The Phase Space of Block Withholding Mining Strategies

Assaf Shomer

December 21, 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 main-branch and rip the rewards associated with the published 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. Such strategies turn out to be beneficial only when the miner is "powerful" enough in a precise sense defined below.

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.

1.2 Three mining strategies

1.2.1 Standard miners

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.

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

1.2.2 Block withholding strategies

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

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 (honestly mined) blocks in favour of their $m > n$

[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.

secretly mined ones.

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.

1.2.3 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 following either one of the block-withholding strategies described above.

1.3 Setup

Let us denote by $\mathcal{H}$ the total hashing power of the network and divide it abstractly into an *Honest* part which holds a portion $p\mathcal{H}$ of the total hashing power (where $p \in [0,1]$) and an *Attacker* 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 honest miners continue to mine on top of it ($B_{L+1}, B_{L+2}, \dots$) while the attackers are building a separate branch on top of B_L ($\widetilde{B}_{L+1}, \widetilde{B}_{L+2}, \dots$) with the aim of overtaking it:

$$\begin{array}{lll} \cdots \to B_L \to \quad B_{L+1} \to B_{L+2} \to \cdots \to B_{L+n} & \text{Main} \\ \qquad\quad \searrow & \\ \qquad\quad \widetilde{B}_{L+1} \to \widetilde{B}_{L+2} \longrightarrow \quad \dots \longrightarrow \widetilde{B}_{L+m} & \text{Secret} \end{array} \tag{1.1}$$

Treating block mining as a negative binomial random variable, the probability $P_{n,p}(m)$ that m blocks are mined by the attackers **before** n blocks were honestly mined is proportional to $p^n q^m$ and can be shown (appendix A.1) to be given by

$$P_{n,q}(m) = \binom{n+m-1}{m}(1-q)^n q^m \quad n = 1, 2, \dots \tag{1.2}$$

The probability $a_{n,m}(q)$ that the attackers manage to catch-up and overtake the blockchain given the situation above[2] is given by a Markov chain that depends only on the advantage z of the honest network over the attackers $z = n - m$ defined by the recurrence relation

$$a_z(q) = (1-q)\,a_{z+1}(q) + q\,a_{z-1}(q) \tag{1.3}$$

The relation can be solved with boundary conditions[3] $a_{-1} = 1, a_\infty = 0$ by

$$a_z(q) = \begin{cases} \left(\dfrac{q}{1-q}\right)^{z+1} & q \in [0, \dfrac{1}{2}] \quad \text{and} \quad z = 0, 1, 2 \dots \\ 1 & \text{otherwise} \end{cases} \tag{1.4}$$

For example, to find the probability of a **double-spend attack** on a transaction included in a block B_L with n confirmations, the attacker needs to catchup from a deficit of $n-(m+1)$. The extra block $m+\mathbf{1}$ is the block where the amount spent in B_L was spent again (or resent to the attacker) thus constituting a double-spend attack. This block is denoted with an asterisk B_L^* in 1.5:

$$\begin{array}{lll} \cdots \to B_{L-1} \to & \overbrace{B_L \to B_{L+1} \to \cdots \to B_{L+n-1}}^{n \text{ confirmations}} & \text{Main} \\ \searrow & & \\ & \underbrace{\widetilde{B}_L^* \to \widetilde{B}_{L+1} \longrightarrow \quad \dots \longrightarrow \widetilde{B}_{L+m}}_{(m+1) \text{ blocks}} & \text{Secret} \end{array} \tag{1.5}$$

This attack was first analyzed in [1] [4], treated more accurately in [2] and was shown to be

$$D_n(p) = \sum_{m=0}^{\infty} P_{n,p}(m)\, a_{n-(m+1)}(p) \tag{1.6}$$

1.4 Block withholding attack - Type I

In this section we calculate the probability of success of a miner with relative power q following the type I strategy in replacing the top of the block-chain with her secret branch. Let $Q(q)$ be the probability that the type I miners succeed in mining a secret branch on top of B_L that is longer than the main branch, which allows them to publish it and replace B_{L+1}, and all the blocks honestly mined on top of it.

