On the profitability of selfish blockchain mining under consideration of ruin

Hansjörg Albrecher[*] and Pierre-O. Goffard[†]

Abstract

Mining blocks on a blockchain equipped with a proof of work consensus protocol is well-known to be resource-consuming. A miner bears the operational cost, mainly electricity consumption and IT gear, of mining, and is compensated by a capital gain when a block is discovered. This paper aims at quantifying the profitability of mining when the possible event of ruin is also considered. This is done by formulating a tractable stochastic model and using tools from applied probability and analysis, including the explicit solution of a certain type of advanced functional differential equation. The expected profit at a future time point is determined for the situation when the miner follows the protocol as well as when he/she withholds blocks. The obtained explicit expressions allow us to analyze the sensitivity with respect to the different model components and to identify conditions under which selfish mining is a strategic advantage.

Keywords: Blockchain; miner; cryptocurrency; ruin theory; dual risk model.

1 Introduction

A blockchain is a distributed public data ledger maintained by achieving consensus among a number of nodes in a *Peer-to-Peer* network. The nodes, referred to as miners, are responsible for the validity of the information recorded in the blocks. Each miner stores a local copy of the data and competes to solve a cryptographic puzzle. The first miner who is able to propose a solution includes the pending information in a block and collects a reward. The mining process is energy-consuming and costly in terms of equipment. The goal of the present paper is to provide insights into how profitable it is to engage in mining activities when keeping the aforementionned expenses in mind.

Miners are supposed to follow an incentive-compatible protocol which consists of releasing immediately any newly discovered block and appending it to the longest existing branch

[*] Department of Actuarial Science, Faculty of Business and Economics, University of Lausanne and Swiss Finance Institute. Batiment Extranef, UNIL-Dorigny, 1015 Lausanne, Switzerland. Email: hansjoerg.albrecher@unil.ch

[†] ISFA, Université Lyon 1, LSAF EA2429. Email: pierre-olivier.goffard@univ-lyon1.fr

of the blockchain. By doing so, miners are paid in proportion to their contribution to the overall computational effort. It was shown by Kroll et al. [14] that following the protocol is a dominant strategy leading to a consistent history of transactions. Later, Eyal and Sirer [6] introduced a blockwithholding strategy, called *selfish mining*, that allows a pool of miners to get a revenue, relative to the network revenue, that is greater than its fair share of the computing power. This strategy consists, for a miner or a mining pool, in hiding discovered blocks before broadcasting them to the network at well-chosen times to fork the chain. By expanding their private branch, selfish miners try to get the upper hand over the honest nodes as the fork develops until it resolves. Other blockwithholding strategies were presented in Sapirshtein et al. [21] and Nayak et al. [18] leading to an optimized relative revenue. These strategies imply a lower revenue, even for the malicious nodes, which led Grunspan and Marco-Pérez in a series of contributions [13, 10, 12, 11] to label them as not profitable. The authors pointed out that the time required to implement such a scheme can be rather long and the time before it becomes profitable even longer exposing them to a significant risk of going bankrupt. Blockchain protocols usually calibrate the difficulty of the cryptopuzzle to ensure a steady flow of confirmed information. The difficulty is adjusted periodically to account for the evolution of the computing power of the network. Because block withholding strategies impede the speed of the block generating process, their application will cause a decrease in the cryptopuzzle difficulty for the next round. The selfish miners then resume to protocol and increase their revenue. Furthermore, the waste of resources will drive some honest miners out of the game, increasing the colluding miners' share of the network computing power. Yet another side effect of selfish mining, noted in Eyal and Sirer [6], is that the revenue of the selfish miners will entice honest miners to join them. The pool will grow and may accumulate more than 50% of the resources putting them in position to perform double spending attacks, described in Nakamoto [17], Rosenfeld [20] and Goffard [8].

In this paper we model the surplus of a miner by a stochastic process that is inspired by risk processes considered for the study of the surplus in insurance portfolios, for which a detailed understanding concerning the probability of that surplus to become negative is available (see e.g. Asmussen and Albrecher [1] for an overview). The latter event is referred to as *ruin* in the insurance context, and we will adopt this terminology in the present setup, even if the investigation of the event of running out of money can be seen as a risk management tool rather than bankruptcy in the literal sense. The profitability will be assessed by computing the expected surplus of a miner at some time horizon given that ruin did not occur until then. It will turn out that under reasonably realistic model assumptions, one can derive closed form expressions for this quantity when letting the time horizon be random, and more in particular, exponentially distributed. Apart from tractability, the assumption of an exponential time horizon also has a natural interpretation in terms of lack-of-memory as to when the surplus process will be observed for the assessment of the profitability. Note that the selfish mining strategy considered in this paper is a simplified version of the one studied in Eyal and Sirer [6], with the purpose of allowing an explicit treatment for the value function under consideration.

The rest of the paper is organized as follows. Section 2 develops a stochastic model for the surplus process of a miner and derives formulas for safety and profitability measures for a miner that follows the prescribed protocol. Mathematically, our profitability analysis will lead to the solution of differential equations with advanced arguments. In Section 3, the study is then extended to the situation of a selfish miner and the resulting system of differential equations with advanced arguments is analytically solved in Appendix B and C. Section 4 subsequently uses the obtained explicit expressions for numerical studies and sensitivity tests with respect to model parameters in order to determine whether block withholding strategies are profitable or not. We find that selfish mining may be profitable, but always to a lesser extent than following the protocol. We also provide a numerical comparison of the proposed selfish mining strategy to the original strategy of Eyal and Sirer. In Section 5, we consider a time horizon large enough to include a difficulty adjustment. We show that, depending on the electricity price, in the presence of difficulty adjustments selfish mining may in fact outperform the alternative of following the protocol. In Section 6 we conclude and outline some directions for future research.

2 Ruin and expected surplus of a miner following the protocol

A miner, referred to as Sam, starts operating with an initial surplus level $u > 0$. We consider the following stochastic model for the surplus process over time. Mining blocks generates steady operational costs of amount $c > 0$ per unit of time, most notably due to electricity consumption. The entire network of miners appends blocks to the blockchain at an exponential rate λ, which means that the length of the blockchain over time is governed by a Poisson process $(N_t)_{t\geq 0}$ with intensity λ. We assume that Sam owns a fraction $p \in (0, 1/2)$ of the overall computing power, which implies that each block is published by Sam with a probability p. The number of blocks found by Sam and therefore the number of rewards of size $b > 0$ he collects up to time $t \geq 0$ is a thinned Poisson process $(\tilde{N}_t)_{t\geq 0}$ with intensity λ and thinning parameter p. Sam's surplus R_t at time t is then given by

$$R_t = u + b \cdot \tilde{N}_t - c \cdot t, \qquad t \geq 0. \tag{1}$$

The stochastic process $(R_t)_{t\geq 0}$ resembles the so-called dual risk process in risk theory, see for instance Avanzi et al. [3]. The focus of this paper is the profitability of mining blocks on the blockchain, but subject to a ruin constraint. In this context, the time of ruin $\tau_u = \inf\{t \geq 0 : \ R_t = 0\}$ is defined as the first time when the surplus reaches zero, i.e. the miner runs out of money and cannot continue to operate. The riskiness of the mining business may be assessed via the finite-time and infinite-time horizon ruin probabilities defined as

$$\psi(u, t) = \mathbb{P}(\tau_u \leq t), \text{ and } \psi(u) = \mathbb{P}(\tau_u < \infty), \tag{2}$$

respectively. The rewards earned through mining must in expectation exceed the operational cost per time unit. The latter condition translates into $p\lambda b > c$, and is referred to as the net profit condition in standard risk theory, see [1]. In particular, this implies $\psi(u) < 1$, i.e. ruin does not occur almost surely. The profitability for a time horizon $t > 0$ is now measured by

$$V(u, t) = \mathbb{E}(R_t \cdot \mathbb{I}_{\tau_u > t}), \tag{3}$$

where $\mathbb{I}_A$ denotes the indicator random variable of an event A. Correspondingly, $V(u, t)$ is the expected surplus level at time t, where in the case of ruin up to t this surplus is 0 (i.e., due to the ruin event the surplus is frozen in at 0). In terms of a conditional expectation, one can equivalently express $V(u,t)$ as the probability to still be alive at t times the expected value of the surplus at that time given that ruin has not occurred:

$$V(u,t) = (1-\psi(u,t)) \cdot \mathbb{E}(R_t|\tau_u > t).$$

The following result provides formulas for the ruin probabilities and $V(u,t)$ in this setting.

Proposition 2.1.

1. *For any $u \geq 0$, the finite-time ruin probability is given by*
$$\psi(u,t) = \sum_{n=0}^{\infty} \frac{u}{u+bn} \, \mathbb{P}\left[\tilde{N}_{\frac{u+bn}{c}} = n\right] \mathbb{I}_{\left\{t>\frac{u+bn}{c}\right\}}. \tag{4}$$

2. *For any $u \geq 0$, the infinite-time ruin probability is given by*
$$\psi(u) = e^{-\theta^* u}, \tag{5}$$
where θ^* is the positive solution in θ of the equation
$$c\,\theta + p\lambda\,(e^{-b\,\theta} - 1) = 0. \tag{6}$$

3. *For any $u \geq 0$, the expected surplus at time t in case ruin has not occurred until then, can be written as*
$$V(u,t) = \mathbb{E}\left[\left(u + b\tilde{N}_t - ct\right)_+ (-1)^{\tilde{N}_t} G_{\tilde{N}_t}\left(0 \,\middle|\, \left\{\frac{u}{ct} \wedge 1, \ldots, \frac{u+(\tilde{N}_t - 1)b}{ct} \wedge 1\right\}\right)\right], \tag{7}$$
where $(.)_+$ denotes the positive part, $\wedge$ stands for the minimum operator and $(G_n(\cdot|\{\ldots\})_{n\in\mathbb{N}}$ is the sequence of Abel-Gontcharov polynomials defined in Appendix A.

Proof. 1. The ruin time τ_u may be rewritten as

$$\tau_u = \inf\left\{t \geq 0 \;;\; \tilde{N}_t = ct/b - u/b\right\}.$$

Note that ruin can only occur at the specific times

$$t_k = \frac{u+bk}{c},\; k \geq 0,$$

when the function $t \mapsto ct/b - u/b$ reaches integer levels. For $t > 0$, define the set of indices $\mathcal{I} = \{k \geq 0 \;;\; t_k \leq t\}$. The finite-time ruin probability can then be written as

$$\psi(u,t) \;=\; \sum_{k\in\mathcal{I}} \mathbb{P}(\tau_u = t_k) \;=\; \sum_{k\in\mathcal{I}} \frac{t_0}{t_k}\, \mathbb{P}\left[\tilde{N}(t_k) = k\right],$$

where the last equality follows from applying Corollary 3.4 of Goffard and Lefevre [9] and is equivalent to (4).

2. This result is standard, see e.g. [1, Th.VI.2.1]. For the sake of completeness, we still prefer to give the main idea behind its derivation and the probabilistic reason for Equation (6) here. The process $\{e^{\theta(ct-b\tilde{N}_t)-t\kappa(\theta)}\}_{t\geq 0}$, is a martingale for any $\theta\in\mathbb{R}$, where $\kappa(\theta)=\log\mathbb{E}(e^{c\theta-b\theta\tilde{N}_1})$, see e.g. [1, Th.II.2.1]. The simplest choice for θ is the one for which $\kappa(\theta)=0$, i.e.

   $$c\theta+p\lambda(e^{-b\theta}-1)=0.$$

   The latter equation admits a unique non-negative solution θ^*, and the process $\left(e^{\theta^*(ct-b\tilde{N}_t)}\right)_{t\geq 0}$ is therefore a martingale. It then follows by the Optional Stopping Theorem (cf. [1, Prop.II.3.1]) that

   $$\psi(u)=e^{-\theta^* u},$$

   since under the assumptions on R_t (with only upward jumps) the surplus at the time of ruin is necessarily zero.

3. Using the tower property, we can express the value function (3) as

   $$\begin{aligned}
V(u,t) &= \mathbb{E}\left[\mathbb{E}\left(R_t\mathbb{I}_{\tau_u>t}\middle|\tilde{N}_t\right)\right]\\
&= \mathbb{E}\left[\left(u+b\tilde{N}_t-ct\right)\mathbb{E}\left(\mathbb{I}_{\tau_u>t}\middle|\tilde{N}_t\right)\right]\\
&= \mathbb{E}\left[\left(u+b\tilde{N}_t-ct\right)_+\mathbb{P}\left(\bigcap_{k=1}^{\tilde{N}_t}\{T_k<t_{k-1}\wedge t\}\middle|\tilde{N}_t\right)\right]\\
&= \mathbb{E}\left[\left(u+b\tilde{N}_t-ct\right)_+\mathbb{P}\left(\bigcap_{k=1}^{\tilde{N}_t}\{U_{1:k}<\frac{t_{k-1}}{t}\wedge 1\}\right)\right], \qquad (8)
\end{aligned}$$

   where $U_{1:n},\dots,U_{n:n}$ denote the order statistics of n i.i.d. standard uniform random variables. Using the interpretation of Abel-Gontcharov polynomials as the joint probabilities of uniform order statistics, see Goffard and Lefevre [9, Prop.2.4] then yields (7).

□

Expression (7) is unfortunately not of closed form. The Abel-Gontcharov polynomials may be evaluated recursively, and acceptable approximations follow from simple truncation or simulation. However, we are interested in a more explicit and amenable expression for this quantity. In addition, the choice of the considered time horizon t is somewhat arbitrary. We therefore propose now to replace the fixed time horizon t by an independent exponential random time horizon T with mean t. This will allow us to derive a simple and explicit expression for the respective quantity, which hopefully will provide a good approximation of $V(u,t)$. At the same time, this random time horizon also has an intuitive interpretation on its own: it can be seen as the first epoch of an independent homogeneous Poisson process, so that there is a lack-of-memory as to when exactly the surplus level is going to be evaluated, with the expected value of that time horizon being t. We hence consider the value function

$$\widehat{V}(u,t):=\mathbb{E}(V(u,T))=\mathbb{E}(R_T\mathbb{I}_{\tau_u>T}), \qquad (9)$$

where $T\sim\operatorname{Exp}(t)$.

Proposition 2.2. *For any $u \geq 0$, the value function $\widehat{V}(u,t)$ satisfies the differential equation*

$$c\widehat{V}'(u,t) + \left(\frac{1}{t} + p\lambda\right)\widehat{V}(u,t) - p\lambda\widehat{V}(u+b,t) - \frac{u}{t} = 0 \tag{10}$$

with boundary condition $\widehat{V}(0,t) = 0$ and $0 \leq \widehat{V}(u,t) \leq u - ct + p\lambda t$ for $u > 0$, a solution of which is given by

$$\widehat{V}(u,t) = u + (p\lambda b - c)\, t\, (1 - e^{\rho^* u}), \tag{11}$$

where ρ^* is the negative solution of the equation

$$- c\rho + p\lambda\, (e^{b\,\rho} - 1) = 1/t. \tag{12}$$

Proof. Let $0 < h < u/c$, so that ruin can not occur in the interval $(0,h)$. We distinguish three cases:

(i) $T > h$ and there is no block discovery in the interval $(0,h)$,

(ii) $T < h$ and there is no block discovery in the interval $(0,T)$,

(iii) There is a block discovery before time T and in the interval $(0,h)$.

