Blockchain mining in pools: Analyzing the trade-off between profitability and ruin

Hansjörg Albrecher, Dina Finger, Pierre-Olivier Goffard

Blockchain mining in pools: Analyzing the trade-off between profitability and ruin

Hansjörg Albrecher* Dina Finger† Pierre-O. Goffard‡

Abstract

The resource-consuming mining of blocks on a blockchain equipped with a *Proof-of-Work* consensus protocol bears the risk of ruin, namely when the operational costs for the mining exceed the received rewards. In this paper we investigate to what extent it is of interest to join a mining pool that reduces the variance of the return of a miner for a specified cost for participation. Using methodology from ruin theory and risk sharing in insurance, we quantitatively study the effects of pooling in this context and derive several explicit formulas for quantities of interest. The results are illustrated in numerical examples for parameters of practical relevance.

1. Introduction

A blockchain is a decentralized data ledger maintained by a *Peer-to-Peer* network. Blockchain users issue transactions to the network peers who agree on those to be recorded by following a consensus protocol. In public and permissionless blockchains, such as the one for Bitcoin, the consensus protocol is called *Proof-of-Work* (PoW). The nodes, referred to as miners, compete to solve a challenging cryptographic puzzle using some brute force search algorithm. The first miner to come up with a solution includes the pending transactions in a block and is rewarded with newly minted crypto-coins. This reward compensates the operational cost of mining mainly induced by the consumption of electricity. The PoW protocol is designed to be incentive compatible in the sense that a miner is compensated proportionally to her computational effort. When the Peer-to-Peer network grows large, the share of the network computing power owned by a given miner shrinks, which in turn makes the gains infrequent. The constant operating costs therefore endanger the solvency of miners and has led them to join forces by forming mining pools.

Mining pools grant miners a steadier income, as block finding rewards are collected more often. The earnings are then fairly distributed to the pool participants based on their contribution to the computational effort. The simplest way to do so consists in splitting the reward whenever a block is found. This is the *proportional* reward system. More sophisticated reward schemes have been put together to increase the amount of risk transferred from the miners to the pool and to fill the gaps

*The Faculty of Business and Economics, University of Lausanne and Swiss Finance Institute, Quartier UNIL-Chamberonne Bâtiment Extranef, 1015 Lausanne, Switzerland, hansjoerg.albrecher@unil.ch

†The Faculty of Business and Economics, University of Lausanne, Quartier UNIL-Chamberonne Bâtiment Extranef, 1015 Lausanne, Switzerland, dina.finger@unil.ch

‡Laboratoire de Sciences Actuarielle et Financière EA2429, Université Claude Bernard Lyon 1, Université de Lyon. Institut de Science Financière et d'Assurances, 50 Avenue Tony Garnier, 69007 Lyon, France, pierre-olivier.goffard@univ-lyon1.fr

of the proportional system that we will discuss later. These more sophisticated systems require the supervision of a manager who undertakes part of the risk in exchange for a commission. An early work of Rosenfeld [21] provides a detailed overview on mining pool reward systems, see also the recent survey of Zhu et al. [24]. In practice, the individual contribution of a miner is measured through a *share* submission process. A *share* refers to an easier-to-find 'fake' solution to the crypto-puzzle that miners must send to the pool manager to prove their involvement (for instance, a solution to the crypto-puzzle with only m instead of the $n > m$ leading zeroes required for the successful mining of a block). In this work we provide a risk analysis of *Pay-per-Share* (PPS) reward systems in which the pool manager pays for each share submitted by the miners. In that way the manager takes on much of the randomness associated to the mining activity, which is therefore very appealing to the participant. Using utility theory, Schrijvers et al. [22] showed that such systems are incentive-compatible for risk-averse miners. Both Rosenfeld [21] and Zhu et al. [24] stressed that a scheme of this kind must go hand in hand with a proper capital allocation strategy on the part of the manager to avoid ruin. Reliable information on mining companies filing for bankruptcy are hard to come by, we are able to provide one. Bcause Mining, LLC, the mining affiliate operating in Virginia Beach, Virginia, filed voluntarily for bankruptcy court protection under Chapter 11 on April 11, 2019 in order to reorganize its debts. Unsecured creditors included a Virginia power company ($\$1,459,267.38$), the U.S. Customs and Border Patrol ($\$737,041.90$), landlords, and staff[1].

The aim of this paper is to provide risk-analytic tools to inform the decision making process of miners and pool managers. This is achieved by taking an approach inspired from insurance risk theory. The wealth of miners and pool managers is modelled via stochastic processes that take into account operational costs, pool participation fees and block finding rewards. The resulting processes are similar to those appearing in the surplus modelling for insurance companies which collect premiums continuously and have to pay loss reimbursements to policyholders in case a claim occurs. A standard risk measure in this context is the ruin probability defined as the probability that the wealth process falls below zero, see e.g. Asmussen and Albrecher [6] for an overview. This analogy was already used in Albrecher and Goffard [3], where the opportunity for miners to deviate from the prescribed protocol by withholding blocks was investigated. A first result was also obtained there in relation to the advantage of joining a mining pool which applies the proportional system. Our objective in this paper is to considerably extend this line of thinking towards the *Pay-per-Share* redistribution systems that are more commonly used in practice. We will also consider a variant of the model in which the collected rewards are random variables. This assumption will enable the application of classical results from double-sided jumps in a risk reserve process for modelling insurance portfolios, see for example Albrecher at al. [2], Labbé and Sendova [16]. Incorporating random rewards allows us to account for the transactions fees and the exchange rate of cryptocurrencies to fiat ones. Transaction fees are included by blockchain users to entice the network to process their transactions, see Easley al. [11] and Kasahara and Kawahara [14]. The redistribution of the revenue generated by the transaction fees among the pool participants also varies from one mining pool to another. Closed-form expressions for the probability of ruin and the expected profit given that ruin has not occurred are provided up to an exponentially distributed time horizon. These formulas are amenable for a quick numerical evaluation to perform a sensitivity analysis of risk and reward indicators with respect to the model parameters.

[1]Source: https://www.theblockcrypto.com

We believe that our results will be useful for miners and pool managers to make the right financial choices. Our indicators can also serve as the basis for a potential future regulatory framework for mining activity on blockchains equipped with the Proof-of-work consensus protocol.

A major concern associated to mining pool formation is the centralization of the network. Cong et al. [9] have explained that miners who direct their mining power to multiple small mining pools enjoy the same risk sharing benefits as miners that choose to join a single mining pool. Hence the intuition that a larger mining pool would grow even larger is misguided. Empirical data shows that the participation fees are greater in larger mining pools, which naturally slows down their growth. We aim at providing more insight on the risk of centralization in the light of our analysis.

The remainder of the paper is organized as follows. Section 2 gives a brief description of the mining process in blockchains equipped with Proof-of-Work. Section 3 provides an overview of the existing reward systems and describes the *Pay-Per-Share* mechanism in more detail, as it will be the focus later on. Formulas for the ruin probability and expected surplus for the pool manager are derived for deterministic rewards in Section 4 and for randomized reward in Section 5. Section 6 provides formulas from the individual miner's perspective. Section 7 is devoted to numerical illustrations where the sensitivity of the risk and performance indicator is analysed with respect to the model parameters. Section 8 concludes.

2. Mining blocks in a Proof-of-Work powered blockchain

A block consists of a header and a list of "transactions" that represents the information recorded through the blockchain. The header usually includes the date and time of creation of the block, the block height which is the index inside the blockchain, the hash of the block and the hash of the previous block. The hash of a block is obtained by concatenating the header and the transactions in a large character string thus forming a "message", to which a hash function is applied. A hash function is a function that can map data of arbitrary size to fixed-sized values. The hash functions used in blockchain applications must be cryptographic, i.e. quick to compute, one way and deterministic. It must be nearly infeasible to generate a message with a given hash value or to find two messages with the same hash value. A small change in the message should change dramatically the hash value so that the new hash value appears to be uncorrelated to the previous hash. We will not expand on how to build such a cryptographic hash function, we refer the interested reader to the work of Al-Kuwari et al. [1]. In the bitcoin blockchain as well as in many other applications, the standard is the SHA-256 function which converts any message into a hash value of 256 bits. The latter is usually translated into a hexadecimal digest, for instance the hash value of the title of the present manuscript reads as

`98b1146926548f6b57c4347457713ff2f035beda9c93f12fbc9b202e9c512e80`.

The information recorded in a public blockchain may be retrieved by anyone and can be accessed through a blockchain explorer such as blockchain.com, the content of the block of height #724724 may be viewed through the following link block content. Mining a block means finding a block hash value lower than some target which can only be achieved by brute force search thanks to the properties of cryptographic hash functions. In practice, the search for an appropriate hash value, referred to as

a solution, is done by appending a nonce to the block message before applying the hash function. A nonce is a 32 bits number, drawn at random by miners until a nonce resulting in a proper block hash value is found. For illustration, consider the block in Figure 1.

```
Block Hash: 1fc23a429aa5aaf04d17e9057e03371f59ac8823b1441798940837fa2e318aaa
Block Height: 0
Time:2022-02-25 12:42:04.560217
Nonce:0
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 0}, {'sen
der': 'Satoshi', 'recipient': 'Pierre-O', 'amount': 5, 'fee': 2}]
Previous block hash: 0
Mined: False
--------------
```

Figure 1: A block that has not been mined yet.

The hash value in decimal notation is $1.43e^{76}$ while the maximum value for a 256 bits number is $2^{256} - 1 \approx 1.16e^{77}$. We refer to the latter as the maximal target and denote it by $T_{\max}$. The Proof-of-Work protocol sets a target $T < T_{\max}$ and ask miners to find a nonce such that the hash value of the block is smaller than T. Practitioners would rather talk about the *difficulty* which is defined as $D = T_{\max}/T$. If the difficulty is one, any hash value is acceptable. Increasing the difficulty reduces the set of allowable hash values, making the problem harder to solve. A hash value is then called *acceptable* if its hexadecimal digest starts with a given number of zeros. If we set the difficulty to 2^4, then the hexadecimal digest of the hash of the block must start with at least 1 leading zero, making the hash value of the block in Figure 1 not acceptable. After completing the nonce search we get the block in Figure 2. Note that it took 5 attempts to find this nonce. The number of needed trials is

```
Block Hash: 0869032ad6b3e5b86a53f9dded5f7b09ab93b24cd5a79c1d8c81b0b3e748d226
Block Height: 0
Time:2022-02-25 13:41:48.039980
Nonce:2931734429
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 0}, {'sen
der': 'Satoshi', 'recipient': 'Pierre-O', 'amount': 5, 'fee': 2}]
Previous block hash: 0
Mined: True
--------------
```

Figure 2: A mined block with a hash value having on leading zero.

geometrically distributed with parameter $1/D$, which means that with a difficulty of $D = 2^4$ it takes on average 16 trials. The protocol adjusts the difficulty automatically every $2,016$ block discoveries so as to (globally) maintain one block discovery every 10 minutes on average. The time between two block discoveries depends on the number of hash values computed by the network at a given instant. At the time of writing, the network computes 182.58 Exahashes per second and the difficulty is $27,967,152,532,434$.[2] For an exhaustive overview of the mining process in the bitcoin blockchain, we refer the reader to the book of Antonopoulos [5, Chapter 10]. 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. This justifies the Poisson process assumption made in the sequel to model the block

[2]Source: bitcoinblockhalf.com

arrival and the reward collecting processes. Empirical studies of the block inter-arrival times data tend to confirm this hypothesis, see the work of Bowden et al. [8].

3. Risk models and reward systems

A risk model defines the wealth of some company or individual as a stochastic process

$$R_t = u - C_t + B_t,\ t \geq 0$$

which corresponds to the income $(B_t)_{t\geq 0}$ net of the expenses $(C_t)_{t\geq 0}$. The surplus process $(R_t)_{t\geq 0}$ starts at some initial level $R_0 = u > 0$. We take a continuous time approach where $t \in \mathbb{R}_+$, and $(C_t)_{t\geq 0}$ and $(B_t)_{t\geq 0}$ define increasing functions or stochastic processes. A risk analysis is relevant only if at least one of the model components is random. The activity of the company is profitable if on average the earnings exceed the expenses, namely $\mathbb{E}(B_t) > \mathbb{E}(C_t)$. Even if the net profit condition holds, the variability of the process $(R_t)_{t\geq 0}$ can lead to bankruptcy as it may become negative. Define the ruin time as

$$\tau_u = \inf\{t \geq 0 :\ R_t < 0\},$$

which corresponds to the first time at which the surplus goes below 0. The risk of bankruptcy is classically assessed by computing the ruin probability up to time $t \geq 0$ defined by

$$\psi(u,t) = \mathbb{P}(\tau_u \leq t). \tag{1}$$

It is sometimes more convenient from a mathematical point of view to consider the infinite-time horizon by letting $t \to \infty$, and in that case we write $\psi(u) := \lim_{t\to\infty} \psi(u,t)$. Following the rationale developed in [3], we also consider a performance indicator defined as

$$V(u,t) = \mathbb{E}(R_t \mathbb{I}_{\tau_u > t}), \tag{2}$$

which corresponds to the expected surplus at time $t \geq 0$ in case ruin did not occur until then.

Consider a network of n miners, where miner $i \in \{1,\dots,n\}$ owns a share $p_i \in (0,1)$ of the network hashpower, i.e. $\sum_{i=1}^n p_i = 1$. If the number of blocks found by the network is governed by a homogeneous Poisson process $(N_t)_{t\geq 0}$ with intensity λ, then the number of blocks found by miner i is a (thinned) Poisson process $(N_t^i)_{t\geq 0}$ with intensity $p_i \cdot \lambda$. Denote by $b > 0$ the amount of the reward for finding a new block and assume that the cumulative operational cost is a linear function with slope $c_i > 0$ which depends on the price of the electricity and the computing power of miner i. The surplus process of miner i is then given by

$$R_t^i = u - c_i \cdot t + N_t^i \cdot b,\ t \geq 0. \tag{3}$$

Model (3) has been considered by Albrecher and Goffard [3], and formulas for both the finite-time ruin probability (1) and the expected surplus (2) were derived. To make the formulas more amenable for numerical evaluation, the authors then decided to approximate the fixed time horizon $t \geq 0$ by an

exponential random variable $T \sim \text{Exp}(t)$ with mean $t \geq 0$, resulting in tractable expressions for

$$\widehat{\psi}(u,t) = \mathbb{E}[\psi(u,T)], \text{ and } \widehat{V}(u,t) := \mathbb{E}[V(u,T)], \tag{4}$$

which were then used to carry out a numerical analysis.

