Probability in the Engineering and Informational Sciences, page 1 of 15, 2021.
doi:10.1017/S026996482100005X

ON PROFITABILITY OF NAKAMOTO DOUBLE SPEND

CYRIL GRUNSPAN
Léonard de Vinci, Pôle University, Research Center, Paris-La Défense, France
E-mail: cyril.grunspan@devinci.fr

RICARDO PÉREZ-MARCO
CNRS, IMJ-PRG, Paris, France
E-mail: ricardo.perez.marco@gmail.com

Nakamoto doublespend strategy, described in Bitcoin foundational article, leads to total ruin with positive probability. The simplest strategy that avoids this risk incorporates a stopping threshold when success is unlikely. We compute the exact profitability and the minimal double spend that is profitable for this strategy. For a given amount of the transaction, we determine the minimal number of confirmations to be requested by the recipient that makes the double-spend strategy non-profitable. This number of confirmations is only 1 or 2 for average transactions and for a small relative hashrate of the attacker. This is substantially lower than the original Nakamoto number, which is about six confirmations and is widely used. Nakamoto analysis is only based on the success probability of the attack instead of on a profitability analysis that we carry out.

Keywords: Bitcoin, blockchain, Gambler's ruin, martingale, proof-of-work, random walk

1. INTRODUCTION AND BACKGROUND

1.1. Bitcoin Network

Satoshi Nakamoto's foundational article [17] describes Bitcoin protocol. Bitcoin is an electronic currency and bitcoin transactions operate through a computer network. This network is *permissionless*: anyone can freely enter or leave the network. Moreover, there is no central authority to act as a referee. The creation of monetary mass is implemented in the protocol. Transactions are packed in chronologically ordered blocks that create an unforgeable public ledger: *the blockchain*. Certain nodes of the network, called miners, play a special role. They secure the blockchain through intensive computation by a "proof of work", a technique originally invented to fight e-mail spam and denial of service attacks. A miner creates a new block of transactions to add to the blockchain by solving a cryptographic puzzle by brute force iterating a simple algorithm (and no other resolution method is known). For this computational work, he is rewarded by a *coinbase reward* of newly minted bitcoins. This is the mechanism that creates Bitcoin monetary mass.

 0269-9648/19 $25.00

1.2. Blocks Counting Process

Section 11 of Nakamoto's article contains an analysis of Bitcoin security by estimating the probability of success of a double-spend attack. This type of attack was the major obstacle to the creation of a permissionless cryptocurrency network. Nakamoto uses a Poisson distribution model for block creation to estimate this probability. For the mathematical justification of this model, the reader can consult the survey [14]. In this model, the probability for a miner of discovering the next block is proportional to his computing power, or his relative hashrate $0 < q \leq 1$. For a relative hashrate $q \geq 1/2$, the network is not secure and the miner can rewrite the blockchain at his will. Thus, a necessary condition for the proper decentralized operations is the condition $0 < q < 1/2$, that we assume in the rest of the article. Assuming the hashing function (constructed from SHA256 for Bitcoin) to be perfect, the time takes for a miner to find the next block follows an exponential law. From this, it follows that the block counting process is Poisson. The mathematics behind Bitcoin mining are Poisson mathematics.

1.3. Original Double-Spend Attack

The attacker attempts the double spend by broadcasting a legitimate transaction and simultaneously starts mining a secret fork with a conflicting transaction invalidating the first one. The recipient requests beforehand at least $z \geq 0$ confirmations of the transaction, that is, z new blocks created counting from the first one containing the transaction, to consider it definitive. The goal of the attacker is to catch-up the official blockchain after these z confirmations and rewrite this last part of the blockchain including the conflicting transaction. His probability of success was computed in closed form by the authors in [13], correcting the original approximate Nakamoto formula given in [17]. If the attacker fails, he will be stuck forever catching-up the official blockchain and will go broke. This scenario of total ruin has a positive probability. The attacker has a small chance of winning, but on average, its revenue is finite while the mean duration time of the attack is infinite. We have the following Lemma (see the Appendix for a proof) which shows that the original Nakamoto double-spend strategy is unsound.

LEMMA 1.1: *Let* $\mathbf{R}$ *be the revenue of a miner following the original Nakamoto's double-spend attack and* $\mathbf{T}$ *the duration time of the attack. Then, we have* $\mathbb{E}[\mathbf{R}] < \infty$ *and* $\mathbb{E}[\mathbf{T}] = \infty$.

1.4. A Sound Double-Spend Attack

For a sound strategy, it is unacceptable to have a positive probability of total ruin. Thus, we are led to introduce some sort of "give-up" mechanism. It is then natural to modify the strategy so that if the attacker lags behind the official blockchain by a predetermined value $A \geq z$, then he gives-up. This A-Nakamoto strategy (the precise definition is given in Section 2) defines an integrable repetition game and fits in the general mining profitability theory developed by the authors in [10].

According to [10], the profitability is compared using the *Revenue Ratio*

$$\Gamma = \frac{\mathbb{E}[\mathbf{R}]}{\mathbb{E}[\mathbf{T}]}$$

where $\mathbf{R}$ and $\mathbf{T}$ are random variables, $\mathbf{R}$ is the revenue, and $\mathbf{T}$ is the duration of the attack. For example, for the honest strategy consisting of mining one block according to the protocol

rules, we have $\mathbb{E}[\mathbf{R}_H] = qb$, where b is the coinbase reward, and $\mathbb{E}[\mathbf{T}_H] = \tau_0$, where τ_0 is the interblock time,[1] thus the honest Revenue Ratio is

$$\Gamma_H = \frac{qb}{\tau_0}.$$

We compare the profitability of two full time mining strategies by comparing their Revenue Ratios (Proposition 3.6 from Section 3 in [10]). Therefore, the A-Nakamoto strategy is profitable if and only if its Revenue Ratio Γ_A is higher than the Revenue Ratio of the honest strategy, $\Gamma_A > \Gamma_H$.

The first result is an exact closed-form formula for the probability of success of the A-Nakamoto strategy.

THEOREM 1.2: *Let $0 < q < 1/2$, resp. $p = 1 - q$, be the relative hashrate of the attacker, resp. of honest miners. We denote $\lambda = q/p < 1$. Let $z \geq 1$ be the number of confirmations requested by the recipient of a transaction. For $A \geq z$, the probability $P_A(z)$ of success for the A-Nakamoto double-spend attack is*

$$P_A(z) = \frac{I_{4pq}(z, 1/2) - \lambda^{A+1}}{1 - \lambda^{A+1}}$$

where $I_a(x, y)$ is the Regularized Incomplete Beta function

$$I_a(x, y) = \frac{\Gamma(x + y)}{\Gamma(x)\Gamma(y)} \int_0^a t^{x-1}(1 - t)^{y-1}\, dt,$$

and Γ is Euler Gamma function.

