Game Theory for Crypto

Alice & Bob Build a DEX

A Visual Introduction — No Prerequisites Required

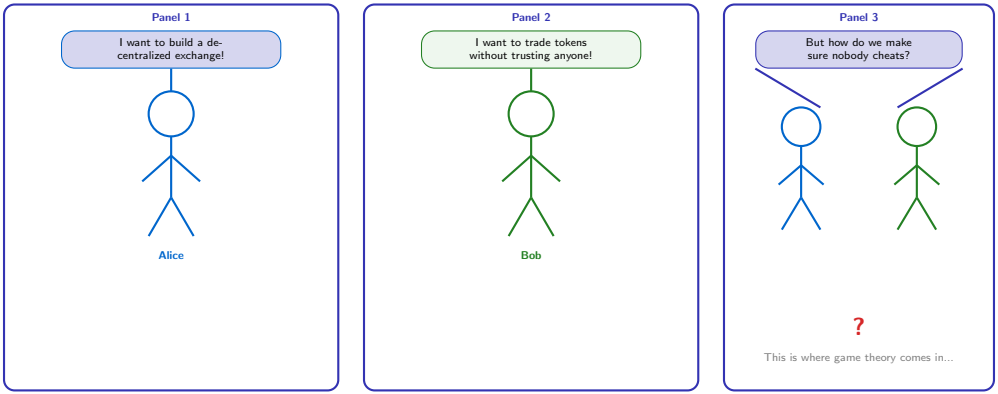
"Every crypto protocol is a carefully designed game"

Prof. Dr. Joerg Osterrieder

University Lecture Series

March 13, 2026

Meet Alice & Bob



Every interaction between people with different goals is a 'game' — game theory studies how rational players make decisions.

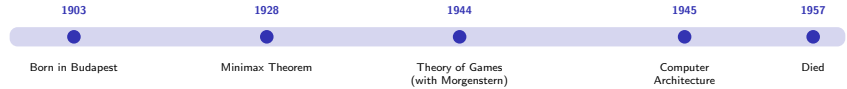
John von Neumann — The Father of Game Theory

JvN

1903–1957

Why does he matter for crypto?

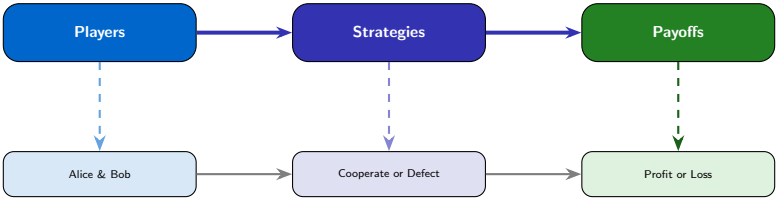
- **Minimax Theorem (1928):** Proved that in zero-sum games, there is always an optimal strategy — the mathematical foundation behind every blockchain security proof.
- **Theory of Games (1944):** Co-authored with Oskar Morgenstern, this book created the entire field. Every mechanism design in DeFi traces back to it.
- **Von Neumann Architecture:** Invented the *stored-program* design — a single memory holds both instructions and data, connected to a CPU via a shared bus. This is the blueprint for virtually every computer ever built, including every blockchain node running today.
- **Also contributed to:** Quantum mechanics, nuclear physics, set theory, economics — one of the greatest minds of the 20th century.



Alice & Bob's takeaway: "Before we can build our DEX, we need the tools von Neumann gave us — how to think about strategies, payoffs, and optimal decisions."

John von Neumann proved the Minimax Theorem in 1928 — the idea that rational players can always find an optimal strategy. This single insight underpins all of blockchain mechanism design.

What Is Game Theory?

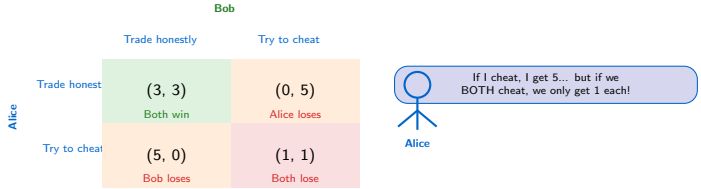


Game theory = predicting what rational people will do

Invented by John von Neumann (1928) — now powers auctions, blockchain protocols, and AI

Game theory was invented by John von Neumann in 1928 — it now powers everything from auctions to blockchain protocols.