Remark 3.1. Model (3) assumes that the block-finding reward is constant, while the bitcoin protocol stipulates a halving of the reward every 210,000 blocks. However, first note that 210,000 blocks take 4 years to be found which is greater than the time horizon we have in mind when defining $\widehat{\psi}(u,t)$ and $\widehat{V}(u,t)$. Second, since these halving dates are known to blockchain networks, the market automatically adjusts the cryptocurrency exchange rate before the halving occurs. Eventually, one could also replace b in Model (3) with a piecewise constant function to account for halving events. However, this would only be relevant for very long time horizons and will not be pursued in the present work.

Consider now a situation where a subset of miners $I \subset \{1, \dots, n\}$ decides to gather in a mining pool. The cumulated hashpower of this pool is then

$$p_I = \sum_{i \in I} p_i,$$

and the arrival rate of block rewards for a given miner i rises from $p_i \cdot \lambda$ to $p_I \cdot \lambda$. Because the reward is shared among the pool participants, the size of the reward collected by miner i decreases from b to $p_i \cdot b$. The expected surplus is the same when mining solo and mining for a pool, but the variance (and therefore the risk) is smaller when mining for a pool. The management of a mining pool relies heavily on the reward distribution mechanism set up by a pool manager. For the redistribution system to be fair, each miner must be remunerated in proportion to her calculation effort. Miner i must earn a share p_i/p_I of the mining pool total income. The pool manager has to find a way to estimate the contribution of each pool participant. This is done by submitting *shares* which are partial solutions to the cryptopuzzle easier to find than the actual solution. Recall from Section 2 that a proper solution corresponds to a hash value starting with a given number of zeros, so *shares* are hash values with a smaller number of leading zeros. If the current difficulty of the cryptopuzzle is D, then the difficulty for finding a *share* is set to $q \cdot D$ by the pool manager, where $q \in (0,1)$. The manager's cut is a fraction $f \in (0,1)$ of the block discovery reward b. We start by presenting the proportional reward system in Section 3.1.

3.1 The proportional reward system

The proportional reward system splits time in *rounds* which correspond to the time elapsed between two block discoveries. During these *rounds*, the miners submit *shares*. The ratio of the number of *shares* submitted by miner i over the total number of *shares* submitted by her fellow mining pool participants determines her share of the reward and should converge to her share of the mining pool computing power, that is p_i/p_I (for sufficiently low complexity of the shares, the latter limit will be a very good approximation for the actual situation indeed). The surplus of miner i is then given

$$R_t^i = u - c_i \cdot t + N_t^I \cdot (1-f) \cdot \frac{p_i}{p_I} \cdot b, \ t \geq 0, \tag{5}$$

where (N_t^I) is a Poisson proccess of intensity $p_I \cdot \lambda$ that gives the number of blocks appended to the blockchain by the mining pool. The duration of a *round* is exponentially distributed Exp $\left[(p_I\lambda)^{-1}\right]$. The uncertainty on the length of the round has undesirable consequences on the time value of the *shares* submitted by the miners. Indeed, if n shares are submitted during a round, then the value of a given *share* is $(1-f)\cdot b/n$. The longer a *round* lasts, the greater the value of n is. The *shares* are worth less in longer rounds which triggers an exodus behavior of miners toward mining pools with shorter rounds. This phenomenon, called pool hopping, has been documented in the early work of Rosenfeld [21]. Yet another drawback is that a miner that has found a full solution may delay the submission until her ratio of *shares* submitted reflects her fraction of the mining pool computing power. The proportional system is not *incentive-compatible* using the terminology of Schrijvers et al. [22]. A discounting factor may be applied to compensate the decreasing value of shares over time, see for instance the slush's method [20].

Our work is also concerned about the risk undertaken by pool managers. Within the frame of the proportional reward system, the surplus of the pool manager is given by

$$R_t^I = u + N_t^I \cdot f \cdot b,\ t \geq 0. \tag{6}$$

Model (6) does not account for any mining pool operating cost. The mining costs are entirely borne by miners and the mining pool manager only serves as coordinator. A proportional-type reward system should therefore lead to a low management fee f.

Although this system provides fairness, it has weaknesses that justify the introduction of a more sophisticated distribution mechanism. In particular, if miners seek to actually transfer some of the risk associated to the mining activity to the pool manager, then they should rather turn to a mining pool based on a *Pay-per-Share* system, which is the focus of this paper and introduced in the next section.

3.2 The Pay-Per-Share reward system

In a *Pay-per-Share* reward system, the pool manager immediately rewards the miners for each *share* submitted. Let $(M_t)_{t\geq 0}$ be a Poisson process of intensity μ that counts the number of *shares* submitted by the entire network of miners up to time $t \geq 0$. Denote by $q \in (0,1)$ the relative difficulty of finding a block compared to finding a share. Let $0 < w < b$ be the reward for finding a *share*. The number of *shares* submitted by miner i is then a (thinned) Poisson process $(M_t^i)_{t\geq 0}$ with intensity $p_i \cdot \mu$, p_i being the share of the individual miner's network hashpower as defined above, and her surplus when joining a PPS mining pool becomes

$$R_t^i = u - c_i \cdot t + M_t^i \cdot w,\ t \geq 0. \tag{7}$$

The intensities of the processes $(N_t)_{t\geq 0}$ and $(M_t)_{t\geq 0}$ are linked through $\lambda = q \cdot \mu$. By setting $w = (1-f)\cdot b \cdot q$, we observe that the surplus (5) and (7) have the same expectation at time t, but the variance and therefore the risk associated to (7) is lower. This reward system has been shown to be resistant to pool hopping and is incentive compatible. It also entails a significant transfer of risk to

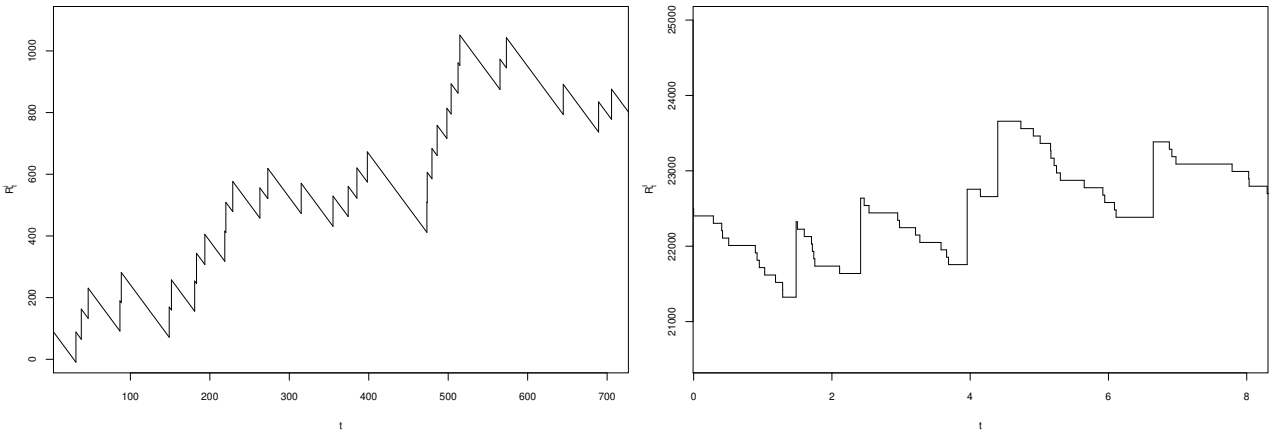
the pool manager whose surplus process is now given by

$$R_t^I = u - M_t^I \cdot w + N_t^I \cdot b,\ t \geq 0, \tag{8}$$

making her subject to the risk of bankruptcy.

Remark 3.2. Since the process $(M_t^I)_{t\geq 0}$ requires solving for a problem of lower complexitiy than $(N_t^I)_{t\geq 0}$, $(N_t^I)_{t\geq 0}$ is a subset of the path defined by the process $(M_t^I)_{t\geq 0}$. It means that both processes are not independent. Concretely, at the moment of the block reward payment b, at the same time there is a realisation of the miners' reward w. As we sometimes will need to isolate downward jumps without the simultaneous upward jump point, we define another process with a reduced intensity. We apply the superposition theorem (see e.g. [15]) to the Poisson process M_t^I by redefining the down jump process as $(M_t^{I,d})_{t\geq 0} \sim Poisson(\mu_d)$, where $\mu_d = \mu - \lambda$.

Figure 3 represents sample paths of the surplus processes for an individual miner and the pool manager.



(a) Individual miner

(b) Pool manager

Figure 3: Illustration of surplus paths for the pool members and the pool manager.

In addition to the bounty for finding a new block, blockchain users usually include a small financial incentive for the network to process their transaction. These transaction fees (e.g. referred to as *gas* within the ETHEREUM blockchain), are known to be variable as they highly depend on the network congestion at a given time. Note also that since the operational cost is paid by miners using a fiat currency, it would be more accurate to account for the exchange rate of the cryptocurrency to some fiat currency. We can therefore model the successive rewards for *shares* and blocks as sequences of nonnegative random variables denoted by $(W_k)_{k\geq 1}$ and $(B_k)_{k\geq 1}$ respectively, which for simplicity we will both assume to be *i.i.d.* in this paper. A reward system that features a *Pay-per-Share* mechanism and includes in the miners' reward the transaction fees is referred to as a *Full Pay-per-Share* reward system by practitioners. The surplus of miner i in a mining pool applying the FPPS system is given by

$$R_t^i = u - c_i \cdot t + \sum_{k=1}^{M_t^i} W_k,\ t \geq 0, \tag{9}$$

and the surplus of the pool manager then becomes

$$R_t^I = u - \sum_{k=1}^{M_t^I} W_k + \sum_{l=1}^{N_t^I} B_l,\ t \geq 0. \tag{10}$$

In the following sections, we will now derive formulas for the ruin probability and expected surplus in case ruin did not occur up to a given time horizon for the models discussed above.

4. Pool analysis with deterministic rewards

We start with a fixed time horizon. For simplicity, we drop the superscript I in the following developments.

4.1 Deterministic time horizon

For the pool manager's side, we first define some measures of interest. Let $\tau = \inf\{t \geq 0 : R_t < 0\}$ be the time of ruin of the pool manager, i.e. the first time his surplus reaches 0. The corresponding ruin probabilities in finite and infinite horizon respectively are given by

$$\psi(u,t) = \mathbb{P}(\tau \leq t),\ \text{and}\ \psi(u) = \mathbb{P}(\tau < \infty). \tag{11}$$

The net profit condition in this case translates to $\lambda b > \mu w$. It implies from [6], that $\psi(u) < 1$. We also define the expected surplus at time t given that ruin has not occurred up to time t:

$$V(u,t) = \mathbb{E}(R_t \mathbb{I}_{\tau > t}). \tag{12}$$

In the sequel, we will use the process $(M_t^d)_{t\geq 0}$ defined in Remark 3.2 representing the pure downward jumps. Note that ruin can only occur at discrete times when the process $(M_t^d)_{t\geq 0}$ admits a jump. We can rewrite the ruin time τ as

$$\tau = \inf\{t \geq 0; M_t^d w > u + N_t(b-w)\} = \inf\{t \geq 0; M_t^d > u/w + N_t(b-w)/w\}. \tag{13}$$

Equivalently, we can rewrite it as

$$\tau = \inf\{t \geq 0; M_t^d w/(b-w) > u/(b-w) + N_t\} \tag{14}$$

to isolate the $(N_t)_{t\geq 0}$ process with unit jumps. The study of the p.d.f. f_τ of τ is analogous to the derivations in [12]. Since $(N_t)_{t\geq 0}$ and $(M_t^d)_{t\geq 0}$ are Poisson process, they enjoy the order statistic property. That is, given that $N_t = n$, the jump times $\{T_1, \ldots, T_n\}$ of the process N_t have the same distribution as the order statistics vector of a random variable having distribution $F_t(s) = s/t,\ 0 \leq s \leq t$. Further, let $\{S_n^d, n \in \mathbb{N}\}$ be the sequence of arrival times associated with the process $(M_t^d)_{t\geq 0}$. Its distribution function is denoted by $F_{S_n^d}(t)$ and its p.d.f. by $f_{S_n^d}(t)$. Denote by $\lceil x \rceil$ the ceiling function. Following Corollary 1 from [12], we proceed from Equation (14) and derive the next steps.

Theorem 4.1. *Let* $(N_t,\ t \geq 0)$ *and* $(M_t^d,\ t \geq 0)$ *be Poisson processes with intensities* $\{\lambda, \mu_d\}$ *respec-*

tively, and assume that the net profit condition $\lambda b > \mu w$ holds, then the p.d.f. of τ is given by

$$f_\tau(t) = \sum_{n=0}^{+\infty} \mathbb{E}\left[\frac{(-1)^n}{t^n} G_n\left[0|S_{v_0}, \ldots, S^d_{v_{n-1}}\right]|S^d_{v_n} = t\right] f_{S^d_{v_n}}(t)\mathbb{P}\left[N_t = n\right], \tag{15}$$

where $(v_n)_{n\geq 0}$ is a sequence of integers defined as $v_n = \lceil n(b-w)/w + u/w \rceil$, $n \geq 0$, and $(G_n(\cdot|\{\ldots\})_{n\in\mathbb{N}}$ is the sequence of Abel-Gontcharov polynomials defined in Appendix A.

