Blockchain Economics

ECOM215: Blockchain Economics and Digital Assets

Dr Daniele Bianchi

Queen Mary, University of London

Semester B, 2025/2026

Today's Agenda

The Consensus Problem

Proof-of-Work

Proof-of-Stake

The Blockchain Trilemma

Economic Implications

Summary and Next Steps

The Consensus Problem

Why Consensus Matters

Recall from Topic 1: blockchain is a shared ledger with no central authority.

The fundamental question:

> How do strangers agree on the state of a shared database when some of them might be lying?

This is the **consensus problem**—and solving it is what makes blockchain work.

What we need:

- All honest participants agree on the same transaction history
- Dishonest participants cannot corrupt the ledger
- The system keeps working even if some nodes fail or misbehave

The Double-Spend Problem

Digital cash has a unique problem: data can be copied perfectly.

Example:

1. Alice has 1 BTC
2. Alice sends 1 BTC to Bob (Transaction A)
3. Alice *simultaneously* sends the same 1 BTC to Carol (Transaction B)
4. Which transaction is valid?

With physical cash, this is impossible—you can't hand the same note to two people.

With digital cash, both transactions are valid copies. **Someone must decide which one counts.**

Traditional solution: A bank maintains the authoritative ledger.
Blockchain solution: The network reaches consensus on transaction ordering.

Byzantine Fault Tolerance

The Byzantine Generals Problem

How can distributed parties reach agreement when some participants may be unreliable or actively malicious?

The setup: Generals surrounding a city must coordinate attack or retreat. They can only communicate by messenger. Some generals may be traitors sending conflicting messages.

The blockchain parallel:

- Thousands of nodes must agree on transaction history
- Some nodes might be offline, buggy, or malicious
- The system must produce a single consistent ledger anyway

A blockchain consensus protocol must be **Byzantine fault tolerant**—it works correctly even when some participants are adversarial.

What Makes Good Consensus?

A consensus protocol should deliver:

Property	**Meaning**
Safety	Honest nodes agree on the same history
Fault tolerance	System works despite failures/attacks
Decentralisation	No single party controls outcomes
Efficiency	Resources aren't wasted unnecessarily

The challenge: These properties often conflict. More security may mean less efficiency. More decentralisation may mean slower consensus.

This tension is formalised as the **blockchain trilemma** (later this lecture).

Proof-of-Work

The Bitcoin Innovation

Before Bitcoin (2009), decentralised digital cash had failed because of the double-spend problem.

Satoshi Nakamoto's insight: Make adding blocks *computationally expensive*.

- Participants ("miners") compete to solve a cryptographic puzzle
- The winner gets to propose the next block and receives a reward (newly minted coins + fees)
- Other nodes verify and accept the valid block

Why this works:

- Attacking the network requires out-computing all honest miners
- Cheating is expensive (you spend resources without receiving the reward), whereas honest behaviour is profitable
- No central authority decides who adds blocks

This is **Proof-of-Work** (PoW): prove you expended computational resources to compete in good faith.

How Mining Works

The puzzle: Find a random number ("nonce") that, when hashed with the block data, produces an output starting with a certain number of zeros.[1]

Since hash outputs are unpredictable, there's no shortcut—miners try billions of numbers until one works.

The process:

1. Collect pending transactions into a candidate block
2. Try random nonces until one meets the difficulty target
3. Broadcast the winning block to the network
4. Other nodes verify (instantly) and append the block to their chain
5. The winner receives a **block reward** and **transaction fees**

