How to Really Mine Bitcoin

A comprehensive guide to Bitcoin mining — theory, practice, and economics

Prof. Dr. Jörg Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

Learning Objectives

By the end of this lecture, you will be able to:

1. Describe the complete mining workflow from hardware purchase to payout [Understand]
2. Calculate whether mining is profitable given your electricity cost and hardware specs [Apply]
3. Explain the protocol mechanics: target, difficulty, nonce search, and block time distribution [Understand]
4. Analyze the energy footprint of mining and evaluate security game-theory trade-offs [Analyze]
5. Compare pool payout methods and select the right pool for your operation [Analyze]

No prerequisites beyond basic blockchain awareness (what blocks and transactions are).

Bloom's levels covered: Understand, Apply, Analyze

This is a practical "how-to" guide — for the theory behind Proof of Work, see Lesson 7

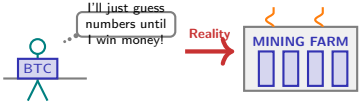
What Problem Does Mining Solve?

Bitcoin needs someone to:

- **Validate** transactions (no double-spending)
- **Order** them into blocks
- **Secure** the chain against tampering

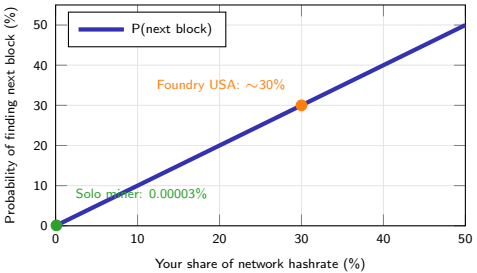
Mining is that job. Miners compete to add the next block and earn a reward. But in 2026, it is an **industrial operation**, not a laptop hobby.

This lecture: How to actually do it — step by step.



Mining creates new bitcoins AND validates every transaction — it is the backbone of Bitcoin security

The Mining Lottery: Why More Hashpower = More Chances

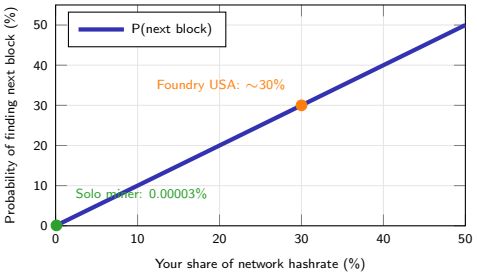


The analogy:

Imagine 1 million people rolling dice every second. The first to roll below a target wins.

- More dice = more chances per second
- But **no guarantee** — it is still a lottery

The Mining Lottery: Why More Hashpower = More Chances

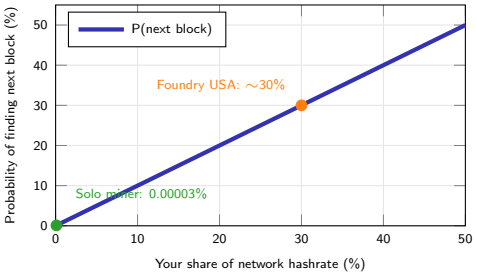


The analogy:

Imagine 1 million people rolling dice every second. The first to roll below a target wins.

- More dice = more chances per second
- But **no guarantee** — it is still a lottery
- One solo ASIC: ∼0.00003% of the network

The Mining Lottery: Why More Hashpower = More Chances



The analogy:

Imagine 1 million people rolling dice every second. The first to roll below a target wins.

- More dice = more chances per second
- But **no guarantee** — it is still a lottery
- One solo ASIC: ∼0.00003% of the network
- Foundry pool: ∼30% of the network

Key Insight

Mining is a **fair lottery**: your probability of winning equals your share of total hashpower.

This is why solo mining is practically hopeless — and why mining pools exist

Six Terms Every Miner Must Know

1. Hash
A digital fingerprint — feed in any data, get a fixed-length output. Bitcoin uses SHA-256 (Secure Hash Algorithm, 256-bit output).

2. Nonce
"Number used once" — the value miners change on each attempt, trying to get a hash below the target.

3. Block Header
An 80-byte structure containing 6 fields. This is what miners actually hash.

4. Target
A very large number. Your hash must be *below* this value to count as valid. The lower the target, the harder mining becomes.

5. Difficulty
Controls how small the target is. Adjusts every 2,016 blocks ($\sim$2 weeks) to keep block time at $\sim$10 minutes.

6. Hashrate
Guesses per second. Modern ASICs (Application-Specific Integrated Circuits) achieve 200+ TH/s (terahashes per second = 200 trillion guesses/s).

Master these six terms and the rest of the lecture will make sense

Block Reward Schedule: The Halving Clock

Halving formula:

$$\text{reward(era)} = \frac{50}{2^{\text{era}}} \text{ BTC}$$

Equivalently in satoshis:

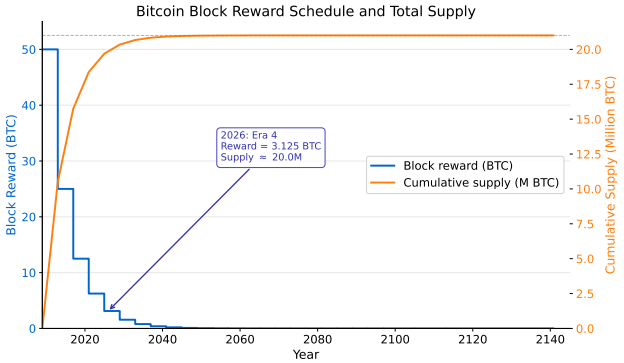
$$\text{sats} = 5{,}000{,}000{,}000 \gg \text{era}$$

Current era 4 (2024–2028): **3.125 BTC**

Supply cap:
Geometric series converges to exactly **21 million BTC** — hard-coded scarcity.

Implication for Miners

Each halving cuts miner revenue in half overnight. Transaction fees must eventually replace block rewards.



The next halving is expected around April 2028 — block reward will drop to 1.5625 BTC

Target and Difficulty: The Inverse Relationship

Target formula:

$$\text{target} = \frac{\texttt{0xFFFF} \times 2^{208}}{D}$$

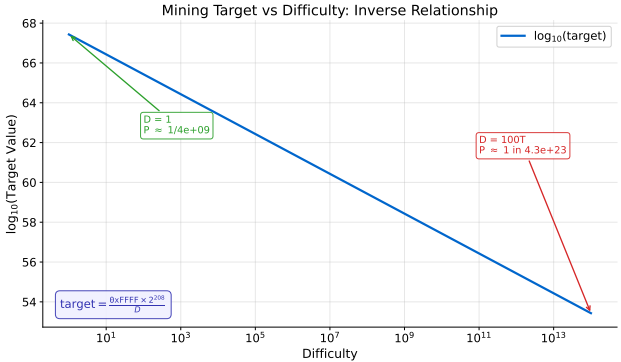
where D is the difficulty parameter.

Key insight:
Higher $D \rightarrow$ lower target $\rightarrow$ fewer valid hashes $\rightarrow$ harder to mine.

Probability of a single hash winning:

$$P = \frac{\text{target}}{2^{256}} \approx \frac{1}{D \times 2^{48}/\texttt{0xFFFF}}$$

At $D \approx 110\text{T}$, the target is a 256-bit number with $\sim$79 leading zeros.



The difficulty parameter D compresses the enormous target space into a single human-readable number

The Hash Race: How Many Guesses to Win?