By conditioning we see that

$$\begin{aligned}\widehat{V}(u,t) \quad &= \quad e^{-h(1/t+p\lambda)}\,\widehat{V}(u-ch,t) + \int_0^h \frac{1}{t}\, e^{-s(1/t+p\lambda)}\,(u-cs)ds \\ &\quad + \int_0^h p\lambda\, e^{-s(1/t+p\lambda)}\,\widehat{V}(u-cs+b,t)ds.\end{aligned}$$

Now we take the derivative with respect to h and set $h = 0$ to obtain

$$c\widehat{V}'(u,t) + \left(\frac{1}{t} + p\lambda\right)\widehat{V}(u,t) - p\lambda\widehat{V}(u+b,t) - \frac{u}{t} = 0, \tag{13}$$

with boundary condition $\widehat{V}(0,t) = 0$ and such that $0 \leq \widehat{V}(u,t) \leq u - ct + p\lambda t$ for $u > 0$.

Here the derivative is with respect to the first argument (note that the above derivation automatically guarantees the existence of the derivative $\widehat{V}'(u,t)$). Equation (13) is an advanced functional differential equation. In order to identify its solution, consider the form

$$\widehat{V}(u,t) = Ae^{\rho u} + Bu + C, \; u \geq 0, \tag{14}$$

where A, B, C and ρ are constants to be determined. Substituting (14) in (13) together with the boundary condition yields the system of equations

$$\begin{cases} 0 &= ct\rho + (1+p\lambda t) - p\lambda t e^{\rho b}, \\ 0 &= B\,(1+tp\lambda) - p\lambda t B - 1, \\ 0 &= Bct + C(1+tp\lambda) - p\lambda t B b - p\lambda t C, \\ 0 &= A + C. \end{cases}$$

We then have $A = -t(p\lambda b - c)$, $B = 1$, $C = t(p\lambda b - c)$ and ρ is solution of Equation (12), which admits one negative and one positive solution. As $A < 0$, we have to choose the negative solution $\rho^* < 0$ in order to ensure $\widehat{V}(u,t) > 0$. Substituting A, B, C and ρ^* in (14) yields the result. □

Remark 2.1. Equation (10) is a particular case of an advanced functional differential equation (concretely, a differential equation with an advanced argument). Strictly speaking, a priori one cannot exclude the possibility of other possible solutions than the one derived above, as (to the best of our knowledge) no general mathematical theory concerning uniqueness of the solution exists for the given boundary conditions. To establish uniqueness mathematically, one would typically need to specify a boundary condition for $\widehat{V}(u,t)$ on the entire (but small) interval $u \in [0,b]$ for any t (see e.g. [22]). Assuming

$$\mathbb{E}(R_T \mathbb{I}_{\tau_u > T}) = u + (p\lambda b - c)\, t\, (1 - e^{\rho^* u}), \quad u \in [0,b] \tag{15}$$

as an additional boundary condition would then establish (11) as the unique solution of (10) for all $u \geq 0$, and hence formally establish that the value function (9) coincides with (11) (by uniqueness any other possibility is then ruled out). Indeed, condition (15) can be checked to hold by stochastic simulation of $\mathbb{E}(R_T \mathbb{I}_{\tau_u > T})$ (and we successfully confirmed that validity for numerous combinations of parameters), so that we know to have captured the right formula for $\widehat{V}(u,t)$ despite the unusual boundary conditions of the advanced functional differential equation. □

Remark 2.2. Note that, as the solution of (12), ρ^* can be expressed through the Lambert W function, see Corless et al. [5], with

$$\rho^* = -\frac{p\lambda t + 1}{ct} - \frac{1}{b}\,\mathrm{W}\left(-\frac{p\lambda\, b}{c}\, e^{-b\left(\frac{p\lambda t+1}{ct}\right)}\right).$$

Furthermore, the similarity of the equations (6) and (12) (referred to as *Lundberg equations* in risk theory) is no coincidence. In contrast to the probabilistic derivation of (6) presented in the proof of Proposition 2.1, one could also mimick the analytic approach above and identify $\psi(u)$ as the solution of the differential equation $c\psi'(u) + p\lambda(\psi(u) - \psi(u+b)) = 0$, of which (6) is the characteristic equation (here $\theta = -\rho$). □

We now complement the results of Proposition 2.1. Define

$$\widehat{\psi}(u,t) := \mathbb{E}(\psi(u,T)) = \mathbb{P}(\tau_u < T), \; u \geq 0, t > 0 \tag{16}$$

as the ruin probability up to an (independent) exponential time horizon T with mean t. Note that

$$\widehat{\psi}(u,t) = \mathbb{E}(\mathbb{P}(T > \tau_u | \tau_u)) = \mathbb{E}(e^{-\delta \tau_u}),$$

with $\delta = 1/t$. Thus, $\widehat{\psi}(u,t)$ is the Laplace transform of the ruin time density. In actuarial language, it is the expected present value (evaluated with the force of interest δ) of 1 that is paid at the time of ruin.

This quantity turns out to have a very simple form (see also Asmussen et al. [2] for ruin probabilities up to a random time horizon in the classical risk model):

Proposition 2.3. *We have*

$$\widehat{\psi}(u,t) = e^{\rho^* u}, \tag{17}$$

where ρ^* is the negative solution in ρ of Equation (12).

Proof. It can be verified that the process $\{\exp(-\delta t_1 + \rho^* R_{t_1})\}_{t_1 \geq 0}$ is a martingale. From the Optional Stopping Theorem it follows that the expectation at the time of ruin is equal to its initial value, which is precisely Formula (17). □

Remark 2.3. While the probabilistic proof given above is in the spirit of the proof of (5), one can alternatively, akin to the approach for proving Proposition 2.2, also follow the analytic route and show that $\widehat{\psi}(u,t)$ is the solution of the differential equation

$$c\widehat{\psi}'(u,t) + (p\lambda + 1/t)\,\widehat{\psi}(u,t) - p\lambda\,\widehat{\psi}(u+b,t) = 0 \tag{18}$$

with initial condition $\widehat{\psi}(0,t) = 1$ and boundary condition $\lim_{u\to\infty}\widehat{\psi}(u,t) = 0$, where the derivative is with respect to the first argument. This is in fact the homogeneous equation of (13) and gives a nice interpretation of the term $1/t$ as the intensity of the dynamic time horizon when moving along the surplus trajectory R_t. Trying a solution of the form $\widehat{\psi}(u,t) = Ae^{\rho u} + C$ then immediately leads to the result, since the boundary condition forces $C = 0$ and the initial condition gives $A = 1$, whereas the exponent ρ has to be the negative solution of (12) (to establish the uniqueness of the solution of (18) one would again have to argue as in Remark 2.1). □

Comparing the expression (4) for $\psi(u,t)$ with deterministic time horizon t and (17) for $\widehat{\psi}(u,t)$ with random time horizon (of the same expected value) shows the substantial simplification one can achieve through the principle of randomization. We refer to Section 4 for a numerical comparison of the two quantities.

3 Ruin and expected surplus of a selfish miner

It has been discussed in the literature for a while already that it may be advantageous to keep newly found blocks hidden (see e.g. [6]). Such a block withholding strategy is referred to as selfish mining. The goal is to build up a stock of blocks and release them publicly at well chosen times so as to fork the chain and make a part of the mining activities of competitors worthless, depending on which branch is followed up in the longer run. A fork happens when two equally long versions of the blockchain coexist, and it resolves whenever one of them becomes longer by at least one block. In the sequel, we consider a variant of the selfish mining strategy introduced by Eyal and Sirer [6]. Let $(N_t)_{t\geq 0}$ be the homogeneous Poisson process with intensity λ that governs the block discovery process of the entire network. As in the previous section, we consider a miner named Sam who owns a share $p \in (0,1)$ of the computing power so that a newly found block belongs to Sam with probability p. We keep track of Sam's lead over the honest chain in terms of number of blocks via a Markov jump process

$$X_t = Z_{N_t},\ t \geq 0,$$

where $(Z_k)_{k\geq 0}$ is a homogeneous Markov chain with finite state space $E = \{0, 1, 0^*\}$ which we define now. Assume that at time $t \geq 0$, the miners have published $N_t = k$ blocks.

- If Sam is not hiding any block, then $Z_k = 0$,
  - if Sam finds the next block, he stores it in a buffer and $Z_{k+1} = 1$,
  - if the other miners discover a block then Sam's buffer remains empty $Z_{k+1} = 0$,

  In both cases, Sam is not collecting any reward.
- If Sam is hiding one block at that time, then $Z_k = 1$,

  - if he then finds a new block, then he broadcasts both blocks immediately (which resets the Markov chain to $Z_{k+1} = 0$), and he collects two rewards,
  - if the others find a block, then Sam also releases his block leading to a fork situation characterized by $Z_{k+1} = 0^*$. At that moment Sam is not collecting any rewards.

- If a fork situation is present at that time ($Z_k = 0^*$), then
  - if Sam finds a new block then he appends it to his branch of the chain and collects the reward for two blocks and $Z_{k+1} = 0$.
  - if the others find a block then
    - they append it to Sam's branch with a probability $0 \leq q \leq 1$, in which case Sam gets the reward for one block.
    - If the block is mined on top of the competing branch, then Sam earns nothing.

    In both cases, the number of hidden blocks then becomes $Z_{k+1} = 0$.

Figure 1 depicts the transition graph of $(Z_k)_{k\geq 0}$. The selfish mining strategy alters the reward collecting process. The surplus process of Sam introduced in (1) now becomes

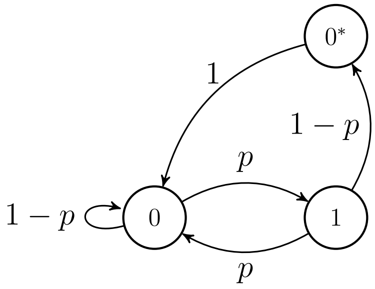


Figure 1: Transition graph of the Markov chain $(Z_k)_{k\geq 0}$ representing the stock of blocks retained by Sam when implementing the simplified selfish mining strategy.

$$R_t = u - c \cdot t + b \cdot \sum_{n=1}^{N(t)} f\left[Z_{n-1}, \xi_n, \zeta_n\right], \tag{19}$$

where the $(\xi_n)_{n\geq 1}$ and $(\zeta_n)_{n\geq 1}$ are i.i.d. Bernoulli random variables with parameter p and q, respectively, and

$$f\left[Z_{n-1}, \xi_n, \zeta_n\right] = \begin{cases} 0, & \text{if } Z_{n-1} = 0, \\ 0, & \text{if } Z_{n-1} = 1 \ \& \ \xi_n = 0, \\ 2, & \text{if } Z_{n-1} = 1 \ \& \ \xi_n = 1, \\ 0, & \text{if } Z_{n-1} = 0^* \ \& \ \xi_n = 0 \ \& \ \zeta_n = 0, \\ 1, & \text{if } Z_{n-1} = 0^* \ \& \ \xi_n = 0 \ \& \ \zeta_n = 1, \\ 2, & \text{if } Z_{n-1} = 0^* \ \& \ \xi_n = 1. \end{cases} \tag{20}$$

Remark 3.1. In contrast to the selfish mining strategy defined above, Eyal and Sirer's [6] more general selfish mining strategy does not automatically release the blocks when the buffer reaches size two. On the contrary, the stock is being built up continuously and the selfish miner releases one block for every block found by the others. As soon as the level of the buffer goes back to two, the selfish miner releases the last two blocks to win over the fork situation. The process $(Z_n)_{n\geq 0}$ remains a proper Markov chain, and the study of its stationary distribution allowed Eyal and Sirer [6] to show how the relative revenue of the selfish miner exceeds his fair share. However, the fact that the state space of $(Z_n)_{n\geq 0}$ is then not finite anymore prevents a solution of the resulting system of differential equations along the lines of Theorem B.1 and Corollary C.1 given below. The reward function (the analogue of (20)) for Eyal and Sirer's strategy is given by

$$f\left[Z_{n-1},\xi_n,\zeta_n\right] = \begin{cases} 0, & \text{if } Z_{n-1}=0, \\ 0, & \text{if } Z_{n-1}=1, \\ 2, & \text{if } Z_{n-1}=2 \ \&\ \xi_n=0, \\ 0, & \text{if } Z_{n-1}\geq 2 \ \&\ \xi_n=1, \\ 1, & \text{if } Z_{n-1}>2 \ \&\ \xi_n=0, \\ 0, & \text{if } Z_{n-1}=0^* \ \&\ \xi_n=0 \ \&\ \zeta_n=0, \\ 1, & \text{if } Z_{n-1}=0^* \ \&\ \xi_n=0 \ \&\ \zeta_n=1, \\ 2, & \text{if } Z_{n-1}=0^* \ \&\ \xi_n=1. \end{cases} \tag{21}$$

The expected income is here higher as soon as the miner manages to accumulate more than two blocks. At the same time, compared to (20) we notice a delay in the earning process (21) when $Z_{n-1}=2$ and $\xi_n=1$, which may impair the miner's solvency. Consequently, for the consideration of solvency aspects we prefer to focus on our slightly simpler selfish mining strategy here. Nevertheless, a simulation study is conducted in Section 4.3 to compare numerically the revenue and ruin probability of a miner implementing Eyal and Sirer's selfish mining strategy instead of the variant studied in this paper. □

It is interesting to see whether selfish mining is still profitable for Sam if the possibility of ruin is included in the analysis. His average earning per time unit is now given by

$$\gamma = \frac{b}{t}\,\mathbb{E}\left[\sum_{k=1}^{N(t)} f(Z_{k-1},\xi_k,\zeta_k)\right] - c. \tag{22}$$

This quantity can be determined if we assume that Sam has been mining in a selfish way for quite some time already, so that we can consider the Markov chain to be in stationarity with stationary probabilities

$$\mathbb{P}(Z=0)=\frac{1}{1+2p-p^2},\ \mathbb{P}(Z=1)=\frac{p}{1+2p-p^2},\ \text{and } \mathbb{P}(Z=0^*)=\frac{p(1-p)}{1+2p-p^2}.$$

The quantities $U_k := f\left(Z_{k-1},\xi_k,\zeta_k\right),\ n\geq 1$ then have a p.m.f. $p_U(\cdot) := \mathbb{P}(U=\cdot)$ given by

$$p_U(0)=\frac{1+p(1-p)+p(1-p)^2(1-q)}{1+2p-p^2},\ p_U(1)=\frac{pq(1-p)^2}{1+2p-p^2},\ \text{and } p_U(2)=\frac{p^2+p^2(1-p)}{1+2p-p^2},$$

and the net profit condition correspondingly reads

$$\gamma = b\lambda \frac{qp(1-p)^2 + 4p^2 - 2p^3}{1 + 2p - p^2} - c > 0. \tag{23}$$

The profitability of selfish mining consequently depends on the interplay between the probabilities p and q, and not all values of p and q will lead to positive expected profit. If we assume for a moment that the U_k's are i.i.d. with p.m.f. p_U (which is of course a strongly simplifying assumption) and the net profit condition holds, then the infinite-time ruin probability is given by

$$\psi(u) = e^{-\theta^* u},$$

where θ^* is the unique positive root of the equation

$$c\theta + \lambda \left[p_U(0) + e^{-b\theta} p_U(1) + e^{-2b\theta} p_U(2) - 1 \right] = 0.$$

The proof is anologous to the one of Proposition 2.1. Deriving the actual ruin probability and the expected surplus under ruin constraints at some deterministic time horizon is more difficult than in the previous section. However, for the exponential time horizon (with mean t), we are able to derive an explicit formula for $\widehat{V}(u,t)$. Since the reward process is modulated by the Markov chain, we have to derive the value function depending on the current state of the Markov chain. The result below in principle provides a formula for

$$\widehat{V}_z(u,t) \equiv \mathbb{E}(V_z(u,T)) = \mathbb{E}\left(R_T \mathbb{I}_{\tau_u > T} \middle| Z_0 = z \right) \tag{24}$$

with $T \sim \mathrm{Exp}(t)$ for any $z \in \{0, 1, 0^*\}$. The most interesting among these is $\widehat{V}_0(u,t)$, which refers to the situation where the buffer is empty at the beginning. Theorem B.1, in Appendix B, provides a tractable formula for $\widehat{V}_0(u,t)$ with

$$\widehat{V}_0(u,t) = A_1\, \mathrm{e}^{\rho_1 u} + \mathrm{e}^{\rho_2 u} \left[A_2\, \cos(\rho_3 u) + A_3\, \sin(\rho_3 u) \right] + u + C, \tag{25}$$

where $A_1, A_2, A_3, \rho_1, \rho_2, \rho_3$ and C are constants defined in the statement of Theorem B.1 in Appendix B.