[2] Namely, that from the beginning of the experiment until the moment the honest network mines it's nth block on top of B_L, the attackers managed to mine m blocks on top of B_L constituting their secret branch.

[3] Note that the condition $a_{-1} = 1$ encodes the fact that the attack is successful once the secret chain is longer than the main chain.

[4] Approximated by a Poisson process.

The type 0 strategy is successful when applied on top of the block B_L if the type 0 miners manage to catch-up on B_{L+1} after starting with $m = 0, 1, \ldots$ blocks. The starting point for the catch-up process for some m is shown below:

$$\begin{array}{lll} \cdots \to B_L \to & B_{L+1} & \text{Main} \\ \quad\searrow & & \\ & \widetilde{B}_{L+1} \to \widetilde{B}_{L+2} \longrightarrow \quad \ldots \longrightarrow \widetilde{B}_{L+m} & \text{Secret} \end{array} \tag{1.7}$$

There are two differences from a double-spend attack described above. One is that we are not requiring a particular number of blocks mined on top of B_L before the secret branch is published. Secondly, we don't require the attacker started the catch-up (with probability of success captured in equation 1.4) after mining at least one block.

Apart from that, the math is very similar. Formally

$$Q(q) = \sum_{m=0}^{\infty} P_{1,q}(m)\, a_{1-m}(q) \tag{1.8}$$

which results to (see details in appendix A.2)

$$Q(q) = \begin{cases} \dfrac{q^2}{1-q}\,(3-2q) & q \in [0, \frac{1}{2}] \\ 1 & q \in [\frac{1}{2}, 1] \end{cases} \tag{1.9}$$

In Figure 1.1 we plot the probability of a successful attack as a function of the relative hashing power q against the probability of the attacker being honest, in which case his probability of success is just q

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 calculate:

$$\frac{q^2}{1-q}\,(3-2q) \geq q \tag{1.10}$$

which since $0 \leq q \leq 1$ gives the condition $q \geq q_0$ where

$$q_0 = 1 - \frac{1}{\sqrt{2}} \sim 0.293 \tag{1.11}$$

Thus, type I strategy is better than the standard strategy for $q > q_0$.

