Transaction Fee Mechanism Design

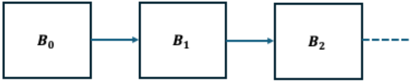
Sankarshan Damle

LIA, EPFL

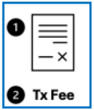
4th December, 2024

Introduction

Introduction

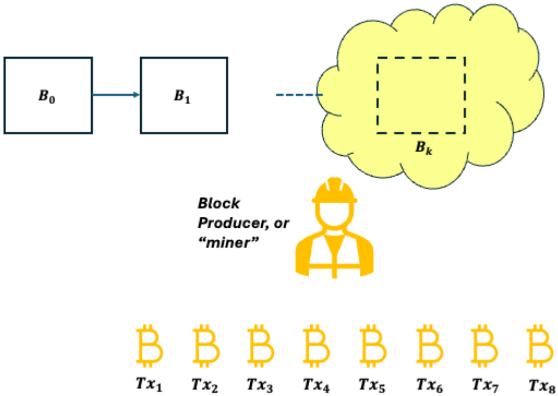


Blocks

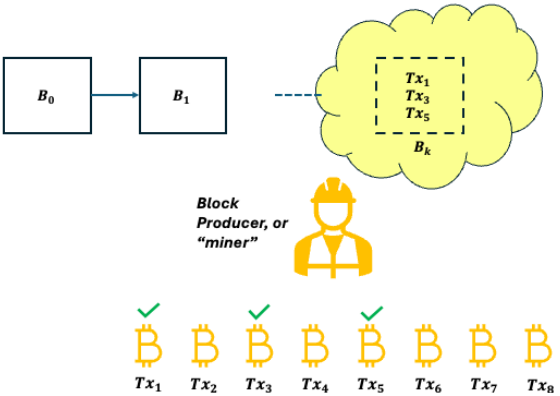


Transaction

Introduction



Introduction



Explosion in Transaction Fees

- Block space is a scarce resource – transaction fees have shot up

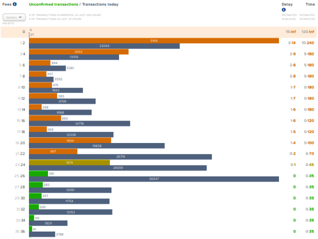


Figure: Transaction Fees vs Processing Latency [7]

EPFL

Explosion in Transaction Fees

- Block space is a scarce resource – transaction fees have shot up
- Transaction latency is inversely proportional to the transaction **bid**

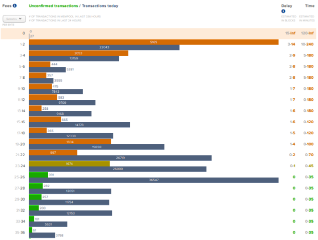


Figure: Transaction Fees vs Processing Latency [7]

Explosion in Transaction Fees

- Block space is a scarce resource – transaction fees have shot up
- Transaction latency is inversely proportional to the transaction **bid**
  - Implication is that transactions with marginal fees have an unbounded waiting time

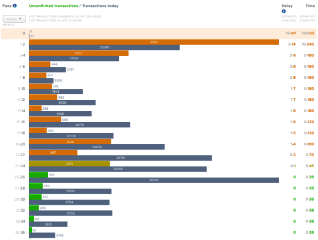


Figure: Transaction Fees vs Processing Latency [7]

Explosion in Transaction Fees

On Blockchain Commit Times: An analysis of how miners choose Bitcoin transactions

minimum of 10^{-5} BTC/kB. A non-trivial percentage of transactions offered feerates that are two orders of magnitude higher than the recommended value; particularly, in data set $\mathcal{B}$, perhaps due to the comparatively high levels of congestion (refer Fig. 3), 34.7% of

Messias *et al.* [5]

The Bitcoin Halving Is Here, and With It a Giant Surge in Transaction Fees

The launch of Casey Rodarmor's new Runes protocol sent fees surging as users rushed to etch new digital tokens that can be launched atop the Bitcoin blockchain.

Credit: CoinDesk

Bitcoin's Unfinished Business: Why Micropayments Still Matter

Tiny, cheap-to-deliver payments can open new markets for small digital goods. Can a new wave of crypto-inflected startups plug a longstanding gap in the internet? This piece is part of CoinDesk's Payments Week.

