# Towards Overcoming the Undercutting Problem

Tiantian Gong[1] (✉), Mohsen Minaei[2⋆], Wenhai Sun[1], and Aniket Kate[1]

[1] Purdue University, West Lafayette, USA,
{tg, sun841, aniket}@purdue.edu
[2] Visa Research, Palo Alto, USA,
mominaei@visa.com

**Abstract.** Mining processes of Bitcoin and similar cryptocurrencies are currently incentivized with voluntary transaction fees and fixed block rewards which will halve gradually to zero. In the setting where optional and arbitrary transaction fee becomes the prominent/remaining incentive, Carlsten et al. [CCS 2016] find that an undercutting attack can become the equilibrium strategy for miners. In undercutting, the attacker deliberately forks an existing chain by leaving wealthy transactions unclaimed to attract petty complaint miners to its fork. We observe that two simplifying assumptions in [CCS 2016] of fees arriving at fixed rates and miners collecting *all* accumulated fees regardless of block size limit are often infeasible in practice and find that they are inaccurately inflating the profitability of undercutting. Studying Bitcoin and Monero blockchain data, we find that the fees deliberately left out by an undercutter may not be attractive to other miners (hence to the attacker itself): the deliberately left out transactions may not fit into a new block without "squeezing out" some other to-be transactions, and thus claimable fees in the next round cannot be raised arbitrarily.

This work views undercutting and shifting among chains rationally as mining strategies of rational miners. We model profitability of undercutting strategy with block size limit present, which bounds the claimable fees in a round and gives rise to a pending (cushion) transaction set. In the proposed model, we first identify the conditions necessary to make undercutting profitable. We then present an easy-to-deploy defense against undercutting by selectively assembling transactions into the new block to invalidate the identified conditions. Indeed, under a typical setting with undercutters present, applying this avoidance technique is a Nash Equilibrium. Finally, we complement the above analytical results with an experimental analysis using both artificial data of normally distributed fee rates and actual transactions in Bitcoin and Monero.

**Keywords:** Bitcoin incentive scheme · Undercutting · Game theory

## 1 Introduction

Bitcoin network [19] and several cryptocurrencies rely on nodes participating in transaction verification, ordering and execution, and mining new blocks for their

⋆ Part of this work was done while the author was at Purdue University.

security and performance. Specifically, with honest majority, Byzantine-fault tolerant consensus is possible with Proof of Work (PoW) assuming network synchrony. With honest majority, attacks like double spending [23] are also harder to implement in practice. Additionally, with more honest computing peers, liveness is provided with a higher probability. A proper incentive design helps attract more honest parties to join. Bitcoin currently incentivizes nodes (or miners) with fixed block rewards and voluntary transaction fees. Historically, the block reward has been the dominating source of miners' revenues. However, for Bitcoin, it is a system parameter that halves approximately every four years.[3] Its domination is expected to vanish due to the deteriorating nature and transaction fees will then become the major mining revenue generator.

With a stable reward, a miner's expected revenues rely mostly on its probability of finding a block, which itself is contingent on the miner's hash power. However, in the fee-based incentive system, the revenues additionally depend on the fee amount inside a block, which further relies on users' offerings and miners' transaction selections. The total fees inside blocks are market-dependent and time-variant because (i) transaction arrival can be arbitrary; (ii) transaction fees are voluntary under the current mechanism, so they can be arbitrary (even 0) and the threshold fee rates for faster confirmation change with supply and demand in the block space market; (iii) miners have the freedom of sampling transactions to form new blocks. As a result, the fair sharing of revenue based on hashing power may not be maintained. For example, consider two miners $A$ and $B$ in the system with the same mining power. If $A$ mines blocks each with total fees of 1 BTC and $B$ always encounters wealthy transactions and mines blocks each with 2 BTC total fees, $B$'s revenue is twice $A$'s revenue.

In particular, the fee-based incentivization framework nurtures a possible new deviating mining strategy called undercutting [4]. In undercutting, the attacker intentionally forks an existing chain by leaving wealthier transactions out in its new block to attract other (petty compliant) miners to join the fork. Unlike honest miners, who follow the longest chain that appears first, petty compliant (PC) miners break ties by selecting the chain that leaves out the most fees. In [4], fees accumulate at a fixed rate and miners claim *all* accumulated fees when creating a new block. Thus, a miner undercuts another miner's block because it receives 0 of the fees in the target block but expects nonzero returns via forking. Similarly, PC miners join the fork because the undercutter leaves out more fees unclaimed (and they can claim *all* fees in the next block). Carlsten et al. find that undercutting can become the equilibrium strategy for miners, thus making the system unstable as miners undercut each other.

However, this result is based on a setting disregarding the block size limit. If the fees claimable in the next block are bounded and a pending transaction set exists due to the block size cap, PC miners may not join the fork and undercutting may not be more profitable than extending the current chain head. The intuition is that the extra claimable fees are bounded, and the fork does not win with absolute probability, while the main chain may provide slightly fewer fees

[3] The next halving event to 3.125 BTC is scheduled for May 2024. [10]

but extends with probability 1 when there's no attack. We give an illustrative example below where undercutting is not rational when we consider the limit. Let there be 33% honest, 17% undercutter, and 50% PC mining power, 100 total token fees with 20 claimable in each block. As we elaborate in the full version of this report [9], the undercutter expects 3.4 token returns by extending the chain head. Suppose it instead undercuts and claims half of the tokens in the target block, 10 tokens, in its first forking block (as in [4]). If PC miners do not shift, they expect 10 tokens from the next main-chain block; if they follow the fork, they expect to gain 10 tokens. But, shifting is not rational for the owner of the undercutting target block and may not be rational for others as they have started mining the main chain for some time. Even if they shift, we find the undercutter's expected return to be $1.717 < 3.4$.

Towards modeling undercutting attacks more realistically and generally, we construct a new model to capture rational behaviors related to and performance of the undercutting strategy. Miners in our model are either honest or rational. A rational miner may **undercut** or **arbitrarily shift among chains** as long as the action maximizes its returns. Fees in our model arrive with transactions. By sorting transactions in the unconfirmed transaction set and packing at most a block size limit of transactions, we obtain the maximum claimable fees at a certain timestamp. Miners can choose to claim no more than this maximum fee.

Essentially, when undercutting, the rational miner's goal is to earn more than what it can potentially gain not undercutting. The attacker needs to first **(i)** attract other rational miners to join its fork if necessary, and second **(ii)** avoid being undercut by others. If it leaves out too many fees, it may end up being worse off undercutting. If it claims more than necessary, other rational miners may undercut its fork, annihilating its efforts. Then how many fees should an undercutter take to achieve both goals simultaneously? And can others make it not possible to do so? We seek to first locate such a feasible area for an undercutter to secure its premiums and next, uncover defenses against this attack. Note that undercutting is not desired because it hurts the expected profits for honest miners. Successful undercutting also harms users who attach high fee rates to have their transactions processed faster.

### 1.1 Contributions

We define an analytical model that captures behaviors that are "rational" but not necessarily "honest" like undercutting and shifting rationally. This can be used to analyze other rational deviating strategies in a fee-based incentive system. The key is to pinpoint reward distributions and probabilities of earning the rewards.

