INFRASTRUCTUREOUTSIDETHEPERIMETER · PART3OF4

The Settlement Layer Nobody Licenses

Public Blockchain Infrastructure and the Regulated Firm

David Newns, Substrate Advisory
July 2026

1. The structural fact

When a licensed firm issues, custodies or settles a tokenised asset on a public blockchain, the settlement layer beneath the transaction is operated by validators no supervisor authorises, upgraded through processes no jurisdictional authority controls and reached, for almost every regulated firm, through a small group of US access providers hosted on the hyperscaler clouds examined in the second report of this series. The asset lives on the chain, and the dependency travels with it.

The thesis of this series is that each of four technologies, AI, cloud, public blockchain infrastructure and post-quantum cryptography, is driving changes in the regulatory environment, and that a licensed firm has three postures available: respond, exploit or ignore. For public blockchain infrastructure the regulatory change has a distinctive shape. Regulators have not extended the perimeter to the chain itself; no instrument anywhere authorises Ethereum. What they have built instead is a set of accommodation regimes around the dependency: the EU's DLT Pilot Regime, which the European Commission proposed in December 2025 to place on a permanent footing,[1] the UK's Digital Securities Sandbox, which produced its first live-approved firm in July 2026,[2] and a Basel prudential standard, in force since 1st January 2026, that prices exposure to permissionless infrastructure directly into bank capital.[3] The firms these regimes were built for are the ones that treat the settlement-layer dependency as an architected risk rather than an inherited fact. That is the response case. The reason it belongs on a board agenda this year rather than next is that the accommodation regimes produced their first live outcomes in 2026, their admission criteria reward demonstrated infrastructure-risk competence, the current windows are finite and the firms admitted early will shape the permanent frameworks that follow them.

2. The dependency as it stands

The dependency decomposes into four layers, and a board should be able to name its exposure at each.

The consensus layer. Bitcoin and Ethereum, the two chains that dominate global digital-asset market capitalisation,[4] are operated by miners and validators that no authority licenses. On Ethereum, participation in consensus is mediated by staking, and staking has concentrated: the largest liquid-staking protocol, Lido, accounted for roughly a quarter of all staked ether at the start of 2026, distributed across a curated set of node operators, with the protocol's own decentralisation modules holding around 2 per cent of total network stake.[5] Concentration at this layer matters because of the arithmetic of finality: it takes two thirds of validators to finalise the chain, so any actor or correlated group approaching that share becomes a settlement-integrity question for everything recorded on the ledger.[6]

The access layer. A firm does not transact with the chain directly; it transacts through node infrastructure. Remote procedure call (RPC) and indexer providers, Infura, Alchemy and QuickNode chief among them, sit between almost every regulated application and the ledger, and they run on the major US clouds: when the US-EAST-1 region failed on 20th October 2025, Infura reported disruption across seven of its network endpoints, Ethereum mainnet among them.[7] The access layer therefore sits inside the cloud concentration described in the second report of this series.[8] A firm can operate its own node, and the more capable custodians do. What resists self-hosting is the indexing and historical-data layer: a node answers questions about current state cheaply, while reconstructing transaction history, token balances across contracts and event logs at production speed requires an indexing estate that in practice concentrates on the same few providers. The dependency is therefore layered even for firms that believe they have removed it.

The oracle and bridge layer. Price feeds and other external data enter the chain through oracle networks steered by commercial developers, Chainlink Labs among them; bridge operators range from commercial

vendors to foundations and developer collectives. None is authorised by any financial supervisor, and the loss record at this layer, set out below, is the documented core of the cost case.

The client-software layer. The software that defines settlement semantics, Bitcoin Core for Bitcoin and Geth foremost among Ethereum's execution clients, is maintained by foundations and volunteer developers. Client concentration is a live consensus risk in its own right: if a client run by more than two thirds of validators carries a consensus bug, the chain can finalise an incorrect fork, and the community's own diversity monitoring relies on self-reported data covering roughly two thirds of the network as at July 2026.[6] The November 2020 incident described below showed what a client bug does when it meets a concentrated access layer.