Credit: CoinDesk

Transaction Fee Mechanism Design

Revisiting: First-price Auction

- The auction setting:

Revisiting: First-price Auction

- The auction setting:
  - An auctioneer interested in selling a non-divisible item

Revisiting: First-price Auction

- The auction setting:
  - An auctioneer interested in selling a non-divisible item
  - We have n interested users

Revisiting: First-price Auction

- The auction setting:
  - An auctioneer interested in selling a non-divisible item
  - We have n interested users
  - Each user has $i \in [n]$ has valuation $\theta_i \in \mathbb{R}_{\geq 0}$ for the item

EPFL

Revisiting: First-price Auction

- The auction setting:
  - An auctioneer interested in selling a non-divisible item
  - We have n interested users
  - Each user has $i \in [n]$ has valuation $\theta_i \in \mathbb{R}_{\geq 0}$ for the item
  - Each user submits their bid $b_i \in \mathbb{R}_{\geq 0}$

Revisiting: First-price Auction

- The auction setting:
  - An auctioneer interested in selling a non-divisible item
  - We have n interested users
  - Each user has $i \in [n]$ has valuation $\theta_i \in \mathbb{R}_{\geq 0}$ for the item
  - Each user submits their bid $b_i \in \mathbb{R}_{\geq 0}$
- First-price auction (FPA):

EPFL

Revisiting: First-price Auction

- The auction setting:
  - An auctioneer interested in selling a non-divisible item
  - We have n interested users
  - Each user has $i \in [n]$ has valuation $\theta_i \in \mathbb{R}_{\geq 0}$ for the item
  - Each user submits their bid $b_i \in \mathbb{R}_{\geq 0}$
- First-price auction (FPA):
  - **Allocation:** The auctioneer gives the highest bidder the item

Revisiting: First-price Auction

- The auction setting:
  - An auctioneer interested in selling a non-divisible item
  - We have n interested users
  - Each user has $i \in [n]$ has valuation $\theta_i \in \mathbb{R}_{\geq 0}$ for the item
  - Each user submits their bid $b_i \in \mathbb{R}_{\geq 0}$
- First-price auction (FPA):
  - **Allocation:** The auctioneer gives the highest bidder the item
  - **Payment:** You pay what you bid!

EPFL

Revisiting: First-price Auction

- The auction setting:
  - An auctioneer interested in selling a non-divisible item
  - We have n interested users
  - Each user has $i \in [n]$ has valuation $\theta_i \in \mathbb{R}_{\geq 0}$ for the item
  - Each user submits their bid $b_i \in \mathbb{R}_{\geq 0}$
- First-price auction (FPA):
  - **Allocation:** The auctioneer gives the highest bidder the item
  - **Payment:** You pay what you bid!
  - The winning user i pays b_i, the others zero!

Revisting: Second-price Auction

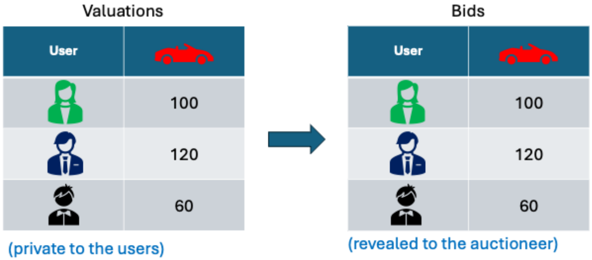
- The auction setting:
  - An auctioneer interested in selling a non-divisible item
  - We have n interested users
  - Each user has $i \in [n]$ has valuation $\theta_i \in \mathbb{R}_{\geq 0}$ for the item
  - Each user submits their bid $b_i \in \mathbb{R}_{\geq 0}$
  - W.l.o.g., assume that the bids are sorted: $b_1, \ldots, b_n$

EPFL

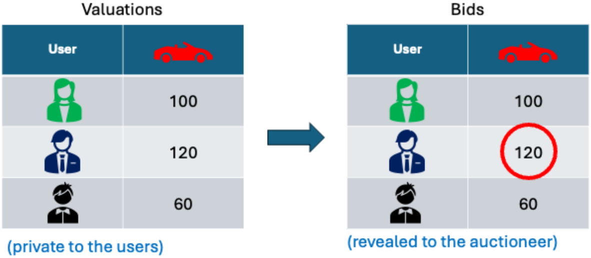
Revisting: Second-price Auction

- The auction setting:
  - An auctioneer interested in selling a non-divisible item
  - We have n interested users
  - Each user has $i \in [n]$ has valuation $\theta_i \in \mathbb{R}_{\geq 0}$ for the item
  - Each user submits their bid $b_i \in \mathbb{R}_{\geq 0}$
  - W.l.o.g., assume that the bids are sorted: $b_1, \ldots, b_n$
- Second-price auction (SPA):
  - **Allocation:** The auctioneer gives the highest bidder (b_1) the item
  - **Payment:** The winning user pays the highest losing bid!
  - The winning user pays b_2, the others zero!

