Analysis of block survival probabilities

Assaf Shomer

November 28, 2013

Abstract

Analysis of block survival probabilities in the presence of miners that employ non-traditional mining strategies in the interest of increasing their reward

Contents

Chapter 1

Introduction

1.1 Bitcoin and mining

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

1.2 The attack strategy

1.2.1 Honest Miners

The honest miners following the bitcoin protocol described in [1], publish each block as soon as it is discovered and switch their mining efforts to the head of the block-chain any time a new block is found.

1.2.2 Block withholding Miners

The attackers do not share their newly found blocks and instead work on a **secret** branch of the block-tree until such time that their branch 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 $m > n$ secretly mined ones.

1.2.3 Goal

Our goal is to calculate the probability that an honestly mined block is retained in the block-chain in the face of an attacker of relative power q. We will calculate this quantity by calculating the complement probability that a block withholding attacker succeeds in decapitating the block-chain mined on top of a given block.

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 block-chain 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 ($\tilde{B}_{L+1}, \tilde{B}_{L+2}, \dots$) with the hope of overtaking it.

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

$$P_{n,p}(m) = \binom{n+m-1}{m} p^n q^m \quad n = 1, 2, \dots \tag{1.1}$$

The probability $a_{n,m}(p)$ that the attackers manage to overtake the block-chain 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 $z = n - m$ defined by the recurrence relation

$$a_z(p) = p a_{z+1}(p) + q a_{z-1}(p) \tag{1.2}$$

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

$$a_z(p) = \begin{cases} \left(\frac{q}{p}\right)^{z+1} & q \in [0, \frac{1}{2}] \quad \text{and} \quad z = 0, 1, 2 \dots \\ 1 & \text{otherwise} \end{cases} \tag{1.3}$$

For example, to find the probability of a double spend after n confirmations, the attacker needs to mine B_{L+1} (assumed as the starting point so no need to multiply by q) and then catchup from a deficit of $n - (m+1)$ where the extra block is the block where the double spend occurs. This was calculated in [2] to be

$$D_n(p) = \sum_{m=0}^{\infty} P_{n,p}(m) a_{n-(m+1)}(p) \tag{1.4}$$

1.4 Probability of success

In this paper, as explained in 1.2.3, we are interested in a different quantity.

[1] Namely, that the honest network mined n blocks on top of B_L and the attackers managed, during that time, to mine m blocks on top of B_L constituting their hidden branch.

Let $Q(p)$ be the probability that the attackers succeed in decapitating the block-chain on top of B_L. This event occurs if the attackers manage to catch-up on B_{L+1} after starting with $m = 0, 1, \ldots$ blocks[2].

Formally

$$Q(p) = \sum_{m=0}^{\infty} P_{1,p}(m) a_{1-m}(p) \tag{1.5}$$

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

$$Q(p) = \begin{cases} \frac{q^2}{1-q}(3-2q) & q \in [0, \frac{1}{2}] \\ 1 & q \in [\frac{1}{2}, 1] \end{cases} \tag{1.6}$$

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

We see that an attacker improves his chances in the range $q > 1 - \frac{1}{\sqrt{2}} \sim 0.293$

[2]Note that we do not need to multiply this by the probability p that the honest miners mine the next block. This fact is implicit in the probability distribution 1.1 calculated under the assumption that the n^{th} block is mined by the honest miners.