Specifically for undercutting and as a key contribution, we offer **closed-form conditions on the unconfirmed transaction set to make undercutting profitable**. The key quantity is the ratio ($\gamma$) between the maximum claimable fees in the next block (w.r.t. block size limit) and the fees in the current block. For clarity, let the mining power fraction of the undercutter be $\beta_u$ and that of the honest miner be $\beta_h$, remaining rational miner be $\beta_r$. **(i)** In the best case for the undercutter in our model, the undercutter forgoes the fork after being one block behind instead of hanging on longer. **(ii)** When $\gamma < \frac{a\beta_r+\beta_u}{1-\beta_u}$, the attacker can expect to earn a premium by proper undercutting. It should carefully craft the first block on its fork (deciding parameter $a$) in such a way that rational miners can be attracted to join the fork when needed but not tempted to undercut it again. We provide more details in Section 4. The conditions for the case where the undercutter holds on for one more block (Appendix A) are stricter, as noted in (i) and the overall expected returns are fewer.

As a side-product and naturally, we provide an **alternative transaction selection rule** to counter undercutting, other than fitting all available transactions into a block. Once we have identified effective conditions for profitable undercutting, we work backward to proactively check the conditions before creating a new block. By making the conditions no longer satisfied, potential undercutters are no longer motivated to undercut. Applying the defense technique is Nash equilibrium in a typical setting. In the equilibrium, we additionally calculate the price of anarchy (PoA) to capture the inefficiency a strong undercutter brings or the advantage it has in a system. To make the system more stable, we can either strengthen the second potential undercutter or weaken the strongest undercutter through decentralization.

We **experiment with real-world data** from Bitcoin and Monero blockchains to evaluate the profitability of undercutting and the effectiveness of avoidance techniques. We decide on the two systems because Bitcoin is representative of swamped blockchains and Monero typically has a small unconfirmed transaction set. **(i)** In Bitcoin, for a 17.6% undercutter, the average return is 17.9%. For a hypothetical 49.9% attacker, the average revenue is 60.8%. In Monero, we observe a profit increase of around 8 percentage points from fair shares for a 35% attacker. **(ii)** After enabling defense, undercutting generates around a fair share for Monero 35% undercutter where the two strongest rational miners possess the same mining powers. We test a strong undercutter's advantage in Bitcoin (49.9%, 20%), which gives the 49.9% attacker around 63.5% of the total returns.

### 1.2 Related Work

Carlsten et al. [4] introduce the undercutting mining strategy to show the instability of the future Bitcoin fee-based incentivization system because undercutting can become the equilibrium strategy. There, transaction fees accumulate at a constant rate and miners can include all fees when creating a new block. But fees essentially are *not* independent of transactions. If we dive into the transaction level and account for the block size limit, the fees one can claim are restricted and there can potentially be a large pending transaction set, which can cushion or even annihilate the effects of undercutting. Based on this intuition, we construct the new model focusing on transaction selection rules, which determine fees claimed and left out. Further, both undercutting and hopping among chains are modeled more generally as actions of rational miners instead of separately as two types of miners as in [4]. This helps quantify the profit margin and brings about opportunities for mitigation.

**Together with other non-compliant mining strategies.** There have already been rigorous discussions on attacks related to mining strategies. Most notable attacks are selfish mining [7,26,20], block withholding [22,17,5,16,6], and fork after withholding [13]. Defenses against these game-theoretic attacks have also been studied [11,28,21,14,15]. It is possible to combine undercutting with other mining strategies like selfish mining and block withholding. For the latter, because undercutters prefer larger mining power, the two attacks have opposite goals, so one needs to balance the computation resource allocation. Selfish mining purposely hides discovered blocks, while undercutting intends to publish a block and attract other miners. They do not share the same rationale, but we can schedule the two strategies and apply the one with higher expected returns at a certain time. In this work, we put our focus on the profitability and mitigation of undercutting, which affects the undercutting part of the strategy scheduler.

**Lemon Market.** Another angle to look at the problem on a higher level is through the market for "lemons" [2], the brand-new car that becomes defective the minute one bought it. In the Bitcoin block space market, users are bidders, and miners are sellers. Users decide prices to pay based on their observation of the relationship between confirmation time and fee rates. They attach fee rates corresponding to the desired waiting time. If undercutting is prevailing, users who attach high fee rates but are ghosted are provided with "lemons" instead of "peaches" – fast confirmation. This can result in a decrease in the overall fee rates, diminishing the profitability of undercutting.

## 2 Preliminaries

**Mempool.** Mempool [3] is an unconfirmed transaction set maintained by miners locally. When a transaction is announced to the network, it enters into miners' mempools. Miners select transactions from their mempools to form new blocks. Usually, a miner chooses the bandwidth set (Definition 1) with respect to the local mempool and global block size limit. An undercutting miner intentionally leaves out wealthy transactions when forming blocks to attract other rational miners. Wealthy transactions are those with high fee rates. When a new block is published, miners verify the block and then update their local mempools to exclude transactions included in the newly published block.

**Definition 1 (Bandwidth Set).** *Given block size limit $B$ and an unconfirmed transaction set $\mathbb{T}$ comprising $N$ transactions, $S^* \in P(\mathbb{T})$ is a bandwidth set of $\mathbb{T}$ with respect to $B$ if $S^*.size \leq B$ and $\forall S_i \in P(\mathbb{T})$ with $S_i.size \leq B, S^*.fee \geq S_i.fee$, where $P(\mathbb{T})$ is the power set of $\mathbb{T}$.*

*Remark 1.* A bandwidth set is a set of transactions in a miner's mempool providing the most fees a miner claimable in one block. If the unconfirmed transaction set is of size $\leq B$, then the bandwidth set is the memory pool itself. Note that the bandwidth set is not necessarily unique.

**Definition 2 (Safe margin).** *When a chain $C^*$ is $D$ block(s) ahead of competing chains, a miner with safe margin parameter $D$ always extends $C^*$.*

*Remark 2.* Honest miners apply the longest chain rule and always have $D = 1$.[4] For rational miners, $D \geq 1$. When the length discrepancy between competing chains is within $D$, they select the chain with the most expected returns.

## 3 Mining Game featuring Undercutting Strategy

In this section, we model the mining game involving the undercutting strategy. We consider honest miners, who follow the default protocol specifications, and rational miners. The latter are addressed as undercutters when they undercut.

**Game definition.** We define the mining game $G = \langle M, A, R \rangle$ as follows:

- $n$ Players $M = \{M_0, M_1, ..., M_{n-1}\}$: without loss of generality, we label a subset of the miners that have a total of $\beta_h$ mining power as honest; we label a miner with $\beta_u$ mining power as the current undercutter under discussion; we label the remaining miners as (currently) non-undercutting rational miners and their total mining power is denoted as $\beta_r = 1 - \beta_h - \beta_u$. Honest miners are treated as one because they follow the same mining rules, and we assume they are informed the same way.
- Actions $A = \{undercut(\cdot), stay(\cdot), shift(\cdot)\}$: we index chains during a game according to their timestamps after the branching point, e.g. the original (main) chain with index $Chain_0$, abbreviated as $C_0$. Honest miners always honest mine and may choose to stay or shift depending on circumstances. Rational miners may choose to undercut an existing chain and start a new chain, stay on a working chain, or shift among existing chains.
- Utility functions $U = \{u_i\}_{M_i \in M}$: we let $u_i = R_i - c_i$, where $R_i$ is the total transaction fees it receives and $c_i$ is the cost. We treat the cost $c_i$ as fixed and reduce the problem of maximizing utility to maximization of obtained fees.