The proof is delegated to Appendix B. The expression of the ruin time p.d.f. (15) is not convenient for numerical purposes. The infinite series in (15) must be truncated, possibly to a high order to reach an acceptable level of accuracy. Also, the evaluation of the Abel-Gontcharov polynomials relies on the recurrence relationships (67) which are known to suffer from numerical instabilities. Moreover, the conditional expectation with respect to $\{S^d_{v_n} = t\}$ itself requires the use of Monte Carlo simulations. Finally, a similar algebraic expression for $V(u,t)$ is out of sight. In view of all these difficulties, we therefore propose as in [3] a workaround which consists of replacing the deterministic time horizon by a random variable with exponential distribution.

4.2 Exponential time horizon

To obtain a nicer solution to the problem, we now randomize the time horizon T. The practical intuition suggests that the time horizon is never fixed in advance and is subject to various external factors, such as bitcoin price fluctuations, in-pool events etc. We choose the time horizon T to be exponentially distributed with rate $1/t$ (so that $\mathbb{E}(T) = t$). This leads to computable expressions having an intuitive justification due to the lack of memory property of the exponential distribution. Let $\hat{V}(u,t) := \mathbb{E}(R_T \mathbb{I}_{\tau>T})$ denote the expected value of the surplus at the exponential time horizon T.

Theorem 4.2. *Let b and w, $b > w$, be fixed positive integers and assume that the net profit condition $\lambda b > \mu w$ holds. Then the expected surplus at an exponential time horizon can be expressed in the form*

$$\hat{V}(u,t) = \sum_{i=1}^{w} c_i x_i^u + u + \lambda b\, t - (\lambda + \mu_d) w\, t,$$

where $x_1, \ldots, x_w$ are the w roots inside the unit disk of the equation

$$\lambda x^b - (\lambda + \mu_d + 1/t)x^w + \mu_d = 0, \tag{16}$$

and the constants $c_1, \ldots, c_w$ are the solution of the linear equation system

$$\begin{pmatrix} \lambda x_1^{b-w} - (\lambda+\mu_d+1/t) & \cdots & \lambda x_w^{b-w} - (\lambda+\mu_d+1/t) \\ \lambda x_1^{b-w+1} - (\lambda+\mu_d+1/t)x_1 & \cdots & \lambda x_w^{b-w+1} - (\lambda+\mu_d+1/t)x_w \\ \vdots & \ddots & \vdots \\ \lambda x_1^{b-1} - (\lambda+\mu_d+1/t)x_1^{w-1} & \cdots & \lambda x_w^{b-1} - (\lambda+\mu_d+1/t)x_w^{w-1} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_w \end{pmatrix} = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_w \end{pmatrix}, \tag{17}$$

with

$$A_i = (i-1)\mu_d + \mu_d t(\lambda b - (\lambda+\mu_d)w) - \mu_d w, \quad i = 1, \ldots, w.$$

Proof. Akin to the approach in [2], consider some small $h > 0$ and condition on the following scenarios during the time interval $(0, h)$:

1. no jump and $T > h$;
2. no jump and $T \leq h$;
3. occurrence of an upward jump;
4. occurrence of a downward jump.

All other combinations of these events have negligible probability in the limit $h \to 0$ that we will pursue below. One then obtains

$$\begin{aligned}\hat{V}(u,t) = e^{-(\frac{1}{t}+\lambda+\mu_d)h}\hat{V}(u,t) + \frac{1}{t}\int_0^h e^{-s/t}e^{-(\lambda+\mu_d)s}u\,ds \\ + \lambda\int_0^h e^{-\lambda s}e^{-(1/t+\mu_d)s}\hat{V}(u+b-w,t)\,ds + \mu_d\int_0^h e^{-\mu_d s}e^{-(1/t+\lambda)s}\hat{V}(u-w,t)\,ds.\end{aligned} \tag{18}$$

We now take the derivative w.r.t. h and set $h = 0$ to obtain

$$\lambda\hat{V}(u+b-w,t) - (\lambda+\mu_d+1/t)\hat{V}(u,t) + \mu_d\hat{V}(u-w,t) + u/t = 0, \quad u \geq 0. \tag{19}$$

By definition of $\hat{V}(u,t)$ we have the boundary conditions $\hat{V}(u,t) = 0$ for all $u < 0$ and the linear boundedness $0 \leq \hat{V}(u,t) \leq u + (\lambda b - \mu_d w)t$ in both u and t for all $u, t \geq 0$.

Equation (19) is an inhomogeneous difference equation with constant coefficients (see e.g. [13] for solution methods), which has the general solution

$$\hat{V}(u,t) = \sum_{i=1}^{b} c_i x_i^u + d_0 + d_1 u$$

with constants $\{c_i\}_{i=1}^b, \{x_i\}_{i=1}^b, d_0, d_1$ still to be determined.

Let us start with the inhomogeneous part: plugging the ansatz $d_0 + d_1 u$ into (19) gives

$$d_1 = 1,\ d_0 = \lambda b t - (\lambda+\mu_d)wt.$$

For the homogeneous part, we consider the characteristic equation (16), which by the Fundamental Theorem of Algebra has exactly b complex roots $x_1, \ldots, x_b$. The linear boundedness of $\hat{V}(u,t)$, however, excludes any solution with absolute value exceeding 1 (i.e., the corresponding constants c_i must be zero). In fact, it turns out that exactly w roots of the polynomial in (16) are located inside the unit disk in the complex plane. To see this, observe first that $(\lambda+\mu_d+1/t)x^w + \mu_d$ has exactly w roots inside the unit disk (due to $\mu_d/(\lambda+\mu_d+1/t) < 1$). Then Rouché's Theorem establishes that the same is true for the entire polynomial in (16), if

$$|\lambda z^b| < |-(\lambda+\mu_d+1/t)z^w + \mu_d| \text{ on } |z| = 1,$$

which translates into the condition

$$|\mu_d - (\lambda+\mu_d+1/t)z^w| > \lambda \text{ on } |z| = 1. \tag{20}$$

The reverse triangle inequality states for any complex $a, b \in \mathbb{C}$ that $|a-b| \geq \big||a|-|b|\big|$, which shows that for $|z| = 1$ the left-hand side of (20) is larger than $\lambda + 1/t$, so that (20) is indeed fulfilled.

It is now only left to determine the coefficients $c_1, \ldots, c_w$ corresponding to the w roots $x_1, \ldots, x_w \in \mathbb{C}$ with $|x_i| < 1$ of (16). To that end, note that (19) evaluated at $u = 0, \ldots, w-1$ gives the following system of equations:

$$\begin{aligned}
&\lambda \hat{V}(b-w,t) - (\lambda + \mu_d + 1/t)\hat{V}(0,t) = 0,\\
&\lambda \hat{V}(b-w+1,t) - (\lambda + \mu_d + 1/t)\hat{V}(1,t) + 1/t = 0,\\
&\ldots\\
&\lambda \hat{V}(b-1,t) - (\lambda + \mu_d + 1/t)\hat{V}(w-1,t) + (w-1)/t = 0.
\end{aligned}$$

Substituting the form

$$\hat{V}(u,t) = \sum_{i=1}^{w} c_i x_i^u + u + a_t$$

with $a_t = \lambda b\, t - (\lambda + \mu_d) w\, t$ into this system leads to

$$\begin{aligned}
&\lambda \sum_{i=1}^{w} c_i x_i^{b-w} + \lambda(b-w) + \lambda a_t - (\lambda + \mu_d + 1/t)\left(\sum_{i=1}^{w} c_i + a_t\right) = 0,\\
&\lambda \sum_{i=1}^{w} c_i x_i^{b-w+1} + \lambda(b-w+1) + \lambda a_t - (\lambda + \mu_d + 1/t)\left(\sum_{i=1}^{w} c_i x_i + (1 + a_t)\right) + 1/t = 0,\\
&\ldots\\
&\lambda \sum_{i=1}^{w} c_i x_i^{b-1} + \lambda(b-1) + \lambda a_t - (\lambda + \mu_d + 1/t)\left(\sum_{i=1}^{w} c_i x_i^{w-1} + (w - 1 + a_t)\right) + (w-1)/t = 0.
\end{aligned}$$

But the latter can be rewritten in the form (17). □

Example 4.3. Figure 4 depicts $\hat{V}(u,t)$ as a function of u for the parameters $b = 100, w = 9, t = 1, \lambda = 10, \mu_d = 90$. Note that for some capital levels u the increase of $\hat{V}(u,1)$ from u to $u+1$ is larger than for others. This is linked to how many down-jumps relative to up-jumps are needed to become negative, and due to the discrete nature of the problem such jumps in $\hat{V}(u,t)$ occur naturally.

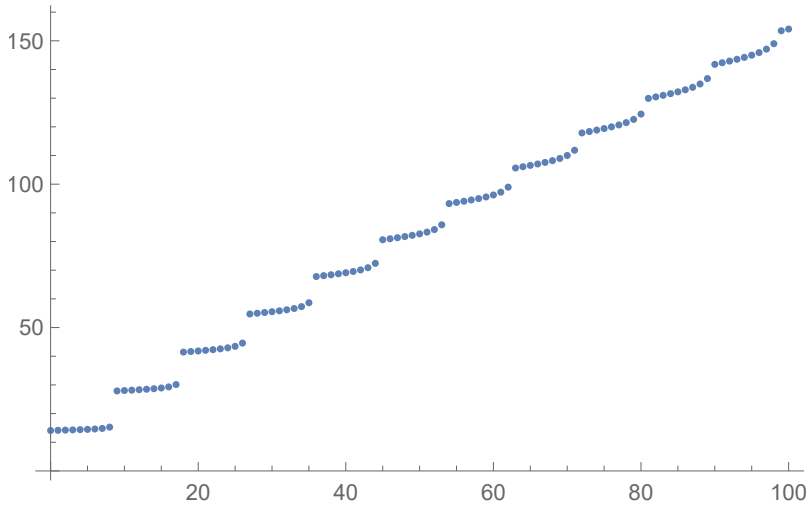


Figure 4: $\hat{V}(u,1)$ as a function of u

In an analogous way, an explicit formula for $\widehat{\psi}(u,t) = \mathbb{E}[\psi(u,T)]$ can be derived.

Theorem 4.4. *Let b and w, $b > w$, be fixed positive integers. Then the ruin probability up to an exponential time horizon with mean t is given by*

$$\widehat{\psi}(u,t) = \sum_{i=1}^{w} c_i x_i^u \tag{21}$$

where $x_1, \dots, x_w$ are the w roots inside the unit disk of Equation (16) and the constants $c_1, \dots, c_w$ are the solution of the linear equation system

$$\begin{pmatrix} \lambda x_1^{b-w} - (\lambda + \mu_d + 1/t) & \cdots & \lambda x_w^{b-w} - (\lambda + \mu_d + 1/t) \\ \lambda x_1^{b-w+1} - (\lambda + \mu_d + 1/t)x_1 & \cdots & \lambda x_w^{b-w+1} - (\lambda + \mu_d + 1/t)x_w \\ \vdots & \ddots & \vdots \\ \lambda x_1^{b-1} - (\lambda + \mu_d + 1/t)x_1^{w-1} & \cdots & \lambda x_w^{b-1} - (\lambda + \mu_d + 1/t)x_w^{w-1} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_w \end{pmatrix} = \begin{pmatrix} -\mu_d \\ -\mu_d \\ \vdots \\ -\mu_d \end{pmatrix}. \tag{22}$$

Proof. We proceed in the same way as in the proof of Theorem 4.2. The analogue of (18) then is

$$\begin{aligned} \widehat{\psi}(u,t) = {} & e^{-(\frac{1}{t}+\lambda+\mu_d)h}\widehat{\psi}(u,t) + \lambda \int_0^h e^{-\lambda s} e^{-(1/t+\mu_d)s} \widehat{\psi}(u+b-w,t)\, ds \\ & + \mu_d \int_0^h e^{-\mu_d s} e^{-(1/t+\lambda)s} \widehat{\psi}(u-w,t)\, ds \end{aligned} \tag{23}$$

and (19) is replaced by

$$\lambda \widehat{\psi}(u+b-w,t) - (\lambda + \mu_d + 1/t)\widehat{\psi}(u,t) + \mu_d \widehat{\psi}(u-w,t) = 0, \quad u \geq 0, \tag{24}$$

which is the homogeneous equation of the former. The boundary conditions here are given by $\widehat{\psi}(u,t) = 1$ for $u < 0$ as well as the obvious bound $\widehat{\psi}(u+b-w,t) \leq 1$ for all $u \geq 0$. Correspondingly, from the proof of the previous theorem we then know that

$$\widehat{\psi}(u,t) = \sum_{i=1}^{w} c_i x_i^u \tag{25}$$

with constants $c_1, \dots, c_w$ still to be determined. Evaluating (24) at $u = 0, \dots, w-1$ gives

$$\lambda \widehat{\psi}(b-w+j,t) - (\lambda + \mu_d + 1/t)\widehat{\psi}(j,t) + \mu_d = 0, \quad j = 0, \dots, w-1.$$

Substituting (25) into these leads to

$$\lambda \sum_{i=1}^{w} c_i x_i^{b-w+j} - (\lambda + \mu_d + 1/t) \left(\sum_{i=1}^{w} c_i x_i^j \right) + \mu_d = 0, \quad j = 0, \dots, w-1,$$

or equivalently (22). □

5. Pool analysis with stochastic rewards

Until this point, we considered deterministic rewards b and w for jump sizes of the surplus process. However, in practice, one may desire to incorporate variability in these quantities to account for instance for the incorporation of variable transaction fees attached to the block reward, or to capture

the price volatilities to convert the reward to a fiat currency.