In the formula for $P_A(z)$, we have that $A + 1$ appears instead of A because we assume that the attacker premines one block (as it is implicit in Satoshi's paper, see Section 2). A Corollary of this first Theorem is the main result from [13] that we can get by taking the limit $A \to +\infty$.

COROLLARY 1.3 [13]: *The probability of success of the ∞-Nakamoto attack is*

$$P_\infty(z) = I_{4pq}(z, 1/2).$$

NOTE 1.4: *This probability is computed at the start of the attack, and at the time, the honest miners have mined z blocks, the number mined by the attacker can exceed z.*

A Corollary of this result is obtained taking the asymptotics.

COROLLARY 1.5 [13]: *When $z \to +\infty$, we have*

$$P_\infty(z) \sim \frac{s^z}{\sqrt{\pi(1 - s)z}}$$

where $s = 4pq < 1$.

This Corollary is important because it proves the profusely cited and "well-known" result that this probability decays exponentially to 0 with the number of confirmations z;

[1] In the current Bitcoin network, $b = 12.5$ and $\tau_0 = 10$ min.

hence, the probability of a reorganization of Bitcoin blockchain decays exponential with the depth. This exponential decay is the fundamental result for Bitcoin security. This was not proved rigorously in the literature before [13].

We observe that $P_A(z)$ decreases with A, and $P_A(z) < \lim_{A\to+\infty} P_A(z) = P_\infty(z)$ as expected. We also have that, when $z \to +\infty$,

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

with an asymptotic that is independent of A. In the next Theorem, we make use of the Beta function

$$B(x,y) = \int_0^1 t^{x-1}(1-t)^{y-1}\,dt = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}.$$

The main result in this article is the computation of the Revenue Ratio Γ_A. We also compute exact formulas for $\mathbb{E}[\mathbf{R}_A]$ and $\mathbb{E}[\mathbf{T}_A]$.

THEOREM 1.6: *With the previous notations, the expected revenue and the expected duration of the A-Nakamoto double-spend strategy is, with the notation* $[n] = (1-\lambda^n)/(1-\lambda)$,

$$\begin{aligned}\frac{\mathbb{E}[\mathbf{R}_A]}{b} &= \frac{qz}{2p} I_{4pq}(z,1/2) - \frac{(A+1)\lambda^{A+1}}{p(1-\lambda)^3[A+1]^2} I_{(p-q)^2}(1/2,z)\\ &\quad + \frac{2-\lambda+\lambda^{A+2}}{(1-\lambda)^2[A+1]}\frac{p^{z-1}q^z}{B(z,z)} + P_A(z)\left(\frac{v}{b}+1\right),\\ \frac{\mathbb{E}[\mathbf{T}_A]}{\tau_0} &= \frac{z}{2p} I_{4pq}(z,1/2) + \frac{A+1}{p(1-\lambda)^2[A+1]} I_{(p-q)^2}(1/2,z) - \frac{p^{z-1}q^z}{p(1-\lambda)B(z,z)} + \frac{1}{q}.\end{aligned}$$

As in the original article [10], and applications to other block withholding strategies [11], the main tool in the proof are martingale techniques and the application of Doob's Stopping Time Theorem. These new techniques proved superior to previous approaches using Markov chains. For example, only with martingale techniques, we can prove [10] that without difficulty adjustment the honest mining strategy is optimal. The profitability analysis is based on attack cycles, modeled by games with repetition. It applies to integrable games, that is those that have a finite expectation duration of cycles $\mathbb{E}[\mathbf{T}] < +\infty$, which is a necessary condition for the application of Doob's Stopping Theorem.

All other parameters being fixed, we observe the asymptotics when $A \to +\infty$,

$$\frac{\mathbb{E}[\mathbf{T}_A]}{\tau_0} \sim \frac{I_{(p-q)^2}(1/2,z)}{p-q}\,A$$

and

$$\lim_{A\to+\infty}\frac{\mathbb{E}[\mathbf{R}_A]}{b} = \frac{\mathbb{E}[\mathbf{R}_\infty]}{b} = \frac{qz}{2p} I_{4pq}(z,1/2) + \frac{2-\lambda}{1-\lambda}\frac{p^{z-1}q^z}{B(z,z)} + P_\infty(z)\left(\frac{v}{b}+1\right).$$

In particular, we have

$$\lim_{A\to\infty}\mathbb{E}[\mathbf{T}_A] = \mathbb{E}[\mathbf{T}_\infty] = +\infty$$

and

$$\lim_{A\to\infty}\mathbb{E}[\mathbf{R}_A] = \mathbb{E}[\mathbf{R}_\infty] < +\infty.$$

Hence, in the non-stopping Nakamoto double-spend strategy where $A = +\infty$, we have $\Gamma_\infty = 0$ and any integrable strategy beats Nakamoto non-stopping strategy. Moreover,

since $\mathbb{E}[\mathbf{R}_\infty] < +\infty$ and $\mathbb{E}[\mathbf{T}_\infty] = +\infty$ Nakamoto's strategy leads to almost sure ruin when considering mining costs.

Another interesting asymptotic is, when $q \to 0$, $z \geq 1$,

$$I_{4pq}(z, 1/2) \sim 2 \binom{2z-1}{z} q^z.$$

If we assume $A \geq 2$, $A \geq z \geq 1$,

$$\frac{\mathbb{E}[\mathbf{R}_A]}{b} \sim \left[2 \binom{2z-1}{z} \left(\frac{v}{b} + 1 \right) + \frac{2}{B(z,z)} \right] q^z$$

and

$$\frac{\mathbb{E}[\mathbf{T}_A]}{\tau_0} \sim \frac{1}{q}.$$

Therefore, we have, when $q \to 0$,

$$\Gamma_A \sim \frac{b}{\tau_0} \left[2 \binom{2z-1}{z} \left(\frac{v}{b} + 1 \right) + \frac{2}{B(z,z)} \right] q^{z+1}.$$

It is noteworthy that this asymptotic is uniform on A. Using it we can prove the following practical Corollary. The A-Nakamoto double spend is profitable when $\Gamma_A \geq \Gamma_H$ and plugging the asymptotics in this profitability inequality we get,

COROLLARY 1.7: *When $q \to 0$, the minimal amount to make profitable a Nakamoto double spend with $z \geq 1$ confirmations is asymptotically*

$$v \geq \frac{q^{-z}}{2 \binom{2z-1}{z}} b = v_0.$$

For example, with $q = 0.01$ and only $z = 1$, we need to double spend more than $v_0/b = 50$ coinbases. For the optimal strategy, the minimal spend for these parameters is $v_0/b = 49.2513$ coinbases as we have computed elsewhere. With the actual reward of $b = 6.25$ and the actual prize of \$11.750, this represents more than \$3.600.000. With $z = 2$, we need more than 1.666 coinbases for a profitable attack, or more than 122 million dollars. These figures are far from the general belief.[2] We observe that there are other sharper strategies and, if ran continuously, we can merge double-spend attacks with other block withholding strategies and this will increase the profitability.