The Trust Dilemma — Prisoner's Dilemma



This is the Prisoner's Dilemma — the most famous game in history. Both players are tempted to cheat, but mutual cooperation gives the best combined outcome.

John Nash — A Beautiful Mind

JN

1928–2015

Why does he matter for crypto?

- **Nash Equilibrium (1950):** His 27-page PhD thesis proved that every finite game has at least one equilibrium — the concept that makes blockchain protocol design possible.
- **Non-cooperative games:** Extended game theory beyond zero-sum to ANY strategic interaction — exactly what happens between miners, validators, and traders.
- **Bargaining theory:** Showed how rational agents negotiate — the basis for automated market makers and governance voting.
- **A Beautiful Mind:** Struggled with schizophrenia for 30 years, recovered, won Nobel Prize (1994) and Abel Prize (2015).

Alice & Bob's takeaway: "Nash proved that in ANY game, there is a predictable outcome. If we can find it, we can DESIGN our DEX so the equilibrium IS cooperation."

John Nash's 27-page PhD thesis changed the world — he proved that every finite game has at least one equilibrium, earning him the Nobel Prize 44 years later.

Nash's Key Insight — Every Game Has an Equilibrium

Nash's Theorem (1950)

"Every finite game with a finite number of players and a finite number of strategies has at least one Nash Equilibrium."

In plain English:
No matter how complex the game, there is always a stable outcome where no player wants to change their strategy — **if** they know what everyone else is doing.

Three games, three equilibria:

bad equilibrium →

Prisoner's Dilemma
Both defect → (1,1)
Equilibrium: both cheat
(even though (3,3) is better for both)

good equilibrium →

Coordination Game
Both pick ETH/USDC → (4,4)
Equilibrium: coordinate on same pair
(TWO equilibria — Schelling Point picks one)

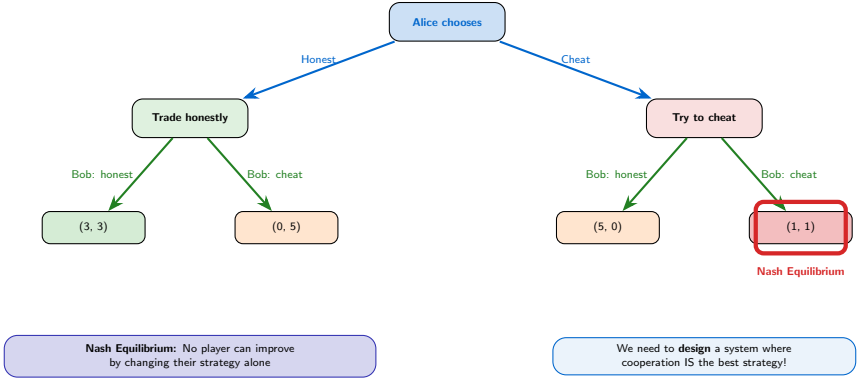
designed equilibrium →

Validator Staking
All validate honestly → (3,3)
Equilibrium: honest validation
(cheating destroys your own stake)

The crypto insight: Nash guarantees an equilibrium EXISTS. Mechanism design is the art of making that equilibrium the COOPERATIVE one — that is exactly what Proof of Stake, AMMs, and governance tokens do.

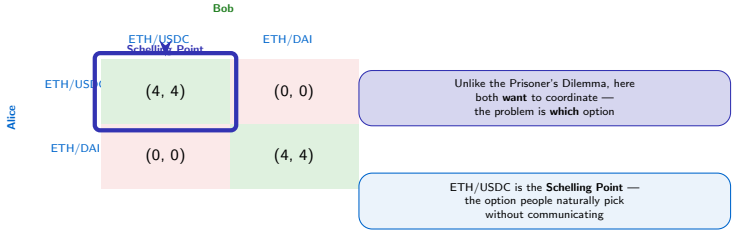
Nash's theorem guarantees every game has a stable outcome — the challenge for crypto protocol designers is engineering the rules so that the stable outcome is also the DESIRABLE one.

