International Journal of Theoretical and Applied Finance
Vol. 21, No. 8 (2018) 1850053 (32 pages)

DOI: 10.1142/S021902491850053X

World Scientific
www.worldscientific.com

DOUBLE SPEND RACES

CYRIL GRUNSPAN*

Research Center, Pôle Universitaire Léonard de Vinci
Labex Réfi, 92916 Paris La Défense Cedex, France
cyril.grunspan@devinci.fr

RICARDO PÉREZ-MARCO

IMJ-PRG, CNRS, Labex Réfi, Université Paris Dıderot
Bâtiment Sophie Germain, 8 place Aurélie Nemours
Boite Courrier 7012, 75205 Paris Cedex 13, France
ricardo.perez.marco@gmail.com

Received 3 January 2018
Revised 18 September 2018
Accepted 24 September 2018
Published 21 November 2018

To the memory of our beloved Teacher André Warusfel who taught us how to have fun with the applications of mathematics.

We correct the double spend race analysis given in Nakamoto's foundational Bitcoin article and find the exact closed-form formula for the probability of success of a double spend attack using the regularized incomplete beta function. We give the first proof of its exponential decay on the number of confirmations, often cited in the literature, and find an asymptotic formula. Larger number of confirmations are required compared to those given by Nakamoto. We also compute this probability conditional to the knowledge of the time of the confirmations. This provides a finer risk analysis than the classical one.

Keywords: Bitcoin; blockchain; double spend; mining; proof-of-work; regularized incomplete beta function.

1. Introduction

The main breakthrough in Nakamoto (2008) is the solution to the *double spend problem*. Before this discovery no one knew how to avoid the double spending of an electronic currency unit without the supervision of a central authority. This made Bitcoin the first form of *peer-to-peer* (P2P) electronic currency.

A double spend attack can only be attempted with a substantial fraction of the hashrate used in the *proof-of-work* of the Bitcoin network. The attackers will

*Corresponding author.

start a *double spend race* against the rest of the network to replace the last blocks of the blockchain by secretly mining an alternate blockchain. In the last section of the Bitcoin's white paper, Nakamoto (2008) computes the probability that the attackers succeed. However, Nakamoto's analysis is not accurate since he makes the simplifying assumption that honest miners validate blocks at the expected rate. We present a correct analysis and give a closed-form formula for the exact probability.

Theorem 1.1. *Let $0 < q < 1/2$, respectively $p = 1 - q$, be the relative hash power of the group of attackers, respectively of honest miners. After $z \geq 1$ blocks have been validated by the honest miners, the probability of success of the attackers is*

$$P(z) = I_{4pq}\left(z, \frac{1}{2}\right),$$

where $I_x(a, b)$ is the regularized incomplete beta function:

$$I_x(a, b) = \frac{\Gamma(a + b)}{\Gamma(a)\Gamma(b)} \int_0^x t^{a-1}(1 - t)^{b-1} dt.$$

In general, for $z \geq 2$, these probabilities $P(z)$ are larger than those $P_{SN}(z)$ obtained by Nakamoto. From the standpoint of Bitcoin security, this shows that larger confirmation times z are necessary compared to those z_{SN} given by Nakamoto, in particular this happens when the share of hashrate q of the attackers is important. Table 1 shows the number of confirmations (z) to wait compared to those z_{SN} given by Nakamoto depending on the attacking hashrate $0 < q < 0.5$ for a probability of success of the attackers less than 0.1%.

Nakamoto (2008) claims that the probability $P(z)$ converges exponentially to 0 with z. This result is intuitively expected and cited at large but there is no proof available in the literature. We give here the first proof of this result. More precisely, using the closed-form formula and the asymptotics for the incomplete beta function, we give precise asymptotics both for $P_{SN}(z)$ and $P(z)$ showing the exponential decay.

Theorem 1.2. *When $z \to +\infty$ we have, with $s = 4pq < 1$,*

$$P(z) \sim \frac{s^z}{\sqrt{\pi(1 - s)z}},$$

and with $\lambda = q/p$, and $c(\lambda) = \lambda - 1 - \log \lambda > 0$,

$$P_{SN}(z) \sim \frac{e^{-zc(\lambda)}}{2}.$$

Table 1. Comparison of the numbers of confirmations.

q	0.10	0.15	0.20	0.25	0.30	0.35	0.40	0.45
z	6	9	13	20	32	58	133	539
z_{SN}	5	8	11	15	24	41	81	340

We check that $-\log s > c(\lambda)$ which means that $P_{SN}(z) \prec P(z)$ for large z. Higher-order asymptotics can be obtained using known higher-order asymptotics for the incomplete beta function and the explicit formulas. Only the first order is relevant for the application to Bitcoin security.

1.1. *A finer risk analysis*

We analyze a new parameter in the risk of a double spend. The probability of success of the attackers increases with the time τ_1 it takes for the z confirmations since then they get more time to secretly mine their alternate blockchain. On the other hand, the task of the attackers is more difficult if the validations happen faster than the expected time. This seems to have been overlooked so far [see the comments in Rosenfeld (2014, p. 8)]. The value of τ_1 is known, therefore what is relevant is the conditional probability assuming τ_1 is known. We introduce the dimensionless parameter κ which measures the deviation from average time:

$$\kappa = \frac{\tau_1}{zt_0},$$

where t_0 is the average time of block validation by honest miners ($t_0 = \tau_0/p$, where $\tau_0 = 10\,\text{min}$ for the Bitcoin network).

We study the probability $P(z, \kappa)$ of success of the attackers. We can recover the previous probabilities with $P(z, \kappa)$, $0 < \kappa < 1$.

Theorem 1.3. *For $z \geq 1$, we have*

$$P_{SN}(z) = P(z, 1),$$

and

$$P(z) = \int_0^{+\infty} P(z, \kappa) d\rho_z(\kappa),$$

with the density function

$$d\rho_z(\kappa) = \frac{z^z}{(z-1)!} \kappa^{z-1} e^{-z\kappa} d\kappa.$$

We also give a closed-form formula for $P(z, \kappa)$ (see Fig. 1).

Theorem 1.4. *For $z \geq 1$, we have*

$$P(z, \kappa) = 1 - Q\left(z, \frac{\kappa z q}{p}\right) + \left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{p}} Q(z, \kappa z).$$

Here, Q denotes the incomplete gamma function:

$$Q(s, x) = \frac{\Gamma(s, x)}{\Gamma(x)},$$

where $\Gamma(s, x) = \int_x^{+\infty} t^{s-1} e^{-t} dt$. We find also the asymptotics for $z \to +\infty$ for different values of κ.

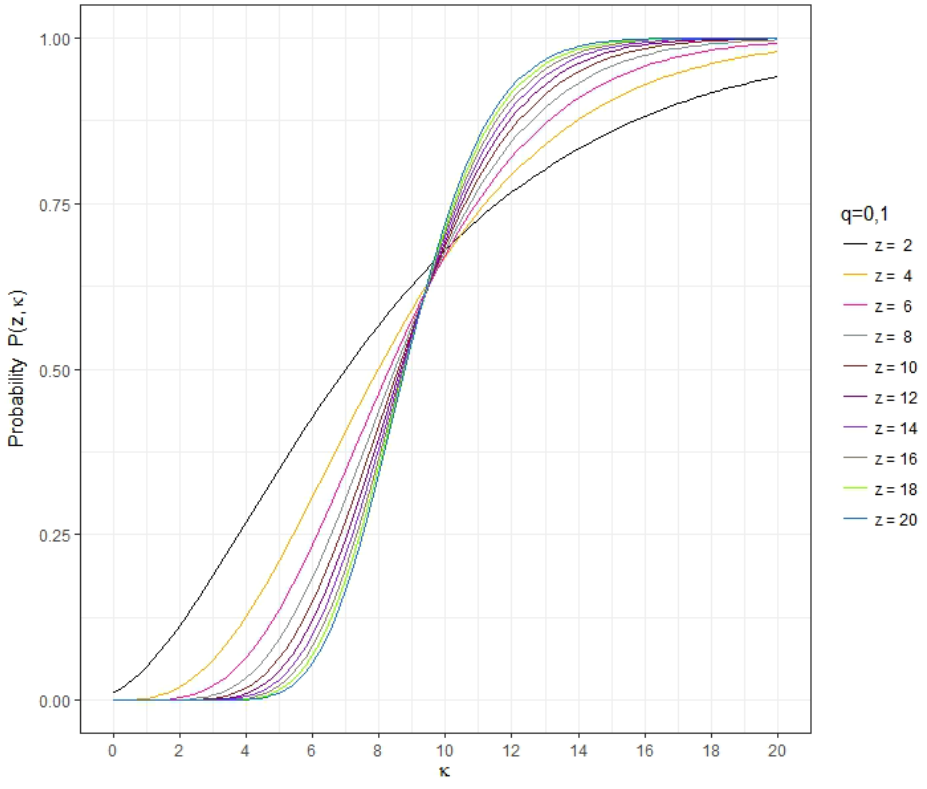

Fig. 1. Probability of success as a function of κ with $q = 0.1$.

Theorem 1.5. *The following hold for* $z \to +\infty$:

(1) *For* $0 < \kappa < 1$,

$$P(z,\kappa) \sim \frac{1}{1-\kappa\lambda}\frac{1}{\sqrt{2\pi z}}e^{-zc(\kappa\lambda)}.$$

(2) *For* $\kappa = 1$,

$$P(z,1) = P_{SN}(z) \sim \frac{1}{2}e^{-zc(\lambda)}.$$

(3) *For* $1 < \kappa < p/q$,

$$P(z,\kappa) \sim \frac{\kappa(1-\lambda)}{(\kappa-1)(1-\kappa\lambda)}\frac{1}{\sqrt{2\pi z}}e^{-zc(\kappa\lambda)}.$$

(4) *For* $\kappa = p/q$, $P(z,p/q) \to 1/2$ *and*

$$P\left(z,\frac{p}{q}\right) - \frac{1}{2} \sim \frac{1}{2\pi z}\left(\frac{1}{3} + \frac{q}{p-q}\right).$$

(5) *For* $p/q < \kappa$, $P(z,\kappa) \to 1$ *and*

$$1 - P(z,\kappa) \sim \frac{\kappa(1-\lambda)}{(\kappa-1)(\kappa\lambda-1)} \frac{1}{\sqrt{2\pi z}} e^{-zc(\kappa\lambda)}.$$

Using a concavity argument we have that $P(1) \leq P_{SN}(1)$, but in general, for $z \geq z_0$, we have $P_{SN}(z) \leq P(z)$. We do compute an explicit, nonsharp, value z_0 for which this inequality holds.

Theorem 1.6. *Let* $z \geq 1$. *A sufficient condition for having* $P_{SN}(z) < P(z)$ *is* $z \geq z_0$ *with* $z_0 = \lceil z_0^* \rceil$ *being the smallest integer greater or equal to*

$$z_0^* = \max\left(\frac{2}{\pi\left(1-\frac{q}{p}\right)^2}, \frac{1}{2\sqrt{2}} - \frac{\left(1+\frac{1}{\sqrt{2}}\right)}{2} \frac{\log\left(\frac{2\psi(p)}{\pi}\right)}{\psi(p)} \right),$$

where $\psi(p) = \frac{q}{p} - 1 - \log(\frac{q}{p}) - \log(\frac{1}{4pq}) > 0$.

We also provide the double entry tables of $P(z,\kappa)$ for different values of (q,κ) for $z = 3$ and $z = 6$. For a complete set of tables for $z = 1, 2, \ldots, 9$ of practical use we refer to the companion article by Grunspan & Pérez-Marco (2017).