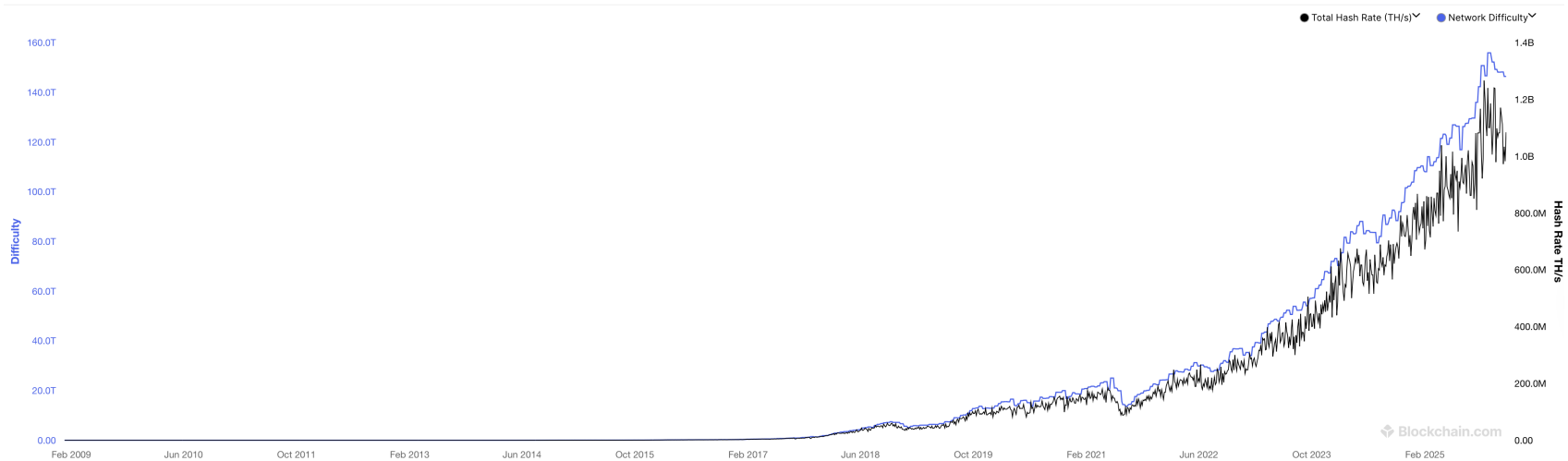
Key insight: Finding a valid nonce requires billions of guesses, but verifying one takes a single operation—hash the winner's answer and check whether it meets the target.

[1] The protocol sets how many zeros are required, adjusting automatically to keep block production steady (10 minutes for Bitcoin).

Difficulty Target Adjustment

Bitcoin targets one block every **10 minutes** on average.

Problem: If more miners join, blocks would be found faster.
Solution: The protocol automatically adjusts difficulty every 2,016 blocks ($\approx$ 2 weeks).



Implication: Mining is an **arms race**. More computing power improves your *relative* chance of winning but doesn't increase total block production.

Block Rewards and Halving

Miners receive two types of compensation:

1. **Block subsidy**: Newly created bitcoins (currently 3.125 BTC/block)
2. **Transaction fees**: Paid by users for inclusion

The halving: The block subsidy is cut in half every 210,000 blocks (≈4 years).

Date	Block Subsidy	Event
Jan 2009	50 BTC	Genesis
Nov 2012	25 BTC	1st halving
Jul 2016	12.5 BTC	2nd halving
May 2020	6.25 BTC	3rd halving
Apr 2024	3.125 BTC	4th halving
2028	1.5625 BTC	5th halving (expected)

This creates a **deflationary supply**: maximum 21 million BTC, reached around 2140.

The Transition to Fee-Based Security

As block subsidies decline, transaction fees must compensate miners.

The concern: Will fees alone provide sufficient security incentive?

Current state (post-April 2024 halving):

- Block subsidy: 3.125 BTC ($\approx$\$200k at \$60k/BTC)
- Average fees: highly variable (spikes during congestion)
- Fees as a share of miner revenue: typically $\approx$5–15%, higher during demand surges

Open question: Bitcoin's long-term security model depends on fees becoming the dominant incentive. Whether this will be sufficient remains debated.

This is a genuine **economic design uncertainty**—not a flaw, but an untested transition.

The Longest Chain Rule

Problem: What if two miners find valid blocks simultaneously?

Nakamoto's solution: Follow the **longest chain** (cumulative work).

1. Temporary "forks" occur naturally when blocks are found near-simultaneously
2. Miners choose which branch to extend
3. Eventually one branch gets ahead; the other is abandoned ("orphaned")
4. Transactions in orphaned blocks return to the mempool

Why it works: An attacker trying to rewrite history must outpace all honest miners. Assuming $>50\%$ hashpower controlled by honest miners, the honest chain grows faster.

