ON PROFITABILITY OF SELFISH MINING

CYRIL GRUNSPAN AND RICARDO PÉREZ-MARCO

Abstract. We review the so called selfish mining strategy in the Bitcoin network and properly evaluate the cost of the attack and its profitability. The expected duration of the attack has been ignored in the literature but is critical. We prove that such strategy can only be profitable after a difficulty adjustment. Therefore, it is an attack on the difficulty adjustment algorithm. We propose an improvement of Bitcoin protocol making it inmune to a selfish mining attack.

1. Introduction

The stability of Bitcoin protocol [7] relies on rules aligned with self-interest of participants in the network. One of its basic rules is that miners make public blocks as soon as they are validated. "Selfish Mining" is a deviant mining strategy described in [5] where a major mining operator withholds mined blocks and releases them with a well timed strategy in order to invalidate the maximum number of blocks mined by the rest of the network. The authors of [5] make the unfounded claim that the selfish mining strategy breaks the Bitcoin protocol [4] which has not been observed in practice.

Other researchers have proposed other selfish mining strategies which are supposed to be "optimal" [9]. The selfish mining strategy is presented in courses and textbooks on Bitcoin such as [2] (in chapter 5 under the name "Temporary Block-Withholding Attack") or [10].

All these articles do not make a proper analysis of the costs of the attack, and, more critically, do ignore time considerations. More precisely, the Markov model used in these papers is flawed by inception since it does not incorporate an analysis of the time duration of the attack. The main goal of this article is to carry out a proper analysis of profitability that is lacking in the literature. It turns out that without difficulty adjustments the strategy is unsound.

2010 *Mathematics Subject Classification.* 68M01, 60G40, 91A60.
Key words and phrases. Bitcoin, blockchain, selfish mining, proof-of-work.

2. Selfish mining strategy.

We describe the selfish mining strategy presented in [5]. The selfish miner attack starts by validating and not broadcasting a block, then continuing mining secretly on top of this block. Then he proceeds as follows:

(1) If the advance of the selfish miner is only equal to 1 block and the honest miners discover a block then the selfish miner broadcasts immediately the block he has mined secretly. A competition then follows. The selfish miner is assumed to be sufficiently well connected with the rest of the network so that a fraction $0 \leq \gamma \leq 1$ of the honest network accepts his block proposal and starts mining on top of it.

(2) If the advance of the selfish miner is 2 blocks and the honest miners discover a block, then the selfish miner broadcasts immediately the two blocks he had mined secretly. Then, the whole network switches to his fork.

(3) If the advance of the selfish miner is greater than 2, then the selfish miner releases a block as soon as the honest miners discovers one.

(4) In other cases, the selfish miner keeps on mining secretly on top of his fork.

Note that if the advance of the miner is greater than 2, then at some point the advance of the selfish miner will be equal to 2 (because we assume that his hashrate is less than 50%, otherwise other more efficient attacks are possible) and then, according to the second point, the whole network ends up adopting the fork proposed by the selfish miner. Therefore, the blocks made public by the selfish miner when his advance is greater than 2 always end up being accepted by the network.

In [5] it is assumed that the fraction γ stays always constant. This is not accurate since γ depends on the timing of the discovery of a new block mined by the network, and therefore cannot be constant. But it is necessary to assume it constant for the sake of the Markov chain model presented in [5] and these authors made such assumption. The analysis of the necessary capital to reach a stable regime is not done. But, more importantly, the cost of deviating from the Bitcoin protocol are not properly accounted. This is fundamental in order to compute the profitability of such a rogue strategy. The time analysis is also critical to estimate the profitability and is ignored.

3. Profitability of selfish vs. honest mining.

3.1. **Profitability in the literature.** Most of the articles on selfish mining strategies fail to consider, explicitely or implicitely, the cost of mining. In particular this is flatly ignored in [5]. In other articles like [3] we can read surprising statements as:

> ***Costs.*** *There is a configurable parameter c_m for every miner m that denotes the cost (i.e. in electricity) for miner m to mine. For our simulations, we always set $c_m = 0$ because we aren't looking at this aspect of mining.*

Obviously if mining blocks was without any energy cost, anyone could try to reverse the history of bitcoin transactions and try double spend attacks, and there will be no economic incentive to respect the Bitcoin protocol. The cost of energy is what makes expensive to falsify the blockchain, and this is at the base of Bitcoin security.