2. Mathematics of Mining

We review some basic results in probability [see Feller (1971, p. 8)] and of Bitcoin mining [see Pérez-Marco (2016) for an overview of Bitcoin protocol].

A hashing algorithm digests any file into a fixed length string of bits. The slightest modification of the original file produces a completely different output. The bits of the output appear with a random frequency and it is computationally hard to find collisions (different inputs yielding the same output). Hashing algorithms are used for example to check the integrity and nontampering of files.

The two main hashing algorithms used in the Bitcoin protocol are RIPEMD-160 and SHA-256 that produce outputs of 160 bits and 256 bits, respectively. The mining algorithm consists in performing the double SHA-256 of the block header (doubled to prevent "padding attacks").

The consensus protocol and security in the Bitcoin network rely on the process of Bitcoin mining and validating transactions. It consists of the iteration of computation of block header hashes changing a nonce[a] in order to find a hash below a predefined threshold, the *difficulty*, Nakamoto (2008). For each new hash the work is started from scratch, therefore the random variable $\boldsymbol{T}$ measuring the time it takes

[a]More precisely, a double hash SHA256(SHA256(header)) is computed, changing a nonce and an extra-nonce.

to mine a block is memoryless, which means that for any $t_1, t_2 > 0$,

$$\mathbb{P}[\boldsymbol{T} > t_1 + t_2 \,|\, T > t_2] = \mathbb{P}[\boldsymbol{T} > t_1].$$

Therefore, we have

$$\mathbb{P}[\boldsymbol{T} > t_1 + t_2] = \mathbb{P}[\boldsymbol{T} > t_1 + t_2 \,|\, T > t_2] \cdot \mathbb{P}[\boldsymbol{T} > t_2] = \mathbb{P}[\boldsymbol{T} > t_1] \cdot \mathbb{P}[\boldsymbol{T} > t_2].$$

This equation and a continuity argument determine the exponential function and imply that $\boldsymbol{T}$ is an exponentially distributed random variable:

$$f_{\boldsymbol{T}}(t) = \alpha e^{-\alpha t},$$

for some parameter $\alpha > 0$, the mining speed, with $t_0 = 1/\alpha = \mathbb{E}[\boldsymbol{T}]$.

If $(\boldsymbol{T}_1, \ldots, \boldsymbol{T}_n)$ is a sequence of independent identically distributed exponential random variables (for example $\boldsymbol{T}_k$ is the mining time of the kth block), then the sum

$$\boldsymbol{S}_n = \boldsymbol{T}_1 + \cdots + \boldsymbol{T}_n$$

is a random variable following a gamma density with parameters (n, α) (obtained by convolution of the exponential density):

$$f_{\boldsymbol{S}_n}(t) = \frac{\alpha^n}{(n-1)!} t^{n-1} e^{-\alpha t},$$

and cumulative distribution

$$F_{\boldsymbol{S}_n}(t) = \int_0^t f_{\boldsymbol{S}_n}(u) du = 1 - e^{-\alpha t} \sum_{k=0}^{n-1} \frac{(\alpha t)^k}{k!}.$$

We define the random process $\boldsymbol{N}(t)$ as the number of mined blocks at time t. Setting $S_0 = 0$, we have

$$\boldsymbol{N}(t) = \#\{k \geq 1; \boldsymbol{S}_k \leq t\} = \max\{n \geq 0; \boldsymbol{S}_n < t\}.$$

Since $\boldsymbol{N}(t) = n$ is equivalent to $\boldsymbol{S}_n \leq t$ and $\boldsymbol{S}_{n+1} > t$ we get

$$\mathbb{P}[\boldsymbol{N}(t) = n] = F_{\boldsymbol{S}_n}(t) - F_{\boldsymbol{S}_{n+1}}(t) = \frac{(\alpha t)^n}{n!} e^{-\alpha t},$$

which means that $\boldsymbol{N}(t)$ has a Poisson distribution with expectation αt.

3. Mining Race

We consider the situation described in Sec. 11 of Nakamoto (2008) where a group of attacker miners attempt a double spend attack. The attacker group has a fraction $0 < q < 1/2$ of the total hashrate, and the rest, the honest miners, has a fraction $p = 1 - q$. Thus the probability that the attackers find the next block is q while the probability for the honest miners is p. Nakamoto computes the probability for the attackers to catch up when z blocks have been mined by the honest group. In general, to replace the chain mined by the honest miners and succeed a double spend the attackers need to mine $z + 1$ blocks, i.e. to mine a longer chain. In the

analysis it is assumed that we are not near an update of the difficulty which remains constant.[b]

The first discussion in Sec. 11 of Nakamoto (2008) is about computing the probability q_z of the attackers catching up when they lag by z blocks behind the honest miners. The analysis is correct and is similar to the Gamblers Ruin problem. We review this.

Lemma 3.1. *Let q_n be the probability of the event E_n, "catching up from n blocks behind". We have*

$$q_n = \left(\frac{q}{p}\right)^n.$$

Proof. Note that after one more block has been mined, we have for $n \geq 1$,

$$q_n = qq_{n-1} + pq_{n+1},$$

and the only solution to this recurrence with $q_0 = 1$ and $q_n \to 0$ is $q_n = (q/p)^n$ [see Feller (1971)]. □

We consider the random variables $\boldsymbol{T}$ and $\boldsymbol{S}_n$, respectively $\boldsymbol{T}'$ and $\boldsymbol{S}'_n$, associated to the group of honest, respectively attacker, miners. And also we consider the random Poisson process $\boldsymbol{N}(t)$, respectively $\boldsymbol{N}'(t)$. The random variables $\boldsymbol{T}$ and $\boldsymbol{T}'$ are clearly independent and have exponential distributions with parameters α and α'. We have

$$\mathbb{P}[\boldsymbol{T}' < \boldsymbol{T}] = \frac{\alpha'}{\alpha + \alpha'},$$

so

$$p = \frac{\alpha}{\alpha + \alpha'}, \quad q = \frac{\alpha'}{\alpha + \alpha'}.$$

Moreover, $\inf(\boldsymbol{T}, \boldsymbol{T}')$ is an exponentially distributed random variable with parameters $\alpha + \alpha'$ which represents the mining speed of the entire network, honest and attacker miners together. The Bitcoin protocol is calibrated such that $\alpha + \alpha' = \tau_0$ with $\tau_0 = 10\,\text{min}$. So we have

$$\mathbb{E}[\boldsymbol{T}] = \frac{1}{\alpha} = \frac{\tau_0}{p}, \quad \mathbb{E}[\boldsymbol{T}'] = \frac{1}{\alpha'} = \frac{\tau_0}{q}.$$

These results can also be obtained in the following alternative way. The hash function used in Bitcoin block validation is $h(x) = \text{SHA256}(\text{SHA256}(x))$. The hashrate is the number of hashes per second performed by the miners. At a stable hashrate regime, the average time it takes to validate a block by the network is $\tau_0 = 10\,\text{min}$. If the difficulty is set to be $d \in (0, 2^{256} - 1]$, a block is validated when a mining node finds a small hash $h(\text{BH}) < d$, where BH is the block header. The

[b]The difficulty is adjusted every 2016 blocks.

pseudo-random output of SHA-256 shows that the whole network needs to compute an average number of $m = 2^{256}/d$ hashes to find a solution. Let h, respectively h', be the hashrates of the group of honest miners, respectively the attackers. The total hashrate of the network is $h + h'$, and we have

$$p = \frac{h}{h+h'}, \quad q = \frac{h'}{h+h'}.$$

Let t_0, respectively t_0', be the average time it takes to validate a block by the honest miners, respectively the attackers. We have

$$\begin{aligned}(h+h')\tau_0 &= m,\\ ht_0 &= m,\\ h't_0' &= m,\end{aligned}$$

and from this we get that τ_0 is half the harmonic mean of t_0 and t_0',

$$\tau_0 = \frac{t_0 t_0'}{t_0 + t_0'},$$

and also

$$\begin{aligned}p &= \frac{t_0'}{t_0+t_0'} = \frac{\tau_0}{t_0},\\ q &= \frac{t_0}{t_0+t_0'} = \frac{\tau_0}{t_0'}.\end{aligned}$$

Going back to the Poisson distribution parameters, we have

$$\begin{aligned}\alpha &= \frac{1}{t_0} = \frac{p}{\tau_0},\\ \alpha' &= \frac{1}{t_0'} = \frac{q}{\tau_0},\end{aligned}$$

and we recover the relations

$$p = \frac{\alpha}{\alpha+\alpha'}, \quad q = \frac{\alpha'}{\alpha+\alpha'}.$$

4. Nakamoto's Analysis

We consider the situation when the honest miners have mined the zth block, $z \geq 1$, and the attackers have mined k blocks. If $k > z$, then the attackers release their secret chain that is adopted and the attack succeeds. Otherwise, when $k \leq z$, the probability that they overtake the public honest blockchain is $(q/p)^z$ as computed above, therefore the probability P of success of the attack is

$$P = \mathbb{P}[\boldsymbol{N}'(\boldsymbol{S}_z) \geq z] + \sum_{k=0}^{z-1} \mathbb{P}[\boldsymbol{N}'(\boldsymbol{S}_z) = k] \cdot q_{z-k}.$$

Then Nakamoto makes the simplifying assumption that the blocks have been mined according to average expected time per block. This is asymptotically true when $z \to +\infty$ but false otherwise. More precisely, he approximates $\boldsymbol{N}'(\boldsymbol{S}_z)$ by the Poisson variable $\boldsymbol{N}'(t_z)$ where

$$t_z = \mathbb{E}[\boldsymbol{S}_z] = z\mathbb{E}[\boldsymbol{T}] = \frac{z\tau_0}{p}.$$

As we have seen above, the random variable $\boldsymbol{N}'(t_z)$ follows a Poisson distribution with parameter

$$\lambda = \alpha' t_z = \frac{z\alpha'\tau_0}{p} = \frac{zq}{p}.$$

The final calculus in Nakamoto (2008) is then

$$\begin{aligned} P_{SN}(z) &= \mathbb{P}[\boldsymbol{N}'(t_z) \geq z] + \sum_{k=0}^{z-1} \mathbb{P}[\boldsymbol{N}'(t_z) = k] \cdot q_{z-k} \\ &= 1 - \sum_{k=0}^{z-1} \mathbb{P}[\boldsymbol{N}'(t_z) = k] + \sum_{k=0}^{z-1} \mathbb{P}[\boldsymbol{N}'(t_z) = k] \cdot q_{z-k} \\ &= 1 - \sum_{k=0}^{z-1} e^{-\lambda} \frac{\lambda^k}{k!}(1 - q_{z-k}). \end{aligned}$$

However, this analysis is not correct since $\boldsymbol{N}'(\boldsymbol{S}_z) \neq \boldsymbol{N}'(t_z)$.

5. The Correct Analysis

Let $\boldsymbol{X}_n = \boldsymbol{N}'(\boldsymbol{S}_n)$ be the number of blocks mined by the attackers when the honest miners have just mined the nth block. We prove that the distribution for $\boldsymbol{X}_n$ is a negative binomial distribution.