Is Truthful Bidding Incentivized?



Is Truthful Bidding Incentivized?



First-price Auction: wins and pays 120! Utility: $\theta - p \Rightarrow 0$

Second-price Auction: wins and pays 100! Utility: $\theta - p \Rightarrow 20$

EPFL

Is Truthful Bidding Incentivized?

Valuations

User	
	100
	120
	60

(private to the users)

Bids

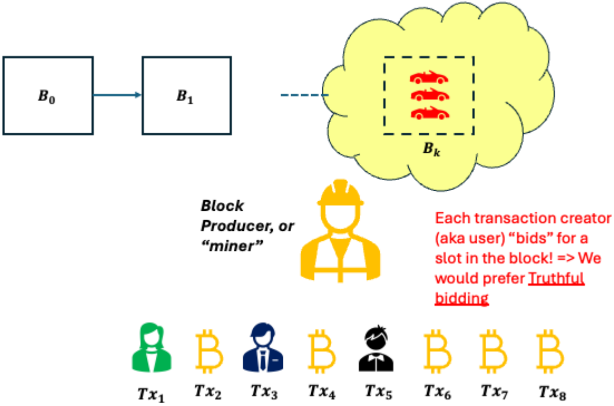
User	
	100
	$100 + \epsilon$
	60

(revealed to the auctioneer)

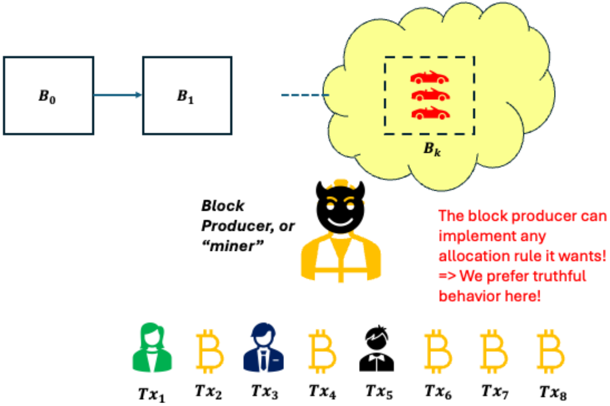
First-price Auction: wins and pays $100 + \epsilon$! Utility: $\theta - p \Rightarrow 20 - \epsilon$

Second-price Auction: wins and pays 100! Utility: $\theta - p \Rightarrow 20$

Bitcoin Implements a First-price Auction



Bitcoin Implements a First-price Auction



EPFL

Defining a TFM and Incentive Properties

TFMs

Definition (Transaction Fee Mechanism [6])

Given the blockchain history $\mathbf{H}$ and the set of outstanding transactions $M = \{b_1, \ldots, b_n\}$, a TFM is defined by the tuple $\tau = \langle \mathbf{x}, \mathbf{p}, \mathbf{q} \rangle$ where:

1. **Allocation Rule (x).** For each $b_t \in M$, $x_t = 1$ if $t \in B_k$, otherwise zero. The allocation rule is *feasible* if: $\sum_{t \in M} s_t \cdot x_t(\mathbf{H}, M) \leq C$
2. **Payment Rule (p).** Each $t \in B_k$ pays $p_t(\mathbf{H}, B_k)$, others zero.
3. **Burning Rule (q).** Each $t \in B_k$ burns $q_t(\mathbf{H}, B_k)$, others zero.

