The Phase Space of Block Withholding Mining Strategies

Assaf Shomer

December 23, 2013

Abstract

We calculate the probability of success of block-withholding mining strategies in bitcoin-like networks. These strategies involve building a secret branch of the block-tree and publishing it opportunistically, aiming to replace the top of the main-branch and rip the reward associated with the secretly mined blocks. We identify two types of block-withholding strategies and chart the parameter space where those are more beneficial than the standard mining strategy described in Nakamoto's paper. Our analysis suggests a generalization of the notion of the relative hashing power as a measure for a miner's influence on the network. Block withholding strategies are beneficial only when this measure of influence exceeds a certain threshold.

Contents

Chapter 1

Introduction

1.1 Bitcoin and mining

Bitcoin is the world's first decentralized digital currency ([1]). blah blah

Motivated by the work done in [3] we are interested in finding out if and when the block-withholding strategy gives the miner a higher probability of success in mining blocks, compared to the standard strategy outlined in the bitcoin protocol.

Chapter 2

Three mining strategies

2.1 The Standard Mining Strategy

The standard mining strategy follow the bitcoin protocol described in [1]. Such miners publish each block as soon as it is discovered and switch their mining efforts to the head of the blockchain[1] as soon as they become aware of a new valid block.

$$\cdots \to B_L \to B_{L+1} \to B_{L+2} \to \dots$$

2.2 Block Withholding Strategies

Miners following this type of mining strategies do not share newly found blocks and instead work on extending a **secret** branch of the block-tree. The miners publish their secret branch when it is most beneficial to them.

$$\begin{array}{lll} \cdots \to B_L \to \quad B_{L+1} \to B_{L+2} \to \cdots \to B_{L+n} & \text{Main} \\ \qquad\quad \searrow & \\ \qquad\quad \widetilde{B}_{L+1} \to \widetilde{B}_{L+2} \longrightarrow \quad \dots \longrightarrow \widetilde{B}_{L+m} & \text{Secret} \end{array} \tag{2.1}$$

2.2.1 Type I (try to win)

The miners mine their secret branch until it is *longer than the main branch*. At this time they can publish it and uproot the last n blocks mined by the Standard miners in favour of their $m > n$ secretly mined ones.

[1] In practice different miners may be aware of different branches of the block-tree at a given moment. Such differences are resolved with very high probability once a new block is found because the protocol names the branch with the maximal difficulty to be the blockchain.

2.2.2 Type 0 (reach a tie and get some help)

The miners mine their secret branch until it is of the *same length as the main branch*. At this time they publish it. Now the network is bifurcated. The type 0 miners joined by some of the standard miners will mine on top of the newly published Type 0 branch. The rest of the standard miners continue working on the standard branch. If the former manage to find a new block first then the Type 0 strategy was successful.

2.3 Our Goal

Our goal is to analyse which mining strategy is the most beneficial as a function of the miner's relative hashing power and the portion of standard miners that join them, in case of a Type 0 strategy. To that effect we calculate the probability that a block-withholding miner succeeds in replacing a block (and possibly some number of confirmation blocks on top of it) by publishing a secretly mined branch of the block-tree.

Chapter 3

Calculation

3.1 Setup

Let us denote by $\mathcal{H}$ the total hashing power of the network and divide it abstractly into a *Standard* part which holds a portion $p\mathcal{H}$ of the total hashing power (where $p \in [0, 1]$) and a *Block Withholding* part, which holds the rest $q\mathcal{H} = (1 - p)\mathcal{H}$.

We start our analysis at a given point in time where the blockchain is of length L and denote the last block mined as B_L. As time marches on the Standard miners continue to mine on top of it ($B_{L+1}, B_{L+2}, \dots$) while the block withholding miners are building a separate branch on top of B_L ($\tilde{B}_{L+1}, \tilde{B}_{L+2}, \dots$). This is depicted in figure 2.1. The block withholding miners aim to replace the top of the chain mined on top of B_L by using one of the two block withholding strategies.

3.2 Calculating the probability of success

Calculating the probability of success for a block withholding strategy involves two parts. We first calculate the probability that the block tree reaches a situation like the one depicted in figure 2.1. Then we multiply this probability with the probability that the block withholders manage to catchup with the main chain. Our analysis follows the one presented in [2].

3.2.1 Getting to the starting point

Treating block mining as a negative binomial random variable, the probability $P_{n,p}(m)$ that m blocks are mined in the secret branch **before** n blocks are mined in the main branchis proportional to $p^n q^m$ and can be shown (appendix A.0.2) to be given by

$$P_{n,q}(m) = \binom{n+m-1}{m}(1-q)^n q^m \quad n = 1, 2, \dots \tag{3.1}$$

3.2.2 Catching up from the starting point

The probability $a^{(r)}_{n,m}(q)$ that the attackers manage to catch-up and overtake the blockchain by at least r blocks, given the situation above[1] is given by a Markov chain that depends only on the advantage z of the honest network over the attackers $z = n - m$, and the parameter r. Formally, the chain satisfies the recurrence relation

$$a^{(r)}_z(q) = (1-q)\, a^{(r)}_{z+1}(q) + q\, a^{(r)}_{z-1}(q) \tag{3.2}$$

with boundary conditions encoding the fact that a success is defined by the secret branch being longer than the main branch by at least r blocks

$$\texttt{Boundary Conditions:} \begin{cases} a^{(r)}_{-r} = 1 \\ a^{(r)}_{\infty} = 0 \end{cases} \tag{3.3}$$