Expected hashes to find a block:

$$E[\text{hashes}] = \frac{D \times 2^{48}}{\texttt{0xFFFF}}$$

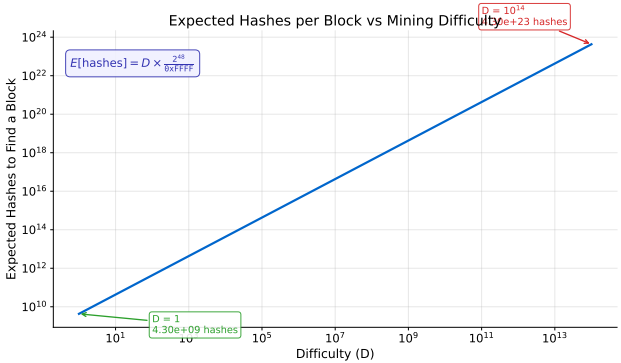
At current $D \approx 110\text{T}$:

$$E \approx 4.2 \times 10^{23} \text{ hashes}$$

What this means:
The entire network (700 EH/s) collectively performs $\sim 4.2 \times 10^{23}$ hashes every 10 minutes.

A single S21 at 200 TH/s contributes:

$$\frac{200 \times 10^{12}}{700 \times 10^{18}} = 0.000029\%$$



Expected hashes scale linearly with difficulty — when D doubles, the work to find a block doubles

Nonce Search: Finding a Needle in a Haystack

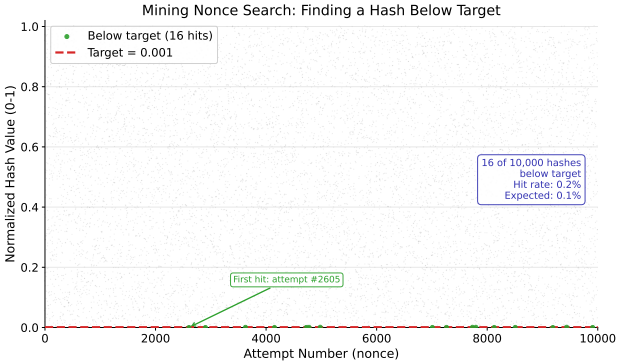
What the miner does:
Try nonce 0, 1, 2, ... and hash each time. If the hash value falls *below* the target line, you win.

Visualization:
Each dot is one hash attempt plotted by its numeric value. The green dots (below target) are valid blocks — but they are extremely rare.

Key property:
SHA-256 output is *uniformly random* — no pattern, no shortcut, no way to predict which nonce will produce a low hash.

Brute Force

There is no strategy — only raw speed. This is why mining is a "lottery."



SHA-256 is designed so that output looks random — each nonce is an independent trial with equal probability

Block Time Distribution: Why 10 Minutes Is Only an Average

Exponential distribution:

$$f(t) = \lambda e^{-\lambda t}, \quad \lambda = \frac{1}{600\text{s}}$$

Properties:

- Mean: 10 minutes
- Median: 6.93 minutes (most blocks are *faster*)

Block Time Distribution: Why 10 Minutes Is Only an Average

Exponential distribution:

$$f(t) = \lambda e^{-\lambda t}, \quad \lambda = \frac{1}{600\text{s}}$$

Properties:

- Mean: 10 minutes
- Median: 6.93 minutes (most blocks are *faster*)
- P(block $>$ 20 min) $= 13.5\%$

Block Time Distribution: Why 10 Minutes Is Only an Average

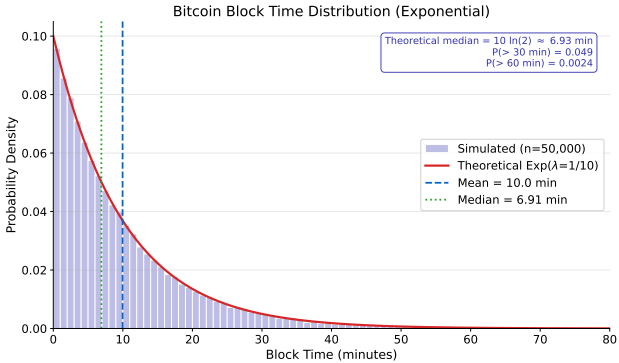
Exponential distribution:

$$f(t) = \lambda e^{-\lambda t}, \quad \lambda = \frac{1}{600\text{s}}$$

Properties:

- Mean: 10 minutes
- Median: 6.93 minutes (most blocks are *faster*)
- P(block $>$ 20 min) $= 13.5\%$
- P(block $>$ 60 min) $= 0.25\%$

Memoryless property:
If 15 minutes have passed, the expected remaining wait is still 10 minutes — past time does not help.



The exponential distribution is the continuous analog of the geometric distribution (each hash is a Bernoulli trial)

The Mining Algorithm in Seven Steps

Building the candidate block:

Step 1: Collect unconfirmed transactions from the mempool.

Step 2: Select by fee priority — maximize revenue per byte.

Step 3: Hash transactions pairwise into a Merkle tree; the root summarizes all transactions.

Step 4: Construct the 80-byte block header: previous hash + Merkle root + timestamp + target + nonce (starts at 0).

The hash race:

Step 5: Apply double SHA-256 to the header.

Step 6: Hash $<$ target? **Yes** $\rightarrow$ valid block! **No** $\rightarrow$ increment nonce, repeat.

Step 7: Broadcast block, collect **3.125 BTC** reward + fees.

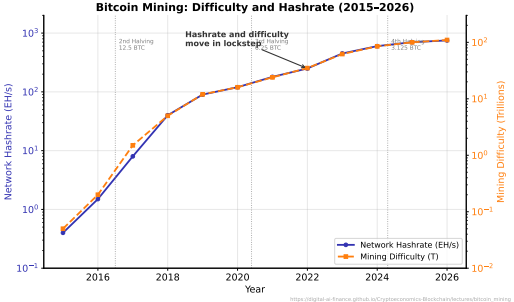
Worked Example

200 TH/s exhausts 2^{32} nonces (4.3B values) in $\sim$22 μs. After that, change the coinbase transaction to get a new Merkle root — the "extra nonce" technique.

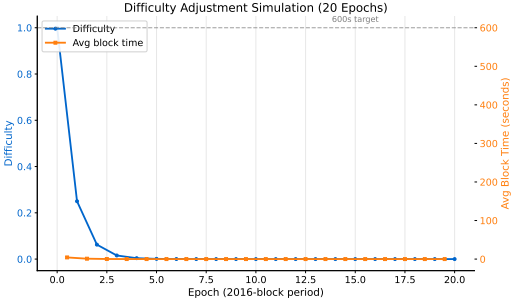
Steps 1–4 take milliseconds; the competitive lottery in Steps 5–7 takes $\sim$75 years on a single ASIC

Difficulty Adjusts to Keep Blocks at 10 Minutes

Every 2,016 blocks (∼2 weeks), difficulty D adjusts: $D_{\text{new}} = D_{\text{old}} \times \frac{20{,}160 \text{ min}}{\text{actual time}}$. If blocks came too fast, D rises; too slow, D falls.



Historical: hashrate and difficulty track each other in lockstep.



Simulation: difficulty chases hashrate across 20 adjustment epochs.

This self-regulating mechanism is why Bitcoin blocks average ∼10 minutes regardless of total hashpower

Shopping for an ASIC: A Buyer's Checklist

Key metrics to compare:

1. **Efficiency (J/TH)** — joules per terahash. *Lower is better.* This is the #1 metric.
2. **Hashrate (TH/s)** — raw speed

Shopping for an ASIC: A Buyer's Checklist

Key metrics to compare:

1. **Efficiency (J/TH)** — joules per terahash. *Lower is better.* This is the #1 metric.
2. **Hashrate (TH/s)** — raw speed
3. **Purchase price ($)** — upfront cost

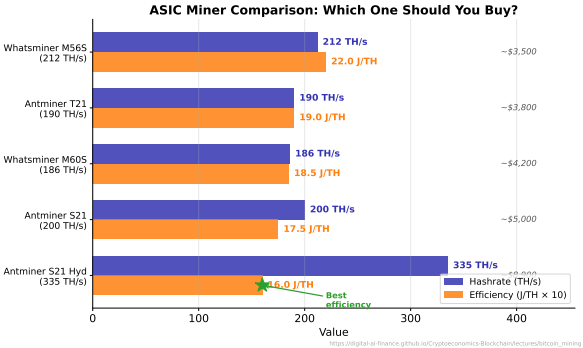
Shopping for an ASIC: A Buyer's Checklist

Key metrics to compare:

1. **Efficiency (J/TH)** — joules per terahash. *Lower is better.* This is the #1 metric.
2. **Hashrate (TH/s)** — raw speed
3. **Purchase price ($)** — upfront cost
4. **Noise (dB)** — 70–80 dB typical

Rule of Thumb

Efficiency (J/TH) matters more than raw hashrate. A 200 TH/s machine at 17 J/TH beats a 300 TH/s machine at 25 J/TH.