Remark 3.2. If the connectivity parameter q equals 1, then the selfish miner will not waste any blocks by withholding them first, he will just append them later. In that sense his surplus process, and correspondingly the value function, is very similar to the one when following the protocol, with the subtle difference that by receiving the rewards later, the likelihood of ruin is increased (reducing the value function). When the initial capital increases indefinitely, that effect evaporates and then the only remaining difference between the two is that for the expected surplus at the evaluation time horizon $T \sim Exp(t)$ the initial state still matters for the selfish miner, since starting – with the same initial capital u – in state 0^* or 1 will lead to overall one more block than when starting in state 0 (i.e., with an empty buffer). This latter difference should then itself disappear when t increases indefinitely. Checking this, $\widehat{V}(u,t) - u$ in (11) converges to $(p\lambda b - c)t$, and $\widehat{V}_0(u,t) - u$ in (25) converges to C, as $u \to \infty$. While C defined (36) of Appendix B is a rather involved function of the parameter t, a simple calculation shows that, for $q = 1$ (and only then!), $C/t \to p\lambda b - c$ as $t \to \infty$, so that the two expressions are indeed asymptotically equivalent. For a numerical comparison of $\widehat{V}_0(u,t)$ and $\widehat{V}(u,t)$ for finite values of u and t, see Section 4. □

Finally, the ruin probability for the selfish miner up to an exponential time horizon can be obtained in an analogous (and slightly simpler) way. Corollary C.1, in Appendix C, provides the following expression for the ruin probability of a selfish miner

$$\widehat{\psi}_0(u,t) = C_1\,\mathrm{e}^{\rho_1\,u} + \mathrm{e}^{\rho_2\,u}\left[C_2\,\cos\left(\rho_3\,u\right) + C_3\,\sin\left(\rho_3\,u\right)\right], \tag{26}$$

where $C_1, C_2, C_3, \rho_1, \rho_2$ and ρ_3 are constants defined in the statement of Corollary C.1 in Appendix C.

4 Numerical illustrations and sensitivity analysis

In this section, we are going to use the formula for the ruin probabilities and expected surplus in case ruin did not occur derived in the previous sections for numerical illustrations and in particular also for sensitivity analysis with respect to the involved parameters. We will first study the profitability of following the protocol in Section 4.1 and proceed to the profitability of selfish mining in Section 4.2. We define the expected profit as the expected surplus under ruin constraints minus the initial capital.

Throughout this section, the time unit is one hour. Since the Bitcoin blockchain protocol is designed to ensure that one block of confirmed transactions is added to the blockchain about every ten minutes, this renders the block arrival intensity in our model to be $\lambda = 6$. The reward b is determined by the number n_{BTC} of bitcoins earned when finding a block and the price π_{BTC} of the bitcoin. For the illustrations in this paper, we use the data of January 1, 2020, when $n_{BTC} = 12.5$ and $\pi_{BTC} = \$7,174.74$[1], so that the reward amounts to

$$b = n_{BTC} \times \pi_{BTC} = \$89,684.30.$$

We assume that the operational cost of mining reduces to the electricity consumed when computing hashes. On January 1, 2020, the yearly consumption of the network was estimated by the Cambridge Bitcoin Electricity Consumption Index[2] to 72.1671 TWh.[3] We denote by

$$W = \frac{72.1671 \times 10^9}{365.25 \times 24}$$

the electricity consumption of the network expressed in kWh. We let the operational cost c of a given miner be proportional to its share $p \in (0,1)$ of the network computing power with

$$c = p \times W \times \pi_W,$$

where π_W denotes the price of the electricity where the miner is located, expressed in USD per kWh.

[1] Source:blockchain.com

[2] Source:CBEI

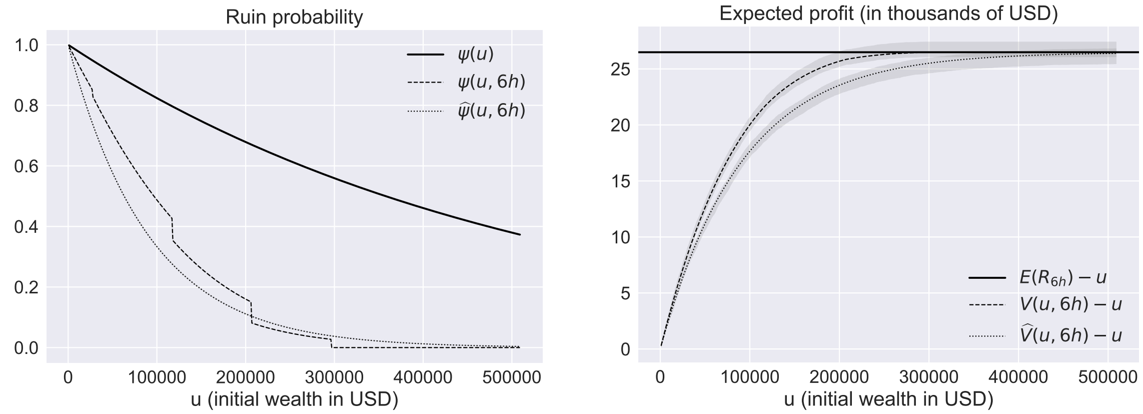
[3] The choice of this concrete date for the illustrations in this paper is somewhat arbitrary. Choosing another date and estimate of the Bitcoin price will, however, not crucially change the conclusions as long as the reward for finding a block compensates the operational cost.

4.1 Expected profit computations for a miner following the protocol

We assume now the assumptions of risk model (1) for the wealth of a miner that follows the protocol. The net profit condition $p\lambda b - c \geq 0$ then translates, in terms of the price of electricity, to

$$\pi_W < \frac{\lambda b}{W} = 0.065.$$

In the sequel, unless otherwise stated, we set $\pi_W = 0.06$ (so the net profit condition is satisfied) and assume the miner to have a share $p = 0.1$ of the network hashpower. Figure 2a displays the infinite-time and finite-time ruin probability (with chosen time horizon to be 6 hours) as a function of initial wealth using the formulas derived in Proposition 2.1.



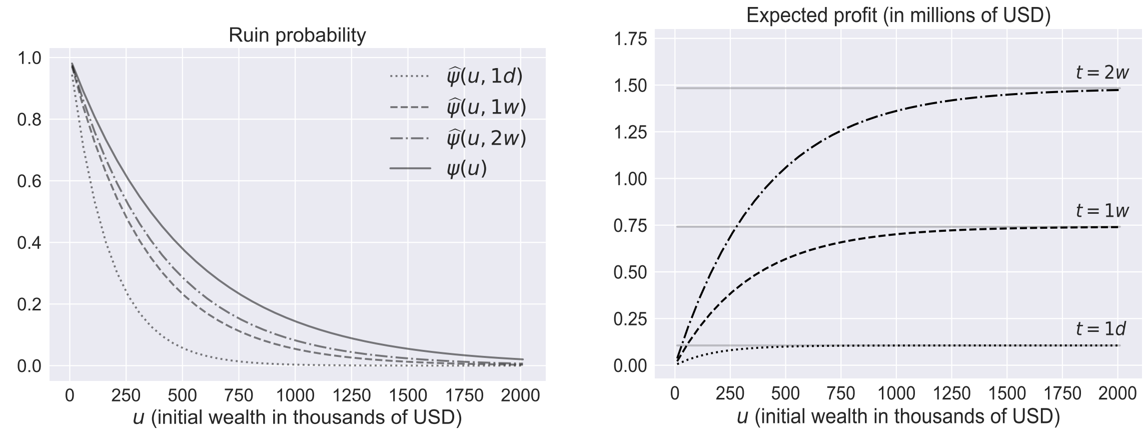
(a) $\psi(u)$ (solid), $\psi(u, 6h)$ (dashed) and $\widehat{\psi}(u, 6h)$ (dotted) as a function of initial wealth u.

(b) $\mathbb{E}(R_{6h}) - u$ (solid) , $V(u, 6h) - u$ (dashed), $\widehat{V}(u, 6h) - u$ (dotted) and as a function of initial wealth u.

Figure 2: Ruin probabilities and expected profit as a function of initial wealth for a miner that follows the protocol with hashpower $p = 0.1$ and electricity price $\pi_W = 0.06$, together with the confidence bands of a Monte-Carlo simulation.

Figure 2b plots the expected profit at that deterministic time horizon $t = 6$ hours (recall that the expected profit corresponds to the expected surplus under ruin constraints net of the initial wealth u) using formula (7) and compares it to $\mathbb{E}(R_t) - u = (p\lambda b - c)t$, which is the expected surplus, again net of the initial wealth, of a miner without that ruin constraint (we will refer to that latter quantity as the *target profitability* in the sequel). One sees that with increasing initial capital the two quantities get closer, as the event of ruin then becomes more and more unlikely. In Figure 2b we also give the quantity $\widehat{V}(u, t)$ as derived in Proposition 2.2 for an exponential time horizon T with expected value 6 hours, net of initial capital u (dashed line). When comparing the deterministic time horizon to the random time horizon with the same expected value, it is clear that the exponential distribution overweights time horizons below the expected value of 6 hours, so that it is intuitive that the expected gain is below the one for the deterministic time horizon (as, due to the net profit condition, the expected income increases with the time horizon). But this difference diminishes for large values of u, as they both approach the target profitability. In order to double-check the validity of the obtained explicit formulas, we also plot in Figure 2 asymptotic 95%-confidence bands of an independent Monte Carlo simulation of all the quantities using 250'000 sample paths, and the exact formulas are nicely in the center of these bands (in Figure 2a these bands are so narrow that one can barely observe them with the naked eye). Another way to read Figure 2a is that it quantifies the amount of initial capital u needed in order to ensure survival within 6 hours, or at any time in the future, for any given probability. Note that as u increases, more and more terms in the finite-sum expression (4) for $\psi(u,t)$ disappear, causing the jumps in the curve. Figure 2a also suggests that switching from a deterministic to a random exponential time horizon with the same mean does not impact the resulting ruin probability substantially. This further justifies the switch from a deterministic to a random time horizon with its enormous computational advantages, particularly for the selfish mining case. The time horizon of 6 hours in Figure 2 was in part chosen to ensure a satisfactory accuracy when evaluating formula (7). While there is no issue for $\psi(u)$ and $\psi(u,t)$, the recursive computation of Abel-Gontcharov polynomials in that formula for $V(u,t)$ becomes numerically unstable for larger time horizons.

Figure 3 displays the ruin probability and expected profit for the larger time horizons 1 day, 1 week and 2 weeks for the otherwise same set of parameters. Figure 3a illustrates quantitatively how $\widehat{\psi}(u,t)$ approaches the infinite-time ruin probability $\psi(u)$ as the expected time horizon t increases.



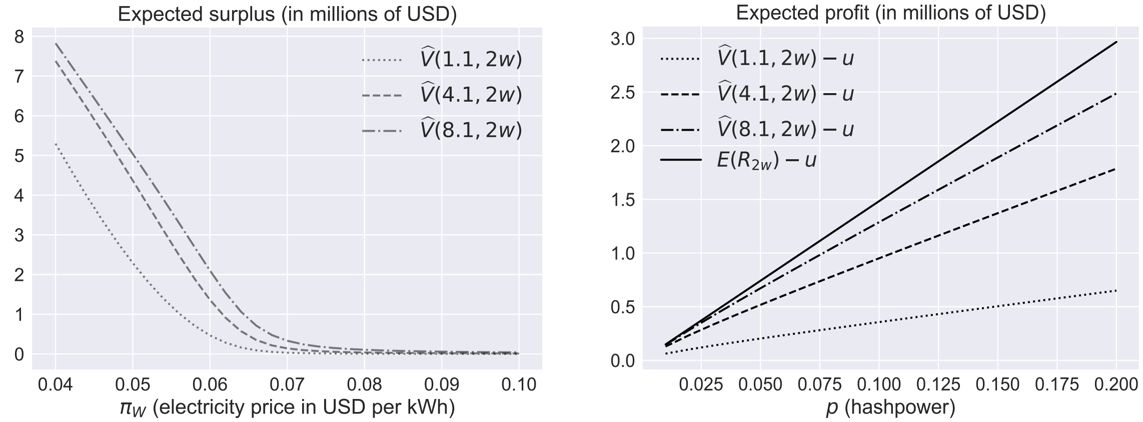
(a) $\widehat{\psi}(u,t)$ as a function of initial wealth u for varying time horizon: (dotted) $t = 1d$, (dashed) $t = 1w$, (dash-dotted) $t = 2w$, and (solid) $t = \infty$.

(b) $\widehat{V}(u,t) - u$ as a function of initial wealth u for varying time horizons: (dotted) $t = 1d$, (dashed) $t = 1w$, and (dash-dotted) $t = 2w$.

Figure 3: Ruin probabilities and expected profit over an exponential time horizon as a function of initial wealth for varying time horizon with hashpower $p = 0.1$ and electricity price $\pi_W = 0.06$.

Figure 3b depicts the expected profit over an exponential time horizon with varying mean, using the explicit formula of Proposition 2.2. It also contains a comparison with the respective target profitability without the ruin constraint for each case. Note that the latter increases with the time horizon due to the net profit condition. For smaller time horizons, the risk of going to ruin is quickly mitigated when increasing the initial reserve, which makes the convergence of the expected profit towards the targeted one swifter.