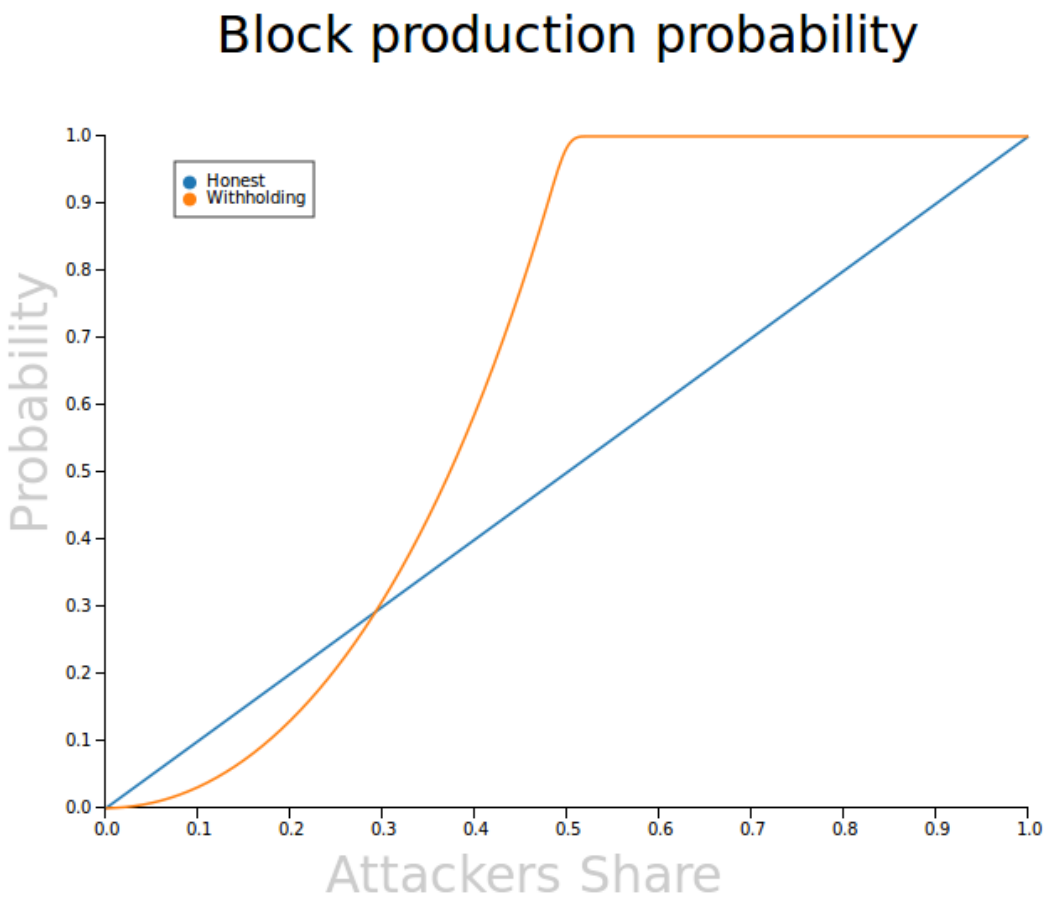

Figure 1.1: The orange curve plots the probability that the attackers manage to uproot the next honest block and replace it with one of their own. The blue curve is the baseline probability for an honest miner with the same hashing power q

1.5 Attacker's reward

Next we calculate the expected reward of a block-withholding attacker. We assume for simplicity that the reward of each party is simply proportional to the number of blocks mined by that party.

Formally

$$R(p) = \sum_{m=0}^{\infty} m \cdot P_{1,p}(m)\, a_{1-m}(p) \tag{1.7}$$

which results to (see details in appendix A.3)

$$R(p) = \begin{cases} \dfrac{q^2}{1-q}\,(3-2q) & q \in [0, \dfrac{1}{2}] \\ \dfrac{q}{1-q} & q \in [\dfrac{1}{2}, 1] \end{cases} \tag{1.8}$$

In Figure 1.2 we plot the attackers reward as a function of the relative hashing power q against the probability of the reward for an honest miner with the same hashing power, which is just q.

We note a few things.

- In the range $q \in [0, \frac{1}{2}]$ $R(p)$ is identical to $Q(p)$.
- As expected the reward of the attackers exceeds the honest reward at the same point where the probability of success exceeds the honest benchmark. i.e. when $q > 1 - \frac{1}{\sqrt{2}} \sim 0.293$
- As $q \to 1$ the reward of the attackers diverges, because he basically controls the blockchain and can plant as many blocks as he desires.
- This may be a little hard to see in Figure 1.2 but The function $R(p)$ is continuous but not continuously differentiable. At the point $q = \frac{1}{2}$ the derivative jumps from 4 to 5 (see appendix **??** for details).