Theorem 5.1. *The random variable $\boldsymbol{X}_n$ has a negative binomial distribution with parameters (n, p), i.e. for $k \geq 0$,*

$$\mathbb{P}[\boldsymbol{X}_n = k] = p^n q^k \binom{k+n-1}{k}.$$

Proof. Let $k \geq 0$. We have that $\boldsymbol{N}'$ and $\boldsymbol{S}_n$ are independent, therefore

$$\begin{aligned} \mathbb{P}[\boldsymbol{X}_n = k] &= \int_0^{+\infty} \mathbb{P}[\boldsymbol{N}'(\boldsymbol{S}_n) = k \mid \boldsymbol{S}_n \in [t, t+dt]] \cdot \mathbb{P}[\boldsymbol{S}_n \in [t, t+dt]] \\ &= \int_0^{+\infty} \mathbb{P}[\boldsymbol{N}'(t) = k] \cdot f_{\boldsymbol{S}_n}(t) dt \\ &= \int_0^{+\infty} \frac{(\alpha' t)^k}{k!} e^{-\alpha' t} \cdot \frac{\alpha^n}{(n-1)!} t^{n-1} e^{-\alpha t} dt \end{aligned}$$

$$= \frac{p^n q^k}{(n-1)!k!} \cdot \int_0^{+\infty} t^{k+n-1} e^{-t} dt$$

$$= \frac{p^n q^k}{(n-1)!k!} \cdot (k+n-1)!.$$

□

Thus, contradicting to Nakamoto's claim, we have proved that the distribution of $\boldsymbol{X}_n$ is not a Poisson law with parameter nq/p. Rosenfeld (2014) noticed the inaccuracy of Nakamoto's approximation and proposed empirically the negative binomial distribution as a better approximation, not realizing that this was the exact distribution.[c] Only asymptotically we have convergence to the Poisson distribution.

Proposition 5.1. *In the limit $n \to +\infty$, $q \to 0$, and $l_n = nq/p \to \lambda$ we have*

$$\mathbb{P}[X_n = k] \to \frac{\lambda^k}{k!} e^{-\lambda}.$$

Proof. We use $(1 + \frac{l_n}{n})^n \to e^{\lambda}$ in

$$\mathbb{P}[X_n = k] = \frac{n^n}{(n+l_n)^n} \frac{l_n^k}{(n+l_n)^k} \frac{(k+n-1)!}{(n-1)!k!}$$

$$= \frac{l_n^k}{k!} \frac{1}{\left(1 + \dfrac{l_n}{n}\right)^n} \frac{n(n+1)\cdots(n+k-1)}{(n+l_n)^k}.$$

□

We can now compute and prove the exact probability of success of the attackers.

Theorem 5.2 (Probability of Success of the Attackers). *The probability of success of the attackers after $z \geq 1$ blocks mined by the honest miners is*

$$P(z) = 1 - \sum_{k=0}^{z-1} (p^z q^k - q^z p^k) \binom{k+z-1}{k}.$$

Proof. As explained before, we have

$$P(z) = \sum_{k>z} p^z q^k \binom{k+z-1}{k} + \sum_{k=0}^{z} \left(\frac{q}{p}\right)^{z-k} p^z q^k \binom{k+z-1}{k}$$

$$= 1 - \sum_{k=0}^{z} (p^z q^k - q^z p^k) \binom{k+z-1}{k}$$

$$= 1 - \sum_{k=0}^{z-1} (p^z q^k - q^z p^k) \binom{k+z-1}{k}.$$

□

[c]In Rosenfeld (2014), it is stated: "We will not use this assumption (Nakamoto's one), but rather model m more accurately as a negative binomial variable", and in Rosenfeld (2012) it is mentioned: "Instead of a Poisson distribution, I used a more accurate negative binomial distribution."

5.1. *Numerical application*

Converting to R code, given $0 < q < 1/2$ and $z \geq 0$, this simple function computes our probability $P(z)$:

```
prob<-function(z,q){
p=1-q;
sum=1;
for (k in 0:(z-1)){sum=sum-(p^z*q^k-q^z*p^k)*choose(k+z-1,k)};
return(sum)
}
```

We can compare with the probability P_{SN} computed in Nakamoto (2008) (see Fig. 2). Notice that the attacker starts the double spend only after having secretly mined a block containing the return transaction. This is assumed implicitly in Nakamoto (2008) and is the reason that the probability of success is 1 if the recipient accepts 0 confirmations.

Therefore, the correct results for Bitcoin security are worse than those given in Nakamoto (2008) (see Tables 1, 2 and 3). The explanation is that Nakamoto's result

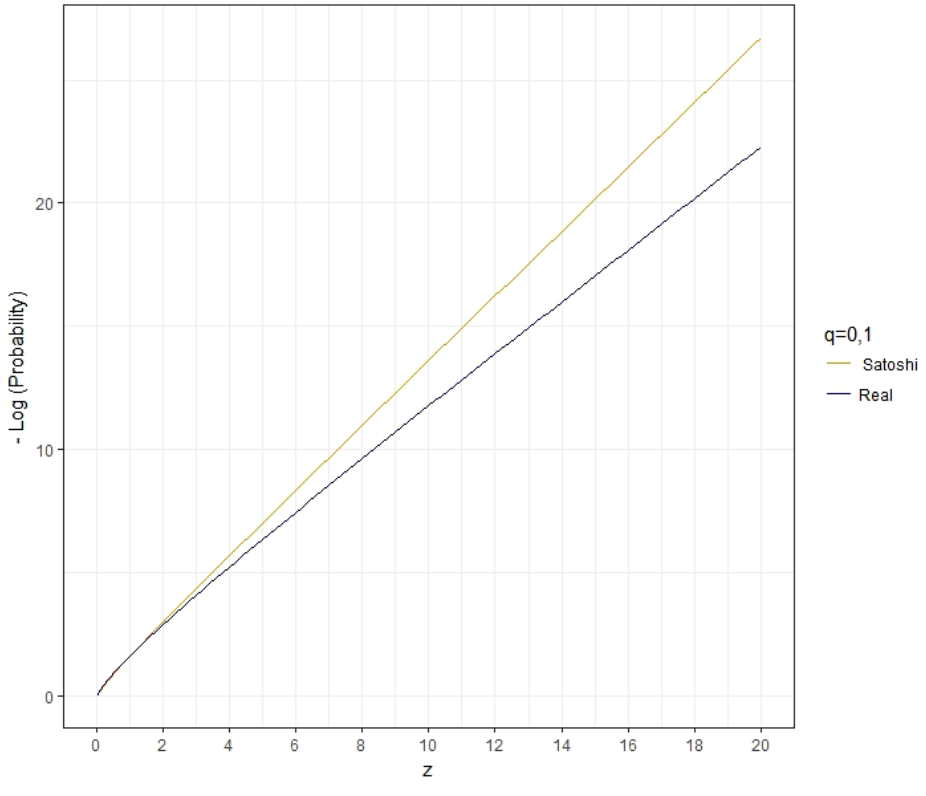

Fig. 2. Nakamoto's and real probabilities.

Table 2. Probabilities for $q = 0.1$.

z	$P(z)$	$P_{SN}(z)$
0	1.0000000	1.0000000
1	0.2000000	0.2045873
2	0.0560000	0.0509779
3	0.0171200	0.0131722
4	0.0054560	0.0034552
5	0.0017818	0.0009137
6	0.0005914	0.0002428
7	0.0001986	0.0000647
8	0.0000673	0.0000173
9	0.0000229	0.0000046
10	0.0000079	0.0000012

Table 3. Probabilities for $q = 0.3$.

z	$P(z)$	$P_{SN}(z)$
0	1.0000000	1.0000000
5	0.1976173	0.1773523
10	0.0651067	0.0416605
15	0.0233077	0.0101008
20	0.0086739	0.0024804
25	0.0033027	0.0006132
30	0.0012769	0.0001522
35	0.0004991	0.0000379
40	0.0001967	0.0000095
45	0.0000780	0.0000024
50	0.0000311	0.0000006

is correct only if the mining time by the honest miners is exactly the expected time. Times longer than average help the attackers.

6. Closed-Form Formula

We give a closed-form formula for $P(z)$ using the regularized incomplete beta function $I_x(a, b)$ [see (6.6.2) in Abramovitch & Stegun (1970)].

Theorem 6.1. *We have, with* $s = 4pq$,

$$P(z) = I_s\left(z, \frac{1}{2}\right).$$

We recall that the incomplete beta function is defined [see (6.6.1) in Abramovitch & Stegun (1970)], for $a, b > 0$ and $0 \leq x \leq 1$, by

$$B_x(a, b) = \int_0^x t^{a-1}(1-t)^{b-1}dt,$$

and the classical beta function is defined [see (6.2.1) in Abramovitch & Stegun (1970)] by $B(a,b) = B_1(a,b)$. The regularized incomplete beta function is defined [see (6.6.2) and (26.5.1) in Abramovitch & Stegun (1970)] by

$$I_x(a,b) = \frac{B_x(a,b)}{B(a,b)} = \frac{\Gamma(a+b)}{\Gamma(a)\Gamma(b)} B_x(a,b).$$

Proof. The cumulative distribution of a random variable $\boldsymbol{X}$ with negative binomial distribution, with $0 < p < 1$ and $q = 1 - p$ as usual [see (26.5.26) in Abramovitch & Stegun (1970)], is given by

$$F_{\boldsymbol{X}}(k) = \mathbb{P}[\boldsymbol{X} \leq k] = \sum_{l=0}^{k} p^z q^l \binom{l+z-1}{l} = 1 - I_p(k+1, z).$$

This results from the formula [see (6.6.1) in Abramovitch & Stegun (1970)]

$$I_p(k+1,z) = I_p(k,z) - \frac{p^k q^z}{kB(k,z)},$$

that we prove by integrating by parts the definition of $B_x(a,b)$. Thus we get

$$P(z) = 1 - I_p(z,z) + I_q(z,z).$$

Making the change of variables $t \mapsto 1 - t$ in the integral definition, we also have a symmetry relation [see (6.6.3) in Abramovitch & Stegun (1970)]

$$I_p(a,b) + I_q(b,a) = 1.$$

Therefore, we have $I_p(z,z) + I_q(z,z) = 1$, and $P(z) = 2I_q(z,z)$. The result follows using [see (26.5.14) in Abramovitch & Stegun (1970)] $I_q(z,z) = \frac{1}{2} I_s(z, 1/2)$, where $s = 4pq$. □

7. Asymptotic and Exponential Decay

Nakamoto makes the observation [see Nakamoto (2008, p. 8)], without proof, that the probability decreases exponentially to 0 when $z \to +\infty$. We prove this fact for the true probability $P(z)$ using the closed-form formula from Proposition 6.1.

Proposition 7.1. *When $z \to +\infty$ we have, with $s = 4pq < 1$,*

$$P(z) \sim \frac{s^z}{\sqrt{\pi(1-s)z}}.$$

We can obtain this result (and higher-order asymptotics) by using the known asymptotic expansions for the incomplete beta function. We prefer to give a direct

and self-contained proof. By integration by parts we get the following elementary version of Watson's lemma.

Lemma 7.1. *Let $f \in C^1(\mathbb{R}_+)$ with $f(0) \neq 0$ and absolutely convergent integral*

$$\int_0^{+\infty} f(u)e^{-zu}du < +\infty,$$

then, when $z \to +\infty$, we have

$$\int_0^{+\infty} f(u)e^{-zu}du \sim \frac{f(0)}{z}.$$

Then we get the following asymptotics [see also López & Sesma (1999)].

