A further study of some Markovian Bitcoin models from Göbel et al

Kayla Javier and Brian Fralix
School of Mathematical and Statistical Sciences, and CORI
Clemson University
Clemson, SC, USA

May 29, 2019

Abstract

We consider two different continuous-time Markov chain models recently studied in Göbel et al [7], which were created to model the interactions between a small pool of miners, and a larger collection of miners, within the Bitcoin network. The first model we discuss represents the case where all miners behave honestly and follow the Bitcoin protocol, while the second model represents the case where the smaller pool of miners use the selfish-mining strategy of Eyal and Sirer [3]. We give a new derivation of the stationary distribution of the process in the honest-mining case and further build on the results of [7] by showing that the normalizing constant can be expressed in closed-form. We also use similar techniques to derive expressions for the Laplace transforms of the transitions functions. We then illustrate how these techniques yield similar expressions for the stationary distribution of the process when the smaller pool implements Selfish Mining: the Laplace transforms of the transition functions can be calculated as well. Lastly, we briefly explain how our methods can be extended to more general models of a similar type.

Keywords: Bitcoin, blockchain, selfish mining, time-dependent behavior
2010 MSC: 60J28; 60K25

1 Introduction

Bitcoin is a decentralized digital payment system that allows users within the system to make transactions between one another without using a central authority (e.g. a bank) to manage the exchange of funds. Bitcoin transactions are stored in *blocks* which make up what is known as a *blockchain*, which is managed and updated by a collection of users known as *miners*. Note that technically, there is no single blockchain to speak of: instead, each miner keeps track of its own version of the blockchain, and the miners communicate with each other in order to come to an overall consensus, based on the Bitcoin protocol, on what blocks should be included in a blockchain.

Ideally, all miners will agree on the structure of the blockchain, but due to communication delays or possible deviations from the standard mining protocol, miners may have different versions of the blockchain for a period of time. Such discrepancies are not good if they exist for a relatively large period of time, as disagreements between blockchain versions could possibly lead to fraudulent behavior, such as double-spending attacks. In this paper, we will study what happens to the Bitcoin network when there are communication delays when all miners are mining according to the Bitcoin protocol and what happens to the Bitcoin network when a portion of miners use a strategy referred to in Eyal and Sirer [3] as Selfish Mining. Under Selfish Mining, a smaller pool of miners working together to mine blocks may choose to withhold information about recently discovered blocks in an attempt to earn more revenue in various ways. Suppose all miners have the same information and the selfish-mining pool discovers a block. They will inform all others in the pool, but they will not inform others outside of the pool. Once they have established a lead of 2 or more, the pool can

publish a block every time the honest community mines a block and the pool publishes two blocks if their lead has been reduced to one. In this way, the pool allows the honest community to waste their time mining blocks that never had a chance to be included in the blockchains of all miners, as miners will always seek to add blocks to the largest chain within the blockchain: such blocks that are not accepted by other miners are referred to as *orphan blocks*. Readers interested in an introduction on how Bitcoin works are referred to the survey paper of Tschorsch and Scheuermann [20].

Our objective is to present a detailed study of two CTMC models introduced in Göbel et al [7], which were introduced in order to better understand how Bitcoin is affected when a smaller pool of miners implement Selfish Mining, in order to gain an advantage over the larger group of miners in the system. In each model we consider, it is assumed that all miners in the smaller pool can communicate instantaneously with one another, all miners in the larger group can communicate instantaneously with one another, but there are communication delays between the smaller pool and the larger group. Section 2 considers first the case where all participants mine in an honest manner: for this model, we present a new derivation of the stationary distribution, and we also present a closed-form expression for $p_{(0,0)}$, which represents the long-run fraction of time both groups completely agree on the structure of the blockchain. Next, we also show how to derive similar expressions for the Laplace transforms of the transition functions of this model, under the assumption that both groups agree on the structure of the blockchain at time zero.

In Section 3, we derive the stationary distribution of the CTMC introduced in [7] which attempts to model the case where the smaller pool of miners implement Selfish Mining. We also show that similar expressions can be derived for the Laplace transforms of the transition functions as well, if we again assume that both the pool and the group agree on the structure of the blockchain at time zero. The analysis technique used in both Sections 2 and 3 involves usage of the recently-discovered random product representation introduced in [2]. Interestingly, some of the ideas used in Section 3 are very similar to ideas often used in the matrix-analytic community: one key step in the derivation of the stationary distribution of the Selfish Mining CTMC involves usage of an idea that is very similar to the idea often used to show a quasi-birth-death process has a matrix-geometric stationary distribution, and parts of the algorithm we use for calculating certain elements of the stationary distribution of the Selfish Mining CTMC involve use of a recursion that is similar in structure to Ramaswami's formula. We refer readers interested in the basics of matrix-analytic methods to the textbooks of Latouche and Ramaswami [14] and He [9]; readers interested in seeing how the random-product representation of [2] can be used to rederive many classical matrix-analytic results are referred to [11]. We conclude the paper in Section 4, by briefly discussing other generalizations that can be analyzed with our approach.