Other authors, like in [1], present Selfish Mining in these terms:

"This [Selfish Mining] does reduce the attacker's revenue in the short term, but it reduces everyone else's revenue even more, so neutral nodes now have the incentive to join the attacker's coalition to increase their own revenue. Eventually, the attacker's coalition would expand to above 50% in size, potentially giving the attacker a high degree of control over the network."

In other words, according to this interpretation, a miner who looses money would be attracted to join another miner who also looses money. And this only because the attacker miner persuades the honest miner that he is loosing less money (!). Aside from the fact that the honest miners will be unable to know for sure the difference of profitability, this naive scenario is very implausible.

From this point of view, selfish mining is justified only as a preparation of a 51% attack to take control of the network. A more likely outcome, is that the honest pools noticing someone selfish mining, will employ the obvious defensive strategy and start to selfish mining themselves making the network stall. This outcome will be highly non profitable for everyone. A form of Nash equilibrium is at play that avoids the described scenario.

Aside from these creative interpretations, what is really laking in the literature is a proper accounting and understanding of the cost of selfish mining attack, with a proper time analysis.

3.2. **Cost of mining.** The key idea in order to evaluate properly the profitability of selfish mining is to compare it to the profitability of honest mining. We assume that miners are in the mining business because the operating cost (equipment, energy power, salaries, etc) are compensated by the block reward of newly generated bitcoins plus transaction fees[1]. Therefore the cost of mining per unit time is independent of the strategy if the hashrate is operate at full capacity. So we have $C_S = C_H$ where C_S, resp. C_H, is the cost of mining per unit time for the selfish, resp. honest, mining strategy. We denote $C_0 = C_S = C_H$. Note that this cost is not only independent of the strategy but also of the block mined being accepted or not by the network.

3.3. **Profit and Loss.** Our goal is to evaluate the profit and loss (PnL) and compare the PnL of selfish mining and honest mining. Profit and loss is the revenue R minus the costs C,

$$PnL = R - C \ .$$

We take a conservative, but sufficient, setup where block rewards are reduced to the bounty $b > 0$ of newly generated bitcoins (thus we don't consider transactions fees, and maybe double spend attempts that may increase the profitability). Unless otherwise stated, we assume that we are not near a halving, so that the reward b stays constant.

What is important, for any business, is the PnL per unit of time, and not the PnL per block solved or accepted by the network. It is worth noting that PnL per block or per unit of time are not equivalent since the strategy employed does delay the speed of validation of blocks in the network.

3.4. **Profit and Loss per unit of time.** A non-stop attack strategy, as selfish mining, consists in a consecutive sequence of "attack cycles".

In the case of selfish mining it starts when both selfish miners and honest miners are working on top of the same public blockchain. The selfish miners aim to getn an advance of their secretly mined blockchain. If, at the beginning, the honest miners find the new block, then a new cycle starts. If the selfish miners succeed in building an advantage, then the cycles lasts until the honest miners catch-up and force the selfish miners to releases all of their secretly mined blocks. Then a new cycle starts.

For this type of strategies of games with repetition, the asymptotic PnL per unit of time, $PnLt_\infty$, can be evaluated. This is the content of the following Theorem.

[1]There may be other non-economic incentives, as transforming non-internationally circulating currency into bitcoins, that we cannot consider.

Theorem 3.1 (Profitability of an attack)**.** *Let R, C and T be the random variables corresponding respectively to the revenue, cost and duration of a cycle for a repetition strategy. We assume these random variables to be integrable. Then in the long run the PnL per unit of time of the repeated strategy is*

$$PnLt_\infty = \frac{\mathbb{E}[R] - \mathbb{E}[C]}{\mathbb{E}[T]} \ .$$

We call $PnLt_\infty$ the profitability of the strategy.

Proof. Let R_i, C_i and T_i, be the corresponding values for the i-cycle. The (R_i) (resp. (C_i), (T_i)) are i.i.d. random variables. The PnL_n after n-cycles is given by

$$PnL_n = \frac{\sum_{i=1}^n R_i - \sum_{i=1}^n C_i}{\sum_{i=1}^n T_i} = \frac{\frac{1}{n}\sum_{i=1}^n R_i - \frac{1}{n}\sum_{i=1}^n C_i}{\frac{1}{n}\sum_{i=1}^n T_i} \ .$$

By the strong law of large numbers [8] we have that almost surely

$$\lim_{n\to+\infty} PnL_n = \frac{\mathbb{E}[R] - \mathbb{E}[C]}{\mathbb{E}[T]} \ .$$

□

We consider integrable games with random variables R, C, and T are all integrable.