Lemma 7.2. *For $s, b \in \mathbb{R}$, we have, when $z \to +\infty$,*

$$B_s(z,b) \sim \frac{s^z}{z}(1-s)^{b-1}.$$

Proof. Making the change of variable $u = \log(s/t)$ in the definition

$$B_s(z,b) = \int_0^s t^{z-1}(1-t)^{b-1}dt,$$

we have

$$B_s(z,b) = s^z \int_0^{+\infty} (1-se^{-u})^{b-1}e^{-zu}du,$$

and the result follows applying Lemma 7.1 with $f(u) = (1-se^{-u})^{b-1}$. □

Now we end the proof of Proposition 7.1 using Stirling asymptotic,

$$B\left(z, \frac{1}{2}\right) = \frac{\Gamma(z)\Gamma\left(\frac{1}{2}\right)}{\Gamma\left(z+\frac{1}{2}\right)} \sim \sqrt{\frac{\pi}{z}},$$

so we have

$$I_s\left(z, \frac{1}{2}\right) = \frac{B_s\left(z, \frac{1}{2}\right)}{B\left(z, \frac{1}{2}\right)} \sim \frac{(1-s)^{-1/2}\frac{s^z}{z}}{\sqrt{\frac{\pi}{z}}} \sim \frac{s^z}{\sqrt{\pi(1-s)z}}.$$

8. A Finer Risk Analysis

In practice, in order to avoid a double spend attack, the recipient of the Bitcoin transaction waits for $z \geq 1$ confirmations. But he also has the information on the time τ_1 it took to confirm the transaction z times. Obviously, the probability of

success of the attackers increases with τ_1. The relevant parameter is the relative deviation from the expected time:

$$\kappa = \frac{\tau_1}{zt_0} = \frac{p\tau_1}{z\tau_0}.$$

Our next goal is the exact computation of the probability $P(z, \kappa)$ of success of the attackers. Note that $P(z, 1)$ is the probability computed by Nakamoto (2008),

$$P_{SN}(z) = P(z, 1).$$

8.1. *Computation of $P(z, \kappa)$*

The number $k \geq 0$ of blocks mined by the attackers during the time τ_1 follows a Poisson distribution with parameter

$$\lambda(z, \kappa) = \alpha' \tau_1 = \kappa \frac{zq}{p},$$

that means

$$\mathbb{P}[\boldsymbol{N}'(\tau_1) = k] = \frac{\left(\frac{zq}{p}\kappa\right)^k}{k!} e^{-\frac{zq}{p}\kappa}.$$

For $\kappa = 1$ we recover Nakamoto's approximation.

The cumulative Poisson distribution can be computed with the incomplete regularized gamma function [see (26.4) in Abramovitch & Stegun (1970)]:

$$Q(s, x) = \frac{\Gamma(s, x)}{\Gamma(x)},$$

where

$$\Gamma(s, x) = \int_x^{+\infty} t^{s-1} e^{-t} dt$$

is the incomplete gamma function and $\Gamma(s) = \Gamma(s, 0)$ is the regular gamma function. We have

$$Q(z, \lambda) = \sum_{k=0}^{z-1} \frac{\lambda^k}{k!} e^{-\lambda}.$$

We compute as before

$$\begin{aligned} P(z, \kappa) &= \sum_{k=z}^{+\infty} \frac{(\lambda(z, \kappa))^k}{k!} e^{-\lambda(z,\kappa)} + \sum_{k=0}^{z-1} \left(\frac{q}{p}\right)^{z-k} \frac{(\lambda(z, \kappa))^k}{k!} e^{-\lambda(z,\kappa)} \\ &= 1 - \sum_{k=0}^{z-1} \left(1 - \left(\frac{q}{p}\right)^{z-k}\right) \frac{(\lambda(z, \kappa))^k}{k!} e^{-\lambda(z,\kappa)} \\ &= 1 - Q\left(z, \frac{\kappa z q}{p}\right) + \left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{p}} Q(z, \kappa z). \end{aligned}$$

Thus we get an explicit closed-form formula for $P(z, \kappa)$ from which we get Fig. 1.

Theorem 8.1. *We have*

$$P(z,\kappa) = 1 - Q\left(z, \frac{\kappa z q}{p}\right) + \left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{p}} Q(z, \kappa z)$$

and

$$P_{SN}(z) = P(z,1) = 1 - Q\left(z, \frac{zq}{p}\right) + \left(\frac{q}{p}\right)^z e^{z\frac{p-q}{p}} Q(z,z).$$

9. Asymptotics of $P(z,\kappa)$ and $P_{SN}(z)$

We find the asymptotics of $Q(z,\lambda z)$ when $z \to +\infty$ for different values of $\lambda > 0$. We can also obtain by the same method higher-order asymptotics.

Lemma 9.1. *We have the following*:

(1) *For* $0 < \lambda < 1$, $Q(z,\lambda z) \to 1$ *and* $1 - Q(z,\lambda z) \sim \frac{1}{1-\lambda}\frac{1}{\sqrt{2\pi z}} e^{-z(\lambda - 1 - \log\lambda)}$.
(2) *For* $\lambda = 1$, $Q(z,z) \to 1/2$ *and* $1/2 - Q(z,z) \sim \frac{1}{3\sqrt{2\pi z}}$.
(3) *For* $\lambda > 1$, $Q(z,\lambda z) \sim \frac{1}{\lambda - 1}\frac{1}{\sqrt{2\pi z}} e^{-z(\lambda - 1 - \log\lambda)}$.

Proof. (1) By (8.11.6) in Olver *et al.* (2018) and Stirling formula, for $\lambda < 1$, we have

$$1 - Q(z,\lambda z) = \frac{\gamma(z,\lambda z)}{\Gamma(z)} \sim \frac{z^z \lambda^z e^{-z\lambda}}{z!(1-\lambda)} \sim \frac{1}{1-\lambda}\frac{1}{\sqrt{2\pi z}} e^{-z(\lambda - 1 - \log\lambda)}.$$

(2) Also by (8.11.12) in Olver *et al.* (2018) and Stirling formula, we have

$$Q(z,z) = \frac{z^{z-1}e^{-z}\sqrt{\frac{\pi z}{2}}}{(z-1)!} \sim \frac{1}{2}\frac{\left(\frac{z}{e}\right)^z \sqrt{2\pi z}}{z!} \to \frac{1}{2}$$

and

$$\begin{aligned}
\frac{1}{2} - Q(z,z) &= \frac{1}{2} - \frac{z^{z-1}e^{-z}\sqrt{\frac{\pi z}{2}}\left(1 - \frac{1}{3}\sqrt{\frac{2}{\pi z}} + o(z^{-1/2})\right)}{(z-1)!} \\
&= \frac{1}{2} - \frac{1}{2}\frac{\sqrt{2\pi z}\left(\frac{z}{e}\right)^z}{z!}\left(1 - \frac{1}{3}\sqrt{\frac{2}{\pi z}} + o(z^{-1/2})\right) \\
&= \frac{1}{2} - \frac{1}{2}\frac{\sqrt{2\pi z}\left(\frac{z}{e}\right)^z}{\sqrt{2\pi z}\left(\frac{z}{e}\right)^z\left(1 + \frac{1}{12z} + o(z^{-1})\right)}\left(1 - \frac{1}{3}\sqrt{\frac{2}{\pi z}} + o(z^{-1/2})\right) \\
&= \frac{1}{2} - \frac{1}{2}\left(1 + \frac{1}{12z} + o(z^{-1})\right)\cdot\left(1 - \frac{1}{3}\sqrt{\frac{2}{\pi z}} + o(z^{-1/2})\right) \\
&= \frac{1}{3\sqrt{2\pi z}} + o(z^{-1/2}).
\end{aligned}$$

(3) By (8.11.7) in Olver *et al.* (2018) and Stirling formula, for $\lambda > 1$, we have

$$\begin{aligned} Q(z, \lambda z) &= \frac{\Gamma(z, \lambda z)}{\Gamma(z)} \\ &\sim \frac{(\lambda z)^z e^{-z\lambda}}{z!(\lambda - 1)} \\ &\sim \frac{1}{\lambda - 1} \frac{1}{\sqrt{2\pi z}} e^{-z(\lambda - 1 - \log \lambda)}. \end{aligned}$$

□

For $x > 0$ we define $c(x) = x - 1 - \log x$, which is positive since the graph of $x \mapsto 1 - x$ is the tangent at $x = 1$ to the concave graph of the logarithm function. We denote $0 < \lambda = q/p < 1$.

We have that the Nakamoto probability $P_{SN}(z)$ also decreases exponentially with z as claimed in Nakamoto (2008) without proof.

Proposition 9.1. *We have for* $z \to +\infty$,

$$P_{SN}(z) \sim \frac{e^{-zc(\lambda)}}{2}.$$

Proof. The result follows from the closed-form formula from Theorem 8.1,

$$P(z, \kappa) = 1 - Q\left(z, \frac{\kappa z q}{p}\right) + \left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{q}} Q(z, \kappa z),$$

and then from points (1) and (2) of Lemma 9.1,

$$1 - Q\left(z, \frac{q}{p} z\right) = o(e^{-zc(q/p)})$$

and

$$\left(\frac{q}{p}\right)^z e^{z(1-\frac{q}{p})} Q(z, z) \sim \frac{1}{2} e^{-zc(q/p)}.$$

□

More generally, we have five different regimes for the asymptotics of $P(z, \kappa)$ for $0 < \kappa < 1$, $\kappa = 1$, $1 < \kappa < p/q$, $\kappa = p/q$ and $\kappa > p/q$.

Proposition 9.2. *We have the following for* $z \to +\infty$:

(1) *For* $0 < \kappa < 1$,

$$P(z, \kappa) \sim \frac{1}{1 - \kappa\lambda} \frac{1}{\sqrt{2\pi z}} e^{-zc(\kappa\lambda)}.$$

(2) *For* $\kappa = 1$,

$$P(z, 1) = P_{SN}(z) \sim \frac{1}{2} e^{-zc(\lambda)}.$$

(3) *For* $1 < \kappa < p/q$,

$$P(z, \kappa) \sim \frac{\kappa(1 - \lambda)}{(\kappa - 1)(1 - \kappa\lambda)} \frac{1}{\sqrt{2\pi z}} e^{-zc(\kappa\lambda)}.$$

(4) *For* $\kappa = p/q$, $P(z, p/q) \to 1/2$ *and*

$$P\left(z, \frac{p}{q}\right) - \frac{1}{2} \sim \frac{1}{2\pi z}\left(\frac{1}{3} + \frac{q}{p-q}\right).$$

(5) *For* $p/q < \kappa$, $P(z,\kappa) \to 1$ *and*

$$1 - P(z,\kappa) \sim \frac{\kappa(1-\lambda)}{(\kappa-1)(\kappa\lambda-1)} \frac{1}{\sqrt{2\pi z}} e^{-zc(\kappa\lambda)}.$$

Proof. (1) If $\kappa < 1$ then also $\kappa q/p < 1$, and

$$1 - Q\left(z, \frac{\kappa z q}{p}\right) \sim \frac{1}{1 - \dfrac{\kappa q}{p}} \frac{1}{\sqrt{2\pi z}} e^{-z(\kappa q/p - 1 - \log(\kappa q/p))}$$

and

$$\begin{aligned}\left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{q}} &= e^{-z(\kappa q/p - 1 - \log(\kappa q/p))} \\ &= e^{-z(1-\kappa)(1-q/p)} \cdot e^{-z(q/p - 1 - \log(q/p))},\end{aligned}$$

and then

$$\begin{aligned}\frac{\left(\dfrac{q}{p}\right)^z e^{\kappa z \frac{p-q}{q}}}{1 - Q\left(z, \dfrac{\kappa z q}{p}\right)} &\sim \left(1 - \frac{\kappa q}{p}\right) \cdot \sqrt{2\pi z} \cdot e^{-z(1-\kappa)(1-q/p)} \\ &\quad \cdot e^{-z(q/p - 1 - \log(q/p) - (\kappa q/p - 1 - \log(\kappa q/p)))} \\ &\sim \left(1 - \frac{\kappa q}{p}\right) \cdot \sqrt{2\pi z} \cdot e^{-z(1-\kappa)(1-q/p)} \cdot e^{-z(1-\kappa)q/p} \cdot e^{-z\log\kappa} \\ &\sim \left(1 - \frac{\kappa q}{p}\right) \cdot \sqrt{2\pi z} \cdot e^{-z(1-\kappa-\log\kappa)} = o(1).\end{aligned}$$

Since $Q(z, \kappa z) \to 1$ we have

$$\begin{aligned}P(z,\kappa) &= 1 - Q\left(z, \frac{\kappa z q}{p}\right) + \left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{q}} Q(z, \kappa z) \\ &\sim 1 - Q\left(z, \frac{\kappa z q}{p}\right) \\ &\sim \frac{1}{\left(1 - \dfrac{\kappa q}{p}\right)\sqrt{2\pi z}} \cdot e^{-z(\kappa q/p - 1 - \log(\kappa q/p))}.\end{aligned}$$

(2) This was proved in Proposition 9.1.

