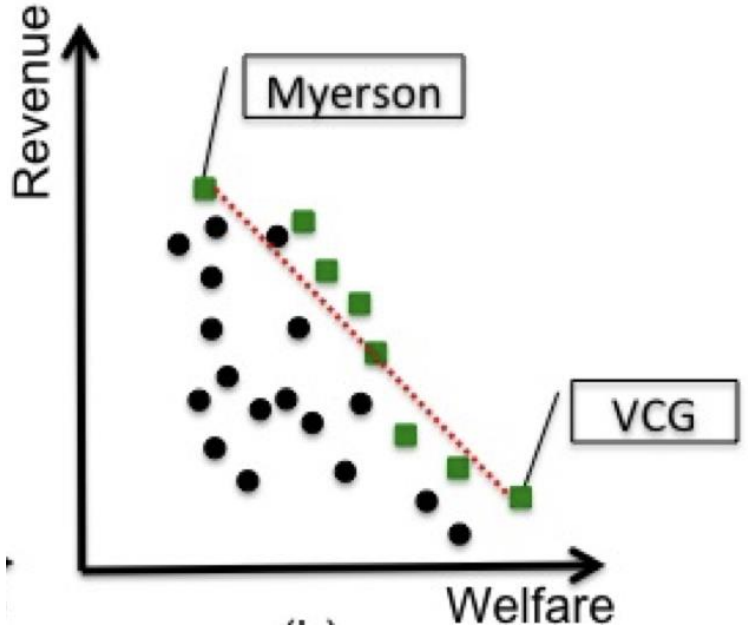
EC'24 Tutorial on Transaction Fee Mechanism Design

PART III : Extensions to the TFM Framework

Revisiting Our Goals and Notions

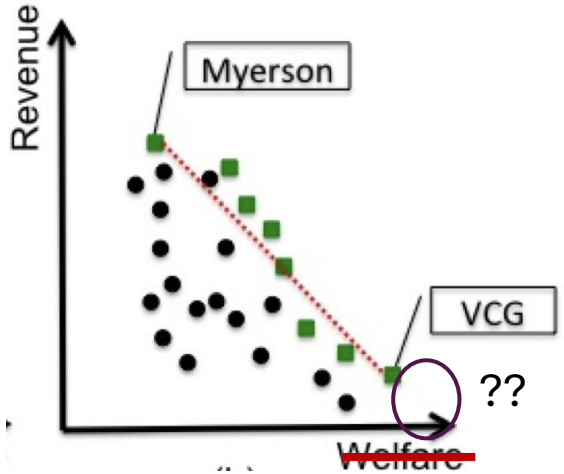
- What is our optimization goal in the mechanism?
- Traditionally: Welfare or Revenue



"Efficiency-Revenue Tradeoffs in Auctions", [Diakonikolas, Papadimitriou, Pierrakos & Singer '12]