We observe that, since $\Gamma_A \to 0$ when $A \to +\infty$, there is a value $A_0 = A_0(q, v, z) \geq z$ that maximizes the revenue ratio:

$$\Gamma_{A_0} = \max_{A \geq z} \Gamma_A.$$

Also, we have $\lim_{z \to +\infty} \Gamma_{A_0} < \Gamma_H$. So given the amount of the purchase (in coinbase b units), we can compute the number z of confirmations that make the A-Nakamoto double-spend attack non-profitable. This is an important data for the vendor or the recipient of the transaction that can set the optimal number of confirmations z by using our formulas.

[2] For instance, many cryptocurrency exchanges require six confirmations for any Bitcoin deposit. Although it is advisable to request two confirmations, to avoid a possible disruption by an orphan block.

We keep the analysis for the A-Nakamoto strategy as simple as possible. We assume no difficulty adjustments and instant block propagation in the network during the attack. Other more sophisticated strategies, as when $A \leq z$, with important premining, or the optimal strategy, or other hybrid strategies combining selfish mining and double spends, will be analyzed elsewhere.

The core of the results presented in this article are a combination the techniques developed in [10,13].

2. NAKAMOTO DOUBLE-SPEND STRATEGY

Let z be the number of confirmations required by the merchant and v is the value of a double spend. We fix a maximal lag $A \geq z$ behind the public blockchain for which the attacker gives-up. The relative hashrate of the attacker (resp. honest miners) is q (resp. p). Nakamoto in [17] tries to prevent premining by the attacker. He proposes the instant generation new keys for each payment, but it is easy to see that this does not prevent double spends. The formulas he gives are only correct premining one block (e.g., when he states that the probability is 1 for $z = 0$ confirmations). The strategy of premining one block is often named as a "Finney attack" because of the clarification that H. Finney provided in 2011 (see [6] bitcointalk post). We can generalize this Finney strategy by premining k of blocks before launching the attack. The precise algorithm employed by the attacker in this (A, k)-Nakamoto double-spend strategy is the following:

(A, k)-Nakamoto double-spend strategy

0. *Start of the attack cycle* (*goto* 1).
1. *The attacker mines honestly on top of the official blockchain k blocks with a transaction that returns the payment funds to an address he controls* (*goto* 2).
2. *If the honest miners get ahead before the attacker premines k blocks, then he restarts mining on top of the new last block of the official blockchain* (*goto* 1).
3. *If the attacker succeeds in premining k blocks leading the honest miners, he keeps his fork secret, sends the purchasing transaction to the vendor, and keeps up mining on his secret fork* (*goto* 4).
4. *If the attacker's lag behind the official blockchain becomes larger than A, then the attacker gives-up and the double spend fails* (*goto* 6).
5. *If the secret fork of the attacker gets longer than the official blockchain that has added z confirmations to the vendor transaction, then the attacker releases his fork and the double spend is successful* (*goto* 6).
6. *End of the attack cycle* (*goto* 0).

We assume that when we reach z confirmations, the attacker receives the goods from the vendor. Hence, for a successful attack, the revenue is v plus all block rewards. When the attack fails, the revenue is 0 (assuming that he can recover the original payment from the purchase). A fundamental observation for the application of the profitability model is that the total costs per unit of time is the same as the total cost of honest mining. Each time the attacker goes to step 0, he can start a new attack cycle that ends when he reaches step 6.

We observe that the strategy has three distinct phases:

- The first phase is the premine (steps 1–2).
- The attacker sends his transaction to the merchant and mines a conflicting transaction on his secret fork until the honest miners have validated z blocks.

- The attacker keeps on mining on his secret fork until his lag is A or his fork catch-up the official blockchain.

During the second phase, the attacker lags behind the official blockchain less than A since we are assuming $A \geq z$. So, the attack cycle cannot terminate before the end of the second phase. Notice also that there are more general Nakamoto strategies by changing the algorithm in the premining phase and the last phase. The $(A, 1)$-Nakamoto strategy is the simplest and closest profitable strategy to Nakamoto's strategy described in his article. This strategy is the one studied in this article.

The study of general (A, k)-Nakamoto strategies is postponed to a future article, as well as the general optimal strategy attack.

3. PROBABILITY OF SUCCESS

We use the same notations and the classical mining model from [13]. The number of blocks mined by the attacker is a Poisson process $(N'(t))_{t\geq 0}$. The random variable $\mathbf{S}_z$ is the time employed by the honest miners to mine z blocks. The random variable $N'(\mathbf{S}_z)$ is a (z, p) negative binomial random variable [13], for $j \geq 0$,

$$\mathbb{P}[N'(\mathbf{S}_z) = j] = p^z q^j \binom{z+j-1}{j}.$$

We recall the basic Euler identity for the Beta function which justifies the Beta distribution,

$$B(x, y) = \int_0^1 t^{x-1}(1-t)^{y-1}\, dt = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x+y)}.$$

We need some basic combinatorial identities from the next Lemma.

LEMMA 3.1: *For integers $m \geq 1$ and $z \geq 0$, and for $p, q > 0$ with $q = 1 - p$, we have*

$$\sum_{j=0}^{m-1} p^z q^j \binom{z+j-1}{j} = I_p(z, m), \tag{1}$$

$$\sum_{j=0}^{m-1} p^z q^j \binom{z+j-1}{j} \cdot j = \frac{qz}{p} I_p(z, m) - \frac{p^{z-1}q^m}{B(z, m)}. \tag{2}$$