Check asicminervalue.com for current prices and specs — they change monthly

What's Inside the Block Header?

The block header is exactly **80 bytes** — this is the only thing miners hash.

Field	Size	What It Contains	Can Miner Change?
Version	4 bytes	Protocol version number	No
Previous Block Hash	32 bytes	Hash of the last confirmed block	No
Merkle Root	32 bytes	Summary hash of all transactions	Indirectly (via coinbase)
Timestamp	4 bytes	Current time (seconds since epoch)	Slightly (± 2 hours)
Difficulty Target (nBits)	4 bytes	Encoded target value	No
Nonce	**4 bytes**	**Counter (0 to 4,294,967,295)**	**Yes — this is the knob**

Key insight: Only the nonce and timestamp can be freely changed. When all 4 billion nonce values are exhausted (in $\sim 22\,\mu$s on modern hardware), miners modify the coinbase transaction to generate a new Merkle root — the "extra nonce" technique.

The block header is tiny (80 bytes) but hashing it trillions of times per second is what makes mining hard

Setting Up Your Mining Rig

Physical setup checklist — what you need before powering on:

1. Power supply
Dedicated 240V circuit, 20A minimum. Most ASICs draw 3,000–3,500W. A standard home outlet (120V/15A) is *not* enough.

2. Cooling
ASICs produce ∼12,000 BTU/hr of heat. You need a dedicated room or garage with intake + exhaust fans. Summer heat kills performance.

3. Internet
Stable connection required, but bandwidth is minimal (∼10 KB/s per miner). Wi-Fi works but Ethernet is more reliable.

4. Noise isolation
Industrial ASICs run at 70–80 dB (vacuum cleaner level). *Not suitable for living spaces.* Garage, basement, or warehouse recommended.

5. Unboxing and connection

- Connect power supply unit (PSU)
- Plug in Ethernet cable

Setting Up Your Mining Rig

Physical setup checklist — what you need before powering on:

1. Power supply
Dedicated 240V circuit, 20A minimum. Most ASICs draw 3,000–3,500W. A standard home outlet (120V/15A) is *not* enough.

2. Cooling
ASICs produce ∼12,000 BTU/hr of heat. You need a dedicated room or garage with intake + exhaust fans. Summer heat kills performance.

3. Internet
Stable connection required, but bandwidth is minimal (∼10 KB/s per miner). Wi-Fi works but Ethernet is more reliable.

4. Noise isolation
Industrial ASICs run at 70–80 dB (vacuum cleaner level). *Not suitable for living spaces.* Garage, basement, or warehouse recommended.

5. Unboxing and connection

- Connect power supply unit (PSU)
- Plug in Ethernet cable
- Power on

Setting Up Your Mining Rig

Physical setup checklist — what you need before powering on:

1. Power supply
Dedicated 240V circuit, 20A minimum. Most ASICs draw 3,000–3,500W. A standard home outlet (120V/15A) is *not* enough.

2. Cooling
ASICs produce ∼12,000 BTU/hr of heat. You need a dedicated room or garage with intake + exhaust fans. Summer heat kills performance.

3. Internet
Stable connection required, but bandwidth is minimal (∼10 KB/s per miner). Wi-Fi works but Ethernet is more reliable.

4. Noise isolation
Industrial ASICs run at 70–80 dB (vacuum cleaner level). *Not suitable for living spaces.* Garage, basement, or warehouse recommended.

5. Unboxing and connection

- Connect power supply unit (PSU)
- Plug in Ethernet cable
- Power on
- Access ASIC web interface via local IP address (e.g., 192.168.1.xxx)

The physical setup is often underestimated — power and cooling are bigger challenges than software

Cooling Your Miners: BTU, CFM, and Heat Management

All electrical power becomes heat.

BTU/hr formula:

$$\text{BTU/hr} = \text{Watts} \times 3.412$$

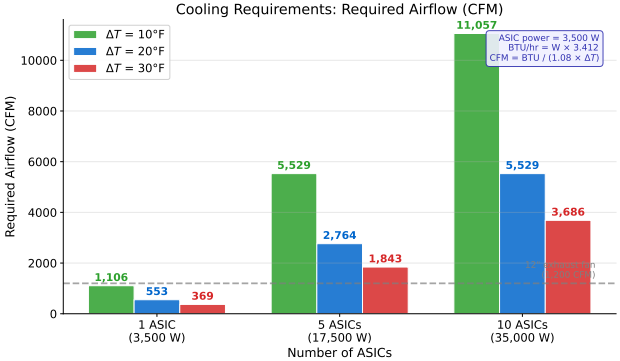
A 3,500W ASIC emits ∼11,940 BTU/hr.

CFM (airflow) needed:

$$\text{CFM} = \frac{\text{BTU/hr}}{1.08 \times \Delta T}$$

With $\Delta T = 20\,^{\circ}\text{F}$: need ∼553 CFM per ASIC.

Rule of thumb:
One industrial exhaust fan (∼1,000 CFM) covers 1–2 ASICs. Five ASICs need dedicated HVAC.



Underestimating cooling is the #1 physical setup mistake — it directly impacts hashrate and hardware lifespan

Installing and Configuring Mining Software

Software options:

- **Built-in firmware** — most modern ASICs ship with a web interface. You configure via browser.
- **Braiins OS+** — open-source firmware with auto-tuning (optimizes hashrate per watt)

Installing and Configuring Mining Software

Software options:

- **Built-in firmware** — most modern ASICs ship with a web interface. You configure via browser.
- **Braiins OS+** — open-source firmware with auto-tuning (optimizes hashrate per watt)
- **CGMiner** — command-line classic (advanced users)

Installing and Configuring Mining Software

Software options:

- **Built-in firmware** — most modern ASICs ship with a web interface. You configure via browser.
- **Braiins OS+** — open-source firmware with auto-tuning (optimizes hashrate per watt)
- **CGMiner** — command-line classic (advanced users)
- **NiceHash** — beginner-friendly GUI (sells your hashpower to highest bidder)

What you type in:

Three configuration fields in every miner:

1. **Pool URL:**
   `stratum+tcp://us.foundryusa.com:3333`
2. **Worker name:**
   `myrig.worker1`
3. **Wallet address:**
   Your Bitcoin address for payouts

Test: After saving, hashrate should appear on the pool dashboard within 60 seconds.