**Threat model.** We allow no miner to own more than 50% mining power (i.e., $\beta_u \leq 0.5$). We let miners publish their discovered blocks immediately to attract other miners to join. We assume the best case for the undercutter and let the mempool be the same for miners on the same chain. Because undercutting is not practical or meaningful if miners have distinct mempools, since wealthy transactions an attacker left unclaimed may not exist in others' mempools in the first place. This assumption makes the attacker stronger, and we intend to uncover what the attacker can obtain in advantageous environment settings.

We let miners know of other miners' types (e.g. honest or rational) after sufficient observations. We assume miners can approximate the amount of mining power concentrated on a chain based on the block generation time on that chain.

**Solution concept.** We solve for Nash Equilibrium (NE) in the mining game with undercutting mining strategy. In a Nash Equilibrium, players do not earn extra utility by unilaterally deviating from the equilibrium strategy.

[4] When there is a tie, they choose the chain with the oldest timestamp. If timestamps should be the same, they select a chain at random.

### 3.1 Miner's Winning Probability

A miner's expected returns from mining equal the product of its winning probability of a block and the fees residing in that block. Firstly, miner $M_i$'s winning probability of a block is simply its mining power when there is only one chain. In the case of competing chains, we need to additionally quantify a chain's winning probability when working in systems where only one chain survives.

**A chain's winning probability.** In undercutting, the attacker forks an existing chain by leaving out wealthy transactions. In the following discussions, we refer to the undercutting chain as $C_1$ and the current main chain as $C_0$. $C_0$ might not be on the main chain eventually if $C_1$ wins the race. The effective height of a chain is the number of blocks it has accumulated after the forking point. These competing blocks are called effective blocks in the game analysis.

Overall, the process proceeds as follows. The undercutter sees a new block is appended to $C_0$ by another miner. It starts to work on a forking block that excludes wealthy transactions appearing in the current chain head. With some probability, it can create the fork faster than the next block appearing on $C_0$. When the undercutter publishes its block, some rational miners consider shifting to $C_1$ because there are more high fee rate transactions that they can benefit from. To model this procedure, we screenshot the state of the system as a tuple that we denote as $\vec{S} = (m_0, m_1, \vec{F^0}, \vec{F^1}, O, \delta, \lambda_0, \lambda_1)$, where $m_0$ and $m_1$ are respectively the effective height of $C_0$ and $C_1$; $\vec{F^0}$ and $\vec{F^1}$ are the list of transaction fee total in effective blocks on $C_0$ and $C_1$; $O$ is the mining power currently working on $C_1$, which updates upon new block appending events; $\delta \in (-1, 1)$ is the mining power shifting from the source chain to the destination chain, which is defined to be positive if miners are shifting to $C_1$ and negative if they are shifting to $C_0$; $\lambda_0$ and $\lambda_1$ are block generation rates for $C_0$ and $C_1$.

To obtain the winning probability measure for a chain from state $\vec{S}$, we view the block generation event as a Poisson process and use a random variable to represent the waiting time between block occurrence events. We denote waiting time for $C_0$ as $X$ and $C_1$ as $Y$. They both follow exponential distribution but with different rates. The rate parameters depend on the mining power distribution. Given the state $\vec{S}$, we obtain the block occurrence rate as: $\lambda_0 = \frac{1-O}{I}$; and $\lambda_1 = \frac{O}{I}$, where $I$ is block generation interval (e.g. 10 minutes for Bitcoin). This is derived from the thinning theorem of the Poisson point process. The main idea is that independent sub-processes of a Poisson process are still Poisson processes with individual rates. With this property, we can determine the time interval for the next block to appear on a chain. Then, the key is the mining power concentrated on a chain, and further is whether honest and rational miners shift.

For $D = 1$, there is only one state that the currently non-undercutting rational miners $\beta_r$ need to make a decision, when the undercutter extends $C_1$ before the $C_0$ extends by one. The two competing chains are in a tie with relative height difference $\tilde{D} = 0$. The probability that $C_1$ wins is simply $p = \Pr[C_1\ Wins] = \Pr[Y < X] = O + \delta$.

For $D = 2$, there is an infinite number of states where flexible rational miners need to make decisions about shifting. We let $\tilde{D} = m_1 - m_0 < D$, denoting the number of blocks by which $C_1$ leads $C_0$. For example, when $\tilde{D} = -1$, $C_1$ is one block behind $C_0$. Then $C_1$ wins if it creates 3 blocks before $C_0$ extends by 1, or discovers 4 blocks before $C_0$ extends by 2, and so on. Thus, we have $p = \sum_{i=0}^{\infty} \Pr[(D - \tilde{D} + i)Y < (i+1)X]$.

**(i) When $\mathbf{\tilde{D} = -1}$**, $C_1$ is behind $C_0$. For $C_1$ to win, we need $p = \sum_{i=0}^{\infty} \Pr[(3+i)Y < (1+i)X] = \sum_{i=0}^{\infty} (\beta_u + \delta)^{3+i}(1 - \beta_u - \delta)^i$.

**(ii) When $\mathbf{\tilde{D} = 0}$**, there is a tie between $C_1$ and $C_0$. In this case, $p = \sum_{i=0}^{\infty} \Pr[(2+i)Y < (1+i)X] = \sum_{i=0}^{\infty} (\beta_u + \delta)^{2+i}(1 - \beta_u - \delta)^i$.

**(iii) When $\mathbf{\tilde{D} = 1}$**, $C_1$ is leading. We have $p = \sum_{i=0}^{\infty} \Pr[(1+i)Y < (1+i)X] = \sum_{i=0}^{\infty} (\beta_u + \delta)^{1+i}(1 - \beta_u - \delta)^i$.

**A miner's probability of winning a block.** Suppose a miner $M_i$ with $\beta_{M_i}$ mining power is mining on a chain $C_j$ with $\beta_{C_j}$ accumulated total mining power which has winning probability $p_{C_j}$. Then $M_i$'s winning probability is $\frac{\beta_{M_i}}{\beta_{C_j}} p_{C_j}$.

## 4 Game Analysis

We analyze the profitability of the undercutting strategy with parameter $D = 1$ in this section and continue the discussion with $D = 2$ in the full report, for which a summary resides in Appendix A. The latter generates fewer profits. We differentiate between scenarios with "abundant" and "limited" amounts of fees. The extreme case where there are only negligible fees claimable for a long period ("drought") is described in the full report.