Definition 3.2 (Integrable games)**.** *A game or strategy is integrable when R, C, and T are integrable. An integrable game or strategy has constant cost if the cost per unit time is a constant C_0, then*

$$\mathbb{E}[C] = C_0 \mathbb{E}[T] \ .$$

We will see below that the selfish mining strategy is integrable and has constant cost. We have:

Corollary 3.3. *For an integrable constant cost strategy we have*

$$PnL_\infty = \frac{\mathbb{E}[R]}{\mathbb{E}[T]} - C_0 \ .$$

Therefore, in order to compare two integrable constant cost strategies we only need to compare $\frac{\mathbb{E}[R]}{\mathbb{E}[T]}$.

Definition 3.4. *The revenue ratio of a strategy ξ is defined as*

$$P(\xi) = \frac{\mathbb{E}[R]}{\mathbb{E}[T]} \ .$$

The revenue ratio is the benchmark for profitability of integrable constant cost strategies, more precisely, strategy ξ is more profitable than strategy ξ' if and only if

$$P(\xi') \leq P(\xi) \ .$$

In the article [5] the authors only consider a "relative revenue". This is a non-standard notion in accountability that they define as the ratio

$$\frac{\mathbb{E}[R_S]}{\mathbb{E}[R_S] + \mathbb{E}[R_N]}$$

where R_S and R_N are the revenues of the selfish miners and the rest of the network. The effect of the selfish mining strategy is to reduce both $\mathbb{E}[R_S]$ and $\mathbb{E}[R_N]$, and to increase this relative revenue on certain conditions on q and γ. Obviously, increasing the relative revenue at the cost of reducing its own revenue is not a sound strategy. Also discussing profitability via a Markov model without time duration consideration of the strategy is unsound. The time dynamics is absent in the Markov model, and cannot take account situations where the expected time of some attack cycles may take much longer which will impact the $PnLt$.

4. Mining strategies.

Let us fix some notations. The reward per block is $b > 0$. We have two sets of miners (for example, honest miners and attacking miners for an attack). The progression of blocks are described by two independent Poisson processes N and N' respectively, with parameter α, resp. α'. Interblock valdation times are denoted by (T_i) for the honest miners and (T'_i) for the selfish miner. We denote for $n \geq 1$

$$\begin{aligned} S_n &= T_1 + T_2 + \ldots + T_n \ , \\ S'_n &= T'_1 + T'_2 + \ldots + T'_n \ . \end{aligned}$$

We recall (see [6]) that the random variables (T_i) (resp. (T'_i)) follow an exponential density with parameter α (resp. α') and the random variable S_n (resp. S'_n) follows a gamma density distribution with parameter (n, α) (resp. (n, α')). We denote

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

We have $p+q=1$ and if $\alpha' < \alpha$ then $0 < q < 1/2 < p < 1$ (and $\tau_0 = 10$ min for the Bitcoin network in normal conditions). The quantities p and q represent relative hashrates, and also probabilities of finding the next block by each group of miners as the following elementary computations show [8]:

Lemma 4.1. *We have*

$$\begin{aligned} \mathbb{P}[T_1 < T_1'] &= p \ , \\ \mathbb{P}[T_1' < T_1] &= q \ , \\ \mathbb{P}[T_1' < T_1 < S_2'] &= pq \ , \\ \mathbb{E}[T_1 \wedge T_1'] &= \tau_0 \ . \end{aligned}$$

4.1. **Honest strategy.** The cycle for the honest strategy last until a block is found. So the stopping time for the honest strategy is

$$\tau_H = T_1' \wedge T_1 \ .$$

We have $\mathbb{E}[\tau_H] = \tau_0$.

The reward in a cycle is 0 or b depending who is the miner, thus

$$\mathbb{E}[R(\tau_H)] = p \cdot 0 + q \cdot b = qb \ ,$$

and we have,

Theorem 4.2. *We have that τ_H and $R(\tau_H)$ are integrable and*

$$\begin{aligned} \mathbb{E}[R(\tau_H)] &= qb \ , \\ \mathbb{E}[\tau_H] &= \tau_0 \ . \end{aligned}$$

Therefore,

$$P(H) = \frac{\mathbb{E}[R(\tau_H)]}{\mathbb{E}[\tau_H]} = \frac{qb}{\tau_0} \ .$$

4.2. **Selfish mining strategy.** We consider now the selfish mining strategy as described in Section 2. We assume that the hashrate of the attackers is less than that of the honest miners (i.e. $\alpha' < \alpha$). We denote by $\tau_{SM,\gamma}$ the duration time of an attack cycle.