Implication for users: Wait for multiple **confirmations** (blocks built on top of yours) before considering a transaction final. The Bitcoin convention is 6 confirmations ($\approx$1 hour).

PoW Security Model

What PoW protects against:

- Double-spending (would require rewriting blocks)
- Censorship (any miner can include any valid transaction)
- Counterfeit coins (invalid blocks are rejected by nodes)

The 51% attack: An attacker controlling majority hashpower could:

- Double-spend their own transactions
- Prevent specific transactions from confirming
- NOT steal others' coins (still need private keys)
- NOT create coins out of thin air (nodes reject invalid blocks)

Cost of attack: Estimated at billions of dollars for Bitcoin (hardware + electricity), making it economically irrational for a well-functioning network.

Smaller PoW chains with less hashpower are more vulnerable—several have suffered 51% attacks.

Proof-of-Stake

Beyond Proof-of-Work

PoW works, but has significant costs:

- Energy consumption: Bitcoin uses ≈100–150 TWh/year (comparable to some countries)
- Hardware waste: Mining rigs become obsolete quickly
- Centralisation pressure: Economies of scale favour large mining operations

Alternative idea: What if block producers had to risk *money* instead of spending *energy*?

Proof-of-Stake (PoS)

Validators are selected to propose blocks based on how much cryptocurrency they have "staked" (locked up as collateral). Misbehaviour results in losing the stake.

Instead of proving you spent resources (work), you prove you have skin in the game (stake).

How Proof-of-Stake Works

Basic mechanism:

1. Validators deposit (stake) cryptocurrency as collateral
2. The protocol randomly selects a validator to propose each block
3. Selection probability is proportional to stake size
4. Other validators attest (vote) that the block is valid
5. Validators earn rewards for honest participation

The enforcement mechanism: **Slashing**

- If a validator misbehaves (e.g., proposes conflicting blocks), a portion of their stake is destroyed
- This makes attacks expensive without wasting energy

Key difference from PoW: Security comes from *economic penalties* rather than *computational cost*.

The Ethereum Merge (September 2022)

Ethereum's transition from PoW to PoS is the largest consensus change in blockchain history.

Before (PoW):

- Miners competed with GPUs/ASICs
- Energy consumption: ≈80–100 TWh/year
- Block time: ≈13 seconds

After (PoS):

- Validators stake 32 ETH (≈$100k at current prices)
- Energy consumption: ≈0.01 TWh/year (99.95% reduction)
- Block time: 12 seconds (fixed slots)

The Merge demonstrated: A major blockchain can successfully change consensus mechanisms—though it required years of testing and coordination.

Staking Economics

To become an Ethereum validator:

- Stake exactly 32 ETH (minimum requirement)
- Run validator software 24/7 (or face penalties)
- Earn rewards for proposing blocks and attesting
- Current yield: ≈3–5% APR (varies with network activity)

Barriers to entry:

- Capital requirement: 32 ETH ≈ \$100,000+
- Technical complexity: Running validator infrastructure
- Illiquidity: Staked ETH was locked until 2023 withdrawals enabled

Liquid staking (e.g., Lido, Rocket Pool) addresses these barriers:

- Pool small amounts from many users
- Issue tradeable tokens representing staked ETH
- We'll discuss this further in Topic 4 (DeFi)

PoW vs PoS: Comparison

	Proof-of-Work	**Proof-of-Stake**
Security basis	Computational cost	Economic stake
Energy use	Very high	Minimal
Hardware needs	Specialised (ASICs)	Standard servers
Attack cost	Buy/rent hashpower	Acquire & risk stake
Barrier to entry	Capital + expertise	Capital (stake)
Example	Bitcoin	Ethereum (post-Merge)
Decentralisation	Mining pools	Staking pools
Finality	Probabilistic	Can be deterministic

Neither is strictly "better": They represent different trade-offs. Bitcoin maximalists argue PoW's energy cost *is* the security. PoS advocates argue it achieves equivalent security more efficiently.