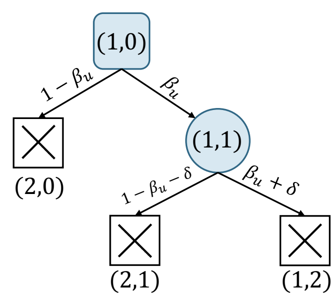



**Fig. 1:** State transition for $D = 1$. "X" Boxes are terminal states. For non-terminal states, circles indicate ties. Every left branch means $C_0$ extends by one and every right branch refers to $C_1$ creating a new block. The quantity on the arrow is the probability of state transition.

### 4.1 Giving Up If One Block Behind

We use the abbreviated state $S^* = (m_0, m_1)$ in discussion. We denote the transaction fees inside the first two blocks of $C_0$ as $F_1^0$ and $F_2^0$, the transaction fees inside blocks of $C_1$ as $F_1^1$ and $F_2^1$, the expected returns for flexible rational miners $\beta_r$ as $R_r$ and the expected returns for the undercutter as $R_u$. When there is no undercutting, we denote their respective expected return as $R_r'$ and $R_{\overline{u}}$.

For $D = 1$, rational miners only need to decide whether to shift at state $S^* = (1,1)$ when undercutting becomes visible as shown in Figure 1. Suppose they shift $x$ of their mining power $\beta_r$ to $C_1$. They can decide $x$ that gives $\max E[R_r]$:

$$\arg\max_{x\in[0,1]} \left(\mathbb{1}_{owner} \cdot (1-p) \cdot F_1^0 + \frac{(1-x)\beta_r}{\beta_h + (1-x)\beta_r}(1-p) \cdot F_2^0 + \frac{x\beta_r}{x\beta_r + \beta_u} p \cdot F_2^1\right) \quad (1)$$

where $p$ is the probability of $C_1$ winning and $\mathbb{1}_{owner}$ indicates whether a rational miner is the owner of the first block on chain 0. The shift can then be calculated as

$\delta = x\beta_r$. Observe that the optimization problem involves fees inside succeeding blocks after the forking point. We represent fees in a relative way for general interpretability: we let $F_1^0 = 1$ and have fee total in other blocks measured relative to it. Now we discuss two different mempool conditions.

**Mempools with limited bandwidth set** By "limited" we mean the current bandwidth set on $C_0$ has a small enough transaction fee total ($< \frac{\beta_u}{1-\beta_u} F_1^0$). We provide more details concerning this threshold as we proceed. WLOG, we assume $F_1^0 = 1$, $F_2^0 = \gamma \geq 0$ (s.t. $\frac{F_2^0}{F_1^0} = \gamma$), $F_1^1 = a$ and $F_2^1 = b$ where $a \in [0, 1]$. We can let $b = 1 + \gamma - a$, assuming the best case for the undercutter that it can compose the first block on $C_1$ in such a way that the second block can claim all unclaimed fees within one block. If a rational miner decides to undercut, with probability $\beta_u$, the undercutter can create a new chain and the game is started. In the remaining game, with probability $p = \beta_u + \delta$, $C_1$ wins and with probability $(1 - p)$, $C_0$ wins. The expected profit of the undercutter is

$$E[R_u] = \beta_u(\beta_u + \delta) \cdot (1 \cdot a + \frac{\beta_u}{\beta_u + \delta} \cdot (1 + \gamma - a))$$

The expected return for the rational miner if it does not undercut is $E[R_{\overline{u}}] = \beta_u \gamma$. The miner will undercut only if $E[R_{\overline{u}}] < E[R_u]$. Then

$$\gamma < \frac{\delta a + \beta_u}{1 - \beta_u} \tag{2}$$

With $\gamma < \frac{\beta_u}{1-\beta_u}$, $E[R_{\overline{u}}] < E[R_u]$ even when $\delta = 0$. That is, even no rational miner shifts to $C_1$, there are so few fees left in the mempool that the attacker is always better off by forking $C_0$ compared with extending it.

One extreme case is when there are no transactions left or the bandwidth set has negligible fees and $F_2^0 = 0$. The rational miner will fork because originally there is nothing left on $C_0$ and $E[R_{\overline{u}}] = 0$. One detail is that the attacker needs to craft the first block (determine $a$) it generates to avoid being undercut again. Suppose when $\gamma < T$ ($T = \frac{\beta_u}{1-\beta_u}$ in our current context), a potential undercutter initiates the attack. Then by choosing $a$ in such a way that $\frac{1+\gamma-a}{a} \geq T_2$ ($T_2 = \frac{\beta_{u_2}}{1-\beta_{u_2}}$ in the current context), the undercutter can avoid being undercut again. Note that here when an undercutter decides $a$, it is picturing a potential undercutter $\beta_{u_2}$ other than itself. We will revisit the choice of $a$ after complete the discussion for $\gamma > \frac{\beta_u}{1-\beta_u}$ case.

In conclusion, for $D = 1$, when the attacker is stronger ($\beta_u$ is larger), the requirements on the mempool bandwidth set fee total for undercutting to be profitable regardless of rational miners' actions is looser. When $\beta_u$ approximates 0.5, the threshold ratio approaches 1, which occurs with high frequency. For $\beta_u = 0.2$, the upper bound is 0.25, where the current bandwidth set is 1/4 of the fees inside the chain head of $C_0$.

**Mempools with sufficient bandwidth set** By "sufficient" we mean the current bandwidth set in the mempool has more than "limited" transaction fee total

($\geq \frac{\beta_u}{1-\beta_u} F_1^0$). In this case, the undercutter needs to attract some rational miners at state (1,1) (make $\delta > 0$). It's straightforward to verify that the owner of the undercutting target block is better off by staying on $C_0$. We treat this miner as honest in the following calculations and only make decisions for the remaining rational players. To decide whether to shift to $C_1$, rational miners solve for $x$ in

$$\arg\max_{x\in[0,1]} E[R_r] = \arg\max_{x\in[0,1]} \big(\frac{(1-x)\beta_r}{\beta_h + (1-x)\beta_r}(1-p)\gamma + \frac{x\beta_r}{x\beta_r + \beta_u} p(1+\gamma-a)\big)$$

Here $p = O + \delta = \beta_u + x\beta_r$. One observation is that the rational miners either move to $C_1$ with all their mining power or none (function is linear in $x$ after simplification). When $x = 1$, we have $E[R_{r|x=1}] = \beta_r(1+\gamma-a)$. Similarly, in setting $x = 0$, we obtain $E[R_{r|x=0}] = \beta_r\gamma$. To encourage shifting of rational miners, we need $E[R_{r|x=1}] > E[R_{r|x=0}]$, which means $a < 1$. To avoid being undercut, the undercutter additionally needs to pick an $a$ such that this condition is not satisfied for the first block on its $C_1$. This is to say the undercutter can profitably undercut $C_0$ in expectation, but others do not expect to attack its $C_1$ successfully. As previously touched on, we need

$$a \leq \frac{1+\bar{\gamma}}{1+T} = \frac{1+\bar{\gamma}}{1+\frac{a_2\beta_{r_2}+\beta_{u_2}}{1-\beta_{u_2}}}, a_2 \leq \frac{1+\bar{\gamma}'}{1+\frac{a\beta_r+\beta_u}{1-\beta_u}} \tag{3}$$

where $\beta_{u_2}$ is the mining power of the strongest potential undercutter for this attacker, $a_2$ is what this opponent would claim in the first block if he forks the undercutter's chain and $\beta_{r_2}, \beta_{h_2}$ is the remaining flexible rational mining power and honest mining power in that case. Here, $\bar{\gamma}, \bar{\gamma}'$ are the fee totals in the respective next bandwidth set measured relative to the respective current bandwidth set, when the strongest and second strongest undercutters are making the attack decisions. We can easily solve for $a$ and $a'$ numerically given assignments for mining power distributions and the mempool (for computing $\bar{\gamma}, \bar{\gamma}'$ from bandwidth sets). A program for this task can be found here [18].

