Game Theory: A Visual Guide

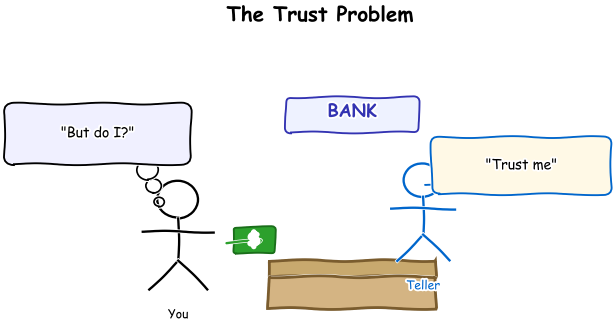
A Story in Pictures

Prof. Dr. Jörg Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

Why Is Trust So Hard on the Internet?



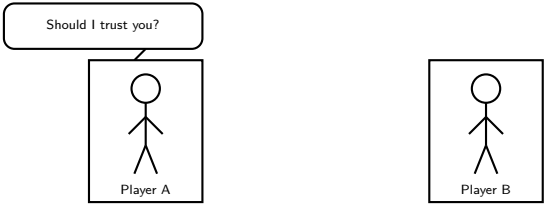
This lecture tells the story of how blockchains use game theory to make honesty the most profitable strategy.

What Will You Understand After This?

1. **Why** strangers do not cooperate without rules
2. **How** blockchain makes honesty the best strategy
3. **Why** attacking costs more than cooperating

Game theory is the science of strategic decisions. Blockchain designers use it to build systems that work even when participants are selfish.

Would You Cooperate or Defect?



Cooperate	Win/Win	Betray
Defect	Betray	Lose/Lose

The Prisoner's Dilemma: both players are better off cooperating, but each is tempted to defect. Blockchain solves this by changing the payoffs.

Why Don't Strangers Cooperate?

Three reasons:

1. **One-shot game** — no repeat interaction, so no reason to build trust
2. **No enforcement** — no police online, no court to appeal to
3. **Anonymous** — no reputation to protect, no identity to verify

The core problem:

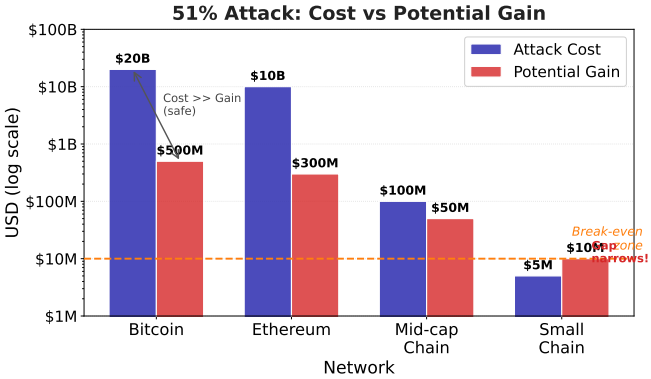
"Rational strangers defect. Always."

Unless you change the rules of the game so that cooperation pays more than defection.

That is what blockchain does.

Game theory predicts that without enforcement, rational players always choose self-interest. Blockchain changes the payoff matrix.

Is Cheating Worth the Cost?



The key insight: well-designed blockchains make the cost of attacking far greater than the potential reward.

What If We Could Make Honesty the Best Strategy?

Real world enforcement:

- Laws define what is allowed
- Police catch violators
- Courts punish offenders

Requires trust in institutions.

Blockchain enforcement:

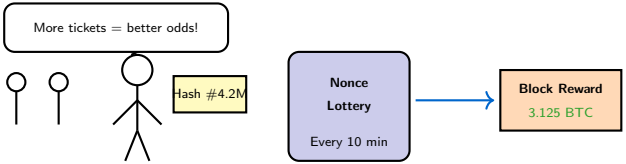
- Math defines what is valid
- Code rejects invalid actions
- Incentives reward honest behavior

Requires trust in math only.