Let us now investigate the effect of the electricity price and the hashpower on the expected surplus under ruin constraints. We consider a random time horizon with mean 2 weeks now, and compute the expected surplus for various initial wealth levels. Figure 4a plots the respective surplus $\widehat{V}(u,t)$ determined in Proposition 2.2 as a function of the electricity price for a fixed hashpower $p = 0.1$ (in this plot we do not subtract u in order to show the decline of $\widehat{V}(u,t)$ more prominently). Rising electricity prices clearly make mining less profitable, and reduces the surplus to virtually zero for π_W around 0.08 even for quite large initial capital. Figure 4b then displays the expected profit as a function of hashpower, when the electricity price is fixed at $\pi_W = 0.06$. One observes that the expected profit increases almost linearly in the hashpower when the net profit condition holds.



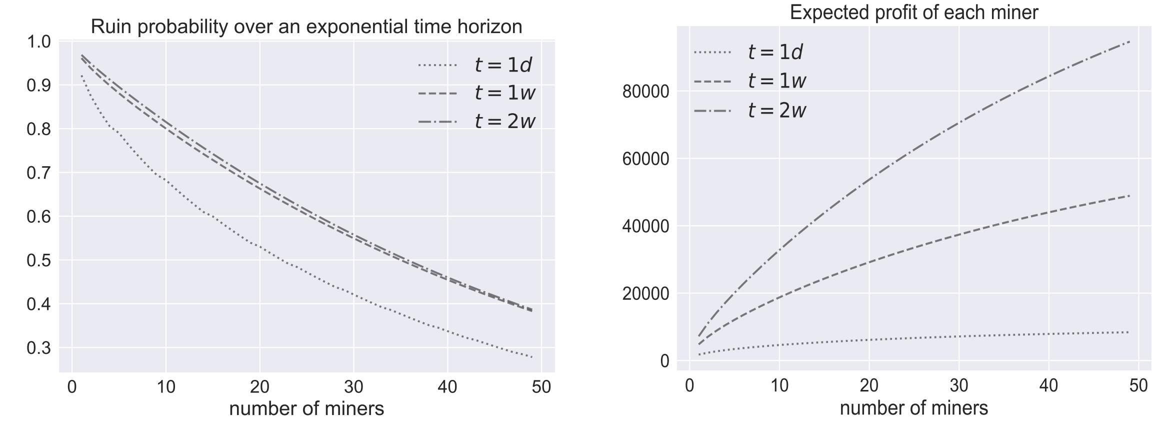
(a) $\widehat{V}(u, 2w)$ as a function of electricity price π_W with hashpower $p = 0.1$ for varying initial wealth: (dotted) $u = 1.1$, (dashed) $u = 4.1$, and (dash-dotted) $u = 8.1$.

(b) $\widehat{V}(u, 2w) - u$ as a function of hashpower p with electricity price $\pi_W = 0.06$ for varying initial wealth: (dotted) $u = 1.1$, (dashed) $u = 4.1$, and (dash-dotted) $u = 8.1$.

Figure 4: Expected surplus as a function of electricity price (left) and expected profit as a function of hashpower (right) under ruin constraints over an exponential time horizon (mean 2 weeks), for varying initial wealth (in tens of thousands of USD).

The magnitude of the reward for discovering a block makes mining very profitable in expectation, but the rarity of such an event also makes it very risky. Miners who seek a more steady income are then incentivized to form teams, called *mining pools* (Rosenfeld [19]), which reduce the variance of the reward process. Our results may be used to gain insight into how beneficial it is for a miner to join a mining pool. Consider 100 miners that start looking for blocks in isolation. Each of them owns 1% of the computing power and has an initial capital of amount \$10, 000. We wish to compare the ruin probability and the expected profit of mining pools of increasing size. We simply assume that when two miners join forces, the resulting pool then has 2% of the overall hashpower and

$u^* = \$20,000$ as initial capital. Figure 5 displays the ruin probability and expected profit per miner over an exponential time horizon as a function of the size of the mining pool for varying time horizon $t \in \{1d, 1w, 2w\}$. The expected profit per miner plotted in Figure 5b corresponds to the expected profit of the mining pool divided by the number of its members. One clearly can see the advantage of joining a pool, when the risk of ruin is added to the analysis.



(a) $\widehat{\psi}(u^*, t)$ as a function of the size of the mining pool for time horizon $t = 1d$ (dotted), $t = 1w$ (dashed) and $t = 2w$ (dash-dotted).

(b) $\widehat{V}(u^*, t) - u^*$ divided by the number of miners as a function of that number with $t = 1d$ (dotted), $t = 1w$ (dashed) and $t = 2w$ (dash-dotted).

Figure 5: Ruin probability and expected profit per miner over an exponential time horizon as a function of size of the mining pool for varying time horizon.

Note that the proportional reward system considered here is slightly simplistic, as it does not prevent miners from switching the pool, which can be an issue in practice, see for instance Rosenfeld [19] and Lewenberg et al. [16].

4.2 Expected profit computations for a selfish miner

We now turn to the study of the profitability of selfish mining using model (19). Assuming again that $c = p \times \pi_W \times W$, the net profit condition (23) is satisfied if the electricity price is bounded by

$$\pi_W \leq \frac{b\lambda}{pW} \frac{qp(1-p)^2 + 4p^2 - 2p^3}{1 + 2p - p^2},$$

where p denotes the hashpower and q is the connectivity parameter. Figure 6 displays the net profit condition frontier as a function of hashpower and electricity price for various values of q. For instance, one can read off from the plot that for a connectivity parameter $q = 0.5$ and hashpower $p = 0.1$ the net profit condition is satisfied whenever $\pi_W \leq 0.43$. Note that the net profit condition for $q = 1$ is identical to that of a miner following the protocol, since it refers to the stationary distribution (cf. Remark 3.2 for further details).

Figure 7 compares the ruin probability and expected profit of a selfish miner (as determined by Theorem B.1) and a miner following the protocol, plotted as a function of initial

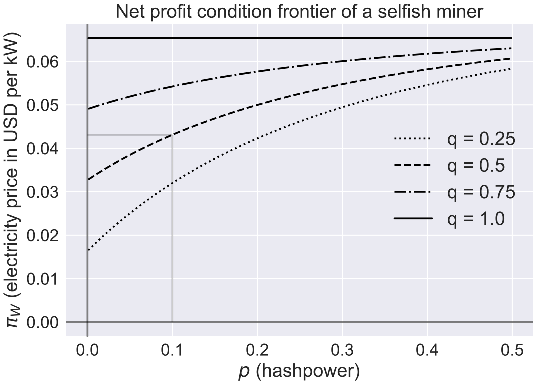
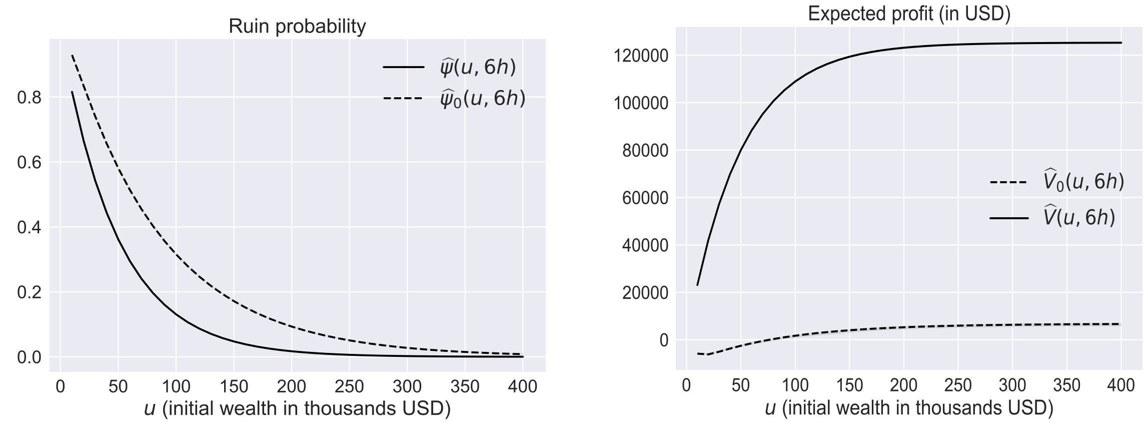


Figure 6: Net profit condition frontier of a selfish miner as a function of electricity price and hashpower for various values of the connectivity parameter q.

wealth for $q = 0.5$, $p = 0.1$ and $\pi_W = 0.04$ (so the net profit condition holds, cf. Figure 6). Here the exponential time horizon is chosen to have a mean of 6 hours. The plot also gives



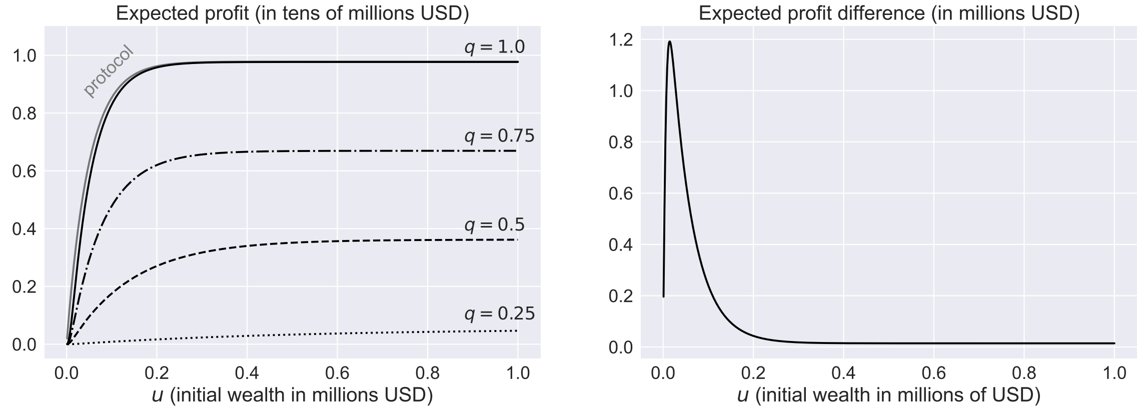
(a) $\widehat{\psi}(u,t)$ (solid) and $\widehat{\psi}_0(u,t)$ (dashed) as a function of initial wealth u.

(b) $\widehat{V}(u,t) - u$ (solid) and $\widehat{V}_0(u,t) - u$ (dashed) as a function of initial wealth u.

Figure 7: Ruin probability and expected profit over an exponential time horizon $T \sim \text{Exp}(6h)$ as a function of initial wealth for a miner following the protocol and for a selfish miner with electricity price $\pi_W = 0.04$, hashpower $p = 0.1$, and connectivity $q = 0.5$, together with the confidence bands of a Monte Carlo simulation.

(the very narrow) 95% confidence bands of an independent Monte Carlo simulation with 250'000 sample paths for $\widehat{\psi}_0(u)$ and $\widehat{V}_0(u,t)$, which nicely shows that the exact formulas are within these bounds. Note the substantial gap between the honest and the selfish miner's ruin probability in Figure 7a and expected profit in Figure 7b.

Let us now look into the impact of the connectivity on the expected profit of a selfish miner. The connectivity depends on the topography of the network as well as on the information propagation delay between the nodes. Göbel et al. [7] showed that the connectivity strongly influences the relative revenue of selfish miners. Figure 8 investigates the impact of q on the absolute revenue of a selfish miner. In Figure 8a, we plot $\widehat{V}_0(u,t)-u$ as a function of initial wealth u for various levels of q (the choice of the other parameters ensures that the net profit condition holds even under the lowest connectivity regime $q = 0.25$). The plot also confirms the relative proximity of the value functions when following the protocol and when withholding blocks with connectivity $q = 1$, respectively (cf. Remark 3.2). However, for small values of u the difference can still be substantial in absolute terms, see Figure 8b where we plot the difference $\widehat{V}(u,t) - \widehat{V}_0(u,t)$ directly.



(a) $\widehat{V}_0(u,2w)-u$ as a function of initial wealth u with haspower $p = 0.1$ and electricity price $\pi_W = 0.03$ for varying connectivity level: $q = 0.25$ (dotted), $q = 0.5$ (dashed), $q = 0.75$ (dash-dotted), $q = 1$ (solid).

(b) $\widehat{V}(u,2w) - \widehat{V}_0(u,2w)$ as a function of initial wealth u with hashpower $p = 0.1$, electricity price $\pi_W = 0.03$ and connectivity $q = 1$.

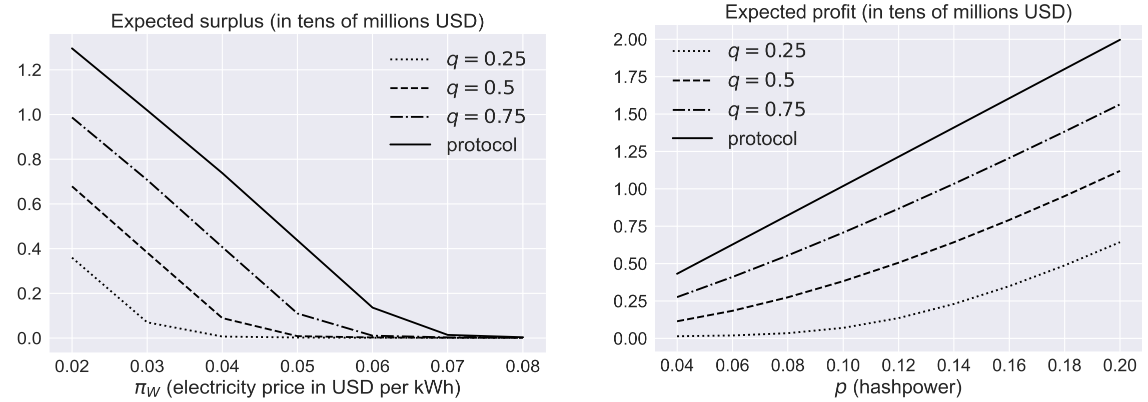
Figure 8: Expected profit of a selfish miner over an exponential time horizon (mean 2 weeks) as a function of initial wealth (left) compared to the expected profit of a miner following the protocol (right).

Figure 9a plots the expected surplus under ruin constraints as a function of the electricity price, and in Figure 9b we see how the choice of the hashpower influences the expected profit $\widehat{V}_0(u,t) - u$ of a selfish miner.

We observe that the influence of the initial wealth, electricity price and hashpower on the expected profit of a selfish miner is similar (in terms of shape) to that of a miner following the protocol, but – compared in absolute terms – withholding blocks leads to substantial losses in expected profit even in high connectivity regimes like $q = 0.75$. This confirms that a miner is better off by following the protocol in terms of 'absolute' (as opposed to 'relative' in Eyal and Sirer [6]) revenue under solvency constraints. In Section 5, we will check whether this also holds true when taking into account an adjustment in the cryptopuzzle difficulty.

