

Full name: Gergo Biro

Question: Is cryptocurrency compatible with government regulation?

Regulating an Equilibrium: Why Cryptocurrency Is Compatible Only with the Regulation It Forces Us to Invent

“The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”¹

The strongest case against compatibility is also the most seductive: cryptocurrency was engineered to make financial regulation unnecessary. Hobbes taught that covenants without the sword are but words; Nakamoto’s wager was that a sword could be forged from arithmetic: proof-of-work could enforce covenants no sovereign underwrites.² Where the rules are code and the ledger has no headquarters, the state’s regulatory grammar — the license, the audit, the subpoena — loses its grammatical object. On this view, regulation must either fail to bind the technology or destroy what it binds.

This essay accepts the incompatibilists’ premise and rejects their conclusion. Financial theory shows that cryptocurrency does defeat one kind of regulation, entity-based coercion. But the same theory specifies the two instruments to which the system is structurally receptive. Cryptocurrency is compatible with government regulation, provided regulation is reconceived: from commanding entities to selecting equilibria, and from auditing intermediaries to reading the ledger itself. The answer must be graded by layer, and the grading is itself part of the answer.

I. The Object Problem: Regulating What Will Not Hold Still

Financial regulation is entity-based. It presupposes a legal person (a bank, a broker, a clearinghouse) that holds still while the state licenses, audits, or punishes it. A cryptocurrency protocol is no such person. Biais, Bisière, Bouvard, and Casamatta model proof-of-work as a stochastic coordination game: miners extend the longest chain because they expect others to do the same; the expectation is self-fulfilling.³ Following one chain is an equilibrium, but so are

¹ The headline embedded by Satoshi Nakamoto in Bitcoin’s genesis block, 3 January 2009; permanently readable on-chain.

² Hobbes, T. (1651). *Leviathan*, ch. XVII; Nakamoto, S. (2008). “Bitcoin: A Peer-to-Peer Electronic Cash System.” Notably, the white paper never names the state: its declared adversary is the “trusted third party.”

³ Biais, B., Bisière, C., Bouvard, M., & Casamatta, C. (2019). “The Blockchain Folk Theorem.” *The Review of Financial Studies*, 32(5), 1662–1715.

forks; nothing in the mathematics privileges a single history. The properties the law would most like to seize are finality, immutability, and ownership: not facts about an object but features of an equilibrium, held in place by beliefs; the profession's survey draws the same boundary: governance by protocol against governance by law.⁴ The law has met this dissolution in the wild: when Washington sanctioned the Tornado Cash mixer, the Fifth Circuit held that its immutable smart contracts were not even "property" capable of designation: a court discovering that its target category had dissolved.⁵

The second dissolution is sharper. Pagnotta shows that a proof-of-work network's economic security and its market price are jointly determined: users price the risk of attack, while the miners supplying security are financed by rewards paid in the token they secure.⁶ In reduced form (compressing a joint equilibrium into comparative statics), security rises with price:

$$S = \sigma(P), \text{ with } \sigma'(P) > 0$$

The sword enforcing Nakamoto's covenants must be perpetually paid for — in the asset's own coin. Hobbes's Leviathan financed its sword by taxation; Nakamoto's is financed by valuation. Any policy that moves the price therefore moves the security: the state cannot touch the market value without altering the ledger's integrity, and cannot stand aside without its abstention being priced. In ordinary markets, regulation changes what a product earns. Here, it changes what the product is.

⁴ Halaburda, H., Haeringer, G., Gans, J., & Gandal, N. (2022). "The Microeconomics of Cryptocurrencies." *Journal of Economic Literature*, 60(3), 971–1013.

⁵ *Van Loon v. Department of the Treasury* (U.S. Court of Appeals for the Fifth Circuit, November 2024); the designation was withdrawn in March 2025.

⁶ Pagnotta, E. (2022). "Decentralizing Money: Bitcoin Prices and Blockchain Security." *The Review of Financial Studies*, 35(2), 866–907.