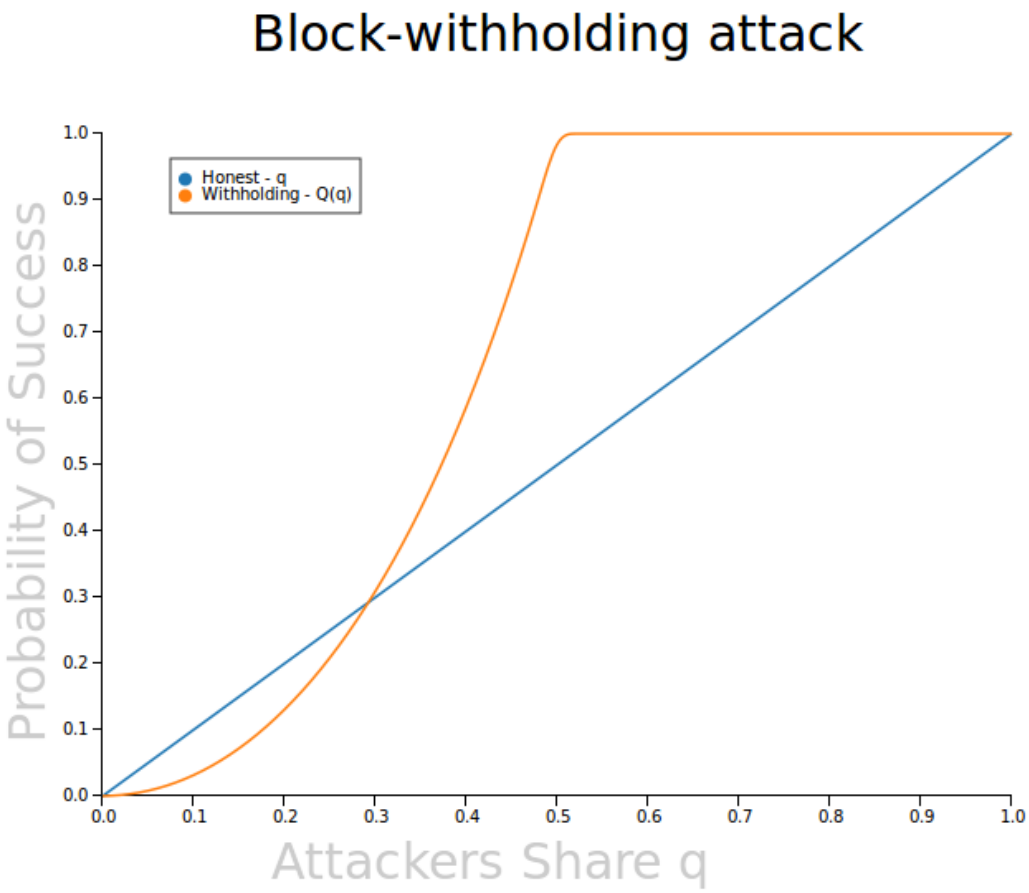

Figure 1.1: The orange curve plots the probability that the attackers manage to uproot the next honest block and replace it with one of their own. The blue curve is the baseline probability for an honest miner with the same hashing power q

1.5 Block withholding attack - Type 0

In this section we analyse the type 0 strategy probability of success. Instead of publishing the secret branch when it is longer than the main branch, the miners that follow this strategy publish it one step before when the length of the secret branch is the same as the length of 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 short period of time different parts of the network may be aware of different, and equally valid, longest branches. In such a case, each sub-network continues mining it's branch until the next block is mined by either one of them and a new block-chain is established[5]. Following the notation used in [3] let us denote by γ the ratio of standard miners that choose to mine on top of the Type 0 branch. This means that $q+\gamma p$ of the total hashing power is now dedicated to making the attackers branch the longest. With some probability the attacker's branch ends 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 1.14 but use a Markov chain with boundary condition reflecting a tie instead of wining, and multiply that by the probability of an attacker with hashing power $q+\gamma p$ wining the race starting from that point.

Formally, we want to solve 1.3 with boundary conditions $b_0 = 1, b_\infty = 0$ which is solved by:

$$b_z(q) = \begin{cases} \left(\frac{q}{1-q}\right)^z & q \in [0, \frac{1}{2}] \quad \text{and} \quad z = 0, 1, 2 \dots \\ 1 & \text{otherwise} \end{cases} \tag{1.12}$$

Using the same logic used to derive 1.13 we get the probability for a tie

$$T(q) = \sum_{m=0}^{\infty} P_{1,q}(m) b_{1-m}(q) \tag{1.13}$$

resulting in (see details in appendix A.3)

$$T(q) = \begin{cases} 2q & q \in [0, \frac{1}{2}] \\ 1 & q \in [\frac{1}{2}, 1] \end{cases} \tag{1.14}$$

Now the attacker, joined by γ of the honest miners are competing with the rest of the honest miners. The probability to win starting from a tie is thus given by 1.4

$$a_0(q_{eff}) = \begin{cases} \frac{q_{eff}}{1-q_{eff}} & q_{eff} \in [0, \frac{1}{2}] \\ 1 & q_{eff} \in [\frac{1}{2}, 1] \end{cases} \tag{1.15}$$

