BITCOIN ACADEMY

● INTERMEDIATE

Going Deeper

Understand the mechanics under the hood — mining, consensus, network economics, and the Lightning Network.

---

7 Modules | ~4 Hours | Course Module 02
bitcoinacademy.online

Contents

MODULE 01

Proof of Work & Mining Economics

Mining is the process that secures Bitcoin and issues new coins. But it's far more than "solving puzzles" — it's an **economic system** that converts real-world energy into digital security.

Here's how it actually works: miners collect pending transactions from the mempool and assemble them into a candidate block. They then repeatedly hash the block header with different nonce values (random numbers), searching for a hash output below a target threshold. This is pure brute-force computation — there's no shortcut.

The first miner to find a valid hash broadcasts their block to the network. Every other node independently verifies it's valid (correct transactions, valid hash, follows all consensus rules), then adds it to their chain. The winning miner receives the block reward (currently 3.125 BTC) plus all transaction fees in the block.

KEY INSIGHT — THE ECONOMICS

Mining is a business. Miners invest in hardware (ASICs costing $2,000–$15,000+), pay for electricity (the largest ongoing cost), and compete globally. The difficulty adjustment ensures that no matter how much computing power joins the network, blocks are found roughly every 10 minutes. More miners = higher difficulty = higher cost to mine. This creates a natural equilibrium: miners only participate when it's profitable, and the most efficient operations survive.

The difficulty adjustment is one of Bitcoin's most elegant mechanisms. Every 2,016 blocks (~2 weeks), the protocol measures how fast blocks were found. If blocks came too fast, difficulty increases. Too slow? It decreases. This self-regulating feedback loop has maintained ~10-minute blocks for over 15 years regardless of hash power changes.

HASH RATE CONTEXT

Bitcoin's hash rate has grown from essentially zero in 2009 to over 700 exahashes per second (EH/s) — that's 700 quintillion hashes per second. This staggering computation makes Bitcoin the most secure computing network ever created. To attack it, you'd need to outpace the combined output of every miner on Earth, simultaneously.

MODULE 02

The Halving Cycle & Supply Dynamics

Every 210,000 blocks (roughly 4 years), the Bitcoin block reward is cut in half. This event, called the **halving**, is the mechanism that controls Bitcoin's monetary inflation rate and ensures its supply approaches — but never reaches — 21 million.

Halving	Year	Block Reward	Daily New BTC	Inflation
Genesis	2009	50 BTC	~7,200	N/A
1st Halving	2012	25 BTC	~3,600	~8.4%
2nd Halving	2016	12.5 BTC	~1,800	~4.2%
3rd Halving	2020	6.25 BTC	~900	~1.8%
4th Halving	2024	3.125 BTC	~450	~0.85%

After each halving, the rate of new supply entering the market is drastically reduced. Meanwhile, demand operates independently — driven by adoption, institutional interest, and macroeconomic conditions. When supply growth shrinks while demand remains constant or grows, basic economics suggests upward price pressure.

KEY INSIGHT — STOCK-TO-FLOW

Bitcoin's "stock-to-flow" ratio — the relationship between existing supply (stock) and annual new production (flow) — surpassed gold's after the 2024 halving. This means Bitcoin is now harder to produce, relative to existing supply, than gold. By the next halving in ~2028, it will be harder still. This increasing scarcity is unique among monetary assets.

IMPORTANT NUANCE

While all four halvings have historically preceded significant price increases, correlation is not causation. Markets are forward-looking, and halvings are predictable events. Some argue the supply shock is already "priced in." Others argue the sustained reduction in sell pressure creates genuine supply squeezes. Never invest based on halving cycles alone.

MODULE 03

On-Chain Analysis Fundamentals

Because Bitcoin's ledger is fully public, anyone can analyse the movement of every coin in existence. This field — **on-chain analysis** — provides insights that are impossible with traditional assets. It's like being able to see every transaction in every bank account, in real time.

UTXO Age Distribution: This shows how long coins have been sitting unmoved. When a large percentage of supply hasn't moved in 1+ years, it suggests holders are accumulating (bullish signal). When old coins suddenly start moving, it may indicate long-term holders are taking profits.