We close this introduction by mentioning a few other studies of aspects of Bitcoin that involve the use of models and techniques from applied probability: mentioning all relevant studies of Bitcoin is impossible, considering that the paper of Nakamoto [18] has been cited close to 6000 times as of now. The papers of Kasahara and Kawahara [12] and Kawase and Kasahara [13] use two different variations of the M/G/1 queue with batch services to model the amount of time it takes a new Bitcoin transaction to be included within a mined block. The papers of Li et al [15, 16] each use a matrix-analytic approach towards modeling transaction-confirmation times, with the model found in [16] being a generalization of the model from [15]. The paper of Huberman et al [10] studies the behavior of the transaction fees associated with arriving transactions to the network, as well as the behavior of the waiting time of an arbitrary transaction until it is included in a block. In the work of Frolkova and Mandjes [6], a notion of one-sided communication between two miners in the network is modeled with a G/M/∞ queue with synchronized departures, which models instances where one particular miner (miner A) has more information about how many blocks have been mined than another (miner B), and there is a delay in the amount of time it takes miner A to inform miner B of the existence of a block. Expressions for various performance measures of this system are given in [6], and the authors of [6] also show that their system can be approximated with a growth-collapse model under a fluid-scaling. A follow-up study to [6] can be found in [5], which shows that many different generalizations of the G/M/∞ model introduced in [6] can be studied in multiple ways with techniques from the theory of point processes. Finally, in the work of Bowden et al [1], the authors present various point processes that seek to model the time instances when

mined blocks are accepted and added to a blockchain: there they argue that these time instances are not necessarily closely modeled by points from a homogeneous Poisson process.

2 When all miners are honest

We first consider the case where both the smaller pool and the larger pool behave honestly, and follow the Bitcoin protocol. In order to model honest-mining behavior among both pools, Göbel et al [7] introduced the CTMC $\{X(t); t \geq 0\}$ whose state space is given by $S := \{(i,j) : i \geq 0, j \geq 0\}$, and whose generator (transition rate matrix) is given by $\mathbf{Q} := [q(x,y)]_{x,y \in S}$. The elements of $\mathbf{Q}$ are defined as follows: given positive rates λ_1, λ_2, and μ, we have that for any two distinct states $(i,j),(k,\ell) \in S$,

$$q((i,j),(k,\ell)) := \begin{cases} \lambda_1, & k = i+1, \ell = j; \\ \lambda_2, & k = i, \ell = j+1; \\ \mu, & k = \ell = 0, i \neq j; \end{cases} \tag{1}$$

with all other off-diagonal entries of $\mathbf{Q}$ set equal to zero. The diagonal elements $\{q(x,x)\}_{x \in S}$ of $\mathbf{Q}$ satisfy

$$q(x,x) := -q(x) \tag{2}$$

where $q(x)$ is the sojourn rate associated with each exponential sojourn time spent in state x by $\{X(t); t \geq 0\}$. Later it will help to partition S into a collection of diagonal subsets $\{D_k\}_{k \in \mathbb{Z}}$ of S, where for each $k \in \mathbb{Z}$,

$$D_k := \{(i,j) : i \geq 0,\ j \geq 0,\ j - i = k\}. \tag{3}$$

This partitioning also makes it easier to describe the diagonal elements of $\mathbf{Q}$: indeed, $q(x) := \lambda_1 + \lambda_2$ for each state $x \in D_0$, while for each integer $k \neq 0$, and each state $x \in D_k$, $q(x) := \lambda_1 + \lambda_2 + \mu$.

2.1 Hitting Times

An important random variable associated with the CTMC $\{X(t); t \geq 0\}$ is the amount of time it takes this chain to reach state $(0,0)$, as this corresponds to the state where the blockchain versions of each of the two pools agree. For each state $x \in S$, define

$$\tau_x := \inf\{t \geq 0 : X(t-) \neq X(t) = x\} \tag{4}$$

where $X(t-) := \lim_{s \uparrow t} X(s)$ is the left-hand limit of X at time t. Observe that when $X(0) \neq x$, τ_x is simply the amount of time it takes $\{X(t); t \geq 0\}$ to reach state x: however, when $X(0) = x$, τ_x is the amount of time it takes $\{X(t); t \geq 0\}$ to *return* to state x. More generally, for each subset A of S, we define

$$\tau_A := \inf\{t \geq 0 : X(t-) \in A^c, X(t) \in A\}$$

which represents the first time $\{X(t); t \geq 0\}$ makes a transition into the set A.