Nash Equilibrium — The Predictable Outcome



John Nash proved every finite game has at least one equilibrium — the challenge is making the cooperative outcome also be the equilibrium.

The Coordination Game — Choosing Token Pairs



A Schelling Point is the option people naturally converge on without communicating — in crypto, ETH is almost always the Schelling Point for trading pairs.

Coordination Games — Why They Matter in Crypto

Real Coordination Problems in Crypto

1. Which blockchain to build on?
Everyone benefits if DApps concentrate on one chain (shared liquidity, composability). But which one? Ethereum won because it was first with smart contracts — the Schelling Point.

2. Which token standard to use?
ERC-20 became the standard not because it was technically best, but because everyone adopted it. Once wallets, DEXs, and tools support ERC-20, using anything else means isolation.

3. Which oracle to trust?
Chainlink dominates because protocols coordinate on the same price feed. If half use Chainlink and half use Band, arbitrage exploits appear at the boundary.

Coordination vs. Prisoner's Dilemma

Prisoner's Dilemma	Coordination Game
Players want to cheat	Players want to agree
Incentive to defect	Incentive to match
One equilibrium (bad)	Multiple equilibria (both good)
Problem: trust	Problem: which option?
Solution: mechanism design	Solution: Schelling Points

How Schelling Points form in crypto:

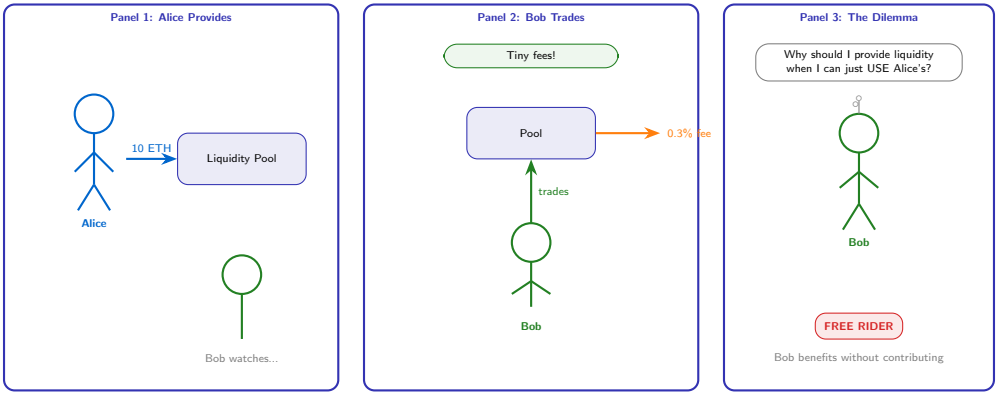
- **First-mover advantage:** Ethereum was first with smart contracts
- **Liquidity begets liquidity:** Traders go where the volume is
- **Developer tools:** More tools → more devs → more tools
- **Cultural consensus:** "ETH is money" becomes self-fulfilling

Once a Schelling Point forms, it is very hard to displace — this is why "Ethereum killers" struggle despite better technology.

Key insight: In coordination games, being RIGHT matters less than being on the SAME SIDE as everyone else. A technically inferior standard that everyone uses beats a superior one that nobody adopts.