4.3 Comparison with the original selfish mining strategy

The selfish mining strategy considered in this work differs from the selfish mining strategy introduced by Eyal and Sirer [6], cf. Remark 3.1. This section is devoted to the numerical



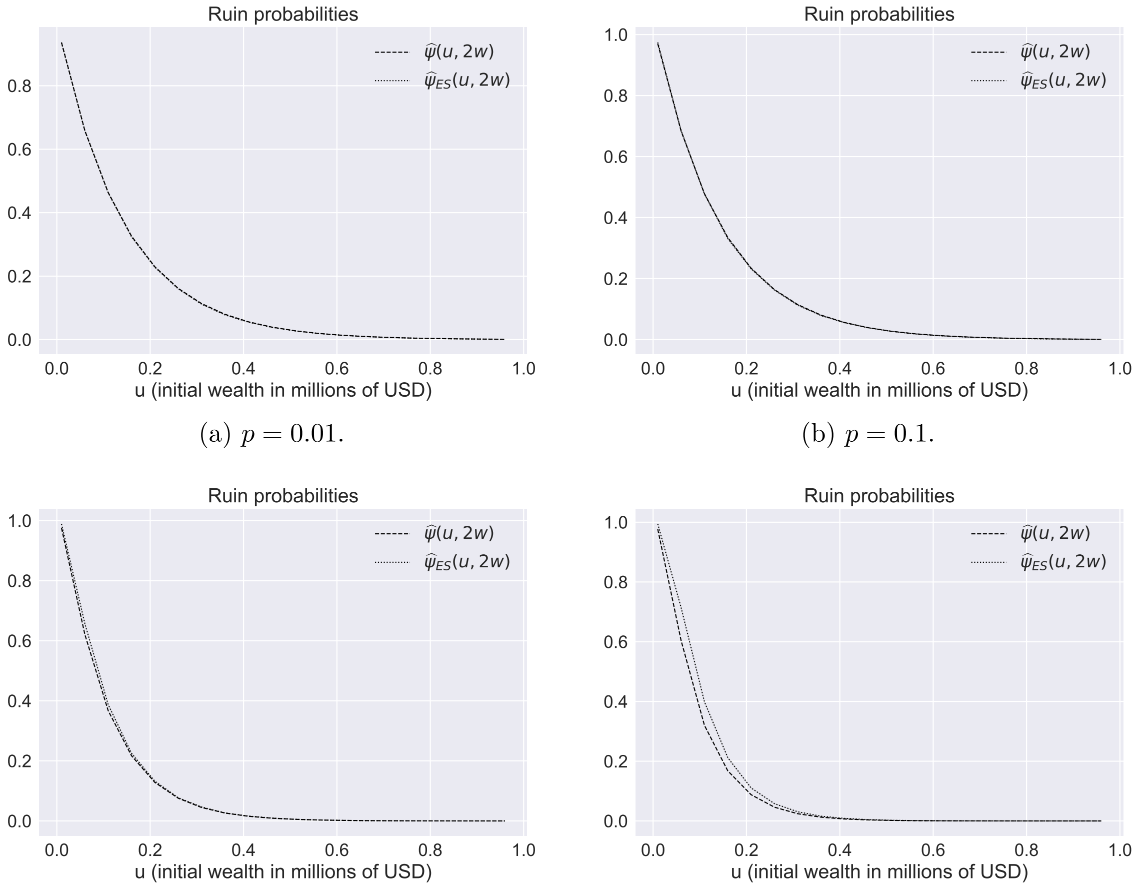
(a) $\widehat{V}_0(u, 2w)$ as a function of electricity price π_W with hashpower $p = 0.1$ and initial wealth $u = \$410,000$.

(b) $\widehat{V}_0(u, 2w) - u$ as a function of hashpower p with electricity price $\pi_W = 0.03$ and initial wealth $u = \$410,000$.

Figure 9: Expected profit of a selfish miner over an exponential time horizon (mean 2 weeks) as a function of electricity price (left) and hashpower (right) for varying connectivity level q, and a comparison with a miner following the protocol (solid).

comparison in terms of ruin probability and expected profit of the two strategies. As for Eyal and Sirer's selfish mine strategy there are no analytical formulas available, we will use crude Monte Carlo estimators in that case. We set the time horizon to $t = 336$ (two weeks) and let the hashpower vary in $p \in \{0.01, 0.1, 0.25, 0.4\}$. Figure 10 displays the ruin probability of a miner that implements the standard selfish mining strategy $\widehat{\psi}_{\text{ES}}(u, t = 2w)$ and our variant $\widehat{\psi}(u, t = 2w)$. Figure 11 displays the expected profit over an exponential time horizon of a miner that implements the standard selfish mining strategy $\widehat{V}_{\text{ES}}(u, t = 2w)$ and our variant $\widehat{V}(u, t = 2w)$. The results are very close when considering values of hashpower ranging in $p \in \{0.01, 0.1\}$, see Figures 10a,10b, 11a and 11b. At such hashpower levels, the likelihood of building up a large stock of blocks plummets, leading to similar results for both strategies. For larger value of hashpower $p \in \{0.25, 0.4\}$, the ruin probability is a bit higher when implementing Eyal and Sirer's strategy, see Figures 10c and 10d. This is mainly due to the delay in getting the reward when the stock of blocks reaches the level 2 (the reward arises one block later within Eyal and Sirer's framework, see Remark 3.1). When ruin is unlikely, that is for large initial reserves, Eyal and Sirer's strategy outperforms the simplified one, see Figures 11c and 11d. The latter is hence only preferable when ruin poses a real threat. A miner should then empty its stock and cash the rewards to avoid bankruptcy. However, one may also conclude from these plots that the simplified strategy already nicely captures most of the model effects, with the advantage of leading to explicit formulas for the involved quantities.

Remark 4.1. One could argue that the reward for finding a block becomes available to the miner only when the transaction that transfers the reward to the miner's wallet is confirmed. A transaction is not yet confirmed if it belongs to a branch of the blockchain competing with another one, namely when a fork is on-going. If we assume that the funds are not available as long as the fork has not been resolved, then the counterpart of



(a) $p = 0.01$.

(b) $p = 0.1$.

(c) $p = 0.25$.

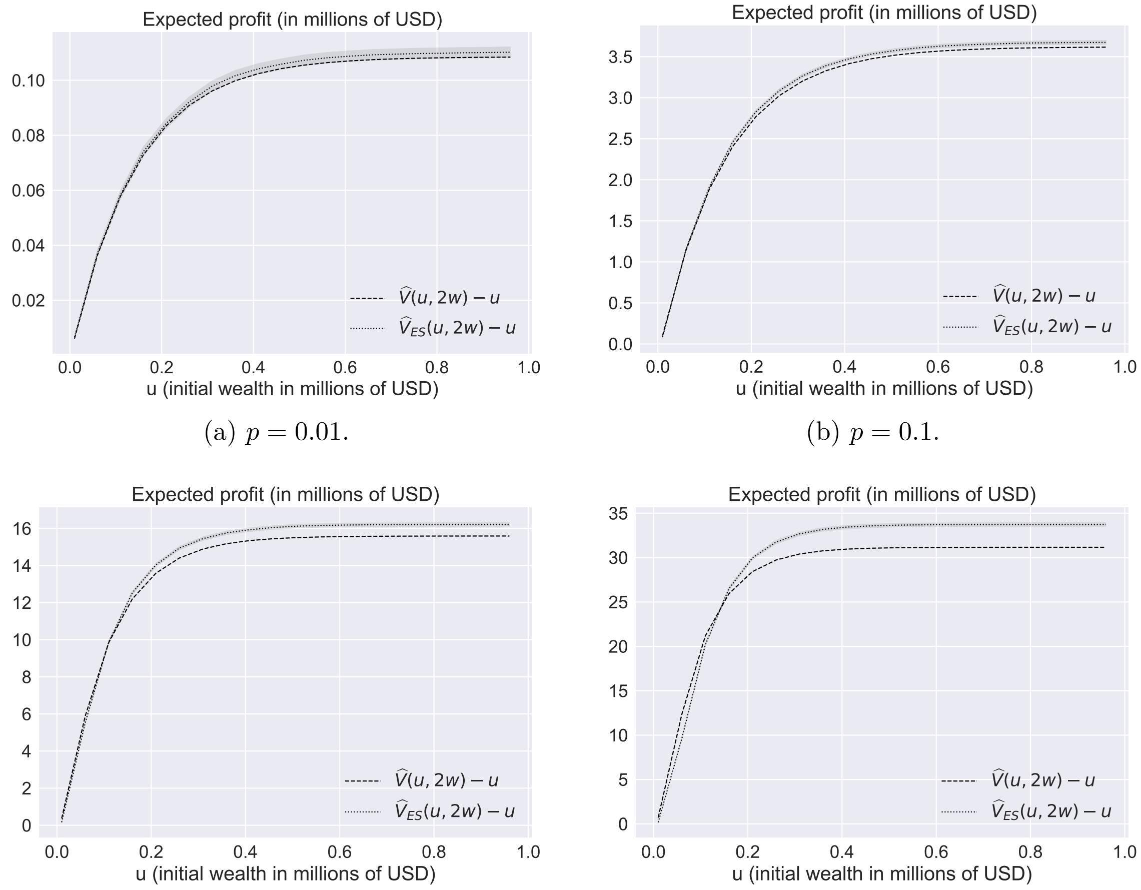
(d) $p = 0.4$.

Figure 10: Ruin probability over an exponential time horizon $T \sim \text{Exp(2w)}$ when implementing Eyal and Sirer selfish mining strategy (dotted) and the simplified one (dashed) for a miner with varying hashpower $p \in \{0.01, 0.1, 0.25, 0.4\}$.

(20) and (21) for the reward function of a miner who implements Eyal and Sirer's selfish mining scheme is

$$f\left[(Z_{n-1}, (\xi_i)_{i\leq n}, \zeta_n\right] = \begin{cases} 0, & \text{if } Z_{n-1} \in \{0, 1\}, \\ \sum_{i=n^*+1}^{n} \xi_i, & \text{if } Z_{n-1} = 2 \ \& \ \xi_n = 0, \\ 0, & \text{if } Z_{n-1} = 2 \ \& \ \xi_n = 1, \\ 0, & \text{if } Z_{n-1} = 0^* \ \& \ \xi_n = 0 \ \& \ \zeta_n = 0, \\ 1, & \text{if } Z_{n-1} = 0^* \ \& \ \xi_n = 0 \ \& \ \zeta_n = 1, \\ 2, & \text{if } Z_{n-1} = 0^* \ \& \ \xi_n = 1, \end{cases} \tag{27}$$

where $n^* = \sup\{k \leq n-1 : \ Z_k = 0\}$. Note that the dependency of the reward process on the current and past values of the sequence $(\xi_n)_{n\geq 1}$ makes it non-Markovian, so that the techniques used in the proof of Theorem B.1 and Corollary C.1 are not applicable. The income processes (21) and (27) lead to the same number of rewards, but the timing is different. Under Eyal and Sirer's assumption, the rewards are staggered in time while they are all earnt whenever the fork situation ends (which means later) in the case of



(a) $p = 0.01$.

(b) $p = 0.1$.

(c) $p = 0.25$.

(d) $p = 0.4$.

Figure 11: Expected profit over an exponential time horizon $T \sim \text{Exp}(2\text{w})$ when implementing Eyal and Sirer selfish mining strategy and the simplified one for a miner with varying hashpower $p \in \{0.01, 0.1, 0.25, 0.4\}$.

(27). The deferral of capital gains in our model jeopardizes the solvency of the miner and reduces the expected profit. The results displayed in Figures 10 and 11 would then look less optimistic by choosing (27) over (21).

5 Expected profit when including a difficulty adjustment

Mining (at least on the bitcoin blockchain) boils down to drawing random numbers, referred to as hashes uniformly inside the set $\{0, \dots, 2^{256} - 1\}$. The block is mined if the computed hash is smaller than some target L. Calibrating L helps to maintain a steady flow of blocks in the blockchain. As each trial (of the system) for mining a block is independent of the others and leads to a success with very small probability, the overall number of successes is binomially distributed and will be very well approximated by a Poisson random variable. Hence the Poisson process assumption for the occurrence of mined blocks is in fact very natural. In the bitcoin blockchain, the target L is set so as to ensure that 6 blocks are generated per hour. The target may be estimated by comparing 2^{256} to the number of hashes computed by the network in ten minutes. On January 1, 2020, the network was computing 97.01[4] exahashes per second. The difficulty is then estimated by $L = 2^{256}/(H/6)$, where $H = 97.01 \times 10^{18} \times 3600$ is the number of hashes computed per hour by the network. The difficulty is adjusted every $2,016$ blocks by changing the target L to

$$L^* = L \times \frac{t^*}{336},$$

where t^* is the time (in hours) it took to mine $2,016$ blocks (here $2016/6 = 336$ hours is the time it should have taken to mine $2,016$ blocks). The difficulty adjustment was studied in Bowden et al. [4] and led them to conclude that the block arrival process is well captured by a non-homogeneous Poisson process. Following their terminology, we refer to the time elapsed between two difficulty adjustments as a *segment*.

We now want to quantitatively address whether selfish mining is worthwhile when considering the possibly implied adjustment of the cryptopuzzle difficulty. We do so in a simplified setup, where only Sam may switch between selfish mining and following the protocol, whereas everyone else follows the protocol. Concretely, we compute the ruin probability and expected profit of Sam over two segments when

(i) he is following the protocol during both segments,

(ii) he applies selfish mining during the first segment and resumes following the protocol during the second segment.

For (i), we compute the expected profit using the result of Proposition 2.2 by setting the average time horizon to $t = 672$ (the number of hours in four weeks). We assume that the arrival intensity of the blocks in the blockchain remains unchanged over the two segments with $\lambda = 6$, as does the cryptopuzzle difficulty L.

For (ii), we proceed as follows. Selfish mining slows down the pace at which the blocks are added to the blockchain, and the number of blocks wasted exactly corresponds to the number of passages of the Markov chain $(Z_n)_{n\geq 0}$ through the state 0^*. We know that once stationarity is reached, the probability for $(Z_n)_{n\geq 0}$ to be in state 0^* is

$$\frac{p(1-p)}{1+2p-p^2}.$$

We therefore approximate the arrival process in this first segment by a homogeneous Poisson process with intensity

$$\lambda_1 = \lambda \times \left(1 - \frac{p(1-p)}{1+2p-p^2}\right).$$

When blocks are being withheld, the average time required to mine $2,016$ blocks increases from 336 to $t_1 = 2016/\lambda_1$. We hence compute the ruin probability and expected surplus over the first segment using Corollary C.1 and Theorem B.1 respectively with time horizon t_1. Selfish mining during the first segment then leads to a downward adjustment of the

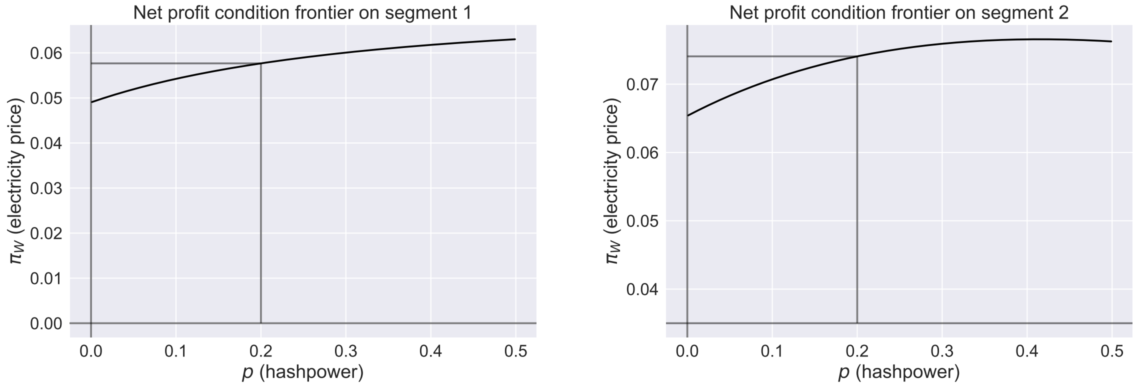
[4] Source: blockchain.com

cryptopuzzle difficulty to $L_2 = L \times t_1/336$ that will be in force during the second segment. As the miner resumes following the protocol on that second segment, the block arrival process becomes again a proper homogeneous Poisson process with intensity λ_2 to be determined as follows. Let H be the number of hashes computed per hour (hashrate) by the network. The number of blocks mined per hour is then given by

$$\lambda_2 = \frac{2^{256}}{L_2 \times H}.$$

The miner's ruin probability and surplus over the second segment are now computed using the formulas of Propositions 2.2 and 2.3 using as initial wealth the miner's expected surplus over the first segment, a block arrival intensity equal to λ_2 and a reduced time horizon equal to $t_2 = 2016/\lambda_2$.