The following proposition shows how to calculate both the first moment, as well as the Laplace-Stieltjes transform (LST) of $\tau_{(0,0)}$, when $X(0) = (i,j)$ for each state $(i,j) \in S$, but before stating this result we first need to define some additional quantities. For each $\alpha \in \mathbb{C}_+ := \{\alpha \in \mathbb{C} : Re(\alpha) > 0\}$, the open halfplane consisting of all complex numbers having a positive real part, let $\phi_1(\alpha)$ denote the Laplace-Stieltjes transform (evaluated at α) of the busy period of an M/M/1 queue whose arrival rate is λ_1, and whose service rate is λ_2. Similarly, let $\phi_2(\alpha)$ denote the Laplace-Stieltjes transform of the busy period of an M/M/1 queue whose arrival rate is λ_2, and whose service rate is λ_1. Recall that for $\alpha \in \mathbb{C}_+$,

$$\phi_1(\alpha) = \frac{\lambda_1 + \lambda_2 + \alpha - \sqrt{(\lambda_1 + \lambda_2 + \alpha)^2 - 4\lambda_1\lambda_2}}{2\lambda_1} \tag{5}$$

and furthermore $\phi_2(\alpha) = \lambda_1 \phi_1(\alpha)/\lambda_2$, so clearly $\lambda_2 \phi_2(\alpha) = \lambda_1 \phi_1(\alpha)$.

Proposition 2.1 *The law of $\tau_{(0,0)}$ under the probability measure $\mathbb{P}_{(i,j)}$ satisfies the following properties.*
(a) For each integer $i \geq 1$, we have

$$\mathbb{E}_{(i,i)}[e^{-\alpha\tau_{(0,0)}}] = \mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}]. \tag{6}$$

(b) For each integer $k \leq -1$, and each state $(i,j) \in D_k$,

$$\mathbb{E}_{(i,j)}[e^{-\alpha\tau_{(0,0)}}] = \phi_1(\alpha+\mu)^{i-j}\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}] + \frac{\mu}{\mu+\alpha}(1-\phi_1(\alpha+\mu)^{i-j}). \tag{7}$$

(c) For each integer $k \geq 1$, and each state $(i,j) \in D_k$,

$$\mathbb{E}_{(i,j)}[e^{-\alpha\tau_{(0,0)}}] = \phi_2(\alpha+\mu)^{j-i}\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}] + \frac{\mu}{\mu+\alpha}(1-\phi_2(\alpha+\mu)^{j-i}). \tag{8}$$

Finally,

$$\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}] = \frac{\mu}{\mu+\alpha}\left[\frac{\frac{\lambda_1}{\lambda_1+\lambda_2+\alpha}(1-\phi_1(\alpha+\mu)) + \frac{\lambda_2}{\lambda_1+\lambda_2+\alpha}(1-\phi_2(\alpha+\mu))}{1-\left(\frac{\lambda_1}{\lambda_1+\lambda_2+\alpha}\phi_1(\alpha+\mu) + \frac{\lambda_2}{\lambda_1+\lambda_2+\alpha}\phi_2(\alpha+\mu)\right)}\right] \tag{9}$$

and

$$\mathbb{E}_{(0,0)}[\tau_{(0,0)}] = \frac{1+\frac{1}{\mu}\left(\lambda_1(1-\phi_1(\mu)) + \lambda_2(1-\phi_2(\mu))\right)}{\lambda_1(1-\phi_1(\mu)) + \lambda_2(1-\phi_2(\mu))}. \tag{10}$$

Proof We first establish (6): for each state $(i,i) \in D_0$, $i \geq 1$, we can show through a 'sum-over-paths from (i,i) to $(0,0)$ approach' that for each $\alpha \in \mathbb{C}_+$,

$$\mathbb{E}_{(i,i)}[e^{-\alpha\tau_{(0,0)}}] = \mathbb{E}[e^{-\alpha\tau_{(0,0)}}]. \tag{11}$$

We omit the details of the proof, as the result can be well-understood on an intuitive level, given the structure of $\mathbf{Q}$.