PROOF: The first identity is classical (see [1] (6.6.3) and (26.5.26), or [4] (8.17.24), or [13] Sect. 6). The second follows from the first one differentiating with respect to p,

$$\frac{\partial I_p(z, m)}{\partial p} = \frac{z}{p} I_p(z, m) - \frac{1}{q} \sum_{j=0}^{m-1} p^z q^j \binom{z+j-1}{j} \cdot j$$

and observing that $(\partial I_p(z, m))/\partial p = p^{z-1}q^{m-1}/B(z, m)$. ■

PROPOSITION 3.2: *If* $\mathbf{X}$ *is a negative binomial random variable with parameters* (p,z)*, then we compute*

$$\sum_{j=0}^{z-1}\mathbb{P}[\mathbf{X}=j]=I_p(z,z), \tag{3}$$

$$\sum_{j=0}^{z-1}\mathbb{P}[\mathbf{X}=j](q/p)^{z-j}=I_q(z,z), \tag{4}$$

$$\sum_{j=0}^{z-1}\mathbb{P}[\mathbf{X}=j]\cdot j=\frac{qz}{p}I_p(z,z)-\frac{p^{z-1}q^z}{B(z,z)}, \tag{5}$$

$$\sum_{j=0}^{z-1}\mathbb{P}[\mathbf{X}=j]j(q/p)^{z-j}=\frac{pz}{q}I_q(z,z)-\frac{q^{z-1}p^z}{B(z,z)}. \tag{6}$$

PROOF: Identities (3) and (5) follow from Lemma 3.1. The two other ones follow from these two using, for $j\geq 0$,

$$p^zq^j\begin{pmatrix} z+j-1 \\ j\end{pmatrix}(q/p)^{z-j}=q^zp^j\begin{pmatrix} z+j-1 \\ j\end{pmatrix}$$

which means that $\mathbb{P}[\mathbf{X}=j](q/p)^{z-j}=\mathbb{P}[\mathbf{Y}=j]$ for $\mathbf{Y}$ a (q,z)-negative binomial random variable. ■

Note also that (1) and (2) can be restated as

$$\mathbb{P}[\mathbf{X}<m]=I_p(z,m)$$
$$\mathbb{E}[\mathbf{X}|\mathbf{X}<m]=\frac{qz}{p}-\frac{p^{z-1}q^m}{B_p(z,m)}$$

where $B_x(a,b)$ is the incomplete Beta function. We are ready to prove Theorem 1.2.

Proof of Theorem 1.2: Recall that the attacker has premined one block. So, if he has added z more blocks to his secret fork during the second phase of the attack, then at the end of this phase his secret fork is longer than the official blockchain. In this case, he publishes his fork and the attack cycle ends successfully. Otherwise, the attacker has mined j blocks during the second phase with $j<z$ and he starts a third phase with a lag of $z-j-1$. The evolution of this lag is a biased random walk $(\mathbf{Z}_n)$ with a probability p (resp. q) to move to the right (resp. left). The cycle ends when there is $n\in\mathbb{N}$ such that $\mathbf{Z}_n=A$ (the attack cycle fails) or $\mathbf{Z}_n=-1$ (the attack cycle is successful). Hence, according to the Gambler's

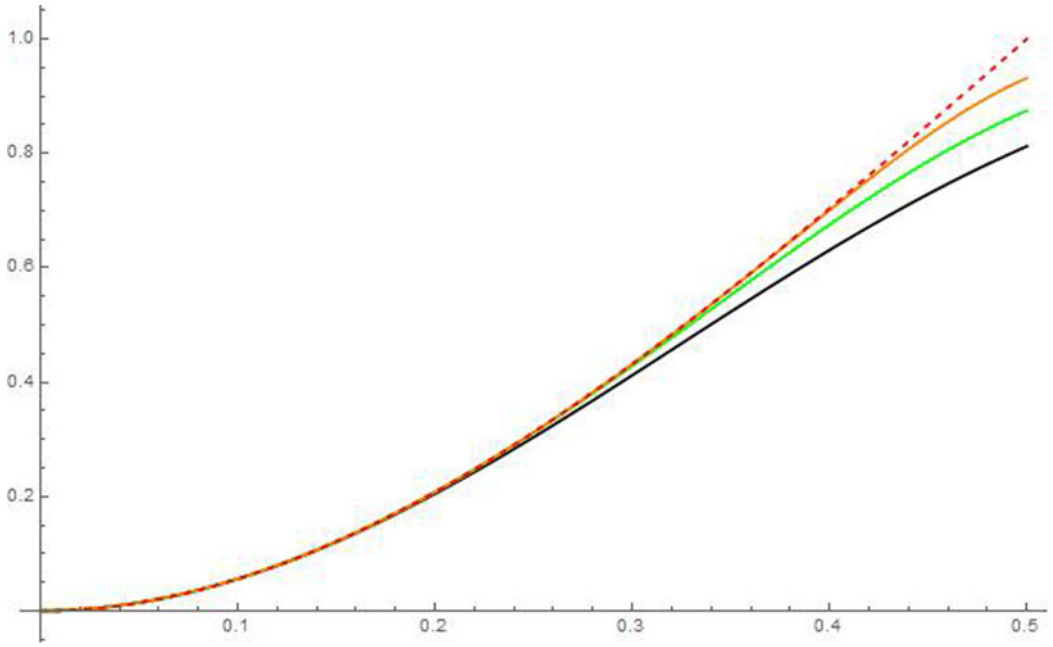

FIGURE **1.** Graph of $q \mapsto P_A(2)$, $A = 3, 5, 10$ and asymptotics $A \to +\infty$.

ruin problem formula (see [5]), and using formulas (3) and (4) from Corollary 3.2, we have

$$\begin{aligned} P_A(z) &= \mathbb{P}[N'(\mathbf{S}_z) \geqslant z] + \sum_{j=0}^{z-1} \mathbb{P}[N'(\mathbf{S}_z) = j] \, \frac{\lambda^{z-j} - \lambda^{A+1}}{1 - \lambda^{A+1}} \\ &= 1 - \sum_{j=0}^{z-1} \mathbb{P}[N'(\mathbf{S}_z) = j] + \sum_{j=0}^{z-1} \mathbb{P}[N'(\mathbf{S}_z) = j] \, \frac{\lambda^{z-j} - \lambda^{A+1}}{1 - \lambda^{A+1}} \\ &= 1 - \left(1 + \frac{\lambda^{A+1}}{1 - \lambda^{A+1}}\right) \sum_{j=0}^{z-1} \mathbb{P}[N'(\mathbf{S}_z) = j] + \frac{1}{1 - \lambda^{A+1}} \sum_{j=0}^{z-1} \mathbb{P}[N'(\mathbf{S}_z) = j] \lambda^{z-j} \\ &= 1 - \frac{I_p(z,z)}{1 - \lambda^{A+1}} + \frac{I_q(z,z)}{1 - \lambda^{A+1}}. \end{aligned}$$

Finally, we use the two classical relations for the incomplete regularized beta function:

$$I_x(a,b) + I_{1-x}(b,a) = 1 \tag{7}$$

for $x \in]0,1[$, $a, b \in \mathbb{R}_+^*$ and

$$I_q(z,z) = \frac{1}{2} I_{4pq}(z, 1/2). \tag{8}$$

See for instance [4] (8.17.4) and (8.17.6) (Figure 1).