The stack beneath regulated activity has always extended below the regulatory perimeter; every bank runs on operating systems it did not write and no supervisor authorises. The difference is substitutability. The operating-system layer is commoditised, multi-vendor and replaceable without moving the business that runs on it. A settlement chain is not: the asset is recorded on the chain, the client relationship assumes the chain and exit from the chain means exit from the asset. That distinction, argued in the first two reports for models and clouds respectively, is at its sharpest here, because at least a workload can in principle be rebuilt on another cloud. A bearer instrument on Ethereum cannot be moved to a different ledger by its custodian.

3. The regulatory response in motion

Start from what no instrument does. No European, UK, Swiss or US authority licenses, inspects or sanctions the operators of a public permissionless chain, and none has proposed to. Every instrument described below is built around that fact: the regimes authorise the regulated firm's use of the infrastructure, adjust the legal framework to accommodate it or price the residual risk into capital. The settlement layer itself remains outside the perimeter at the end of this section exactly as it stood at the beginning.

European Union: the DLT Pilot Regime. Regulation (EU) 2022/858 has applied since 23rd March 2023 and allows market infrastructures using distributed ledger technology to operate trading and settlement under specific permissions with targeted exemptions from MiFIR, MiFID II and CSDR, including from the conventional separation of trading and settlement.[9] Uptake was slow: the first specific permission came only in October 2024, and by July 2025 four DLT market infrastructures had been authorised, a settlement system in Prague in October 2024, a trading and settlement system in Germany in December 2024, an MTF in Germany in April 2025 and a second trading and settlement system in Lithuania in July 2025.[10,11] ESMA's June 2025 review nonetheless recommended making the regime permanent, with tiered thresholds and a wider asset scope,[10] and on 4th December 2025 the Commission moved: its Market Integration and Supervision Package proposes removing all time limits on DLT Pilot Regime authorisations, with ESMA's next review report due by 24th March 2030.[1] The direction, subject to the legislative process, is that the accommodation becomes permanent.

Two points about the regime matter for this report's argument. The authorised infrastructures are not all on private ledgers; one of the four operates its trading and settlement system on a public permissionless Ethereum-compatible network,[10] which means the EU has, in a supervised setting, already accepted regulated settlement running on infrastructure it does not control. And the regime is deliberately an experiment in what compensatory measures make that acceptable, which is why its supervisory record, exemptions granted, conditions imposed, incidents observed, is the closest thing Europe has to an evidence base on the question this report poses.

European Union: MiCAR. For crypto-asset service providers, the Markets in Crypto-Assets Regulation has applied since 30th December 2024. A custodian authorised under MiCAR carries liability to clients for the loss of crypto-assets held in custody and must segregate client holdings,[12] yet the settlement layer on which those holdings exist is untouched by the authorisation: the regime reaches the custodian's keys, systems and conduct, and stops at the chain. Liechtenstein's Token and TT Service Provider Act, in force since 1st January 2020, made the same structural choice five years earlier, regulating the service providers around the token rather than the ledger beneath it, and remains the earliest dedicated framework of its kind in Europe.[13]

United Kingdom. The Digital Securities Sandbox, operated by the Bank of England and the FCA, opened on 30th September 2024 and runs to December 2028, with the application window expected to close around March 2027 so that entrants can transition to a possible permanent regime.[14] It is built as a sequence of gates: entry at Gate 1, live issuance, trading and settlement of real digital securities after Gate 2, then scaling stages under limits.[14] The regime crossed from framework to fact in July 2026, when HSBC's Orion platform became the first entrant approved through Gate 2, permitted to operate live as a digital securities depository, including for the issuance and settlement of DIGIT, the UK government's digital gilt pilot.[2] The sandbox modifies UK legislation temporarily for its entrants; like the EU regime, it accommodates the technology inside the perimeter rather than extending the perimeter to the infrastructure.