(3) When $1 < \kappa < p/q$ then by Lemma 9.1,

$$\left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{q}} Q(z, \kappa z) \sim \frac{1}{(\kappa-1)\sqrt{2\pi z}} \cdot e^{-z(\kappa q/p - 1 - \log(\kappa q/p))}$$

and

$$1 - Q\left(z, \frac{\kappa z q}{p}\right) \sim \frac{1}{\left(1 - \frac{\kappa q}{p}\right)\sqrt{2\pi z}} \cdot e^{-z(\kappa q/p - 1 - \log(\kappa q/p))}.$$

So we have

$$\begin{aligned} P(z,\kappa) &\sim \left(\frac{1}{1-\frac{\kappa q}{p}} + \frac{1}{\kappa - 1}\right) \cdot \frac{1}{\sqrt{2\pi z}} \cdot e^{-z(\kappa q/p - 1 - \log(\kappa q/p))} \\ &\sim \frac{\kappa\left(1 - \frac{q}{p}\right)}{(\kappa-1)\left(1 - \frac{\kappa q}{p}\right)} \frac{1}{\sqrt{2\pi z}} \cdot e^{-z(\kappa q/p - 1 - \log(\kappa q/p))}. \end{aligned}$$

(4) The previous asymptotic at the start of the proof of (3) is also valid for $1 < \kappa = p/q$ and gives

$$\left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{q}} Q(z, \kappa z) \sim \frac{q}{p-q} \frac{1}{\sqrt{2\pi z}},$$

and by Lemma 9.1,

$$\begin{aligned} P\left(z, \frac{p}{q}\right) &= 1 - Q(z,z) + \left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{q}} Q(z, \kappa z) \\ &= \frac{1}{2} + \frac{1}{\sqrt{2\pi z}}\left(\frac{1}{3} + \frac{q}{p-q}\right) + o\left(\frac{1}{\sqrt{z}}\right). \end{aligned}$$

(5) For $\kappa > p/q$ we use again the same asymptotic of (3) to get

$$Q\left(z, \frac{\kappa z q}{p}\right) \sim \frac{1}{\frac{\kappa q}{p} - 1} \frac{1}{\sqrt{2\pi z}} e^{-z(\kappa q/p - 1 - \log(\kappa q/p))},$$

and again

$$\left(\frac{q}{p}\right)^z e^{\kappa z \frac{p-q}{q}} Q(z, \kappa z) \sim \frac{1}{(\kappa-1)\sqrt{2\pi z}} e^{-z(\kappa q/p - 1 - \log(\kappa q/p))},$$

so

$$1-P(z,\kappa)\sim\left(\frac{1}{\frac{\kappa q}{p}-1}-\frac{1}{\kappa-1}\right)\sqrt{2\pi z}e^{-z(\kappa q/p-1-\log(\kappa q/p))}$$

$$\sim\frac{\kappa\left(1-\frac{q}{p}\right)}{\left(\frac{\kappa q}{p}-1\right)(\kappa-1)}\sqrt{2\pi z}e^{-z(\kappa q/p-1-\log(\kappa q/p))}.$$ □

10. Comparing Asymptotics of $P(z)$ and $P_{SN}(z)$

We have an asymptotic comparison.

Proposition 10.1. *We have for $z\to+\infty$,*

$$P_{SN}(z)\prec P(z).$$

Proof. Note that

$$\frac{q}{p}-1-\log\left(\frac{q}{p}\right)-\log\left(\frac{1}{4pq}\right)=2\left[\frac{1}{2p}-1-\log\left(\frac{1}{2p}\right)\right]>0.$$

So with $s=4pq<1$ we have

$$0<\log\frac{1}{s}<\frac{q}{p}-1-\log\frac{q}{p}=c\left(\frac{q}{p}\right)=c(\lambda),$$

and for large z,

$$P_{SN}(z)<e^{-zc(\lambda)}\prec\frac{s^z}{\sqrt{\pi(1-s)z}}\sim P(z).$$ □

As we will see later we can be more explicit about the inequality between $P_{SN}(z)$ and $P(z)$.

11. Recovering $P(z)$ from $P(z,\kappa)$

We have seen above that $P_{SN}(z)$ can be recovered from $P(z,\kappa)$ by taking the value of $\kappa=1$. It turns out that we can also recover $P(z)$ as a weighted average on κ of $P(z,\kappa)$.

Theorem 11.1. *We have*

$$P(z)=\int_0^{+\infty}P(z,\kappa)d\rho_z(\kappa),$$

with the density function

$$d\rho_z(\kappa)=\frac{z^z}{(z-1)!}\kappa^{z-1}e^{-z\kappa}d\kappa.$$

We check that

$$\int_0^{+\infty} d\rho_z(\kappa) = 1.$$

We can write

$$P(z) = 1 - \sum_{k=0}^{z-1} f_k(\kappa),$$

where

$$f_k(\kappa) = \left(1 - \left(\frac{q}{p}\right)^{z-k}\right) \frac{\left(\frac{zq}{p}\right)^k}{k!} \kappa^k e^{\frac{zq}{p}\kappa}.$$

Then the theorem follows from a direct computation.

Lemma 11.1. *For $k \geq 0$, we have*

$$\int_0^{+\infty} f_k(\kappa) d\rho_z(\kappa) = (p^z q^k - q^z p^k) \binom{k+z-1}{k}.$$

We give a second more conceptual proof.

Proof. Consider the random variable

$$\boldsymbol{\kappa} = \frac{p}{z\tau_0} \boldsymbol{S}_z.$$

We have seen above that $\boldsymbol{S}_z \sim \Gamma(z, \alpha)$ so $\boldsymbol{\kappa} \sim \Gamma(z, \alpha\frac{z\tau_0}{p}) = \Gamma(z, z)$. So the density $d\rho_z$ is the distribution of $\boldsymbol{\kappa}$. It is enough to prove that

$$P(z) = \mathbb{E}[P(z, \boldsymbol{\kappa})].$$

We have

$$P(z) = \mathbb{P}[\boldsymbol{N}'(\boldsymbol{S}_z) \geq z] + \sum_{k=0}^{z-1} \mathbb{P}[\boldsymbol{N}'(\boldsymbol{S}_z) = k] \cdot q_{z-k}$$

$$= 1 - \sum_{k=0}^{z-1} (1 - q_{z-k}) \mathbb{P}[\boldsymbol{N}'(\boldsymbol{S}_z) = k].$$

And by conditioning with $\boldsymbol{S}_z$ we get

$$P(z) = 1 - \sum_{k=0}^{z-1} (1 - q_{z-k}) \mathbb{E}[\mathbb{P}[\boldsymbol{N}'(\boldsymbol{S}_z) = k \,|\, \boldsymbol{S}_z]]$$

$$= 1 - \mathbb{E}\left[\sum_{k=0}^{z-1} \frac{(\alpha' \boldsymbol{S}_z)^k}{k!} e^{-\alpha' \boldsymbol{S}_z}\right] + \left(\frac{q}{p}\right)^z \mathbb{E}\left[e^{\alpha' \frac{p-q}{q} \boldsymbol{S}_z} \sum_{k=0}^{z-1} \frac{\left(\frac{\alpha' p}{q} \boldsymbol{S}_z\right)^k}{k!} e^{-\frac{\alpha' p}{q} \boldsymbol{S}_z}\right]$$

$$= \mathbb{E}\left[1 - Q\left(z, \frac{zq}{p}\boldsymbol{\kappa}\right) + \left(\frac{q}{p}\right)^z e^{z(1-\frac{q}{p})\boldsymbol{\kappa}} Q(z, z\boldsymbol{\kappa})\right]$$
$$= \mathbb{E}[P(z, \boldsymbol{\kappa})],$$

since $\mathbb{P}[\boldsymbol{N}'(\boldsymbol{S}_z) = k \mid \boldsymbol{S}_z] = \frac{(\alpha' \boldsymbol{S}_z)^k}{k!} e^{\alpha' \boldsymbol{S}_z}$, $q_{z-k} = (q/p)^{z-k}$, and

$$Q(z, x) = \sum_{k=0}^{z-1} \frac{x^k}{k!} e^{-x}.$$

□

We also note that $\mathbb{E}[\boldsymbol{\kappa}] = 1$.

12. Range of $\boldsymbol{\kappa}$

The probability to observe a deviation greater than κ is $\mathbb{P}[\boldsymbol{\kappa} > \kappa]$ with $\boldsymbol{\kappa} = \frac{p}{z\tau_0}\boldsymbol{S}_z$. We have that $\boldsymbol{\kappa}$ follows a Γ-distribution, $\boldsymbol{\kappa} \sim \Gamma(z, z)$, so

$$\mathbb{P}[\boldsymbol{\kappa} > \kappa] = \frac{1}{\Gamma(z)} \int_\kappa^{+\infty} z^z t^{z-1} e^{-zt} dt$$
$$= \frac{1}{\Gamma(z)} \int_{\kappa z}^{+\infty} t^{z-1} e^{-t} dt = \frac{\Gamma(z, \kappa z)}{\Gamma(z)} = Q(z, \kappa z).$$

Then, by Lemma 9.1, $\mathbb{P}[\boldsymbol{\kappa} > \kappa] \sim \frac{1}{\kappa - 1} \frac{1}{\sqrt{2\pi z}} e^{-zc(\kappa)}$ for $\kappa > 1$. Note that this probability does not depend on p. For $z = 6$, we have $\mathbb{P}[\boldsymbol{\kappa} > 4] \approx 3 \cdot 10^{-6}$ and for $z = 10$, $\mathbb{P}[\boldsymbol{\kappa} > 4] \approx 4 \cdot 10^{-9}$. So, in practice, the probability to have $\boldsymbol{\kappa} > 4$ is very unlikely. In Fig. 3, we have represented the graph of $\kappa \mapsto P(z, \kappa)$ for different values of z ($q = 0.1$) and $0 < \kappa < 4$.

We see that $\kappa \mapsto P(z, \kappa)$ is convex in the range of values of κ considered. We study the convexity in more detail in the next section.