In conclusion, for $D = 1$, the undercutter sets $a$, the fees to claim in the first block (measured relative to the fees in the target block), properly and undercut if $\gamma < \frac{a\beta_r+\beta_u}{1-\beta_u}$ for a potentially profitable attack. We say "potentially" because new transactions may arrive and change the bandwidth set, resulting in uncertainties in implementing undercutting. We summarize below the algorithm for $D = 1$.

**(Part 1)** A potential **undercutter** decides whether to undercut:
Compute $a$ numerically according to Inequalities 3 that maximizes $E[R_u]$ and check if $\gamma < \frac{a\beta_r+\beta_u}{1-\beta_u}$. If Yes, start undercutting.
**(Part 2) Flexible rational miners** decide mining resource distribution:
Solve for $x$ (proportion of resources to shift to the chain) in Equation 1.
**(Part 3) Miners** avoid being undercut:
Calculate the attack condition $T(= \frac{a\beta_r+\beta_u}{1-\beta_u})$ for the strongest undercutter a miner is defending against. Check if the current $\bar{\gamma} < T$. If Yes, include in the current block $< \frac{1+\bar{\gamma}}{1+T}$ of the fees in the bandwidth set; otherwise, use the bandwidth set.

**Treating rational miners as a whole.** In the above analysis, rational miners make decisions from a collective perspective by maximizing $E[R_r]$ instead of the expected returns for a specific rational miner. This can give rise to coordination problems. Fortunately, rational miners either move all their mining power or stay on their current chain. There is one scenario in practice when a rational miner may not be flexible, which is when this miner owns the current chain head of $C_0$. When a rational miner owns the $C_0$ head, as mentioned in the previous analysis, we treat it like honest miners. Since miners are aware of other miners' types across time, they will be able to adjust their reasoning process.

**When to apply undercutting avoidance.** Suppose the current bandwidth set contains fees of 1 and the remaining next bandwidth set contains fees of $\gamma$. The mempool is always sorted so $\gamma \leq 1$ (except when no transaction exists and $\gamma$ is not well-defined). Suppose we have computed the corresponding threshold attacking condition $T$ for a rational attacker and $\gamma < T$. Then this attacker undercuts if a miner simply assembles the current bandwidth set into a block or claims $\geq \frac{1+\gamma}{1+T}$ of the fees in the bandwidth set. We state the following theorem.

**Theorem 1.** *In setting $D = 1$, each miner applying avoidance procedure when creating a new block is NE.*

*Proof.* Let $M_i \in M$ be a miner with mining power $\beta_{M_i}$ and $M_i$ calculates $T = \frac{a\beta_r+\beta_u}{1-\beta_u}$. When $\gamma \geq T$, $M_i$ proceeds as normal. Therefore, we only need to show that for $M_i$, when $\gamma < T$, $M_i$ is better off by claiming $a < \frac{1+\gamma}{1+T}$ of the fees in bandwidth set. The key element here is that the decision of how many fees to claim in a block is decided before one successfully generates the proof of work. Let the current bandwidth set $BS_0$ have a fee total of 1, and we measure the expected returns relative to it. We denote $M_i$'s expected return from not applying avoidance as $E[R_{M_i}]$ and applying avoidance as $E[R_{M_i,avoid}]$.

It's straightforward to see that $E[R_{M_i,avoid}] = 1 \cdot \beta_{M_i} = \beta_{M_i}$ because the strongest and other rational miners do not undercut. $M_i$ can claim fees in the current bandwidth set $BS_0$ in different rounds. Each time, $M_i$ generates a successful proof of work with probability $\beta_{M_i}$.

If $M_i$ does not apply avoidance and claim all fees in $BS_0$, at least the strongest rational miner is incentivized to undercut given that $\gamma < T$. From previous analysis (see Figure 1 for a quick reference), we know that the undercutter wins with probability $\beta_u(\beta_u + \delta)$ where $0 \leq \delta \leq \beta_r - \beta_u$. Thus, $M_i$ can expect to gain profits $E[R_{M_i}] = 1 \cdot \beta_{M_i}(1 - \beta_u(\beta_u + \delta)) < E[R_{M_i,avoid}]$.

By unilaterally deviating from avoidance when $\gamma$ satisfies undercutting conditions of a potential undercutter, $M_i$ receives smaller expected returns. □

There are two special cases worth noting: (1) all miners are honest ($\beta_h = 1$) so that $T = 0$. We know that $\gamma \geq 0$. No effective avoidance is ever needed in this case; (2) $M_i$ is the only rational miner ($\beta_r = 0$) so that $T = 0$ for itself. $M_i$ does not need to apply avoidance since $\gamma \geq 0$.

**Quantifying Strong Undercutter's Advantage.** Let the strongest undercutter have mining power $\beta_u$ and the second strongest undercutter have mining power $\beta_{u_2}$. We know from the previous discussion that a miner should always apply avoidance techniques to avoid being undercut in our current setting. For miners other than the strongest undercutter $\beta_u$, they need to defend against $\beta_u$ while $\beta_u$ itself only needs to defend against $\beta_{u_2}$. Let $T, T'$ be the threshold ratio computed for $\beta_u$ and $\beta_{u_2}$ respectively. We can capture its advantage with the ratio $\frac{1+T}{1+T'}$. For example, if $\beta_u = 0.5, \beta_{u_2} = 0.2, \beta_h = 0$, $\frac{1+T}{1+T'} = 4$, which means that the strongest undercutter can claim 4 times than what the other miners are collecting each time. When the discrepancy between $\beta_u, \beta_{u_2}$ approaches 0, $\frac{1+T}{1+T'}$ approaches 1. More formally, we capture this inefficiency brought by selfish behavior with the price of anarchy (PoA) [12].