The relation 3.2 can be solved with boundary conditions 3.3 by

$$a^{(r)}_z(q) = \begin{cases} \left(\dfrac{q}{1-q}\right)^{z+r} & q \in [0, \frac{1}{2}] \quad \text{and} \quad z = 0, 1, 2 \dots \\ 1 & \text{otherwise} \end{cases} \tag{3.4}$$

3.3 Block Withholding Strategy - Type I

The type I strategy is successful when applied on top of B_L if the miner manages to catch-up on B_{L+1} and win by at least one block, after starting with $m = 0, 1, \dots$ secret blocks. By publishing the secret branch the miner can now replace B_{L+1} and any blocks mined by the network on top of it. Let $Q(q)$ be the probability that a type I miner succeeds.

The starting point for the catch-up process for some m is shown below:

$$\begin{array}{lll} \cdots \to B_L \to & B_{L+1} & \text{Main} \\ \quad \searrow & & \\ & \widetilde{B}_{L+1} \to \widetilde{B}_{L+2} \longrightarrow \quad \dots \longrightarrow \widetilde{B}_{L+m} & \text{Secret} \end{array} \tag{3.5}$$

By definition of the Type I strategy, the secret branch needs to be longer by at least one block[2], so we need to set the boundary condition in 3.3 to $r = 1$, giving:

$$Q(q) = \sum_{m=0}^{\infty} P_{1,q}(m)\, a^{(1)}_{1-m}(q) \tag{3.6}$$

which gives (see details in appendix A.0.3)

[1] Namely, that until the moment the main network mines it's nth block on top of B_L, the block withholders manage to mine m blocks on top of B_L constituting their secret branch.

[2] Hence the name: "Type **I**".

$$Q(q) = \begin{cases} \dfrac{q^2}{1-q}(3-2q) & q \in [0, \frac{1}{2}] \\ 1 & q \in [\frac{1}{2}, 1] \end{cases} \tag{3.7}$$

In Figure 3.1 we plot the probability of a successful Type I strategy as a function of the relative hashing power q. As a reference we also plot the probability of success in mining a block for a standard miner with the same hashing power q.

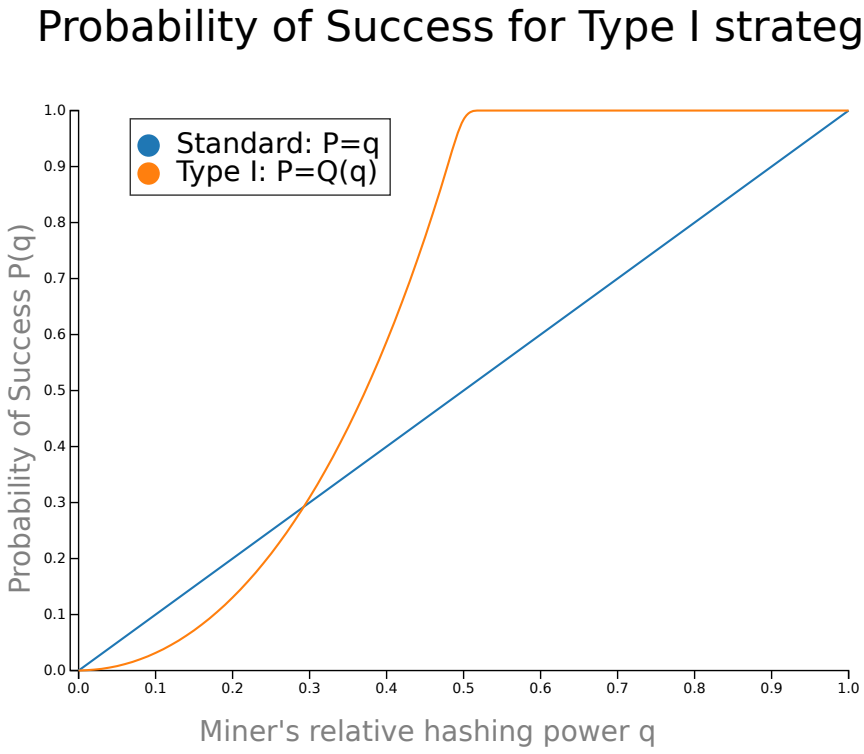

Figure 3.1: The orange curve plots the probability that a Type I miner manages to uproot the next block mined by the network and replace it (and any blocks mined on top of it) with blocks she mined in her secret branch. The blue curve is the baseline probability for an Standard miner with the same hashing power q

3.3.1 When is Type I better than Standard?

To find out how big q needs to be for this type of strategy to become more beneficial than the standard strategy we need to solve for $Q(q) \geq q$

$$\frac{q^2}{1-q}(3-2q) \geq q \tag{3.8}$$

which since $0 \leq q \leq 1$ gives the condition

$$q \geq q_0 = 1 - \frac{1}{\sqrt{2}} \sim 0.293 \tag{3.9}$$

We conclude that type I strategy is better than the standard strategy for $q > q_0$. Once $q \geq \frac{1}{2}$ we get to the famous "51% attack" where the type I strategy is guaranteed to succeed, but even for $q_0 \leq q \leq \frac{1}{2}$ type I increases the probability of success for mining a new block compared to the standard strategy

3.4 Block Withholding Strategy - Type 0

In this section we analyse calculate the probability of success of a type 0 mining strategy. Instead of publishing the secret branch when it is longer than the main branch, a type 0 miner publishes it one step before, when his secret branch is of the same length as the main branch (i.e. when they reach a tie).