We now establish (7): fix a state (i,j) satisfying $i > j$. Given the dynamics of $\{X(t); t \geq 0\}$, observe that under the measure $\mathbb{P}_{(i,j)}$, $\tau_{(0,0)}$ can be expressed as

$$\tau_{(0,0)} = \tau_{D_0} + (\tau_{(0,0)} - \tau_{D_0}) \tag{12}$$

where under $\mathbb{P}_{(i,j)}$,

$$\tau_{D_0} := \inf\{t \geq 0 : X(t) \in D_0\} \tag{13}$$

represents the amount of time it takes $\{X(t); t \geq 0\}$ to reach the diagonal D_0.

We can use the strong Markov property, applied at the stopping time τ_{D_0} to make the following claim about the joint distribution of τ_{D_0} and $\tau_{(0,0)} - \tau_{D_0}$. Let e_μ and γ_1 denote two independent random variables, where e_μ is exponentially distributed with rate μ, and γ_1 is equal in distribution to the amount of time it takes an M/M/1 queueing system, having arrival rate λ_1 and service rate λ_2, to move from state $i-j$ to state 0. From the transition structure of $\mathbf{Q}$, we can see that

$$\tau_{D_0} \stackrel{d}{=} \min(e_\mu, \gamma_1).$$

To see why, observe that while the chain is in the set $\cup_{k\leq -1} D_k$, each transition to the East corresponds to a movement from a diagonal D_j to a diagonal D_{j-1}, which corresponds to an arrival from an M/M/1 queueing system with arrival rate λ_1. Similarly, each transition to the North corresponds to a movement from a diagonal D_j to a diagonal D_{j+1}, which corresponds to a service completion from an M/M/1 queueing system with service rate λ_2; finally, a transition from a state in $\cup_{k\leq -1} D_k$ to state $(0,0)$ corresponds to an exponential clearing instant (which removes all work from the M/M/1 queue) with rate μ.

Using the strong Markov property, we can see that under the measure $\mathbb{P}_{(i,j)}$, if $\{X(t); t \geq 0\}$ reaches $D_0 \setminus \{(0,0)\}$ before it reaches state $(0,0)$, then $\tau_{(0,0)} - \tau_{D_0}$ is equal in distribution to a random variable Z, which, by (6), is equal in distribution to $\tau_{(0,0)}$ under the law $\mathbb{P}_{(0,0)}$, and independent of the process up to the stopping time τ_{D_0}. Otherwise, if $\{X(t); t \geq 0\}$ reaches $(0,0)$ before $D_0 \setminus \{(0,0)\}$, then we set $\tau_{(0,0)} - \tau_{D_0}$ to be zero. Thus,

$$\tau_{(0,0)} - \tau_{D_0} \stackrel{d}{=} \mathbf{1}(e_\mu > \gamma_1) Z$$

and moreover,

$$(\tau_{D_0}, \tau_{(0,0)} - \tau_{D_0}) \stackrel{d}{=} (\min(e_\mu, \gamma_1), \mathbf{1}(e_\mu > \gamma_1) Z) \tag{14}$$

where e_μ, γ_1, and Z are all independent of each other.

The next step is to express $\mathbb{E}_{(i,j)}\left[e^{-\alpha\tau_{(0,0)}}\right]$ in terms of $\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}]$. Using (12) and(14), we get

$$\mathbb{E}_{(i,j)}[e^{-\alpha\tau_{(0,0)}}] = \mathbb{E}\left[e^{-\alpha(\min(e_\mu,\gamma_1)+\mathbf{1}(\gamma_1<e_\mu)Z)}\right] \tag{15}$$

and this Laplace-Stieltjes transform has a closed-form representation: first, observe that conditioning on both e_μ and γ_1 gives

$$\begin{aligned}
\mathbb{E}\left[e^{-\alpha(\min(e_\mu,\gamma_1)+\mathbf{1}(\gamma_1<e_\mu)Z)}\right] &= \mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}e^{-\alpha\mathbf{1}(\gamma_1<e_\mu)Z}\right] \\
&= \mathbb{E}\left[\mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}e^{-\alpha\mathbf{1}(\gamma_1<e_\mu)Z} \mid e_\mu, \gamma_1\right]\right] \\
&= \mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}\mathbb{E}\left[e^{-\alpha\mathbf{1}(\gamma_1<e_\mu)Z} \mid e_\mu, \gamma_1\right]\right]. \qquad (16)
\end{aligned}$$