Key idea: design the rules so cheating is always more expensive than playing fair.

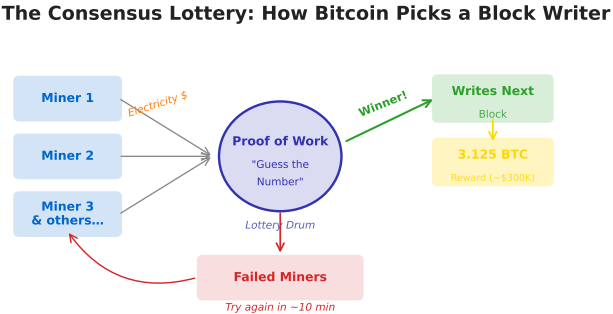
This is mechanism design — engineering the game so that selfish behavior produces collectively good outcomes.

Enter the Mining Lottery



Mining is a lottery: miners guess nonces, and the first to find a valid hash wins the block reward. More computation = more guesses.

How Does the Network Pick a Leader?



Proof of Work selects a leader randomly, weighted by computational power. This lottery runs every 10 minutes in Bitcoin.

What Happens When Everyone Plays Their Best Move?

Nash equilibrium:

The point where *no single player* can improve their outcome by changing strategy alone.

In plain language:

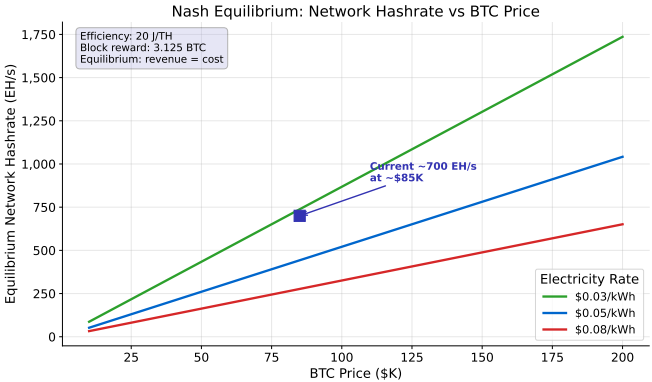
"The move you will not regret, even after seeing what everyone else did."

In Bitcoin mining:

- When every miner follows the rules, no single miner gains by cheating alone
- Honest mining earns steady rewards
- Selfish mining risks losing everything
- The equilibrium is honesty

John Nash proved that every finite game has at least one equilibrium. Bitcoin's design ensures that equilibrium is honest behavior.

Why Do Miners Stay Honest?



The point where mining stops being profitable — the market self-corrects. Honest mining is the Nash equilibrium.

What If Someone Tries to Break the Rules?

Three attack strategies:

1. **Selfish mining** — withhold blocks to gain advantage, but risk losing all work
2. **Double-spend** — spend the same coins twice, but need massive hash power
3. **51% attack** — control the network, but cost exceeds any possible gain

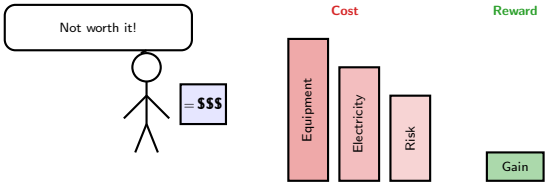
The game theory answer:

Every attack costs more than honest mining earns.

Rational players cheat only when it is profitable. Good design makes cheating unprofitable.

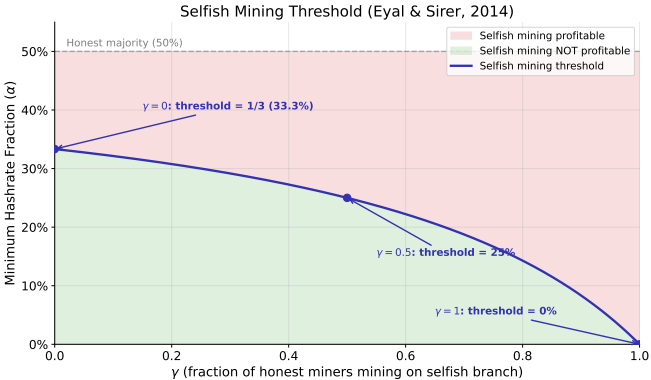
This is the beauty of Bitcoin's design: even if you assume everyone is selfish, the system still works correctly.