13. Comparing $P_{SN}(z)$ and $P(z)$

Now we study the convexity of $\kappa \mapsto P(z, \kappa)$. Recall that $\lambda = q/p < 1$. From Theorem 8.1 we have

$$P(z, \kappa) = 1 - Q(z, z\lambda\kappa) + \lambda^z e^{z(1-\lambda)\kappa} Q(z, z\kappa).$$

Since

$$\Gamma(z)\partial_2 Q(z, x) = -x^{z-1} e^{-x},$$

we get, after some cancellations,

$$\Gamma(z)\partial_2 P(z, \kappa) = \lambda^z z(1-\lambda) e^{z(1-\lambda)\kappa} \Gamma(z, z\kappa).$$

We observe that $\partial_2 P(z, \kappa) > 0$, so $P(z, \kappa)$ is an increasing function of κ as expected. For the second derivative we have

$$\Gamma(z)\partial_2^2 P(z, \kappa) = \lambda^z z^2 (1-\lambda) e^{z(1-\lambda)\kappa} [(1-\lambda)\Gamma(z, z\kappa) - (z\kappa)^{z-1} e^{-\kappa z}]$$
$$= \lambda^z z(1-\lambda) e^{-\lambda\kappa z} (z\kappa)^z [(1-\lambda) Q(z, z\kappa) z! e^{\kappa z} (z\kappa)^{-z} - \kappa^{-1}].$$

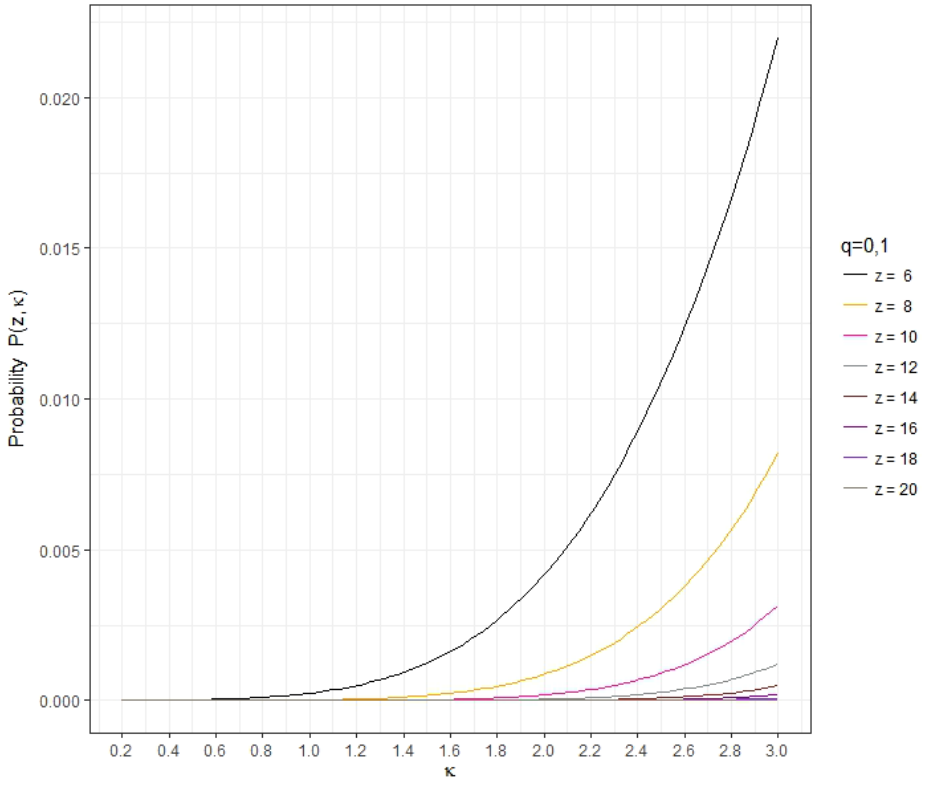

Fig. 3. Probability $P(z,\kappa)$ as a function of κ.

Therefore we study the sign of

$$\begin{aligned} g_{\lambda,z}(\kappa) &= (1-\lambda)Q(z,z\kappa)z!e^{\kappa z}(z\kappa)^{-z} - \kappa^{-1} \\ &= (1-\lambda)\sum_{k=0}^{z-1}\frac{z!}{z^{z-k}k!}\frac{1}{\kappa^{z-k}} - \kappa^{-1} \\ &= \frac{1-\lambda}{\kappa}\left(\left(1-\frac{1}{z}\right)\frac{1}{\kappa} + \left(1-\frac{1}{z}\right)\left(1-\frac{2}{z}\right)\frac{1}{\kappa^2} + \cdots\right) - \frac{\lambda}{\kappa}. \end{aligned}$$

For $z=1$ we have

$$g_{\lambda,1}(\kappa) = -\frac{\lambda}{\kappa} < 0,$$

therefore $\kappa \mapsto P(1,\kappa)$ is a concave function and by Jensen's inequality

$$P(1) = \int_0^{+\infty} P(z,\kappa)d\rho_1(\tau) \leq P(1,\bar{\kappa}) = P(1,1) = P_{SN}(1).$$

Corollary 13.1. *We have (for all* $0 < q < 1/2$*)*

$$P(1) \leq P_{SN}(1).$$

In general, for $z \geq 2$, we have the reverse inequality. To determine the sign of $g_{\lambda,z}$ we study its zeros. The equation to solve is

$$\left(1-\frac{1}{z}\right)\frac{1}{\kappa}+\left(1-\frac{1}{z}\right)\left(1-\frac{2}{z}\right)\frac{1}{\kappa^2}+\cdots+\left(1-\frac{1}{z}\right)\cdots\left(1-\frac{z-1}{z}\right)\frac{1}{\kappa^{z-1}} = \frac{\lambda}{1-\lambda}.$$

This is a polynomial equation in $1/\kappa$, the coefficients are increasing on z, and the left-hand side is decreasing on $\kappa \in (0,+\infty)$ from $+\infty$ to 0, therefore there is a unique solution $\kappa(z)$, and

$$\kappa(2) < \kappa(3) < \cdots.$$

We compute

$$\kappa(2) = \frac{1-\lambda}{2\lambda} = \frac{1}{2q} - 1 > 0.$$

In this case the function $\kappa \mapsto P(z,\kappa)$ is convex only in the interval $(0,\kappa(z))$. For large z, most of the support of the measure $d\rho_z$ is contained in this interval and we have by Jensen's inequality

$$P(z) \approx \int_0^{\kappa(z)} P(z,\kappa)d\rho_z(\kappa) \geq P(z,\bar{\kappa}_z) \approx P(z,1) = P_{SN}(z),$$

where

$$\bar{\kappa}_z = \int_0^{\kappa(z)} \kappa d\rho_z(\kappa) \approx \int_0^{+\infty} \kappa d\rho_z(\kappa) = 1.$$

We can get some estimates on $\kappa(z)$ for $z \to +\infty$. The first observation is that for large z we have $\kappa(z) > 1$. The asymptotic limits for $Q(z,\kappa z)$ for $\kappa < 1$ and $\kappa = 1$ (Lemma 9.1) and Stirling asymptotic formula give that

$$Q(z,\kappa z)z!e^{\kappa z}(z\kappa)^z \to +\infty,$$

and $g_{\lambda,z}(\kappa) \neq 0$.

For $\kappa > 1$, we can use the asymptotic (8.11.7) in Olver *et al.* (2018), $z \to +\infty$, to get

$$\Gamma(z,\kappa z) \sim \frac{(\kappa z)^z e^{-\kappa z}}{(\kappa-1)z}$$

and

$$(1-\lambda)\Gamma(z,\kappa z) - (\kappa z)^{z-1}e^{-\kappa z} \sim (\kappa z)^{z-1}e^{-\kappa z}\left((1-\lambda)\frac{\kappa}{\kappa-1} - 1\right),$$

thus, since

$$g_{\lambda,z}(\kappa) = (1-\lambda)\Gamma(z,\kappa z)ze^{\kappa z}(\kappa z)^{-z} - \kappa^{-1},$$

we have

$$g_{\lambda,\infty}(\kappa) = \lim_{z\to+\infty} g_{\lambda,z}(\kappa) = \frac{1}{\kappa}\left((1-\lambda)\frac{\kappa}{\kappa-1} - 1\right) = \frac{1-\lambda}{\kappa-1} - \frac{1}{\kappa}.$$

Now, if

$$\kappa(\infty) = \lim_{z\to+\infty} \kappa(z),$$

we have $g_{\lambda,\infty}(\kappa_\infty) = 0$, so we get the following proposition.

Proposition 13.1. *We have*

$$\kappa(\infty) = \lim_{z\to+\infty} \kappa(z) = \lambda^{-1} = \frac{p}{q}.$$

Using the second-order asymptotic [see (8.11.7) in Olver *et al.* (2018)], for $\kappa > 1$, $z \to +\infty$, we get

$$\Gamma(z, \kappa z) \sim \frac{(\kappa z)^z e^{-\kappa z}}{z(\kappa-1)}\left(1 - \frac{\kappa}{(\kappa-1)^2 z}\right),$$

so

$$g_{\lambda,z}(\kappa) \sim \frac{1-\lambda}{\kappa-1}\left(1 - \frac{\kappa}{(\kappa-1)^2 z}\right) - \kappa^{-1}.$$

Writing

$$\kappa(z) = \frac{p}{q} - \frac{a}{z} + o(z^{-1}),$$

and using

$$\frac{1-\lambda}{\kappa(z)-1}\left(1 - \frac{\kappa(z)}{(\kappa(z)-1)^2 z}\right) - \kappa(z)^{-1},$$

we get the following proposition.

Proposition 13.2. *For $z \to +\infty$*

$$\kappa(z) = \frac{p}{q} - \frac{p^2}{q(p-q)}\frac{1}{z} + o(z^{-1}).$$

Also we have

$$\frac{p}{q} - 1 > \frac{p^2}{q(p-q)}\frac{1}{z},$$

for

$$z > \left(\frac{p}{p-q}\right)^2,$$

so, for z of the order of $(1-\lambda)^{-2}$ we have $\kappa(z) > 1$.

14. Bounds for $P(z)$

Remember that we have set $s = 4pq$. We have the following inequality that is a particular case of more general Gautschi's (1959) inequalities.

Lemma 14.1. *Let $z \in \mathbb{R}_+$. We have*

$$\sqrt{\frac{z}{z+\frac{1}{2}}} \leq \frac{\Gamma\left(z+\frac{1}{2}\right)}{\sqrt{z}\Gamma(z)} \leq 1.$$

Proof. By Cauchy–Schwarz inequality, we have

$$\begin{aligned}
\Gamma\left(z+\frac{1}{2}\right) &= \int_0^{+\infty} t^{z-\frac{1}{2}} e^{-t} dt \\
&\leq \int_0^{+\infty} (t^{\frac{z}{2}} e^{-\frac{t}{2}}) \cdot (t^{\frac{z}{2}-\frac{1}{2}} e^{-\frac{t}{2}}) dt \\
&\leq \left(\int_0^{+\infty} t^z e^{-t} dt\right)^{\frac{1}{2}} \cdot \left(\int_0^{+\infty} t^{z-1} e^{-t} dt\right)^{\frac{1}{2}} \\
&\leq \Gamma(z+1)^{\frac{1}{2}} \cdot \Gamma(z)^{\frac{1}{2}} \leq (z\Gamma(z))^{\frac{1}{2}} \cdot \Gamma(z)^{\frac{1}{2}} \leq \sqrt{z}\Gamma(z).
\end{aligned}$$

On the other side, the last inequality with z replaced by $z+\frac{1}{2}$ gives

$$z\Gamma(z) = \Gamma\left(z+\frac{1}{2}+\frac{1}{2}\right) \leq \sqrt{z+\frac{1}{2}}\Gamma\left(z+\frac{1}{2}\right). \qquad \square$$

Lemma 14.2. *For $z > 1$, we have*

$$\sqrt{\frac{z}{z+\frac{1}{2}}} \cdot \frac{s^z}{\sqrt{\pi z}} \leq P(z) \leq \frac{1}{\sqrt{1-s}} \cdot \frac{s^z}{\sqrt{\pi z}}.$$