Second, we simplify the inner conditional expectation within (16) by summing over indicator functions in the following manner:

$$\begin{aligned}
\mathbb{E}\left[e^{-\alpha\mathbf{1}(\gamma_1<e_\mu)Z} \mid e_\mu, \gamma_1\right] &= \mathbb{E}\left[e^{-\alpha\mathbf{1}(\gamma_1<e_\mu)Z} \mid e_\mu, \gamma_1\right]\mathbf{1}(e_\mu < \gamma_1) \\
&+ \mathbb{E}\left[e^{-\alpha\mathbf{1}(\gamma_1<e_\mu)Z} \mid e_\mu, \gamma_1\right]\mathbf{1}(\gamma_1 < e_\mu) \\
&= \mathbf{1}(e_\mu < \gamma_1) + \mathbb{E}[e^{-\alpha Z} \mid \gamma_1, e_\mu]\mathbf{1}(\gamma_1 < e_\mu) \\
&= \mathbf{1}(e_\mu < \gamma_1) + \mathbb{E}_{(0,0)}\left[e^{-\alpha\tau_{(0,0)}}\right]\mathbf{1}(\gamma_1 < e_\mu). \qquad (17)
\end{aligned}$$

After plugging (17) into (16), we conclude that

$$\begin{aligned}
\mathbb{E}_{(i,j)}\left[e^{-\alpha\tau_{(0,0)}}\right] &= \mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}\mathbf{1}(e_\mu < \gamma_1)\right] \\
&+ \mathbb{E}_{(0,0)}\left[e^{-\alpha\tau_{(0,0)}}\right]\mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}\mathbf{1}(\gamma_1 < e_\mu)\right]. \qquad (18)
\end{aligned}$$

The next step is to simplify the two unknown expectations appearing in (18) that are expressed in terms of e_μ and γ_1. First,

$$\begin{aligned}
\mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}\mathbf{1}(\gamma_1 < e_\mu)\right] &= \mathbb{E}\left[e^{-\alpha\gamma_1}\mathbf{1}(\gamma_1 < e_\mu)\right] \\
&= \mathbb{E}\left[\mathbb{E}\left[e^{-\alpha\gamma_1}\mathbf{1}(\gamma_1 < e_\mu) \mid \gamma_1\right]\right] \\
&= \mathbb{E}\left[e^{-\alpha\gamma_1}e^{-\mu\gamma_1}\right] \\
&= \mathbb{E}\left[e^{-(\mu+\alpha)\gamma_1}\right] = \phi_1(\mu+\alpha)^{i-j}. \qquad (19)
\end{aligned}$$

The other unknown expectation satisfies

$$\begin{aligned}
\mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}\mathbf{1}(e_\mu < \gamma_1)\right] &= \mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}\right] - \mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}\mathbf{1}(\gamma_1 < e_\mu)\right] \\
&= \mathbb{E}\left[e^{-\alpha\min(e_\mu,\gamma_1)}\right] - \phi_1(\mu+\alpha)^{i-j} \qquad (20)
\end{aligned}$$

and by using Fubini's Theorem,

$$\begin{aligned}
\mathbb{E}\left[e^{-\alpha \min(e_\mu,\gamma_1)}\right] &= \mathbb{E}\left[1-\left(1-e^{-\alpha \min(e_\mu,\gamma_1)}\right)\right] \\
&= 1-\mathbb{E}\left[\int_0^{\min(e_\mu,\gamma_1)} \alpha e^{-\alpha y} dy\right] \\
&= 1-\alpha\int_0^{\infty} e^{-\alpha y}\mathbb{P}(e_\mu > y, \gamma_1 > y) dy \\
&= 1-\alpha\int_0^{\infty} e^{-(\alpha+\mu) y}\mathbb{P}(\gamma_1 > y) dy \\
&= 1-\frac{\alpha}{\mu+\alpha}(1-\phi_1(\mu+\alpha)^{i-j}) \qquad (21)
\end{aligned}$$

which means that

$$\begin{aligned}
\mathbb{E}\left[e^{-\alpha \min(e_\mu,\gamma_1)}\mathbf{1}(e_\mu < \gamma_1)\right] &= 1-\frac{\alpha}{\mu+\alpha}(1-\phi_1(\mu+\alpha)^{i-j})-\phi_1(\mu+\alpha)^{i-j} \\
&= \frac{\mu}{\mu+\alpha}(1-\phi_1(\mu+\alpha)^{i-j}). \qquad (22)
\end{aligned}$$

Plugging both (19) and (22) into (18) gives

$$\mathbb{E}_{(i,j)}[e^{-\alpha\tau_{(0,0)}}] = \frac{\mu}{\mu+\alpha}(1-\phi_1(\mu+\alpha)^{i-j})+\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}]\phi_1(\mu+\alpha)^{i-j} \qquad (23)$$

which establishes (7). Furthermore, due to the symmetry present in the transition structure of $\{X(t); t \geq 0\}$, we can clearly see that for each state (i,j) satisfying $i < j$,

$$\mathbb{E}_{(i,j)}[e^{-\alpha\tau_{(0,0)}}] = \frac{\mu}{\mu+\alpha}(1-\phi_2(\mu+\alpha)^{j-i})+\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}]\phi_2(\mu+\alpha)^{j-i}. \qquad (24)$$

thus proving (8).