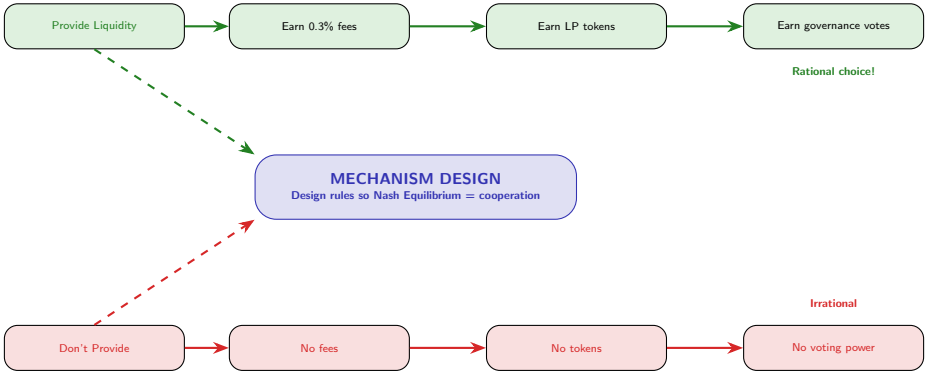
Coordination games explain why crypto has "winner-take-most" dynamics — once a standard or platform becomes the Schelling Point, network effects make it nearly impossible to displace.

Who Provides Liquidity? — The Free Rider Problem



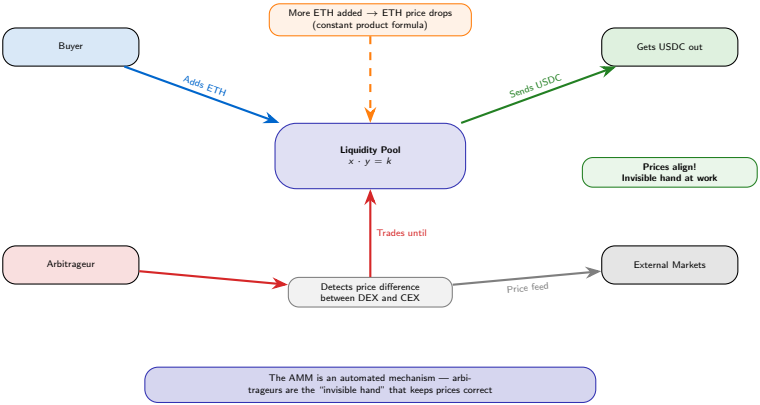
The Free Rider Problem occurs when individuals benefit from a public good without paying for it — Uniswap solved this with liquidity mining rewards.

Mechanism Design — Incentivizing Cooperation



Mechanism design is 'reverse game theory' — instead of predicting behavior, you design the rules so the desired behavior becomes the rational choice.

The Price Discovery Game — How AMMs Work



Automated Market Makers replace traditional order books with a mathematical formula — game theory ensures arbitrageurs keep prices aligned with the market.

How AMMs Really Work — The Game Behind the Formula

The Constant Product Formula

$x \cdot y = k$ (Uniswap V2)

- x = amount of Token A in pool (e.g., ETH)
- y = amount of Token B in pool (e.g., USDC)
- k = constant (never changes during a swap)

Example: Pool has 10 ETH and 20,000 USDC
$k = 10 \times 20{,}000 = 200{,}000$

If you add 1 ETH, the pool now has 11 ETH.
New USDC = $200{,}000/11 = 18{,}181$
You receive $20{,}000 - 18{,}181 = \mathbf{1{,}819}$ USDC
Effective price: 1,819 USDC per ETH
(less than the 2,000 "spot price" — this is **slippage**)

Three Players, Three Strategies

Liquidity Provider (LP)
Strategy: Deposit equal value of both tokens into the pool
Payoff: Earn 0.3% fee on every trade
Risk: Impermanent loss — if prices move, LPs lose value vs. holding
Game theory: LPs accept short-term loss for long-term fee income

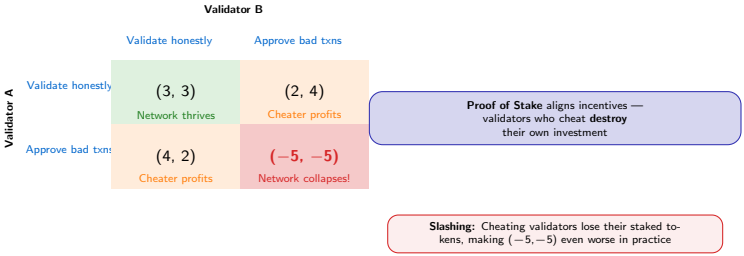
Trader
Strategy: Swap tokens when price is favorable
Payoff: Get tokens at the pool's current price
Risk: Slippage on large orders; sandwich attacks by MEV bots
Game theory: Traders accept slippage because pools offer instant liquidity