The reason this is potentially beneficial is that due to latency effects in the bitcoin network (recently discussed in [4]) not all miners share the same view of the entire block-tree at all moments. All honest miners shift their efforts to the longest branch they know of, but for some period of time different parts of the network may be aware of different, and equally valid, longest branches. In such a case the network bifurcates. Each sub-network continues mining it's longest-branch until the next block is mined by either one and a new block-chain is established[3]. Following the notation used in [3] let us denote by γ the ratio of standard miners that choose to mine on top of the newly-published-used-to-be-secret Type 0 branch. This means that $q + \gamma p$ of the total hashing power is now dedicated to making the Type 0 branch the longest and with some probability this branch will end up as the winner.

Let us denote the probability that this type of tie strategy succeeds by $S_\gamma(q)$. We can calculate $S_\gamma(q)$ starting the same way as we did when we derived 3.12 but use a Markov chain with boundary condition reflecting a tie instead of wining. We then multiply that probability by the probability of catching up and wining the race with hashing power $q+\gamma p$, starting from that point.

Formally, we want to solve 3.2 with boundary conditions $r = 0$:

$$a_z^{(0)}(q) = \begin{cases} \left(\frac{q}{1-q}\right)^z & q \in [0, \frac{1}{2}] \quad \text{and} \quad z = 0, 1, 2 \dots \\ 1 & \text{otherwise} \end{cases} \tag{3.10}$$

Using the same logic used to derive 3.11 we get the probability for a tie is given by

$$T(q) = \sum_{m=0}^{\infty} P_{1,q}(m) a_{1-m}^{(0)}(q) \tag{3.11}$$

resulting in (see details in appendix A.0.4)

[3] In principle this type of block-chain bifurcation can continue to span multiple blocks, with exponentially decreasing probability.

$$T(q) = \begin{cases} 2q & q \in [0, \frac{1}{2}] \\ 1 & q \in [\frac{1}{2}, 1] \end{cases} \tag{3.12}$$

Now the type 0 miner, **joined by γ of the standard miners**, are competing with the rest of the standard miners. The probability to **win** starting from a tie is thus given by (see equation 3.4)

$$a_0^{(1)}(q_{eff}) = \begin{cases} \dfrac{q_{eff}}{1 - q_{eff}} & q_{eff} \in [0, \frac{1}{2}] \\ 1 & q_{eff} \in [\frac{1}{2}, 1] \end{cases} \tag{3.13}$$

where

$$q_{eff} = q + \gamma p = q + \gamma(1 - q). \tag{3.14}$$

The condition $q_{eff} \in [0, \frac{1}{2}]$ translates to

$$0 \leq q \leq q_c(\gamma) = \frac{1 - 2\gamma}{2 - 2\gamma} \tag{3.15}$$

The curve $q_c(\gamma)$ (depicted in figure 3.2) satisfies $0 \leq q_c(\gamma) \leq \dfrac{1}{2}$, monotonically decreases with γ and hits 0 when[4] $\gamma = \frac{1}{2}$.

Based on all that, the solution to $S_\gamma(q) = T(q) \cdot a_0^{(1)}(q_{eff})$ breaks into three regimes:

$$S_\gamma(q) = \underbrace{T(q)}_{\text{reach a tie}} \cdot \underbrace{a_0^{(1)}(q_{eff})}_{\text{win given a tie}} = \begin{cases} 2q \cdot \frac{q_{eff}}{1-q_{eff}} = 2q \cdot \frac{q(1-\gamma)+\gamma}{(1-q)(1-\gamma)} & q \in [0, q_c] \\ 2q & q \in [q_c, \frac{1}{2}] \\ 1 & q \in [\frac{1}{2}, 1] \end{cases} \tag{3.16}$$

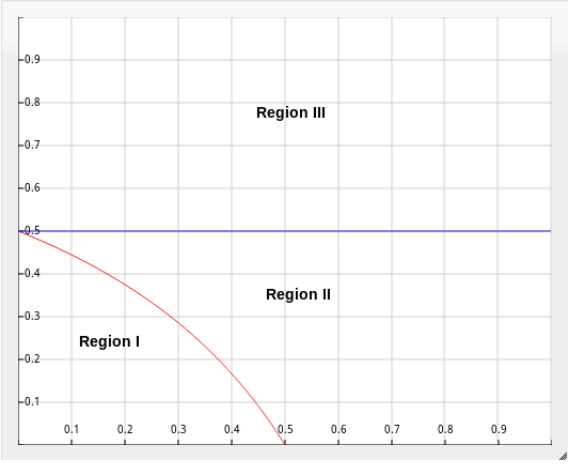

Figure 3.2: The three regions of the solution to $S_\gamma(q)$. The red curve is $q_c(\gamma)$.

[4] $q_{eff}(\frac{1}{2}) = \frac{1}{2}(1 + q)$ which is bigger than $\frac{1}{2}$ for any q.

