A Truthful Profit-maximizing Bitcoin Fee Design

Computational Economics Final Report

Qian Xie
Institute of Interdisciplinary Information Sciences

Contents

1 Introduction

Satoshi Nakamoto introduced the Bitcoin system, a peer-to-peer electronic cash system, in 2008 [5]. Since then, both the industry and academia have made great efforts to improve the performance, consensus, privacy, security and functionality of the Bitcoin system and the broader concept Blockchain systems. Besides the fields of system, network, cryptography and distributed computing, game theory also provides an insight into the issues of Blockchain system, say selfish mining and the instability of Bitcoin without block reward. Recently, Ron Lavi, Or Sattath and Aviv Zohar [2] started a new direction of research, the design of Bitcoin Fee's market.

1.1 Bitcoin Fee Market

In the Bitcoin fee market, there are two kinds of players: users who have transactions needed to be validated and miners who create blocks to include the transactions. Each user declares the transaction fee he or she would like to pay and miners follow a mechanism to decide which transactions to include in the block. Bitcoin provides two kinds of incentives for miners: block reward and transaction fees. The block reward cuts to half every four years. Hence in the long term, transaction fees will become the main source of miners' income. Since the security of the Bitcoin system is ensured by the computational power invested by miners, it is essential to motivate miners participating in the system. Considering the security of the Bitcoin system as a kind of public good, Bitcoin fee market creates competition between users so that no one could be a free rider.

1.2 Desired Properties of Bitcoin Fee Mechanism

In [2], the authors listed some desired properties of a Bitcoin fee mechanism and pointed out that there can be conflict between them and they may not be satisfied simultaneously.

- **High social welfare.** Transactions with higher fees should be included before those with lower fees.
- **Revenue extraction.** The amount of fees transferred to the miners is high, which would buy more security for the system.
- **Truthful bidding.** The mechanism allows users to state their preferences clearly and encourage honest reporting.
- **No manipulation by users should be profitable.** Users have no incentive to split a single transaction into two transfers of smaller amounts, add more transactions between two bitcoin addresses of the same client, etc.
- **Resistance to manipulation by miners.** The mechanism is resistant to selfish behavior by the miners such as adding transactions of their own into their own blocks, withholding transactions and selecting other sets of transactions, etc.

Besides security, functionality is also an important aspect of the Bitcoin system. Therefore, if we regard the Bitcoin system as a To C Product or service, the following properties should also be considered.

- **Practicality.** It is not difficult to implement in the real-world system. Users can understand the mechanism and respond to it.
- **User engagement.** Users can tolerate the barriers to entry and they are willing to stay in the system. If the fee charge is too high, the users would vote with there feet and choose other systems.

1.3 Some Bitcoin Fee Designs

The following are some Bitcoin fee designs. The first one is the current Bitcoin fee mechanism. The second and the third one are the alternative auction based mechanisms introduced in [2].

- **Pay your bid.** The miner simply chooses the the transactions with highest bids to fill the capacity of the block. Included transactions always pay the amount they proposed.
- **Monopolistic Price.** The miner chooses the number of accepted transactions in the block, then all transactions pay exactly the smallest bid included in the block.
- **Random Sampling Optimal Price.** The transactions in each block are partitioned to two sets using a random assignment. For each set, only transactions that bid higher than the monopolistic price in the complementary set are accepted, and all pay that monopolistic price.

In [2] and [6], the authors have discussed some properties of those Bitcoin fee designs.

- **Pay your bid.** It does not extract revenue well when the block is not crowded. As the block size increases, revenue from transactions may decrease.
- **Monopolistic Price.** It extracts revenue better than "pay your bid" but not incentive compatible (IC) in the strict sense. Bid shading can be profitable, that is, the users may wish to bid lower than his or her true evaluation. The Multiple Strategic Bids (MSB) attack is also likely. However, the mechanism is nearly-IC for general i.i.d. distributions and holds true against MSB attack. The miners as auctioneers are also incentivized to follow the protocol.
- **Random Sampling Optimal Price.** It is truthful, so users are encouraged to simply reveal their true preferences, that is, the transaction fees they are willing to pay. However, its revenue is always dominated by Monopolistic Price revenue.

Considering the property of user engagement, I suggest a simple Bitcoin fee design here.

- **Discounted Price.** A user can pay a discounted transaction fee (or the probability that the transaction be included is increased) the first few times he or she participates in the system. As the participation gets higher, the transaction fee can also go lower.

1.4 Similarity and Difference Between Bitcoin Fee Market and Digital Goods Market

The Random Sampling Optimal Price mechanism was first defined by Goldberg et al. [1] in the digital goods context where the items are in unlimited supply. The Monopolistic Price mechanism is actually the optimal single price omniscient auction introduced in [1]. We can borrow ideas from the study of auctions for digital goods. But there are also notable differences between Bitcoin Fee Market and Digital Goods Market.

- **Auctioneer Honesty.** The miner (auctioneer) may delete or insert bids.
- **Multiple Strategic Bids Attack.** The users may split a bid to several transactions with several bids.

2 A New Bitcoin Fee Design

In this section, I will introduce a new Bitcoin fee design inspired from [3] that satisfies some of the desired properties mentioned in 1.2.

