L12: Controversies & Future – Lecture

BSc Blockchain Course

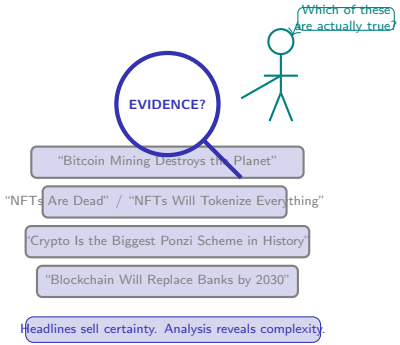
Digital Finance

Why Must We Evaluate Blockchain Claims with the Same Rigour We Apply to Any Other Technology?

Blockchain is surrounded by more marketing than almost any technology in recent memory. Startup pitches promise to "revolutionise" industries. Critics dismiss the entire space as a speculative bubble. Between these extremes lies a narrow band of legitimate innovation – but finding it requires analytical tools, not tribal loyalty. **The analytical challenge:**

- **Enthusiasm bias:** Early adopters have financial incentives to promote adoption, making their claims unreliable as neutral evidence.
- **Scepticism bias:** Critics who dismissed the internet in the 1990s remind us that blanket rejection is also a poor analytical strategy.
- **Complexity barrier:** The technology is genuinely difficult – cryptographic proofs, consensus mechanisms, game theory – which means most commentators operate on second-hand summaries.

This lecture equips you with a framework to cut through both the hype and the dismissal. By the end, you will have four diagnostic questions that separate substance from noise.



The most dangerous position in blockchain is not being wrong – it is being certain. Both uncritical enthusiasm and reflexive dismissal substitute tribal identity for analysis.

Critical evaluation is not scepticism – it is the discipline of demanding evidence before forming conclusions.

Can You Tell Which of These Blockchain Claims Are True?

You have spent eleven weeks studying blockchain technology. You understand hashing, consensus, smart contracts, DeFi, and DAOs. Now test whether that knowledge translates into controversy detection.

Quick Exercise – Myth or Fact? (2 minutes)

Read each statement. For each, write M (myth), F (fact), or C (it's complicated). No peeking ahead.

1. **"Bitcoin uses more energy than some countries."** M / F / C .....
2. **"Ethereum's Merge eliminated blockchain's energy problem."** M / F / C .....
3. **"Most cryptocurrency transactions are used for crime."** M / F / C .....
4. **"Decentralized systems cannot be regulated."** M / F / C .....
5. **"CBDCs will make Bitcoin obsolete."** M / F / C .....

Hold your answers. We will revisit each claim with evidence over the next eight slides. By slide 9, you will have the tools to evaluate claims like these independently.

The correct answer to most blockchain controversies is "it's complicated" – but the reasons why are where the learning happens.

What Controversies Divide the Blockchain Community Most Deeply?

Four controversy domains, four types of evidence needed:

Domain	Core Tension	Proponent View	Critic View	Evidence Type
Energy & Environment	Security vs cost	Renewables growing	PoW wastes energy	Measurable (TWh, mix)
Scams & Consumer harm	Freedom vs protection	Bad actors everywhere	Crypto enables fraud at scale	On-chain analytics
Regulation & Compliance	Innovation vs stability	Rules stifle growth	Consumers need guardrails	Comparative law
Centralization & Power	Ideal vs reality	Spectrum, not binary	Whales and VCs control chains	Nakamoto coefficient

Pattern to notice:

Each domain requires a different KIND of evidence. Energy disputes need physics and grid data. Scam debates need transaction forensics. Regulation needs comparative law. Centralization needs network metrics. No single expertise can settle all four.

Why four domains, not one:

- **The energy debate** is the most public-facing controversy. Headlines comparing Bitcoin to countries make it visceral – but the comparison hides the nuance of energy source and marginal utility.
- **The scam debate** is the most emotionally charged. Billions lost in rug pulls and exchange collapses make real victims, but the illicit share of total crypto volume has declined steadily.
- **The regulation debate** is the most consequential for builders. Where you incorporate, which tokens you list, and how you handle KYC depend entirely on jurisdiction.
- **The centralization debate** is the most philosophical. If three mining pools control over half of Bitcoin's hashrate, the "decentralized" label requires qualification.

These four domains interact: regulation affects energy (mining bans), scams trigger regulation, and centralization undermines the philosophical case for the whole ecosystem.

Blockchain controversies cluster into four domains that require four different kinds of expertise – which is why most public debates oversimplify.

The Nakamoto coefficient measures decentralization: the minimum number of entities needed to compromise a network.

What Actually Happened to Energy Consumption When Ethereum Switched to Proof of Stake?