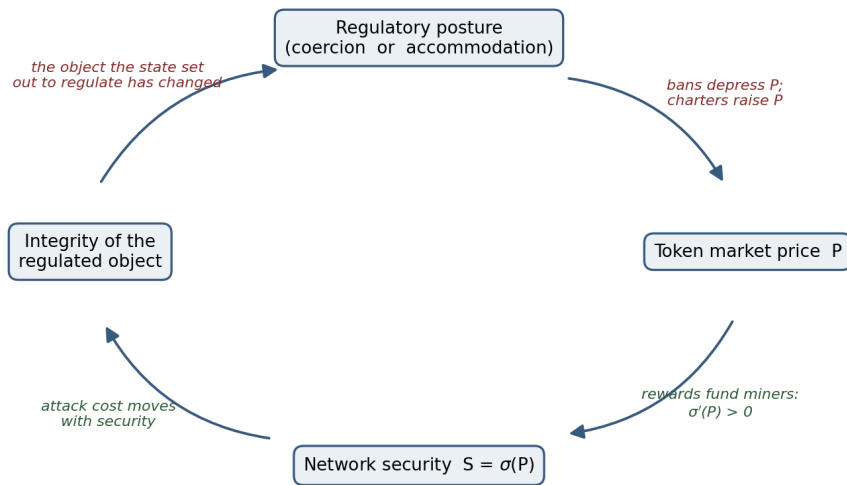


Figure 1: The Reflexivity Loop (reduced form of Pagnotta, 2022).

II. The Reflexivity Trap

This endogeneity generates what I will call the Reflexivity Trap: under decentralized consensus, both classical regulatory postures defeat themselves.

Coercion first. Bans, punitive taxes, and criminalized custody do depress demand and price, and through σ they de-fund the miners, cheapening attacks on the very ledger where the state's own citizens still hold assets. Enforcement can seize people and interfaces, never the protocol; what it cannot reach re-forms as a fork beyond the border. China proved it at scale: after the 2021 mining ban, the hashrate re-emerged abroad within months.⁷ The policy does not discipline the object; it degrades it and relocates it.

Accommodation fails symmetrically. The spot bitcoin funds approved in January 2024, the European Union's MiCA regime in force from December 2024, and the American stablecoin charter of July 2025 each drew institutional capital in and raised the price.⁸ By the same loop, the

⁷China's reported share of global hashrate fell to zero after the June 2021 ban, and aggregate hashpower regained its prior level within roughly six months (Cambridge Centre for Alternative Finance mining map). Industry data, cited as such.

⁸ U.S. SEC approval of spot bitcoin exchange-traded products, 10 January 2024; Regulation (EU) 2023/1114 (MiCA), fully applicable 30 December 2024; GENIUS Act (S.1582, 119th Congress), signed 18 July 2025.

state's embrace subsidizes the security of the censorship-resistant core it never intended to strengthen. Tolerance is not neutrality; no neutral posture exists. The regulator is a player, not an umpire.

Yet the trap is not impotence: state rules bind these markets hard. Makarov and Schoar document large, persistent cross-country gaps in bitcoin's price (Korea's "kimchi premium" exceeded 15% for weeks) because capital controls stopped arbitrageurs at borders.⁹ A truly stateless money would obey the law of one price; bitcoin's price data have borders drawn through them. The gaps closed only when regulated arbitrageurs entered: integration came through the state's legal perimeter, not around it. Nor do these markets discipline themselves: suspicious algorithmic trading likely drove bitcoin's 2013 rise from \$150 to \$1,000 on a single exchange, and evidence from the 2017 boom is consistent with unbacked stablecoin issuance propping the price.¹⁰ Market-integrity regulation is demanded by cryptocurrency's own economics, not imported from outside.

The geometry, then: a market layer regulation demonstrably binds and visibly needs, wrapped around a protocol layer where both classical postures misfire. The question is with which instruments the inner layer can be reached.

III. The Two Instruments: Coordination and Code

The state's loudest weapon was never the subpoena; it was the announcement. That is the folk theorem's deepest implication: where multiple equilibria exist, outcomes hinge on expectations, and expectations can be steered by public signals. Twice the system has chosen between rival histories at scale: the 2017 Bitcoin/Bitcoin Cash split and Ethereum's 2022 migration to

⁹Makarov, I., & Schoar, A. (2020). "Trading and Arbitrage in Cryptocurrency Markets." *Journal of Financial Economics*, 135(2), 293–319. The sample is 2017–18; the deviations have since narrowed.

¹⁰Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). "Price Manipulation in the Bitcoin Ecosystem." *Journal of Monetary Economics*, 95, 86–96; Griffin, J. M., & Shams, A. (2020). "Is Bitcoin Really Untethered?" *The Journal of Finance*, 75(4), 1913–1964. Tether has disputed the latter findings and no court has adjudicated them; its 2021 settlement with the CFTC over reserve disclosures is a separate, established fact.

proof-of-stake. Both times, selection came not from hashpower alone but from coordination: exchanges, custodians, and stablecoin issuers announced which chain they would recognize; liquidity, price, and therefore security followed.¹¹ Those coordinators were private. The state — the most permanent announcer, the only one whose recognitions are backed by courts — has entered this channel only by accident. Deployed deliberately, announcement becomes regulation: declaring which chain's assets the courts will treat as property, which ledger state bankruptcy will honor, which issuers' liabilities may touch the banking system, selects an equilibrium without a single seizure.