Note that if $\gamma \geq \frac{1}{2}$ the first regime does not exist and the solution degenerates to:

$$S_{\gamma \geq \frac{1}{2}}(q) = T(q) \cdot a_0(q_{eff}) = \begin{cases} 2q & q \in [0, \frac{1}{2}] \\ 1 & q \in [\frac{1}{2}, 1] \end{cases} = min(2q, 1) \tag{3.17}$$

In figure 3.3 we plot the probability of success of the Type 0 strategy $S_\gamma(q)$ for various values of the parameter γ, side by side with the probabilities of success of the Standard and Type I strategies.

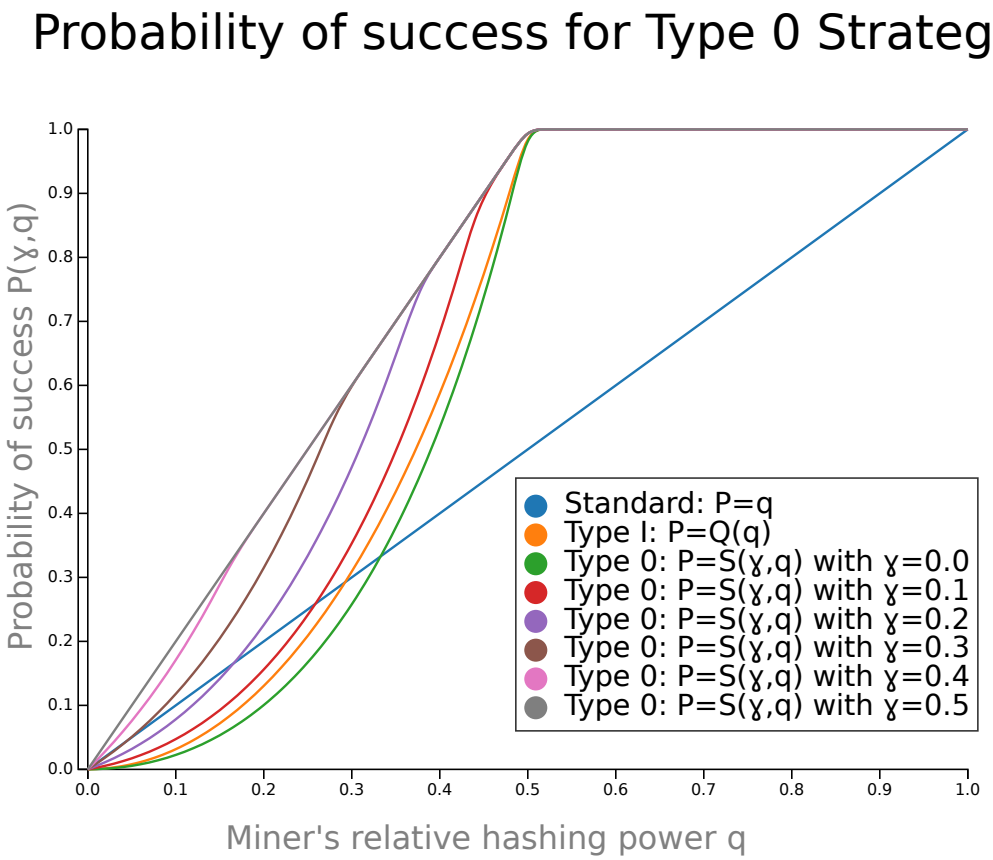

Figure 3.3: The Type 0 strategy probability of success $S_\gamma(q)$, plotted for various values of the parameter γ and against the probabilities for the Standard and Type I strategies.

Chapter 4

The γ, q phase space

Our aim in this chapter is to map the γ, q phase space and find which strategy yields the maximal probability of success for the miner in each region. From section 3.3.1 we already know that the Type I strategy is better than the Standard strategy if $q \geq q_0$. To decide if a block-withholding strategy of type 0 is beneficial or not we should compare it first to the standard probability of success and then, if it is more beneficial, compare it to the Type I strategy to decide which block withholding strategy wins.

4.1 Type 0 vs. Standard

A Type 0 strategy is more beneficial than the standard strategy when $S_\gamma(q) \geq q$ where $S_\gamma(q)$ is given in equation 3.16.

In the second and third regimes of equation 3.16 (or for any q if $\gamma \geq \frac{1}{2}$, see equation 3.17 and figure 3.2) the type 0 attacks is beneficial over the standard strategy for any q, because it is always true that $0 \leq q \leq min(2q, 1)$.

In the first regime (i.e. when $q < q_c(\gamma)$) we can find at what value of q the type 0 strategy starts being more beneficial than the standard strategy by solving

$$2q \cdot \frac{q(1-\gamma)+\gamma}{(1-q)(1-\gamma)} \geq q \tag{4.1}$$

which gives the condition $q_b(\gamma) \leq q \leq q_c(\gamma)$, where

$$q_b = \frac{1-3\gamma}{3-3\gamma} \tag{4.2}$$

The curve $q_b(\gamma)$ designating the boundary where the Type 0 strategy starts becoming more beneficial than the standard strategy is plotted in Figure 4.1. Note that if $\gamma = 0$ this strategy is beneficial only when $q > \frac{1}{3}$ and if $\gamma \geq \frac{1}{3}$ it is beneficial for all q.