**Corollary 1 (Price of Anarchy).** *In setting $D = 1, \beta_h < 1, \beta_r > 0$, with the strongest and the second-strongest undercutters respectively having mining power $\beta_u, \beta_{u_2}$, the Price of Anarchy is $PoA = \frac{1+T}{(T-T')\beta_u+1+T'}$, where $T, T'$ are as defined above.*

This follows from the above analysis. When all miners stay honest, the "undercutter" is expected to earn a fair share $\beta_u$. When miners apply avoidance, the strongest undercutter claims $\frac{1+\gamma}{1+T'}$ each time while others claim $\frac{1+\gamma}{1+T}$. We can obtain its share $\frac{\beta_u \frac{1+\gamma}{1+T'}}{\beta_u \frac{1+\gamma}{1+T'} + (1-\beta_u)\frac{1+\gamma}{1+T}}$. Then we can calculate the PoA as the ratio between the strongest undercutter's shares in its optimal situation (the worst-case NE for the system) and in its worst case (the optimal all honest outcome). We do not include other miners' returns in the calculation because the total shares always sum up to 1 regardless of the outcome and our focus is on capturing the advantage of the undercutter. To give a demonstrative example, let $\beta_u = 0.499, \beta_{u_2} = 0.176$ and $\beta_h \in \{0, 0.05, 0.10, \dots, 0.30\}$, on average (over $\beta_h$) $T = 1.30, T' = 0.29$ and $PoA = 1.29$. This means that for $\beta_u$, the mean revenue proportion from undercutting is $0.499 \times 1.29 = 0.63$.

One observation is that when $\beta_u$ and $T - T'$ are large, PoA is large. To move it towards 1 (a more stable system), we can either strengthen the second potential undercutter or downsize $\beta_u$ through further decentralization.

## 5 System Evaluation

In this section, we evaluate the profitability of undercutting using data obtained from Bitcoin and Monero, along with artificial transactions generated from normal distributions. Bitcoin is a typical example of congested blockchains, and Monero is a more available one. The simulation codes and a sample data set have been made open source [18]. In the previous analysis, we let the undercutter be aware of future transaction flows in and out of the mempool. In reality, there is more uncertainty involved. Another difference is that now mining powers are discrete, and we model each miner individually.

### 5.1 Data Collection and Experiment Setup

**Transactions.** We obtain the blocks from height $630,457$ (May 15th, 2020 after the Bitcoin's block reward halving) to $634,928$ (June 15th, 2020) from the Bitcoin blockchain using the API provided by blockchain.com [24], comprising $9,167,040$ transactions. The Monero blockchain data are collected using a similar API from `xmrchain.net`. In total, we acquire $1,482,296$ transactions from block height $2,100,000$ (May 17th, 2020) to $2,191,000$ (Sept 20th, 2020). For each of these transactions, we extract the size, fee, and timestamp attributes. Note that transactions that appeared during the sample period but not in any of the collected blocks are not included. Thus, the memory pools reconstructed are not the exact mempools miners were faced with. We also create artificial transaction data sets with normally distributed fee rates.

**Miners.** To mimic the actual Bitcoin network, we follow the mining power distribution of miners published by blockchain.com [25] on July 30th, 2020. We make the strongest miner with 17.6% mining power the undercutting miner. We additionally consider a hypothetical undercutter with 49.9% mining power. This is to uncover the profitability of undercutting for a strong attacker and its advantage over other miners when avoidance techniques are adopted by all. For the Monero network, we follow the mining power distributions published by exodus [27] and moneropool.com [1]. The strongest pool with 35% mining power is made the undercutting miner.

**Setup.** We model the blockchain system as event-based, with new block creation being the event. Parameters and states of the system are updated upon a new block creation event that we denote as $B_i$ for the remaining of this section. Miners have the same view of the network and the same latency in propagating the blocks and transactions. So miners working on the same chain see the same mempool. We initialize the time of the system to the earliest transaction timestamp. As shown in Algorithm 1, new block creation first happens (lines 2-4). Then chains, miners, and mempools are updated in lines 5-7. We include more details for chain and miner updating routines in Algorithm 2. Detailed descriptions for each routine can be found in the full report.

**Simulation run.** In a normal run, we repeat the above steps until we exhaust all transactions. In an avoidance-enabled simulation run, we repeat the procedure but with all miners actively defending against undercutting in line 4, according to the two summarized algorithms in Section 4.1 and Appendix A.

### 5.2 Experiment Results

**Normal runs.** Overall in a normal run, a strong undercutter can expect to earn more than fair shares by conditional undercutting as shown in figures 2b and 2d. **(i)** In Bitcoin runs, the 17.6% undercutter receives on average (for $D = 1$) 17.9% shares for 0-50% honest mining power (Figure 2a). The strong 49.9% undercutter receives a greater profit of 60.8% of the shares (Figure 2b). **(ii)** In runs with artificial transactions, the profits for $D = 1, 2$ bear a wider gap than with actual Bitcoin transactions (Figure 2c). **(iii)** In Monero runs, the 35%

**Algorithm 1:** Simulation Overview

```
input : txSet, minerSet, chainsTime
while txSet not empty do
    extChain ← nextChainToExtend(chainsTime);
    m ← selectNextBlockMiner(extChain);
    nextBlock ← publishBlock(m);
    updateChains(extChain, nextBlock);
    updateMiners(extChain);
    updateMempool(extChain);
```

**Algorithm 2:** Chain and Miner Updates

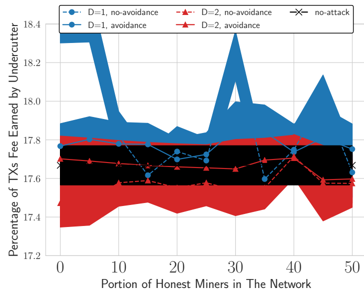
```
Function updateChains(extChain, nextBlock):
    extChain.append(nextBlock);
    foreach chain in chainsTime do
        remove from chainsTime if it is non-wining
    t ← NextBlockCreationTime(extChain);
    update chainsTime with tuple (extChain, t);

Function updateMiners(extChain):
    foreach miner in minerSet do
        if miner = undercutter then
            decide to fork or not and craft the new block as described in Part 1 of
              the D = 1 algorithm in 4.1, the D = 2 algorithm in Appendix A;
        if miner = honest then
            if extChain longest chain then
                switch to extChain;
        if miner = rational then
            decide to switch to extChain or stay on current chain as described in
              Part 2 of the D = 1 algorithm in 4.1, the D = 2 algorithm in
              Appendix A;
```

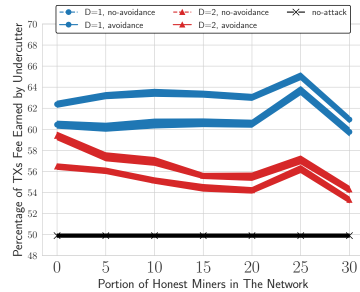
undercutter obtains 43.2% of the profit on average (for $D = 1, 2$) for different honest miner portions (Figure 2d). Undercutting is especially efficient in Monero because of its small mempools, which provide limited cushion effects.

**With undercutting avoidance.** As noted by PoA, the attacker has an advantage over others in equilibrium. The predicted average revenue proportion (adjusted for rounds where the undercutter mines a block and attacking is unnecessary) for the 49.9% attacker is around 63%. **(i)** In Bitcoin actual and artificial data runs, the return proportion is close to this predicted average. Avoidance runs can result in better revenues for the undercutter if the attack *cannot* be carried out to its ideal extent. That is because a large mempool along with continual incoming transactions lowers the profitability of undercutting. The implication is that if undercutting cannot be implemented ideally, avoidance can be relaxed from the exact extent. **(ii)** For Monero, we observe profit reduction for attackers in both margins after enabling avoidance, as shown in Figure 2d. **(iii)** Monero runs and Bitcoin runs for 17.6% undercutter provide more straightforward results, compared to Bitcoin runs with 49.9% attacker. Because the second undercutter in Monero has 35% mining power, which equals the strongest undercutter's mining power and in Bitcoin, the configuration is that the second-strongest mining power is 15.3% for 17.6% attacker and 20% for 49.9% attacker.