Most ASICs come pre-loaded with firmware — you often just need to enter pool URL and wallet address

Mining Pools: Why Solo Is Not an Option

Pool registration walkthrough:

1. Go to pool website (e.g., foundrydigital.com)
2. Create account with email

Mining Pools: Why Solo Is Not an Option

Pool registration walkthrough:

1. Go to pool website (e.g., foundrydigital.com)
2. Create account with email
3. Set your **payout address** (your Bitcoin wallet)

Mining Pools: Why Solo Is Not an Option

Pool registration walkthrough:

1. Go to pool website (e.g., foundrydigital.com)
2. Create account with email
3. Set your **payout address** (your Bitcoin wallet)
4. Choose payout method:

Mining Pools: Why Solo Is Not an Option

Pool registration walkthrough:

1. Go to pool website (e.g., foundrydigital.com)
2. Create account with email
3. Set your **payout address** (your Bitcoin wallet)
4. Choose payout method:
   - **FPPS** — steady income, pool absorbs variance

Mining Pools: Why Solo Is Not an Option

Pool registration walkthrough:

1. Go to pool website (e.g., foundrydigital.com)
2. Create account with email
3. Set your **payout address** (your Bitcoin wallet)
4. Choose payout method:
   - **FPPS** — steady income, pool absorbs variance
   - **PPLNS** — higher average, more variance

Mining Pools: Why Solo Is Not an Option

Pool registration walkthrough:

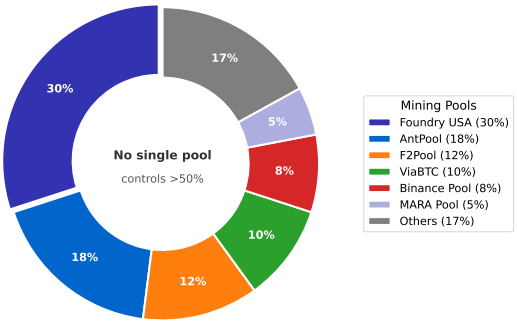
1. Go to pool website (e.g., foundrydigital.com)
2. Create account with email
3. Set your **payout address** (your Bitcoin wallet)
4. Choose payout method:
   - **FPPS** — steady income, pool absorbs variance
   - **PPLNS** — higher average, more variance
5. Copy pool URL + port

Mining Pools: Why Solo Is Not an Option

Pool registration walkthrough:

1. Go to pool website (e.g., foundrydigital.com)
2. Create account with email
3. Set your **payout address** (your Bitcoin wallet)
4. Choose payout method:
   - **FPPS** — steady income, pool absorbs variance
   - **PPLNS** — higher average, more variance
5. Copy pool URL + port
6. Enter in ASIC configuration

Bitcoin Mining Pool Distribution (2025–2026)



https://digital-ai-finance.github.io/Cryptoeconomics-Blockchain/lectures/bitcoin_mining

Why Foundry? Largest US-based pool (∼30% of hashrate), transparent fees, institutional-grade infrastructure.

FPPS is recommended for beginners — predictable daily payouts regardless of pool luck

Solo Mining: A Statistical Reality Check

How unlikely is solo mining?

With one S21 (200 TH/s) against the full network (700 EH/s):

$$P(\text{block in 1 year}) \approx 0.015$$

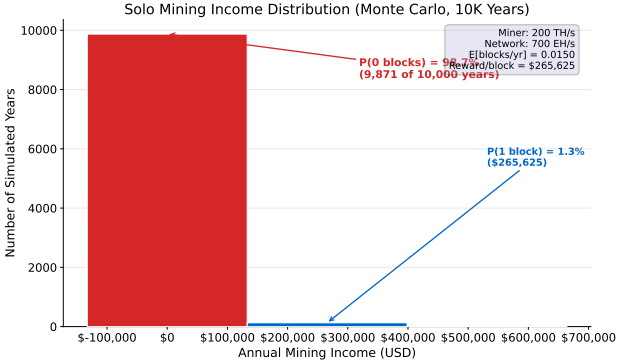
Monte Carlo simulation of 10,000 years:

- **98.5%** of years: earn **$**0
- **1.5%** of years: hit a block (∼**$**265K)

Expected value is the same as pooled mining, but the **variance** is catastrophic.

Analogy

Solo mining = buying one lottery ticket per year. Pooled mining = sharing a syndicate ticket every day.



Solo mining is mathematically fair but practically hopeless — pools exist to make income predictable

Pool Size and Income Variance

Pools do not increase expected income — they reduce *variance*.

How it works:

- Pool combines hashrate of thousands of miners
- When the pool finds a block, reward is split proportionally
- Your daily income becomes predictable

Variance by pool size:

- Solo: coefficient of variation $\gg 100\%$
- 0.1% pool: still high variance

Pool Size and Income Variance

Pools do not increase expected income — they reduce *variance*.

How it works:

- Pool combines hashrate of thousands of miners
- When the pool finds a block, reward is split proportionally
- Your daily income becomes predictable

Variance by pool size:

- Solo: coefficient of variation $\gg 100\%$
- 0.1% pool: still high variance
- 1% pool: smoothed weekly income

Pool Size and Income Variance

Pools do not increase expected income — they reduce *variance*.

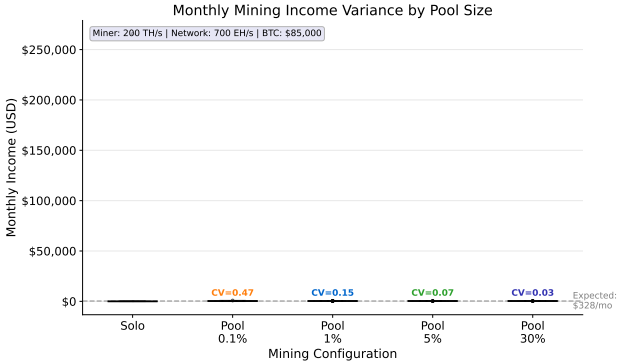
How it works:

- Pool combines hashrate of thousands of miners
- When the pool finds a block, reward is split proportionally
- Your daily income becomes predictable

Variance by pool size:

- Solo: coefficient of variation $\gg 100\%$
- 0.1% pool: still high variance
- 1% pool: smoothed weekly income
- 30% pool: near-constant daily payout

Larger pool = smoother income = faster ROI confidence.



Pool size matters for income stability but not expected returns — the law of large numbers does the work

FPPS vs PPLNS: Choosing Your Payout Method

FPPS (Full Pay Per Share):

- Pool pays you for every valid share
- Pool absorbs luck variance

FPPS vs PPLNS: Choosing Your Payout Method

FPPS (Full Pay Per Share):

- Pool pays you for every valid share
- Pool absorbs luck variance
- Steady daily income

FPPS vs PPLNS: Choosing Your Payout Method

FPPS (Full Pay Per Share):

- Pool pays you for every valid share
- Pool absorbs luck variance
- Steady daily income
- Pool charges higher fee ($\sim$2–3%)

PPLNS (Pay Per Last N Shares):

- Paid only when pool finds a block
- Your payout depends on pool luck

FPPS vs PPLNS: Choosing Your Payout Method

FPPS (Full Pay Per Share):

- Pool pays you for every valid share
- Pool absorbs luck variance
- Steady daily income
- Pool charges higher fee ($\sim$2–3%)

PPLNS (Pay Per Last N Shares):

- Paid only when pool finds a block
- Your payout depends on pool luck
- Higher average payout (lower fee)

FPPS vs PPLNS: Choosing Your Payout Method

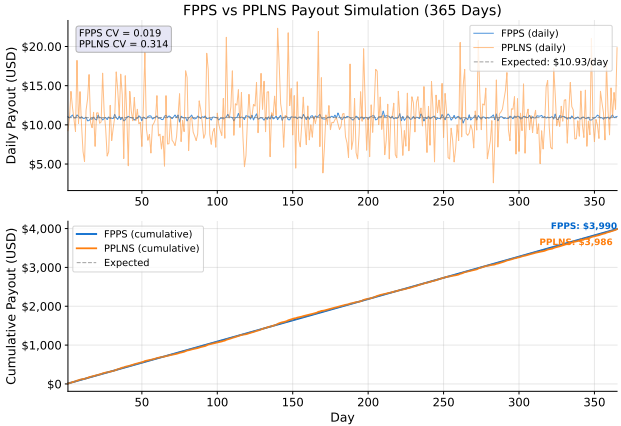
FPPS (Full Pay Per Share):

- Pool pays you for every valid share
- Pool absorbs luck variance
- Steady daily income
- Pool charges higher fee (∼2–3%)

PPLNS (Pay Per Last N Shares):

- Paid only when pool finds a block
- Your payout depends on pool luck
- Higher average payout (lower fee)
- More variance day-to-day

Recommendation:
Beginners → FPPS.
Large operators → PPLNS (can tolerate variance).