TFMs: FPA and SPA Revisited

First-price Auction:

- Allocation Rule: Feasible **x** such that $\sum_{t \in M} s_t \cdot x_t \cdot b_t$ is maximized
- Payment Rule: For all $t \in B_k$, $p_t(\cdot) = b_t$
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = 0$

EPFL

TFMs: FPA and SPA Revisited

First-price Auction:

- Allocation Rule: Feasible $\mathbf{x}$ such that $\sum_{t \in M} s_t \cdot x_t \cdot b_t$ is maximized
- Payment Rule: For all $t \in B_k$, $p_t(\cdot) = b_t$
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = 0$

Second-price Auction:

- Allocation Rule: Feasible $\mathbf{x}$ such that $\sum_{t \in M} s_t \cdot x_t \cdot b_t$ is maximized
- Payment Rule: For all $t \in B_k$, pay the highest losing bid (e.g., b_{k+1} is transactions are of the same size)
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = 0$

EPFL

TFMs: FPA and SPA Revisited

First-price Auction:

- Allocation Rule: Feasible $\mathbf{x}$ such that $\sum_{t \in M} s_t \cdot x_t \cdot b_t$ is maximized
- Payment Rule: For all $t \in B_k$, $p_t(\cdot) = b_t$
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = 0$

EPFL

TFMs: FPA and SPA Revisited

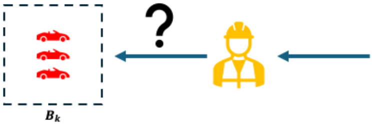
First-price Auction:

- Allocation Rule: Feasible $\mathbf{x}$ such that $\sum_{t \in M} s_t \cdot x_t \cdot b_t$ is maximized
- Payment Rule: For all $t \in B_k$, $p_t(\cdot) = b_t$
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = 0$

Second-price Auction:

- Allocation Rule: Feasible $\mathbf{x}$ such that $\sum_{t \in M} s_t \cdot x_t \cdot b_t$ is maximized
- Payment Rule: For all $t \in B_k$, pay the lowest winning bid
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = 0$

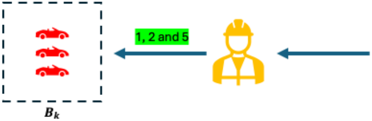
Example



User	Valuation (private)	Tx Fee (revealed)
1	30	30
2	120	120
3	20	20
4	10	10
5	140	140

Available Transactions

Example



User	Valuation (private)	Tx Fee (revealed)
1	30	30
2	120	120
3	20	20
4	10	10
5	140	140

Available Transactions

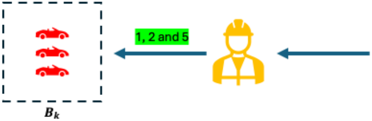
First-price Auction as a TFM:

1. Block producer's revenue = $30 + 120 + 140 = 290$

2. User's utility :
   - User 1: $30 - 30 = 0$
   - User 2: $120 - 120 = 0$
   - User 5: $140 - 140 = 0$

EPFL

Example



User	Valuation (private)	Tx Fee (revealed)
1	30	30
2	120	120
3	20	20
4	10	10
5	140	140

Available Transactions

First-price Auction as a TFM:

1. Block producer's revenue =
$30 + 120 + 140 = 290$

2. User's utility :
- **User 1: 30 – 30 = 0**
- **User 2: 120 – 120 = 0**
- **User 5: 140 – 140 = 0**

Second-price Auction as a TFM:

1. Block producer's revenue =
$30 + 30 + 30 = 90$

2. User's utility :
- **User 1: 30 – 30 = 0**
- **User 2: 120 – 30 = 90**
- **User 5: 140 – 30 = 100**

30 is the lowest winning bid!

EPFL

Utilities

- Users: Each user's $t \in M$ utility is, if $x_t = 1$ is:

$$u_t(b_t) = (\theta_t - p_t(\cdot) - q_t(\cdot)) \cdot s_t$$

and zero otherwise.

Utilities

- Users: Each user's $t \in M$ utility is, if $x_t = 1$ is:

$$u_t(b_t) = (\theta_t - p_t(\cdot) - q_t(\cdot)) \cdot s_t$$

  and zero otherwise.
- Miner: Block B_k's miner receives with "F" as the set of fake transactions such that $B_k \subseteq M \cup F$:

$$u(F, B_k) = \sum_{t \in B_k \cap M} p_t \cdot s_t - \sum_{t \in B_k \cap F} q_t \cdot s_t$$

EPFL

Can Block Producers Earn More with Fake Txs?

User	Valuation (private)	Tx Fee (revealed)
1	30	30
2	120	120
3	20	20
4	10	10
5	140	140
6 (fake)	0	110

Available Transactions

110 is the NEW lowest winning bid!