Let us therefore assume now that the up- and downward jumps in the dynamics of the pool manager's surplus are stochastic. Under certain assumptions on the nature of these jumps, this will allow us to still derive closed form formulas for $\widehat{\psi}$ and $\hat{V}$ in the spirit of [2], see also [6, Ch. 4]. Equation (8) then is replaced by

$$R_t = u - \sum_{n=1}^{M_t^d} W_n + \sum_{n=1}^{N_t} B_{r,n}, \quad t \geq 0, \tag{26}$$

where we assume W_n, $n \in \mathbb{N}$ to be i.i.d. positive random variables with cumulative distribution function F_W and finite mean representing payments to the pool members, and $B_{r,n}$, $n \in \mathbb{N}$ are assumed to be i.i.d. positive random variables with distribution function F_{B_r} and finite mean representing the remaining inflow of bounty rewards diminished by the simultaneous payout to the respective pool member. If one wishes to draw a parallel to the previous case with deterministic rewards, the random variable B_r assumes the role of $b - w$, the fixed block reward minus the payout to the pool member.

Consider the expected surplus of the pool manager as defined previously with a random time horizon T. Concretely, T follows an exponential distribution with mean t. As in the previous section, we are interested in $\hat{V}(u,t)$.

Proposition 5.1. *The quantity $\hat{V}(u,t) = \mathbb{E}(R_T \mathbb{I}_{\tau > T})$ for the pool surplus process (26) is a solution of the integral equation*

$$\lambda \int_0^\infty \hat{V}(u+b_r,t)\, dF_{B_r}(b_r) - (\lambda + \mu_d + 1/t)\hat{V}(u,t) + \mu_d \int_0^u \hat{V}(u-w,t)\, dF_W(w) + u/t = 0, \quad u \geq 0, \tag{27}$$

with boundary conditions $\hat{V}(u,t) = 0$ for all $u < 0$ and $0 \leq \hat{V}(u,t) \leq u + (\lambda \mathbb{E}[B_r] - \mu_d \mathbb{E}[W])t$ for all $u, t \geq 0$.

Proof. We extend the approach of the proof of Theorem 4.2 by conditioning on the size of the jump in case a jump occurs. For some small $h > 0$ we correspondingly get

$$\begin{aligned} \hat{V}(u,t) = {} & e^{-(\frac{1}{t}+\lambda+\mu_d)h}\hat{V}(u,t) + \frac{1}{t}\int_0^h e^{-s/t} e^{-(\lambda+\mu_d)s} u\, ds \\ & + \lambda \int_0^h e^{-\lambda s} e^{-(1/t+\mu_d)s} \int_0^\infty \hat{V}(u+b_r,t)\, dF_{B_r}(b_r)\, ds \\ & + \mu_d \int_0^h e^{-\mu_d s} e^{-(1/t+\lambda)s} \int_0^u \hat{V}(u-w,t)\, dF_W(w)\, ds. \end{aligned} \tag{28}$$

Taking the derivative w.r.t. h and setting $h = 0$, one obtains (27). The property $\hat{V}(u,t) = 0$ for all $u < 0$ follows by definition and the linear upper bound in u and t is obtained from the inequality $\hat{V}(u,t) \leq \mathbb{E}(R_T)$. □

Remark 5.2. For degenerate F_{B_r} and F_W (i.e. for constant B_r and W), the integral equation (27) simplifies to (19) (and for integer constants, we get back to the setting of Theorem 4.2).

For our purposes, it is very reasonable to assume (and will lead to simplified notation) that the generic random variables B_r and W are connected via

$$B_r = a\, W \tag{29}$$

for some constant $a > 1$ that depends on the number of miners in the pool. Indeed, W is the payment to the pool miner for solving a less complex puzzle, and B_r can be seen as the bounty reward when the more complex puzzle is solved minus the payment to the miner who solved it, and that latter payment will be a constant fraction, depending on the specification of the pool rules. Note that for most positive random variables, a scaled version of it belongs to the same class of random variables with only the parameter(s) changed, and the latter is indeed the case for all distributional assumptions that we will pursue in this paper. In any case, all results below can easily be adapted to the case when B_r and W follow distributions that are unrelated combinations of exponentials with different n and A_i's.

Let us now consider in more detail the case where both the up- and down-jumps are random variables whose distributions are combinations of exponentials. The latter class is dense in the class of all random variables on the positive half-line, so that the result is in fact quite general (see e.g. Dufresne [10]). Concretely, the density of downward jumps is then assumed to be of the form

$$f_W(w) = \sum_{i=1}^{n} A_i \alpha_i e^{-\alpha_i w}, \quad w > 0, \tag{30}$$

where $\alpha_1 < \alpha_2 < \ldots < \alpha_n$ and $A_1 + \cdots + A_n = 1$ (but the A_i are not necessarily positive). The Laplace transform of this density is given by

$$\tilde{f}_W(s) := \mathbb{E}(e^{-sW}) = \sum_{i=1}^{n} A_i \frac{\alpha_i}{\alpha_i + s}, \quad \mathrm{Re}(s) > -\alpha_1.$$

From (29), we then have

$$f_{B_r}(b_r) = \sum_{i=1}^{n} A_i \beta_i e^{-\beta_i b_r}, \quad b_r > 0 \tag{31}$$

with $\beta_i = \alpha_i / a$, $i = 1, \ldots, n$.

Theorem 5.3. *If W and B_r are random variables with densities given in (30) and (31), then we have*

$$\hat{V}(u,t) = \sum_{k=1}^{n} C_k e^{-r_k u} + u + t \sum_{i=1}^{n} A_i \left(\frac{\lambda}{\beta_i} - \frac{\mu_d}{\alpha_i} \right), \tag{32}$$

where $r_1, \ldots, r_n$ are the solutions with positive real parts of

$$\lambda \sum_{i=1}^{n} A_i \frac{\beta_i}{\beta_i + r} + \mu_d \sum_{i=1}^{n} A_i \frac{\alpha_i}{\alpha_i - r} - (\lambda + \mu_d + 1/t) = 0 \tag{33}$$

and

$$C_k = \frac{\sum_{j=1}^{n} B_j \prod_{h=1}^{n} (\alpha_j - r_h) \prod_{i=1, i\neq j}^{n} \frac{r_k - \alpha_i}{\alpha_j - \alpha_i}}{\prod_{h=1, h\neq k}^{n} (r_k - r_h)}, \quad k = 1, \ldots, n \tag{34}$$

with

$$B_j = \frac{1}{\alpha_j^2} - \frac{t}{\alpha_j} \sum_{i=1}^{n} A_i \left(\frac{\lambda}{\beta_i} - \frac{\mu_d}{\alpha_i} \right), \quad j = 1, \ldots, n.$$

Proof. Substituting (30) and (31) into (27), we get

$$\lambda \sum_{i=1}^{n} A_i \beta_i \int_0^\infty \hat{V}(u+b_r,t) e^{-\beta_i b_r} db_r \\ - (\lambda + \mu_d + 1/t)\hat{V}(u,t) + \mu_d \sum_{i=1}^{n} A_i \alpha_i \int_0^u \hat{V}(u-w,t) e^{-\alpha_i w} dw + u/t = 0, \quad u \geq 0.$$

The function $\hat{V}(u,t)$ then has the form

$$\hat{V}(u,t) = \sum_{k=1}^{n} C_k e^{-r_k u} + d_1 u + d_0,$$

for constants $C_1, \ldots, C_n, r_1, \ldots, r_n, d_0, d_1$ to be determined. In fact, plugging this ansatz into the above equation shows that comparing coefficients of $e^{-r_k u}$ exactly gives (33) (which is a generalized Lundberg equation in the terminology of ruin theory, cf. [6]). That equation has exactly n solutions with positive real part $r_1, \ldots, r_n$ and n solutions with negative real part (see e.g. [23]). The solutions with negative real part would enter $\hat{V}$ with positive real part and are correspondingly irrelevant for our purpose, as that would violate the linear boundedness of the resulting $\hat{V}$ (in other words, the coefficients in front of such terms need to be zero). Comparing coefficients of $e^{-\alpha_i u}$, $i = 1, \ldots, n$ gives

$$\sum_{k=1}^{n} \frac{C_k}{\alpha_i - r_k} = \frac{d_1}{\alpha_i^2} - \frac{d_0}{\alpha_i}, \quad i = 1, \ldots, n. \tag{35}$$

Coefficients in front of $u\, e^{-\alpha_i u}$, $i = 1, \ldots, n$ all cancel. After a little algebra, one sees that a comparison of coefficients of u in that equation establish $d_1 = 1$ and a comparison of the constant coefficients gives

$$d_0 = t \sum_{i=1}^{n} A_i \left(\frac{\lambda}{\beta_i} - \frac{\mu_d}{\alpha_i} \right).$$

These obtained values of d_1 and d_0 can now be plugged into (35), and the resulting system of linear equations can be solved explicitly to give (34), either by realizing that the coefficient matrix is a Cauchy matrix or by using the trick of rational function representation developed in [2, Sec.4]. □

Example 5.4. A particular simple example of the above is the case where W is exponentially distributed with parameter α and B_r is exponentially distributed with parameter β. In that case $n = 1$ in Theorem 5.3 and we obtain

$$\hat{V}(u,t) = \left(\frac{1}{\alpha^2} - \frac{t}{\alpha} \left(\frac{\lambda}{\beta} - \frac{\mu_d}{\alpha} \right) \right) (\alpha - R) e^{-Ru} + u + t \left(\frac{\lambda}{\beta} - \frac{\mu_d}{\alpha} \right), \tag{36}$$

where R is the (unique) solution with positive real part of

$$\lambda \frac{\beta}{\beta + r} + \mu_d \frac{\alpha}{\alpha - r} - (\lambda + \mu_d + 1/t) = 0. \tag{37}$$

Let us now move on to study the ruin probability $\widehat{\psi}(u,t) = \mathbb{E}\left[\psi(u,T)\right]$ in the present context.

Theorem 5.5. *If W and B_r are random variables with densities given in (30) and (31), then we have*

$$\widehat{\psi}(u,t) = \sum_{k=1}^{n} D_k e^{-r_k u}, \tag{38}$$

where $r_1, \dots, r_n$ are the n solutions with positive real parts of (33) and

$$D_k = \frac{\sum_{j=1}^{n} \frac{1}{\alpha_j} \prod_{h=1}^{n} (\alpha_j - r_h) \prod_{i=1, i\neq j}^{n} \frac{r_k - \alpha_i}{\alpha_j - \alpha_i}}{\prod_{h=1, h\neq k}^{n} (r_k - r_h)}, \quad k = 1, \dots, n. \tag{39}$$

Proof. We can proceed in the same way as in the proof of Proposition 5.1 to derive an integral equation for the ruin probability. The analogue of Equation (28) here is

$$\begin{aligned} \widehat{\psi}(u,t) = e^{-(\frac{1}{t}+\lambda+\mu_d)h}\widehat{\psi}(u,t) + \lambda \int_0^h e^{-\lambda s} e^{-(1/t+\mu_d)s} \int_0^\infty \widehat{\psi}(u+b_r,t)\, dF_{B_r}(b_r)\, ds \\ + \mu_d \int_0^h e^{-\mu_d s} e^{-(1/t+\lambda)s} \left(\int_0^u \widehat{\psi}(u-w,t)\, dF_W(w) + \int_u^\infty 1\, dF_W(w) \right) ds. \end{aligned} \tag{40}$$

Taking the derivative w.r.t. h and evaluating at $h = 0$ then gives

$$\lambda \int_0^\infty \widehat{\psi}(u+b_r,t)\, dF_{B_r}(b_r) - (\lambda+\mu_d+1/t)\widehat{\psi}(u,t) + \mu_d \int_0^u \widehat{\psi}(u-w,t)\, dF_W(w) + \mu_d(1-F_W(u)) = 0, \quad u \geq 0. \tag{41}$$

Here the boundary conditions are $\widehat{\psi}(u,t) = 1$ for $u < 0$ and $\widehat{\psi}(u,t) \leq 1$ for $u \geq 0$ and arbitrary $t > 0$, and uniqueness of its solution follows analogously to Theorem 5.3. Under the assumptions on F_{B_r} and F_W this reads

$$\begin{aligned} \lambda \sum_{i=1}^{n} A_i \beta_i \int_0^\infty \widehat{\psi}(u+b_r,t)\, e^{-\beta_i b_r}\, db_r - (\lambda + \mu_d + 1/t)\widehat{\psi}(u,t) \\ + \mu_d \sum_{i=1}^{n} A_i \alpha_i \int_0^u \widehat{\psi}(u-w,t)\, e^{-\alpha_i w}\, dw + \mu_d \sum_{i=1}^{n} A_i e^{-\alpha_i u} = 0, \quad u \geq 0. \end{aligned} \tag{42}$$

In analogy to the proof of Theorem 5.3 we then see that the ruin probability must have the form

$$\widehat{\psi}(u,t) = \sum_{k=1}^{n} D_k e^{-r_k u}$$

for constants $D_1, \dots, D_n$ to be determined, and $r_1, \dots, r_n$ being the n positive solutions of (33). The constants D_k are now obtained by substituting the above expression into (42) and comparing coefficients of $e^{-\alpha_i u}$, $i = 1, \dots, n$. This gives

$$\sum_{k=1}^{n} \frac{D_k}{\alpha_i - r_k} = \frac{1}{\alpha_i}, \quad i = 1, \dots, n. \tag{43}$$

This system of linear equations is again of Cauchy matrix form with explicit solution (39), establishing the result. □

Example 5.6. If W and B_r are exponentially distributed with parameter α and β, respectively, then

(38) simplifies to

$$\widehat{\psi}(u,t) = (1 - R/\alpha)e^{-Ru},\ u \geq 0, \tag{44}$$

where R is the (unique) solution with positive real part of (37).
Note that for $t \to \infty$ one obtains $R = (\lambda\alpha - \mu_d\beta)/(\lambda + \mu_d) > 0$, so that

$$\psi(u) = \frac{\mu_d(1+\beta/\alpha)}{\lambda+\mu_d} e^{-\frac{\lambda\alpha-\mu_d\beta}{\lambda+\mu_d}u},\ u \geq 0. \tag{45}$$

In particular, without initial capital in the pool, the infinite-time ruin probability amounts to

$$\psi(0) = \frac{\mu_d(1+\beta/\alpha)}{\lambda+\mu_d},$$

in accordance with Formula (8.1) in [2].