Arbitrageur
Strategy: Buy low on one exchange, sell high on another
Payoff: Risk-free profit from price differences
Risk: Gas costs may exceed arbitrage profit; competition from bots
Game theory: Arbitrageurs serve a PUBLIC GOOD — they keep prices accurate

The Nash Equilibrium: LPs provide liquidity (earn fees) → traders use the pool (pay fees) → arbitrageurs correct prices (earn profits). Each player's selfish strategy creates a functioning market — no coordinator needed.

AMMs are a triumph of mechanism design — three types of selfish players (LPs, traders, arbitrageurs) each pursuing profit, yet together they create a fair, efficient, 24/7 market.

The Validator's Dilemma



This is why validators must 'stake' tokens — it makes honest behavior the dominant strategy because cheating destroys your own wealth.

The Validator's Dilemma — Why Proof of Stake Works

The Economics of Honest Validation

Path A: Validate Honestly

- Stake 32 ETH (∼$60,000 at $1,875/ETH)
- Earn ∼4–5% annual yield = ∼$2,400–$3,000/yr
- ETH value grows as network is trusted
- Compound rewards over years

Total payoff over 5 years:
$12,000–$15,000 in rewards + potential ETH appreciation
Risk: near zero (hardware costs, minor downtime penalties)

Path B: Cheat (Approve Bad Transactions)

- Accept bribes to include malicious transactions
- Short-term gain: maybe $500–$5,000 per attack
- **Slashing:** Lose part or ALL of 32 ETH stake
- Network detects cheating → validator is ejected
- If many cheat: ETH crashes → stake worthless

Total payoff: $5,000 bribe minus $60,000 slashed stake
= **net loss of $55,000**

Why This Game Is "Solved"

Three mechanisms that force honest behavior:

1. Slashing (punishment):
Validators who sign conflicting blocks lose 1/32 to ALL of their stake. The penalty is proportional to how many validators cheat simultaneously — if 1/3 cheat, they lose everything.

2. Inactivity leak (participation):
Validators who go offline slowly lose stake. You must actively participate to keep your deposit.

3. Social consensus (nuclear option):
If a majority attack succeeds, the community can hard fork and slash the attackers' stake on the new chain — making the attack retroactively worthless.

PoW vs PoS — Different games, same goal

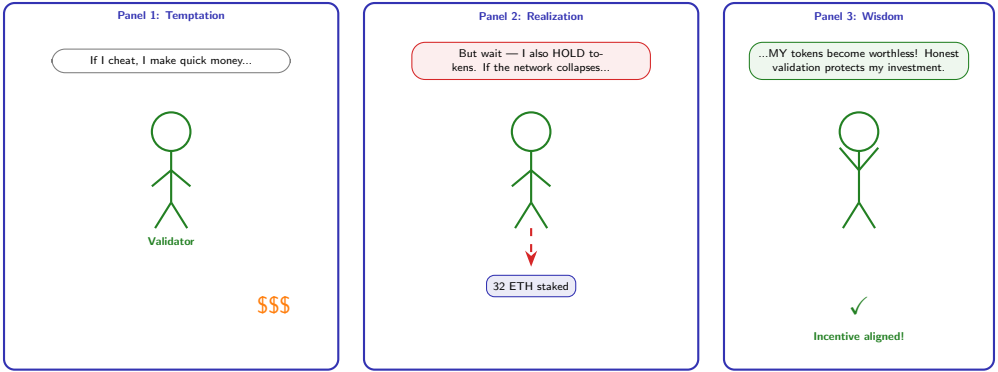
Proof of Work	Proof of Stake
Cost to attack: buy hardware	Cost to attack: buy & stake ETH
Punishment: wasted electricity	Punishment: slashed stake
Attacker keeps hardware	Attacker loses deposit
External cost (energy)	Internal cost (own tokens)

PoS makes attacks **self-destructive** — you must burn your own wealth to attack, then your attack devalues that wealth further.