Two disciplines keep the instrument honest. First, selection is not authorship. A focal point must still be an equilibrium of the underlying game: the state chooses from the set the technology offers; it cannot decree outcomes the game does not contain. No announcement can make a 51%-attacked chain legitimate. That constraint is what separates coordination from coercion. Second, the instrument runs on credibility, which is scarce. Recognition that is weaponized or capriciously reversed stops coordinating: Kydland and Prescott's time-consistency problem in new dress.¹²

The second instrument relocates the rulebook. Zetzsche, Arner, and Buckley argue that where decentralization deletes the intermediary, compliance can be embedded in the protocol layer itself;¹³ Auer's "embedded supervision" (the regulator reading the market's ledger rather than collecting reports about it) is the same insight in central-bank form.¹⁴ Cong and He supply the economics: smart contracts can carry enforceable conditions (collateral floors, disclosure triggers, position limits) executed at the moment of transaction: compliance becomes a condition of settlement, not an administrative afterthought.¹⁵ Their darker finding: the same verifiability

¹¹Both episodes are offered as evidence that the coordination channel operates, not that states have used it: in each case the decisive recognitions came from private market infrastructure.

¹²Kydland, F. E., & Prescott, E. C. (1977). "Rules Rather than Discretion: The Inconsistency of Optimal Plans." *Journal of Political Economy*, 85(3), 473–491.

¹³Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). "Decentralized Finance." *Journal of Financial Regulation*, 6(2), 172–203.

¹⁴Auer, R. (2019). "Embedded Supervision: How to Build Regulation into Decentralised Finance." BIS Working Paper No. 811 (a working paper, cited as such).

¹⁵Cong, L. W., & He, Z. (2019). "Blockchain Disruption and Smart Contracts." *The Review of Financial Studies*, 32(5), 1754–1797.

that enables encoded compliance also eases collusion among the monitored; a transparent financial system needs more antitrust attention, not less.

The program is feasible because scale itself cooperates: Hinzen, John, and Saleh prove that permissionless consensus caps its own throughput as network delay grows with adoption, so scale returns only through hubs, custodians, and layer-two intermediaries: precisely the regulable entities the first layer deleted.¹⁶ Privacy-preserving, sovereign execution environments can be built without regulable operators, but they cannot conjure liquidity. Institutional capital, which alone supplies scale, transacts where compliance is legible: depth pools in chartered venues, stateless ones self-segregate into thin, high-slippage niches, and the state need not ban what capital efficiency filters out. Whatever outgrows the niche re-intermediates into caps, bridges, operators: handles either way. Abstention was never on the menu: Schilling and Uhlig show that the dollar and bitcoin are fiscally entangled by construction: miners' new coins claim real goods, and a central bank defending its inflation target must withdraw dollars in step; in equilibrium, bitcoin's block rewards are thus financed by an implicit tax on holders of the sovereign's money.¹⁷ The systems already interact; the question is whether the interaction is governed.

IV. Objections, a Leak, and a Wager

Is embedded regulation centralization with extra steps? Partly, and the layers make the concession precise. The base consensus layer remains permissionless: the state gains nothing by conquering it and, by the Trap, damages what it touches. The application layer (stablecoins, tokenized credit, anything performing money-like functions) must interface with property law to scale, and there the compliance code lives. I concede the bifurcation leaks: after the 2022 mixer sanctions, a majority of new Ethereum blocks passed through compliance-filtering relays before censorship-resistant relays recovered share.¹⁸ The episode is the Reflexivity Trap running

¹⁶Hinzen, F. J., John, K., & Saleh, F. (2022). "Bitcoin's Limited Adoption Problem." *Journal of Financial Economics*, 144(2), 347–369.

¹⁷Schilling, L., & Uhlig, H. (2019). "Some Simple Bitcoin Economics." *Journal of Monetary Economics*, 106, 16–26.

¹⁸Industry relay monitoring (e.g., mevwatch.info) documented that a majority of post-Merge Ethereum blocks in late 2022 were built through OFAC-compliant relays; the share later declined as non-censoring relays gained ground.

through a second circuit, application-layer pressure feeding back into base-layer neutrality; the response completes the lesson: neutrality is priced, so the network pays to defend it, and protocol engineering has since moved to make filtering structurally harder. The leak does not break the framework; it is its warning label: a state that over-uses the application layer degrades the neutrality it profits from, meets the network's countermeasures, and re-enters the trap.