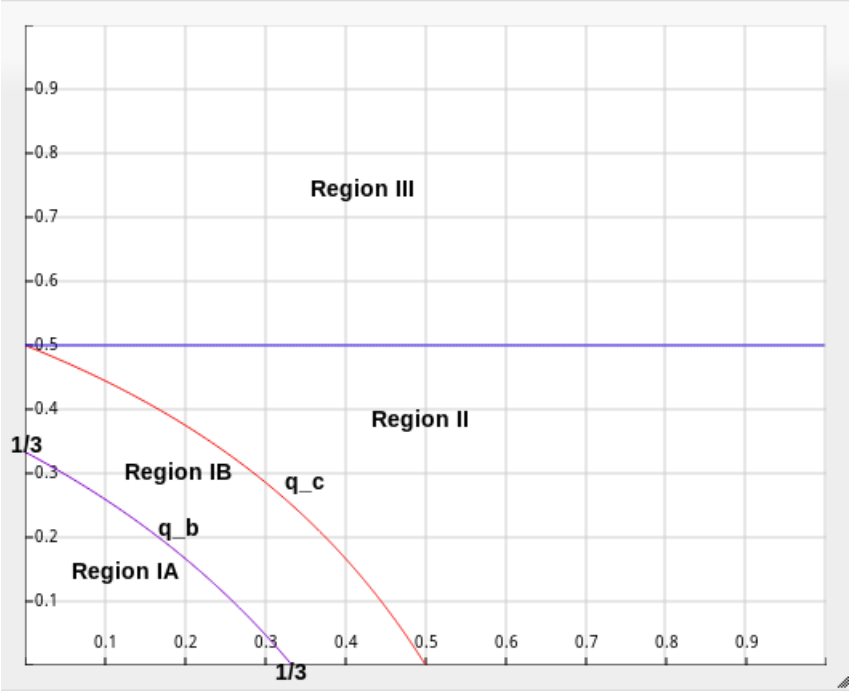

Figure 4.1: The Type 0 strategy is more beneficial than the standard strategy outside of the inner curve $q_b(\gamma)$. Standard mining is more beneficial only in region IA.

Taking all three regimes into account we conclude that the Type 0 strategy is more beneficial than the Standard strategy when

$$S_\gamma(q) \geq q \Longrightarrow \begin{cases} q > \dfrac{1-3\gamma}{3-3\gamma} & \gamma \in [0, \frac{1}{3}] \\ any\ q & \gamma \in [\frac{1}{3}, 1] \end{cases} \tag{4.3}$$

or, summarized further by

$$S_\gamma(q) \geq q \Longrightarrow q > max\left\{\frac{1-3\gamma}{3-3\gamma}, 0\right\} \tag{4.4}$$

Next we compare between the two block withholding strategies.

4.2 Comparing Type 0 to Type I

There are two interesting comparisons one can make between Type 0 and Type I strategies. One is to compare how they match against the standard strategy,namely, for a given γ do we first hit the regime where a Type 0 or a Type I strategy is more beneficial than the standard strategy. The other is to ignore the standard strategy and ask, for a given value of γ, q which is better, Type 0 or Type I.

4.2.1 Which block withholding is beneficial first

Let us first tackle the first question and find out for a given γ whether Type 0 or Type I wins first. For $\gamma \geq \frac{1}{3}$, Type 0 wins already at $q = 0$, so the interesting part is where $\gamma < \frac{1}{3}$ where we can compare $q_b(\gamma)$ (given in equation 4.2) with q_0 (given in equation 3.9). Solving for the intersectin of the two curves

$$\frac{1-3\gamma}{3-3\gamma} = 1 - \frac{1}{\sqrt{2}} \tag{4.5}$$

We get a single intersection at a special value of γ

$$\gamma_c = 1 - \frac{2}{3}\sqrt{2} \sim 0.0572 \tag{4.6}$$

A type 0 strategy is more beneficial than the standard strategy sooner (i.e. smaller q) than type I for $\gamma \geq \gamma_c$.

Indeed, you can see in Figure 3.3 that the green curve representing $\gamma = 0$ lies below the orange curve which represents the Type I strategy, while the red curve representing $\gamma = 0.1 > \gamma_c$ lies above it.

To summarize, when $\gamma \geq \frac{1}{3}$ the Type 0 strategy is beneficial over the standard strategy for any value of q. When $\gamma < \frac{1}{3}$, the hashing power of the attacker needs to exceed a threshold before a block withholding strategy is beneficial. If $\gamma_c \leq \gamma \leq \frac{1}{3}$ we bump into the Type 0 first (the threshold given by $q_b = \frac{1-3\gamma}{3-3\gamma}$), while if $\gamma < \gamma_c$ we bump into Type I first (the threshold is given by $q_0 = 1 - \frac{1}{\sqrt{2}}$).