Lemma 4.3. *We have*

$$\tau_{SM,\gamma} = \inf\{t \geq T_1; N(t) = N'(t) - 1 + 2 \cdot \mathbf{1}_{T_1 < T_1'} + 2 \cdot \mathbf{1}_{T_1' < T_1 < S_2 < S_2'}\} \ ,$$

and the stopping time $\tau_{SM,\gamma}$ is finite almost surely.

Proof. Note that if $T_1 < T_1'$, then $\tau_{SM,\gamma} = T_1$. If $T_1' < T_1 < S_2 < S_2'$ then $\tau_{SM,\gamma} = S_2$. If $T_1' < T_1 < S_2' < S_2$ then $\tau_{SM,\gamma} = S_2'$. Otherwise we have $S_2' \leq T_1$ and $N(T_1) = 1 \leq N'(T_1) - 1$, and in that case $\tau_{SM,\gamma} = \inf\{t \geq T_1; N(t) = N'(t) - 1\}$ exists and is finite almost surely since $\alpha' < \alpha$. $\square$

Theorem 4.4. *We have that $\tau_{SM,\gamma}$ and $R(\tau_{SM,\gamma})$ are integrable, and*

$$\mathbb{E}[R(\tau_{SM,\gamma})] = \frac{(1+pq)(p-q)+pq}{p-q}\, qb - (1-\gamma)p^2 q\, b \ ,$$
$$\mathbb{E}[\tau_{SM,\gamma}] = \frac{(1+pq)(p-q)+pq}{p-q}\, \tau_0 \ .$$

Therefore,

$$P(SM,\gamma) = \frac{\mathbb{E}[R(\tau_{SM,\gamma})]}{\mathbb{E}[\tau_{SM,\gamma}]} = \frac{qb}{\tau_0} - (1-\gamma)\frac{p^2 q(p-q)b}{((1+pq)(p-q)+pq)\,\tau_0} \ .$$

Corollary 4.5. *For $\gamma < 1$, we have that*

$$P(SM,\gamma) = \frac{\mathbb{E}[R(\tau_{SM,\gamma})]}{\mathbb{E}[\tau_{SM,\gamma}]} < \frac{qb}{\tau_0} = P(H) \ ,$$

so, the Selfish Mining strategy with $\gamma < 1$ is strictly less profitable than the honest strategy.

Proof of the Theorem. For any $t_0 \in \mathbb{R}$, the stopping time $\tau_{SM,\gamma} \wedge t_0$ is bounded. Moreover, the compensated Poisson process $N(t) - \alpha t$ (resp. $N'(t) - \alpha' t$) is a well known martingale. So, using Doob's theorem [8], we have:

$$\begin{aligned}
&\alpha'\mathbb{E}[\tau_{SM,\gamma} \wedge t_0] = \mathbb{E}[N'(\tau_{SM,\gamma} \wedge t_0)] \\
&= \mathbb{E}[N'(\tau_{SM,\gamma} \wedge t_0)|\tau_{SM,\gamma} < t_0] \cdot \mathbb{P}[\tau_{SM,\gamma} < t_0] + \mathbb{E}[N'(\tau_{SM,\gamma} \wedge t_0)|\tau_{SM,\gamma} > t_0] \cdot \mathbb{P}[\tau_{SM,\gamma} > t_0] \\
&= \mathbb{E}[N'(\tau_{SM,\gamma})|\tau_{SM,\gamma} < t_0] \cdot \mathbb{P}[\tau_{SM,\gamma} < t_0] + \mathbb{E}[N'(t_0)|\tau_{SM,\gamma} > t_0] \cdot \mathbb{P}[\tau_{SM,\gamma} > t_0] \\
&= \mathbb{E}[N(\tau_{SM,\gamma}) + 1 - 2(\mathbf{1}_{T_1 < T_1'} + \mathbf{1}_{S_1' < S_1 < S_2 < S_2'})|\tau_{SM,\gamma} < t_0] \cdot \mathbb{P}[\tau_{SM,\gamma} < t_0] \\
&\quad + \mathbb{E}[N'(t_0)] \cdot \mathbb{P}[\tau_{SM,\gamma} > t_0] \\
&= \mathbb{E}[N(\tau_{SM,\gamma})|\tau_{SM,\gamma} < t_0] \cdot \mathbb{P}[\tau_{SM,\gamma} < t_0] + \mathbb{P}[\tau_{SM,\gamma} < t_0] \\
&\quad + \mathbb{E}[N'(t_0)] \cdot \mathbb{P}[\tau_{SM,\gamma} > t_0] - 2 \cdot \mathbb{E}[\mathbf{1}_{T_1 < T_1'} + \mathbf{1}_{S_1' < S_1 < S_2 < S_2'}|\tau_{SM,\gamma} < t_0] \cdot \mathbb{P}[\tau_{SM,\gamma} < t_0] \\
&= \mathbb{E}[N(\tau_{SM,\gamma} \wedge t_0)] - \mathbb{E}[N(\tau_{SM,\gamma} \wedge t_0)|\tau_{SM,\gamma} > t_0] \cdot \mathbb{P}[\tau_{SM,\gamma} > t_0] + \mathbb{P}[\tau_{SM,\gamma} < t_0] \\
&\quad - 2 \cdot \mathbb{E}[\mathbf{1}_{T_1 < T_1'} + \mathbf{1}_{S_1' < S_1 < S_2 < S_2'}|\tau_{SM,\gamma} < t_0] \cdot \mathbb{P}[\tau_{SM,\gamma} < t_0] + \alpha' t_0 \cdot \mathbb{P}[\tau_{SM,\gamma} > t_0] \\
&= \alpha\mathbb{E}[\tau_{SM,\gamma} \wedge t_0] - \mathbb{E}[N(t_0)] \cdot \mathbb{P}[\tau_{SM,\gamma} > t_0] + \mathbb{P}[\tau_{SM,\gamma} < t_0] \\
&\quad - 2 \cdot \mathbb{E}[(\mathbf{1}_{T_1 < T_1'} + \mathbf{1}_{S_1' < S_1 < S_2 < S_2'}) \cdot \mathbf{1}_{\tau_{SM,\gamma} < t_0}] + \alpha' t_0 \cdot \mathbb{P}[\tau_{SM,\gamma} > t_0]
\end{aligned}$$