Calculate the Cost of Cheating



The cost of attacking (hardware, electricity, opportunity cost) dwarfs any potential reward. Rational actors mine honestly.

When Does Selfish Mining Pay Off?



The red zone is where cheating pays — but notice how small it is. You need at least 33% of total hash power, and even then the gains are marginal.

How Much Does It Cost to Attack the Network?

What a 51% attack means:

- Control more than half of the network's computing power
- Rewrite transaction history
- Double-spend coins

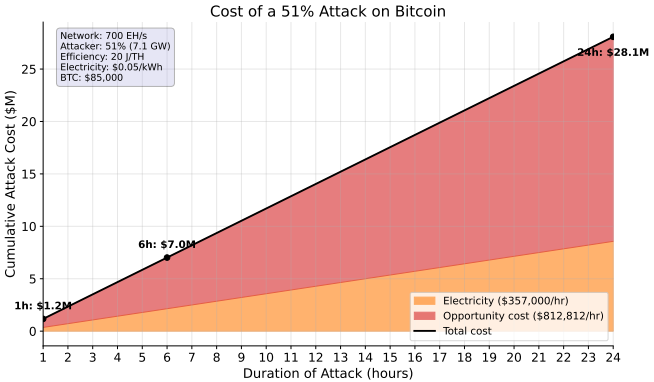
What it costs:

- Billions in mining hardware
- Massive ongoing electricity bills
- The attack destroys the value of the very coins you are trying to steal

You burn down the house to steal the furniture.

A successful 51% attack on Bitcoin would cost billions and would likely crash the price, making the stolen coins worthless.

See the Price Tag of a 51% Attack



Look at the price tag. For major networks, the cost of attack far exceeds any possible profit — that is the whole point.

Where Else Does Game Theory Appear in Blockchain?

Consensus:

- **Staking** — validators lock deposits; cheating means losing them
- **Governance** — token holders vote on upgrades; bad votes hurt token value

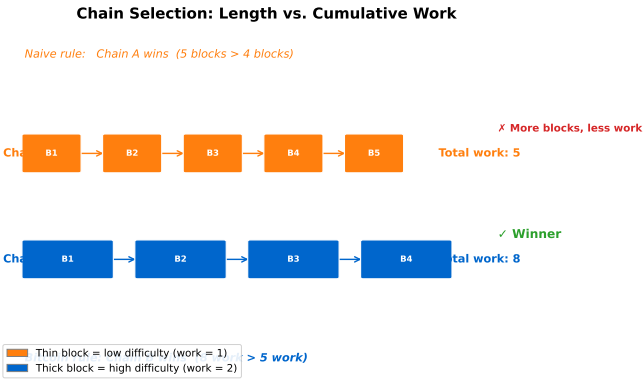
Markets:

- **MEV** — traders compete to extract value from transaction ordering
- **Fork choice** — nodes follow the longest valid chain; deviation is punished

Every blockchain decision is a strategic game. Game theory helps us predict — and design — the outcomes.

Game theory is not just for mining. Staking, governance, trading, and even fork selection are all strategic interactions.

Which Chain Should a Node Follow?



Nodes follow the longest valid chain. This rule creates a focal point — a natural equilibrium that all honest nodes converge on.

What Five Blockchain Games Do You Already Play?