4.2.2 Type 0 vs. Type I

Finally, ignoring the standard strategy for a moment, we can ask for the range of parameters q, γ where the Type 0 strategy is more beneficial than the Type I strategy. Formally we need to solve:

$$2q \cdot \frac{q(1-\gamma)+\gamma}{(1-q)(1-\gamma)} \geq \frac{q^2}{1-q}(3-2q) \tag{4.7}$$

which gives the condition

$$2q^2 - q + \frac{2\gamma}{1-\gamma} \geq 0 \tag{4.8}$$

This condition is satisfied in two regimes for γ.

$$S_\gamma(q) \geq Q(q) \Longrightarrow \begin{cases} any\ q & \gamma \in [\frac{1}{17}, 1] \\ q < q_-(\gamma) \quad or \quad q > q_+(\gamma) & \gamma \in [0, \frac{1}{17}] \end{cases} \tag{4.9}$$

where

$$q_{\pm}(\gamma) = \frac{1}{4}\left(1 \pm \sqrt{\frac{1-17\gamma}{1-\gamma}}\right) \tag{4.10}$$

4.3 The Strategy Phase Space

We can chart the strategy phase space parametrized by $\gamma, q \in [0,1]^2$, and divide it into regions characterized by the most beneficial mining strategy: **Standard**, **Type 0** or **Type I**.

The γ, q phase space is governed by four functions (really three intersecting curves):

- $q_0 = 1 - \frac{1}{\sqrt{2}}$ determining for what q type I is better than standard.
- $max\{q_b(\gamma) = \frac{1-3\gamma}{3-3\gamma}, 0\}$ determining for what q Type 0 is better than standard.
- $q_+(\gamma) = \frac{1}{4}\left(1 + \sqrt{\frac{1-17\gamma}{1-\gamma}}\right)$
- $q_-(\gamma) = \frac{1}{4}\left(1 - \sqrt{\frac{1-17\gamma}{1-\gamma}}\right)$

where the last two determine which strategy is better, Type 0 or I when $\gamma < \frac{1}{17}$. Interestingly enough, the 3 functions $q_0, q_b(\gamma), q_+(\gamma)$ intersect in a single point $\gamma = \gamma_c, q = q_0$ which simplifies the structure of the phase space diagram, slicing it into exactly 6 regions each characterized by one of the 6 possible orderings between the 3 available strategies.

- The circular curve (created by the two branches $q_{\pm}$) determines, for a given γ, which of the two block-withholding strategies, Type 0 or Type I is more beneficial. Inside the circular region (and all the way to the q axis) is the region where Type I is better than type 0. Outside this region Type 0 is better than Type 1. This is determined by equation 4.8. Note that this division doesn't specify whether any of the strategies is better than the standard one.
- Type I strategy is more beneficial than the Standard strategy in the region above the horizontal line $q = q_0$. .
- Type 0 strategy is more beneficial than the Standard strategy in the region above the monotonically decreasing curve $q_b(\gamma)$ (extending from $\frac{1}{3}$ on the q axis to $\frac{1}{3}$ on the γ axis and the continuing on the γ axis all the way to $\gamma = 1$).

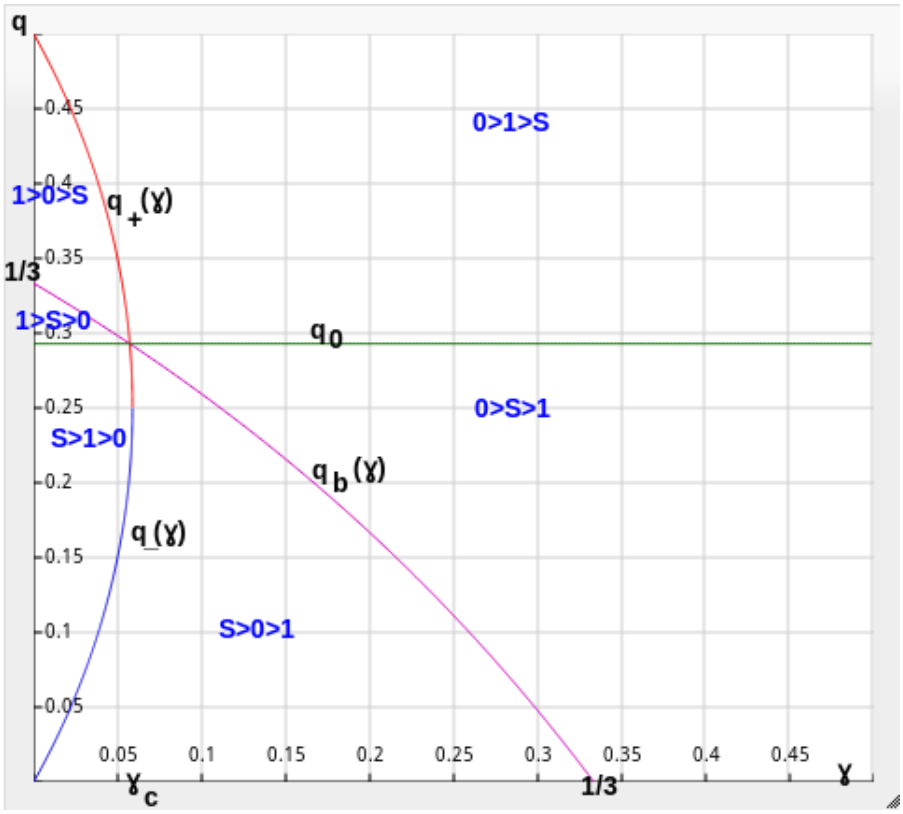

Figure 4.2: The 3 curves sectioning the γ, q phase space into 6 regions characterized by a hierarchy of the 3 strategies. For brevity we denote the Type I strategy by "1", the Type 0 strategy by "0" and the Standard strategy by "S". For example, in the top region Type 0 is more beneficial than Type I which in turn is more beneficial than the standard strategy.