PPLNS earns slightly more over a year but FPPS gives you predictable cash flow for electricity bills

Your First Profitability Calculation

Worked example (Antminer S21):

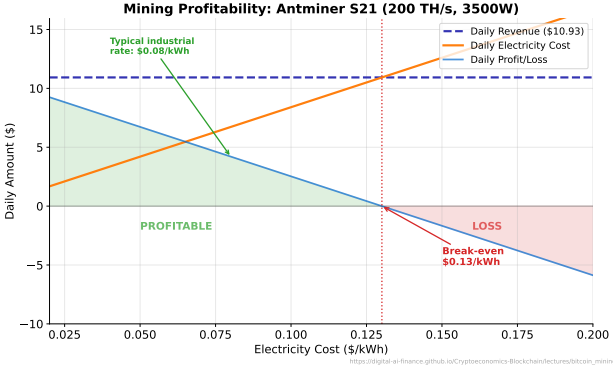
Revenue:
Hashrate share: $\frac{200 \text{ TH/s}}{700 \text{ EH/s}}$

Daily BTC $= \frac{200 \times 10^{12}}{700 \times 10^{18}} \times 3.125 \times 144$

≈ 0.000129 BTC/day
$\approx$ **\$10.93/day** (at \$85K BTC)

Electricity:
3,500W $\times$ 24h $=$ 84 kWh/day
At \$0.08/kWh $=$ **\$6.72/day**

Daily profit: \$4.21
ROI: \$5,000 / \$4.21 $\approx$ 3.3 years



Cheap electricity ($<$\$0.08/kWh) is the difference between a business and a hobby.

Always calculate BEFORE buying — use whattomine.com or nicehash.com/profitability-calculator

Profitability Heatmap: BTC Price vs Electricity Rate

Two-dimensional parameter space:

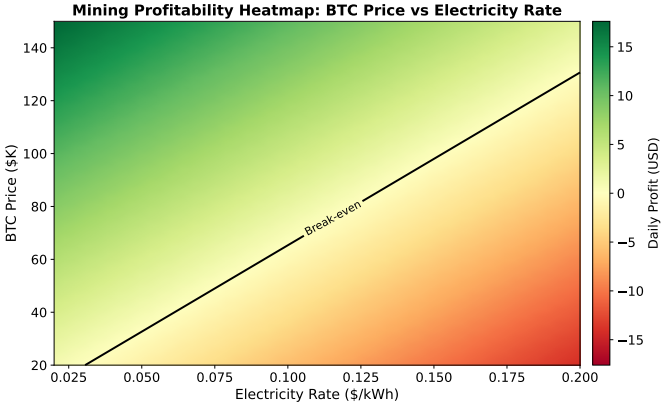
Profitability depends primarily on two variables:

- **BTC price** (x-axis)
- **Electricity rate** (y-axis)

Reading the heatmap:

- Green = profitable
- Red = unprofitable
- White contour = break-even line

The break-even contour shows the minimum BTC price needed at each electricity rate.



Most of the heatmap is red at residential electricity rates ($0.12+/kWh) — industrial power is essential

Sensitivity Analysis: Which Factors Matter Most?

Tornado diagram:
Shows how a $\pm 20\%$ change in each input affects daily profit.

Top factors:

1. **BTC price** — largest impact
2. **Electricity rate** — second largest

Sensitivity Analysis: Which Factors Matter Most?

Tornado diagram:
Shows how a $\pm 20\%$ change in each input affects daily profit.

Top factors:

1. **BTC price** — largest impact
2. **Electricity rate** — second largest
3. **Network difficulty** — rising trend

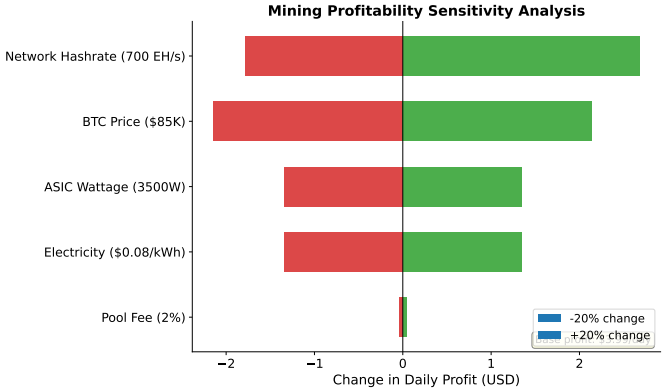
Sensitivity Analysis: Which Factors Matter Most?

Tornado diagram:
Shows how a $\pm 20\%$ change in each input affects daily profit.

Top factors:

1. **BTC price** — largest impact
2. **Electricity rate** — second largest
3. **Network difficulty** — rising trend
4. **Hashrate** — hardware dependent

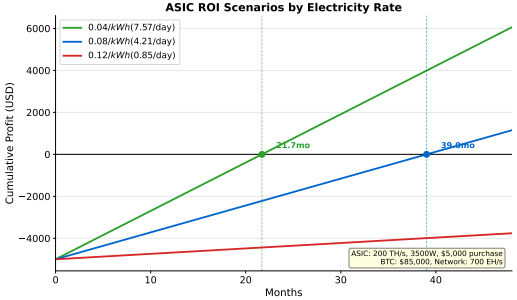
Implication:
You cannot control BTC price or difficulty. The only lever you truly control is electricity cost.



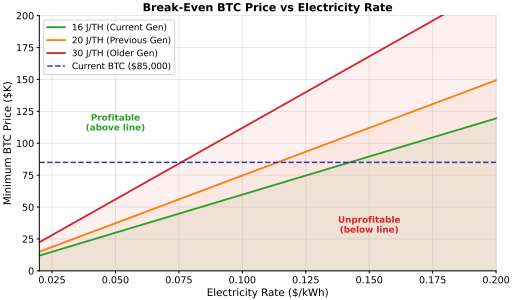
Smart miners focus on what they can control: electricity contracts, hardware efficiency, and cooling

ROI Scenarios and Break-Even BTC Price

When does your ASIC pay for itself? It depends on electricity rates and BTC price.



Cumulative profit at 3 electricity rates. Cheap power ($0.04) reaches ROI in ∼18 months; expensive power ($0.12) may never break even.



Minimum BTC price needed to break even as a function of electricity rate and difficulty.

ROI timelines assume constant BTC price and difficulty — reality is far more volatile

Revenue Decomposition: Block Rewards vs Transaction Fees

Halvings erode block rewards:

- 2024: 3.125 BTC/block
- 2028: 1.5625 BTC/block
- 2032: 0.78125 BTC/block

The transition:
Transaction fees must eventually replace block rewards as the primary miner income source.

Fee model:
A logistic BTC price growth model projects the crossover point where fees dominate revenue.

This transition is critical to Bitcoin's long-term security model.

If fees remain too low after 2040, miners may exit — reducing security. This is Bitcoin's "security budget" debate.