6. Individual miner analysis

6.1 Deterministic rewards

Comparing the formula describing the miner's surplus under the PPS pooling scheme (7) with the solo-mining surplus (3), one can see that they are in fact the same type of process, only distinguished by the reward amount and frequency. Correspondingly, the formulas obtained by Albrecher and Goffard [3] for the expected value of the surplus and the ruin probability of a honest miner apply in the PPS case with deterministic rewards. Adapted to the present context, we hence get:

Theorem 6.1. *[3] For the miner's surplus process $R_t^i = u - c_i \cdot t + M_t^i \cdot w,\ t \geq 0$, with $M_t^i \sim Poisson(p_i\mu t)$, the value function $\hat{V}(u,t)$ can be expressed as*

$$\hat{V}(u,t) = u + (p_i\mu w - c_i)t(1 - e^{\rho^* u}), \tag{46}$$

where ρ^* is the negative solution of the equation

$$-c_i\rho + p_i\mu(e^{w\rho} - 1) = 1/t. \tag{47}$$

Theorem 6.2. *[3] For the same surplus process, the ruin probability with exponential time horizon is given by $\hat{\psi}(u,t) = e^{\rho^* u}$, where ρ^* is the negative solution of (47).*

6.2 Stochastic rewards

Consider now the same surplus process as in the previous section, but with stochastic rewards. Let us define this process by

$$R_t^i = u - c_i \cdot t + \sum_{n=1}^{M_t^i} W_n,\ t \geq 0, \tag{48}$$

where we assume $W_n,\ n \in \mathbb{N}$ to be i.i.d. positive random variables with cumulative distribution function F_W and finite mean and $M_t^i \sim Poisson(p_i\mu t)$ as previously. This type of process is denominated as the *dual problem* in the insurance context, see e.g. [7]. We assume that the net profit condition

$p_i\mu\mathbb{E}[W_n] > c_i$ is satisfied.
We are again interested in deriving the expected value of the surplus and the ruin probability for the miner. To simplify the computations, we consider again an exponential time horizon.

Theorem 6.3. *For exponential time horizon, the expected value of the miner's surplus $\hat{V}(u,t)$ can be expressed as the solution of the integro-differential equation*

$$c_i\hat{V}'(u,t) + (\frac{1}{t} + p_i\mu)\hat{V}(u,t) - p_i\mu\int_0^{+\infty}\hat{V}(u+w,t)dF_W(w) - u/t = 0, \tag{49}$$

with boundary conditions $\hat{V}(0,t) = 0$ and $0 \leq \hat{V}(u,t) \leq u - c_it + p_i\mu\mathbb{E}[W]$.

Proof. As in previous sections, by conditioning the occurrence of T to a small time interval $(0,h)$, we can write the value function as

$$\begin{aligned}\hat{V}(u,t) = e^{-h(\frac{1}{t}+p_i\mu)}\hat{V}(u-c_ih,t) + \int_0^h \frac{1}{t}e^{-s(\frac{1}{t}+p_i\mu)}(u-c_is)ds \\ + \int_0^h p_i\mu e^{-s(\frac{1}{t}+p_i\mu)}\int_0^{+\infty}\hat{V}(u-c_ih+w,t)dF_W(w)ds.\end{aligned} \tag{50}$$

Taking the derivative w.r.t. h and evaluating it at $h = 0$ gives us (49). The boundary condition follows from ruin considerations. □

For rewards whose distribution is a combination of exponentials (30), we can refine Theorem 6.3.

Theorem 6.4. *When W has density $f_W(w) = \sum_{j=1}^n A_j\alpha_j e^{-\alpha_j w}$, $w > 0$, then*

$$\hat{V}(u,t) = t\left(c_i - p_i\mu\sum_{j=1}^n\frac{A_j}{\alpha_j}\right)e^{-Ru} + u + t\left(p_i\mu\sum_{j=1}^n\frac{A_j}{\alpha_j} - c_i\right),\ u > 0, \tag{51}$$

where R is the unique solution with positive real part of the equation

$$c_iR + p_i\mu\sum_{j=1}^n\frac{A_j\alpha_j}{R+\alpha_j} - (\frac{1}{t} + p_i\mu) = 0.$$

Proof. Equation (49) translates into

$$c_i\hat{V}'(u,t) + (\frac{1}{t} + p_i\mu)\hat{V}(u,t) - p_i\mu\sum_{j=1}^n A_j\alpha_j\int_0^{+\infty}\hat{V}(u+w,t)e^{-\alpha_j w}dw - u/t = 0. \tag{52}$$

This equation has a solution of the form

$$\hat{V}(u,t) = Ce^{-Ru} + d_1u + d_0 \tag{53}$$

and we plug this ansatz into (52)

$$\begin{aligned}&c_i(-RCe^{-Ru} + d_1) + (\frac{1}{t} + p_i\mu)(Ce^{-Ru} + d_1u + d_0) \\ &- p_i\mu\sum_{j=1}^n A_j\alpha_j\int_0^{+\infty}(Ce^{-R(u+w)} + d_1(u+w) + d_0)e^{-\alpha_j w}dw - u/t = 0.\end{aligned} \tag{54}$$

Comparing coefficients, we obtain

$$d_1 = 1, \quad d_0 = t\left(p_i\mu \sum_{j=1}^{n} \frac{A_j}{\alpha_j} - c_i\right).$$

Further, a comparison of the coefficients in front of e^{-Ru} simplifies to the following equation:

$$c_i R + p_i\mu \sum_{j=1}^{n} \frac{A_j\alpha_j}{R+\alpha_j} - (\frac{1}{t} + p_i\mu) = 0. \tag{55}$$

Similarly to the Lundberg equation derived in [18], we note that there is one positive root R to this equation. To complete the proof, we consider the boundary condition $\hat{V}(0,t) = 0$ and substituting into the ansatz gives $C = -d_0$. □

Example 6.5. When W is exponentially distributed, i.e. $f_W(w) = \alpha e^{-\alpha w}$, $w > 0$, Equation (51) simplifies to

$$\hat{V}(u,t) = t\left(c_i - \frac{p_i\mu}{\alpha}\right)e^{-Ru} + u + t\left(\frac{p_i\mu}{\alpha} - c_i\right), \ u > 0, \tag{56}$$

where R is the solution with positive real part of

$$c_i R^2 + (\alpha c_i - \frac{1}{t} - p_i\mu)R - \alpha\frac{1}{t} = 0.$$

Theorem 6.6. *For exponential time horizon, the miner's ruin probability can be expressed as*

$$\hat{\psi}(u,t) = e^{-R\cdot u}, \tag{57}$$

where R is the unique positive root of

$$p_i\mu + \frac{1}{t} - c_i R = p_i\mu\mathbb{E}[e^{-RW_n}]. \tag{58}$$

Proof. The proof is adapted from Example 2 of Mazza and Rullière [19]. From the latter, we have that the Laplace transform of the ruin time τ in the dual problem is $\mathbb{E}[e^{-s\tau}] = e^{-R(s)\cdot u}$, with $R(s)$ being the unique positive root of $p_i\mu + s - c_i R = p_i\mu\mathbb{E}[e^{-RW_n}]$. Since the ruin probability up to an exponential time horizon can be rewritten as

$$\hat{\psi}(u,t) = \mathbb{E}[\mathbb{P}(T > \tau) \mid \tau], \tag{59}$$

with $T \sim Exp(1/t)$, it immediately follows that

$$\hat{\psi}(u,t) = \mathbb{E}[e^{\tau/t}] \tag{60}$$

which completes the proof. □

Example 6.7. If W is an exponential random variable, i.e. $f_W(w) = \alpha e^{-\alpha w}$, $w > 0$, then the ruin probability reduces to

$$\hat{\psi}(u,t) = e^{-R^* u}, \tag{61}$$

where

$$R^* = \frac{1/t + p_i\mu - c_i\alpha + \sqrt{\Delta}}{2c_i},\ \Delta = (c_i\alpha - p_i\mu - 1/t)^2 + 4c_i\alpha/t. \tag{62}$$

Remark 6.8. Results concerning the ruin probability can also be retrieved from the respective results for a more general renewal model considered in Alcoforado et al. [4].

7. Numerical illustration

7.1 Pool manager

In this section, we will illustrate the pool dynamics in both the deterministic and stochastic setting. In addition, we will perform a sensitivity analysis on main decision variables from the pool's perspective.

First, let us define the set of parameters used in the following examples. For each illustration, we keep all the parameters fixed to these levels except the one that is varying : $t = 336,\ p_I = 0.1,\ q = 0.1,\ f = 0.02,\ b = 1000MU,\ w = (1-f)bq = 98MU,\ \lambda = 6p_I = 0.6,\ \mu_d = 6p_I(1/q - 1) = 5.4.$

The units we use are hours (h) for the time parameters and monetary units (MU) for the value functions. The choice for the time horizon t is equal to 2 weeks because it is linked to the period of difficulty adjustment. The monetary units are related to bitcoin in this way : $1000MU = 6.25BTC$. The reason for this scaling is purely practical to solve the deterministic problem which involves integer constraints. As of May 28th 2021, $1BTC \approx \$35670.5$, so $1MU \approx \$231.85$.

Figure 5 compares the function $\hat{V}(u,t)$ defined in Theorem 4.2 with the Monte Carlo simulation of the mining process with deterministic and exponential time horizon fixed at the same mean parameter. The functions are reduced by u to isolate the expected gain realized by the pool manager. We can see that the exact formula falls nicely within the 95% confidence interval bounds of the MC simulations within fixed or exponential time horizon. The red line represents the upper limit of the function to which it converges as $u \to +\infty$, which is also the expected value of the gain in absence of ruin considerations. One can see that for small levels of initial capital potential ruin affects the resulting profit considerably, and for any given u the pool manager can quantify the undesirable effect of ruin. Figure 6 exhibits the corresponding ruin probability $\hat{\psi}(u,t)$ for the mining pool. We can note that ruin is highly non-negligible for low levels of initial capital. Indeed, $\hat{\psi}(u, t = 336) < 5\%$ for $u > 22594$, which is equivalent to \$5238419. We also see how the exponential time horizon slightly underestimates the ruin probability for low capital levels, which is due to the skewness of the exponential distribution. This graph can also be interpreted sideways: if one fixes a threshold for the ruin probability on the vertical axis, the corresponding initial capital can be read off on the horizontal axis.

In Figure 7, we depict the sensitivity of the expected surplus and the ruin probability to the management fee f. Not surprisingly, the relationship between f and $\hat{\psi}(u,t)$ is decreasing, as the pool retains more reward for itself. The parameter f impacts the expected gain of the pool manager.

Remark 7.1. Note that here we consider the interplay of all factors in a static set-up for a fixed number of participants in the pool. One may then go one step further to consider the fact that a higher fee f may deter some participants to join the pool, with respect to their willingness to pay and

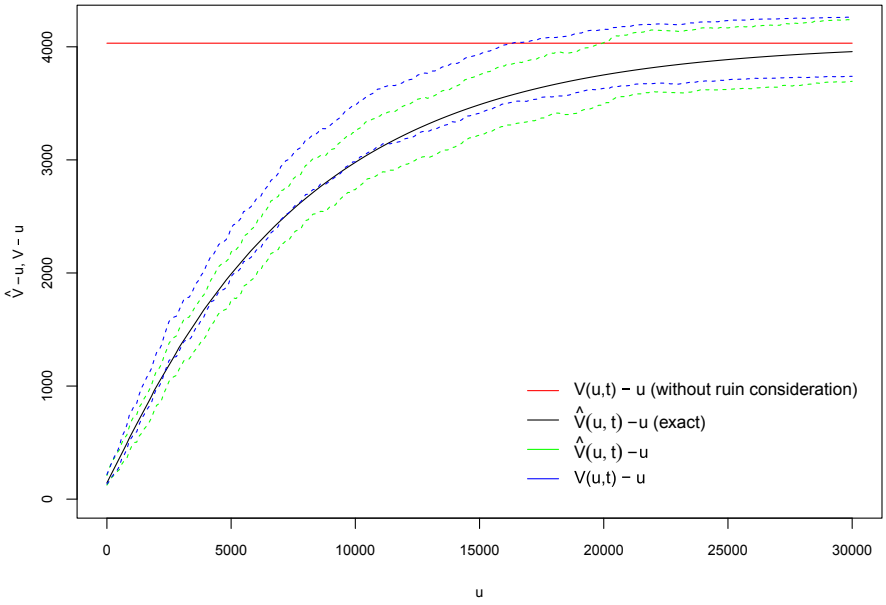


Figure 5: $\hat{V}(u,t) - u$ as a function of u and simulated $\hat{V}(u,t) - u$ and $V(u,t) - u$ with their 95% confidence interval bound in dashed with deterministic size jumps b and w.