It remains to show both (9) and (10). Conditioning on the first transition shows that

$$\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}] = \frac{\lambda_1}{\lambda_1+\lambda_2+\alpha}\mathbb{E}_{(1,0)}[e^{-\alpha\tau_{(0,0)}}]+\frac{\lambda_2}{\lambda_1+\lambda_2+\alpha}\mathbb{E}_{(0,1)}[e^{-\alpha\tau_{(0,0)}}]. \qquad (25)$$

Plugging both (7) and (8) into the right-hand-side of (25) and solving for the single unknown $\mathbb{E}[e^{-\alpha\tau_{(0,0)}}]$ yields (9), while (10) follows immediately from (9) by taking derivatives and setting $\alpha = 0$. $\diamondsuit$

2.2 Deriving the stationary distribution

Our first task is to present a new derivation of the stationary distribution $\mathbf{p} := [p_y]_{y\in S}$ of this CTMC, which exists when λ_1, λ_2, and μ are all positive. We derive $\mathbf{p}$ by making use of a lattice path counting technique from the recent paper [17], which itself involves usage of the random-product technique introduced in [2]. Given our CTMC $\{X(t); t \geq 0\}$ with state space S and generator $\mathbf{Q}$, we construct another CTMC $\{\tilde{X}(t); t \geq 0\}$ whose state space is also S, but whose generator $\tilde{\mathbf{Q}}$ satisfies the following two properties: (i) for each pair of distinct states $x, y \in S$,

$$\tilde{q}(x,y) > 0 \quad \text{if and only if} \quad q(y,x) > 0 \qquad (26)$$

and (ii) for each state $x \in S$,

$$\sum_{y\neq x}\tilde{q}(x,y) = \sum_{y\neq x} q(x,y). \qquad (27)$$

Observe that one possible choice for $\tilde{\mathbf{Q}}$ is the generator of the time-reversal of $\{X(t); t \geq 0\}$, but choosing this generator requires knowledge of the stationary distribution $\mathbf{p}$, which we do not know. Fortunately, our analysis will not require us to choose a specific $\tilde{\mathbf{Q}}$: what is important here is the structure of the transition diagram of $\tilde{\mathbf{Q}}$—which is completely determined by the structure of the transition diagram of $\mathbf{Q}$—not the actual values of the transition rates within $\tilde{\mathbf{Q}}$.

Further associated with $\{\tilde{X}(t); t \geq 0\}$ is its collection of transition times $\{\tilde{T}_n\}_{n\geq 0}$, where $\tilde{T}_0 := 0$ and for each integer $n \geq 1$, $\tilde{T}_n$ denotes the nth transition time of $\{\tilde{X}(t); t \geq 0\}$. From these transition times, we define the embedded discrete-time Markov chain (DTMC) $\{\tilde{X}_n\}_{n\geq 0}$, where $\tilde{X}_n := \tilde{X}(T_n)$ represents the state of the CTMC immediately after its nth transition. Finally, for each state $x \in S$ we define the hitting-time random variables

$$\tilde{\eta}_x := \inf\{n \geq 0 : \tilde{X}_n = x\}, \quad \tilde{\tau}_x := \inf\{t \geq 0 : \tilde{X}(t) = x\}. \tag{28}$$

The following result, Theorem 2.1, was established in [2].

Theorem 2.1 *Suppose $\{X(t); t \geq 0\}$ is an ergodic CTMC, and fix a state $x \in S$. Then its stationary distribution $\mathbf{p}$ satisfies, for each state $y \in S$,*

$$p_y = p_x w_y \tag{29}$$

where $w_x := 1$, and for each state $y \neq x$,

$$w_y := \mathbb{E}_y \left[\mathbf{1}(\tilde{\eta}_x < \infty) \prod_{\ell=1}^{\tilde{\eta}_x} \frac{q(\tilde{X}_\ell, \tilde{X}_{\ell-1})}{\tilde{q}(\tilde{X}_{\ell-1}, \tilde{X}_\ell)} \right]. \tag{30}$$

We will occasionally refer to the fixed state x within Theorem 2.1 as the reference point. In order to derive the stationary distribution $\mathbf{p}$ of $\{X(t); t \geq 0\}$, we will find it useful to set $x := (0, 0)$.