Your Share Decays Over Time

Fixed hashrate + growing network:

If the network grows at $g = 30\%$/year and your hashrate is fixed:

$$\text{share}(t) = \frac{h_0}{H_0 \cdot e^{g \cdot t}}$$

Exponential decay:

- Year 0: your share = 100% of initial
- Year 1: $\sim$74% of initial

Your Share Decays Over Time

Fixed hashrate + growing network:

If the network grows at $g = 30\%$/year and your hashrate is fixed:

$$\text{share}(t) = \frac{h_0}{H_0 \cdot e^{g \cdot t}}$$

Exponential decay:

- Year 0: your share = 100% of initial
- Year 1: $\sim$74% of initial
- Year 2: $\sim$55%

Your Share Decays Over Time

Fixed hashrate + growing network:

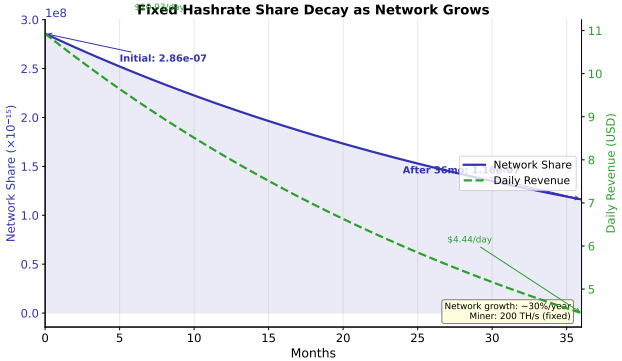
If the network grows at $g = 30\%$/year and your hashrate is fixed:

$$\text{share}(t) = \frac{h_0}{H_0 \cdot e^{g \cdot t}}$$

Exponential decay:

- Year 0: your share = 100% of initial
- Year 1: ∼74% of initial
- Year 2: ∼55%
- Year 3: ∼41%

Implication:
Standing still means falling behind. You must upgrade hardware or accept declining revenue.



Network hashrate has grown ∼30%/year historically — your ASIC's revenue halves every ∼2.3 years from decay alone

Hardware Depreciation: When to Sell vs Keep Mining

ASICs depreciate rapidly:

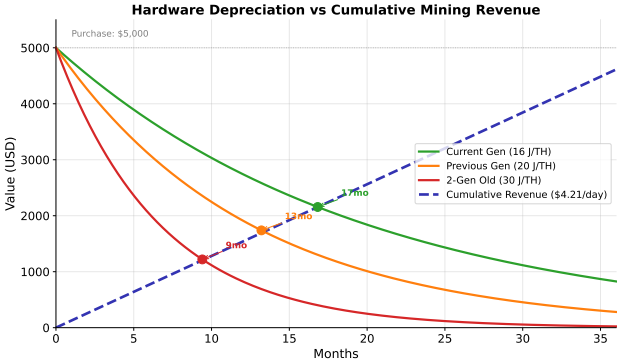
Resale value follows an exponential decay model:

$$V(t) = V_0 \cdot e^{-\delta \cdot t}$$

Depreciation rates:

- Aggressive: $\delta = 1.0$ (50% in 8 months)
- Moderate: $\delta = 0.7$ (50% in 12 months)
- Conservative: $\delta = 0.5$ (50% in 17 months)

Decision rule:
When daily mining revenue $<$ daily depreciation cost, *sell the hardware* and exit.



ASIC resale markets (Kaboom Mining, Bitmain resellers) exist but liquidity drops fast after the next generation ships

Your Electricity Bill: The #1 Cost Factor

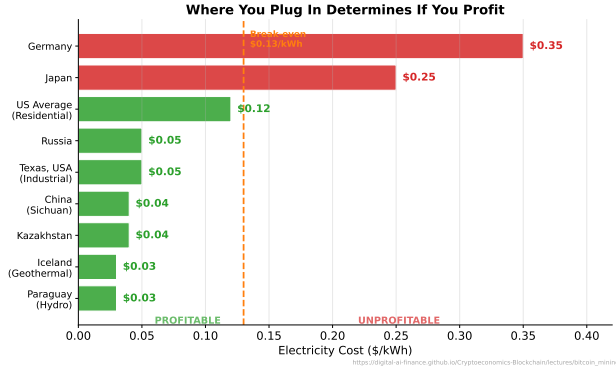
Electricity is **60–80%** of ongoing mining costs.

Where miners find cheap power:

- Iceland — geothermal, ∼$0.03/kWh
- Paraguay — hydroelectric, ∼$0.03/kWh
- Texas — wind/solar curtailment, ∼$0.05/kWh

Daily cost formula:
Power (kW) × 24 × Rate ($/kWh)

Example: At $0.10/kWh:
3.5 kW × 24 = **$8.40/day**
Revenue ≈ $10.93/day
Profit = $2.53/day (thin margin!)

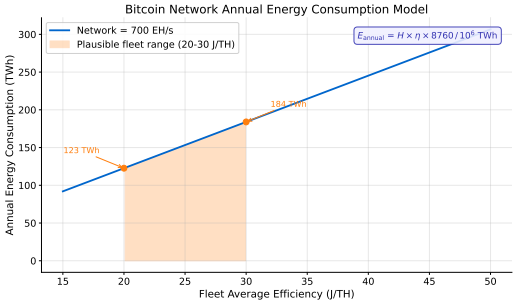


Residential rates ($0.12–0.20/kWh) make home mining unprofitable for most people.

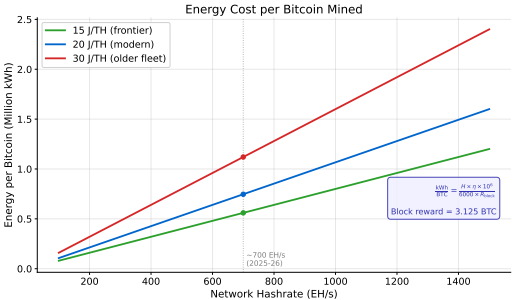
This is why large mining operations locate near hydroelectric dams, geothermal plants, or stranded natural gas

Bitcoin's Network Energy Consumption

Energy model: E_{annual} = hashrate × efficiency × 8,760 hrs. At 700 EH/s and 25 J/TH ≈ **153 TWh/yr** (∼0.6% of global electricity). Per coin: ∼**932,000 kWh/BTC** mined.



Annual network energy consumption (TWh) as hashrate and efficiency evolve.

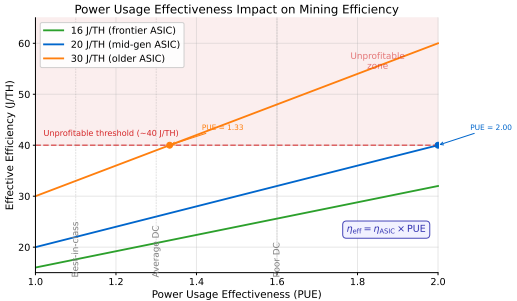


Energy cost per BTC mined — rising as difficulty grows and rewards halve.

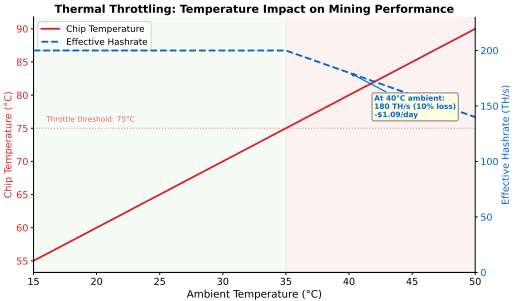
Bitcoin's energy use is debated — proponents argue it incentivizes renewable energy development in remote areas

PUE and Thermal Throttling: Wasted Energy

PUE (Power Usage Effectiveness) = total facility power / IT equipment power. Ideal = 1.0; typical mining farm = 1.1–1.3. Poor cooling wastes 10–30% of your electricity budget.



Impact of PUE on effective energy cost — every 0.1 PUE increase adds ∼10% to your electricity bill.



Thermal throttling: hashrate drops sharply above 80°C as chips protect themselves.