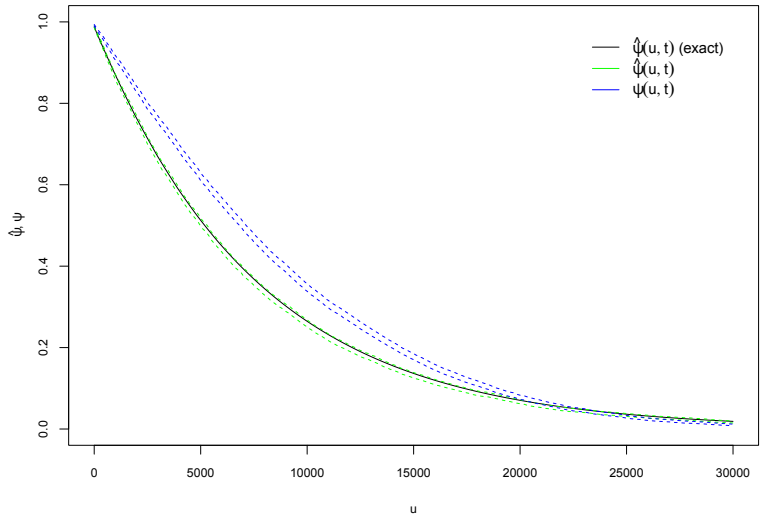
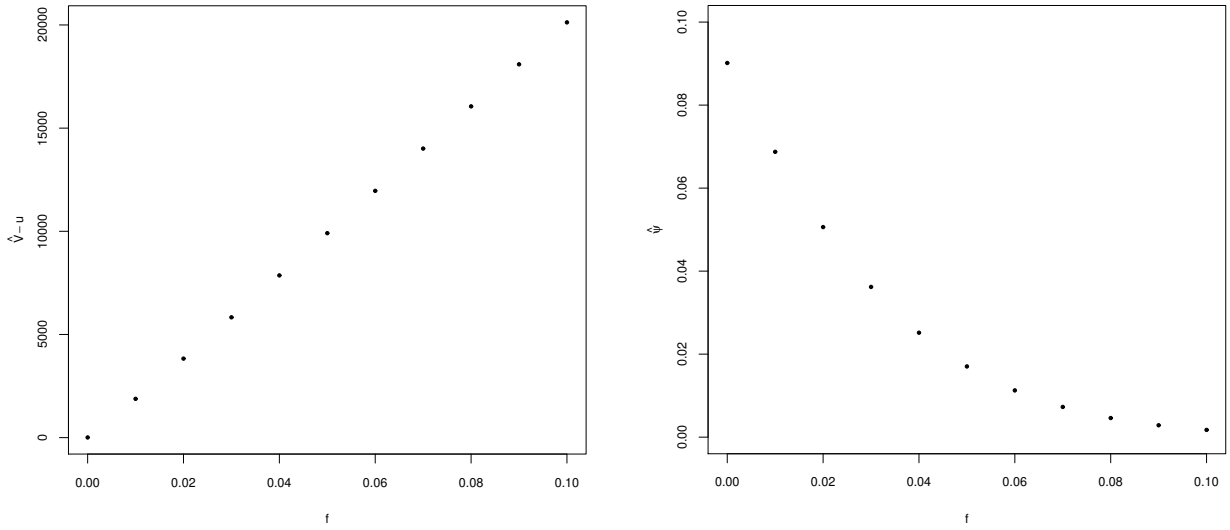


Figure 6: $\hat{\psi}(u,t)$ as a function of u and simulated $\hat{\psi}(u,t)$ and $\psi(u,t)$ with their 95% confidence interval bound in dashed with deterministic size jumps b and w.

when comparing with fees of other competitive pools in the market. This outflow of miners would consequently impact negatively the expected profit of the pool. However, such considerations naturally ask for an analysis with competing pools, which is beyond the scope of this paper.

In Figure 8, we explore the impact of the relative difficulty to find a share q on ruin and expected surplus.

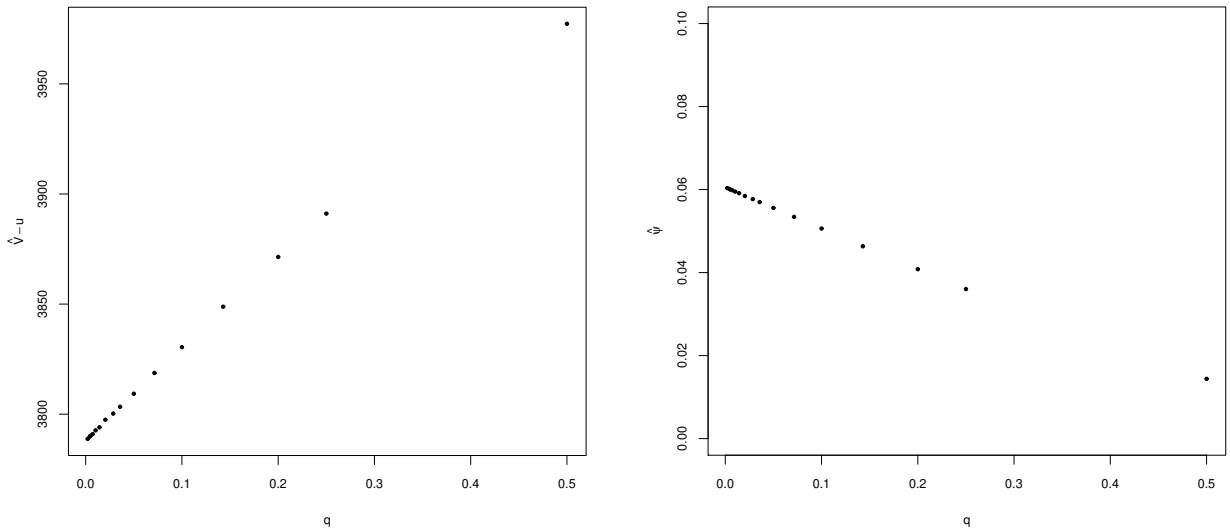
It is worthwhile to note that increasing q is profitable to the pool manager. Indeed, as q increases,



(a) $\hat{V}(u,t) - u$ as a function of f.

(b) $\hat{\psi}(u,t)$ as a function of f.

Figure 7: Sensitivity to f in case of deterministic rewards and exponential time horizon.



(a) $\hat{V}(u,t) - u$ as a function of q.

(b) $\hat{\psi}(u,t)$ as a function of q.

Figure 8: Sensitivity to q in case of deterministic rewards and exponential time horizon.

the payout of shares to the pool members is getting less frequent, thus the pool manager retains more liquidity and controls his probability of ruin at lower levels. The parameter q adjusts the magnitude of the risk transfer between the miners and their manager.

Figures 9, 10, 11, 12 illustrate the same concepts with exponentially distributed rewards. For comparison, the parameters for the exponential distributions are chosen so that the resulting mean matches the deterministic jump sizes, i.e. $\alpha = 1/w = 1/98, \beta = 1/b = 1/1000$.

Figure 13 gives a two-way sensitivity analysis with respect to the pool size p_I and the pool fee f. The

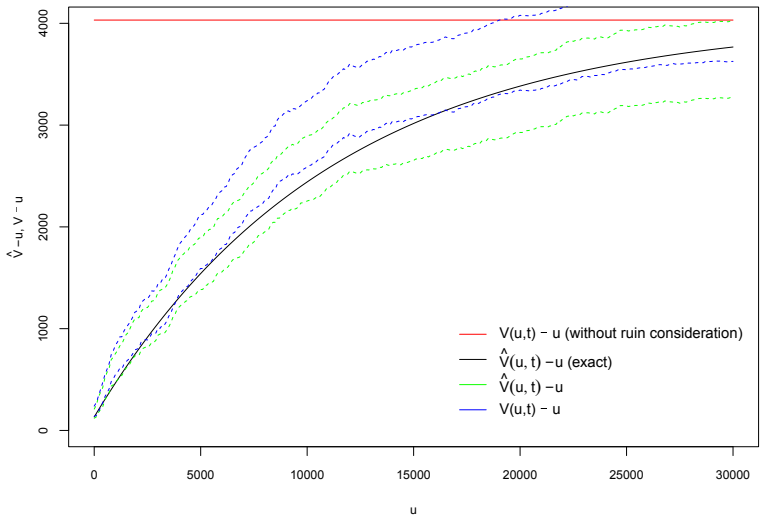


Figure 9: $\hat{V}(u,t) - u$ as a function of u and simulated $\hat{V}(u,t) - u$ and $V(u,t) - u$ with their 95% confidence interval bound in dashed. Both jumps are exponentially distributed.

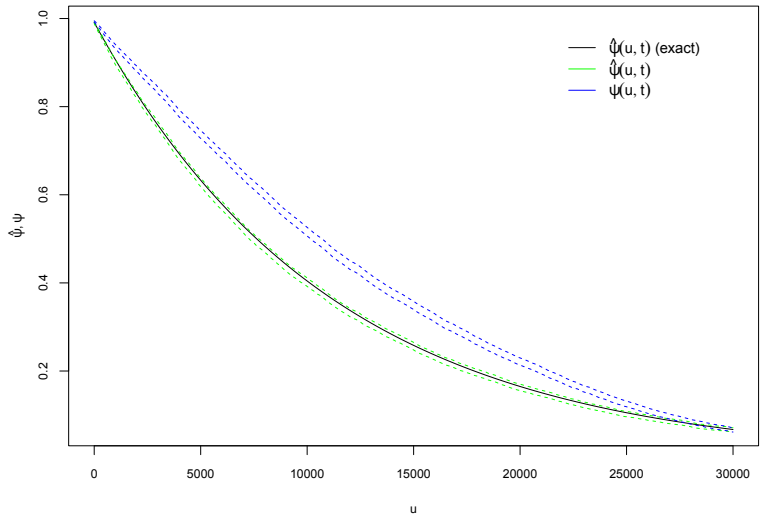
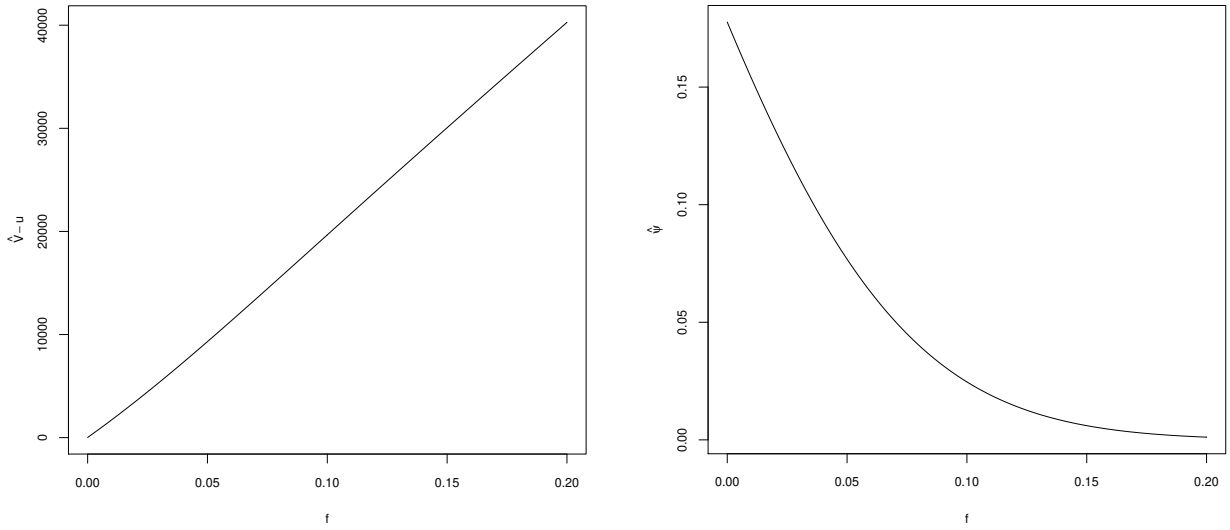


Figure 10: $\hat{\psi}(u,t)$ as a function of u and simulated $\hat{\psi}(u,t)$ and $\psi(u,t)$ with their 95% confidence interval bound in dashed. Both jumps are exponentially distributed.

level curves indicate the expected profit for the pool manager for different pool sizes.

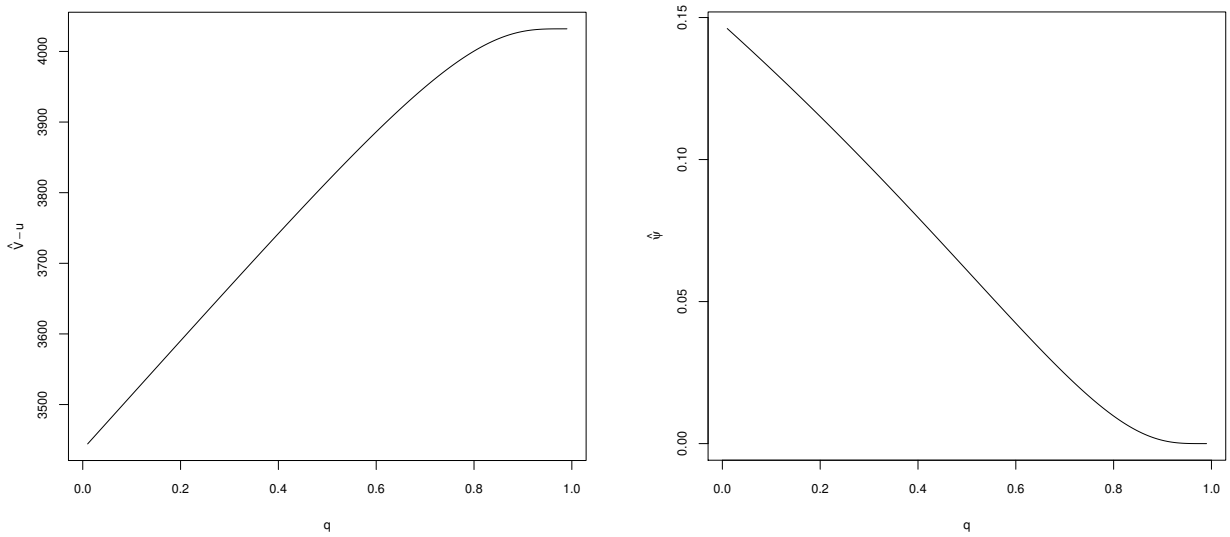
For a bigger pool size p_I, in order to maintain the same level of expected profit, the pool manager can reduce the fee size. One can clearly see an inverse relationship between the pool size and the fee. Thus, a bigger pool can diminish its fees to attract more miners and thus to grow even more. This implies a threat on the decentralized nature of the consensus protocol. If a mining pool manager concentrates more than 50% of the total hashpower, then the blockchain is prone to 51%-type attacks such as double spending in the bitcoin context. How can a smaller mining pool tackle this problem? One solution consists in offering to take on more risk by decreasing the difficulty of finding a share



(a) $\hat{V}(u,t) - u$ as a function of f.

(b) $\hat{\psi}(u,t)$ as a function of f.

Figure 11: Sensitivity to f in case of exponentially distributed rewards and exponential time horizon.