Switzerland. The Swiss DLT Act, fully in force since 1st August 2021, took the civil-law route: it created ledger-based securities as a category of Swiss law and a DLT trading facility licence under FINMA, embedding the accommodation in the statute book rather than in a time-limited pilot.[15]

United States. The statutory picture moved in 2025 and stalled in 2026. The GENIUS Act, signed on 18th July 2025, created a federal framework for payment stablecoins, the settlement asset for a large share of public-chain activity.[16] The market-structure legislation, the Digital Asset Market Clarity Act, passed the House on 17th July 2025 by 294 votes to 134 and was approved by the Senate Banking Committee on 14th May 2026 and placed on the Senate calendar on 1st June, but as at 18th July 2026 no Senate floor vote has been scheduled and the bill's 2026 prospects narrow with each week before the August recess.[17] The relevance to a European firm is indirect but real: the chains, the access providers and most of the oracle and bridge operators are US entities, and the statutory framework that eventually governs them will be set in Washington, on Washington's timetable.

International. The Basel Committee's cryptoasset standard, SCO60, entered into force in the Basel Framework on 1st January 2026 after a one-year deferral.[3] Its design encodes the thesis of this report in capital terms: tokenised traditional assets on permissionless blockchains cannot qualify for the preferential Group 1 treatment, whatever the quality of the asset, because the Committee judged the risks of permissionless infrastructure insufficiently mitigated, and unbacked cryptoassets in Group 2b attract a 1,250 per cent risk weight.[3] A targeted review is under way in 2026 and industry associations have pressed for recalibration of the permissionless-chain treatment,[18] so the position may soften. As it stands, SCO60 is the one instrument anywhere that prices the settlement-layer dependency itself, and it prices it punitively.

The pattern across jurisdictions is consistent. The perimeter is not being extended to the chain. The firm's use of the chain is being accommodated, and the residual risk is being priced into the firm's own capital and controls. Which means the infrastructure risk sits, by regulatory design, with the firm, and the next section is about carrying it deliberately.

4. What response looks like

The compliance floor for an EEA firm is set by DORA and, where applicable, the conditions of a DLT Pilot Regime permission or MiCAR authorisation. The work that distinguishes a well-run firm sits above that floor, in five areas.

Put the chain stack in the dependency inventory. DORA's register of information compels an inventory of ICT third-party arrangements. In my experience the chain-facing entries are the weakest part of most registers: the RPC providers, the indexing services, the oracle networks relied on for pricing or settlement triggers and the client software versions in production are dependencies of the kind the register exists to capture, and they are frequently absent because no contract exists or the service is free. A board should be able to see, for each regulated product, the chain, the access route, the physical and jurisdictional location of that access route and the external data feeds on the critical path. The access route usually resolves to a US-headquartered provider on a US cloud. Recording that fact is the point of the exercise, and not knowing it is the failure.

Decide the node posture deliberately. Operating one's own nodes removes the availability and integrity dependence on RPC providers for current-state operations, keeps transaction submission under the firm's control and is, for the chains on a custodian's critical path, the defensible default. It does not remove the indexing dependency, and it does not touch protocol governance. The honest architecture statement is therefore layered: self-operated nodes for consensus-critical functions, multi-provider RPC routing with tested failover for everything else and a documented, accepted residual dependency on external indexing. What the November 2020 record punishes is the unexamined single-provider default.

Treat unlicensable vendors as vendors. Oracle networks and bridge operators cannot be brought inside a contract regime the way a cloud provider can, and several are foundations or collectives with no entity to paper. The absence of a contract is not an exemption from vendor risk management. What changes is the form the discipline takes: exposure minimisation and due diligence on the mechanism, what the oracle's data sources and aggregation are, what the bridge's trust model is, who holds the keys and what the incident history says. For a regulated custody or settlement flow, the strong default is that bridges do not sit on the critical path at all; the loss record set out below is the reason.