A miner, seeking to maximize profit, can select the most beneficial strategy in each region. The resulting phase space is divided into 3 regions characterized by the winning strategy, is depicted in figure 4.3.

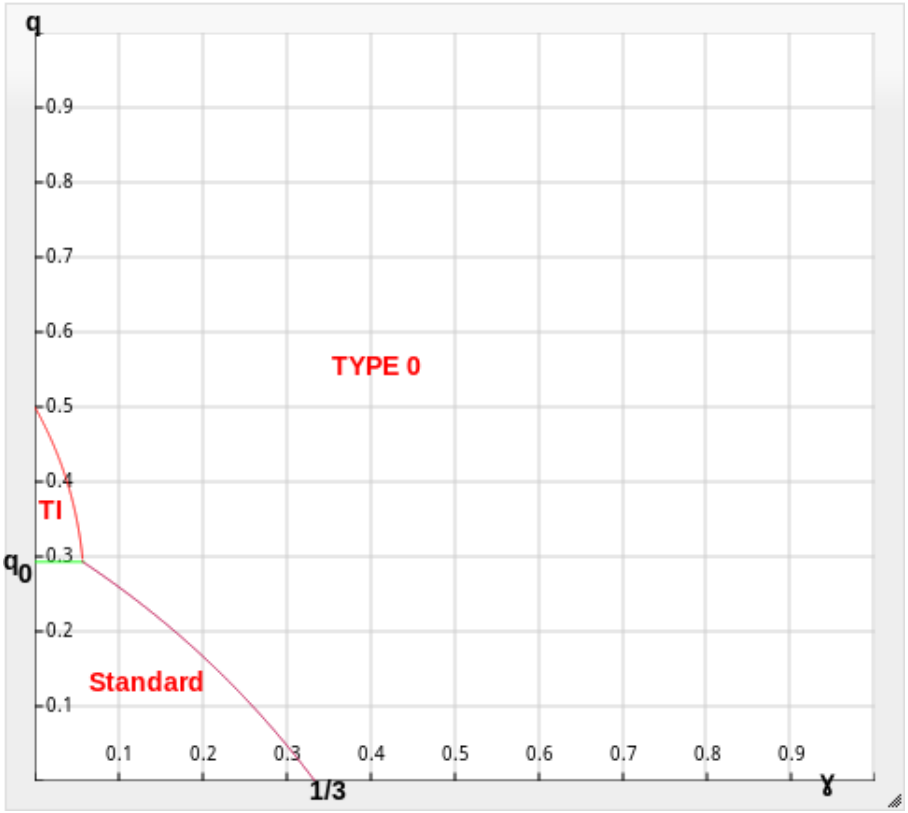

Figure 4.3: The 3 regions of the q, γ phase space. The standard strategy is best in the region near the origin. Type I is best in the little area on top of the standard region. In the rest of phase space the Type 0 strategy is most beneficial.

4.3.1 Discussion

Note that the regime where either block-withholding strategies are more beneficial than the standard strategy is bounded away from the origin. It is tempting to look at the radial distance from the origin of phase space as a measure of a "miner's *Influence*"

$$\mathtt{I}(q, \gamma) \equiv \sqrt{q^2 + \gamma^2}. \tag{4.11}$$

This definition is motivated by the rough symmetry[1] between the parameters γ and q which seems to suggest that having a large γ is "similarly difficult" to having a large q and a typical miner will have both parameters in similar scales.

There are a few remarks in order:

- Figure 4.3 marks the regions where a block-withholding strategy in beneficial, but does not guarantee success. Success of either strategies is still guaranteed (i.e. the

[1] All we mean by that is that figure 4.3 is almost symmetric under a rotation along the 45° angle that rotates $\gamma \leftrightarrow q$.

probability of success is strictly 1) only in the top half of phase space, in the region where $q \geq \frac{1}{2}$ (the infamous 51% attack).

- The authors of [3] identified a region delimited by the curve $\frac{1-\gamma}{3-2\gamma} \leq q \leq \frac{1}{3}$ where the "selfish" mining strategy is more beneficial than the standard one. As one would expect based on the fact that the "selfish" strategy utilizes a combination of the two strategies discussed here, this curve intersects both Type I and Type 0 regions as depicted in figure 4.4.