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

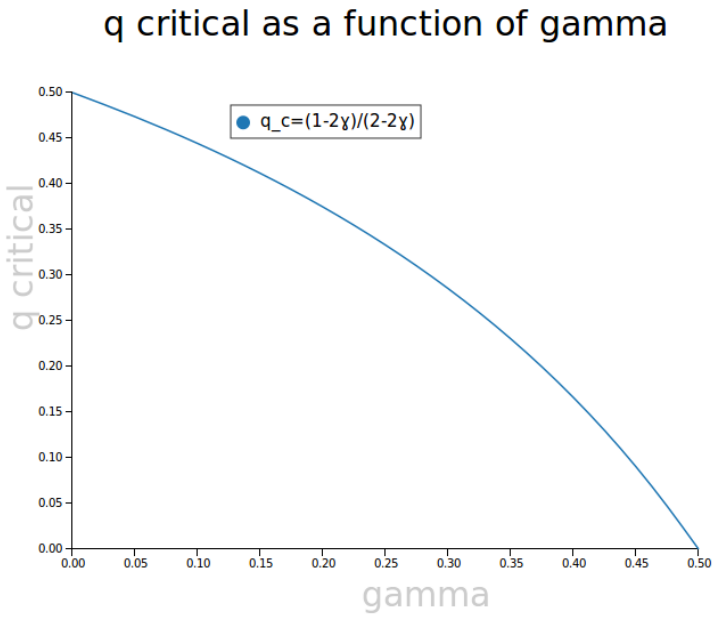

Figure 1.2: The value of q_c as a function of γ.

where

$$q_{eff} = q + \gamma p = q + \gamma(1-q) \tag{1.16}$$

The condition $q_{eff} \in [0, \frac{1}{2}]$ translates to $0 \leq q \leq q_c(\gamma)$ where

$$q_c(\gamma) = \frac{1-2\gamma}{2-2\gamma} \tag{1.17}$$

q_c (depicted in figure 1.2) satisfies $0 \leq q_c(\gamma) \leq \frac{1}{2}$, monotonically decreases with γ and hits 0 when[6] $\gamma = \frac{1}{2}$.

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

$$S_\gamma(q) = \underbrace{T(q)}_{\text{reach a tie}} \cdot \underbrace{a_0(q_{eff})}_{\text{win given a tie}} = \begin{cases} 2q \cdot \frac{q_{eff}}{1-q_{eff}} = 2q \cdot \frac{q(1-\gamma)+\gamma}{(1-q)(1-\gamma)} & q \in [0, q_c] \\ 2q & q \in [q_c, \frac{1}{2}] \\ 1 & q \in [\frac{1}{2}, 1] \end{cases} \tag{1.18}$$

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

$$S_{\gamma \geq \frac{1}{2}}(q) = T(q) \cdot a_0(q_{eff}) = \begin{cases} 2q & q \in [0, \frac{1}{2}] \\ 1 & q \in [\frac{1}{2}, 1] \end{cases} = min(2q, 1) \tag{1.19}$$

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

In figure 1.3 we plot the probability of a successful type 0 attack for various values of the parameter γ, against the benchmark honest probability of success and the Type I attack probability of success.

