Smart Contracts and Game Theory

Lesson 7: Summary

Prof. Joerg Osterrieder

Spring 2026

Smart Contracts

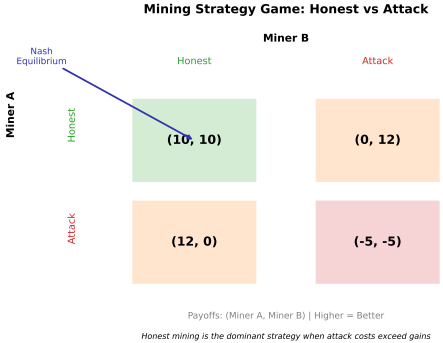
Definition: Self-executing code on blockchain.
Key Properties:

- Deterministic, immutable, transparent
- Execute without intermediaries
- Limited by oracle problem (need external data)

"Code is law" – executes exactly as written.

contracts enable trustless automation

Prisoner's Dilemma



With

proper incentives, rational actors reach suboptimal outcomes

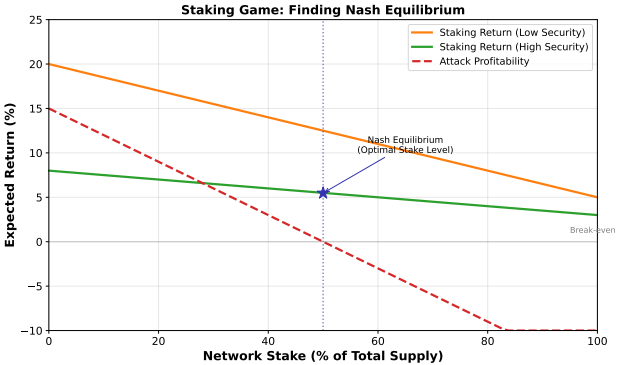
Game Theory Basics

Key Concepts:

- **Players**: Decision makers (miners, validators, users)
- **Strategies**: Available actions
- **Payoffs**: Rewards for strategy combinations
- **Nash Equilibrium**: No one wants to change unilaterally

Why it matters: Protocols must work when everyone acts selfishly.

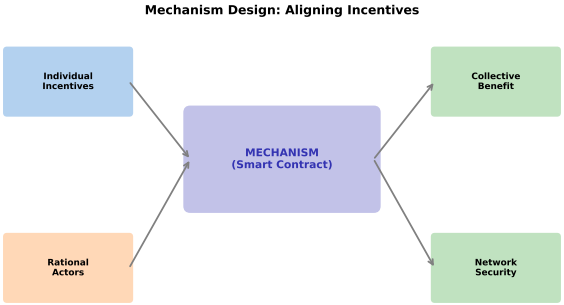
Nash Equilibrium in Staking



Equili

stake level where returns equal opportunity cost

Mechanism Design



Desig

rules so self-interest produces desired outcomes

Incentive Compatibility

Definition: Honest behavior is the best strategy.
Examples in Crypto:

- PoW: Mining honestly earns rewards
- PoS: Slashing makes attacks costly
- Oracles: Penalize liars, reward truth-tellers

Bitcoin's insight: Aligned miner incentives with network security.

compatible systems don't rely on trust

MEV and Governance

MEV (Maximal Extractable Value):

- Frontrunning, sandwich attacks, arbitrage
- Billions extracted annually

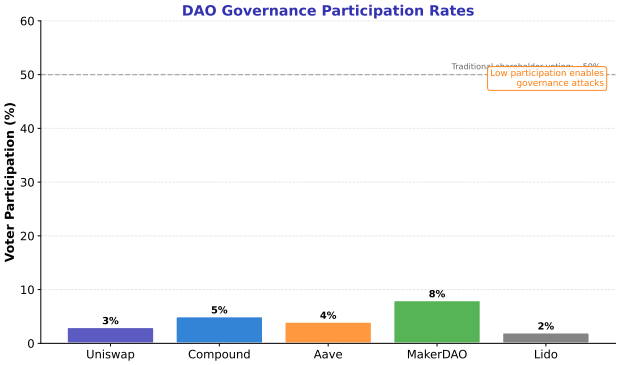
Governance Challenges:

- Voter apathy, plutocracy, vote buying
- No perfect system exists

Activ

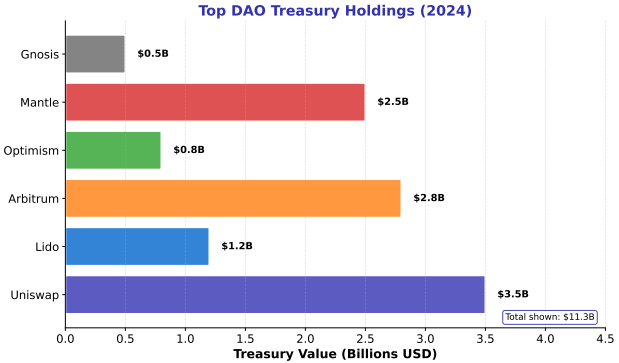
areas of mechanism design research

Governance Participation



Low participation enables minority control and governance attacks

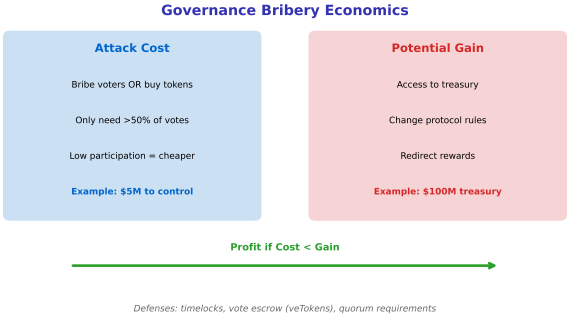
DAO Treasuries



Billio

in DAO treasuries: governance = control over real resources

Bribery Attack Economics



If bribe cost $<$ treasury value, attack is profitable

Key Takeaways

1. **Smart contracts:** Trustless, deterministic execution
2. **Game theory:** Studies strategic decision-making
3. **Nash equilibrium:** Stable state where no one changes
4. **Mechanism design:** Make honest behavior profitable

Core Insight: Crypto works because it makes honesty the most profitable strategy.

Next:

Regulation, Risks, and Future Trends

Thank You

Questions?