We consider a miner who owns a share $p = 0.2$ of the network computing power. If he follows the protocol, then the net profit condition holds if $\pi_W < 0.065$. If he withholds blocks on the first segment, then the net profit condition frontier depends on the electricity price and the hashpower provided that his connectivity is fixed, for instance set to $q = 0.75$. Figure 12 shows the net profit condition frontiers for a selfish miner on Segment 1 who starts following again the protocol on Segment 2.



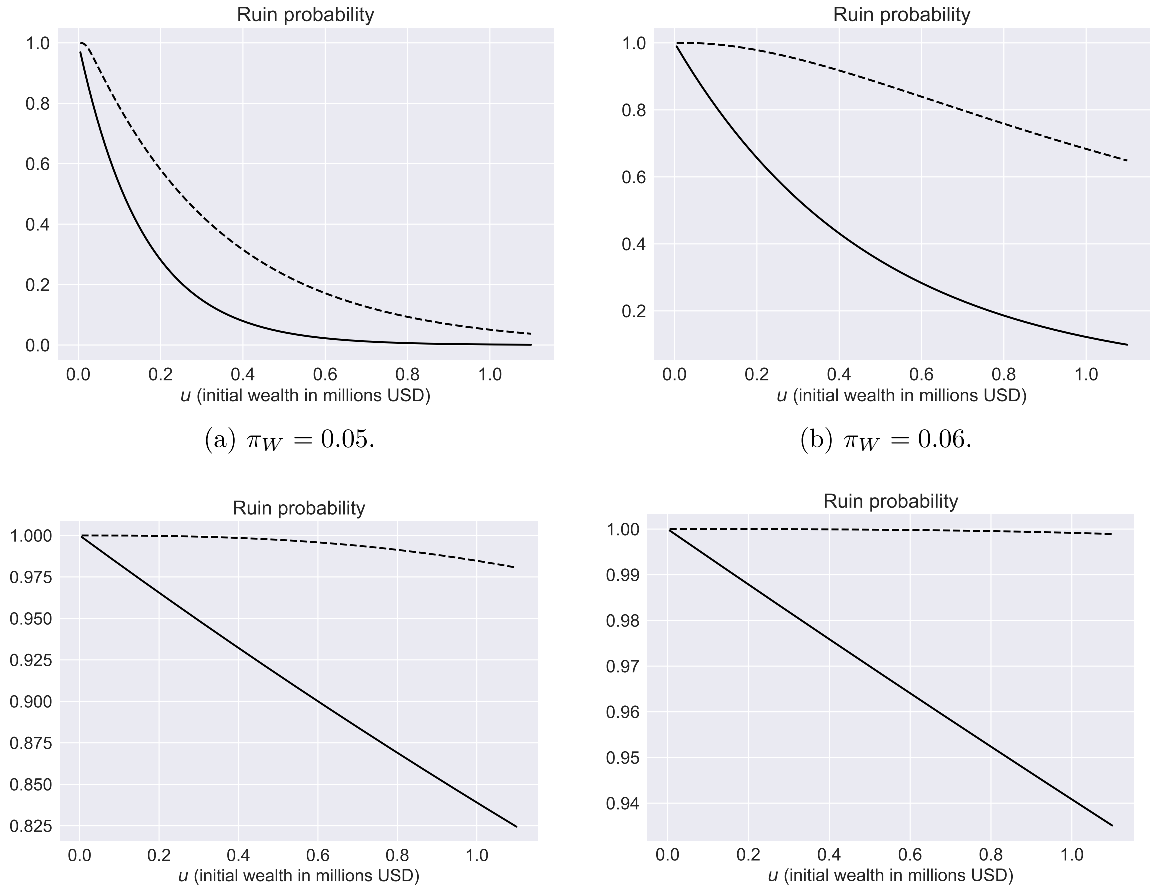
(a) Net profit condition frontier on Segment 1

(b) Net profit condition frontier on Segment 2.

Figure 12: Net profit condition frontier on Segment 1 and 2 for a selfish miner.

In absence of ruin considerations, selfish mining on Segment 1 is profitable only if the price of electricity is lower than 0.058, see Figure 12a. Only when the selfish miner owns the totality of the hashpower, is selfish mining as profitable as following the protocol. On Segment 2, the profitability is always greater than when following the protocol. The profitability on Segment 2 holds in our case if the electricity price is lower than 0.074, see Figure 12b. It is interesting to note that by increasing the hashpower beyond a certain threshold we actually lower the profitability during Segment 2. At higher hashpower levels, the probability of the Markov chain $(Z_n)_{n\geq 0}$ visiting state 0^* becomes small. In that case fewer blocks are being wasted, which in turn reduces the downward adjustment of the cryptopuzzle difficulty and hence the profitability during Segment 2.

Figure 13 shows the ruin probability of a selfish miner and a miner following the protocol as a function of initial wealth for a range of electricity prices. From a ruin probability perspective, reducing the difficulty adjustment does not compensate for the risk involved in implementing selfish mining.



(a) $\pi_W = 0.05$.

(b) $\pi_W = 0.06$.

(c) $\pi_W = 0.07$.

(d) $\pi_W = 0.08$.

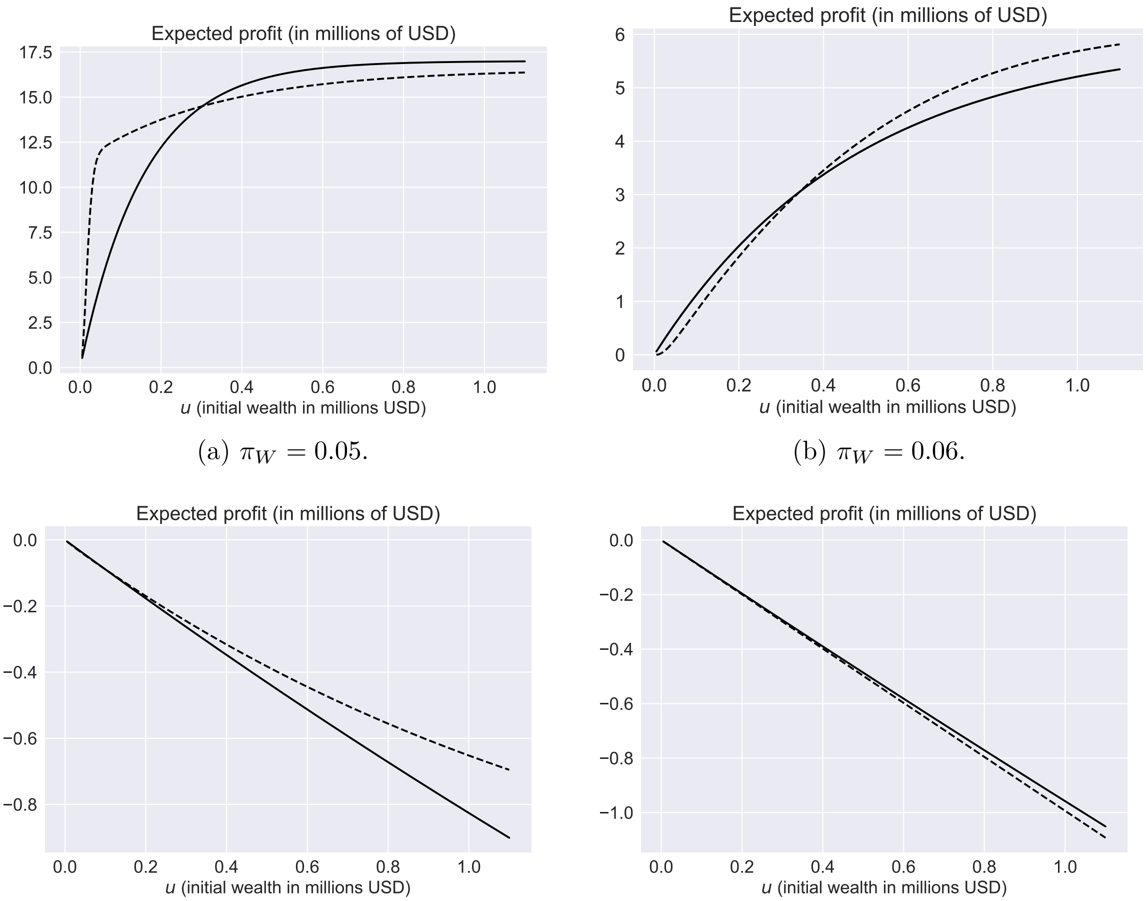
Figure 13: Ruin probability over two segments as a function of initial wealth of a miner following the protocol (solid) and a selfish miner (dashed) for various electricity prices with hashpower $p = 0.2$ and connectivity $q = 0.75$.

Figure 14 displays the expected profit of a selfish miner and a miner following the protocol as a function of initial wealth for a range of electricity prices. One can observe the different profit and loss profile of a selfish miner compared to that of a miner following the protocol on both segments. If the net profit condition holds when following the protocol, then it also holds for the second segment when blocks were withheld during the first segment. For electricity prices $\pi_W = 0.05, 0.06$, the expected profit as a function of u reaches a plateau of level

$$(c - b\lambda p) \times t \tag{28}$$

when following the protocol, and

$$(c - b\lambda_2 p) \times t_2, \tag{29}$$



(a) $\pi_W = 0.05$.

(b) $\pi_W = 0.06$.

(c) $\pi_W = 0.07$.

(d) $\pi_W = 0.08$.

Figure 14: Expected profit over two segments as a function of initial wealth of a miner following the protocol (solid) and a selfish miner (dashed) for various electricity prices with hashpower $p = 0.2$ and connectivity $q = 0.75$.

when selfish mining is applied during the first segment. For $\pi_W = 0.05$, the plateau when following the protocol (28) is higher than the plateau when withholding blocks (29), but the expected profit at lower initial wealth is greater for the selfish miner, see Figure 14a. The exact opposite holds when $\pi_W = 0.06$, see Figure 14b. The latter is probably the most desirable situation for a selfish miner. For $\pi_W = 0.07$, the net profit condition no longer holds when following the protocol which entails a loss, it holds however on the second segment of the selfish miner but it does not compensate for the loss incurred during the first segment, see Figure 14c. Selfish mining helps at least in slightly mitigating the losses in this case. For electricity prices $\pi_W > 0.074$, the net profit condition breaks down in each case, resulting in huge losses for both the selfish and the honest miner (cf. Figure 14d).

The above analysis allowed us to distinguish situations where selfish mining can be considered worthwile and when it may not. In particular, it turns out that selfish mining can be advisable when following the protocol is not profitable.

6 Conclusion

In this paper we proposed a risk and profitability analysis framework adapted to the profit and loss profile of blockchain miners. The surplus of the miners is modelled as a stochastic process akin to the risk process in insurance risk theory. In addition to studying the standard ruin probability, we have defined a value function as the expected surplus over an exponentially distributed time horizon. This assumption allowed us to work out closed form expressions for the expected profit of a miner that follows the prescribed protocol, and of a miner who seeks to optimize his expected profit by withholding blocks. The explicit solutions enabled a sensitivity analysis with respect to the model parameters and features, and a profitability comparison between the two types of miners.

We find that mining is a business for risk lovers as large expected profits are compensated by great odds of running out of financial resources. While earlier studies suggested that selfish mining can be worthwhile, our analysis gives a quantitative description of the significantly increased risk caused by the delay of capital gains, so that in an analysis that includes the consideration of ruin, selfish mining becomes less attractive. At the same time, we find that selfish mining can be a reasonable strategy if following the protocol is not profitable.

The main purpose of the present study was to provide a concrete link between the analysis of mining strategies and modelling tools in applied probability and mathematics. There are of course various directions for future research concerning refinements and extensions of the approach proposed here. It will be interesting in future studies to account for the variability of the electricity cost over time and the even higher variability of the miner's reward due to the well known volatility of the Bitcoins. The incorporation of transaction fees will also become more relevant in the future as the reward for finding blocks keeps being halved as the number of remaining Bitcoins to be issued declines. In addition, it would be nice to look into further consequences of selfish mining on the remaining network participants beyond the ones considered here.

We have found that deferring the reward associated with newly found blocks puts the miners' solvency at risk. This motivates a stochastic control problem for a miner to decide whether to hide or release a block depending on the current financial situation. The approach of Sapirshtein et al. [21] could then be re-examined within the framework of the present paper. Finally, the organization of selfish mining in pools may lead to additional features beyond the ones considered in the present approach.

A Abel-Gontcharov polynomials

Let $U = \{u_i\ ,\ i \geq 1\}$ be a sequence of real non-decreasing numbers. The (unique) family $\{G_n(x|U)\ ,\ n \geq 0\}$ of *Abel-Gontcharov polynomials* of degree n in x attached to U is defined as follows. Starting with $G_0(x|U) = 1$, the polynomials $G_n(x|U)$ satisfy the differential equations

$$G_n^{(1)}(x|U) = n\, G_{n-1}(x|\mathcal{E}U), \tag{30}$$

where $\mathcal{E}U$ is the shifted family $\{u_{i+1}\ , i \geq 1\}$, and with boundary conditions

$$G_n(u_1|U) = 0, \quad n \geq 1. \tag{31}$$

So, each G_n, $n \geq 1$, has the integral representation

$$G_n(x|U) = n! \int_{u_1}^{x} \left[\int_{u_2}^{y_1} \mathrm{d}y_2 \ldots \int_{u_n}^{y_{n-1}} \mathrm{d}y_n \right] \mathrm{d}y_1. \tag{32}$$

The polynomials G_n, $n \geq 1$, can be interpreted in terms of the joint distribution of the order statistics $(U_{1:n}, \ldots, U_{n:n})$ of a sample of n independent uniform random variables on $(0,1)$. Indeed, for $0 \leq x \leq u_1 \leq \ldots \leq u_n \leq 1$, we have that

$$P[U_{1:n} \leq u_1, \ldots, U_{n:n} \leq u_n \text{ and } U_{1:n} \geq x] = (-1)^n\, G_n(x|u_1, \ldots, u_n).$$

This last interpretation is used in the proof of Proposition 2.1. The numerical evaluation of (7) then relies on the recursive relations

$$G_n(x|U) = x^n - \sum_{k=0}^{n-1} \binom{n}{k} u_{k+1}^{n-k} G_k(x|U), \quad n \geq 1. \tag{33}$$

Formula (33) follows from an Abelian expansion of x^n based on (30), and (31). For further details we refer to Lefèvre and Picard [15], where also applications in risk and epidemic modelling are given.