2.1 Unparameterized Profit-maximizing Auction Design

When the distribution of valuations is known or can be obtained by statistical means, VCG mechanism with a proper reserved price such as Myerson's auction [4] can achieve very tight bounds on the expected profits.

When the auction mechanism does not have any knowledge of bidders' valuations, there are two problems. First, determining the prior distribution in advance may not be possible or convenient. Second, calculating and setting a new reservation price for each one may be infeasible or inconvenient.

We can assume that the Bitcoin fee market is an unknown market without full knowledge of the valuation distributions. A space in a block is similar to a copy of an item to be sold.

2.2 Randomized Truthful Profit-maximizing Mechanism

Assume that there are n users each with his or her transactions. Each transaction includes a bid (the fee that the user is willing to pay). The bids are denoted as $b_1 \geq b_2 \geq \cdots b_n \geq 1$. If there are bids below 1, we can multiply all bids with a constant factor to scale them. A miner constructing the block chooses transactions to be included in the block. A block can contain c transactions. Since there is no difference between the case $c > n$ and the case $c = n$, we can assume that $c \leq n$.

2.3 Evaluation

- **Manipulation by miners.** Yes. The miner can add a fake transaction with bid slightly below b_c, then with probability $1 - \delta$, his profit increases nearly $c(b_c - b_{c+1})$,

Algorithm 1 Randomized Truthful Profit-maximizing Mechanism

Data: $k \in \mathbb{Z}^+$, $\epsilon > 0$, and $\delta > 0$. The bids of all users $\mathbf{b} = (b_1, b_2, \cdots, b_n)$ where $b_1 \geq b_2 \geq \cdots \geq b_n$. The number of transactions a block can contain $c \leq n$.

Result: The transactions be included and the prices they pay.

1. If $c = n$, set $b_{n+1} = 1$.
2. With probability $1 - \delta$, the c transactions with highest bids are chosen to be included in the block and each pay b_{c+1}.
3. With probability δ, the c transactions with highest bids are chosen to be included in the block and each pays a reserved price $r \in [b_{c+1}, \infty]$ according to the distribution with density $f_{k,\epsilon,b_{c+1}}(x)$ defined in [3].

and with probability δ, his or her profit remains.

- **Bid shading.** No. Universally truthfulness assured by [3].
- **Revenue extraction.** An expected profit of $\Omega(\frac{OPT}{\ln OPT \ln\ln OPT \cdots (\ln^{(k)} OPT)^{1+\epsilon}})$ is guaranteed where OPT is maximal social utility of the auction [3], and no truthful auction can guarantee that expected profit which means Random Sampling Optimal Price is not better than this mechanism in terms of revenue extraction.
- **Multiple Strategic Bids Attack.** No, under assumption of impatient users.
  Proof. Suppose a bidder b_i would like to split his or her bid to $b_i = s + t$ $(i \leq c)$. To avoid losing transactions, s and y must among the c highest bids. Hence $s \geq b_c$, $t \geq b_c$.
  Now with probability $1 - \delta$, according to the VCG mechanism, the bidder has to pay $2b_c > b_{c+1}$; with probability δ, according to the reserved price mechanism, the expected price the bidder has to pay is

$$\int_{b_c}^{s} xg(x)dx + \int_{b_c}^{t} xg(x)dx \geq \int_{b_{c+1}}^{b_i} xf(x)dx$$

  where $g(x) = f_{k,\epsilon,b_c}(x)$ and $f(x) = f_{k,\epsilon,b_{c+1}}(x)$. For simplicity, let $k = 1, \epsilon = 1$, then $g(x) = \frac{1}{x \ln(\frac{x}{b_c}+1)^2}$ and $f(x) = \frac{1}{x \ln(\frac{x}{b_{c+1}}+1)^2}$. Note that

$$\int \frac{1}{\ln(\frac{x}{b}+1)^2} dx = \frac{bEi(\log \frac{x}{b} + 1)}{e} - \frac{x}{\log \frac{x}{b} + 1} + C.$$

  Therefore, the bidder would either lose transactions or pay more, he or she has no incentive to split the bid.

3 Conclusion

In this paper, I suggest some new desired properties of Bitcoin fee mechanism and a simple Discounted Price mechanism that satisfies them. Considering Bitcoin fee market as an unknown market without full knowledge of the valuation distributions, I also propose an unparametrized truthful profit-maximizing mechanism that can extract more revenue than Random Sampling Optimal Price mechanism do and resist to bid shading and multiple strategic bids attack that Monopolistic Price mechanism can not.

References

[1] A. V. Goldberg, J. D. Hartline, A. R. Karlin, M. Saks, and A. Wright. Competitive auctions. *Games and Economic Behavior*, 55(2):242–269, 2006.

[2] R. Lavi, O. Sattath, and A. Zohar. Redesigning bitcoin's fee market. *arXiv preprint arXiv:1709.08881*, 2017.

[3] P. Lu, S.-H. Teng, and C. Yu. Truthful auctions with optimal profit. In *International Workshop on Internet and Network Economics*, pages 27–36. Springer, 2006.

[4] R. B. Myerson. Optimal auction design. *Mathematics of operations research*, 6(1):58–73, 1981.

[5] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[6] A. C.-C. Yao. An incentive analysis of some bitcoin fee design. *arXiv preprint arXiv:1811.02351*, 2018.