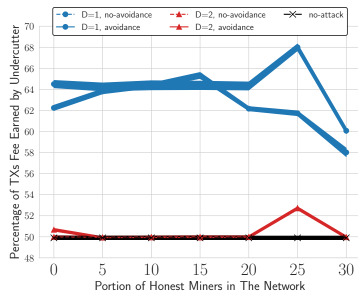
**Minor changes to Bitcoin core codebase.** We provide discussions concerning undercutting avoidance implementation and other possible defenses in the



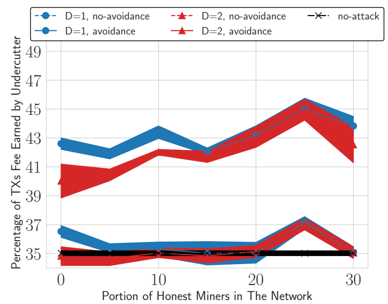

**(a)** Bitcoin: Returns for 17.6% Miner.




**(b)** Bitcoin: Returns for 49.9% Miner.




**(c)** Artificial transactions with normal distributed fee rates: returns for 49% Miner.




**(d)** Monero: Returns for 35% attacker.

**Fig. 2:** Undercutting Returns: normal runs (dashed lines) and runs with avoidance feature enabled (solid lines). The shadowed band is statistics' 95% confidence interval.

full report. We note that only light code changes in the Bitcoin core codebase are needed, which we demonstrate in this source [8].

## 6 Conclusion

We study the profitability of the undercutting mining strategy with the block size limit present. The intentional balancing of undercutting others and avoiding one's fork being undercut again demands specific conditions on the unconfirmed transaction set at the time of decision-making. Once conditions are met, an attacker can expect positive premiums. However, because such conditions are not easy to satisfy, are time-dependent (can be invalidated if new transactions arrive), and can be manipulated, it opens a door for mitigation. By applying an avoidance technique to invalidate the aforementioned conditions, miners can avoid being undercut. Avoidance encourages miners to claim fewer fees if the current bandwidth set is sufficiently wealthier than the next bandwidth set. As a result, the competition of undercutting can involuntarily promote the fair sharing of fees even in a time-variant fee system. Nevertheless, in a one-sided competition where the mining power discrepancy between the first and second strongest undercutters is large, the stronger undercutter has a natural advantage over others because it only has to defend against the weaker.

**Acknowledgement.** We would like to thank our shepherd Marko Vukolic and anonymous reviewers for their valuable comments. We thank Dankrad Feist for his feedback in the early stage of this project. This work has been partially supported by the National Science Foundation under grant CNS-1846316.

## A Giving Up After Two Blocks Behind

We present major steps for analyzing the $D = 2$ case and the complete analysis can be found in the full report. Rational miners now make decisions at states $S^* = \{(1,1), (1,2), (2,1), (2,2), ...\}$. The winning probabilities now comprise infinite series. Without loss of generality, we let $F_1^0 = 1$, $F_2^0 = F_3^0 = \gamma$, $F_1^1 = a$, $F_2^1 = b$ and $F_3^1 = 1 + 2\gamma - a - b$ (where $a \in [0,1], \gamma \geq 0$). $F_2^0, F_3^0$ can be of different values in reality but here we use the same value to highlight the wealthiness of $F_1^0$. Suppose eventually we derive an attacking condition $T$ for setting $D = 2$ as well, then the undercutter would want to set $a$ and $b$ to satisfy $\frac{1+\gamma-a}{a} > T$ and $\frac{1+2\gamma-a-b}{b} > T$ to avoid being undercut.

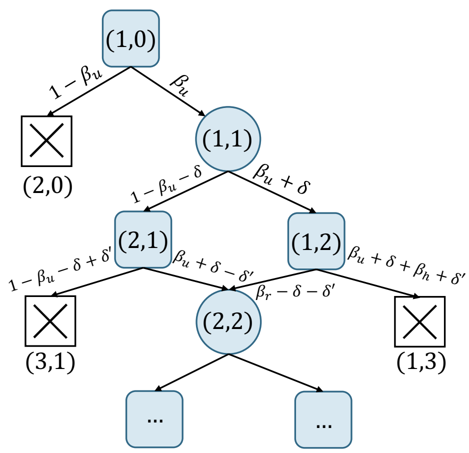


**Fig. 3:** State transition for $D = 2$. Notations are the same as Figure 1. Now we have infinite state transitions. $\delta'$ and $\delta''$ are the amount of rational mining power shifting from one chain to another.

We take the same route as in the $D = 1$ case. We know that if there is no attack, the undercutter expects to receive $E[R_{\overline{u}}] = 2\beta_u\gamma$. If it starts the attack, its expected return from the right branches (shown in Figure 3) when the undercutter succeeds and no rational miners assist is

$$E[R_u] = \beta_u(2\gamma + 1)\sum_{i=0}^{\infty}\beta_u^{i+2}(1-\beta_u)^i = \frac{\beta_u^3(2\gamma+1)}{1-\beta_u(1-\beta_u)}$$

The limited bandwidth set condition, $\gamma < \frac{\beta_u^2}{2(1-\beta_u)}$, is more demanding than the one for $D = 1$. For $\beta_u = 0.5$, the upper bound is now 0.25 instead of 1. For $\beta_u = 0.2$, the bound is 0.025 instead of 0.25. Overall, for weak attackers, the condition is way more demanding than before.

Next, we consider $\gamma \geq \frac{\beta_u^2}{2(1-\beta_u)}$ (with sufficient bandwidth set) and the undercutter needs rational miners to join $C_1$. Same as before, rational miners allocate their mining power among the two chains to maximize their expected returns:

$$\underset{x\in[0,1]}{\arg\max}\, E[R_r] = \underset{x\in[0,1]}{\arg\max} \Bigg( \mathbb{1}_{owner} \cdot p_0 + \frac{(1-x)\beta_r}{\beta_h + (1-x)\beta_r} p_0 \cdot 2\gamma + \frac{x\beta_r}{x\beta_r+\beta_u} p_1 \cdot b + \frac{x\beta_r}{x\beta_r+\beta_u+\beta_h} p_1 \cdot (1+2\gamma-a-b) \Bigg) \quad (4)$$

where $p_0 \leq (1-\beta_u - x\beta_r)^2$ is the probability of $C_0$ leading by 2 blocks first and $p_1 \geq (\beta_u + x\beta_r)(\beta_u + x\beta_r + \beta_h)$ is the probability of $C_1$ leading by 2 blocks first. Here we only consider the leftmost and rightmost branch in Figure 3 because they are the two most significant paths. We can observe that the objective function is convex. By Jensen's inequality, the expected returns reach maximum at either of the two ends. Again we let $E[R_{r|x=0}] < E[R_{r|x=1}]$ and obtain

$$2(1-\beta_u)\gamma < b + (\beta_u+\beta_r)(1+2\gamma-a-b) \overset{\beta_h \geq \beta_u}{\Rightarrow} \gamma < \tfrac{(\beta_u+\beta_r)(1-a)+\beta_h b}{2(\beta_h-\beta_u)}$$