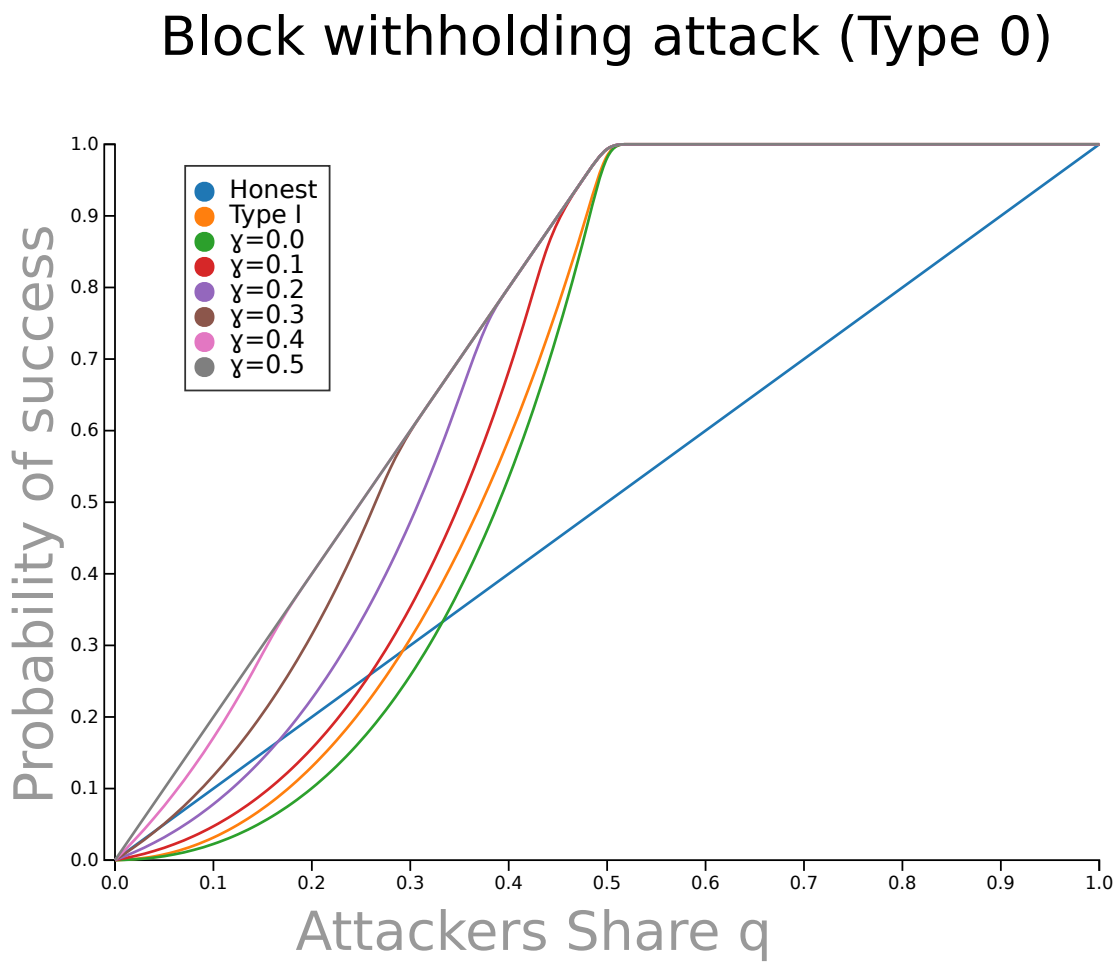

Figure 1.3: The probability of success of a type II block withholding attack as a function of γ. The blue curve plots the honest probability of success, and the orange curve plots the type I attack.

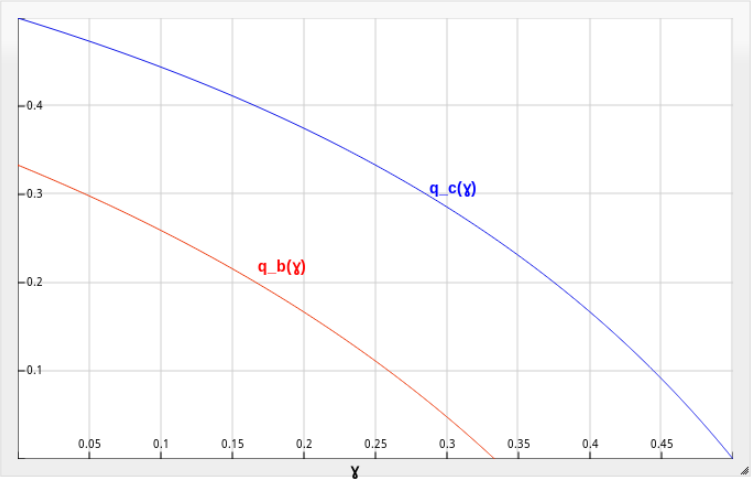

Figure 1.4: The value of q_c and q_b as a function of γ.

1.6 The γ, q phase space

1.6.1 When is a Type 0 attack beneficial

To decide if a block-withholding attack of type 0 is beneficial or not we should compare it to the honest probability of success and to a Type I attack.

Comparing type 0 to the standard strategy

First note that in the second and third regimes in equation 1.18 (or for any q if $\gamma \geq \frac{1}{2}$) the type 0 attacks is beneficial over the honest strategy for any q, because for any q it holds 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 attacks starts being beneficial over the honest strategy by solving

$$2q \cdot \frac{q(1-\gamma)+\gamma}{(1-q)(1-\gamma)} \geq q \tag{1.20}$$

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

$$q_b = \frac{1-3\gamma}{3-3\gamma} \tag{1.21}$$

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 1.4.