Theorem 2.1 can be used to establish the following result, which provides a closed-form expression for each element of $\mathbf{p}$.

Theorem 2.2 *The stationary distribution of the honest-mining CTMC is as follows: for $(i, j) \neq (0, 0)$,*

$$p_{(i,j)} = p_{(0,0)} \sum_{x=0}^{\min(i,j)} \left[\frac{2^x(x + |i - j|)}{i + j - x} \binom{i + j - x}{j} \right] \frac{\lambda_1^i \lambda_2^j}{(\lambda_1 + \lambda_2)^x (\lambda_1 + \lambda_2 + \mu)^{i+j-x}}. \tag{31}$$

Furthermore,

$$p_{(0,0)} = \frac{1 - \frac{2\lambda_1}{\lambda_1+\lambda_2}\phi_1(\mu)}{1 + \frac{\lambda_1+\lambda_2}{\mu} - \frac{2\lambda_1}{\mu}\phi_1(\mu)}. \tag{32}$$

Formula (31) was derived in the work of Göbel et al [7] by verifying that (31) satisfies the global balance equations of $\{X(t); t \geq 0\}$. Not only do we give a different approach for deriving this formula, we further build on the results found in [7] by establishing (32), which shows that the stationary probability $p_{(0,0)}$ can be expressed explicitly in terms of λ_1, λ_2, and μ.

Proof We begin our proof of Theorem 2.2 by proving (32), but this follows immediately from applying (10) to the well-known formula

$$p_{(0,0)} = \frac{1}{q((0,0))\mathbb{E}_{(0,0)}[\tau_{(0,0)}]} = \frac{1}{(\lambda_1 + \lambda_2)\mathbb{E}_{(0,0)}[\tau_{(0,0)}]}. \tag{33}$$

It remains to establish (31) for each state $(i, j) \neq (0, 0)$, but this can be done via Theorem 2.1 by simplifying $w_{(i,j)}$, where we choose state $(0, 0)$ to be the reference point. Readers should note that the steps we use to simplify $w_{(i,j)}$ are very similar to the lattice path counting technique introduced

in [17] to study both the M/E$_r$/1 and E$_r$/M/1 queueing systems, but since the lattice path counting technique we invoke here does not technically fall within the framework of [17], we present a detailed proof.

Given a fixed state $(i,j) \neq (0,0)$, define, for each integer $n \geq 1$, $\mathcal{C}_n$ as the set of all feasible paths $(x_0, x_1, \ldots, x_n)$ with respect to $\tilde{\mathbf{Q}}$ that satisfy (i) $x_0 = (i,j)$, (ii) $x_n = (0,0)$, and (iii) $x_1, x_2, \ldots, x_{n-1} \neq (0,0)$. Then

$$\begin{aligned} w_{(i,j)} &= \sum_{n=1}^{\infty} \sum_{x_0,x_1,\ldots,x_n \in \mathcal{C}_n} \left[\prod_{\ell=1}^{n} \frac{q(x_n, x_{n-1})}{\tilde{q}(x_{n-1}, x_n)} \right] \left[\prod_{\ell=1}^{n} \frac{\tilde{q}(x_{n-1}, x_n)}{\tilde{q}(x_{n-1})} \right] \\ &= \sum_{n=1}^{\infty} \sum_{x_0,x_1,\ldots,x_n \in \mathcal{C}_n} \left[\prod_{\ell=1}^{n} \frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1})} \right] \end{aligned} \tag{34}$$

where the second equality follows from the fact that the diagonal terms of $\tilde{\mathbf{Q}}$ and $\mathbf{Q}$ agree.

Next, note that every transition made by $\tilde{\mathbf{Q}}$ is always either (i) to the West, or (ii) to the South, until the process reaches state $(0,0)$. If a feasible step $(x_{\ell-1}, x_\ell)$ is a Western transition, then its corresponding term in the product is

$$\frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1})} = \frac{\lambda_1}{\lambda_1 + \lambda_2 + \mu} \tag{35}$$

if $x_{\ell-1}$ is not an element of D_0. If $x_{\ell-1} \in D_0$, then

$$\frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1})} = \frac{\lambda_1}{\lambda_1 + \lambda_2}. \tag{36}$$

A similar statement can be made when $(x_{\ell-1}, x_\ell)$ represents a transition to the South: when $x_{\ell-1}$ is not an element of D_0,

$$\frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1})} = \frac{\lambda_2}{\lambda_1 + \lambda_2 + \mu} \tag{37}$$

and when $x_{\ell-1} \in D_0$,

$$\frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1})} = \frac{\lambda_2}{\lambda_1 + \lambda_2}. \tag{38}$$