1. **Mining** — guess nonces, win block rewards, follow the rules or waste energy
2. **Staking** — lock tokens as collateral, validate honestly or lose your deposit
3. **Governance** — vote on protocol upgrades, balance short-term gains vs long-term value
4. **Fork choice** — pick the longest valid chain, reject invalid blocks or get orphaned
5. **Trading** — compete for fair execution, front-running vs protocol protections

---

Every time you interact with a blockchain, you are a player in a game. Understanding the game helps you make better decisions.

How Does Game Theory Apply Across Blockchain?

Game	Players	Honest Move	Cheat Move	Why Honesty Wins
Mining	Miners	Follow rules	Selfish mining	Rewards $>$ attack cost
Staking	Validators	Validate honestly	False attestation	Slashing destroys deposit
Governance	Token holders	Vote wisely	Extract value	Reputation + long-term value
Fork choice	Nodes	Longest valid chain	Relay invalid	Peers reject invalid blocks
Trading	Traders	Play fair	Front-run (MEV)	Protocol protections growing

In every game, the protocol makes the honest move the most profitable one.

This table summarizes the core insight: good mechanism design aligns individual incentives with collective welfare.

Think Like a Game Designer

Three-step recipe:

1. **Define the players** — who participates and what do they want?
2. **Set the payoffs** — make honesty pay more than cheating
3. **Test for exploits** — what is the cheapest attack? Is it still too expensive?

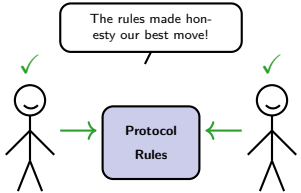
The designer's mantra:

"Assume everyone is selfish. Then build a system that works anyway."

This is called **mechanism design** — the reverse engineering of game theory.

Satoshi Nakamoto was a mechanism designer. Bitcoin works not because people are good, but because the rules make goodness profitable.

Celebrate Honesty by Design



The same two strangers from Slide 4, no longer trapped in a dilemma. Protocol rules turned a Prisoner's Dilemma into a cooperation game.

Design Your Own Game

Thought exercise:

Pick any blockchain scenario. Then answer:

1. Who are the players?
2. What are their possible moves?
3. What are the payoffs for each combination?
4. How do you make the honest move the best one?

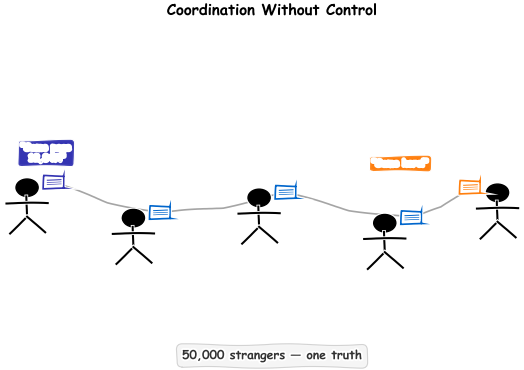
Example: NFT auction

- **Players:** bidders, seller, platform
- **Honest:** bid your true value
- **Cheat:** shill bidding, wash trading
- **Fix:** on-chain bids are transparent, reputation is permanent

Can you find a scenario where honesty does not win? That is a design flaw worth fixing.

The best way to understand game theory is to design a game yourself. Start simple, add complexity, and test for exploits.

Can We Coordinate Without a Boss?



Blockchain proves that thousands of strangers can coordinate without a leader — if the incentives are right.

Remember These Five Ideas

1. **Game theory** predicts how rational players behave — blockchain uses it to align incentives
2. **Nash equilibrium** means no player gains by changing strategy alone — honest mining is the equilibrium
3. **Mechanism design** is reverse game theory — build rules that make honesty the best strategy
4. **Attacks cost more than cooperation** — 51% attacks, selfish mining, and double-spends are all unprofitable
5. **Every blockchain interaction is a game** — mining, staking, governance, trading, and fork choice

Assume everyone is selfish.
Design so it works anyway.

You now understand how game theory keeps blockchains secure. For formal models, equilibrium proofs, and advanced attacks, see the full lecture.