First-price Auction as a TFM:

1. Block producer's revenue = 120 + 140 = 260 (!!!)
2. User's utility:
   - User 2: 120 − 120 = 0
   - User 5: 140 − 140 = 0

Second-price Auction as a TFM:

1. Block producer's revenue = 110 + 110 = 220 (!!!)
2. User's utility:
   - User 2: 120 − 110 = 10
   - User 5: 140 − 110 = 30

TFMs: Incentive Properties

Definition (User Incentive Compatibility (UIC) [6])

A TFM $\tau = \langle \mathbf{x}, \mathbf{p}, \mathbf{q} \rangle$ is UIC if bidding truthfully is the best response for each user $t \in M$, irrespective of the other users' response:

$$u_t(\theta_t) \geq u_t(b_t), \forall b_t$$

Definition (Miner Incentive Compatibility (MIC) [6])

A TFM $\tau = \langle \mathbf{x}, \mathbf{p}, \mathbf{q} \rangle$ is MIC if the miner maximizes its utility (i) by following $\mathbf{x}$ the miner and (ii) setting $F = \emptyset$.

TFMs: Are FPA and SPA Any Good?

Mechanism	UIC	MIC
FPA		
SPA		

TFMs: Are FPA and SPA Any Good?

Mechanism	UIC	MIC
FPA	✗	✓
SPA	✓*	✗

TFMs: Incentive Properties

Definition (Off-chain Collusion Proofness (OCAP) [6])

A TFM $\tau = \langle \mathbf{x}, \mathbf{p}, \mathbf{q} \rangle$ is OCAP, if no *off-chain agreement* between users $T \subseteq M$ and the miner pareto-improves the canonical on-chain outcome.

TFMs: Are FPA and SPA Any Good?

Mechanism	UIC	MIC	OCAP
FPA	✗	✓	✓
SPA	✓*	✗	✓

[1]

[1] Proofs: [6]

What about a Posted-price Auction?

Posted-price Auction (PPA):

- Allocation Rule: Feasible $\mathbf{x}$ such that $\sum_{t \in M, b_t \geq b^\star} s_t \cdot x_t \cdot (b_t - b^\star)$ is maximized
- Payment Rule: For all $t \in B_k$, $p_t = b^\star$, where $b^\star$ is public
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = 0$

[2] Proofs: [3]

What about a Posted-price Auction?

Posted-price Auction (PPA):

- Allocation Rule: Feasible $\mathbf{x}$ such that $\sum_{t \in M, b_t \geq b^\star} s_t \cdot x_t \cdot (b_t - b^\star)$ is maximized
- Payment Rule: For all $t \in B_k$, $p_t = b^\star$, where $b^\star$ is public
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = 0$

Mechanism	UIC	MIC	OCAP
FPA	✗	✓	✓
SPA	✓*	✗	✓
PPA	✗	✓	✗

EPFL

[2] Proofs: [3]

What about a Posted-price Auction?

Posted-price Auction (PPA):

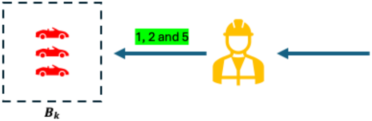
- Allocation Rule: Feasible $\mathbf{x}$ such that $\sum_{t \in M, b_t \geq b^\star} s_t \cdot x_t \cdot (b_t - b^\star)$ is maximized
- Payment Rule: For all $t \in B_k$, $p_t = b^\star$, where $b^\star$ is public
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = 0$

Mechanism	UIC	MIC	OCAP
FPA	✗	✓	✓
SPA	✓*	✗	✓
PPA	✗	✓	✗
PPA (Random $\mathbf{x}$)	?	?	?

[2]

[2] Proofs: [3]

Example



User	Valuation (private)	Tx Fee (revealed)
1	30	30
2	120	120
3	20	20
4	10	10
5	140	140

Available Transactions

Posted-price Auction as a TFM:

1. Block producer's revenue = 10 + 10 + 10 = 30

2. User's utility:

- **User 1: 30 – 10 = 20**
- **User 2: 120 – 10 = 110**
- **User 5: 140 – 10 = 130**

Let us say that the posted-price is 10!

EPFL

EIP-1559

EIP-1559: What is it?