and,

$$
\begin{aligned}
(\alpha'-\alpha)\mathbb{E}[\tau_{SM,\gamma}\mathbf{1}_{\tau_{SM,\gamma}>t_0}] &= (\alpha'-\alpha)\mathbb{E}[\tau_{SM,\gamma}\wedge t_0] - (\alpha'-\alpha)t_0\cdot\mathbb{P}[\tau_{SM,\gamma}>t_0] \\
&= \mathbb{P}[\tau_{SM,\gamma}<t_0] - 2\cdot\mathbb{E}[(\mathbf{1}_{T_1<T_1'}+\mathbf{1}_{S_1'<S_1<S_2<S_2'})\cdot\mathbf{1}_{\tau_{SM,\gamma}<t_0}]
\end{aligned}
$$

The monotone convergence theorem implies that $\mathbb{E}[\tau_{SM,\gamma}]$ if finite and

$$
\begin{aligned}
(\alpha'-\alpha)\mathbb{E}[\tau_{SM,\gamma}] &= 1-2\cdot\mathbb{E}[(\mathbf{1}_{T_1<T_1'}+\mathbf{1}_{S_1'<S_1<S_2<S_2'})] \\
&= 1-2(p+p^2q)
\end{aligned}
$$

This gives

$$
\mathbb{E}[\tau_{SM,\gamma}] = \frac{(1+pq)(p-q)+pq}{p-q}\,\tau_0\ .
$$

Also we have

$$
\begin{aligned}
\mathbb{E}[N'(\tau_{SM,\gamma})\cdot\mathbf{1}_{\tau_{SM,\gamma}<t_0}] &= \mathbb{E}[N'(\tau_{SM,\gamma})|\tau_{SM,\gamma}<t_0]\cdot\mathbb{P}[\tau_{SM,\gamma}<t_0] \\
&= \mathbb{E}[N'(\tau_{SM,\gamma}\wedge t_0)] - \mathbb{E}[N'(\tau_{SM,\gamma}\wedge t_0)|\tau_{SM,\gamma}>t_0]\cdot\mathbb{P}[\tau_{SM,\gamma}>t_0] \\
&= \alpha'\mathbb{E}[\tau_{SM,\gamma}\wedge t_0] - \mathbb{E}[N'(t_0)]\cdot\mathbb{P}[\tau_{SM,\gamma}>t_0] \\
&= \alpha'\mathbb{E}[\tau_{SM,\gamma}\wedge t_0] - \alpha' t_0\cdot\mathbb{P}[\tau_{SM,\gamma}>t_0] \\
&= \alpha'\mathbb{E}[\tau_{SM,\gamma}\cdot\mathbf{1}_{\tau_{SM,\gamma}<t_0}]
\end{aligned}
$$

So, by the monotone convergence theorem again, we get $\mathbb{E}[N'(\tau_{SM,\gamma})] = \alpha'\mathbb{E}[\tau_{SM,\gamma}]$. In the same way, $\mathbb{E}[N(\tau_{SM,\gamma})] = \alpha\mathbb{E}[\tau_{SM,\gamma}]$.