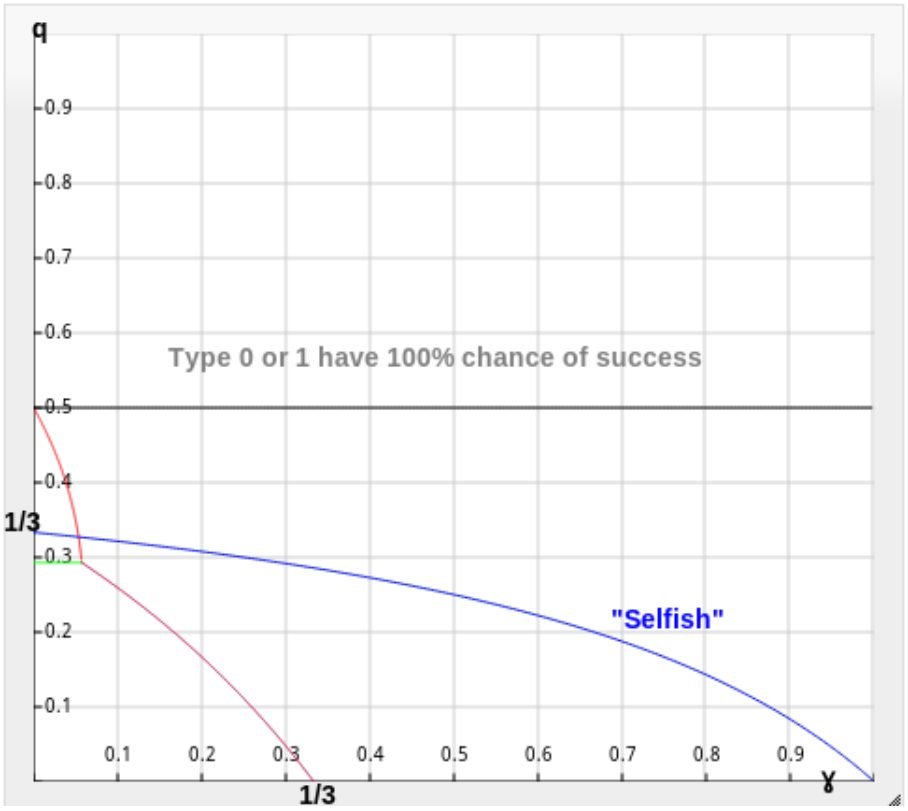

Figure 4.4: In this plot we see the location of the curve describing the "seflish" strategy of [3] within the γ, q phase space.

Appendix A

Calculation Details

A.0.2 Probability distribution

$$\sum_{m=0}^{\infty} P(n,m,p) = p^n \sum_{m=0}^{\infty} \binom{n+m-1}{m} q^m = p^n \frac{1}{(1-q)^n} = 1 \tag{A.1}$$

where we used the binomial identity holding for any complex s inside the unit circle ($|s|<1$) $\frac{1}{(1-s)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} s^k$.

A.0.3 $Q(q)$

$Q(q)$ can be solved in the two regions for the parameter q given in 3.4.

In the case that $q \in [0, \frac{1}{2}]$

$$Q(q) = \textstyle\sum_{m=0}^{\infty} P_{1,q}(m)\, a_{1-m}^{(1)}(q) = (1-q) \sum_{m=0}^{\infty} q^m a_{1-m}^{(1)}(q) =$$

$$(1-q)\left(a_1^{(1)}(q) + q a_0^{(1)}(q) + \textstyle\sum_{m=2}^{\infty} q^m\right) = (1-q)\left(\left(\frac{q}{1-q}\right)^2 + q\frac{q}{1-q} + (\textstyle\sum_{m=0}^{\infty} q^m) - 1 - q\right) =$$

$$\frac{1}{1-q}\left(q^2(2-q) + 1 - q - (1-q)^2(1+q)\right) =$$

$$\frac{1}{1-q}\left(2q^2 - q^3 + 1 - q - 1 + 2q - q^2 - q + 2q^2 - q^3\right) = \frac{q^2}{1-q}(3-2q)$$

In the case that $q \in [\frac{1}{2}, 1]$

$$Q(1) = p \textstyle\sum_{m=0}^{\infty} q^m a_{1-m}^{(1)}(1) = (1-q)\left(a_1^{(1)}(q) + q a_0^{(1)}(q) + \textstyle\sum_{m=2}^{\infty} q^m\right) =$$

$$(1-q)\left(1 + q + (\textstyle\sum_{m=0}^{\infty} q^m) - 1 - q\right) = (1-q)\frac{1}{1-q} = 1$$

A.0.4 $T(q)$

$T(q)$ can be solved in the two regions for the parameter q given in 3.4.

In the case that $q \in [0, \frac{1}{2}]$

$$Q(q) = \sum_{m=0}^{\infty} P_{1,q}(m) a_{1-m}^{(0)}(q) = p \sum_{m=0}^{\infty} q^m a_{1-m}^{(0)}(q) = (1-q)\left(a_1^{(0)}(q) + \sum_{m=1}^{\infty} q^m\right) =$$

$$p\left(\frac{q}{1-q} + (\sum_{m=0}^{\infty} q^m) - 1\right) = (1-q)\left(\frac{q}{1-q} + \frac{1}{1-q} - 1\right) = q + 1 - (1-q) = 2q.$$

The case $q \in [\frac{1}{2}, 1]$ is identical to the one carried above for $Q(q)$.

Bibliography

[1] Satoshi Nakamoto. Bitcoin p2p virtual currency. http://www.bitcoin.org/.

[2] Meni Rosenfeld. Analysis of hashrate-based double-spending. https://bitcoil.co.il/Doublespend.pdf/.

[3] Ittay Eyal, Emin Gun Sirer. Majority is not Enough: Bitcoin Mining is Vulnerable. http://arxiv.org/abs/1311.0243

[4] Yonatan Sompolinsky, Aviv Zohar Accelerating Bitcoins Transaction Processing http://www.cs.huji.ac.il/ avivz/pubs/13/btc$_s calability_f ull.pdf$