(a) $\hat{V}(u,t) - u$ as a function of q.

(b) $\hat{\psi}(u,t)$ as a function of q.

Figure 12: Sensitivity to q in case of exponentially distributed rewards and exponential time horizon.

which reduces to decreasing the value of q. Figure 14 shows the expected profit of two mining pools, one for which $p_I = 0.1$ and a smaller one for which $p_I = 0.02$, both having an initial capital level $u = 22500$, for both the reward and the time horizon being exponentially distributed. The level curves indicate that in terms of expected profit a smaller miner may decrease q without increasing the pool fee f, while maintaining the same level of profitability. That is not the case for the larger mining pool whose expected profit turns out to more sensitive to q.

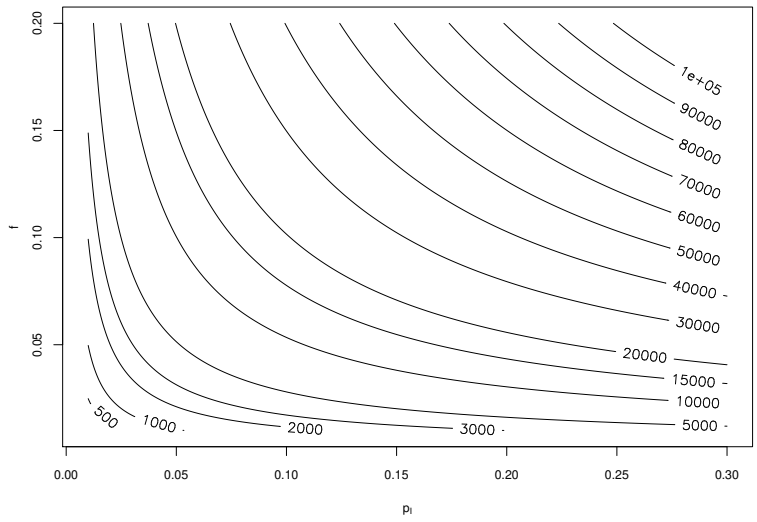
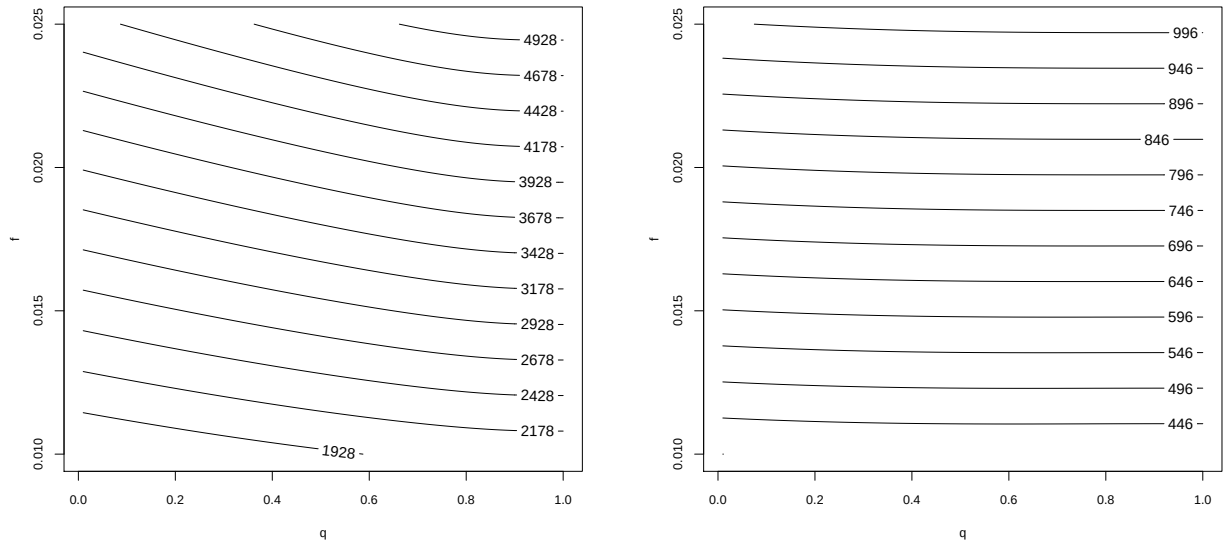


Figure 13: $\hat{V}(u,t)$ as a function of p_I and f for $u = 22500$. Both jumps are exponentially distributed.



(a) $\hat{V}(u,t) - u$ as a function of q and f for a large mining pool ($p_I = 0.1$).

(b) $\hat{V}(u,t) - u$ as a function of q and f for a small mining pool ($p_I = 0.02$).

Figure 14: Sensitivity to q and f of the expected profit of two mining pools of different size over and exponentially distributed time horizon and reward for $u = 22500$.

7.2 Individual miner

Let us now compare the situation of an individual miner before and after joining the pool. We recall Figure 3 (left panel), which examplifies the pool members' surplus. Also, the surplus of the member is described by (9). Finally, we use the results presented in Sections 6.1 and 6.2 to assess the pool effect for the individual miner's surplus following the protocol. Consider a miner in a deterministic rewards environment. We assume a PPS pool and consider a pool member whose hashpower is equal

to 1% of the pool's total hashpower, i.e. $p_i = 0.001$. For the choice of other parameters, we assume that the cost of electricity c is given by

$$c = p_i \times e_W \times \pi_W,$$

where e_W is the electricity consumption of the network expressed in kWh, and π_W is the price of electricity per kWh. For the sake of our example, we take the estimate of e_W as $\frac{115.541 \times 10^9}{365.25 \times 24}$.[3] The price of electricity is taken to be \$0.06, then converted to our MU. Therefore, the net profit condition is satisfied both with and without joining the pool. Figures 15 and 16 illustrate the expected surplus and ruin probability with deterministic rewards and exponential time horizon. One can observe how effective the risk reduction in case of joining the pool is for the individual miner. Figure 16 particularly emphasizes the drastic decrease of ruin probability for low capital levels.

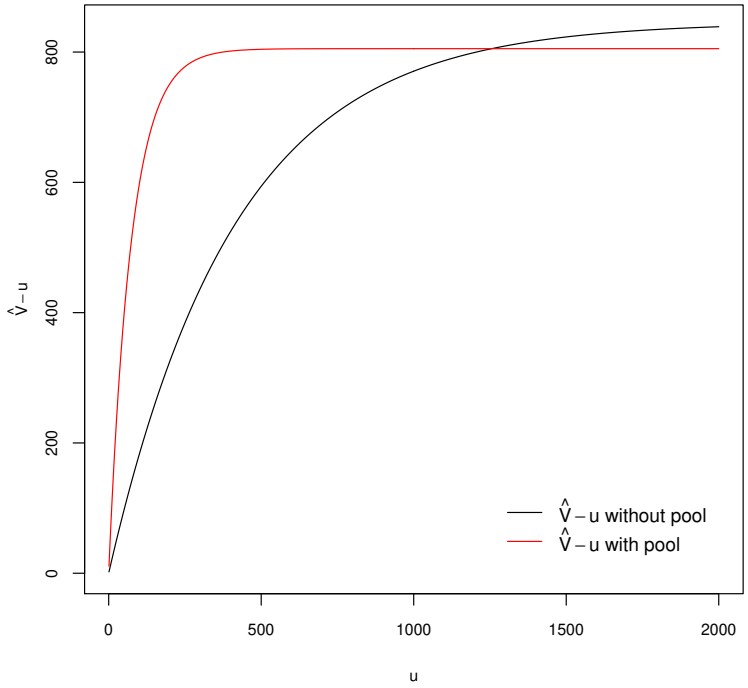


Figure 15: $\hat{V}(u,t) - u$ as a function of u for an individual pool miner alone in black and within the pool in red.

Up until a level of initial capital of $u = 1255$, it is more profitable for the miner to join the pool, whereas for higher levels of capital the pool fee becomes the main decision driver instead of the ruin considerations. Converted to USD, this amounts to approximately \$290,971. Recall that this is akin to the effects of reinsurance, as the miner cedes part of his risk to the pool in exchange of a fixed contractual payment (pool fee).

Finally, we investigate the sensitivity of the miner's expected surplus with respect to the key model parameters. In Figure 17, the miner can see for his level of initial capital u whether it is better to join the pool or not, depending on the employed fee f. As before, for higher levels of capital, the miner

[3] https://cbeci.org/, consulted on May 28th 2021.

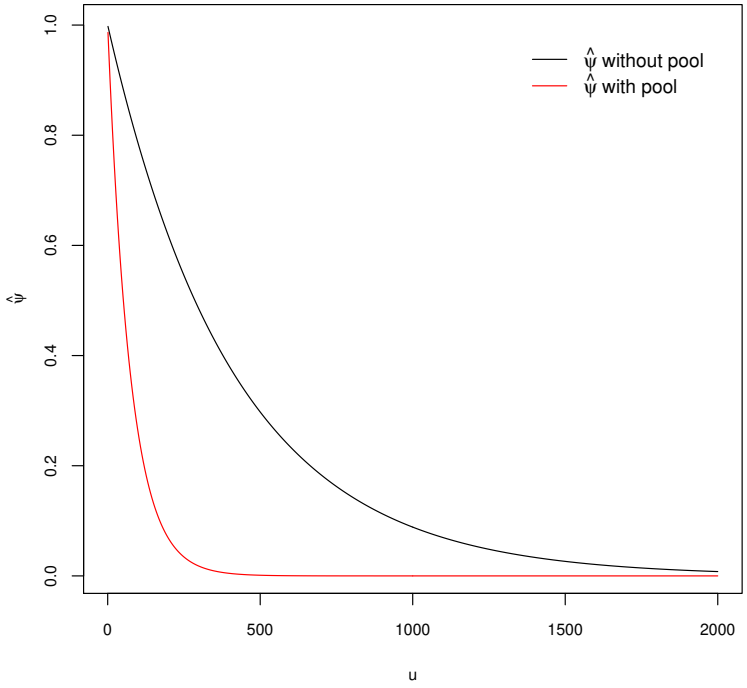


Figure 16: $\hat{\psi}(u,t)$ as a function of u for an individual pool miner alone in black and within the pool in red.

is less willing to accept high fees than a miner with less initial capital. We also observe that the two red lines (miner in the pool with different initial capital u) are much closer to each other than the two black lines (miner outside of the pool with different initial capital u). This is due to the risk reduction of the miner inside the pool, since he is transferring part of the risk to the pool and getting more frequent rewards.

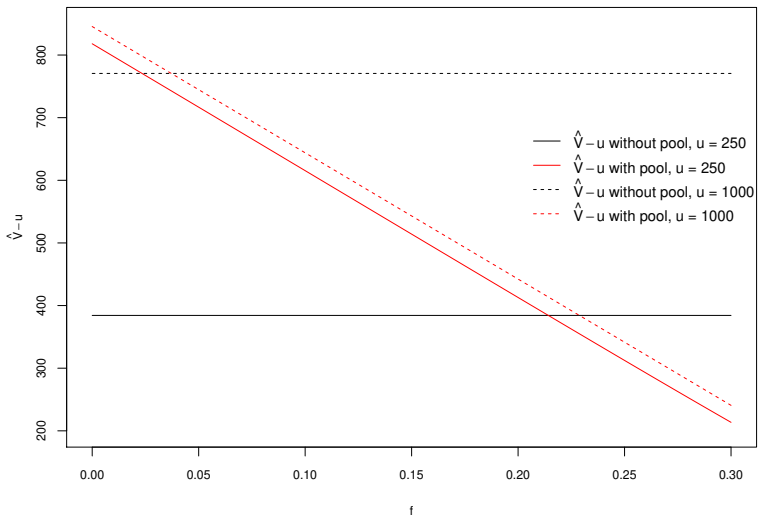


Figure 17: $\hat{V}(u,t) - u$ as a function of f for an individual pool miner alone in black and within the pool in red.

Figure 18 shows the level curves of $\hat{V}(u,t)$ with a varying difficulty for the miner's problem q and pool fee f. Note that not joining the pool is equivalent to setting the difficulty level equal to the block finding problem level and letting the pool fee be $f = 0$.

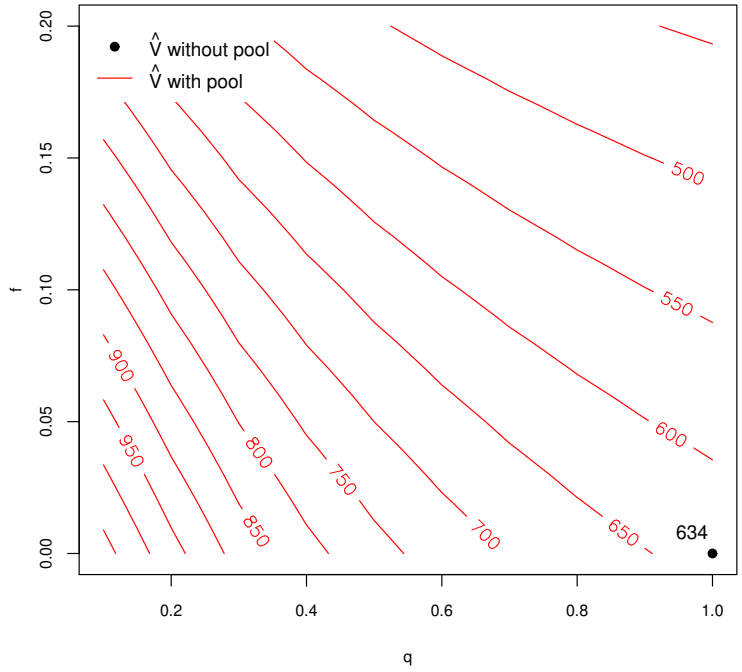


Figure 18: $\hat{V}(u,t)$ as a function of q and f for an individual pool miner alone in black and within the pool in red.

With such a two-way analysis, the pool can fix an appropriate fee and the miner can see whether he is better off joining the pool for his given level of capital u.