Hold a fork and upgrade playbook. Protocol upgrades are decided by developer communities and validator adoption, not by the firm or its supervisor. Most are routine. The playbook is for the ones that are not: a contentious fork that splits the asset, an emergency patch to a consensus bug or an upgrade that changes settlement semantics the firm's reconciliation assumes. The playbook names who decides which chain the firm follows, on what criteria, how client assets and claims are treated across a split and what is communicated to clients and the supervisor while the question is open. Writing it during the event is the failure mode.

Know the cryptographic exposure now. Bitcoin and Ethereum secure their wallets with elliptic-curve signatures, the primitive that Shor's algorithm breaks, and any address whose public key is already visible on-chain can be attacked the day a sufficiently capable quantum computer exists, whatever post-quantum scheme the chains later migrate to.[19] The chains' own developer communities will lead the protocol migration and a custodian will largely inherit it; what a custodian cannot inherit is the exposure that precedes migration, which is set by its own key-management and address-reuse practices today. The fourth report in this series takes this up in full. The board-tractable step now is an inventory: which holdings sit on which signature schemes, with which key-exposure characteristics, against the NIST draft timeline that deprecates current elliptic-curve cryptography after 2030.[20]

5. The advantage case

The advantage here is more concrete than for AI or cloud, because the accommodation regimes are gated and their current windows are constrained: the UK sandbox admits firms to live activity under limits and expects to close its application window around March 2027,[14] and the EU regime runs under aggregate value thresholds that the December 2025 reform proposal would lift from 6 billion to 100 billion euros.[1] The scarce commodity is not a permanently capped seat count but a supervised live position obtained before the permanent framework crystallises, and the gate is application quality.

A firm that can evidence the architecture described above, the dependency inventory, the node posture, the fork playbook, the exposure minimisation at the oracle and bridge layer, is presenting a supervisor with exactly the compensatory-measures story the DLT Pilot Regime and the Digital Securities Sandbox were designed to elicit. The regimes' early record rewards it: four authorisations in the EU regime and one live approval in the UK sandbox as at July 2026 mean that each successful applicant to date has obtained something scarce, a supervised route to operating settlement infrastructure on new technology ahead of a permanent framework whose shape its early participants will influence.[2,10] The UK's first Gate 2 approval going to the platform selected for the government's own digital gilt issuance shows what the position is worth: the early mover becomes the infrastructure on which the official-sector experiment runs.[2]

There is a second, quieter advantage in counterparty terms. In my experience institutional clients and their consultants now run digital-asset due-diligence questionnaires that ask the questions in the closing section of this report, and a custodian that can answer them from an existing inventory rather than a scramble is an easier counterparty to approve, on a timetable the client controls rather than the firm.

The honest caveats are two. The population of authorised firms is small, so the advantage is demonstrable in individual cases but proves nothing statistically; and I cannot evidence a funding-cost or valuation premium attaching to settlement-layer risk maturity as at July 2026. The claim that survives the evidence is narrower: in regimes where admission is discretionary and the windows are finite, demonstrated infrastructure-risk competence is the currency of admission, and admission is where the optionality sits.

6. The cost of ignoring it

The loss record at the unregulated layers is documented and large, and it requires no embellishment.

Bridges are the worst of it. Chainalysis estimated that around 2 billion US dollars had been stolen across thirteen cross-chain bridge attacks in 2022 by early August of that year, roughly 69 per cent of all crypto-asset theft over that period.[21] The Ronin bridge lost approximately 620 million US dollars in March 2022 through compromised validator keys, a theft the FBI attributed to the North Korean Lazarus Group;[22] the Wormhole bridge lost around 320 million US dollars in February 2022 through a signature-verification flaw; the Nomad bridge lost around 190 million US dollars in August 2022 after an upgrade error caused it to treat effectively any message as valid.[21]

Oracles have produced losses without, so far, producing durable enforcement precedent. In October 2022 a trader manipulated the price inputs to Mango Markets' oracle and withdrew crypto-assets the SEC valued at approximately 116 million US dollars; the CFTC brought its first oracle-manipulation enforcement action in January 2023 and a federal jury convicted the trader in April 2024, though the trial court overturned all three convictions in May 2025, finding among other things that the platform's permissionless design left insufficient evidence of any false representation.[23,24,25,26] The episode carries two lessons for a regulated firm: the infrastructure was manipulable, and the criminal law reached its limits because the infrastructure

had no rules to break. A regulated firm depending on oracle inputs cannot assume the courts will backstop the feed.