When $\beta_h \leq \beta_u$, flexible rational miners move to the fork if $a < 1$. Same as before, we denote the right-hand side condition as $T$ and solve for $a$ and $b$ numerically by considering the strongest potential undercutter the attacker is facing.

$$a \leq \frac{1+\bar{\gamma}}{1+T} = \frac{1+\bar{\gamma}}{1+\frac{(\beta_{u_2}+\beta_{r_2})(1-a_2)+\beta_{h_2}b_2}{2(\beta_{h_2}-\beta_{u_2})}}, a_2 \leq \frac{1+\bar{\gamma}'}{1+\frac{(\beta_u+\beta_r)(1-a)+\beta_h b}{2(\beta_h-\beta_u)}},$$
$$b \leq \frac{1+2\tilde{\gamma}-a}{1+T}, b_2 \leq \frac{1+2\tilde{\gamma}'-a}{1+\frac{(\beta_u+\beta_r)(1-a)+\beta_h b}{2(\beta_h-\beta_u)}} \quad (5)$$

Here, $\tilde{\gamma}, \tilde{\gamma}'$ are the fee totals in the respective third bandwidth set measured relative to the respective next bandwidth set. With rational miners joining, the expected return for undercutter on the rightmost branch is now $E[R_u] = \big(a + \frac{\beta_u}{\beta_u+\beta_r} b + \beta_u(1+2\gamma-a-b)\big) \cdot \beta_u(\beta_u+\beta_r)$. We let $E[R_u] > E[R_{\overline{u}}]$ and obtain the condition on $\gamma$ for profitable undercutting:

$$\gamma < \min\{\frac{\beta_u+\beta_r a}{2(1-\beta_u)}, \frac{(\beta_u+\beta_r)(1-a)+\beta_h b}{2(\beta_h-\beta_u)}\} \quad (6)$$

We present the algorithm for $D = 2$ below.

**(Part 1)** A potential **undercutter** decides whether to undercut:
Compute $a, b$ numerically according to Inequalities 5 that maximizes $E[R_u]$ and check if $\gamma$ satisfies Inequality 6. If Yes, start undercutting.
**(Part 2) Flexible rational miners** decide mining resource distribution:
Solve for $x$ in a generalized Equation 4.
**(Part 3) Miners** avoid being undercut:
Calculate the attack condition $T$ (right-hand side of Inequality 6) for the strongest undercutter a miner is defending against. Check if current $\bar{\gamma} < T$. If Yes, include in the current block $< \frac{1+\bar{\gamma}}{1+T}$ of the fees in the bandwidth set; otherwise, use the bandwidth set.

## References


1. Monero pools since 2016. http://moneropools.com/ (2020)
2. Akerlof, G.A.: The market for "lemons": Quality uncertainty and the market mechanism. In: Uncertainty in economics, pp. 235–251. Elsevier (1978)
3. Bitcoin.org: Memory pool, https://developer.bitcoin.org/devguide/p2p_network.html#memory-pool
4. Carlsten, M., Kalodner, H., Weinberg, S.M., Narayanan, A.: On the instability of bitcoin without the block reward. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 154–167. ACM (2016)
5. Courtois, N.T., Bahack, L.: On subversive miner strategies and block withholding attack in bitcoin digital currency. arXiv preprint arXiv:1402.1718 (2014)
6. Eyal, I.: The miner's dilemma. In: 2015 IEEE Symposium on Security and Privacy. pp. 89–103. IEEE (2015)
7. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: International conference on financial cryptography and data security. pp. 436–454. Springer (2014)
8. Gong, T.: Bitcoin core source code updated to account for undercutting avoidance, https://github.com/haas256/bitcoin
9. Gong, T., Minaei, M., Sun, W., Kate, A.: Towards overcoming the undercutting problem. arXiv preprint arXiv:2007.11480 (2020)
10. Half, B.B.: Bitcoin halving 2024. https://www.bitcoinblockhalf.com/ (2020), accessed: 2020-07-22
11. Heilman, E.: One weird trick to stop selfish miners: Fresh bitcoins, a solution for the honest miner. In: International Conference on Financial Cryptography and Data Security. pp. 161–162. Springer (2014)
12. Koutsoupias, E., Papadimitriou, C.: Worst-case equilibria. In: Annual Symposium on Theoretical Aspects of Computer Science. pp. 404–413. Springer (1999)
13. Kwon, Y., Kim, D., Son, Y., Vasserman, E., Kim, Y.: Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. pp. 195–209. ACM (2017)
14. Kwon, Y., Kim, H., Yi, Y., Kim, Y.: An eye for an eye: Economics of retaliation in mining pools. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. pp. 169–182 (2019)
15. Lavi, R., Sattath, O., Zohar, A.: Redesigning bitcoin's fee market. In: The World Wide Web Conference. pp. 2950–2956. ACM (2019)
16. Luu, L., Saha, R., Parameshwaran, I., Saxena, P., Hobor, A.: On power splitting games in distributed computation: The case of bitcoin pooled mining. In: 2015 IEEE 28th Computer Security Foundations Symposium. pp. 397–411. IEEE (2015)
17. Luu, L., Teutsch, J., Kulkarni, R., Saxena, P.: Demystifying incentives in the consensus computer. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. pp. 706–719 (2015)
18. Mohsen Minaei, T.G.: Source code of the blockchain simulation and undercutting experiments, https://github.com/haas256/UP
19. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
20. Nayak, K., Kumar, S., Miller, A., Shi, E.: Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P). pp. 305–320. IEEE (2016)

21. Pass, R., Shi, E.: Fruitchains: A fair blockchain. In: Proceedings of the ACM Symposium on Principles of Distributed Computing. pp. 315–324. ACM (2017)
22. Rosenfeld, M.: Analysis of bitcoin pooled mining reward systems. arXiv preprint arXiv:1112.4980 (2011)
23. Rosenfeld, M.: Analysis of hashrate-based double spending. arXiv preprint arXiv:1402.2009 (2014)
24. S.A., B.L.: Bitcoin blockchain api. https://www.blockchain.com/api (2020)
25. S.A., B.L.: Bitcoin miners mining power. https://www.blockchain.com/en/pools (2020), accessed: 2020-02-27
26. Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in bitcoin. In: International Conference on Financial Cryptography and Data Security. pp. 515–532. Springer (2016)
27. Won, D.: 2020's best monero pools. https://www.exodus.io/blog/best-monero-pools/ (2020)
28. Zhang, R., Preneel, B.: Publish or perish: A backward-compatible defense against selfish mining in bitcoin. In: Cryptographers' Track at the RSA Conference. pp. 277–292. Springer (2017)