business analytics company.

Argument II. The firm earns revenue by licensing data and analytics outputs. The economic substance is that of a software firm whose value rises with installed base and product depth, not that of a utility whose value comes from regulated entitlements or scarce natural-monopoly access.

Argument III. Customers can in principle replace Chainalysis with a competing analytics product. The market has alternatives with overlapping coverage and competing methodologies. Substitutability is high enough that the firm faces vendor competition, which is the defining feature of a software vendor and not of a utility.

Concession. The strongest argument against Team A is that, in practice, regulators and large compliance teams treat Chainalysis outputs as the reference data — which gives the firm utility-like dependence regardless of its legal form.

Closing. Software firms can become reference data sources without becoming utilities. Reliance is not the same as regulation; the right answer is software vendor with reference-data influence, not utility.

Team B (Chainalysis Is a Regulated Utility) — sample arguments

Argument I. The Chainalysis attribution graph is treated by many regulators and most large crypto venues as the reference dataset for sanctions screening, transaction monitoring, and law-enforcement investigations. When a single firm's data product becomes the reference for an entire compliance regime, the firm functions as shared infrastructure — the defining feature of a utility, regardless of legal form.

Argument II. Switching costs are extremely high. Compliance teams build evidence files, examiner expectations, and audit-trail standards around the specific outputs of one analytics provider. Replacing the provider would require re-tooling not just the software but the supervisory expectations of regulators and external auditors. That kind of switching cost is characteristic of a utility, not a software vendor.

Argument III. Because the firm sits in the data-foundation layer beneath all sanctions-screening, investigations, and reporting work, its operational availability has utility-like criticality. An outage or data-quality failure would propagate across many regulated entities simultaneously, which is exactly the systemic-risk profile that triggers utility-style supervision.

Concession. The strongest argument against Team B is that the firm has not been formally designated as a critical service provider by most major regulators, and it competes in an open market with substitute analytics firms.

Closing. Functional reality outruns formal designation. The firm is a regulated utility in substance even if regulators have not yet formalised the status; supervision should follow the function rather than wait for the label.

© Joerg Osterrieder 2026

Debrief Q1 — Supervisory treatment

Whether Chainalysis should be supervised as a software vendor or as a regulated utility depends on the systemic risk it creates, not on the label it prefers. A firm whose data outputs are relied on across many regulated entities for sanctions screening and law-enforcement investigations carries operational-resilience and concentration risk that ordinary software vendors do not. If the firm's outputs underpin the supervisory expectations of multiple regulators, the supervisory toolkit applied to critical service providers — exit-planning requirements, operational-resilience testing, concurrent-supervision arrangements — becomes appropriate. The answer matters because the toolkit available for critical service providers is calibrated for systemic dependencies, while a software-vendor framework is not.

Debrief Q2 — "Both" as an answer

The answer can genuinely be "both". Chainalysis operates with the legal form of a software vendor and the functional reality of shared compliance infrastructure. That duality reveals that traditional industry categories, designed for a world where data foundations were built inside regulated institutions rather than outside them, cannot cleanly classify a firm that sits in the data-foundation layer of an entire compliance regime. If "both" is correct, regulators need new functional categories that focus on systemic dependence rather than legal form, and investors need to value the firm on a hybrid lens that combines software-vendor growth multiples with utility-like risk-of-regulation discount factors.

Debrief Q3 — Cross-sector blurring example

The credit-rating agencies are the canonical parallel. They operate with the legal form of analytical research firms but function as embedded infrastructure for the entire regulated investment-management apparatus. Mutual-fund mandates, pension-fund eligibility lists, banking-capital risk weights, and many regulatory thresholds all cite a small number of these firms by name. They earn under software-vendor-like commercial terms but carry utility-like systemic dependence. The tension this creates is acute for regulators (formalise the status, or accept the systemic-risk concentration?), for investors (apply growth or utility multiples?), and for competitors (the entrenched names are extraordinarily hard to displace because the regulatory references themselves are baked into the regime). The parallel to Chainalysis is direct: both are data-foundation firms whose outputs were absorbed into the regulatory apparatus they serve.

© Joerg Osterrieder 2026

Exercise 2: Value-Chain Mapping Sample Answers

Value Chain Link	Firm Owning It	Friction Removed or Filled	Replaces or Improves?	Bank Loses or Adapts?
Identity Onboarding	Coinbase (regulated retail onboarding)	Assembly cost of identity, fiat-rails, and compliance posture into one onboarding flow	Replaces	Bank Adapts
Venue Matching	Kraken (advanced trader matching engine)	Order-book depth and ergonomic familiarity for power users on a regulated venue	Replaces	Bank Loses
Custody / Wallet	Anchorage (qualified-custody trust company)	Absence of a regulated qualified-custody charter for digital assets in a heavily regulated jurisdiction	Replaces (where absent)	Bank Adapts
Key Management	Fireblocks (institutional MPC infrastructure)	Operational risk of bespoke key-management engineering for institutional treasuries	Replaces	Bank Adapts
Address Attribution	Chainalysis (attribution graph)	Absence of an entity-level attribution layer that no individual venue could build alone	Replaces (no legacy substitute)	Bank Adapts
Reporting / Investigations	Chainalysis (case files and exports)	Manual evidence-building from raw chain data for investigators and supervisors	Improves	Bank Adapts

Synthesis Question Sample Answer

The most vulnerable link is Identity Onboarding. Switching costs at the onboarding stage are low: a customer can re-onboard with another regulated venue in minutes. Brand and marketing dominate the win-rate at this link, and brand can be eroded by a sufficiently aggressive entrant with a comparable compliance posture. The most resistant link is Address Attribution. Building a global attribution graph requires patient accumulation of behavioural data across many chains, persistent investment in tagging and clustering methodology, supervised model validation under regulatory scrutiny, and trust relationships with law-enforcement counterparties that take many years to develop. The data moat compounds with every additional case worked, and the regulatory references that cite the dataset by reputation effectively raise the bar for any new entrant. A new firm can launch a venue, a wallet, or a key-management product in a single product cycle, but it cannot recreate a multi-year attribution graph in any reasonable horizon.

© Joerg Osterrieder 2026