Revisiting Our Goals and Notions

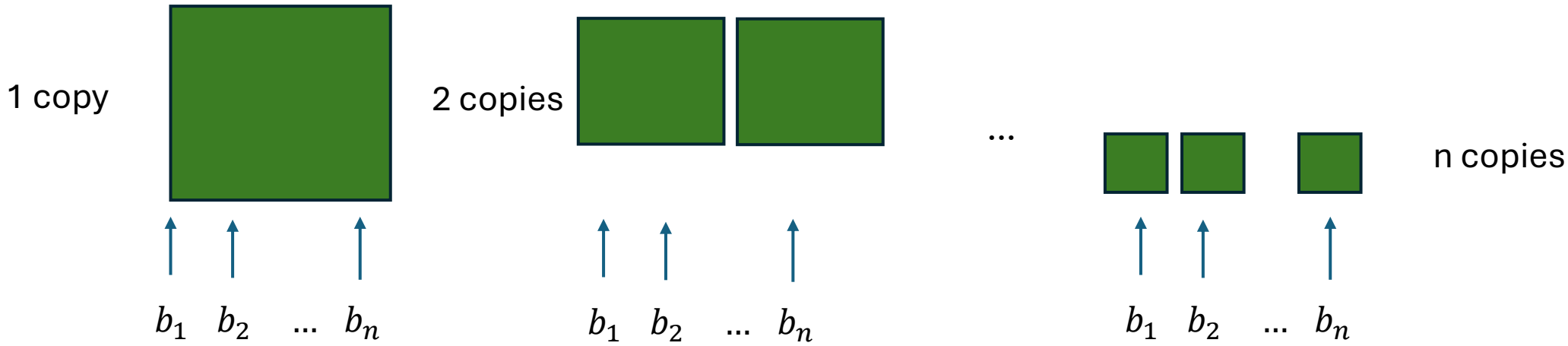
- In Blockchains:
  - Miners offer security, so need to be guaranteed *some* revenue…[1,2]
  - But the main objective is really to benefit the community of *users*. *So:*
    - Maximize user surplus subject to a minimal revenue constraint?
    - Maximize user surplus overall?[3,4]



1. “Redesigning Bitcoin’s Fee Market”, [Lavi, Sattath & Zohar ’19]
2. "On the Instability of Bitcoin Without the Block Reward" [Carlsten, Kalodner, Weinberg & Narayan ‘16]
3. ”Optimal Mechanisms for Consumer Surplus Maximization”, [Ezra, Schoepflin & Shaulker ‘24]
4. ”Simple Mechanisms for Utility Maximization: Approximating Welfare in the I.i.D Unit-Demand Setting”, [Goldner & Lundy ‘24]

User Surplus Maximization

- With unit-demand / multi-unit-submodular valuations, optimal user surplus is O(log(n)) apx of the social welfare (extending the single-parameter result[1])
- This is done through running "VCG with copies"[2]:
  - VCG (with 1 copy) attains the optimal social welfare, but may have high prices
  - VCG with n copies is akin to letting each agent win all the items w.p. 1/n
  - Randomizing over the number of copies balances the spectrum of such cases



1. "Optimal Mechanism Design and Money Burning", [Hartline & Roughgarden '08]
2. "Optimal Mechanisms for Consumer Surplus Maximization", [Ezra, Schoepflin & Shaulker '24]

Rethinking the Collusion & IC Desiderata

- Let’s revisit an example of what we consider a viable collusion…

"Revisiting the Primitives of Transaction Fee Mechanism Design" [Ganesh, Thomas & Weinberg ‘24]
“Incentive-Compatible Collusion-Resistance via Posted Prices” [Ferreira, Gafni & Resnick ‘24]

Collusion vs. a Posted Price

(Think about the fixed-tip version of EIP-1559)

Ok, bidder 1, just say you're willing to pay 1.5, and I'll cash you back 1

We are selling 1 item at a price of 1.5

Posted Price

$b_1 = 1$

$b_2 = \frac{1}{2}$

$b_3 = \frac{1}{4}$

Arbitrary winner above a set price, pays set price

UIC ✅

MIC ✅

Let the price be 1.5

Collusion vs. a Posted Price??

Ok, bidder 1, just say you're willing to pay 1.5, and I'll cash you back 1

Posted Price

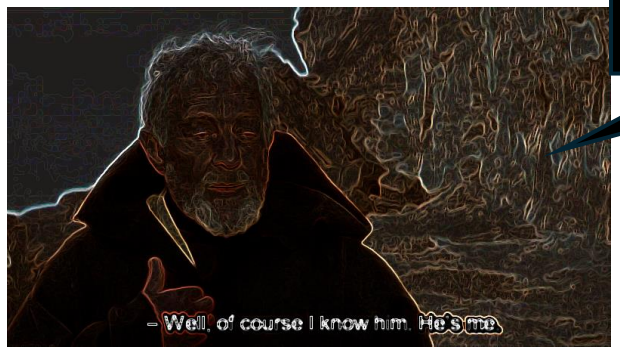
$b_1 = 1$

$b_2 = \frac{1}{2}$

$b_3 = \frac{1}{4}$

Arbitrary winner above a set price, pays set price

Hold on Mr. Miner: Wouldn't **everyone** ask for a cashback in this case?