■

4. PROFITABILITY OF THE ATTACK

4.1. Expected Cycle Duration Time

According to the definition of the strategy in Section 2, the attack cycle cannot terminate before the attacker has mined one block (the premined block). So, the duration time of an attack cycle $\mathbf{T}$ satisfies $\mathbf{T} = \mathbf{S}'_1 + \mathbf{T}'$, where $\mathbf{S}'_1$ is the time before the attacker discovers a new block and $\mathbf{T}'$ is the remaining time of the attack.

PROPOSITION 4.1: *We assume that the attacker has already premined one block. Then, the mean duration time for the end of an attack cycle is*

$$\frac{\mathbb{E}[\mathbf{T}']}{\tau_0} = \frac{A+1}{p-q} \cdot \frac{1}{1-\lambda^{A+1}} - \frac{p^{z-1}q^z}{(p-q)B(z,z)} + \left(\frac{z}{p} - \frac{2(A+1)}{(p-q)(1-\lambda^{A+1})}\right) I_q(z,z).$$

PROOF: We follow the proof of Theorem 1.2. By definition of the strategy, the attack cycle cannot end before the honest miners have mined z blocks since $A \geq z$. So, we have $\mathbf{T}' \geq \mathbf{S}_z$ (the initial date $t = 0$ is the start of the second phase). Moreover, $\mathbf{T}' = \mathbf{S}_z$ if the attacker has mined z blocks or more during the second phase of the attack. Otherwise, the attacker tries to build a fork whose length is greater than the official blockchain, starting with an initial lag of $z - \mathbf{N}'(\mathbf{S}_z) - 1$ and gives up if this lag becomes greater or equal than A (third phase of the attack). So, we have

$$\mathbf{T}' = \mathbf{S}_z + 1_{\mathbf{N}'(\mathbf{S}_z)<z} \cdot \tilde{\mathbf{T}}_{A+1-(z-\mathbf{N}'(\mathbf{S}_z)),z-\mathbf{N}'(\mathbf{S}_z)}$$

with $\tilde{\mathbf{T}}_{X,Y} = \text{Inf}\,\{t \in \mathbb{R}_+; (\tilde{\mathbf{N}}(t) = \tilde{\mathbf{N}}'(t) + X) \vee (\tilde{\mathbf{N}}'(t) = \tilde{\mathbf{N}}(t) + Y)\}$ for $X, Y \in \mathbb{R}$, $\tilde{\mathbf{N}}(t) = \mathbf{N}(t + \mathbf{S}_z) - \mathbf{N}(\mathbf{S}_z)$ and $\tilde{\mathbf{N}}'(t) = \mathbf{N}'(t + \mathbf{S}_z) - \mathbf{N}'(\mathbf{S}_z)$. By the Markov property, $\tilde{\mathbf{N}}$ and $\tilde{\mathbf{N}}'$ are two Poisson processes with parameters p/τ_0 and q/τ_0 independent of $\mathbf{S}_z$ and $\tilde{\mathbf{T}}_{X,Y}$ is also independent of $\mathbf{S}_z$. Moreover, we have

$$\frac{\mathbb{E}[\tilde{\mathbf{T}}_{X,Y}]}{\tau_0} = \frac{X+Y}{p-q}\left(\frac{1-\lambda^Y}{1-\lambda^{X+Y}} - \frac{Y}{X+Y}\right).$$

This computation is classical and can be found in Appendix A of [12] for example (see Theorem A.1). So, we have using Proposition 3.2 together with (7) and (8),

$$\begin{aligned}
\frac{\mathbb{E}[\mathbf{T}']}{\tau_0} &= \mathbb{E}[\mathbf{S}_z] + \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j] \cdot \mathbb{E}[\tilde{\mathbf{T}}_{A+1-(z-j),z-j}] \\
&= \frac{z}{p} + \frac{A+1}{p-q}\left(\frac{1}{1-\lambda^{A+1}} - \frac{z}{A+1}\right) \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j] \\
&\quad - \frac{A+1}{p-q}\left(\frac{1}{1-\lambda^{A+1}}\right) \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j]\lambda^{z-j} \\
&\quad + \frac{1}{p-q} \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j] j
\end{aligned}$$

$$= \frac{z}{p} + \frac{A+1}{p-q}\left(\frac{1}{1-\lambda^{A+1}} - \frac{z}{A+1}\right) I_p(z,z) - \frac{A+1}{p-q}\cdot\frac{1}{1-\lambda^{A+1}} I_q(z,z)$$
$$+ \frac{1}{p-q}\left(\frac{qz}{p} I_p(z,z) - \frac{p^{z-1}q^z}{B(z,z)}\right)$$
$$= \frac{A+1}{p-q}\frac{1}{1-\lambda^{A+1}} - \frac{p^{z-1}q^z}{(p-q)B(z,z)} + \left(\frac{z}{p} - \frac{2(A+1)}{(p-q)(1-\lambda^{A+1})}\right) I_q(z,z). \quad \blacksquare$$

4.2. Expected Revenue by Cycle

PROPOSITION 4.2: *The expected revenue per cycle is*

$$\frac{\mathbb{E}[\mathbf{R}_A]}{b} = \frac{qz}{2p} I_{4pq}(z,1/2) - \frac{(A+1)\lambda^{A+1}}{p(1-\lambda)^3[A+1]^2} I_{(p-q)^2}(1/2,z)$$
$$+ \frac{2-\lambda+\lambda^{A+2}}{(1-\lambda)^2[A+1]}\frac{p^{z-1}q^z}{B(z,z)} + P_A(z)(v+1)$$

with $[A+1] = (1-\lambda^{A+1})/(1-\lambda)$.