B Proof of Theorem B.1

Theorem B.1. *For any $u \geq 0$, the value function under selfish mining as defined in* (24) *satisfies the differential equation* (45) *with boundary conditions* (43) *and* (44)*, a solution of which is given by*

$$\widehat{V}_0(u,t) = A_1\, \mathrm{e}^{\rho_1 u} + \mathrm{e}^{\rho_2 u} \left[A_2\, \cos(\rho_3 u) + A_3\, \sin(\rho_3 u) \right] + u + C, \tag{34}$$

where ρ_1 and $\rho_2 \pm i\rho_3$ are the only solutions in ρ of the equation

$$(D_1\, \rho + D_2)\, \mathrm{e}^{2\,\rho\, b} + D_3\, \mathrm{e}^{\rho\, b} = D_4\, \rho^3 + D_5\, \rho^2 + D_6\, \rho + D_7 \tag{35}$$

with negative real parts. The constants $C, D_1, \ldots, D_7$ are given by

$$\begin{aligned} C &= -\frac{\lambda^2 t^3 \left\{ \lambda p b \left[(q-2)\, p^2 + (4 - 2\,q)\, p + q \right] + c\,(p^2 - 2\,p - 1) \right\}}{\lambda^2 t^2\,(p^2 - 2\,p - 1) - (p+2)\,\lambda\, t - 1} \\ &\quad - \frac{\lambda\, t^2\ (2bp^2\lambda - c\,(p+2)) - ct}{\lambda^2 t^2\,(p^2 - 2\,p - 1) - (p+2)\,\lambda\, t - 1} \end{aligned} \tag{36}$$

$$D_1 = \frac{pc}{1-p},\ D_2 = \frac{p\,(1 + t\,(2-p)\,\lambda)}{t\,(1-p)},\ D_3 = (1-p)\,\lambda\, q,\ D_4 = \frac{c^3}{\lambda^2\,(1-p)\,p},$$

$$D_5 = \frac{c^2\,(3 + \lambda\, t\,(p+2))}{\lambda^2 t\,(1-p)\,p},\ D_6 = \frac{(3 + \lambda\, t\,(2p+1))\, c\,(\lambda\, t + 1)}{t^2 \lambda^2\,(1-p)\,p},\ \textit{and}$$

$$D_7 = \frac{1 + \lambda\, t\,(p+2) + \lambda^2 t^2\,(2p+1) + \lambda^3 t^3 p\,(p(1-q)(2-p) + q)}{\lambda^2 t^3\,(1-p)\,p}.$$

The constants A_1, A_2 and A_3 are the solution of the linear equation system

$$\begin{pmatrix} 1 & 1 & 0 \\ \rho_1 & \rho_2 & \rho_3 \\ B_1 & B_2 & B_3 \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ A_3 \end{pmatrix} = \begin{pmatrix} -C \\ -1 \\ -2b - C - \frac{1}{ct} \end{pmatrix}, \tag{37}$$

with

$$\begin{aligned} B_1 &= -\rho_1^2 + \lambda^2 p^2 \, e^{2b\rho_1}/c^2, \\ B_2 &= -\rho_2^2 + \rho_3^2 + \lambda^2 p^2 \, e^{2b\rho_2} \cos(2b\rho_3)/c^2, \\ B_3 &= -2\rho_2\rho_3 + \lambda^2 p^2 \, e^{2b\rho_2} \sin(2b\rho_3)/c^2. \end{aligned} \tag{38}$$

Using the same reasoning as in the proof of Proposition 2.2 yields the following system of advanced differential equations

$$\begin{cases} 0 = & c\widehat{V}_0'(u,t) + (\lambda p + 1/t)\widehat{V}_0(u,t) - \lambda p \widehat{V}_1(u,t) - u/t, \\ 0 = & c\widehat{V}_1'(u,t) + (\lambda + 1/t)\widehat{V}_1(u,t)) - \lambda p \widehat{V}_0(u+2b,t) - \lambda(1-p)\widehat{V}_{0^*}(u,t) - u/t, \\ 0 = & c\widehat{V}_{0^*}'(u,t) + (\lambda + 1/t)\widehat{V}_{0^*}(u,t) - \lambda p \widehat{V}_{0^*}(u+2b,t) - \lambda(1-p)q\widehat{V}_{0^*}(u+b,t) \\ & -\lambda(1-p)(1-q)\widehat{V}_0(u,t) - u/t. \end{cases} \tag{39}$$

Here again the derivative is always with respect to the first argument. From the first equation we deduce that

$$\widehat{V}_1(u,t) = \frac{c}{\lambda p}\widehat{V}_0'(u,t) + \frac{\lambda p + 1/t}{\lambda p}\,\widehat{V}_0(u,t) - \frac{u}{t\lambda p}. \tag{40}$$

Inserting (40) into the second equation of the system (39) yields

$$\begin{aligned} \widehat{V}_{0^*}(u,t) &= \frac{c}{\lambda(1-p)}\widehat{V}_1'(u,t) + \frac{\lambda + 1/t}{\lambda(1-p)}\widehat{V}_1(u,t) - \frac{\lambda p}{\lambda(1-p)}\widehat{V}_1(u+2b,t) \\ &\quad - \frac{u}{\lambda(1-p)t} \\ &= \frac{c^2}{\lambda^2\,(1-p)\,p}\widehat{V}_0''(u,t) + \frac{c\,(2+(p+1)\,\lambda\,t)}{\lambda^2\,(1-p)\,tp}\widehat{V}_0(u,t) \\ &\quad + \frac{(\lambda\,t+1)\,(\lambda\,t\,p+1)}{\lambda^2\,(1-p)\,t^2 p}\widehat{V}_0(u,t) - \frac{p}{1-p}\widehat{V}_0(u+2b,t) \\ &\quad - \frac{1+\lambda\,t\,(p+1)}{\lambda^2\,(1-p)\,t^2 p}u - \frac{c}{\lambda^2\,(1-p)\,tp}, \end{aligned} \tag{41}$$

with boundary conditions $\widehat{V}_0(0,t) = \widehat{V}_1(0,t) = \widehat{V}_{0^*}(0,t) = 0$. Substituting (41) into the third equation of the system (39) then yields an advanced differential equation for $\widehat{V}_0(u,t)$

with

$$\begin{aligned}
0 \;=\;& \frac{c^3}{\lambda^2\,(1-p)\,p}\widehat{V}_0'''\,(u,t)+\frac{(3+\lambda\,t\,(p+2))\,c^2}{\lambda^2 t\,(1-p)\,p}\widehat{V}_0''(u,t)\\
&+\frac{(\lambda\,t+1)\,c\,(3+\lambda\,t\,(2p+1))}{\lambda^2t^2\,(1-p)\,p}\widehat{V}_0'(u,t)\\
&+\frac{1+\lambda\,t\,(p+2)+\lambda^2t^2\,(2p+1)+\lambda^3t^3p\,((q-1)\,p^2+2p\,(1-q)+q)}{t^3\lambda^2\,(1-p)\,p}\widehat{V}_0\,(u,t)\\
&-\lambda\,q\,(1-p)\,\widehat{V}_0\,(u+b,t)+\frac{(\lambda\,t\,(p-2)-1)\,p}{(1-p)\,t}\widehat{V}_0(u+2b,t)\\
&-\frac{cp}{1-p}\widehat{V}_0'\,(u+2\,b,t)-\frac{1+\lambda\,t\,(p+2)-\lambda^2t^2\,(p^2-2\,p-1)}{t^3\lambda^2\,(1-p)\,p}u\\
&-\frac{(2+\lambda\,t\,(p+2))\,c}{\lambda^2t^2\,(1-p)\,p}.
\end{aligned}\tag{42}$$

The above boundary conditions now translate to

$$\widehat{V}_0(0,t)=0,\ \widehat{V}_0'(0,t)=0 \text{ and } \widehat{V}_0''(0,t)=\frac{\lambda^2p^2}{c^2}\widehat{V}_0(2b,t)+\frac{1}{ct},\tag{43}$$

and from the problem construction we again have the linear growth condition

$$\widehat{V}_0(u,t)\le ku \qquad \text{for some } k\ge 0.\tag{44}$$

This equation constitutes another instance of an advanced functional differential equation, and concerning mathematical considerations of the existence and uniqueness of a solution to it, we refer to the corresponding comments in Remark B.1, where here we even have the additional complication of order 3. We will again construct its solution explicitly (one can again confirm that the solution is the correct one by comparing it to the outcome of a stochastic simulation of $V_0(u)$). Concretely, we seek a solution of the form $\widehat{V}_0(u,t)=\widehat{V}_0^{\text{part}}(u,t)+\widehat{V}_0^{\text{hom}}(u,t)$, where $\widehat{V}_0^{\text{part}}(u,t)$ is a particular solution of (42) and $\widehat{V}_0^{\text{hom}}(u,t)$ solves the homogeneous equation associated to (42)

$$\begin{aligned}
0 \;=\;& \frac{c^3}{\lambda^2\,(1-p)\,p}\widehat{V}_0'''\,(u,t)+\frac{(3+\lambda\,t\,(p+2))\,c^2}{\lambda^2 t\,(1-p)\,p}\widehat{V}_0''(u,t)\\
&+\frac{(\lambda\,t+1)\,c\,(3+\lambda\,t\,(2p+1))}{\lambda^2t^2\,(1-p)\,p}\widehat{V}_0'(u,t)\\
&+\frac{1+\lambda\,t\,(p+2)+\lambda^2t^2\,(2p+1)+\lambda^3t^3p\,((q-1)\,p^2+2p\,(1-q)+q)}{t^3\lambda^2\,(1-p)\,p}\widehat{V}_0\,(u,t)\\
&-\lambda\,q\,(1-p)\,\widehat{V}_0\,(u+b,t)+\frac{(\lambda\,t\,(p-2)-1)\,p}{(1-p)\,t}\widehat{V}_0(u+2b,t)\\
&-\frac{cp}{1-p}\widehat{V}_0'\,(u+2\,b,t)\,.
\end{aligned}\tag{45}$$

Inserting a particular solution of the form $\widehat{V}_0^{\text{part}}(u,t)=Bu+C$ in (42) yields $B=1$ and

$$\begin{aligned}
C \;=\;& -\frac{\lambda^2t^3\left\{\lambda pb\left[(q-2)\,p^2+(4-2\,q)\,p+q\right]+c\,(p^2-2\,p-1)\right\}}{\lambda^2t^2\,(p^2-2\,p-1)-(p+2)\,\lambda\,t-1}\\
&-\frac{\lambda\,t^2\,\left(2bp^2\lambda-c\,(p+2)\right)-ct}{\lambda^2t^2\,(p^2-2\,p-1)-(p+2)\,\lambda\,t-1}.
\end{aligned}$$

Trying the ansatz $\widehat{V}(u,t) = e^{\rho u}$ in the homogeneous equation (45), we get the characteristic equation

$$(D_1\,\rho + D_2)\,\mathrm{e}^{2\,\rho\,b} + D_3\,\mathrm{e}^{\rho\,b} = D_4\,\rho^3 + D_5\,\rho^2 + D_6\,\rho + D_7, \tag{46}$$

for ρ, where

$$\begin{aligned}
D_1 &= \frac{pc}{1-p} \geq 0,\ D_2 = \frac{p\,(1+\lambda\,t\,(2-p))}{t\,(1-p)} \geq 0,\ D_3 = (1-p)\,\lambda\,q \geq 0,\\
D_4 &= \frac{c^3}{\lambda^2\,(1-p)\,p} \geq 0, \quad D_5 = \frac{c^2\,(3+\lambda\,t\,(p+2))}{t\lambda^2\,(1-p)\,p} \geq 0,\\
D_6 &= \frac{(3+\lambda\,t\,(2p+1))\,c\,(\lambda\,t+1)}{t^2\lambda^2\,(1-p)\,p} \geq 0 \quad \text{and}\\
D_7 &= \frac{1+\lambda\,t\,(p+2)+\lambda^2t^2\,(2p+1)+\lambda^3t^3p\,(p(1-q)(2-p)+q)}{\lambda^2t^3\,(1-p)\,p} \geq 0.
\end{aligned}$$

Note that due to the linear growth condition for $\widehat{V}_0(u,t)$ in u, any candidate for ρ needs to have negative real part. In fact, in the following lemma we will prove that (46) has exactly three such solutions with negative real part.

Lemma B.1. *For any choice of parameters $\lambda, c, b, t > 0$ and $0 < p, q < 1$, Equation* (46) *has exactly three solutions in ρ with negative real part, one of which is real-valued.*

Proof. Define the functions

$$f(\rho) = D_4\,\rho^3 + D_5\,\rho^2 + D_6\,\rho + D_7 \text{ and } g(\rho) = (D_1\,\rho + D_2)\,\mathrm{e}^{2\,\rho\,b} + D_3\,\mathrm{e}^{\rho\,b},$$

and note that both are holomorphic in the complex plane. We will first show that all three zeros of $f(\rho)$ in the complex plane have negative real part. Define a closed curve K by considering the arc $[-iR, +iR]$ on the imaginary axis together with the semi-circle of radius R to the left of it that is centered in zero, with $R \to \infty$. Going on the semi-circle from iR to $-iR$, the term $D_4\,\rho^3$ dominates the value of f, and $f(\rho)$ winds 1.5 times around the origin on the way (from $D_4(ix)^3 = -iD_4x^3$ to $D_4(-ix)^3 = +iD_4x^3$ for $x \in \mathbb{R}$). For the part of K on the imaginary axis we have

$$f(ix) = D_7 - D_5x^2 + i(D_6x - D_4x^3), \quad x \in \mathbb{R}. \tag{47}$$

As x goes from $-\infty$ to $+\infty$, the real part of (47) becomes positive at $x_1 = -\sqrt{D_7/D_5}$ and again negative at $x_2 = \sqrt{D_7/D_5}$, and the imaginary part of (47) is negative for x_1 and positive for x_2 if and only if

$$D_4D_7 < D_5D_6.$$

But the latter condition holds for any choice of parameters $\lambda, c, b, t > 0$ and $0 < p, q < 1$, which can be checked with a little algebra (in fact, writing $D_5D_6 - D_4D_7$ as a polynomial in the argument λt, one can verify that all the coefficients of that polynomial are positive). Due to $D_4(ix)^3 = -iD_4x^3$, this then means that 1.5 further windings are added on the part of K on the imaginary axis, so that altogether we have 3 windings around the origin when going along K. By Cauchy's argument principle for holomorphic functions, we hence have established that $f(\rho)$ has three zeros in the negative halfplane.