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.

Taking all three regimes into account we conclude that the type 0 attack is beneficial over the honest strategy when

$$S_\gamma(q) \geq q \Longrightarrow \begin{cases} q > \dfrac{1-3\gamma}{3-3\gamma} & \gamma \in [0, \frac{1}{3}] \\ any\ q & \gamma \in [\frac{1}{3}, 1] \end{cases} \tag{1.22}$$

we can summarize further by writing

$$S_\gamma(q) \geq q \Longrightarrow q > max \left\{ \frac{1-3\gamma}{3-3\gamma}, 0 \right\} \tag{1.23}$$

Next we compare this attack to a Type I attack.

1.6.2 Comparing Type 0 to Type I

There are two interesting comparisons one can make between Type 0 and Type I attacks.

One is to compare how they match against the honest 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.

This type 0 strategy wins earlier (in fact already at $q = 0$) when $\gamma \geq \frac{1}{3}$. When $\gamma < \frac{1}{3}$ we can compare $q_b(\gamma)$ (given in equation 1.21) with q_0 (given in equation 1.11).

$$\frac{1-3\gamma}{3-3\gamma} < 1 - \frac{1}{\sqrt{2}} \tag{1.24}$$

Solving for γ we obtain that for $\gamma_c \leq \gamma$ a type 0 strategy is beneficial over the standard strategy sooner (i.e. smaller q) than a type I strategy, where γ_c is given by:

$$\gamma_c = 1 - \frac{2}{3}\sqrt{2} \sim 0.0572 \tag{1.25}$$

Indeed, you can see in Figure 1.3 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 honest 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 $q_0 = 1 - \frac{1}{\sqrt{2}}$).

Finally, ignoring the honest 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:

$$2q \cdot \frac{q(1-\gamma)+\gamma}{(1-q)(1-\gamma)} \geq \frac{q^2}{1-q}(3-2q)\text{‘} \tag{1.26}$$

which gives the condition

$$2q^2 - q + \frac{2\gamma}{1-\gamma} \geq 0 \tag{1.27}$$

This condition is satisfied in two regimes for γ.

$$S_\gamma(q) \geq Q(q) \Longrightarrow \begin{cases} any\ q & \gamma \in [\frac{1}{17}, 1] \\ q < q_-(\gamma) \quad or \quad q > q_+(\gamma) & \gamma \in [0, \frac{1}{17}] \end{cases} \tag{1.28}$$

where

$$q_\pm(\gamma) = \frac{1}{4}\left(1 \pm \sqrt{\frac{1-17\gamma}{1-\gamma}}\right) \tag{1.29}$$

1.7 The Strategy Phase Space

Now we can chart the strategy phase space parametrized by γ, q.

Let us explore the $\gamma \in [0,1] \times q \in [0,1]$ phase space 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 $\gamma < \frac{1}{17}$.

In figure 1.5 we those three curves are plotted. Note the interesting fact that all three curves intersect in the single point $\gamma = \gamma_c, q = q_0$. This fact makes the phase space much simpler to analyse.

