Tutorial 2: The Ethereum Merge

From Proof-of-Work to Proof-of-Stake

ECOM215: Blockchain Economics and Digital Assets

Week 3 | Blockchain Economics

Semester B, 2025/2026

CASE BRIEF FOR STUDENTS

Please read before the tutorial. Estimated reading time: 15 minutes.

Background

On 15 September 2022, at 06:42:42 UTC, Ethereum completed "The Merge"—the largest infrastructure change in blockchain history. In a single moment, the network switched from Proof-of-Work (PoW) to Proof-of-Stake (PoS), eliminating an entire industry of Ethereum miners and reducing the network's energy consumption by over 99.9%.

The Merge had been planned for years, delayed multiple times, and was widely considered the most technically ambitious upgrade ever attempted on a live blockchain with hundreds of billions of dollars in assets. Many predicted it would fail catastrophically. It didn't.

This case examines what the Merge was, why it mattered, and what it reveals about the economics of consensus mechanisms.

Why the Merge Happened

Ethereum launched in 2015 using Proof-of-Work, the same consensus mechanism as Bitcoin. By the early 2020s, Ethereum's PoW mining consumed approximately 80–100 TWh of electricity per year—comparable to the annual consumption of countries like the Netherlands or Chile.

The case against PoW:

- **Environmental criticism**: Climate activists, ESG-focused investors, and regulators increasingly targeted PoW's carbon footprint
- **Energy inefficiency**: The computational work in PoW serves only to prove resource expenditure—it produces nothing useful beyond security
- **Centralisation pressure**: Mining economies of scale pushed hashpower toward large industrial operations with access to cheap electricity

- **Hardware waste**: Mining equipment (GPUs, ASICs) became obsolete every 1–2 years

The case for switching to PoS:

- Energy reduction of 99.95%—from $\sim$100 TWh/year to $\sim$0.01 TWh/year
- Security through economic stake rather than computational waste
- Reduced barrier to participation (no specialised hardware needed)
- Foundation for future scalability improvements (sharding)

How the Merge Worked

The Merge was not a simple software update. It required replacing the core consensus mechanism of a live network securing over $200 billion in assets, without any downtime.

The technical approach:

1. **Beacon Chain launch (December 2020)**: A separate PoS chain ran in parallel for nearly two years, allowing validators to stake ETH and the new system to be tested without risking the main network
2. **Shadow forks and testnets**: The Merge was rehearsed on multiple test networks to identify and fix bugs
3. **Terminal Total Difficulty**: A specific cumulative mining difficulty was set as the trigger point. When the PoW chain reached this difficulty, it would stop accepting PoW blocks
4. **The Merge itself**: At the trigger point, the execution layer (transactions, smart contracts) merged with the Beacon Chain's consensus layer (PoS validation)

What changed immediately:

- Block production switched from miners to validators
- Block time became fixed at 12 seconds (previously variable, averaging $\sim$13 seconds)
- New ETH issuance dropped by $\sim$90% (validators require less compensation than miners)
- Energy consumption fell by 99.95%

What did NOT change:

- Transaction fees (still determined by demand for block space)
- Transaction speed (scalability improvements came later, via Layer 2)
- Smart contract functionality
- User experience for holding or transacting ETH

The Stakeholders

The Merge created clear winners and losers:

Winners:

- **ETH holders**: Reduced issuance means less dilution; ESG concerns addressed
- **Stakers**: Can now earn yield (∼3–5% APR) by validating
- **Environmental advocates**: Ethereum removed from climate criticism
- **Liquid staking protocols** (Lido, Rocket Pool): Massive growth in deposits

Losers:

- **Ethereum miners**: Billions of dollars in mining equipment became worthless overnight
- **GPU manufacturers**: Lost a major customer segment
- **Mining pool operators**: Had to pivot or shut down
- **Electricity providers** in mining-heavy regions

A note on the miners: Ethereum miners had invested heavily in hardware and infrastructure. Some attempted to continue mining on a forked "Ethereum PoW" chain, but it failed to gain meaningful adoption. Most mining equipment was sold at steep discounts or repurposed.