In order to extend this result now to $f(\rho) - g(\rho)$ also having exactly three zeros in the negative halfplane, we invoke Rouché's theorem. The latter guarantees the same number of zeroes for $f(\rho)$ and $f(\rho) - g(\rho)$ inside the closed curve K, if

$$|-g(\rho)| < |f(\rho)| \tag{48}$$

for all ρ on the curve K. On the semi-circle, (48) is clear due to the dominance of $D_4\,\rho^3$ as $R \to \infty$. This is likewise true for the part of K on the imaginary axis for sufficiently large R, so that we are only left to deal with $\rho \in [-iR, iR]$ for not so large R. Note that

$$g(ix) = D_3\cos(xb) + D_2\cos(2xb) - D_1 x\sin(2xb) + i(D_1 x\cos(2xb) + D_2\sin(2xb) + D_3\sin(xb))$$

for any $x \in \mathbb{R}$. Together with (47), the condition (48) now translates into

$$\begin{aligned}(D_1 x\cos(2xb) + D_2\sin(2xb) + D_3\sin(xb))^2 + (D_3\cos(xb) + D_2\cos(2xb) - D_1 x\sin(2xb))^2 \\ < (D_7 - D_5 x^2)^2 + (D_6 x - D_4 x^3)^2\end{aligned} \tag{49}$$

for all $x \in \mathbb{R}$. Observe that both sides of (49) are symmetric around $x = 0$. The right-hand side of (49) can be written as

$$D_7^2 + (D_6^2 - 2D_5D_7)x^2 + (D_5^2 - 2D_4D_6)x^4 + D_4^2x^6.$$

and the left-hand side of (49) has the following expansion around zero

$$(D_2 + D_3)^2 + (D_1^2 - 2bD_1D_3 - b^2D_2D_3)\,x^2 + O(x^4).$$

In order to show $D_7 > D_2 + D_3$, one writes $D_7 - D_3 - D_2$ again as a polynomial in the argument λt and can then verify that all coefficients of that polynomial are positive. In a similar way, one can show that $D_6^2 > 2D_5D_7$ and $D_5^2 > 2D_4D_6$ as well as $D_5^2 - 2D_4D_6 > D_1^2 - 2bD_1D_3 - b^2D_2D_3$ for all $b > 0$. One then sees that (49) indeed holds for all $x \in \mathbb{R}$, so that (48) applies and we have established the existence of exactly three zeros of (46) in the negative halfplane.

It only remains to show that exactly one of these zeros is real-valued. In fact, g is positive and monotone increasing with $\lim\limits_{\rho\to-\infty} g(\rho) = 0$ and $\lim\limits_{\rho\to+\infty} g(\rho) = +\infty$. On the other hand, with $D_4 > 0$ we see that $\lim\limits_{\rho\to-\infty} f(\rho) = -\infty$ and $\lim\limits_{\rho\to+\infty} f(\rho) = +\infty$. The derivative of f

$$f'(\rho) = 3D_4\rho^2 + 2D_5\rho + D_6$$

is a polynomial of degree 2 with two negative real roots

$$r_1 = -\frac{1}{ct} - \frac{\lambda}{c} \text{ and } r_2 = -\frac{1}{ct} - \frac{\lambda}{c}\frac{2\,p+1}{3} > r_1.$$

Since

$$f(r_1) = -\,(1-q)\,(1-p)\,\lambda \le 0 \text{ and } f(r_2) = -\,\frac{(-27\,pq + 23\,p + 4)\,(1-p)\,\lambda}{27p} \le 0,$$

the function f is negative for $\rho \leq r_2$ and cannot intersect with g there. At the same time,

$$f(0) - g(0) = \frac{1 + t^2\left(-p^2 + 2\,p + 1\right)\lambda^2 + t\,(p+2)\,\lambda}{\lambda^2\,(1-p)\,pt^3} \geq 0,$$

which implies the existence of a unique negative $\rho_1 \in (r_2, 0)$ such that $f(\rho_1) = g(\rho_1)$ (there must also exist some real solution $\rho > 0$ to (46) as g grows to infinity faster than f, but a positive solution is not relevant here). Since $f(\overline{\rho}) = \overline{f(\rho)}$ and $g(\overline{\rho}) = \overline{g(\rho)}$, where $\overline{z}$ denotes the complex conjugate, for every non-real zero ρ its complex conjugate $\overline{\rho}$ also must be a zero, so that the second and third root of (46) are complex conjugates $\rho_2 \pm i\rho_3$. □

The solution of the homogeneous equation is then of the form

$$\widehat{V}_0^{\text{hom}}(u,t) = A_1\,\mathrm{e}^{\rho_1\,u} + \mathrm{e}^{\rho_2\,u}\left[A_2\,\cos\left(\rho_3\,u\right) + A_3\,\sin\left(\rho_3\,u\right)\right], \tag{50}$$

which together with the particular solution $\widehat{V}_0^{\text{part}}$ provides the generic solutions of the equation (42) with

$$\widehat{V}_0(u,t) = A_1\,\mathrm{e}^{\rho_1\,u} + \mathrm{e}^{\rho_2\,u}\left[A_2\,\cos\left(\rho_3\,u\right) + A_3\,\sin\left(\rho_3\,u\right)\right] + bu + C. \tag{51}$$

Finally, the boundary conditions (43) lead, after some algebra, to the system of equations (37) for the determination of A_1, A_2 and A_3. □

Remark B.1. *Like for Proposition 2.2 (see Remark 2.1), the uniqueness of the solution to advanced functional differential equation* (45) *derived above is not evident from the type of given boundary conditions. Equation* (45) *involves two advanced arguments at $u + b$ and $u + 2b$. Formally, one can correspondingly require that*

$$\mathbb{E}\left(R_T \mathbb{I}_{\tau_u > T}\middle| Z_0 = z\right) = A_1\,\mathrm{e}^{\rho_1\,u} + \mathrm{e}^{\rho_2\,u}\left[A_2\,\cos\left(\rho_3\,u\right) + A_3\,\sin\left(\rho_3\,u\right)\right] + u + C$$

holds for $u \in [0, 2b]$ as an additional boundary condition to ensure that (24) *and* (34) *coincide. One can then for instance confirm that the proposed solution is the correct one by verifying the additionally imposed boundary condition with the outcome of a stochastic simulation of $V_0(u)$ over $u \in [0, 2b]$ (which we did for various choices of parameters). In any case, stochastic simulation of $V_0(u)$ over the entire range $u \in [0, \infty)$ also confirms that in fact our obtained solution is the required one.* □

C Proof of Corollary C.1

Corollary C.1. *For any $u \geq 0$, the ruin probability $\widehat{\psi}_0(u,t)$ up to an exponential time horizon $T \sim Exp(t)$ for a selfish miner starting in state* 0 *satisfies the differential equation* (55) *with boundary conditions* (56) *and* (57)*, a solution of which is given by*

$$\widehat{\psi}_0(u,t) = C_1\,\mathrm{e}^{\rho_1\,u} + \mathrm{e}^{\rho_2\,u}\left[C_2\,\cos\left(\rho_3\,u\right) + C_3\,\sin\left(\rho_3\,u\right)\right], \tag{52}$$

where ρ_1 and $\rho_2 \pm i\rho_3$ are (again the same) only solutions in ρ of Equation (35) *with negative real parts. The constants C_1, C_2 and C_3 are the solution of the linear equation system*

$$\begin{pmatrix} 1 & 1 & 0 \\ \rho_1 & \rho_2 & \rho_3 \\ B_1 & B_2 & B_3 \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 1 \\ -\frac{1}{ct} \\ \frac{\lambda^2 p^2}{c^2} - \frac{1}{c^2 t^2} \end{pmatrix}, \tag{53}$$

where B_1, B_2, B_3 are again given by (38)*.*

The corollary follows indeed by a suitable adaptation of the proof of Theorem B.1. Denote by $\widehat{\psi}_z(u,t)$ the ruin probability up to the finite exponential time horizon (with mean t) when starting in state z ($z \in \{0, 1, 0^*\}$). Adapting the above arguments to the case of the ruin probability, the system of advanced differential equations in this case is

$$\begin{cases} 0 = & c\,\widehat{\psi}_0'(u,t) + (\lambda p + 1/t)\,\widehat{\psi}_0(u,t) - \lambda p\,\widehat{\psi}_1(u,t), \\ 0 = & c\,\widehat{\psi}_1'(u,t) + (\lambda + 1/t)\,\widehat{\psi}_1(u,t) - \lambda p\,\widehat{\psi}_0(u+2b,t) - \lambda(1-p)\,\widehat{\psi}_{0^*}(u,t), \\ 0 = & c\,\widehat{\psi}_{0^*}'(u,t) + (\lambda + 1/t)\,\widehat{\psi}_{0^*}(u,t) - \lambda p\,\widehat{\psi}_0(u+2b,t) - \lambda(1-p)q\,\widehat{\psi}_0(u+b,t) \\ & \quad -\lambda(1-p)(1-q)\,\widehat{\psi}_0(u,t), \end{cases} \tag{54}$$

which is exactly the homogeneous version of (39) (again the derivative is always with respect to the first argument). However, now the boundary conditions are $\widehat{\psi}_0(0,t) = \widehat{\psi}_1(0,t) = \widehat{\psi}_{0^*}(0,t) = 1$, as in each state ruin is immediate when starting without initial capital. Analogously to above this translates into a differential equation of order 3 with advanced argument for $\widehat{\psi}_0(u,t)$, namely

$$\begin{aligned} 0 \;=\;& \frac{c^3}{\lambda^2\,(1-p)\,p}\,\widehat{\psi}_0'''\,(u,t) + \frac{(3+\lambda\,t\,(p+2))\,c^2}{\lambda^2 t\,(1-p)\,p}\,\widehat{\psi}_0''(u,t) \\ & + \frac{(\lambda\,t+1)\,c\,(3+\lambda\,t\,(2p+1))}{\lambda^2 t^2\,(1-p)\,p}\,\widehat{\psi}_0'(u,t) \\ & + \frac{1+\lambda\,t\,(p+2)+\lambda^2 t^2\,(2p+1)+\lambda^3 t^3 p\,((q-1)\,p^2+2p\,(1-q)+q)}{t^3\lambda^2\,(1-p)\,p}\,\widehat{\psi}_0\,(u,t) \\ & -\lambda\,q\,(1-p)\;\widehat{\psi}_0\,(u+b,t) + \frac{(\lambda\,t\,(p-2)-1)\,p}{(1-p)\,t}\,\widehat{\psi}_0(u+2b,t) \\ & -\frac{cp}{1-p}\,\widehat{\psi}_0'\,(u+2\,b,t)\,. \end{aligned} \tag{55}$$

The latter corresponds to the homogeneous equation of (42). However, the boundary conditions are now slighty different and amount to

$$\widehat{\psi}_0(0,t) = 1,\ \widehat{\psi}_0'(0,t) = -\frac{1}{ct} \text{ and } \widehat{\psi}_0''(0,t) = \frac{\lambda^2 p^2}{c^2}\,(\widehat{\psi}_0(2b,t) - 1) + \frac{1}{c^2 t^2}. \tag{56}$$

Furthermore, we know that

$$\lim_{u\to\infty} \widehat{\psi}_0(u,t) = 0. \tag{57}$$

Like in the proof of Theorem B.1, the solution can then be found to be of the form

$$\widehat{\psi}_0(u,t) = C_1\,\mathrm{e}^{\rho_1\,u} + \mathrm{e}^{\rho_2\,u}\left[C_2\,\cos(\rho_3\,u) + C_3\,\sin(\rho_3\,u)\right], \tag{58}$$

where the linear system (53) for the constants C_1, C_2, C_3 is finally derived from (56) by some elementary calculations. □

Remark C.1. In order to establish the uniqueness of the above solution for our problem setting, a similar approach as in Remark B.1 can be applied here (namely posing an additional boundary condition whose validity can then be checked by stochastic simulation). This then guarantees that our solution (52) indeed coincides with the actual ruin probability for a selfish miner up to an exponential time horizon.

Acknowledgements

The authors would like to thank Hans Gerber for helpful discussions concerning the presentation of the manuscript and Joel Cohen for his insightful remarks about the mathematical resolution of Lemma B.1., as well as the anonymous referees and the editor for their comments and remarks. Hansjörg Albrecher acknowledges financial support from the Swiss National Science Foundation Project 200021_191984. Pierre-O. Goffard acknowledges the support of l'Université Claude Bernard Lyon 1 via the Bonus Qualité Recherche (BQR) starting grant. The code to reproduce all the plots from the paper are available on the following Github repository `https://github.com/LaGauffre/Blockchain_mining_risk_analysis`.

References

[1] S. Asmussen and H. Albrecher. *Ruin Probabilities.* World Scientific, Singapore, 2010.

[2] S. Asmussen, F. Avram, and M. Usabel. Erlangian approximations for finite-horizon ruin probabilities. *ASTIN Bulletin*, 32(2):267–281, 2002.

[3] B. Avanzi, H. U. Gerber, and E.S.W. Shiu. Optimal dividends in the dual model. *Insurance: Mathematics and Economics*, 41(1):111 – 123, 2007.

[4] R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor. Modeling and analysis of block arrival times in the bitcoin blockchain. *Stochastic Models*, 36(4):602–637, jul 2020.

[5] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth. On the Lambert W function. *Advances in Computational mathematics*, 5(1):329–359, 1996.

[6] I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7):95–102, 2018.

[7] J. Göbel, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor. Bitcoin blockchain dynamics: The selfish-mine strategy in the presence of propagation delay. *Performance Evaluation*, 104:23–41, oct 2016.

[8] P.-O. Goffard. Fraud risk assessment within blockchain transactions. *Advances in Applied Probability*, 51:443–467, 2019.

[9] P.-O. Goffard and C. Lefèvre. Boundary crossing of order statistics point processes. *Journal of Mathematical Analysis and Applications*, 447(2):890–907, 2017.

[10] C. Grunspan and R. Pérez-Marco. On profitability of selfish mining. *arXiv preprint arXiv:1805.08281*, 2018.

[11] C. Grunspan and R. Pérez-Marco. On profitability of stubborn mining. *arXiv preprint arXiv:1808.01041*, 2018.

[12] C. Grunspan and R. Pérez-Marco. On profitability of trailing mining. *arXiv preprint arXiv:1811.09322*, 2018.

[13] C. Grunspan and R. Perez-Marco. On profitability of block withholding strategies. *ACM SIGMETRICS Performance Evaluation Review*, 46(3):126–126, 2019.

[14] J. A. Kroll, I. C. Davey, and E. W. Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *Proceedings of WEIS*, volume 2013, page 11, 2013.

[15] C. Lefèvre and P. Picard. Risk models in insurance and epidemics: A bridge through randomized polynomials. *Probability in the Engineering and Informational Sciences*, 29(3):399–420, mar 2015.

[16] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and Jeffrey S. Rosenschein. Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems*, AAMAS '15, page 919–927, Richland, SC, 2015. International Foundation for Autonomous Agents and Multiagent Systems.

[17] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Available at https://bitcoin.org/bitcoin.pdf, 2008.

[18] K. Nayak, S. Kumar, A. Miller, and E. Shi. Stubborn mining: Generalizing selfish mining and combining with an eclipse attack. In *Security and Privacy (EuroS&P), 2016 IEEE European Symposium on*, pages 305–320. IEEE, 2016.

[19] M. Rosenfeld. Analysis of bitcoin pooled mining reward systems. *arXiv preprint arXiv:1112.4980*, 2011.

[20] M. Rosenfeld. Analysis of hashrate-based double spending. *arXiv preprint arXiv:1402.2009*, 2014.

[21] A. Sapirshtein, Y. Sompolinsky, and A. Zohar. Optimal selfish mining strategies in bitcoin. In *International Conference on Financial Cryptography and Data Security*, pages 515–532. Springer, 2016.

[22] H. L. Smith. *An introduction to delay differential equations with applications to the life sciences.* Springer, New York, 2011.