1. Pre-Merge
PoW mining, 78 TWh/yr

↓

2. Beacon Chain (2020)
Parallel PoS chain; stake 32 ETH

↓

3. Testing (18 months)
Shadow forks to catch bugs

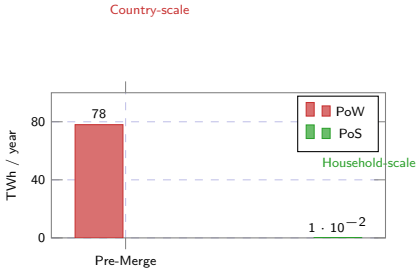
↓

4. The Merge (Sep 2022)
PoW stopped permanently

↓

5. Post-Merge
Energy: 78 TWh → 0.01 TWh

Before vs After:



What this proves – and does not:

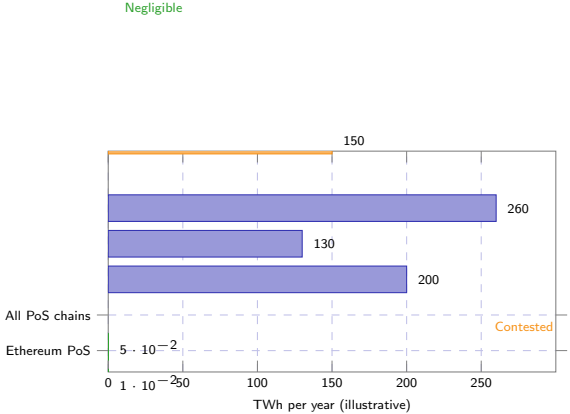
- **Proves:** PoS secures a major chain at negligible energy cost.
- **Does not prove:** Bitcoin will switch. Its community views PoW as a feature.
- **Open:** Does lower energy cost reduce security?

The Merge is the most significant natural experiment in blockchain energy policy: a live network worth hundreds of billions of dollars switched consensus mechanisms without downtime and cut energy use by over 99%.

Source: Illustrative data based on Ethereum Foundation energy estimates and Cambridge CCAF reports.

How Do We Measure Blockchain's Energy Impact Fairly Against Other Systems?

Annual energy comparison (illustrative TWh):



Illustrative figures. Banking includes branches, ATMs, data centres.

Three measurement traps to avoid:

- **Trap 1: Comparing totals without output.**
  Bitcoin processes seven transactions per second; Visa processes thousands. Comparing total energy without normalising by output is misleading.
- **Trap 2: Ignoring energy source.**
  A mine on stranded hydropower differs from one on coal. Over half of mining reportedly uses renewables – but "reportedly" does heavy lifting.
- **Trap 3: Comparing unlike systems.**
  Bitcoin provides censorship-resistant settlement; Visa provides fast payments. They solve different problems and are not substitutes.

Honest analysis: energy per what? what source? compared to what?

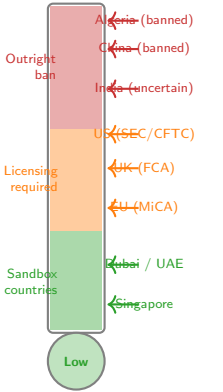
Energy comparisons are only meaningful when they specify three things: total consumption, energy source mix, and useful output per unit of energy.

Source: Illustrative comparison based on IEA, Cambridge CCAF, World Gold Council, and BIS estimates.

What Regulatory Risks Could Shut Down a Crypto Project Overnight?

Regulation is not a distant threat – it is the single largest source of existential risk for blockchain projects today. A token classified as a security in one country may be a commodity in another, and a banned instrument in a third. **Five regulatory actions that changed the industry:**

1. **China's mining ban (2021):** Hashrate dropped by half overnight; miners relocated globally. Proved that a single government can disrupt a "decentralized" network.
2. **SEC vs Ripple (2020–):** Multi-year lawsuit over whether XRP is a security. The legal ambiguity froze institutional adoption in the US.
3. **EU MiCA (2024):** First comprehensive crypto regulation. Stablecoin issuers must hold reserves; exchanges need licenses. Sets a global template.
4. **Tornado Cash sanctions (2022):** US Treasury sanctioned a smart contract – not a company, not a person, but code. Raised the question: can open-source software be illegal?
5. **Travel Rule expansion:** Financial Action Task Force requires exchanges to share sender and receiver identity for transfers above a threshold – extending banking surveillance to crypto.

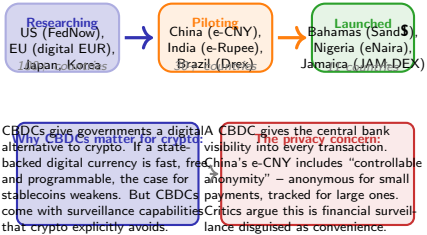


The same token can be legal, licensed, or banned depending on which country you are standing in.

Regulatory risk is not hypothetical – it has already shut down mining operations, frozen token trading, and sanctioned smart contract code. Projects must design for regulatory diversity from day one.

MiCA = Markets in Crypto-Assets; FATF = Financial Action Task Force; the Tornado Cash case tested whether code is speech.

Where Are Central Bank Digital Currencies Emerging – and Why Does It Matter for Crypto?



CBDCs and crypto solve opposite problems: state control vs individual sovereignty.