New Risks and Trade-offs

The Merge solved some problems but introduced others:

Staking centralisation:

- Lido, a liquid staking protocol, controls ∼30% of all staked ETH
- Combined with Coinbase and other large stakers, a small number of entities control a majority of validation
- If these entities coordinated, they could potentially censor transactions

Regulatory risk:

- The SEC has suggested staking services may be securities
- Centralised staking providers (Coinbase, Kraken) face regulatory pressure
- Some validators have complied with OFAC sanctions by refusing to include certain transactions

Economic security questions:

- PoW security is "external"—attacking requires acquiring hardware and electricity
- PoS security is "internal"—attacking requires acquiring the network's own token
- Critics argue this makes PoS more vulnerable to well-funded attackers who can buy stake

"Rich get richer" concerns:

- Validators earn rewards proportional to their stake
- Large stakers earn more, can compound faster
- Unlike mining, there's no opportunity cost driving hardware obsolescence

The Broader Debate: PoW vs PoS

The Merge reignited a long-standing debate in the cryptocurrency community:

Bitcoin maximalist view (pro-PoW):

- PoW's energy cost IS the security—it's a feature, not a bug
- External costs (electricity) are harder to manipulate than internal costs (stake)
- Bitcoin's simplicity and stability are virtues; Ethereum's complexity is a risk
- "Digital gold" doesn't need to be energy-efficient; it needs to be secure

Ethereum/PoS advocate view:

- PoS achieves equivalent security without environmental damage
- The Merge proves that PoS works at scale on a major network
- PoS enables future scalability improvements not possible with PoW
- Energy criticism was a genuine threat to mainstream adoption

Neither side has definitively "won" this debate. Bitcoin remains on PoW with no plans to change. Ethereum's PoS has operated successfully since September 2022, but hasn't yet been tested by a determined, well-funded attacker.

Key Facts Summary

Item	Detail
Merge date	15 September 2022
Energy reduction	99.95% (from ∼100 TWh/yr to ∼0.01 TWh/yr)
ETH issuance reduction	∼90%
Validator requirement	32 ETH (∼$50–100k depending on price)
Current staking yield	∼3–5% APR
Lido market share	∼30% of staked ETH
Total ETH staked	∼30 million ETH (∼25% of supply)

Questions to Consider

1. The Merge eliminated an entire industry (Ethereum mining). Was this justified by the benefits? How should we think about such transitions?
2. Lido controls ∼30% of staked ETH. Is this a problem? How is it similar to or different from mining pool concentration?
3. Bitcoin advocates argue that PoW's energy cost IS the security. Ethereum advocates argue PoS is more efficient. Who is right?
4. The Merge required years of planning and coordination. What does this say about blockchain governance and the ability to make changes?
5. Some validators now comply with government sanctions (OFAC). Does this undermine Ethereum's censorship resistance? Is censorship resistance even desirable?

Further Reading (Optional)

- Ethereum Foundation: "The Merge" documentation (ethereum.org)
- Vitalik Buterin: "Why Proof of Stake" (2020 blog post)
- Nic Carter: "The Case for Bitcoin's Energy Use" (opposing view)
- Galaxy Digital Research: "Ethereum's Validator Set" (centralisation analysis)

Session Timeline

Time	Activity
0:00–0:08	Context setting: What the Merge was and why it happened
0:08–0:22	Discussion Question 1: Winners and losers
0:22–0:36	Discussion Question 2: PoW vs PoS security
0:36–0:48	Discussion Question 3: Staking centralisation
0:48–0:55	Discussion Question 4: Censorship and regulation
0:55–1:00	Synthesis and key takeaways

Discussion Questions with Guidance

Question 1: Was eliminating Ethereum mining justified?

"The Merge made billions of dollars in mining equipment worthless overnight. Miners who had invested in the ecosystem were wiped out. Was this justified by the environmental and efficiency benefits?"

Points that may emerge:

Arguments that it was justified:

- The environmental benefits are massive and real (99.95% energy reduction)
- Miners knew the Merge was planned—they had years of warning
- The network's long-term health matters more than incumbent interests
- Creative destruction is normal in technology—buggy whip manufacturers also went out of business

Arguments for sympathy with miners:

- Miners provided security and invested based on the system's rules
- The transition was repeatedly delayed, creating uncertainty
- "Ethereum PoW" fork attempt shows some miners felt betrayed
- Precedent concern: If the rules can change once, they can change again

Key insight: Blockchains are social systems, not just technical ones. Changes to the rules create winners and losers. The ability to make such changes demonstrates that "immutability" applies to transaction history, not protocol rules. Governance matters.

Question 2: Is PoW or PoS more secure?