EIP-1559[3]:

- Allocation Rule: Feasible $\mathbf{x}$ such that $\sum_{t \in M, b_t \geq b^\star} s_t \cdot x_t \cdot (b_t - b^\star)$ is maximized
- Payment Rule: For all $t \in B_k$, $p_t = (b_t - b^\star)$, where $b^\star$ is public
- Burning Rule: For all $t \in B_k$, $q_t(\cdot) = b^\star$

[3] https://eips.ethereum.org/EIPS/eip-1559

EIP-1559: How Good is it?

Mechanism	UIC	MIC	OCAP
FPA	✗	✓	✓
SPA	✓*	✗	✓
PPA	✗	✓	✗
EIP-1559			

EIP-1559: How Good is it?

Mechanism	UIC	MIC	OCAP
FPA	✗	✓	✓
SPA	✓*	✗	✓
PPA	✗	✓	✗
EIP-1559	✓‡	✓	✓

‡: When $b^\star$ is not excessively low

4

4 Proofs: [6]

Moving Forward

Current State-of-the-Art

- A “dream” TFM remains elusive

Current State-of-the-Art

- A "dream" TFM remains elusive
- Gafni and Yaish [4] fully characterize deterministic TFMs and show that only the trivial TFM – that never confirms any transaction – is UIC, MIC and OCAP

EPFL

Current State-of-the-Art

- A “dream” TFM remains elusive
- Gafni and Yaish [4] fully characterize deterministic TFMs and show that only the trivial TFM – that never confirms any transaction – is UIC, MIC and OCAP
- Chung and Shi [1] add a future cost to fake transaction to present a randomized TFM (based on the second-price auction) that is UIC, MIC and OCAP

EPFL

Current State-of-the-Art

- A "dream" TFM remains elusive
- Gafni and Yaish [4] fully characterize deterministic TFMs and show that only the trivial TFM – that never confirms any transaction – is UIC, MIC and OCAP
- Chung and Shi [1] add a future cost to fake transaction to present a randomized TFM (based on the second-price auction) that is UIC, MIC and OCAP
- Relaxations such as Bayesian IC have also been explored [8]

Current State-of-the-Art

- A "dream" TFM remains elusive
- Gafni and Yaish [4] fully characterize deterministic TFMs and show that only the trivial TFM – that never confirms any transaction – is UIC, MIC and OCAP
- Chung and Shi [1] add a future cost to fake transaction to present a randomized TFM (based on the second-price auction) that is UIC, MIC and OCAP
- Relaxations such as Bayesian IC have also been explored [8]
- Price of consumption [2]

Research Directions

- The current TFM modeling is limited
- User and block producers are assumed to be myopic
- The probability of a block producer producing a block is assumed to be constant
- Is block-space a private good?

Still Interested?

- Reach out: sankarshan.damle@epfl.ch

EPFL

References I

[1] Hao Chung and Elaine Shi. Foundations of transaction fee mechanism design. In *ACM-SIAM SODA*, pages 3856–3899, 2023.

[2] Sankarshan Damle, Manisha Padala, and Sujit Gujar. Designing redistribution mechanisms for reducing transaction fees in blockchains. In *Proceedings of the 23rd International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pages 416–424, 2024.

[3] Matheus V. X. Ferreira, Daniel J. Moroz, David C. Parkes, and Mitchell Stern. Dynamic posted-price mechanisms for the blockchain transaction-fee market. In *ACM Conference on Advances in Financial Technologies (AFT)*, pages 86–99, 2021.

[4] Yotam Gafni and Aviv Yaish. Barriers to collusion-resistant transaction fee mechanisms. *arXiv preprint arXiv:2402.08564*, 2024.

[5] Johnnatan Messias, Mohamed Alzayat, Balakrishnan Chandrasekaran, and Krishna P Gummadi. On blockchain commit times: An analysis of how miners choose bitcoin transactions. In *The Second International Workshop on Smart Data for Blockchain and Distributed Ledger (SDBD2020)*, 2020.

[6] Tim Roughgarden. Transaction fee mechanism design. In *ACM Conference on Economics and Computation (ACM EC)*, page 792, 2021.

References II

[7] Shoeb Siddiqui, Ganesh Vanahalli, and Sujit Gujar. Bitcoinf: Achieving fairness for bitcoin in transaction fee only model. In *AAMAS*, pages 2008–2010, 2020.

[8] Zishuo Zhao, Xi Chen, and Yuan Zhou. Bayesian-nash-incentive-compatible mechanism for blockchain transaction fee allocation. In *Crypto Economics Security Conference (CESC)*, 2022.