# REDESIGNING BITCOIN'S FEE MARKET arXiv:1709.08881


Ron Lavi - Technion

Aviv Zohar - Hebrew U.

Or Sattath Ben-Gurion U.


Scaling Bitcoin 2017

# CURRENT FEE MECHANISM IN BITCOIN

- Miners can only include txs that fit in at most 1MB.
- Pay what you bid: users specify the fees, and they pay it only if they are included in a block.
- Miner's inclusion strategy: include the highest transactions by their fee/byte that fit into 1MB.
- From now on we assume all txs are of the same size in bytes.

# WHAT IF HARDWARE PARAMETERS WEREN'T AN ISSUE?

- Suppose there are negligible block rewards, and the bandwidth, CPU and disk-space get a x100 boost. How should Bitcoin be changed?
- First guess: increase the block-size by a factor of 100.
- Economically risky – tragedy of the commons / race to the bottom:
  - Blocks are not full
  - Miners do not have incentives not to take ~0 fees.
  - Users decrease fees to ~0
  - <u>Revenue for the miners diminishes</u>
  - Double spending becomes very cheap

# DESIGN GOALS

- Increasing the block-size can decrease the miners' revenue
- In the long run, fees are the main income for the miners.
- Design goal: maximize the revenue for the miners. In particular, increasing the bandwidth etc. should increase the miner's revenue.
- The block size affects the security (orphaning rate, decentralization, etc.) and economic aspects (revenue for the miners).
- Design goal: decouple economic and security concerns.
- Design goal: a simple way for the user to decide on her fee.

# BITCOIN MINING AS AN AUCTION

- Bitcoin users willing to pay tx fees = Buyers
- Miner = Auctioneer (+seller)
- Auction theory standard assumptions: buyers do not collude & have strong identities, auctioneer is trusted (but not the seller), and the auction is conducted once.

# RESULTS: TWO BITCOIN FEE MECHANISMS

## RSOP MECHANISM

- Beautiful but not very useful
- Sensitive to miners' manipulation

## MONOPOLISTIC PRICE MECHANISM

- Not so beautiful, but more useful

# MONOPOLISTIC REVENUE & PRICE

- How to price an ebook, assuming you can't do price discrimination?
- Let $v_i$ denote the i'th user's valuation, where $v_1 \geq v_2 \geq \cdots v_n$.
- Monopolistic revenue: $R(v_1, \ldots, v_n) = \max_i v_i \cdot i$
- Monopolistic price: the price which maximizes the monopolistic revenue.

# MONOPOLISTIC REVENUE & PRICE: EXAMPLE

- Example: $v_1 = 3, v_2 = 2, v_3 = 1.$
- Monopolistic price = 2, Monopolistic revenue = 4.

# CHALLENGE: MANIPULATIONS

- A users bid $b_i$ may be different than her valuation (maximal willingness to pay) $v_i$.
- In Bitcoin, a user may place multiple bids – addressed in the manuscript, but not in the talk.

# RSOP AUCTION (Random Sampling Optimal Price)
Goldberg et al. 2006

A

$\cancel{p^{mon}(B) = 4}$

5

4

3

2

1

B

$\cancel{p^{mon}(A) = 2}$

# RSOP AUCTION (Random Sampling Optimal Price) Goldberg et al. 2006

- This auction is truthful: you loose nothing from setting $b_i \coloneqq v_i$ and encourages the users to reveal their true values.
- Reason: the offer price you are offered is determined by the choice of people in the other group.
- Revenue converges to the monopolistic price: for bounded range b,

$$\lim_{n\to\infty} \frac{R(b)}{RSOP(b)} = 1$$

# RSOP MECHANISM - BITCOIN

- Users specify a maximal fee (they may pay <u>less</u>).
- Miner include <u>all</u> mempool tx in their block.
- Block hash used to randomly partition the bids [*Bonneau-Clark-Goldfeder'15*].
- Only txs that "win" according to the RSOP auction are considered valid.
- 2 problems:
  - <u>Blocks are huge</u>: including all the transactions is unrealistic
  - <u>Prone to miners' manipulation:</u> Miners gain by including fake transactions / not including valid ones.

# MONOPOLISTIC PRICE MECHANISM

- Users specify a maximal fee (they may pay less).
- If a block contains transactions $b_1 \geq \cdots \geq b_m$, all users pay the minimal fee $b_m$.
- Miners are advised to include all txs that pay at least the monopolistic price, up to some upper bound on the block size.
- Definition: impatient users are only interested in being included in the next block (and have 0 utility from inclusion in later blocks).
- Caveat: our analysis assumes that users are impatient.
- Problem: Even impatient strategic users may gain (very) little by reporting $b_i \leq v_i$.
- Essentially, the manipulation decreases the monopolistic price.