The key insight: Honest validation is the **dominant strategy** — it pays more ($15K over 5 years) with less risk than cheating (net loss of $55K). Proof of Stake is game theory in action.

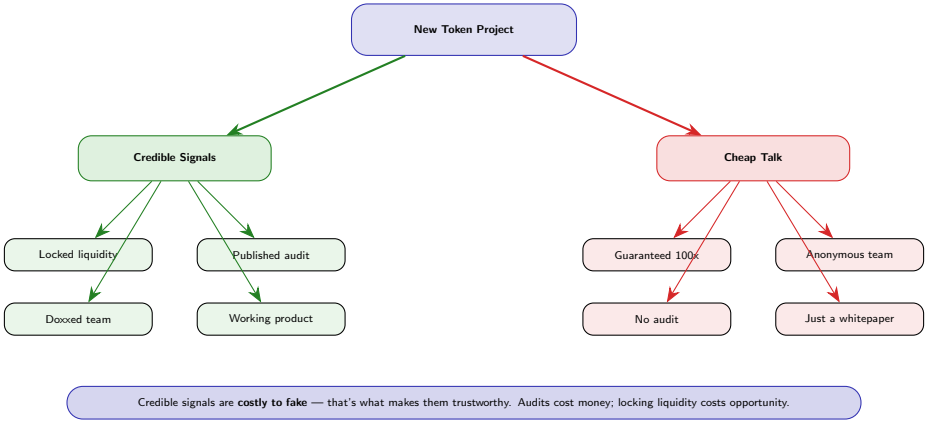
Proof of Stake turns blockchain security into a game theory problem with a clear solution: staking makes honesty profitable and cheating financially suicidal.

Skin in the Game — Why Staking Works



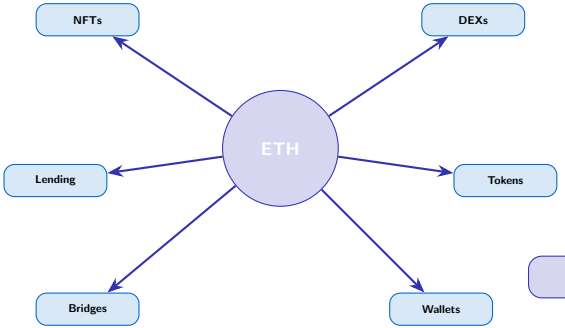
Staking creates 'skin in the game' — validators who cheat destroy their own wealth, so honest behavior is the rational choice.

Signaling — How to Spot Good Projects



In game theory, a credible signal is one that is expensive to produce if you're lying — audits cost money, locking liquidity costs opportunity.

Why Everyone Uses ETH — Schelling Points & Network Effects



Why not Solana? Avalanche?

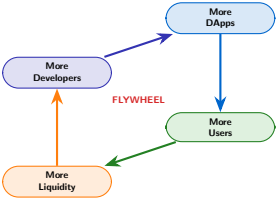
Network effects — once everyone coordinates on ETH, switching is **costly**

We built our DEX on Ethereum because that's where the users already are!

Network effects create powerful Schelling Points — the more people use a platform, the more valuable it becomes, making it the rational default choice.

Network Effects — The Flywheel That Cannot Be Stopped

The Ethereum Flywheel



The Numbers Tell the Story (2025)

Metric	Ethereum
DeFi TVL	∼$50B+ (60% of all chains)
Active developers	∼5,800/month
ERC-20 tokens deployed	>500,000
Daily active addresses	∼400,000+
Smart contracts deployed	>50 million
DEX daily volume	∼$1–3B
Validator count	∼900,000

Every metric reinforces every other metric. This is the Schelling Point made manifest.

Metcalfe's Law in action:

The value of a network is proportional to n^2 (where n = users).

- A network with 10 users: $10^2 = 100$ potential connections
- A network with 100 users: $100^2 = 10{,}000$ connections
- A network with 1,000 users: $1{,}000^2 = 1{,}000{,}000$ connections

Ethereum has **millions of users** — any competitor starts with a $10{,}000\times$ disadvantage in network value, even with identical technology.