Concerns About Proof-of-Stake

PoS is not without criticism:

"Rich get richer": Validators with more stake earn more rewards, potentially increasing concentration over time.

Nothing-at-stake problem: In theory, validators could vote for multiple chain forks costlessly. Addressed through slashing, but adds complexity.

Long-range attacks: An attacker with old keys could try to rewrite history. Mitigated by checkpointing and social consensus.

Validator centralisation: Large staking pools (Lido controls 30% of staked ETH) raise concerns similar to mining pool concentration.

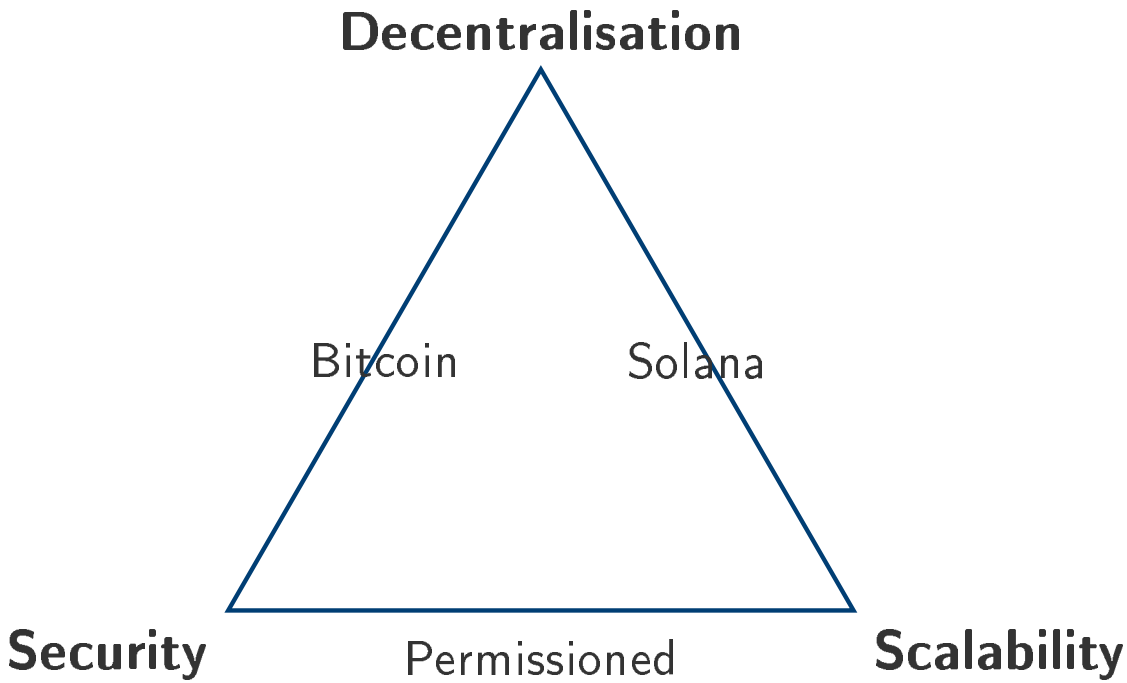
Bottom line: PoS solves PoW's energy problem but introduces different trust assumptions and centralisation risks. The long-term security properties are still being tested in production.

The Blockchain Trilemma

The Trilemma

Blockchain Trilemma (Vitalik Buterin)

A blockchain can optimise for at most two of three properties: **decentralisation**, **security**, and **scalability**.



This is not a proven theorem—it's an observed engineering trade-off.

Understanding the Trade-offs

Decentralisation $\longleftrightarrow$ Scalability

- More nodes = more communication overhead, slower consensus
- Bitcoin: 15,000 nodes, 7 transactions/second
- Visa: Centralised, 65,000 transactions/second

Security $\longleftrightarrow$ Scalability

- Faster blocks mean less time for propagation, creating more forks and easier attack opportunities
- Larger blocks process more transactions but require more storage and bandwidth, pricing out smaller validators

Security $\longleftrightarrow$ Decentralisation

- Stronger security requires more resources (hashpower or stake)
- Higher costs push participants toward pools, concentrating power

Different blockchains make different choices based on their intended use case.