Finally, we observe that at the end of an attack cycle, the selfish miner has no orphan block unless $T_1' < T_1 < S_2 < S_2'$ and the second block of the honest miners is found by a fraction $1-\gamma$ of all honest miners. This event occurs with a probability $p^2q(1-\gamma)$ and, in this case the selfish, miner has exactly one orphan block. Therefore, we have

$$
\begin{aligned}
\mathbb{E}[R(\tau_{SM,\gamma})] &= \mathbb{E}\left[N'\left(\tau_{SM,\gamma}\right)\right]b - p^2q(1-\gamma)b \\
&= \alpha'\mathbb{E}[\tau_{SM,\gamma}]b - p^2q(1-\gamma)b
\end{aligned}
$$

and we get

$$
\mathbb{E}[R(\tau_{SM,\gamma})] = \frac{(1+pq)(p-q)+pq}{p-q}\,qb - (1-\gamma)p^2q\,b\ .
$$

$\square$

Remark 1. The introduction of t_0 in the above proof is a technical point so that we can use Doob's stopping time theorem.

4.3. **Poisson games.** Theorem 4.4 is a variation of the following result.

Theorem 4.6 (Poisson games)**.** *Let N_1 and N_2 be two independent Poisson processes with parameters α_1 and α_2 with $\alpha_1 < \alpha_2$ and $N_1(0) = N_2(0) = 0$. Then, the stopping time*

$$\tau = \inf\{t > 0; N_1(t) = N_2(t) + 1\}$$

is finite a.s. and integrable. Moreover, we have $\mathbb{E}[\tau] = \frac{1}{\alpha_1 - \alpha_2}$, $\mathbb{E}[N_1(\tau)] = \frac{\alpha_1}{\alpha_1 - \alpha_2}$, $\mathbb{E}[N_2(\tau)] = \frac{\alpha_2}{\alpha_1 - \alpha_2}$.

4.4. **Apparent hashrate.** As discussed before, the good notion for accounting is the revenue of the miner by unit of time. However, we can also compute the revenue of the miner by unit of block. We compute the proportion q' of blocks mined by the selfish miner in the official blockchain. This represents the apparent hashrate of the selfish miner.

Proposition 4.7. *We have $q' = \frac{((1+pq)(p-q)+pq)q-(1-\gamma)p^2q(p-q)}{p^2q+p-q}$*

Proof. In all cases we observe that after one cycle of attack, the number of official blocks mined is always $\frac{N(\tau_{SM,\gamma})+N'(\tau_{SM,\gamma})+1}{2}$. So, by the proof of Theorem 4.4, we get

$$\mathbb{E}\left[\frac{N(\tau_{SM,\gamma}) + N'(\tau_{SM,\gamma}) + 1}{2}\right] = 1 + \frac{p^2q}{p-q} \ .$$

Hence, to get n validated blocks in the official blockchain, the selfish miner needs to repeat his attack X_n times with

$$\mathbb{E}[X_n] = \frac{n}{1 + \frac{p^2q}{p-q}} \ . \tag{1}$$

Therefore the average number of blocks mined by the selfish miner in a sequence of n blocks is (we take $n \leq 2016$ to avoid a difficulty adjustment)

$$\begin{aligned} q' &= \frac{\mathbb{E}[X_n]}{n} \cdot \frac{\mathbb{E}[R(\tau_{SM,\gamma})]}{b} \\ &= \frac{((1+pq)(p-q)+pq)q - (1-\gamma)p^2q(p-q)}{p^2q+p-q} \end{aligned}$$

□

We can rearrange this expression to get formula (8) for R_{pool} from [5],

$$q' = \frac{q(1-q)^2(4q+\gamma(1-2q)) - q^3}{1-q(1+q(2-q))} \ .$$

5. Selfish mining and difficulty adjustment

We examine now the impact of a difficulty's adjustment on the selfish mining strategy. After $n_0 = 2016$ blocks have been validated, the protocol modifies the speed of mining α and α' by a factor $\delta = \frac{\tilde{S}_{n_0}}{n_0 t_0}$ where $\tilde{S}_{n_0}$ is the time needed by the network to validate the sequence of n_0 blocks and $t_0 = 10$ min.