Why "Ethereum Killers" struggle:

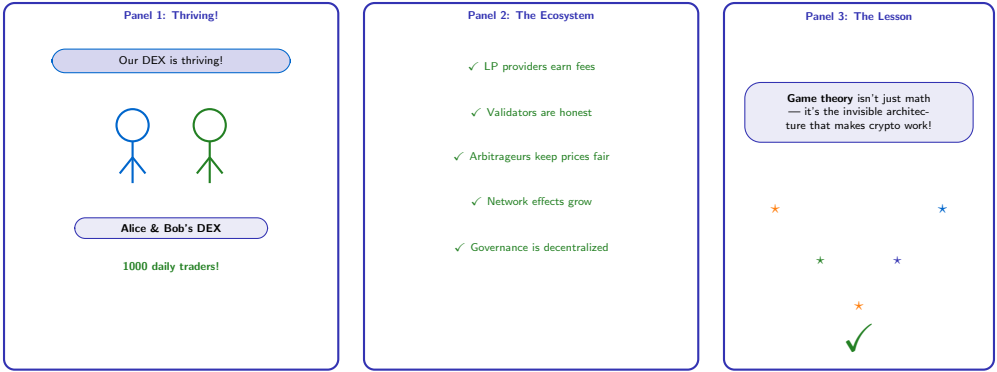
- **Solana:** Faster, cheaper, but 10x fewer DApps
- **Cardano:** Formally verified, but minimal DeFi TVL
- **Avalanche:** EVM-compatible, but fraction of liquidity

They can match Ethereum's *technology* but not its *network effects*.

The game theory lesson: Once a Schelling Point is established, switching costs make it a self-reinforcing equilibrium. The rational choice for any new project is to build where the users already are — even if alternatives are technically superior.

Metcalfe's Law means network effects grow quadratically — Ethereum's dominance is not about better technology, it is about having a flywheel that competitors cannot replicate without matching its entire ecosystem.

Alice & Bob's DEX — Game Theory in Action



Every DeFi protocol is a carefully designed game — understanding game theory helps you evaluate which ones will succeed and which will fail.

Key Terms for Beginners

Term	Definition
Game Theory	Study of strategic decision-making between rational players
Player	A decision-maker in a game (Alice, Bob, a validator)
Strategy	A complete plan of action (cooperate or defect)
Payoff	The reward or penalty from a strategy outcome
Nash Equilibrium	No player can improve by changing strategy alone
Dominant Strategy	Best response regardless of what others do
Prisoner's Dilemma	Both tempted to defect, but cooperation is better

Term	Definition
Coordination Game	Players benefit from choosing the same option
Free Rider	Benefits from a public good without contributing
Mechanism Design	Designing rules so desired behavior is rational
Schelling Point	The option people naturally converge on
Signaling	Costly actions that reveal private information
Network Effect	More users = more value for everyone
AMM	Automated Market Maker — math replaces order books

Master these 14 terms and you can analyze any crypto protocol through a game theory lens.

Key Takeaways

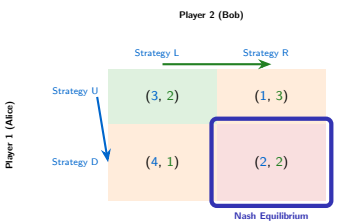
#	Takeaway
1	Every crypto interaction is a **game** with players, strategies, and payoffs — understanding the game is the first step to understanding the protocol.
2	The **Prisoner's Dilemma** explains why trust-free systems need mechanism design — without it, rational players defect and the system collapses.
3	**Proof of Stake** works because validators have skin in the game — cheating costs more than cooperating (slashing makes honesty the dominant strategy).
4	**Schelling Points** and network effects explain why everyone uses ETH — coordination on a focal point creates a self-reinforcing equilibrium.
5	Good **mechanism design** makes cooperation the Nash Equilibrium — the protocol designer's job is to align individual incentives with collective welfare.