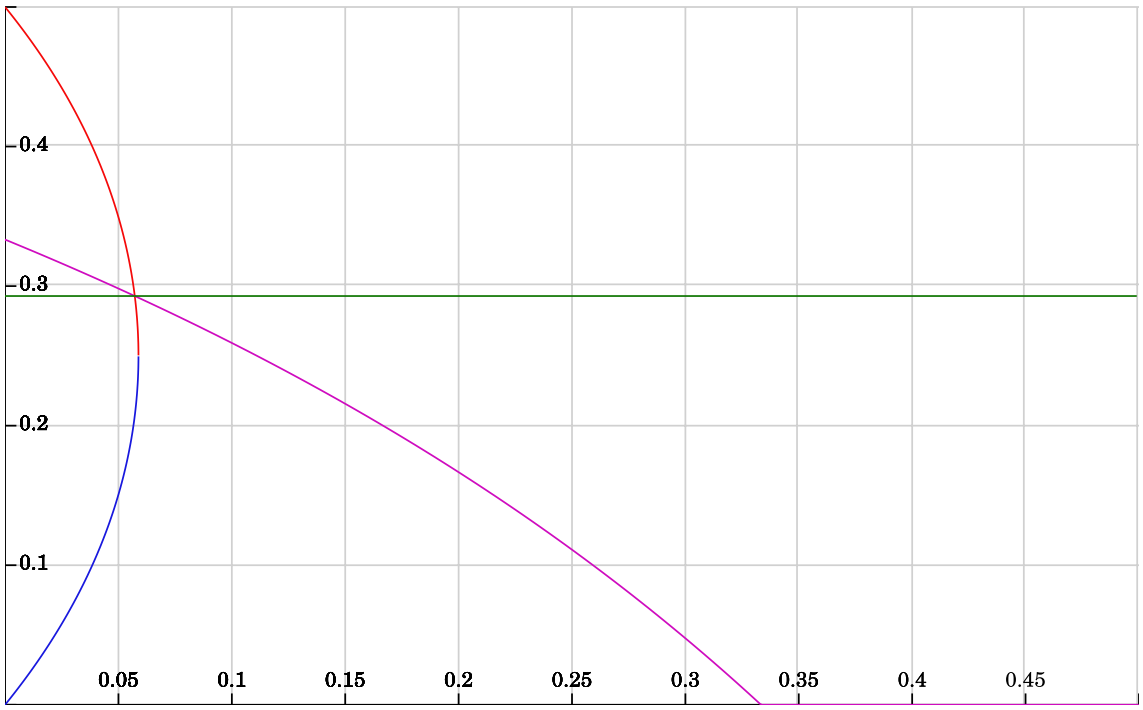

Figure 1.5: The 4 functions sectioning the γ, q phase space.

- 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 1.27. Note that this division doesn't specify whether any of the strategies is better than the standard one.

- The Type I strategy is more beneficial than the standard strategy in the region above the horizontal line $q = q_0$. .

- The 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 $\gamma = 1$).

The resulting phase space division is thus given by figure 1.6.