UIC ✅

MIC ✅

Let the price be 1.5

Rethinking the Collusion & IC Desiderata

- Refining the collusion notion to incorporate incentive-compatibility and individual-rationality *within* the collusion (“No honor among thieves”)
- Circumvents some impossibility results, in particular through posted prices

“Incentive-Compatible Collusion-Resistance via Posted Prices” [Ferreira, Gafni & Resnick ‘24]

Main Caveat: The Model May Be Oversimplified

- Different transactions are co-dependent
- Transactions come in different sizes
- The miners spend valuable time building and verifying blocks
- Different end-applications may induce different strategic environment

- Auction theorists may call this a ~‘Combinatorial’ setting (but not really…)
- Blockchain-ers may call this ‘MEV’

Examples of MEV (Miner/Maximal Extractable Value)

Bad MEV:

- “Stealing” arbitrage ideas
- Sandwich attacks

Good MEV?

- CEX-DEX arbitrage
- Multi-AMM arbitrage at the end of a transaction (“Backrunning”)

Approaches to Address MEV

- MEV Minimization
  - Encrypted Mempools
  - Uniform execution prices across the block (vs. Sandwich attacks)
- MEV Maximization (‘as a service’)
  - MEV-boost
  - **Proposer-Builder Separation (PBS)**
- MEV Redistribution[1,2]
  - MEV-share

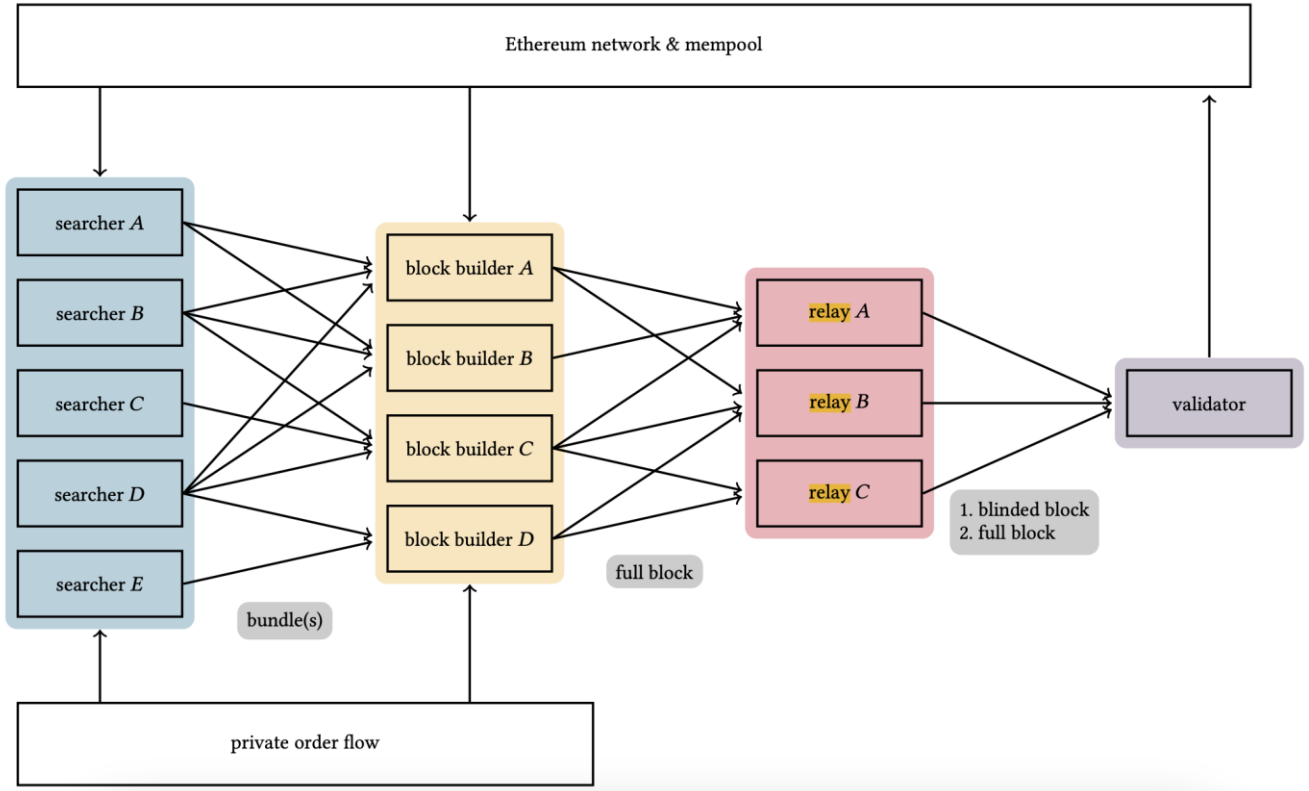
1. "Improving Proof of Stake Economic Security via MEV Redistribution" [Chitra & Kshitij ‘22]
2. "On the Redistribution of Maximal Extractable Value: A Dynamic Mechanism" [Braga, Chionas, Leonardos, Krysta, Piliouras & Ventre '24]