Proposition 5.1. *In presence of a single selfish miner with relative hashrate q, after the validation by the network of n_0 blocks, the parameter δ updating the difficulty's adjustment satisfies*

$$\mathbb{E}[\delta] = \frac{p - q + pq(p-q) + pq}{p^2 q + p - q} \ .$$

Proof. Before the difficulty adjustment we have $\frac{1}{\alpha+\alpha'} = t_0$. So, by (1) and Theorem 4.4 with $n_0 = 2016$, we have,

$$\begin{aligned}
\mathbb{E}[\tilde{S}_{n_0}] &= \mathbb{E}[X_{n_0}] \cdot \mathbb{E}[\tau_{SM,\gamma}] \\
&= \frac{p - q + pq(p-q) + pq}{p^2 q + p - q} \cdot n_0 t_0
\end{aligned}$$

□

We prove now that after a difficulty adjustment, the apparent hashrate and the profitability ratio coincide.

Theorem 5.2. *After a difficulty adjustment, the profitability ratio of the selfish miner is $P(SM,\gamma) = \frac{q'b}{t_0}$*

Proof. Before a difficulty adjustment, the speeds of validation α and α' were $\alpha = \frac{p}{t_0}$ and $\alpha' = \frac{q}{t_0}$. After a difficulty adjustment these quantities are both multiplied by a factor δ. So, the profitability ratio $P(SM,\gamma)$ is also multiplied by δ. Therefore, by Theorem 4.4 and Proposition 5.1, we get

$$P(SM,\gamma) = \left(qb - (1-\gamma)\frac{p^2 q(p-q)b}{(1+pq)(p-q)+pq}\right) \cdot \frac{p - q + pq(p-q) + pq}{p^2 q + p - q} \cdot \frac{b}{t_0}$$

After arranging this expression, we get $P(SM,\gamma) = \frac{q'b}{t_0}$. □

Corollary 5.3. *After a period of difficulty adjustment, the selfish mining strategy becomes more profitable than staying honest if* $\gamma > \frac{p-2q}{p-q} = \frac{1-3q}{1-2q}$.

Proof. The selfish mining strategy outperforms the strategy of "staying honest forever" if $P(SM,\gamma) > \frac{qb}{t_0}$. The condition is equivalent to $q' > q$. Hence we get the result by Proposition 4.7. □

This condition is also equivalent to the condition $q > \frac{1-\gamma}{3-2\gamma}$ from [5]. Note, and this point is crucial, that after a first period of difficulty's adjustment, the difficulty remains constant on average. So, the selfish mining strategy becomes more profitable than the honest strategy if the hashrates of the miners stay the same.

6. A proposition to prevent selfish mining

6.1. **The origin of the problem.** Basically, the atttack exploits the difficulty adjustment law. The protocol underestimates the real hashing power in the network since only the blocks that are in the (official) blockchain are taken into account. The number of orphan blocks grows in the presence of a selfish miner and a significant amount of honest hashrate is lost. The average time used by the network to validate blocks increases. After 2016 blocks, a difficulty adjustment is done automatically ignoring the production of orphan blocks. Despite the fact that the total hashing power of the network remains the same, the new difficulty is lower than it should be, and the block validation time decreases. So the revenue per unit of time of the selfish miner improves and makes the attack profitable.

6.2. **A new difficulty adjustment formula.** To mitigate this attack, the idea is to incorporate the count of orphan blocks in the difficulty adjustment formula. This can be implemented with miners indicating the presence of "uncles' in the blocks they mine by including their header and peers relaying this data. Nodes would not need to broadcast whole orphan blocks but only their headers. It is possible to incentive miners to include proofs of existence of uncles in their blocks by including a rule that, in case of competition between two blocks with the same height, nodes should always broadcast **the block with the most proof-of-work** i.e., the block which includes the most proofs of existence of "uncles". According to [11], this rule would also be profitable to honest miners in case of blocks competition with selfish miners. At the end of a period of $n_0 = 2016$ blocks validated by the network, the new formula of difficulty adjustment would be

$$D_{\text{new}} = D_{\text{old}} \cdot \frac{(n_0 + n')\tau_0}{S_{n_0}} \tag{2}$$

where n' is the total number of orphan blocks mined during this period of time and S_{n_0} is the time used by the network to validate the n_0 blocks (and evaluated with the formula $S_{n_0} = T_{n_0} - T_1$ where T_i denotes the timestamp in the header of block i).