PROOF: We will use the following notations. If $\mathbf{Z}$ is a biased simple random walk starting at $\mathbf{Z}_0 = k$ with a probability p (resp. q) to go right (resp. left), we denote by ν_i^k with $i \in \mathbb{Z}$ the hitting time of i and $\nu_{i,j}^k = \nu_i^k \wedge \nu_j^k$ with $j \in \mathbb{Z}$. We also denote by $\mathcal{L}(n)$ the number of steps to the left between 0 and n, that is,

$$\mathcal{L}(n) = \sum_{i=1}^{n} \mathbf{1}_{\mathbf{Z}_i = \mathbf{Z}_{i-1}-1}.$$

After the premining phase, the attacker waits for the honest miners to mine z blocks. Suppose that he has mined j blocks during this second phase. If $j \geq z$, then the attack cycle ends and the attacker wins the double-spend amount v and all the $j+1$ blocks he has mined. Otherwise, there is a third phase. The attack cycle still goes on and does not end before the attacker builts a fork whose length is larger than the official blockchain or his lag becomes larger or equal than A. We denote by $\mathbf{Z}_n$ the lag of the attacker plus one when n blocks have been discovered by the attacker or the honest miners since the start of the third phase. Then, $\mathbf{Z}_0 = z - j$ and $(\mathbf{Z}_n)_{n\in\mathbb{N}}$ is a biased simple random walk as before. The attack cycle ends when there is n such that $\mathbf{Z}_n = 0$ or $\mathbf{Z}_n = A+1$. Therefore, we have

$$\frac{\mathbb{E}[\mathbf{R}_A]}{b} = \sum_{j=z}^{\infty} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j](j+1+v) + \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j] \cdot \mathbb{P}[\nu_{0,A+1}^{z-j} = \nu_0^{z-j}]$$
$$\cdot (j+1+v+\mathbb{E}[\mathcal{L}(\nu_{0,A+1}^{z-j})|\nu_{0,A+1}^{z-j} = \nu_0^{z-j}])$$
$$= \mathbb{E}[[\mathbf{N}'((\mathbf{S}_z)] - \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j]j + P_A(z)(v+1)$$
$$+ \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j]j \cdot \mathbb{P}[\nu_{0,A+1}^{z-j} = \nu_0^{z-j}]$$
$$+ \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j] \cdot \mathbb{P}[\nu_{0,A+1}^{z-j} = \nu_0^{z-j}] \cdot \mathbb{E}[\mathcal{L}(\nu_{0,A+1}^{z-j})|\nu_{0,A+1}^{z-j} = \nu_0^{z-j}].$$

Now, we use again the classical relation for the Gambler's ruin formula $\mathbb{P}[\nu_{0,M}^m = \nu_0^m] = (\lambda^m - \lambda^M)/(1-\lambda^M)$ (see e.g. [5]) and

$$\mathbb{E}[\mathcal{L}(\nu_{0,M}^m)|\nu_{0,M}^m = \nu_0^m]) = \frac{m}{2} + \frac{m\lambda^m - (2M-m)\lambda^M + (2M-m)\lambda^{M+m} - m\lambda^{2M}}{2p(1-\lambda)(\lambda^m - \lambda^M)(1-\lambda^M)}$$

from [12] (See Corollary 2.5) which is a consequence of Stern's formula [20]. So, using Proposition 3.2, we compute

$$\begin{aligned}
\frac{\mathbb{E}[\mathbf{R}_A]}{b} &= \frac{qz}{p} + P_A(z)(v+1) \\
&- \left(\frac{(2(A+1)-z)\lambda^{A+1} + z\lambda^{2(A+1)}}{2p(1-\lambda)(1-\lambda^{A+1})^2} + \frac{\lambda^{A+1}}{1-\lambda^{A+1}} \cdot \frac{z}{2}\right) \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j] \\
&+ \left(\frac{z + (2(A+1)-z)\lambda^{A+1}}{2p(1-\lambda)(1-\lambda^{A+1})^2} + \frac{1}{1-\lambda^{A+1}} \cdot \frac{z}{2}\right) \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j]\lambda^{z-j} \\
&- \left(\frac{1}{1-\lambda^{A+1}} + \frac{\lambda^{A+1} - \lambda^{2(A+1)}}{2p(1-\lambda)(1-\lambda^{A+1})^2} - \frac{\lambda^{A+1}}{1-\lambda^{A+1}} \cdot \frac{1}{2}\right) \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j]j \\
&+ \left(\frac{1}{1-\lambda^{A+1}} - \frac{1-\lambda^{A+1}}{2p(1-\lambda)(1-\lambda^{A+1})^2} - \frac{1}{1-\lambda^{A+1}} \cdot \frac{1}{2}\right) \sum_{j=0}^{z-1} \mathbb{P}[\mathbf{N}'(\mathbf{S}_z) = j]j\lambda^{z-j}
\end{aligned}$$

and

$$\begin{aligned}
\frac{\mathbb{E}[\mathbf{R}_A]}{b} &= \frac{qz}{p} + P_A(z)(v+1) - \frac{\lambda^{A+1}(A+1-q(1-\lambda^{A+1})z)}{p(1-\lambda)(1-\lambda^{A+1})^2} I_p(z,z) \\
&+ \frac{(A+1)\lambda^{A+1} + p(1-\lambda^{A+1})z}{p(1-\lambda)(1-\lambda^{A+1})^2} I_q(z,z) \\
&- \frac{p-q+q\lambda^{A+1}}{p(1-\lambda)(1-\lambda^{A+1})} \left(\frac{qz}{p} I_p(z,z) - \frac{p^{z-1}q^z}{B(z,z)}\right) \\
&- \frac{\lambda}{(1-\lambda)(1-\lambda^{A+1})} \left(\frac{pz}{q} I_q(z,z) - \frac{q^{z-1}p^z}{B(z,z)}\right).
\end{aligned}$$

We note that

$$\frac{\lambda^{A+1}(A+1-q(1-\lambda^{A+1})z)}{p(1-\lambda)(1-\lambda^{A+1})^2} + \frac{p-q+q\lambda^{A+1}}{p(1-\lambda)(1-\lambda^{A+1})} \cdot \lambda z = \lambda z + \frac{(A+1)\lambda^{A+1}}{p(1-\lambda)(1-\lambda^{A+1})^2}.$$

So, using again (7) and (8), we get

$$\begin{aligned}
\frac{\mathbb{E}[\mathbf{R}_A]}{b} &= \left(\frac{1}{2}\lambda z + \frac{(A+1)\lambda^{A+1}}{p(1-\lambda)(1-\lambda^{A+1})^2}\right) I_{4pq}(z, \frac{1}{2}) + P_A(z)(v+1) \\
&- \frac{(A+1)\lambda^{A+1}}{p(1-\lambda)(1-\lambda^{A+1})^2} + \frac{2-\lambda+\lambda^{A+2}}{(1-\lambda)(1-\lambda^{A+1})} \frac{p^{z-1}q^z}{B(z,z)}.
\end{aligned}$$