Immersion cooling (PUE ≈ 1.02) is gaining adoption at scale — submerging ASICs in dielectric fluid

Selfish Mining: The 33% Threat

Eyal & Sirer (2014):

A selfish miner withholds blocks and releases them strategically. The profitability threshold:

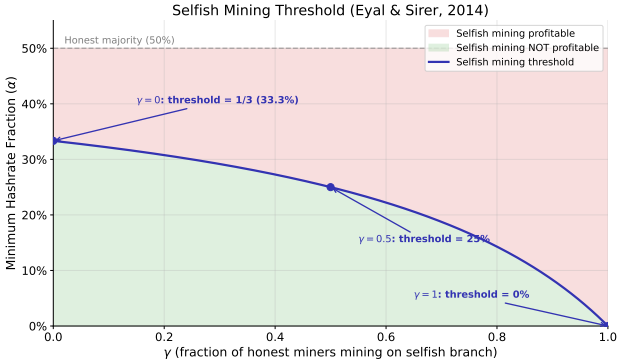
$$\alpha^* = \frac{1-\gamma}{3-2\gamma}$$

where γ = fraction of honest miners that mine on the selfish miner's chain when a fork occurs.

Implications:

- At $\gamma = 0$: threshold = **33%** (not 50%!)
- At $\gamma = 0.5$: threshold = **25%**
- At $\gamma = 1$: threshold = 0% (always profitable)

This challenges the "51% security" assumption.



In practice, selfish mining has not been observed at scale — the social/reputational cost deters rational miners

Double-Spend Probability: Nakamoto's Formula

Whitepaper §11:

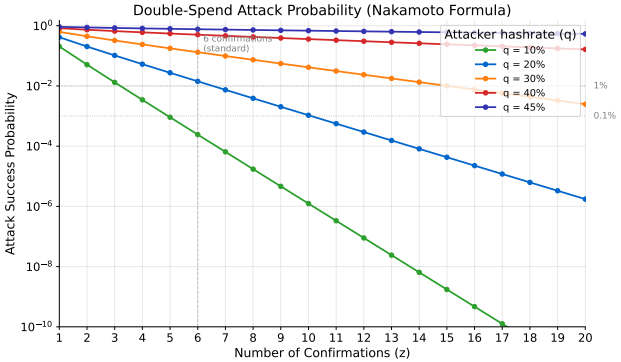
An attacker with fraction q of hashrate tries to reverse a transaction after z confirmations:

$$P = 1 - \sum_{k=0}^{z} \frac{(\lambda)^k e^{-\lambda}}{k!} \left(1 - \frac{q^{z-k}}{p^{z-k}}\right)$$

where $\lambda = z \cdot q/p$ and $p = 1 - q$.

Practical rule:

- $q < 10\%$: 2 confirmations suffice
- $q < 30\%$: 6 confirmations suffice
- $q > 45\%$: no number is truly safe



The "6 confirmations" convention (∼1 hour) provides exponentially decreasing attack probability for $q < 0.3$

Cost of a 51% Attack

Attack cost has two components:

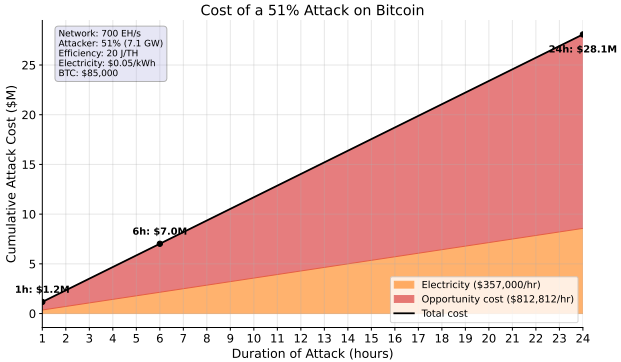
1. Electricity cost:
Must sustain >50% of network hashrate. At 700 EH/s and $0.05/kWh:

$$\text{cost/hr} \approx \$1.17\text{M}$$

2. Opportunity cost:
While attacking, you forgo honest mining rewards (∼$1.5M/hr at current prices).

Total: ∼$2.7M/hr to sustain a 51% attack.

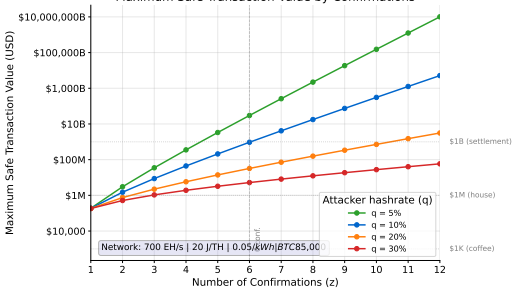
Over 24 hours: ∼$65M — and you still need to profit enough to justify the cost.



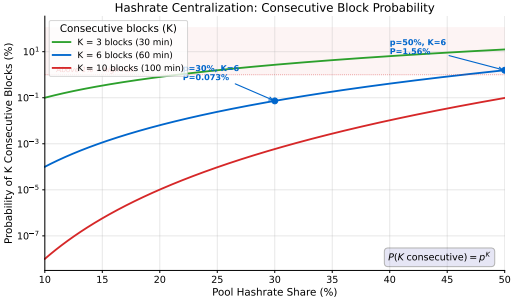
Bitcoin's security is economic: the cost of attacking exceeds what an attacker can steal via double-spends

How Many Confirmations Do You Need?

Safe transaction value: $V_{\text{safe}} = \text{attack\_cost}(z)/P_{\text{attack}}(z)$. Merchants set confirmation requirements based on transaction size.



Safe transaction value increases exponentially with confirmations — 6 blocks covers most use cases.

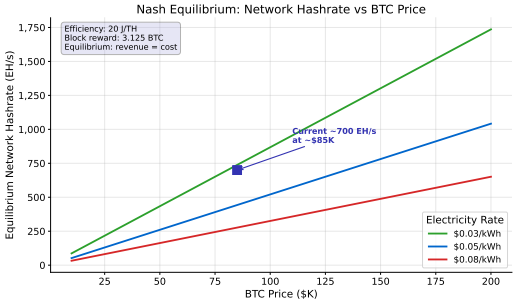


Pool concentration risk: if top 2–3 pools collude, they could exceed 51%.

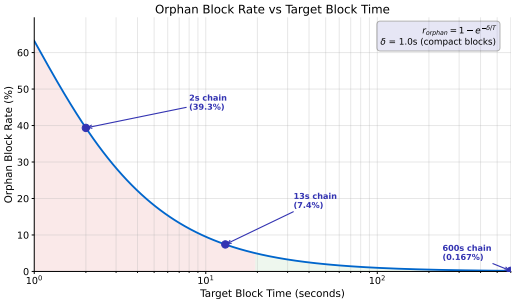
Decentralization of hashrate is a public good — pool concentration creates systemic risk even without malice

Nash Equilibrium and the Orphan Rate Trade-Off

Miner entry game: Miners enter the network until expected profit = 0 (zero-profit equilibrium). Hashrate is linear in BTC price. **Orphan rate:** Shorter block times → more orphans (wasted blocks).



At Nash equilibrium, total mining cost ≈ total mining revenue. No excess profit remains.



Orphan rate rises sharply below 5-minute block times — 10 minutes is a design trade-off.