Exchange Flows: Coins moving to exchanges typically signal intent to sell. Coins moving off exchanges signal accumulation and self-custody. Net exchange outflows have historically correlated with price appreciation.

Realised Price: The average price at which every Bitcoin last moved on-chain. This gives a "cost basis" for the entire network. When the market price is above the realised price, the average holder is in profit. When below, the average holder is underwater.

MVRV Ratio: Market Value to Realised Value. When this ratio is extremely high (>3), the market may be overheated. When it dips below 1, Bitcoin is historically undervalued relative to aggregate cost basis.

PRACTICAL APPLICATION

On-chain analysis doesn't predict the future, but it reveals the behaviour of market participants with mathematical certainty. Unlike traditional market analysis which relies on price and volume alone, on-chain data shows you what long-term holders, miners, and whales are actually doing with their coins — not what they say they're doing.

Miner behaviour is especially informative. When miners accumulate (hold their newly minted coins), it suggests they expect higher prices. When they rapidly sell, they may be covering costs or de-risking. Miner reserve data is publicly trackable.

FREE ON-CHAIN TOOLS

You can explore on-chain data for free using platforms like Glassnode (limited free tier), Blockchain.com's explorer, Mempool.space (for real-time mempool and fee data), and Clark Moody's Bitcoin Dashboard for a comprehensive live overview of network statistics.

MODULE 04

Lightning Network Deep Dive

Bitcoin's base layer processes ~7 transactions per second. Visa handles ~24,000. This is not a bug — Bitcoin's base layer prioritises **security and decentralisation** over speed. The Lightning Network is how Bitcoin scales without compromising those properties.

Lightning works by creating **payment channels** between two parties. Once a channel is open (via a single on-chain transaction), those parties can transact thousands of times between themselves — instantly and with near-zero fees — without touching the main blockchain. When they're done, a single closing transaction settles the final balances on-chain.

The genius is in **routing**: you don't need a direct channel with everyone. If Alice has a channel with Bob, and Bob has a channel with Carol, Alice can pay Carol through Bob — automatically and trustlessly. The network finds optimal routes in milliseconds.

REAL-WORLD IMPACT

Lightning enables Bitcoin for everyday purchases — coffee, groceries, ride-sharing. El Salvador's Chivo wallet uses Lightning for its national Bitcoin infrastructure. Strike uses it for cross-border remittances at nearly zero cost. Apps like Wallet of Satoshi and Phoenix make Lightning accessible to anyone with a smartphone. The network now has over 15,000 nodes and growing capacity.

TRADE-OFFS

Lightning is not perfect. It requires recipients to be online, channels need liquidity management, and routing large payments can be challenging. It's best suited for small-to-medium everyday payments, while the base layer handles large settlements and long-term storage. Think of Lightning as Bitcoin's "checking account" and the base layer as its "vault."

MODULE 05

Bitcoin vs Altcoins: A Framework

There are over 20,000 cryptocurrencies. How do you evaluate them? Rather than comparing individual projects, let's build a **framework** for thinking about what makes Bitcoin fundamentally different from everything else.

1. True Decentralisation: Bitcoin has no CEO, no foundation with controlling power, no pre-mine, and no venture capital investors who got special allocations. Satoshi disappeared. No one can change Bitcoin's rules unilaterally. Most altcoins have identifiable founders, foundations, or companies with outsized influence.

2. Immaculate Conception: Bitcoin launched with no pre-mine, no ICO, no venture funding, and no insider allocation. Satoshi mined alongside everyone else using basic hardware. This "fair launch" has never been replicated — every subsequent project has had some form of insider advantage.

3. Monetary Policy Credibility: Bitcoin's 21 million supply cap has never been changed. Ethereum has changed its monetary policy multiple times. Many altcoins have inflationary schedules controlled by small teams. The credibility of a monetary policy is proportional to its resistance to change.

4. The Lindy Effect: Bitcoin has been running since 2009 without a single minute of downtime or a successful attack on its base protocol. The longer a system survives, the longer it's likely to continue surviving. No other cryptocurrency has this track record.