■

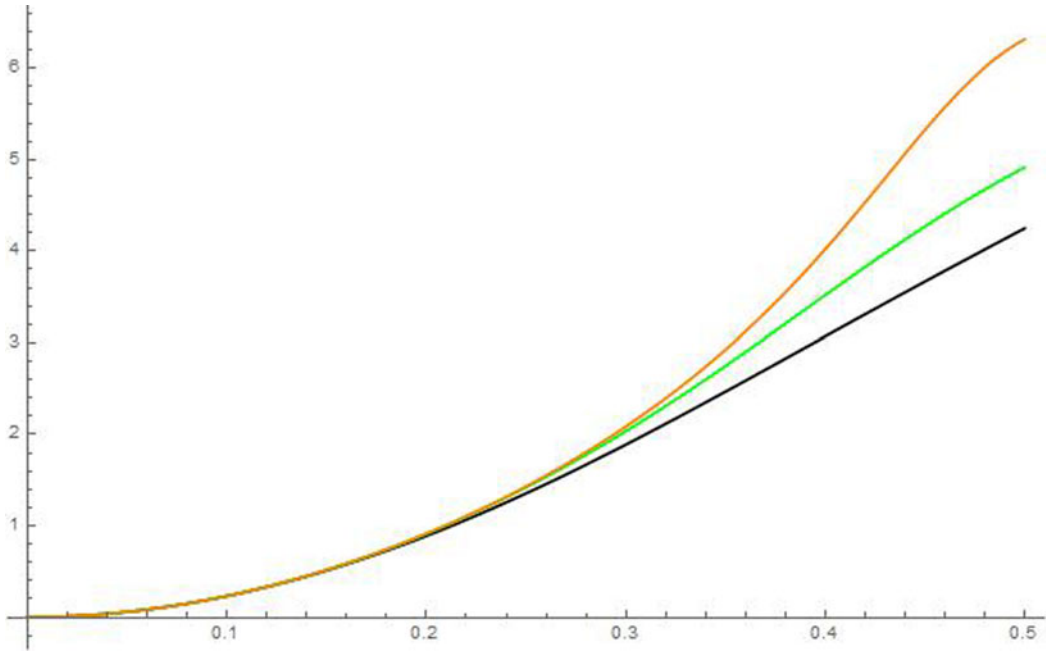

FIGURE **2.** Graph of $q \mapsto \mathbb{E}[\mathbf{R}_A]$ with $z = 2$ and $v = b$ for $A = 3, 5, 10$.

In Figures 2 and 3, we plot the graphs of $q \mapsto \mathbb{E}[\mathbf{R}_A]$ and $q \mapsto \Gamma_A$. In Figure 3, Γ_H is the dashed line. We have $\lim_{q \to 0.5} \Gamma_{10}(q) = \frac{139}{286} < \frac{1}{2}$ and $\Gamma_{10}(q) < q$ for any q. The $(10, 1)$-Nakamoto double-spend strategy with $z = 2$ and $v = b$ is always less profitable than honest mining.

5. RELATED WORK

In [18], the author proposes as a better approximation a correct formula for the computation of the probability of success of the Nakamoto double-spend attack, correcting the formula from [17]. A mathematical derivation later appears in [8]. This probability is computed in closed-form using special functions in [13]. As Corollary of this closed-form formula, it is proved in [13] that the probability decays exponentially to 0 with the number of confirmations $z \to +\infty$. This result was believed by the community on the basis of numerical evidence, but no mathematical proof was available. In [7], asymptotics at higher orders are computed by combinatorical methods (higher-order asymptotics are classical also from the integral expression in [13]). The authors also discuss the initial assumptions of the Nakamoto double-spend strategy. In fact, Section 11 of [17] contains several incoherences. All authors agree with Nakamoto that z is the number of confirmations, which assumes a 1 block premining (see [15,18] or [13]). In [19], the authors look for the best security protocol that a merchant should adopt to counter a double-spend attack. They consider attacks that are long enough to impact the difficulty adjustment parameter. They propose to merge double-spend attacks with selfish mining or other blocks witholding strategies (it is proven in [10] that these attacks are only profitable on the long run only after an adjustment of the difficulty parameter). These articles only study double-spend attacks from the point of view of the probability of success rather than from profitability. A first attempt, without

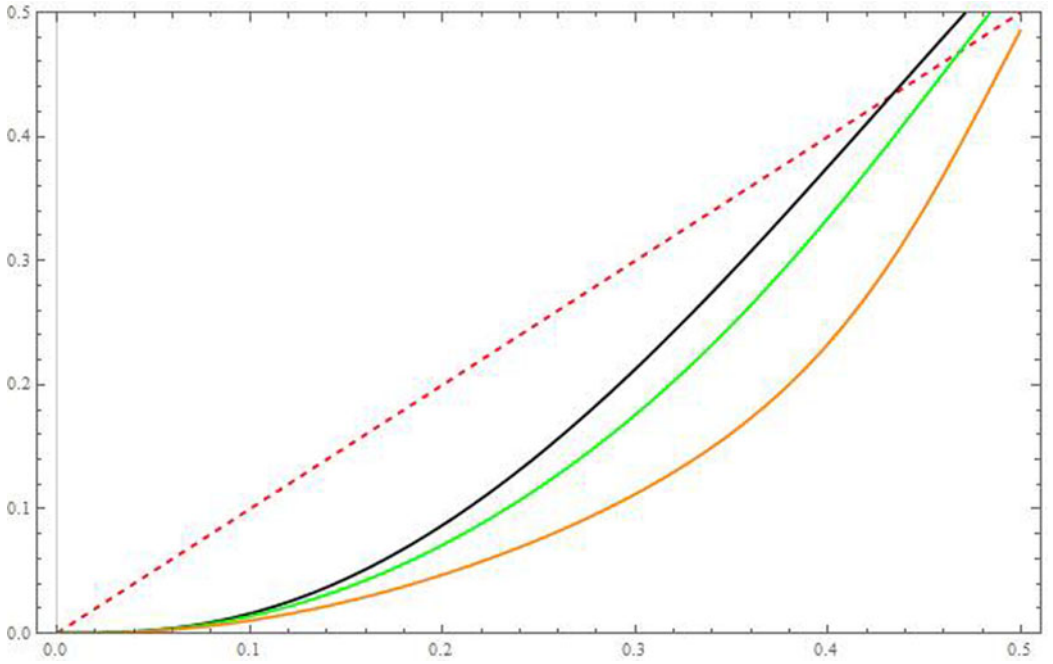

FIGURE **3.** Graph of $q \mapsto \Gamma_A$, $z = 2$, $v = b$ for $A = 3, 5, 10$.

a proper time modeling, to study the profitability of the attack can be found in the last section of [18] (where the A-Nakamoto strategy is numerically studied with $A = 20$). The duration time of the attack is studied in [9]. The author computes the conditional probability density function of the time before an attacker catches up the honest miner, knowing that the honest miners have already mined z blocks. A simplified expression can be found in [3]. In [15], the authors introduce a profitability setup and look for the optimal number of blocks that an attacker should premine before launching a double-spend attack (we will answer this question in a future article). In [2], the authors study the profitability of a double-spend attack with a cutoff time strategy, $S_{z+1} \wedge S'_{z+1}$ (in our notation). In [16], the authors consider a fixed cutoff time (in case of failure, the attack ends at a fixed time).