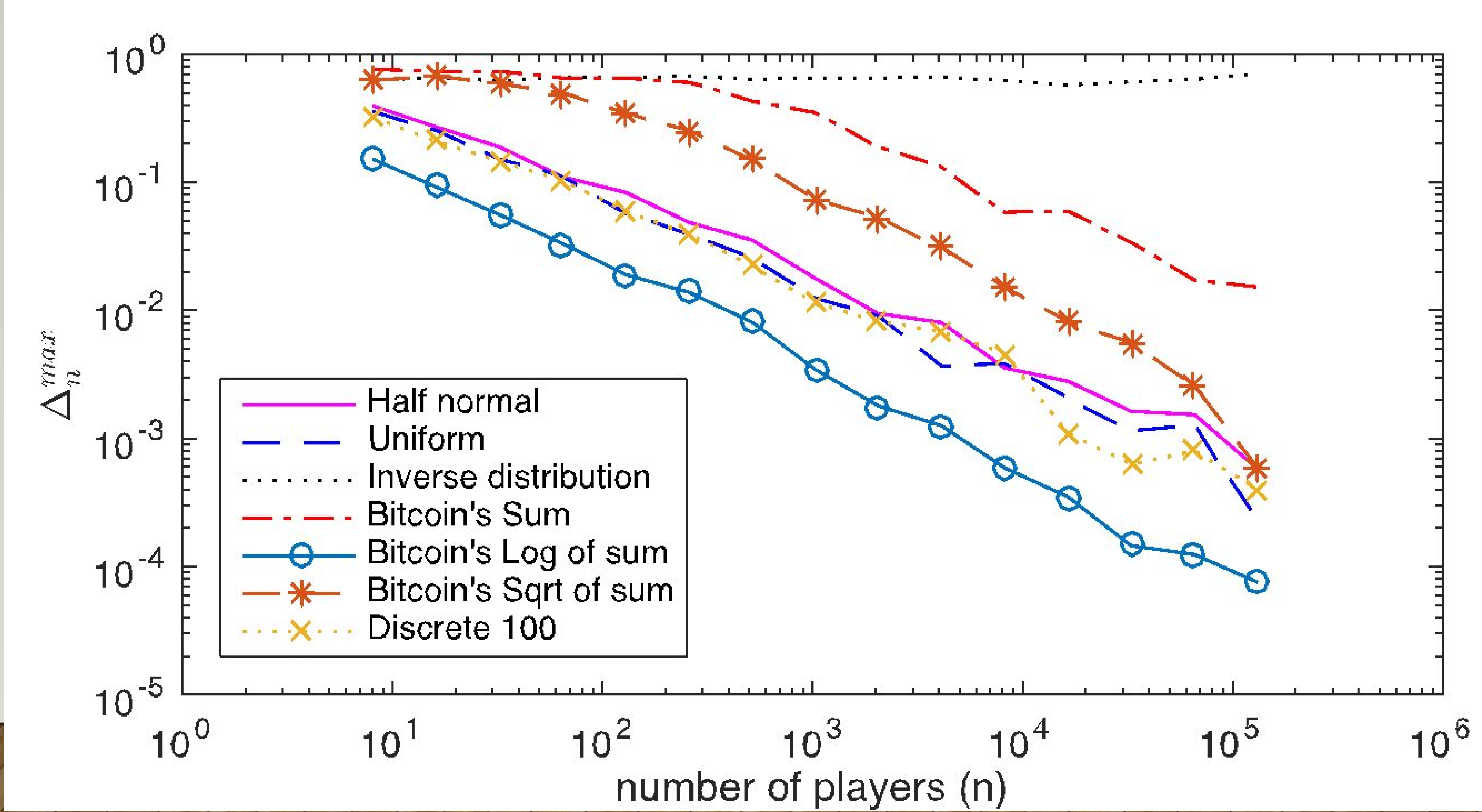
# MANIPULATING THE MONOPOLISTIC PRICE MECHANISM

- $p^{mon}(2.5,2,1) = 2.$
- $p^{mon}\left(\frac{2}{3} + \epsilon, 2,1\right) = \frac{2}{3} + \epsilon.$ ← Called the Strategic Price.
- Instead of paying 2, the first player pays ~2/3 – 66% discount!

# MONOPOLISTIC PRICE MECHANISM - MANIPULATIONS

- Theorem (informal): For any finite support users' valuation distribution, the worst discount ratio from a manipulation of a single player (assuming all others are honest), goes to 0 as the number of users grow.
- Concerns we evaluated empirically:
  - How fast does the manipulation ratio decreases?
  - What if the valuation distribution does not have finite support size?

# MONOPOLISTIC PRICE MECHANISM: EMPIRICAL RESULTS



# DISCUSSION & OPEN PROBLEMS

- How much security should the Bitcoin network “buy”? Are we buying too much / too little security in terms of hash-power?
- The current fee mechanism is not the most “natural” one
- How can we get real data on the “willingness to pay” for the fees? Important to understand how well this proposal would preform.
- An applicable RSOP mechanism?
- Bitcoin Dev. mailing list has an interesting discussion, also about implementation.

# THANK YOU!

# MULTI-BID STRATEGY

- Values: 5, 2, 1, 1.
- Everyone honest – first player wins, pays 5.
- If player two submits two bids with a value of 1, she gets in, everyone win and she pays two.
- Non-trivial: we show an efficient O(n) algorithm to find the optimal multi-bid strategy.
- <u>In practice, barely happens</u>: never happened during our simulations when number of users ≥ ~10.