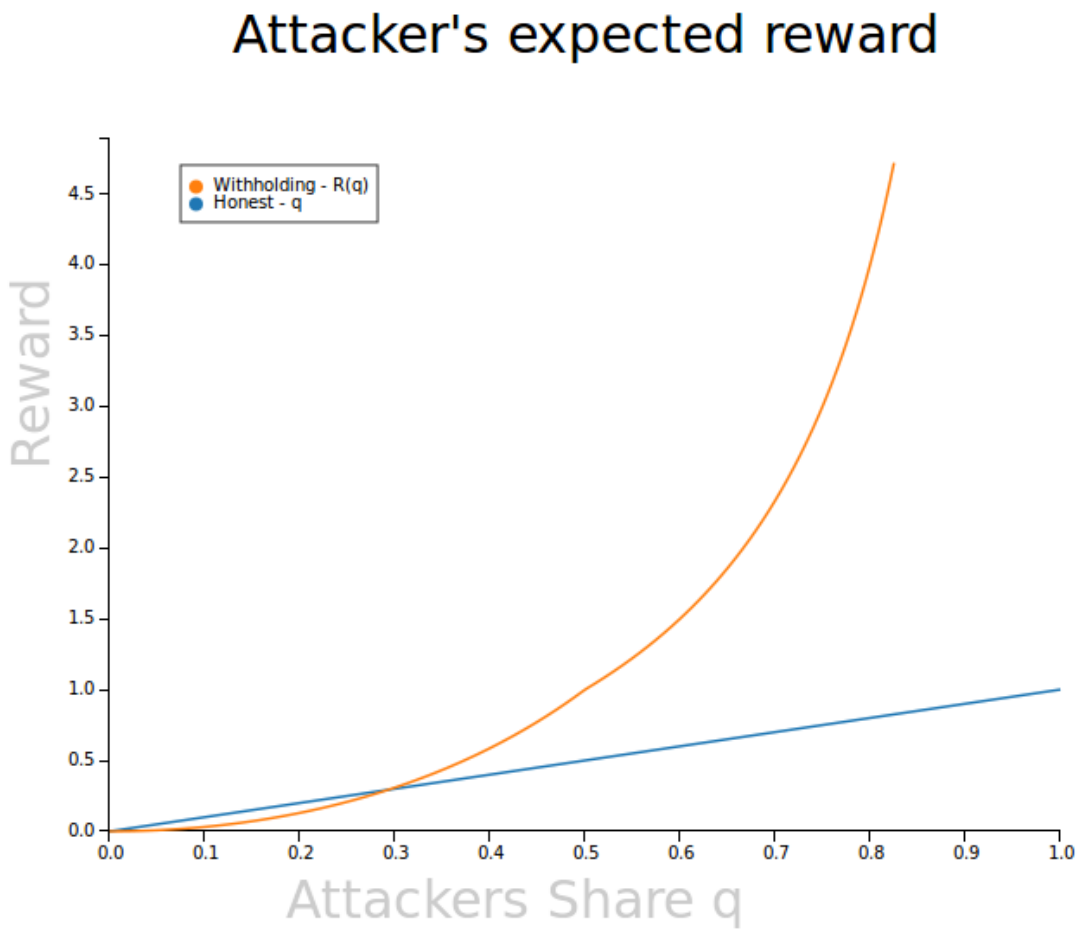

Figure 1.2: The orange curve plots the attacker's reward. The blue curve is the baseline reward for an honest miner with the same hashing power q.

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 1.1 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 $Q(p)$

$Q(p)$ can be solved in the two regions for the parameter q given in 1.3.

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

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

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

$$Q(p) = p\sum_{m=0}^{\infty} q^m a_{1-m}(p) = p\left(a_1(p) + qa_0(p) + \sum_{m=2}^{\infty} q^m\right) =$$
$$p\left(1 + q + \left(\sum_{m=0}^{\infty} q^m\right) - 1 - q\right) = p\frac{1}{p} = 1$$

A.3 Calculating $R(p)$

$R(p)$ can be solved in the two regions for the parameter q given in 1.3.

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

$$R(p) = p\sum_{m=0}^{\infty} m \cdot q^m a_{1-m}(p) = p\left(qa_0(p) + \sum_{m=2}^{\infty} m \cdot q^m\right) =$$
$$p\left(q\frac{q}{p} + \left(\sum_{m=0}^{\infty} m \cdot q^m\right) - q\right) = p\left(\frac{q^2}{p} + q\partial_q\left(\sum_{m=0}^{\infty} q^m\right) - q\right) =$$
$$q^2 + pq\partial_q\left(\frac{1}{1-q}\right) - pq = q^2 + pq\left(\frac{1}{p^2} - 1\right) = q^2 + q\frac{(1+p)(1-p)}{p} =$$
$$q^2\left(1 + \frac{2-q}{1-q}\right) = \frac{q^2}{1-q}(3 - 2q) = Q(p)$$

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

$$R(p) = p\sum_{m=0}^{\infty} m \cdot q^m a_{1-m}(p) = p\left(qa_0(p) + \sum_{m=2}^{\infty} m \cdot q^m\right) =$$
$$p\left(q + \left(\sum_{m=0}^{\infty} m \cdot q^m\right) - q\right) = pq\partial_q\left(\frac{1}{1-q}\right) = \frac{q}{1-q}$$

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/.