Mechanism Design and Optimistic Blockchain

JC, Siyuan
0xpantarhei, THU, PKU
2024

Applications of Game Theory

- Ethereum Transaction Fee Mechanism (EIP-1559)
- Optimal MPC Wallet Profile
- Optimal Mining Strategy
- Optimal AMM
- Texas Hold’em
- FCC wireless spectrums auction
- Sponsored search and ads auctions
- Kidney exchange system
- College admission, stable marriage
- Crowdsourcing
- Prediction Market

Public Blockchain and Mechanism Design

The Academic Viewpoint

- Areas: Blockchain, Distributed Systems, Economics, Game Theory, OR…
- Conferences
  - FC / AFT / SBC / CMU-CBS / …
  - EC / AAMAS / WINE / SAGT / ...
  - AAAI / IJCAI / WWW /…
  - FOCS / SODA / STOC / / ...
  - SP / NDSS / CCS / Crypto / Eurocrypt / UsenixSec / Asiacrypt /...
  - OSDI / SOSP / ATC / DAC / ...
  - DISC / PODC / SIGCOMM / MobiCom / NSDI / ...

The

- Areas: Blockchain, Distributed Systems, Economics, Game Theory, …
- Conferences
  - FC / AFT / SBC / CMU-CBS / …
  - EC / AAMAS / WINE / SA
  - AAAI / IJCAI / WWW /
  - …
  - SP / NDSS / CCS / Crypto / Eurocrypt / UsenixSec / Asiacrypt /...
  - OSDI / SOSP / ATC / DAC / ...
  - DI

The Economic Limits of Permissionless Consensus

Optimal Selfish Mining Strategies in Bitcoin

Collusion-Resilience in Transaction Fee Mechanism Design

Bitcoin Mining Pools: A Cooperative Game Theoretic Analysis

T. Roughgarden: Transaction Fee Mechanism Design for the Ethereum Blockchain: An Economic Analysis of EIP-1559

Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol

Byzantine Ordered Consensus without Byzantine Oligarchy (fair seq)


大愛HD
P
AHD-


鴻運當頭
今谁要给1,000

Game

- Player
- Action
- Utility (payoff)

	Rock	Paper	Scissors
Rock	$0, 0$	$-1, 1$	$1, -1$
Paper	$1, -1$	$0, 0$	$-1, 1$
Scissors	$-1, 1$	$1, -1$	$0, 0$

Rules

- Form
- Information
- …

Equilibrium

- Strategy
  - Pure Strategy
  - Mixed Strategy
  - Dominant Strategy, Dominated Strategy
- Best Response
- Nash Equilibrium: a solution concept.

	囚徒 B 合作	囚徒 B 背叛
囚徒 A 合作	(3, 3)	(0, 5)
囚徒 A 背叛	(5, 0)	(1, 1)

Game Theory Problems

- Does an NE exist?
- How many?
- How to compute?
- Score in NE?

Auction

- Item(s)
- Auctioneer
- Bidders
  - Value
    - Private, Independency, …
  - Bid
  - Risk Aversion
- Mechanism
  - Reserved Price
  - Allocation
  - Payment

Examples of Auctions

- Ascending-bid Auctions
  - English Auction
  - Japanese Auction
- Dutch auctions
- Sealed-bid auction
  - F-SBP-A
  - S-SBP-A
- (GSP) Generalized second-price auction: keyword auctions
- All-pay Auction: Bitcoin Miner
- 1st price auction: (infinite block size, congested) EIP-1559

Mechanism

- Resource Allocation
  - Allocation
  - Payment
  - Winner’s Utility = Value - Payment

Mechanism

- Dreams
  - Truthfulness / Incentive Compatibility / Strategy-proof
  - Social Welfare / Efficiency
  - Budget Balance
  - Individual Rationality
  - Tractability
  - Revenue Max
  - Fairness Max
  - PoA Min

Mechanism Design Problems

- How to design the “Dream” mechanism? Is it even possible?