What was lacking before was a rigorous model of profitability to make exact comparisons of profitabilities of different mining strategies, in particular with the honest strategy. This ingredient is provided by Grunspan and Pérez-Marco [10] and it is what we use in the present article.

Acknowledgments

The authors are grateful for remarks and corrections of the referee that greatly improved the presentation.

References

1. Abramovitch, M. & Stegun, I.A. (1970). *Hanbook of mathematical functions*. New York: Dover.
2. Bissias, G., Levine, B.N., Ozisik, A.P., & Andresen, G. (2016). An analysis of attacks on blockchain consensus, arXiv:1610.07985.
3. Brown, M., Peköz, E., & Ross, S. (2020). Blockchain double-spend attack duration. *Probability in the Engineering and Informational Sciences*: 1–9. https://doi.org/10.1017/S0269964820000212
4. DLMF (2018). Digital library of mathematical functions. dlmf.nist.gov.

5. Feller, W. (1991). *An introduction to probability theory and its applications*, 2nd ed. Wiley.
6. Finney, H. (2011). Best practice for fast transaction acceptance - How high is the risk? Bitcointalk.org post. https://bitcointalk.org/index.php?topic=3441.msg48384#msg48384.
7. Georgiadis, E. & Zeilberger, D. (2019). A combinatorial-probabilistic analysis of Bitcoin attacks. *Journal of Difference Equations and Applications* 25: 56–63.
8. Göbel, J., Keeler, H.P., Krzesinski, A.E., & Taylor, P.G. (2016). Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay. *Performance Evaluation* 104: 23–41.
9. Goffard, P.-O. (2019). Fraud risk assessment within blockchain transactions. *Advances in Applied Probability* 51, 443–467.
10. Grunspan, C. & Pérez-Marco, R. (2018). On profitability of selfish mining, arXiv:1805.08281.
11. Grunspan, C. & Pérez-Marco, R. (2018). On profitability of stubborn mining, arXiv:1808.01041.
12. Grunspan, C. & Pérez-Marco, R. (2018). On profitability of trailing mining, arXiv:1811.09322.
13. Grunspan, C. & Pérez-Marco, R. (2018). Double spend races. *International Journal of Theoretical and Applied Finance* 21(08): 1850053.
14. Grunspan, C. & Pérez-Marco, R. (2020). The mathematics of Bitcoin. *Newsletter of the European Mathematical Society* 115: 31–37.
15. Hinz, J. & Taylor, P. (2017). A note on optimal double spending attacks. *MATRIX Annals* 2: 545–551.
16. Jang, J. & Lee, H-N. (2019). Profitable double-spending attacks, arXiv:1903.01711.
17. Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system, Bitcoin.org.
18. Rosenfeld, M. (2014). Analysis of hashrate-based double spending, arXiv:1402.2009v1.
19. Sompolinsky, Y. & Zohar, A. (2016). Bitcoin's security model revisited, arXiv:1605.09193.
20. Stern, F. (1975). Conditional expectation of the duration in the classical ruin problem. *Mathematics Magazine* 48(4): 200–203.

APPENDIX A. THE ORIGINAL NAKAMOTO DOUBLE-SPEND ATTACK IS UNSOUND

LEMMA A.1: *Let* $\mathbf{R}$ *be the revenue of a miner following the original Nakamoto's double-spend attack and* $\mathbf{T}$ *is the duration time of the attack. Then, we have* $\mathbb{E}[\mathbf{R}] < \infty$ *and* $\mathbb{E}[\mathbf{T}] = \infty$.

PROOF: Clearly, we have $\mathbb{E}[\mathbf{T}] = \infty$ since the event $\mathbf{T} < \infty$ means that the attack is succesful and the probability of success $P(z)$ of a double-spend attack is < 1 [13]. To prove $\mathbb{E}[\mathbf{R}] < \infty$, we model the progression of the blockchain by a simple biased random walk $\mathbf{X}$ on $\mathbb{Z}$ with $\mathbf{X}_0 = 0$. Each block validated by the honest miners (resp. attacker) corresponds to a step to the right (resp. left). So, $\mathbb{P}[\mathbf{X}_{i+1} = \mathbf{X}_i + 1] = p$ with $p = 1 - q > \frac{1}{2}$. We denote by $\mathcal{L}(n) = \sum_{i=1}^{n} \mathbf{1}_{\mathbf{X}_i = \mathbf{X}_{i-1} - 1}$, the number of blocks mined by the attacker after n blocks discovery. Similarly, $\mathcal{R}(n) = \sum_{i=1}^{n} \mathbf{1}_{\mathbf{X}_i = \mathbf{X}_{i-1} + 1}$ is the number of blocks mined by the honest miners. The exact delay in block of the attacker with the official blockchain (possibly negative) is $\mathbf{X} - 1$ since we assume a premined block.

If the attack is succesful, the attacker's revenue is made of the value v of the double spend and all the blocks he has mined including the premined block. In case of failure, we have $\mathbf{R} = 0$.

At the time, the honest miners have mined z blocks, the attacker has mined Z blocks where Z is a negative binomial law with parameter (p, z) [13]. For a biased random walk $\tilde{\mathbf{X}}$ such that at each step there is a probability p to move to the right and for $k \in \mathbb{Z}$, we consider the time to go below zero starting from k: $\nu_k = \mathrm{Inf}\{n \in \mathbb{N}\,;\, \tilde{\mathbf{X}}_n \leq 0 \,|\, \tilde{\mathbf{X}}_0 = k\}$. By conditioning at the time when the honest miners have mined z blocks and using the Markov property, we have (v is the double-spend amount):

$$\mathbb{E}[\mathbf{R}] = (v+1)P(z) + \sum_{k=z}^{\infty} \mathbb{P}[Z = k]k + \sum_{k=0}^{z-1} \mathbb{P}[Z = k](k + \mathbb{E}[\mathcal{L}(\nu_{z-k}) | \nu_{z-k} < \infty])\mathbb{P}[\nu_{z-k} < \infty]$$

$$\leq v + 1 + \mathbb{E}[Z] + \sum_{j=1}^{z} \mathbb{E}[\nu_j \,|\, \nu_j < \infty].$$

To conclude, we now use the facts that $\mathbb{E}[Z] < \infty$ and $\mathbb{E}[\nu_j | \nu_j < \infty] < \infty$. The last result is due to Stern [20]. ■