Proposer-Builder Separation (PBS)

- Main concern: Can outsourcing MEV opportunities to sophisticated actors help/harm decentralization of miners?
- MEV itself is a secondary consideration

The ‘Separation of Duties’ in PBS[1]

- What is the right way to distribute roles in the block building pipeline?
- Duties/Roles (as done by MEV-boost):
  - Searcher: Looks for MEV opportunities and create bundles
  - Builder: Out of all transactions and bundles, builds a valid block
  - Relayers: Provide abstraction between builders and validators
  - Proposer/Validator: Has the right to publish a block, publishes it



1. See, e.g., the overview in "Ethereum's Proposer-Builder Separation: Promises and Realities" [Heimbach, Kiffer, Torres & Wattenhofer ‘23]. The drawing is from the paper.

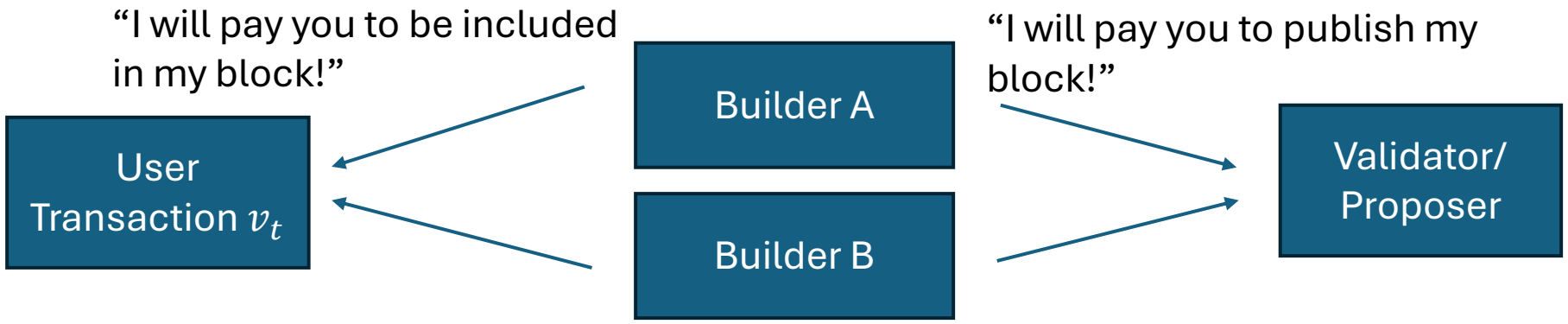
PBS Effect on Decentralization?