Famous Conclusions

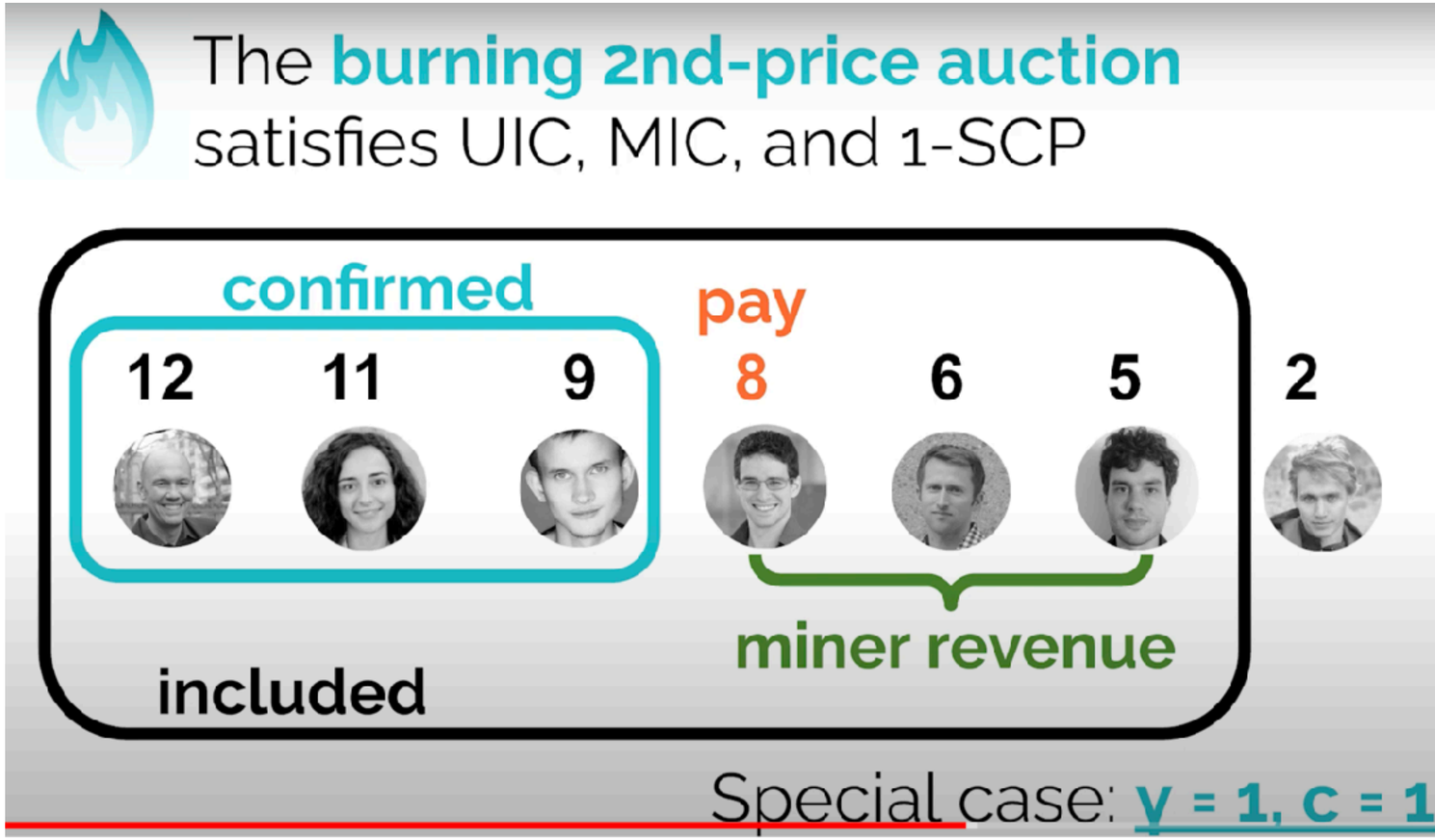
- Winner’s Curse
- Strategic Equivalence
- (RET) Revenue Equivalence Theorem
- Revelation Principle
- S-SBP-A (Vickrey’s)
- Myerson’s Auction

More to know

- Collusion in Auction
- Cooperative Game
  - Core
  - Shapley Value

ETH TFM (Tx Fee Mechanism)

- Dream: U-IC, M-IC, No-Collusion
- No Dream TFM
- Weakly Dream TFM: B2PM
- B2PM: U-IC, M-IC, side-contract-proofness (γ-strict)
- Randomness is necessary
- Unconfirmed inclusion is necessary
- Weakly all-pay is necessary



Optimistic Mechanism (OP9)

- Wide Application
  - OP-RollUp
  - OPML (OP-MachineLearning)
  - OP+ZK (Naysayer-Proof, AVS + ZK-Coprocessor)
- Questions to answer
  - Can we trust the validators? Will they always challenge when the proposer makes a mistake?

Optimistic Mechanism (OP9)

- Players
  - Proposer
  - Validator
- Stake
  - Both P and V
- Reward
  - Both P and V
- Challenge
  - Win / Lose : Penalty / Reward
- Malicious Block Value

Optimistic Mechanism (OP9)

- Related
  - PoSP (Proof-of-Sampling)
  - *On the Security of Optimistic Blockchain Mechanisms*
  - *Incentive Schemes for Rollup Validators*
  - *Incentive Non-Compatibility of Optimistic Rollups*