Bitcoin's 10-minute block time balances security (low orphan rate) against user experience (confirmation speed)

Reading Your Mining Dashboard

Metrics to monitor:

- **Hashrate** (actual vs expected) — within 5% of spec
- **Accepted shares** — proportional to income

Reading Your Mining Dashboard

Metrics to monitor:

- **Hashrate** (actual vs expected) — within 5% of spec
- **Accepted shares** — proportional to income
- **Rejected shares** — healthy $<1\%$

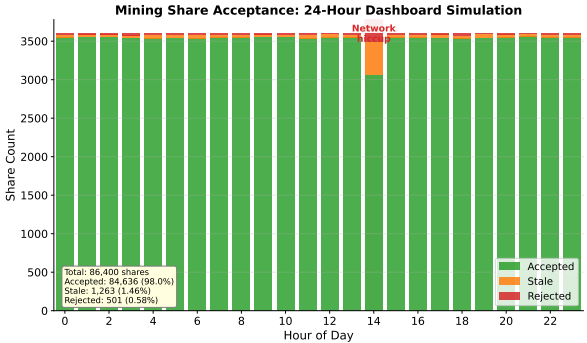
Reading Your Mining Dashboard

Metrics to monitor:

- **Hashrate** (actual vs expected) — within 5% of spec
- **Accepted shares** — proportional to income
- **Rejected shares** — healthy $<1\%$
- **Temperature** — 65–75°C normal; >85°C shutdown risk

Troubleshooting:

- Hashrate drops $\rightarrow$ check temp/fans
- High rejects $\rightarrow$ check internet/latency
- Revenue below expected $\rightarrow$ difficulty increased



A 24-hour share simulation showing normal operation with a mid-day connectivity hiccup (spike in rejected shares).

Pool dashboards show all these metrics in real time — set up email/Telegram alerts for anomalies

BTC Price Uncertainty and Mining Profitability

Geometric Brownian Motion:

$$dS = \mu S\, dt + \sigma S\, dW$$

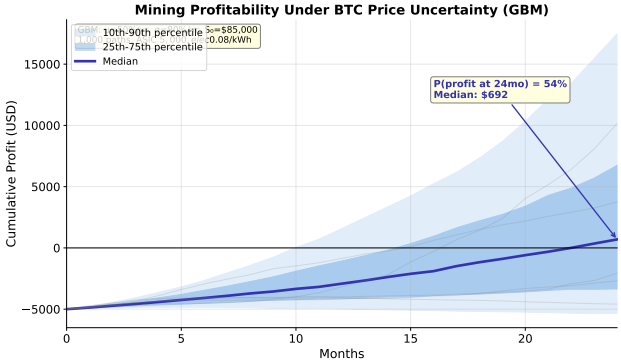
Parameters: $\mu = 50\%$/yr (drift), $\sigma = 80\%$/yr (volatility).

Monte Carlo fan chart:
500 simulated price paths over 3 years.

Key takeaway:
Mining is a *leveraged bet on BTC price*:

- If BTC doubles: profits soar
- If BTC halves: you mine at a loss
- Difficulty adjusts with delay

Buying BTC directly is simpler and has no electricity cost.



Mining only beats buying if you have access to electricity below $0.05/kWh — otherwise just buy BTC

Common Mistakes and Red Flags

Mistakes new miners make:

1. **Ignoring electricity costs**
   Mining at $0.15/kWh is almost always unprofitable
2. **Buying previous-gen hardware at "discount"**
   The efficiency gap kills ROI — old machines use more power per hash

Common Mistakes and Red Flags

Mistakes new miners make:

1. **Ignoring electricity costs**
   Mining at $0.15/kWh is almost always unprofitable
2. **Buying previous-gen hardware at "discount"**
   The efficiency gap kills ROI — old machines use more power per hash
3. **Not accounting for difficulty increases**
   Profitability calculators show *today's* difficulty, not next month's

Common Mistakes and Red Flags

Mistakes new miners make:

1. **Ignoring electricity costs**
   Mining at $0.15/kWh is almost always unprofitable
2. **Buying previous-gen hardware at "discount"**
   The efficiency gap kills ROI — old machines use more power per hash
3. **Not accounting for difficulty increases**
   Profitability calculators show *today's* difficulty, not next month's
4. **Trusting cloud mining services**
   Most are scams or unprofitable after fees

Red flags — run away if you see:

- × "Guaranteed 10% monthly returns"
- × "Mine Bitcoin on your phone"

Common Mistakes and Red Flags

Mistakes new miners make:

1. **Ignoring electricity costs**
   Mining at $0.15/kWh is almost always unprofitable
2. **Buying previous-gen hardware at "discount"**
   The efficiency gap kills ROI — old machines use more power per hash
3. **Not accounting for difficulty increases**
   Profitability calculators show *today's* difficulty, not next month's
4. **Trusting cloud mining services**
   Most are scams or unprofitable after fees

Red flags — run away if you see:

- × "Guaranteed 10% monthly returns"
- × "Mine Bitcoin on your phone"
- × "No electricity costs"

Common Mistakes and Red Flags

Mistakes new miners make:

1. **Ignoring electricity costs**
   Mining at $0.15/kWh is almost always unprofitable
2. **Buying previous-gen hardware at "discount"**
   The efficiency gap kills ROI — old machines use more power per hash
3. **Not accounting for difficulty increases**
   Profitability calculators show *today's* difficulty, not next month's
4. **Trusting cloud mining services**
   Most are scams or unprofitable after fees

Red flags — run away if you see:

- × "Guaranteed 10% monthly returns"
- × "Mine Bitcoin on your phone"
- × "No electricity costs"
- × "Revolutionary new mining algorithm"

Common Mistakes and Red Flags

Mistakes new miners make:

1. **Ignoring electricity costs**
   Mining at $0.15/kWh is almost always unprofitable
2. **Buying previous-gen hardware at "discount"**
   The efficiency gap kills ROI — old machines use more power per hash
3. **Not accounting for difficulty increases**
   Profitability calculators show *today's* difficulty, not next month's
4. **Trusting cloud mining services**
   Most are scams or unprofitable after fees

Red flags — run away if you see:

- × "Guaranteed 10% monthly returns"
- × "Mine Bitcoin on your phone"
- × "No electricity costs"
- × "Revolutionary new mining algorithm"
- × "Invest $100, earn $1,000/month"

Reality Check

If someone could guarantee mining returns, they would not need your money. Real mining has real costs and real risks.

The most common mistake is buying hardware BEFORE calculating profitability at YOUR electricity rate

Key Takeaways

Protocol:

- Mining = SHA-256 lottery; hash below target wins
- Difficulty adjusts every 2,016 blocks ($\sim$2 weeks) to maintain 10-min blocks
- Block reward halves every $\sim$4 years (now 3.125 BTC)
- Block times follow an exponential distribution

Economics:

- Electricity is 60–80% of costs — calculate BEFORE buying
- Your hashrate share decays exponentially as the network grows
- Hardware depreciates rapidly — know when to sell
- Nash equilibrium: miners enter until profit ≈ 0

Practical:

- ASIC efficiency (J/TH) $>$ raw hashrate
- Join a pool; FPPS for beginners
- Monitor: hashrate, temp, rejected shares
- Selfish mining lowers the security threshold below 50%
- Cloud mining is almost always a bad deal

The Bottom Line

Profitable mining requires: (1) efficient hardware, (2) cheap electricity ($<$\$0.08/kWh), (3) patience (ROI in years), and (4) understanding the game theory that secures the network.

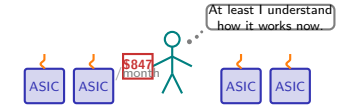
For PoW theory: Lesson 7. For fork resolution: Block Consensus lecture. For security attacks: Lesson 43.

The Reality of Mining in 2026

Understanding mining makes you a better Bitcoin participant, even if you never plug in an ASIC.

The economics, the incentives, the competition — it all connects back to how Bitcoin works:

- Why are transactions secure? *Miners.*
- Why does Bitcoin have a fee market? *Block space is scarce.*
- Why can't someone "hack" Bitcoin? *Rewriting history costs more than the reward.*



Final Thought

The best investment in mining might be understanding it — not doing it.

Next steps: explore Lesson 7 (Proof of Work theory), Lesson 6 (Bitcoin Protocol), Block Consensus (fork resolution)