- Sophisticated builders dominate the bi-level auction for transactions
- Take CEX-DEX arbitrage as an example…

"The Centralizing Effects of Private Order Flow on Proposer-Builder Separation" [Gupta, Pai & Resnick ‘23]
”Proposer-Builder Separation, Payment for Order Flows, and Centralization in Blockchain” [Capponi, Jia & Olafsson ‘24]

PBS Effect on Decentralization II

- Assume A,B are builders with values $v_A > v_B$ to be the builder
- They compete in a second-price auction over a user transaction with fee v_t
- They then compete in a second-price auction for the validator to propose their block
- B can potentially have its block published: It has $v_B + v_t > v_A$. Whoever wins the user transaction auction, wins the proposer auction as well
- A has higher value for this outcome
- So A has higher willingness to pay in the user transaction auction, and so it always wins.



"The Centralizing Effects of Private Order Flow on Proposer-Builder Separation" [Gupta, Pai & Resnick '23]

PBS Effect on Decentralization III

- Anti-concentration results[1] for a contest between integrated BPs that have different multiples over the user transaction value, and for a Polya urn model where BPs can reinvest their block rewards to increase their probability of proposing again.

<u>Open Challenge:</u>

Can we find a succint framework, so that separation of duties can be analyzed as an optimization problem (a-la-Myerson for auctions), rather than on a case-by-case basis?

1. "Centralization in Block-Building and Proposer-Builder Separation" [Bahrani, Garimidi & Roughgarden '24]

The General MEV setting

- Block producers (BPs) have preferences over outcomes
- No DSIC+MMIC mechanism with active BPs
- Active BPs are ‘integrated’: What if we separate to searchers & passive BPs?
  - Searchers: Convert user transactions to bundles together with added transactions
  - Passive BPs: Correspond to miners in the core model (but can accept bundles)
- The ‘tipless’ mechanism (posted-price with constant burn) is IC for all
- A knapsack auction is IC for all & yields ½ welfare apx with small transactions

"Transaction Fee Mechanism Design in a Post-MEV World" [Bahrani, Garimidi & Roughgarden ‘24]

Many topics that I did not cover…

- Verifiable Sequencing Rules for automated market makers[1,2]
- Applying the TFM framework to NFT auctions[3]
- Mechanism design of L2s and Rollups[4,5]
- Timing games[6,7,8]
- Multi-dimensional fees[9]

1. "Credible Decentralized Exchange Design via Verifiable Sequencing Rules" [Ferreira & Parkes ‘23]
2. ”MEV Makes Everyone Happy under Greedy Sequencing Rule” [Y. Li, J. Li, E. Chen, X. Chen & Deng ’23]
3. “A Framework for Single-Item NFT Auction Mechanism Design” [Arditi, Garimidi, Hirsch & Milionis ‘22]
4. “LedgerHedger: Gas Reservation for Smart-Contract Security” [Tsabary, Manushkin, Bar-Zur & Eyal ‘24]
5. “Optimal Publishing Strategies on a Base Layer” [Bar-On & Mansour ‘24]
6. “Time is Money: Strategic Timing Games in Proof-of-Stake Protocols” [Schwarz-Schilling, Saleh, Thiery, Pan, Shah & Monnot ‘23]
7. “Buying Time: Latency Racing vs. Bidding for Transaction Ordering” [Mamageishvili, Kelkar, Schlegel & Felten ‘23]
8. ”Uncle Maker: (Time)Stamping Out The Competition in Ethereum” [Yaish, Stern & Zohar ‘23]
9. “Multidimensional Blockchain Fees are (Essentially) Optimal” [Angeris, Diamandis & Moallemi ‘24]