THE NETWORK EFFECT

Bitcoin's value isn't just technical — it's sociological. It has the most miners (security), the most nodes (decentralisation), the most liquidity (market depth), the most regulatory clarity, and the most brand recognition. These network effects compound over time. Technology alone doesn't win — adoption does.

BALANCED PERSPECTIVE

This isn't to say all altcoins are worthless — some explore genuine innovations in smart contracts, privacy, or scalability. But applying this framework helps separate signal from noise. Ask: who controls it, how was it launched, can the rules change, and how long has it survived?

MODULE 06

Self-Custody & Hardware Wallets

Self-custody means holding your own private keys, rather than trusting a third party (exchange, bank, or custodian) to hold them for you. When you self-custody, your Bitcoin exists as a mathematical relationship between your private key and the blockchain. No one can freeze it, seize it, or deny you access — as long as you have your keys.

Feature	Exchange	Software Wallet	Hardware Wallet
Who holds keys?	The exchange	You (on device)	You (secure chip)
Internet exposure	Always online	When app open	Keys never online
Hack risk	High (target)	Medium (malware)	Very low (air-gapped)
Counterparty risk	High	None	None
Best for	Active trading	Small daily use	Savings & long-term

ADVANCED: MULTI-SIGNATURE

For larger holdings, consider a multi-signature (multisig) setup — requiring 2-of-3 or 3-of-5 keys to authorise a transaction. This means no single key compromise can steal your funds. Services like Unchained Capital, Casa, and Nunchuk offer guided multisig setups that balance security with usability.

THE FTX LESSON

In November 2022, the FTX exchange — once valued at $32 billion — collapsed overnight. Millions of customers lost access to billions of dollars worth of crypto. The founder was later convicted of fraud. Every user who had self-custodied was completely unaffected. This is why "not your keys, not your coins" exists.

MODULE 07

Reading the Mempool & Fee Markets

The **mempool** (memory pool) is Bitcoin's waiting room — the collection of all valid transactions that have been broadcast to the network but haven't yet been included in a block. Understanding the mempool is essential for timing transactions and managing fees intelligently.

When you send Bitcoin, you attach a fee measured in **satoshis per virtual byte (sat/vB)**. Miners are economically rational — they include the highest-fee transactions first. Your transaction's position in the queue depends entirely on what fee you offer relative to everyone else.

When to send: The mempool fluctuates dramatically. During weekends and late nights (UTC), it's often nearly empty — you can send transactions for 1–3 sat/vB. During hype events, NFT mints, or heavy trading periods, fees can spike to 200+ sat/vB. Patience saves money.

PRO TIPS

Mempool.space is the best free tool for visualising the mempool in real-time — it shows pending transaction volume, fee estimates, and block predictions. Use it before every transaction. Many wallets also support RBF (Replace-By-Fee), which lets you bump a stuck transaction's fee if it's taking too long. Always enable RBF when available.

The Long-Term Fee Market: As block rewards halve every 4 years and eventually approach zero (around 2140), transaction fees will become the primary incentive for miners. This means Bitcoin's long-term security depends on a robust fee market.

UTXO MANAGEMENT

Advanced users practise "UTXO consolidation" — combining many small UTXOs into fewer large ones during low-fee periods. This is like exchanging a jar of coins for notes. Spending many small UTXOs in a single transaction is expensive because each input adds to the transaction size. Consolidating when fees are low saves significant money when fees spike later.

Congratulations!

You've completed Course Module 02 — Going Deeper. You now have a solid understanding of Bitcoin's mechanics, economics, and infrastructure.

Head to the website to take the interactive quiz. Score 70% or higher to earn your official Bitcoin Academy Intermediate Certificate — print it, frame it, put it on the wall.

Take the Quiz

Earn Your Certificate

You've completed the Going Deeper course material.

Now test your knowledge and earn your official Bitcoin Academy certificate.

Step 1 — Visit the link below

Step 2 — Scroll to the Final Quiz section

Step 3 — Score 70% or higher to pass

Step 4 — Enter your name and print your certificate

Your quiz is waiting at:

bitcoinacademy.online/course-intermediate.html

Frame your certificate. Put it on the wall.
You've earned it.