Does proof-of-stake escape the loop? It tightens it. The ledger is secured by the market value of the staked token itself, so depressing the price lowers the cost of assembling an attacking stake in proportion: the reflexivity is consensus-independent because it is economic, not mechanical. Who audits the auditing code? I refuse the customary escape of "further research." The first principle of cryptographic administrative law can be stated now — call it habeas corpus for code: a compliance contract may execute a freeze only on presentation of a cryptographically signed judicial warrant, and the freeze expires of its own accord (the contract self-releases) unless a named human judge confirms it within a fixed interval; every such contract published open-source, formally verified, and sunset-claused. The state thereby enters the protocol as a constrained peer inside its transition rules, not an operator above them. Habeas corpus disciplined the king's jailers by demanding a body and a reason before a judge; its digital descendant demands a judge's signature before an algorithm's freeze becomes a seizure. The institution does not yet exist. Its principle now does.

The argument closes with a wager, because a thesis that risks nothing explains nothing. If this essay is right, jurisdictions that regulate by recognition and embedded code will, within a decade, host the compliant application layer, while coercion-first jurisdictions export their crypto economies without extinguishing them. If adversarial enforcement instead proves able to shrink the protocol layer itself (its activity and its security budget, not merely its address), the thesis fails. I accept the bet.

Conclusion

Subsequent protocol research (proposer-level inclusion lists, encrypted transaction pools) aims to make such filtering structurally harder. Industry data and protocol documentation, cited as such.

Is cryptocurrency compatible with government regulation? The question smuggles in two fixities, a technology that never changes and a state that never learns, and in their falsity lies the graded answer. At the market layer: compatible, trivially; the price data carry the state's borders. At the application layer: compatible by charter, as 2024 and 2025 legislated. At the protocol layer: compatible only through the two instruments native to the object, coordination of expectations and compliance written into the ledger's own state. And at the constitutional layer: not yet, for the last untransformed party is the state itself, whose algorithmic arm still awaits its habeas corpus. The residual incompatibility is not between cryptocurrency and regulation; it is between algorithmic regulation and the rule of law. "Don't trust, verify" was coined as a declaration of independence from the state; embedded supervision is the state obeying it, reading the ledger instead of trusting reports about it. The maxim was never crypto's escape from the state; it was its syllabus for the state. Covenants without the sword are but words, and this century has learned to forge swords from arithmetic. Compatibility is not the surrender of either side. It is mutual transformation — and the state's turn has come.

Bibliography

- Auer, R. (2019). Embedded supervision: How to build regulation into decentralised finance. BIS Working Paper No. 811 (working paper).
- Biais, B., Bisière, C., Bouvard, M., & Casamatta, C. (2019). The blockchain folk theorem. *The Review of Financial Studies*, 32(5), 1662–1715.
- Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies*, 32(5), 1754–1797.
- Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics*, 95, 86–96.
- Griffin, J. M., & Shams, A. (2020). Is Bitcoin really untethered? *The Journal of Finance*, 75(4), 1913–1964.
- Halaburda, H., Haeringer, G., Gans, J., & Gandal, N. (2022). The microeconomics of cryptocurrencies. *Journal of Economic Literature*, 60(3), 971–1013.
- Hinzen, F. J., John, K., & Saleh, F. (2022). Bitcoin's limited adoption problem. *Journal of Financial Economics*, 144(2), 347–369.
- Hobbes, T. (1651). *Leviathan*. London: Andrew Crooke.

- Kydland, F. E., & Prescott, E. C. (1977). Rules rather than discretion: The inconsistency of optimal plans. *Journal of Political Economy*, 85(3), 473–491.
- Makarov, I., & Schoar, A. (2020). Trading and arbitrage in cryptocurrency markets. *Journal of Financial Economics*, 135(2), 293–319.
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.
- Pagnotta, E. (2022). Decentralizing money: Bitcoin prices and blockchain security. *The Review of Financial Studies*, 35(2), 866–907.
- Schilling, L., & Uhlig, H. (2019). Some simple bitcoin economics. *Journal of Monetary Economics*, 106, 16–26.
- Van Loon v. Department of the Treasury (U.S. Court of Appeals for the Fifth Circuit, November 2024).
- Zetsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance. *Journal of Financial Regulation*, 6(2), 172–203.