6.3. **Analysis of the formula.** Let ω be the average number of orphan blocks observed during a period of $\tau_0 = 600$ sec. So, on average, every τ_0, there are ω orphan blocks and $(1-\omega)$ non-orphan blocks. Only the last ones will add to the official blockchain. The time used by the network to grow the blockchain by $n_0 = 2016$ blocks is then $S_{n_0} = \frac{n_0 \tau_0}{1-\omega}$. During this interval, we observe $n' = \frac{n_0 \omega}{1-\omega}$ orphan blocks. Thus we have $\frac{(n_0+n')\tau_0}{S_{n_0}} = 1$ and Formula (2) cannot lead to a fall of difficulty.

7. Conclusion

Selfish mining is a trick that slows down the network and reduces the mining difficulty. The attack diminishes the profitability of honest miners and the one of selfish miners before a difficulty adjustment. Selfish mining only becomes profitable after lowering the difficulty. Another way to achieve that would be to withdraw from the network and start mining another cryptocurrency with the same hashing function. The existence of other cryptocurrenies with the same validation algorithm that allows to switch mining without cost is a vector of attack in itself. When the attacker withdraws and comes back the mining difficulty will increase again after 2016 blocks unless the miner executes a selfish mining strategy. Then after a first difficulty's adjustment, the difficulty mining will stay constant on average.

Selfish mining is an attack on the Bitcoin protocol, but the arguments present in the literature do not properly justify the attack. They lack of a correct evaluation of the cost of the attack and a proper analysis of profit and loss per unit of time. To compare the profitability of different mining strategies one needs to compute the average length of their cycles and their profitability ratio, that is a new notion introduced in this article.

The attack exploits a flaw in the difficulty adjustment formula. The parameter used to update the mining difficulty is supposed to measure the actual hashing power of the network. In the presence of a selfish miner, this is no longer true.

We have proposed a formula that corrects this anomaly by taking into account the production of orphan blocks. We propose to reinforce the protocol which states that the official blockchain is the chain which contains the most proof-of-work by requiring peers to give priority to those containing the most proof-of-work (with "uncles").

The proposed formula, if adopted, would not eliminate the possibility of selfish mining but it would make it non-profitable compared to honest mining even after a difficulty adjustment. So this will keep the individual incentives properly aligned in the protocol rules, as intended in the original inception of Bitcoin [7].

References

[1] V. Buterin. *Selfish mining: a 25% attack against the bitcoin network*, bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440, 2013.
[2] J. Bonneau, E. Felten, S. Goldfeder, A. Miller , A. Narayanan. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press, NJ, USA, 2016.
[3] M. Carlsten, H. Kalodner, A. Narayanan , S. M. Weinberg.*On the instability of bitcoin without the block reward*, Proc. ACM SIGSAC Conf. Comp. and Comm. Sec., p.154-167, NY, 2016.
[4] I. Eyal, E. G. Sirer.*Bitcoin is broken*, hackingdistributed.com/2013/11/04/bitcoin-is-broken/ (accessed 1/2018), 2013.
[5] I. Eyal, E. G. Sirer.*Majority is not enough: bitcoin mining is vulnerable*, Int. Conf. Financial Cryptography and Data Security, Springer, p.436-454, 2014.
[6] C. Grunspan and R. Pérez-Marco. *Double spend races. ArXiv:1702.02867*, 2017.
[7] S. Nakamoto. *Bitcoin: a peer-to-peer electronic cash system. Bitcoin.org*, 2008.
[8] S. Ross. *Introduction to Probability Models 10th Edition.* Academic Press Inc, 2012
[9] A. Sapirshtein, Y. Sompolinsky , A. Zohar, *Optimal selfish mining strategies in bitcoin*, International Conference on Financial Cryptography and Data Security, Springer, p.515-532, 2016.
[10] R. Wattenhofer. *Distributed Ledger Technology: The Science of the Blockchain*, 2nd Ed., Create Space Independent Publishing Platform, 2017.
[11] R. Zhang, B. Preneel. *Publish or perish: a backward-compatible defense against selfish mining in bitcoin.* In *Topics in Cryptology - The Cryptographers Track at the RSA Conference 2017*, Springer, p.277-292, 2017.

Cyril Grunspan
Léonard de Vinci Pôle Univ, Finance Lab, Labex Réfi
Paris, France,

E-mail address: cyril.grunspan@devinci.fr

Ricardo Pérez-Marco
CNRS, IMJ-PRG, Labex Réfi
Paris, France

E-mail address: ricardo.perez.marco@gmail.com

Author's Bitcoin Beer Address (ABBA)[2]:
1KrqVxqQFyUY9WuWcR5EHGVvhCS841LPLn

[2]Send some bitcoins to support our research at the pub.