The access layer has its own record. On 11th November 2020 a consensus bug in older versions of the Geth client split Ethereum at block 11234873, and because Infura's infrastructure was running affected versions, its outage took down the default access route for a large share of the ecosystem for several hours: exchanges including Binance and Bithumb suspended ether and ERC-20 withdrawals, and applications built on the default provider stopped.[27] The incident is the settlement-layer analogue of the US-EAST-1 outage of 20th October 2025 examined in the second report:[28] a fault in shared infrastructure, propagated simultaneously to every firm on the same dependency, with the additional feature that the chain itself briefly disagreed about its own state.

None of these losses has yet fallen on the regulated custody activity of an EEA-licensed firm in a way that produced a published supervisory finding, and that should be said plainly. The record shows where the losses concentrate, at bridges, oracles and concentrated access, which is the map a firm needs for the exposure-minimisation work above. A firm that ignores the layer is choosing to discover the map from its own incident.

7. Board questions

1. For each regulated product touching a public chain, can the executive name the chain, the access route, the provider and cloud region behind that route and the external data feeds on the critical path, and does our DORA register of information contain those entries?
2. What is our node posture, which functions run through our own nodes as against third-party RPC providers, and when did we last exercise failover between access providers?
3. Do any bridges or cross-chain transfers sit on a regulated custody or settlement flow, and if so, what is the documented trust model and who accepted the exposure?
4. Where do we depend on oracle data for pricing, settlement or collateral triggers, and what happens to each dependent process if the feed is wrong for thirty minutes?
5. What is our playbook for a contentious fork or an emergency consensus-bug patch on a chain where we hold client assets, and who decides which chain we follow?
6. Which of our holdings sit on signature schemes that the post-quantum transition will deprecate, and what do our address-reuse and key-exposure practices add to that exposure today?

8. Sources and notes

1. European Commission, Market Integration and Supervision Package, 4th December 2025 (proposal to reform Regulation (EU) 2022/858, including the removal of time limits on DLT Pilot Regime authorisations, the lifting of the aggregate market-value threshold from 6 billion to 100 billion euros and a further ESMA report due by 24th March 2030): https://finance.ec.europa.eu/publications/market-integration-and-supervision-package_en See also Taylor Wessing, "DLT Pilot Regime Reform: A new dawn for tokenisation of financial assets in the EU?", June 2026: https://www.taylorwessing.com/en/insights-and-events/insights/2026/06/dlt-pilot-regime-reform
2. HSBC, "HSBC is first company to get Bank of England regulatory approval to go live in the Digital Securities Sandbox," July 2026 (HSBC Orion approved through Gate 2 to operate as a digital securities depository, including for the issuance and settlement of DIGIT, the UK digital gilt): https://www.business.hsbc.com/en-gb/insights/hsbc-approved-for-digital-securities-sandbox