"Bitcoin advocates say PoW's energy cost IS the security—you can't fake having spent real-world resources. Ethereum advocates say PoS achieves the same security more efficiently. Who is right?"

The case for PoW security:

- **External costs**: Attacking requires resources from outside the system (hardware, electricity)
- **Physical constraints**: You can't "print" hashpower; it requires real-world manufacturing and energy
- **Battle-tested**: Bitcoin has operated for 15+ years without a successful attack on consensus
- **Simplicity**: Fewer attack vectors, easier to reason about

The case for PoS security:

- **Slashing**: Attackers lose their stake—they can't just walk away with equipment
- **Cost equivalence**: Acquiring 51% of stake is comparably expensive to 51% of hashpower
- **No external market**: You can't rent stake the way you can rent hashpower
- **Recovery possible**: A PoS network can slash attackers and recover; PoW attacks are harder to punish

Unresolved questions:

- PoS hasn't been tested by a well-funded nation-state adversary
- Long-range attacks and "nothing at stake" are theoretical concerns not yet exploited
- The "true" security comparison may not be knowable until an attack is attempted

Key insight: This is a genuine debate without a definitive answer. Both mechanisms provide security through different means. PoW makes attacks expensive through energy; PoS makes attacks expensive through capital at risk. The right choice may depend on threat models and values.

Question 3: Is staking centralisation a problem?

"Lido controls ∼30% of staked ETH. Combined with Coinbase and a few other large stakers, a small number of entities control most validation. Is this a problem? How does it compare to mining pool concentration?"

Why it might be a problem:

- Coordinated validators could censor transactions
- Regulatory pressure on large stakers could force compliance (already happening with OFAC)
- "Decentralisation" was the whole point; this looks like re-centralisation
- Liquid staking creates governance concentration (Lido token holders control protocol decisions)

Why it might be overstated:

- Lido uses dozens of independent node operators, not a single validator
- Users can withdraw from Lido if it misbehaves (unlike mining pools, stake is more liquid)
- Mining pools also had concentration; top 4 Bitcoin pools control ∼70% of hashrate
- Protocol-level solutions are being discussed (e.g., caps on any single entity's share)

Comparison to mining pools:

- Mining pools: Miners can switch pools instantly; pool operators don't own the hardware
- Staking pools: Withdrawals take time; liquid staking tokens add intermediation
- Both face concentration pressure from economies of scale
- Neither achieves the "one CPU, one vote" ideal from Bitcoin's whitepaper

Key insight: Centralisation pressure exists in both PoW and PoS. The mechanisms differ, but the outcome is similar: a relatively small number of entities control most block production. "Decentralisation" is a spectrum, not a binary.

Question 4: Does OFAC compliance undermine censorship resistance?

"Some Ethereum validators now comply with US Treasury sanctions (OFAC) by refusing to include transactions from sanctioned addresses. Does this undermine Ethereum's censorship resistance? Is censorship resistance even a good thing?"

The censorship resistance view:

- Censorship resistance is a core blockchain value proposition
- If validators can exclude transactions, what's the point of decentralisation?
- Today it's OFAC; tomorrow it could be political dissidents
- This is a slippery slope toward permissioned networks

The compliance view:

- Validators are businesses operating in jurisdictions with laws
- OFAC sanctions target terrorist financing and sanctions evasion—legitimate goals
- Non-compliant validators still exist; transactions eventually get included
- Mainstream adoption may require some accommodation of legal systems

The nuanced middle:

- Currently, OFAC-compliant validators slow but don't stop sanctioned transactions
- The network as a whole remains censorship-resistant even if individual validators comply

- But: If compliance becomes mandatory or dominant, this could change
- The Tornado Cash sanctions show regulators are willing to target DeFi directly

Key insight: Censorship resistance exists on a spectrum. Individual validators may comply with local laws; the question is whether enough non-compliant validators exist to ensure eventual inclusion. This is an active tension with no clear resolution.

Extension Question (if time permits)

"The Merge required years of coordination and planning. Ethereum has a clear leadership (Vitalik Buterin, Ethereum Foundation). Bitcoin has no such central coordination. Is Ethereum's ability to make changes a strength or a weakness?"

This connects to blockchain governance. Ethereum can evolve but depends on coordination around influential figures. Bitcoin is more resistant to change but also more resistant to improvement. Different values lead to different conclusions.

End of Tutorial 2 Materials