Game theory is the invisible engine behind every successful blockchain protocol.

Appendix: Going Deeper

Formal concepts, advanced examples, and further resources

Formal Payoff Matrices Explained



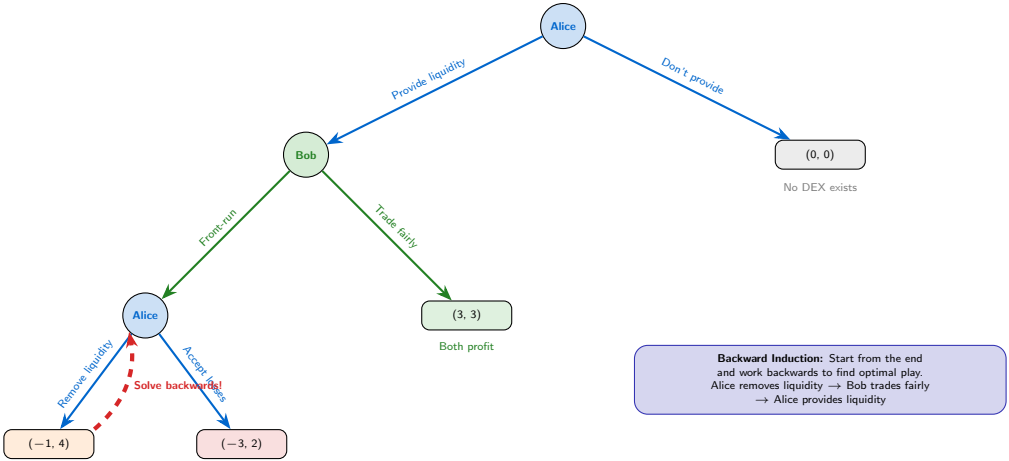
Step 1: For each column, find Alice's best response
Column L: Alice compares 3 vs 4 → picks **D** (payoff 4)
Column R: Alice compares 1 vs 2 → picks **D** (payoff 2)

Step 2: For each row, find Bob's best response
Row U: Bob compares 2 vs 3 → picks **R** (payoff 3)
Row D: Bob compares 1 vs 2 → picks **R** (payoff 2)

Step 3: Nash Equilibrium = where best responses intersect
Alice plays D, Bob plays R → cell (D,R) = **(2, 2)**
Neither can improve by switching alone

This mechanical process works for any 2-player game — find best responses, then find where they intersect.

Game Trees — Extensive Form Games



Extensive form games show the order of decisions — solve them by working backwards from the final payoffs.

Real Crypto Game Theory — Case Studies

MEV

Miner Extractable Value

Validators reorder transactions for profit

Game: Validator vs. trader

Attack: Reorder txns to extract value

Solutions:
- Flashbots (fair ordering)
- PBS (proposer-builder separation)

Sandwich Attack

Front-run + Back-run

Attacker buys before you, sells after

Game: Attacker vs. user

Attack: Profit from price impact

Solutions:
- Private mempools
- MEV protection (e.g., Flashbots Protect)

Governance Attack

Hostile Takeover

Whale buys tokens, votes to drain treasury

Game: Whale vs. community

Attack: Majority vote manipulation

Solutions:
- Time-locks on proposals
- Quadratic voting

These are real game-theory attacks happening on-chain today — understanding them is essential for building secure DeFi protocols.

Your Game Theory Toolkit

The Evolution of Trust

By: Nicky Case

Type: Interactive web game

Teaches repeated games through play.
Takes only 30 minutes.

ncase.me/trust

Game Theory 101

By: William Spaniel

Type: YouTube channel

Visual explanations of game theory
concepts from basics to advanced.

Flashbots Research

By: Flashbots team

Type: Research papers

MEV and mechanism design papers.
The frontier of crypto game theory.

writings.flashbots.net

Token Engineering Commons

By: Community

Type: Community / DAO

For token mechanism design.
Learn how to design incentives.

tecommons.org

Start with 'The Evolution of Trust' — it teaches repeated games through play and takes only 30 minutes.