3. Basel Committee on Banking Supervision, SCO60: Cryptoasset exposures, in force in the Basel Framework from 1st January 2026 (implementation date 1st January 2026, one year later than originally scheduled; targeted amendments and disclosure framework finalised July 2024; tokenised assets on permissionless blockchains excluded from Group 1; Group 2b risk weight 1,250 per cent): https://www.bis.org/basel_framework/chapter/SCO/60.htm
4. FCA, "Description of the UK Cryptoasset Market," July 2026 (global cryptoasset market of approximately 2.7 trillion US dollars as at June 2026, most of it accounted for by Bitcoin, followed by Ethereum and stablecoins): https://www.fca.org.uk/publication/fca-research/crypto-market-description.pdf
5. Lido, "Lido Validator and Node Operator Metrics: Q4 2025," published 2026 (Community Staking Module and Simple DVT Module at nearly 800,000 ETH, 2.2 per cent of total Ethereum stake, as at 1st January 2026; Lido protocol stake of roughly 9 million ETH implying approximately a quarter of total staked ether): https://blog.lido.fi/lido-validator-and-node-operator-metrics-q4-2025/
6. clientdiversity.org, Ethereum client diversity monitoring (finality requires two thirds of validators; a client with a two-thirds share carrying a consensus bug can finalise an incorrect fork; execution-layer data self-reported, covering approximately 68.5 per cent of the network as at 18th July 2026): https://clientdiversity.org/
7. CoinDesk, "Crypto's Decentralized Illusion Shattered Again by Another AWS Meltdown," 21st October 2025 (Infura statement that the 20th October 2025 AWS outage disrupted its Ethereum Mainnet, Polygon, Optimism, Arbitrum, Linea, Base and Scroll endpoints): https://www.coindesk.com/news-analysis/2025/10/21/crypto-s-decentralized-illusion-shattered-again-by-another-aws-meltdown
8. Synergy Research Group, Q1 2026 cloud infrastructure market data (AWS 28 per cent, Microsoft 21 per cent, Google 14 per cent of a quarterly market of 129 billion US dollars): https://www.srgresearch.com/articles/cloud-market-annual-revenue-run-rate-topped-half-a-trillion-dollars-in-q1-as-growth-surge-continues
9. Regulation (EU) 2022/858 on a pilot regime for market infrastructures based on distributed ledger technology, applicable from 23rd March 2023: https://eur-lex.europa.eu/eli/reg/2022/858/oj
10. ESMA, "Report on the functioning and review of the DLT Pilot Regime" (Article 14 DLTR), ESMA75-117376770-460, 25th June 2025 (authorised DLT market infrastructures as at 31st May 2025: CSD Prague, DLT SS, permission from 11th October 2024; 21X AG, DLT TSS, from 3rd December 2024; 360X AG, DLT MTF, from 29th April 2025; 21X operating on a public permissionless Ethereum-compatible network; recommendations to make the regime permanent): https://www.esma.europa.eu/sites/default/files/2025-06/ESMA75-117376770-460_Report_on_the_functioning_and_review_of_the_DLTR_-_Art.14.pdf
11. Bank of Lithuania, financial market participants register (specific permission to operate a DLT trading and settlement system under Regulation (EU) 2022/858, valid from 9th July 2025): https://www.lb.lt/en/sfi-financial-market-participants/uab-axiology-dlt
12. Regulation (EU) 2023/1114 on markets in crypto-assets (MiCAR), Title V applicable from 30th December 2024; Article 75 sets the obligations of crypto-asset service providers providing custody and administration of crypto-assets on behalf of clients, including segregation of client holdings and liability for loss: https://eur-lex.europa.eu/eli/reg/2023/1114/oj
13. TVTG (Token and TT Service Provider Act), in force 1st January 2020. FMA Liechtenstein: https://www.fma-li.li/en/supervision-regulation/fintech/tvtg
14. FCA, Digital Securities Sandbox (opened 30th September 2024; operational until December 2028; application window expected to close around March 2027; live activity in real digital securities after Gate 2): https://www.fca.org.uk/firms/innovation/digital-securities-sandbox
15. Swiss Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, fully in force 1st August 2021 (ledger-based securities in the Code of Obligations; DLT trading facility licence under the Financial Market Infrastructure Act). Swiss Federal Council announcement: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-84035.html
16. GENIUS Act (Guiding and Establishing National Innovation for US Stablecoins Act), signed 18th July 2025: https://www.congress.gov/bill/119th-congress/senate-bill/1582
17. Digital Asset Market Clarity Act, H.R. 3633, 119th Congress (passed the House 17th July 2025, 294 to 134; approved by the Senate Banking Committee 14th May 2026; reported with an amendment and placed on the Senate Legislative Calendar, Calendar No. 423, 1st June 2026; no floor vote scheduled as at 18th July 2026): https://www.congress.gov/bill/119th-congress/house-bill/3633
18. Joint trade associations letter to the Basel Committee on Banking Supervision calling for recalibration of SCO60, August 2025: https://www.gfma.org/wp-content/uploads/2025/08/bcbs-prudential-letter-final-public-version.pdf