Proof. The function $x \mapsto (1-x)^{-\frac{1}{2}}$ is nondecreasing. So, by definition of I_s and the upper bound of the inequality of Lemma 14.1, we have

$$\begin{aligned}
P(z) = I_s\left(z, \frac{1}{2}\right) &= \frac{\Gamma\left(z+\frac{1}{2}\right)}{\Gamma\left(\frac{1}{2}\right)\Gamma(z)} \int_0^s t^{z-1}(1-t)^{-\frac{1}{2}} dt \\
&\leq \frac{1}{\sqrt{\pi}} \frac{\Gamma\left(z+\frac{1}{2}\right)}{\Gamma(z)} \int_0^s t^{z-1}(1-s)^{-\frac{1}{2}} dt \\
&\leq \frac{\Gamma\left(z+\frac{1}{2}\right)}{\sqrt{z}\Gamma(z)} \cdot \frac{s^z}{\sqrt{\pi(1-s)z}} \leq \frac{1}{\sqrt{1-s}} \cdot \frac{s^z}{\sqrt{\pi z}}.
\end{aligned}$$

In the same way, using the lower bound of the inequality of Lemma 14.1, we have

$$P(z) = I_s\left(z, \frac{1}{2}\right) \geq \frac{1}{\sqrt{\pi}} \frac{\Gamma\left(z+\frac{1}{2}\right)}{\Gamma(z)} \int_0^s t^{z-1} dt$$

$$\geq \frac{\Gamma\left(z+\frac{1}{2}\right)}{\sqrt{z}\Gamma(z)} \cdot \frac{s^z}{\sqrt{\pi z}} \geq \sqrt{\frac{z}{z+\frac{1}{2}}} \cdot \frac{s^z}{\sqrt{\pi z}}. \qquad \square$$

Note that this gives again the exponential decrease of Nakamoto's probability.

15. An Upper Bound for $P_{SN}(z)$

Proposition 15.1. *We have*

$$P_{SN}(z) < \frac{1}{1-\frac{q}{p}} \frac{1}{\sqrt{2\pi z}} e^{-(\frac{q}{p}-1-\log\frac{q}{p})z} + \frac{1}{2} e^{-(\frac{q}{p}-1-\log(\frac{q}{p})z)}.$$

This upper bound is quite sharp [see the asymptotics in Proposition 9.2(2)].

Lemma 15.1. *Let $z \in \mathbb{N}^*$ and $\lambda \in \mathbb{R}_+^*$:*

(1) *If $\lambda \in]0,1[$, then $1 - Q(z, \lambda z) < \frac{1}{1-\lambda} \frac{1}{\sqrt{2\pi z}} e^{-(\lambda-1-\log\lambda)z}$.*
(2) *$Q(z,z) < \frac{1}{2}$.*

Proof. For (1) We use (8.7.1) in Olver *et al.* (2018) to get

$$\gamma(a,x) = e^{-x} x^a \sum_{n=0}^{\infty} \frac{\Gamma(a)}{\Gamma(a+n+1)} x^n,$$

which is valid for $a, x \in \mathbb{R}$. Let $\lambda \in]0,1[$. Using $\Gamma(z+1) = z\Gamma(z)$, we get

$$\gamma(z,\lambda z) = e^{-\lambda z}(\lambda z)^z \sum_{n=0}^{+\infty} \frac{\Gamma(z)}{\Gamma(z+n+1)} (\lambda z)^n$$

$$= e^{-\lambda z}(\lambda z)^z \left(\frac{1}{z} + \frac{1}{z(z+1)}(\lambda z) + \frac{1}{z(z+1)(z+2)}(\lambda z)^2 + \cdots\right)$$

$$\leq e^{-\lambda z}(\lambda z)^z \left(\frac{1}{z} + \frac{1}{z^2}(\lambda z) + \frac{1}{z^3}(\lambda z)^2 + \cdots\right)$$

$$\leq e^{-\lambda z}(\lambda z)^z \frac{1}{z} \frac{1}{1-\lambda} \leq \frac{\lambda^z z^{z-1} e^{-\lambda z}}{1-\lambda}.$$

On the other hand, by (5.6.1) in Olver *et al.* (2018), we have

$$\frac{1}{\Gamma(z)} < \frac{e^z}{\sqrt{2\pi z} z^{z-1}},$$

and for any $0 < \lambda < 1$,

$$1 - Q(z, \lambda z) = \frac{\gamma(z, \lambda z)}{\Gamma(z)} < \frac{1}{1-\lambda} \frac{1}{\sqrt{2\pi z}} e^{-(\lambda - 1 - \log \lambda) z}.$$

For (2) this comes directly from (8.10.13) in Olver *et al.* (2018). □

Recalling that $P_{SN}(z) = P(z, 1) = 1 - Q(z, \frac{q}{p} z) + (q/p)^z e^{z(p-q)/p} Q(z, z)$, we get Proposition 15.1.

16. Comparing Again $P_{SN}(z)$ and $P(z)$

The aim of this section is to compute an explicit rank z_0 (not sharp) for which $P_{SN}(z) < P(z)$ for $z \geq z_0$ (see also Table 4).

Lemma 16.1. *Let $\alpha > 0$. For all $x > \log \alpha$, $e^x - \alpha x > \frac{\alpha}{2}(x - \log \alpha)^2 + \alpha(1 - \log \alpha)$.*

Proof. Let $g(x) = e^x - \alpha x - \frac{\alpha}{2}(x - \log \alpha)^2 - \alpha(1 - \log \alpha)$. We have $g'(x) = e^x - \alpha - \alpha(x - \log \alpha)$, $g''(x) = e^x - \alpha$ and $g^{(3)}(x) = e^x$. So, $g(\log \alpha) = g'(\log \alpha) = g''(\log \alpha) = 0$ and $g^{(3)} > 0$. Therefore, $g(x) > 0$ for $x > \log \alpha$. □

Lemma 16.2. *For $\alpha > 0$ and $x > (1 + 1/\sqrt{2}) \log \alpha$ we have $e^x > \alpha x$.*

Proof. The inequality is trivial when $x \leq 0$. So, we can assume that $x > 0$. For $0 < \alpha < 1$, we have $e^x > x > \alpha x$. For $1 < \alpha < e$, by Lemma 16.1, we have $e^x - \alpha x > 0$ for $x > \log \alpha$. For $\alpha > e$, the largest root of the polynomial $\frac{\alpha}{2}(x - \log \alpha)^2 + \alpha(1 - \log \alpha)$ is $\log \alpha + \sqrt{2(\log \alpha - 1)}$ which is smaller than $(1 + 1/\sqrt{2}) \log \alpha$ since $\sqrt{2(u-1)} \leq u/\sqrt{2}$ for $u \geq 1$. So, the inequality results from Lemma 16.1 again. □

Lemma 16.3. *For $\mu, \psi, x > 0$, if*

$$x > \frac{1}{2\sqrt{2}} - \frac{1 + \sqrt{2}}{2\sqrt{2}} \frac{\log(2\psi\mu^2)}{\psi},$$

then we have

$$e^{-\psi x} < \frac{\mu}{\sqrt{x + \frac{1}{2}}}.$$

Proof. We have

$$e^{-\psi \cdot x} < \frac{\mu}{\sqrt{x + \frac{1}{2}}} \Leftrightarrow \left(x + \frac{1}{2}\right) e^{-2\psi \cdot x} < \mu^2$$

$$\Leftrightarrow \left(x + \frac{1}{2}\right) e^{-2\psi \cdot \left(x + \frac{1}{2}\right)} < \mu^2 e^{-\psi}$$

$$\Leftrightarrow e^{2\psi\cdot(x+1/2)} > \frac{x+\frac{1}{2}}{\mu^2 e^{-\psi}}$$

$$\Leftrightarrow e^{2\psi\cdot(x+1/2)} > \frac{1}{2\psi\mu^2 e^{-\psi}}\, 2\psi\cdot\left(x+\frac{1}{2}\right).$$

By Lemma 16.2, the last inequality is satisfied as soon as

$$2\psi\cdot\left(x+\frac{1}{2}\right) > \left(1+\frac{1}{\sqrt{2}}\right)\log\left(\frac{1}{2\psi\mu^2 e^{-\psi}}\right).$$

Moreover, we have

$$\begin{aligned}
2\psi\cdot\left(x+\frac{1}{2}\right) &> \left(1+\frac{1}{\sqrt{2}}\right)\log\left(\frac{1}{2\psi\mu^2 e^{-\psi}}\right)\\
&\Leftrightarrow 2\psi\cdot x+\psi > \left(1+\frac{1}{\sqrt{2}}\right)\log\left(\frac{e^{\psi}}{2\psi\mu^2}\right)\\
&\Leftrightarrow 2\psi\cdot x+\psi > \left(1+\frac{1}{\sqrt{2}}\right)\psi-\left(1+\frac{1}{\sqrt{2}}\right)\log(2\psi\mu^2)\\
&\Leftrightarrow 2\psi\cdot x > \frac{1}{\sqrt{2}}\cdot\psi-\left(1+\frac{1}{\sqrt{2}}\right)\log(2\psi\mu^2)\\
&\Leftrightarrow x > \frac{1}{2\sqrt{2}}-\frac{1+\frac{1}{\sqrt{2}}}{2}\frac{\log(2\psi\mu^2)}{\psi}.
\end{aligned}$$

□

Theorem 16.1. *Let $z\in\mathbb{N}$. A sufficient condition for having $P_{SN}(z)<P(z)$ is $z\geq z_0$ with $z_0=\lceil z_0^*\rceil$ being the smallest integer greater or equal to*

$$z_0^*=\max\left(\frac{2}{\pi\left(1-\frac{q}{p}\right)^2},\frac{1}{2\sqrt{2}}-\frac{\left(1+\frac{1}{\sqrt{2}}\right)}{2}\frac{\log\left(\frac{2\psi(p)}{\pi}\right)}{\psi(p)}\right),$$

where $\psi(p)=\frac{q}{p}-1-\log(\frac{q}{p})-\log(\frac{1}{4pq})>0$.

Proof. First, note that

$$\begin{aligned}
\psi(p) &= \frac{q}{p}-1-\log\left(\frac{q}{p}\right)-\log\left(\frac{1}{4p^2}\frac{p}{q}\right)\\
&= 2\left[\frac{1}{2p}-1-\log\left(\frac{1}{2p}\right)\right].
\end{aligned}$$

Table 4. Sharp values.

z_0	2	3	4	5	6	7	8	9	10	11
$q \geq$	0.000	0.232	0.305	0.342	0.365	0.381	0.393	0.401	0.409	0.415

So, $\psi(p) > 0$ and z_0 is well defined. Let $z > z_0$. By Lemma 14.2 and Corollary 15.1 it is enough to prove that

$$\frac{1}{1-\frac{q}{p}}\frac{1}{\sqrt{2\pi z}}e^{-z(\frac{q}{p}-1-\log\frac{q}{p})}+\frac{1}{2}e^{-z(\frac{q}{p}-1-\log(\frac{q}{p}))}<S\sqrt{\frac{z}{z+\frac{1}{2}}}\frac{s^z}{\sqrt{\pi z}}.$$

We have $z \geq z_0 \geq \frac{2}{\pi(1-\frac{q}{p})^2}$, thus $\frac{1}{1-\frac{q}{p}}\frac{1}{\sqrt{2\pi z}} \leq \frac{1}{2}$. So, the inequality is satisfied as soon as $e^{-z\psi(p)} < \frac{(\frac{1}{\sqrt{\pi}})}{\sqrt{z+\frac{1}{2}}}$ and the result follows from Lemma 16.3. □

17. Tables for $P(z, \kappa)$

For complete Satoshi tables see Grunspan & Pérez-Marco (2017).