The miner's decision to join a *pay-per-share* mining pool does not depend on the size of the mining pool. Hence a miner will be indifferent whether to direct her hashpower towards a small or large pool. All that matters is the level of expected profit (decreasing in f) and the share of risk transferred to the mining pool (decreasing in q). Decentralization will prevail if the preferences, more specifically the risk aversion, of both the pool managers and the individual miners are sufficiently heterogeneous. Note that a situation where a mining pool would control most of the computing power is not desirable for anyone. The blockchain would then be prone to attacks and the associated cryptocurrency would no longer be of value.

8. Conclusion

In this paper, we developed a framework for a bitcoin mining pool analysis from a risk and profitability perspective. Given a pay-per-share pooling scheme, we investigated the profitability of a pool under ruin probability considerations, which allows us to derive original results for the pool manager's expected profit. When describing the pool income process as a stochastic double-sided jump process, one can adapt techniques developed in the actuarial literature for applications in the blockchain universe.

In addition, we also looked at the problem from the individual miner's side, to identify conditions under which it is profitable for her to enter the pool or not.

We find that ignoring ruin considerations highly overestimates the expected gain for a pool for small values of initial capital and quantify the required capital level needed for which the ruin aspect becomes negligible. Moreover, we define a trade-off between the main pool defining parameters to set up conditions for optimizing the pool profit for different levels of capital. For an individual miner, pooling has similar effects as a reinsurance treaty for an insurer. We provide a sensitivity analysis that can be helpful for the miner to select the most appropriate pool given his initial parameters.

For a randomized time horizon, it was possible to obtain explicit formulas for all quantities of interest. The flexibility of our model enabled to consider deterministic as well as stochastic reward sizes. The established formulas for combinations of exponentials are in fact quite flexible, as any other distribution on the positive halfline can be approximated arbitrary well with such distributions (cf. [10]). Naturally, some restrictive assumptions were needed to enable the explicit mathematical treatment in this paper, in particular the assumption of independent and identically distributed jump sizes. It will be interesting in future research to look into relaxing these assumptions.

The study of the formation of mining pools naturally raises the question of whether they pose a threat to the decentralized nature of blockchain-based applications. We find that the size of the mining pool does not interfere in a miner's decision making process. A miner chooses a mining pool according to the share of risk she wishes to cede and the profit she wishes to make. The preferences of miners and pool managers have been analysed using game theory in Cong et al. [9] and Li et al. [17]. The results of the present paper may serve as concrete risk management tools for miners and pool managers that could also be integrated as value or cost functions within such a game-theoretic approach.

Acknowledgements

Hansjörg Albrecher acknowledges financial support from the Swiss National Science Foundation Project 200021_191984.

References

[1] S. Al-Kuwari, J. H. Davenport, and R. J. Bradford. *Cryptographic Hash Functions: Recent Design Trends and Security Notions*. Cryptology ePrint Archive, Report 2011/565. https://ia.cr/2011/565. 2011 (↑ 3).

[2] H. Albrecher, H. U. Gerber, and H. Yang. "A direct approach to the discounted penalty function". In: *North American Actuarial Journal* 14.4 (2010), pp. 420–434 (↑ 2, 10, 14, 16, 18).

[3] H. Albrecher and P.-O. Goffard. "On the profitability of selfish blockchain mining under consideration of ruin". In: *Operations Research* 70.1 (2022), pp. 179–200 (↑ 2, 5, 10, 18).

[4] R. G. Alcoforado, A. I. Bergel, R. M. R. Cardoso, A. D. E. dos Reis, and E. V. Rodríguez-Martínez. "Ruin and Dividend Measures in the Renewal Dual Risk Model". In: *Methodology and Computing in Applied Probability* (2021). DOI: 10.1007/s11009-021-09876-4 (↑ 21).

[5] A. Antonopoulos. *Mastering Bitcoin*. O'Reilly UK Ltd., July 2017. ISBN: 1491954388. URL: https://www.ebook.de/de/product/26463992/andreas_antonopoulos_mastering_bitcoin.html (↑ 4).

[6] S. Asmussen and H. Albrecher. *Ruin probabilities*. World Scientific, Singapore, 2010 (↑ 2, 9, 14, 16).

[7] B. Avanzi, H. U. Gerber, and E. S. Shiu. "Optimal dividends in the dual model". In: *Insurance: Mathematics and Economics* 41.1 (2007), pp. 111–123. DOI: 10.1016/j.insmatheco.2006.10.002 (↑ 18).

[8] R Bowden, H. Keeler, A. Krzesinski, and P. Taylor. "Modeling and analysis of block arrival times in the Bitcoin blockchain". In: *Stochastic Models* 36.4 (2020), pp. 602–637 (↑ 5).

[9] L. W. Cong, Z. He, and J. Li. "Decentralized Mining in Centralized Pools". In: *The Review of Financial Studies* 34.3 (Apr. 2020), pp. 1191–1235. ISSN: 0893-9454. DOI: 10.1093/rfs/hhaa040. eprint: https://academic.oup.com/rfs/article-pdf/34/3/1191/36264472/hhaa040.pdf. URL: https://doi.org/10.1093/rfs/hhaa040 (↑ 3, 30).

[10] D. Dufresne. "Fitting combinations of exponentials to probability distributions". In: *Applied Stochastic Models in Business and Industry* 23.1 (2007), pp. 23–48 (↑ 15, 30).

[11] D. Easley, M. O'Hara, and S. Basu. "From mining to markets: The evolution of bitcoin transaction fees". In: *Journal of Financial Economics* 134.1 (2019), pp. 91–109 (↑ 2).

[12] P.-O. Goffard. "Fraud risk assessment within blockchain transactions". In: *Advances in Applied Probability* 51.2 (2019), pp. 443–467 (↑ 9).

[13] A. J. Jerri. *Linear difference equations with discrete transform methods*. Vol. 363. Springer Science & Business Media, 2013 (↑ 11).

[14] S. Kasahara, and J. Kawahara. "Effect of Bitcoin fee on transaction-confirmation process". In: *Journal of Industrial & Management Optimization* 15.1 (2019), pp. 365–386. DOI: 10.3934/jimo.2018047 (↑ 2).

[15] J. Kingman. *Poisson Processes*. Oxford Studies in Probability. Clarendon Press, 1992. URL: https://books.google.ch/books?id=VEiM-OtwDHkC (↑ 8).

[16] C. Labbé and K. P. Sendova. "The expected discounted penalty function under a risk model with stochastic income". In: *Applied Mathematics and Computation* 215.5 (2009), pp. 1852–1867 (↑ 2).

[17] Z. Li, A. M. Reppen, and R. Sircar. *A Mean Field Games Model for Cryptocurrency Mining*. 2019. arXiv: 1912.01952 [math.OC] (↑ 30).

[18] Y. Lu. ""A Direct Approach to the Discounted Penalty Function", Hansjörg Albrecher, Hans U. Gerber, and Hailiang Yang, Volume 14, No. 4, 2010". In: *North American Actuarial Journal* 14.4 (2010), pp. 438–441. DOI: 10.1080/10920277.2010.10597601 (↑ 20).

[19] C. Mazza and D. Rullière. "A link between wave governed random motions and ruin processes". In: *Insurance: Mathematics and Economics* 35.2 (2004), pp. 205–222. DOI: 10.1016/j.insmatheco.2004.07.014 (↑ 20).

[20] slush pool. "Reward system specifications". In: (2021). URL: https://help.slushpool.com/en/support/solutions/articles/77000426280-reward-system-specification (↑ 7).

[21] M. Rosenfeld. "Analysis of Bitcoin Pooled Mining Reward Systems". In: *CoRR* abs/1112.4980 (2011). arXiv: 1112.4980. URL: http://arxiv.org/abs/1112.4980 (↑ 2, 7).

[22] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden. "Incentive Compatibility of Bitcoin Mining Pool Reward Functions". In: *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2017, pp. 477–498. DOI: 10.1007/978-3-662-54970-4_28 (↑ 2, 7).

[23] Z. Zhang, H. Yang, and S. Li. "The Perturbed Compound Poisson Risk Model with Two-Sided Jumps". In: *Journal of Computational and Applied Mathematics* 233 (2010), pp. 1773–1784 (↑ 16).

[24] S. Zhu, W. Li, H. Li, C. Hu, Z. Cai, and and. "A survey: Reward distribution mechanisms and withholding attacks in Bitcoin pool mining". In: *Mathematical Foundations of Computing* 1.4 (2018), pp. 393–414. DOI: 10.3934/mfc.2018020 (↑ 2).

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

$$G_n^{(1)}(x|U) = n\, G_{n-1}(x|\mathcal{E}U), \tag{63}$$

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

$$G_n(u_1|U) = 0, \quad n \geq 1. \tag{64}$$

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

$$G_n(x|U) = n! \int_{u_1}^{x} \left[\int_{u_2}^{y_1} \mathrm{d}y_2 \ldots \int_{u_n}^{y_{n-1}} \mathrm{d}y_n \right] \mathrm{d}y_1. \tag{65}$$

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 identity is used inside the proof of Theorem 4.1 together with the following property Note that

$$G_n(x|a + bU) = b^n G_n\left((x-a)/b\,|U\right), \quad n \geq 1, \tag{66}$$

Lastly, the numerical evaluation of (15) can rely on the recursive relations

$$G_n(x|U) = x^n - \sum_{k=0}^{n-1} \binom{n}{k} u_{k+1}^{n-k} G_k(x|U), \quad n \geq 1. \tag{67}$$

Formula (67) follows from an Abelian expansion of x^n based on (63), and (64).

B. Proof of Theorem 4.1

The event $\{\tau \in (t, t+dt)\}$ can be viewed conditioned over the values of the process $(N_t)_{t\geq 0}$. In other terms,

$$\{\tau \in (t, t+dt)\} = \bigcup_{n=0}^{+\infty} \{\tau \in (t, t+dt)\} \cap \{N_t = n\}. \tag{68}$$

We distinguish according to the value of N_t. For $N_t = 0$, Equation (14) can be rewritten as

$$\tau = \inf\{t \geq 0; M_t^d > u/w\}, \tag{69}$$

which occurs when the $\lceil \frac{u}{w} \rceil^{th}$ jump of M_t^d occurs at t, where $\lceil x \rceil$ denotes the ceiling function. It follows that

$$\{\tau \in (t, t+dt)\} \cap \{N_t = 0\} = \{S^d_{\lceil \frac{u}{w} \rceil} \in (t, t+dt)\} \cap \{N_t = 0\} \tag{70}$$

and

$$f_{\tau | N_t = 0}(t) = f_{S^d_{\lceil \frac{u}{w} \rceil}}(t), \ t \geq 0. \tag{71}$$

In case $N_t \geq 1$, one needs to constrain $\{M_t^d, \ t \geq 0\}$ so it does not reach $N_{u,s}w/(b-w)+u/(b-w)$ for any time $s < t$ but does so at t. Let $(v_n)_{n\geq 0}$ is a sequence of integers defined as $v_n = \lceil n(b-w)/w + u/w \rceil$, $n \geq 0$. We have

$$\{\tau \in (t, t+dt)\} \cap \{N_t \geq 1\} = \bigcup_{n=1}^{+\infty} \bigcap_{k=1}^{n} \{T_k \leq S^d_{v_{k-1}}\} \cap \{S^d_{v_n} \in (t, t+dt)\} \cap \{N_t = n\}, \tag{72}$$

as $M_t^d > \underbrace{N_t}_{=n}(b-w)/w + u/w$ at the time of the fatal jump (and before t, N_t reaches each step before the payout process surpasses it). Now

$$\mathbb{P}\left[\{\tau \in (t, t+dt)\} \cap \{N_t \geq 1\}\right] = \sum_{n=1}^{+\infty} \mathbb{P}\left[\bigcap_{k=1}^{n} \{T_k \leq S^d_{v_{k-1}}\} \cap \{S^d_{v_n} \in (t, t+dt)\} \mid N_t = n\right] \mathbb{P}\left[N_t = n\right]. \tag{73}$$

By the order statistic property, we get

$$\begin{aligned}
&\mathbb{P}\left[\bigcap_{k=1}^{n} \{T_k \leq S^d_{v_{k-1}}\} \cap \{S^d_{v_n} \in (t, t+dt)\} \mid N_t = n\right] \\
&= \mathbb{P}\left[\bigcap_{k=1}^{n} \{U_{k:n} \leq F_t\left(S^d_{v_{k-1}}\right)\} \cap \{S^d_{v_n} \in (t, t+dt)\}\right] \\
&= \mathbb{P}\left[\bigcap_{k=1}^{n} \{U_{k:n} \leq F_t\left(S^d_{v_{k-1}}\right)\} \mid S^d_{v_n} \in (t, t+dt)\right] \mathbb{P}\left[S^d_{v_n} \in (t, t+dt)\right] \\
&= \mathbb{E}\left[(-1)^n G_n\left[0 \mid F_t\left(S^d_{v_0}\right), \ldots, F_t\left(S^d_{v_{n-1}}\right)\right] \mid S^d_{v_n} \in (t, t+dt)\right] \mathbb{P}\left[S^d_{v_n} \in (t, t+dt)\right],
\end{aligned} \tag{74}$$

where $(U_{1:n}, \ldots, U_{n:n})$ denote the order statistics of n i.i.d. unit uniform r.v. and $G_n(. \mid .)$ denote the Abel-Gontcharov polynomials, see Appendix A for a short presentation. Now take $F_t(s) = s/t, \ s \leq t$.

In virtue of the property (66), we have

$$\begin{aligned} G_n\left[0 \mid F_t\left(S^d_{v_0}\right), \ldots, F_t\left(S^d_{v_{n-1}}\right)\right] &= G_n\left[0 \mid S^d_{v_0}/t, \ldots, S^d_{v_{n-1}}/t\right] \\ &= \frac{1}{t^n} G_n\left[0 \mid S^d_{v_0}, \ldots, S^d_{v_{n-1}}\right]. \end{aligned} \tag{75}$$

Inserting that last expression into (74) yields the announced result (15).