19. Technical note: secp256k1 / ECDSA is the signing algorithm for Bitcoin and Ethereum; the curve is not a NIST-approved curve, but the same Shor's-algorithm vulnerability applies to all elliptic-curve cryptography of this family.

20. NIST IR 8547 (initial public draft, 12th November 2024; proposes deprecating current elliptic-curve cryptography and RSA-2048 after 2030 and disallowing them after 2035; the dates are NIST's technical judgement and remain in draft): https://csrc.nist.gov/pubs/ir/8547/ipd

21. Chainalysis, cross-chain bridge attack estimates, 2nd August 2022 (approximately 2 billion US dollars stolen across thirteen bridge attacks in 2022 to that date, roughly 69 per cent of crypto-asset theft over that period; Wormhole approximately 320 million US dollars, February 2022; Nomad approximately 190 million US dollars, August 2022): https://www.chainalysis.com/blog/cross-chain-bridge-hacks-2022/

22. FBI statement attributing the theft of 620 million US dollars in Ethereum reported on 29th March 2022, the Ronin bridge incident, to the Lazarus Group and APT38, 14th April 2022: https://www.fbi.gov/news/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea

23. US Securities and Exchange Commission, "SEC Charges Avraham Eisenberg with Manipulating Mango Markets' Governance Token to Steal $116 Million of Crypto Assets," 20th January 2023: https://www.sec.gov/newsroom/press-releases/2023-13

24. US Commodity Futures Trading Commission, first oracle-manipulation enforcement action, 9th January 2023: https://www.cftc.gov/PressRoom/PressReleases/8647-23

25. US Department of Justice, conviction of Avraham Eisenberg by federal jury for commodities fraud, commodities manipulation and wire fraud, 18th April 2024 (convictions subsequently overturned; see source 26): https://www.justice.gov/usao-sdny/pr/avraham-eisenberg-convicted-manipulation-mango-markets

26. United States v. Eisenberg, No. 23-cr-10 (S.D.N.Y.), opinion and order of 23rd May 2025 (Rule 29 ruling vacating the commodities fraud and manipulation convictions for improper venue and entering a judgment of acquittal on the wire fraud count for insufficient evidence of a materially false representation). See The Block, "U.S. judge overturns fraud convictions of Mango Markets exploiter Eisenberg, determining improper venue," 24th May 2025: https://www.theblock.co/post/355666/u-s-judge-overturns-fraud-convictions-of-mango-markets-exploiter-eisenberg-determining-improper-venue

27. The Block, "Ethereum infrastructure provider Infura is down, crypto exchanges begin to disable ETH withdrawals," 11th November 2020 (consensus bug at block 11234873 affecting older Geth versions; Binance and Bithumb suspended ether and ERC-20 withdrawals; MetaMask affected as a default Infura client): https://www.theblock.co/post/84232/ethereum-infrastructure-provider-infura-is-down

28. AWS post-event summary, US-EAST-1 service disruption, 20th October 2025 (latent race condition in DynamoDB automated DNS management): https://aws.amazon.com/message/101925/

David Newns is an Advisor to BPX Markets Limited and an Independent Non-Executive Director of Axiology Group. The views expressed are personal and do not represent the positions of any organisation with which he is associated. Nothing in this report constitutes legal, regulatory or investment advice.