Table 5. $P(3, \kappa)$ $(z = 3)$ for different values of κ and q in %.

$\kappa\backslash q$	0.02	0.04	0.06	0.08	0.1	0.12	0.14	0.16	0.18	0.2	0.22	0.24	0.26
0.1	0	0.01	0.03	0.09	0.18	0.33	0.55	0.88	1.34	1.96	2.78	3.87	5.27
0.2	0	0.01	0.05	0.11	0.23	0.42	0.71	1.12	1.68	2.44	3.44	4.74	6.39
0.3	0	0.02	0.06	0.15	0.3	0.55	0.91	1.42	2.11	3.04	4.24	5.77	7.7
0.4	0	0.02	0.08	0.19	0.39	0.69	1.14	1.77	2.62	3.74	5.17	6.98	9.22
0.5	0	0.03	0.1	0.24	0.49	0.87	1.43	2.2	3.22	4.56	6.25	8.36	10.93
0.6	0	0.04	0.13	0.31	0.61	1.08	1.76	2.69	3.92	5.49	7.47	9.9	12.83
0.7	0.01	0.05	0.16	0.38	0.75	1.33	2.14	3.25	4.7	6.54	8.82	11.59	14.89
0.8	0.01	0.06	0.19	0.46	0.92	1.61	2.58	3.88	5.57	7.7	10.3	13.42	17.11
0.9	0.01	0.07	0.24	0.56	1.11	1.92	3.06	4.58	6.53	8.96	11.9	15.39	19.45
1	0.01	0.08	0.28	0.67	1.32	2.27	3.6	5.36	7.58	10.32	13.61	17.47	21.9
1.1	0.01	0.1	0.34	0.8	1.55	2.66	4.19	6.2	8.71	11.78	15.42	19.64	24.44
1.2	0.02	0.12	0.4	0.94	1.81	3.09	4.84	7.1	9.92	13.32	17.32	21.91	27.05
1.3	0.02	0.14	0.47	1.09	2.1	3.55	5.53	8.07	11.2	14.95	19.3	24.24	29.72
1.4	0.02	0.16	0.54	1.26	2.4	4.06	6.27	9.1	12.55	16.64	21.34	26.62	32.41
1.5	0.02	0.19	0.62	1.44	2.74	4.59	7.06	10.18	13.96	18.39	23.44	29.04	35.12
1.6	0.03	0.22	0.71	1.64	3.1	5.17	7.9	11.32	15.43	20.2	25.58	31.49	37.83
1.7	0.03	0.25	0.81	1.85	3.48	5.78	8.78	12.51	16.95	22.06	27.76	33.96	40.53
1.8	0.04	0.28	0.91	2.08	3.89	6.42	9.7	13.75	18.52	23.95	29.96	36.42	43.2
1.9	0.04	0.32	1.03	2.33	4.32	7.1	10.67	15.03	20.13	25.88	32.18	38.88	45.84
2	0.05	0.36	1.15	2.58	4.78	7.8	11.67	16.35	21.77	27.83	34.4	41.32	48.43
2.1	0.05	0.4	1.28	2.86	5.26	8.54	12.71	17.7	23.44	29.8	36.62	43.74	50.96
2.2	0.06	0.44	1.41	3.15	5.77	9.31	13.78	19.09	25.14	31.78	38.84	46.12	53.43
2.3	0.07	0.49	1.56	3.46	6.3	10.11	14.88	20.51	26.86	33.77	41.04	48.46	55.84
2.4	0.07	0.54	1.71	3.78	6.85	10.94	16.01	21.95	28.59	35.75	43.21	50.76	58.17
2.5	0.08	0.6	1.87	4.11	7.42	11.79	17.17	23.41	30.34	37.73	45.36	53	60.43
2.6	0.09	0.65	2.04	4.46	8.01	12.67	18.35	24.89	32.09	39.7	47.48	55.19	62.6
2.7	0.1	0.71	2.22	4.83	8.62	13.57	19.56	26.39	33.84	41.65	49.56	57.32	64.7

Table 5. (*Continued*)

$\kappa\backslash q$	0.02	0.04	0.06	0.08	0.1	0.12	0.14	0.16	0.18	0.2	0.22	0.24	0.26
2.8	0.11	0.78	2.41	5.21	9.26	14.49	20.78	27.9	35.59	43.59	51.6	59.38	66.71
2.9	0.12	0.85	2.6	5.6	9.91	15.44	22.02	29.42	37.34	45.5	53.6	61.39	68.64
3	0.13	0.92	2.81	6.01	10.58	16.4	23.28	30.94	39.08	47.38	55.55	63.32	70.49
3.1	0.14	0.99	3.02	6.44	11.27	17.38	24.55	32.47	40.81	49.24	57.45	65.19	72.25
3.2	0.15	1.07	3.24	6.87	11.97	18.38	25.83	34	42.52	51.06	59.31	67	73.93
3.3	0.16	1.15	3.47	7.32	12.69	19.39	27.12	35.52	44.22	52.85	61.11	68.73	75.53
3.4	0.17	1.23	3.7	7.78	13.43	20.42	28.42	37.05	45.9	54.61	62.86	70.39	77.05
3.5	0.19	1.32	3.95	8.26	14.18	21.46	29.73	38.56	47.56	56.32	64.55	71.99	78.5

Table 6. $P(6, \kappa)$ ($z = 6$) for different values of κ and q in %.

$\kappa\backslash q$	0.02	0.04	0.06	0.08	0.1	0.12	0.14	0.16	0.18	0.2	0.22	0.24	0.26
0.1	0	0	0	0	0	0	0	0.01	0.02	0.04	0.08	0.15	0.28
0.2	0	0	0	0	0	0	0.01	0.01	0.03	0.06	0.12	0.23	0.41
0.3	0	0	0	0	0	0	0.01	0.02	0.05	0.09	0.18	0.34	0.6
0.4	0	0	0	0	0	0.01	0.01	0.03	0.07	0.15	0.28	0.51	0.88
0.5	0	0	0	0	0	0.01	0.02	0.05	0.11	0.23	0.42	0.75	1.28
0.6	0	0	0	0	0	0.01	0.04	0.08	0.17	0.34	0.63	1.1	1.84
0.7	0	0	0	0	0.01	0.02	0.06	0.13	0.26	0.51	0.91	1.57	2.57
0.8	0	0	0	0	0.01	0.03	0.08	0.19	0.39	0.73	1.3	2.19	3.53
0.9	0	0	0	0	0.02	0.05	0.12	0.28	0.55	1.03	1.81	2.99	4.73
1	0	0	0	0.01	0.02	0.07	0.18	0.39	0.78	1.43	2.45	3.99	6.19
1.1	0	0	0	0.01	0.04	0.1	0.25	0.54	1.06	1.92	3.25	5.2	7.93
1.2	0	0	0	0.01	0.05	0.14	0.35	0.74	1.42	2.53	4.21	6.63	9.94
1.3	0	0	0	0.02	0.07	0.2	0.47	0.98	1.86	3.26	5.35	8.29	12.23
1.4	0	0	0	0.03	0.09	0.26	0.62	1.28	2.39	4.14	6.68	10.19	14.79
1.5	0	0	0.01	0.03	0.12	0.34	0.8	1.64	3.02	5.15	8.19	12.3	17.58
1.6	0	0	0.01	0.05	0.16	0.45	1.02	2.06	3.76	6.31	9.89	14.63	20.59
1.7	0	0	0.01	0.06	0.21	0.57	1.29	2.56	4.6	7.62	11.77	17.16	23.78
1.8	0	0	0.02	0.08	0.27	0.71	1.6	3.14	5.56	9.07	13.82	19.86	27.13
1.9	0	0	0.02	0.1	0.34	0.89	1.96	3.79	6.63	10.67	16.04	22.72	30.59
2	0	0	0.03	0.12	0.42	1.09	2.37	4.53	7.82	12.42	18.4	25.71	34.14
2.1	0	0	0.03	0.15	0.51	1.32	2.83	5.35	9.12	14.29	20.9	28.81	37.73
2.2	0	0	0.04	0.19	0.62	1.58	3.36	6.26	10.54	16.29	23.51	31.98	41.34
2.3	0	0	0.05	0.23	0.75	1.88	3.95	7.26	12.06	18.41	26.23	35.21	44.94
2.4	0	0.01	0.06	0.28	0.89	2.21	4.59	8.35	13.69	20.64	29.02	38.47	48.49
2.5	0	0.01	0.07	0.33	1.05	2.59	5.3	9.52	15.42	22.95	31.87	41.73	51.97
2.6	0	0.01	0.09	0.4	1.24	3	6.08	10.78	17.24	25.35	34.77	44.98	55.35
2.7	0	0.01	0.1	0.47	1.44	3.45	6.92	12.12	19.15	27.81	37.69	48.19	58.63
2.8	0	0.01	0.12	0.55	1.67	3.95	7.82	13.54	21.14	30.33	40.62	51.34	61.78
2.9	0	0.02	0.14	0.64	1.92	4.49	8.79	15.04	23.19	32.89	43.54	54.42	64.8
3	0	0.02	0.17	0.74	2.2	5.08	9.82	16.6	25.31	35.48	46.44	57.41	67.66
3.1	0	0.02	0.19	0.85	2.5	5.71	10.91	18.24	27.47	38.08	49.29	60.3	70.38
3.2	0	0.03	0.22	0.97	2.83	6.39	12.06	19.93	29.68	40.68	52.1	63.09	72.94
3.3	0	0.03	0.26	1.11	3.18	7.11	13.27	21.68	31.93	43.28	54.84	65.75	75.33
3.4	0	0.03	0.3	1.25	3.57	7.88	14.54	23.48	34.2	45.86	57.52	68.3	77.57
3.5	0	0.04	0.34	1.41	3.98	8.69	15.86	25.33	36.48	48.41	60.11	70.72	79.66

Acknowledgments

We are grateful to N. Emerson for his comments and remarks.

References

M. Abramovitch & I. A. Stegun (1970) *Handbook of Mathematical Functions*. New York: Dover.

W. Feller (1971) *An Introduction to Probability Theory and Its Applications*, Vol. 2, Second edition. Wiley Series in Probability and Mathematical Statistics. New York: Wiley.

W. Gautschi (1959) Some elementary inequalities relating to the gamma and incomplete gamma function, *Journal of Mathematics and Physics* **38**, 77–81.

C. Grunspan & R. Pérez-Marco (2017) Satoshi risk tables. arXiv:1702.04421 [cs.CR].

J. L. López & J. Sesma (1999) Asymptotic expansion of the incomplete beta function for large values of the first parameter, *Integral Transforms and Special Functions* **8** (3–4), 233–236.

S. Nakamoto (2008) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

F. W. J. Olver, A. B. Olde Daalhuis, D. W. Lozier, B. I. Schneider. R. F. Boisvert, C. W. Clark, B. R. Miller & B. V. Saunders (eds.) (2018) *NIST Digital Library of Mathematical Functions*. Gaithersburg: NIST.https://dlmf.nist.gov.

R. Pérez-Marco (2016) Bitcoin and decentralized trust protocols, *Newsletter of the European Mathematical Society* **100**, 32–38.

M. Rosenfeld (2012) Analysis of hashrate-based double-spending. https://bitcointalk.org/index.php?topic=130222.msg1396932#msg1396932.

M. Rosenfeld (2014) Analysis of hashrate-based double spending. arXiv:1402.2009v1 [cs.CR].