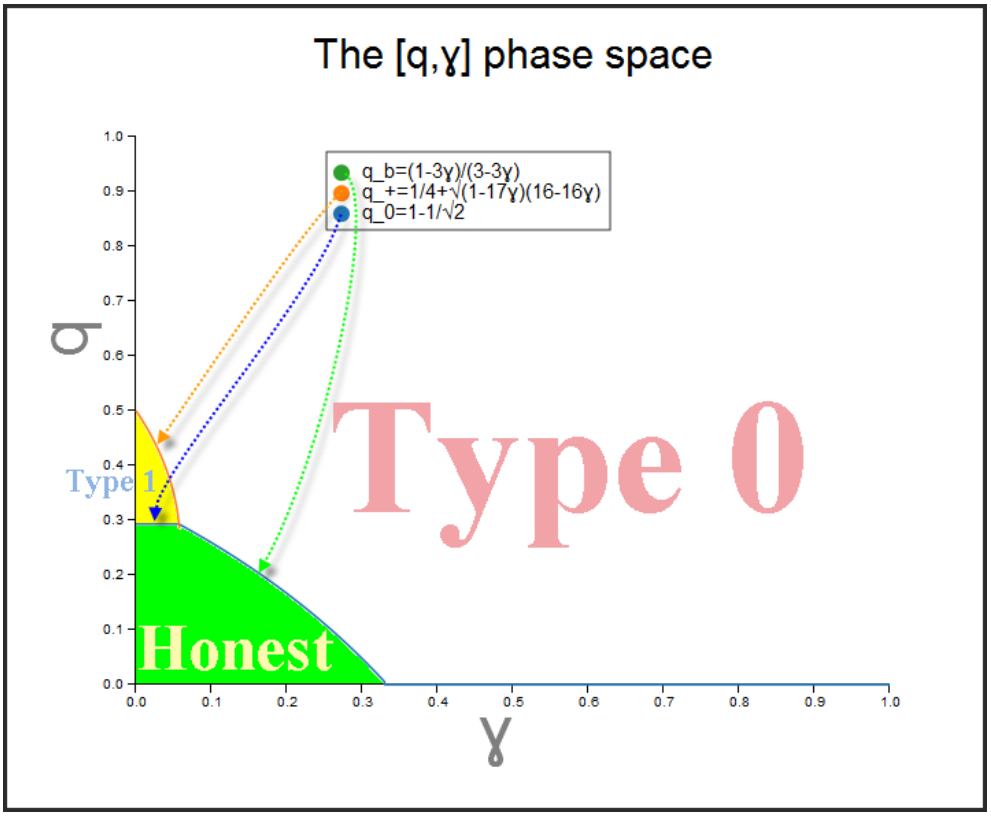

Figure 1.6: The 3 regions of the q, γ phase space. The standard strategy is best in the region near the origin. Type I is best in the little area on top of the standard region. In the rest of phase space the Type 0 strategy is most beneficial.

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 *strength*" $\mathtt{S}(q,\gamma) \equiv \sqrt{q^2+\gamma^2}$.

This definition is partly motivated by the intuitive notion that having a large γ is (in some vague sense) "similarly difficult" to having a large q and a typical miner will have both parameters in similar scales. In a sense, the above phase space diagram lends credibility to this intuitive notion because it suggest a rough symmetry[7] between the parameters γ and q.

There are a few remarks in order:

- Figure 1.6 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 probability of success is strictly 1) only in the top half of phase space, in the region where $q \geq \frac{1}{2}$, a.k.a the 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 **??**.

[7] All we mean by that is that figure 1.6 is almost symmetric under a rotation along the 45^{deg} angle that rotates $\gamma \leftrightarrow q$.

Appendix A

Calculation Details

A.1 Probability distribution

To find the normalization in the case $n > 0$ we use the useful binomial identity holding for any complex s inside the unit circle ($|s| < 1$)

$$\frac{1}{(1-s)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} s^k.$$

It is now straightforward to show that 1.2 is indeed a probability distribution

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

A.2 Calculating $Q(q)$

$Q(q)$ can be solved in the two regions for the parameter q given in 1.4.

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

$$Q(q) = \sum_{m=0}^{\infty} P_{1,q}(m) a_{1-m}(q) = p \sum_{m=0}^{\infty} q^m a_{1-m}(p) = p\left(a_1(p) + q a_0(p) + \sum_{m=2}^{\infty} q^m\right) =$$
$$p\left(\left(\frac{q}{p}\right)^2 + q\frac{q}{p} + \left(\sum_{m=0}^{\infty} q^m\right) - 1 - q\right) = p\left(\left(\frac{q}{p}\right)^2 + \frac{q^2 p}{p^2} + \frac{1}{p} - (1+q)\right) =$$
$$\frac{1}{p}\left(q^2(1+p) + p - p^2(1+q)\right) = \frac{1}{p}\left(q^2(1+p) + p - p^2(1+q)\right) =$$
$$\frac{1}{1-q}\left(q^2(2-q) + 1 - q - (1-q)^2(1+q)\right) =$$
$$\frac{1}{1-q}\left(2q^2 - q^3 + 1 - q - 1 + 2q - q^2 - q + 2q^2 - q^3\right) = \frac{q^2}{1-q}(3-2q)$$

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

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

A.3 Calculating $T(q)$

$T(q)$ can be solved in the two regions for the parameter q given in 1.4.

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

$$Q(q) = \sum_{m=0}^{\infty} P_{1,q}(m) b_{1-m}(q) = p\sum_{m=0}^{\infty} q^m b_{1-m}(p) = p\left(b_1(q) + \sum_{m=1}^{\infty} q^m\right) =$$
$$p\left(\frac{q}{p} + (\sum_{m=0}^{\infty} q^m) - 1\right) = p\left(\frac{q}{p} + \frac{1}{1-q} - 1\right) = q + 1 - p = 2q.$$

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$_s calability_f ull.pdf$