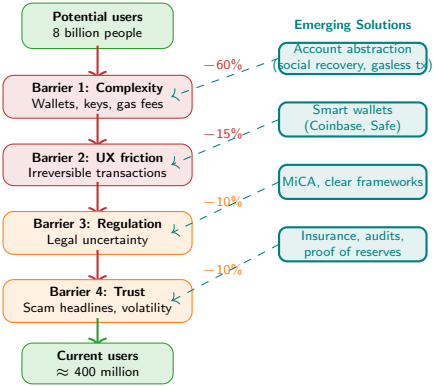
CBDC adoption pipeline – three key observations:

- **Scale:** Over 100 countries are researching CBDCs – covering over 95% of global GDP. This is not a fringe experiment; it is a coordinated response to the decline of physical cash and the rise of private digital money.
- **Pilot results are mixed:** China's e-CNY has been tested in dozens of cities but adoption remains low relative to Alipay and WeChat Pay. Nigeria's eNaira had limited uptake. The technology works; the demand question is unsettled.
- **Privacy is the battleground:** Crypto advocates view CBDCs as surveillance tools. Central bankers view them as financial stability instruments. The design choice – how much transaction data the state can see – is the defining political question.
- **Coexistence is likely:** CBDCs, stablecoins, and decentralized crypto will likely coexist, serving different user needs: state payments via CBDC, commerce via stablecoins, censorship resistance via Bitcoin and Ethereum.

CBDCs represent government's response to private digital money – they offer programmability and efficiency but introduce state visibility into every digital transaction.

Source: Illustrative pipeline based on Atlantic Council CBDC Tracker and BIS Annual Survey.

What Barriers Prevent Blockchain from Reaching the Next Billion Users?



Who is blocked, and who benefits from the barrier?

- **Technical complexity** blocks the vast majority.
  Managing private keys, understanding gas fees, and navigating bridge protocols requires knowledge most users do not have. Account abstraction (ERC-4337) aims to hide this complexity behind familiar login flows.
- **UX friction** punishes mistakes permanently.
  Send tokens to the wrong address? Gone forever. No customer support, no refund, no reversal. This is a feature for censorship resistance – and a catastrophic flaw for everyday payment use.
- **Regulatory uncertainty** freezes institutional capital.
  Banks and funds will not allocate to assets they cannot classify legally. Clear rules (even strict ones) unlock more capital than ambiguity.
- **Trust deficit** is the hardest to fix.
  Every scam headline erodes public confidence faster than any technical improvement can rebuild it. Proof of reserves and insurance products are emerging responses.

Each barrier has a corresponding solution under development – but solutions take years while headlines about losses travel instantly.

Account abstraction (ERC-4337) and smart wallets are the most promising UX improvements currently in production.

Four Questions That Reveal Whether a Blockchain Claim Is Substance or Hype

After twelve weeks of studying blockchain, you now have enough context to evaluate any claim independently. Apply these four questions in order:

Question 1: What specific problem does this solve?

If the pitch says "decentralization" without naming a concrete pain point – a cost, a delay, an exclusion – it is marketing, not engineering. Legitimate projects name the problem in one sentence. **Question 2:**

Could a traditional database solve this more cheaply?

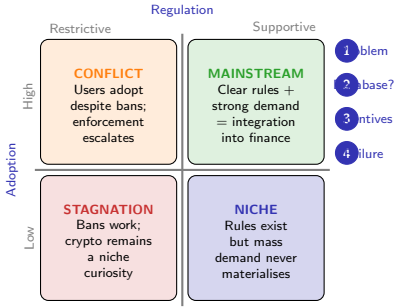
Blockchains add value only when multiple parties must write to a shared ledger without trusting a single operator. If one company controls the system, a database is faster, cheaper, and simpler. **Question 3:**

Who pays, who benefits, and who bears the risk?

Every system has a distribution of gains and losses. Token holders, validators, users, and regulators have different incentives. Map them before committing resources. **Question 4: What is the failure**

mode?

Ask what happens when core assumptions break: oracle manipulation, validator collusion, regulatory action, or a smart contract bug. If the team has no answer, the project has not been stress-tested.



Every claim bets on a quadrant. The four questions tell you which.

The four questions are a portable evaluation framework. They work for startup pitches, policy papers, and media headlines equally well – because hype fails the same tests regardless of source.

Evidence-based evaluation: what problem? could a database suffice? who pays and who bears risk? what breaks?

Your Challenge

You now have four diagnostic questions and twelve weeks of blockchain knowledge. Apply them.

Evaluate This Claim Using the Four-Question Framework (5 minutes)

Claim: "A startup proposes using blockchain to track organic food certifications. Farmers record harvests on-chain; consumers scan QR codes to verify origin. The token appreciates as more farms join."

Apply the four questions:

Question	Pass / Fail?	Your reasoning (one sentence)
Q1: What problem does this solve?	.....	.....
Q2: Could a database do this cheaper?	.....	.....
Q3: Who pays, benefits, bears risk?	.....	.....
Q4: What is the failure mode?	.....	.....

Discuss with your neighbour (3 min):

- Does this project need a blockchain, or would a database with an auditor suffice?
- The token "appreciates" – utility or speculation? Does it pass Q3?
- Revisit your myth/fact answers from Slide 2. Have any changed?

The best framework is one you actually use. Apply these four questions to every blockchain claim you encounter from today onward.