Where Blockchains Sit

Blockchain	Decent.	Security	Scalability
Bitcoin	High	High	Low (≈7 TPS)
Ethereum	High	High	Low (≈15 TPS)
Solana	Lower	Medium	High (≈5000 TPS)
BNB Chain	Low	Medium	High
Hyperledger	Permissioned	High	High

Note: "High security" for permissioned chains means something different—they trust the known validators rather than relying on economic incentives.

The question is not which is "best" but which trade-off suits the application.

Layer 2: Escaping the Trilemma?

The idea: Don't do everything on the main chain (Layer 1).

Layer 2 Solutions

Process transactions off-chain, but inherit security from the main chain by periodically posting proofs or summaries.

Examples:

- **Lightning Network** (Bitcoin): Payment channels for instant, low-fee transactions
- **Rollups** (Ethereum): Bundle hundreds of transactions, post compressed data to L1

Layer 2 doesn't "solve" the trilemma—it moves the trade-off. You get scalability but add complexity and different trust assumptions.

Layer 2 in Practice

Ethereum's scaling roadmap centres on rollups:

- Arbitrum, Optimism (Optimistic Rollups): ≈$10B+ Total Value Locked (TVL) combined
- zkSync, StarkNet (ZK-Rollups): Emerging, more complex
- Fees: Often 10–100x cheaper than Ethereum mainnet
- Speed: Near-instant confirmation, periodic settlement to L1

Bitcoin's Lightning Network:

- Enables instant Bitcoin payments
- Capacity: ≈5,000 BTC locked in channels
- Adoption: Growing for micropayments, El Salvador's Chivo wallet

Trade-off: Layer 2 users must trust the rollup operators to some degree, and bridging between L1 and L2 introduces risk. We'll explore DeFi on L2 in Topic 4.

Economic Implications

Energy Consumption: The Updated Picture

Bitcoin (PoW): estimated ≈100–150 TWh/year

- Comparable to countries like Argentina or Norway
- Criticism: Environmental impact, carbon footprint
- Defence: Increasingly uses renewable/stranded energy; secures $1T+ network

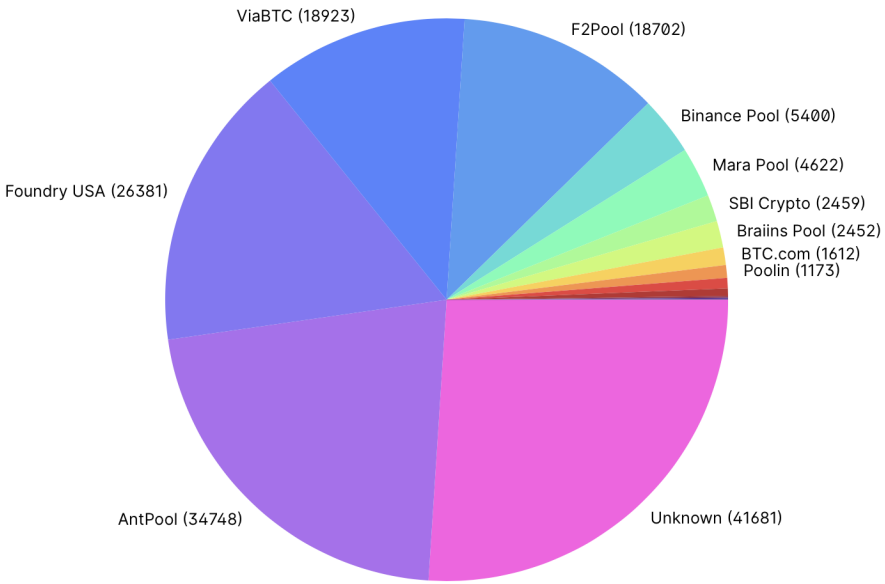
Ethereum (post-Merge PoS): ≈0.01 TWh/year

- 99.95% reduction from pre-Merge levels
- Comparable to a few thousand households

Implication: Energy criticism now applies specifically to PoW chains (primarily Bitcoin), not blockchain technology generally.

Mining Concentration

Despite decentralisation goals, mining tends toward concentration:



Summary of Mined Blocks

Miner / Pool	Percent	Blocks Mined
Unknown	26.029%	41681
AntPool	21.699%	34748
Foundry USA	16.474%	26381
ViaBTC	11.817%	18923
F2Pool	11.679%	18702
Binance Pool	3.372%	5400
Mara Pool	2.886%	4622
SBI Crypto	1.536%	2459
Braiins Pool	1.531%	2452
BTC.com	1.007%	1612
Poolin	0.733%	1173
BTC M4	0.596%	955
Ultimus	0.433%	693
Kucoin	0.086%	137
Luxor	0.046%	73
1THash	0.037%	60
Solo CKPool	0.027%	43
BTC M19	0.008%	13
KanoPool	0.004%	6
Zulu Pool	0.001%	2
CKPool	0.001%	1

Why concentration occurs:

- Economies of scale in hardware and electricity
- Access to cheap energy sources

Nuance: Pool operators don't control miners' machines. Miners can switch pools, providing some check on pool behaviour.

Wealth Concentration

Cryptocurrency holdings are highly concentrated:

Bitcoin distribution (approximate):

- ≈70% of addresses hold less than $1,000 worth of BTC
- ≈0.01% of addresses hold more than $10 million
- Concentration is real, but can be misleading: large addresses often represent exchanges, funds, or custodians holding on behalf of many users

Caveats:

- One person can have many addresses
- One address can represent many people (exchanges, funds)
- Early adopters naturally hold more (bought at $1, not $60,000)

Economic question: Does this concentration undermine the "democratising" narrative? Or is it simply reflecting early-stage adoption patterns?

Staking Concentration

PoS introduces similar concentration dynamics:

Ethereum staking (as of 2024):

- Lido (liquid staking): ≈30% of all staked ETH
- Coinbase, Kraken (exchanges): ≈15% combined
- Independent validators: minority share

Concern: If Lido validators collude, they could potentially censor transactions or extract value.

Mitigations:

- Lido uses multiple independent node operators
- Protocol-level discussions on capping any single entity's share
- Rocket Pool and others offer more decentralised alternatives

Takeaway: Decentralisation is a spectrum, not a binary. Both PoW and PoS face concentration pressures.

Scalability and Adoption

The challenge: Blockchain throughput vs real-world demand

System	Transactions/second
Bitcoin	≈7
Ethereum L1	≈15
Solana	≈5,000 (theoretical)
Visa	≈65,000 (peak capacity)

When demand exceeds capacity:

- Fees spike (Bitcoin fees hit $60+ in congestion)
- Users priced out of the network
- Adoption stalls for everyday use cases

Layer 2 helps: Arbitrum, Optimism process millions of transactions settling to Ethereum. But bridging complexity remains a barrier.

Summary and Next Steps

Key Takeaways

1. **Consensus is the core innovation**
   - Solves the double-spend problem without trusted third parties
   - Must be Byzantine fault tolerant
2. **Proof-of-Work**: Security through computational cost
   - Battle-tested (Bitcoin since 2009), but energy-intensive
   - Halving schedule creates transition to fee-based security
3. **Proof-of-Stake**: Security through economic stake
   - 99.95% less energy (Ethereum Merge demonstrated this)
   - Different trust assumptions and centralisation risks
4. **The trilemma**: Decentralisation, security, scalability—pick two
   - Layer 2 solutions shift trade-offs, don't eliminate them
5. **Concentration is real**: Mining pools, staking pools, wealth

What's Next

Topic 3: Smart Contracts and Decentralised Applications

- What is a smart contract?
- Ethereum Virtual Machine (EVM)
- DApp architecture and examples
- Smart contract security and risks
- Gas fees and EIP-1559

Preparation:

- Think about: What kinds of agreements could be automated if a computer could verify conditions and execute transfers?
- Explore: Look at a transaction on Etherscan (etherscan.io)—what information is visible?

Questions?