Observe also that every feasible path from state (i,j) to state $(0,0)$ must consist of exactly $i+j$ steps, which implies

$$w_{(i,j)} = \sum_{x_0,x_1,\ldots,x_{i+j} \in C_{i+j}} \prod_{\ell=1}^{i+j} \frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1})} \tag{39}$$

and in each feasible path found in C_{i+j}, exactly i transitions are to the West, and j are to the South. Each term within the product corresponding to each feasible path from state (i,j) to state $(0,0)$ has to take one of the four values found in (35), (36), (37), and (38), and from the structure of these products, we can see that in order to simplify $w_{(i,j)}$ completely, we only need to keep track of the number of times a transition is made from D_0. For instance, each Western transition made by $\tilde{X}$ yields a product term whose numerator is λ_1, but whose denominator is either $(\lambda_1 + \lambda_2)$ or $(\lambda_1 + \lambda_2 + \mu)$, depending on whether or not the transition was made from a state in D_0, and a similar statement may be made with regard to Southern transitions. Let $d_x(i,j)$ denote the number of feasible paths under $\tilde{\mathbf{Q}}$ that start at (i,j), end at $(0,0)$, and make a transition from a state in D_0 exactly x times: then

$$w_{(i,j)} = \sum_{x=0}^{\min(i,j)} d_x(i,j) \frac{\lambda_1^i \lambda_2^j}{(\lambda_1 + \lambda_2)^x (\lambda_1 + \lambda_2 + \mu)^{i+j-x}}. \tag{40}$$

It remains to compute $d_x(i,j)$ for each $x \geq 0$. These terms were stated correctly in [7], but here we choose to derive them explicitly, as this will help us later. Clearly $d_0(i,i) = 0$ whenever $i \geq 1$, because in order for $\tilde{X}$ to move from state (i,i) to state $(0,0)$, it must make a transition from diagonal D_0 at least once. For $i,j \geq 0$ satisfying $i \neq j$,

$$d_0(i,j) = \frac{|j-i|}{j+i}\binom{j+i}{i} \tag{41}$$

which follows from the classical Ballot Theorem: see e.g. Renault [19].

We are now ready to calculate $d_x(i,i)$, for each integer $x \geq 1$ and each integer $i \geq 1$. Using (41), notice that for $i \geq 1$,

$$\begin{aligned} d_1(i,i) &= d_0(i-1,i) + d_0(i,i-1) \\ &= \frac{1}{2i-1}\binom{2i-1}{i} + \frac{1}{2i-1}\binom{2i-1}{i} = \frac{2}{2i-1}\binom{2i-1}{i}. \end{aligned} \tag{42}$$

Next, note that by (42), for $i \geq 2$,

$$\begin{aligned} d_2(i,i) &= \sum_{\ell=1}^{i-1} d_1(\ell,\ell) d_1(i-\ell, i-\ell) \\ &= \sum_{\ell=1}^{i-1} \frac{2}{2\ell-1}\binom{2\ell-1}{\ell} \frac{2}{2(i-\ell)-1}\binom{2(i-\ell)-1}{i-\ell-1} \\ &= 4\sum_{\ell=0}^{i-2} \frac{1}{2\ell+1}\binom{2\ell+1}{\ell} \frac{1}{2(i-2-\ell)+1}\binom{2(i-2-\ell)+1}{i-2-\ell} \\ &= \frac{4(2)}{2(i-2)+2}\binom{2(i-2)+2}{i-2} \\ &= \frac{(2)2^2}{2i-2}\binom{2i-2}{i} \end{aligned} \tag{43}$$

where the fourth equality follows from an application of Identity (5.63) on page 202 of Graham et al [8]; this identity is sometimes known as the Rothe-Hagen identity. From here, one can use (43) combined with induction to verify that for $x \geq 1$, $i \geq x$,

$$d_x(i,i) = \frac{x2^x}{2i-x}\binom{2i-x}{i}. \tag{44}$$

A similar argument can be used to derive $d_x(i,j)$ for the case where $i \neq j$: it suffices to consider only the case where $j > i$. Observe that for $x \geq 1$, $i \geq x$,

$$\begin{aligned} d_x(i,j) &= \sum_{\ell=x}^{i} d_x(\ell,\ell) d_0(i-\ell, j-\ell) \\ &= \sum_{\ell=x}^{i} \frac{x2^x}{2\ell-x}\binom{2\ell-x}{\ell-x} \frac{j-i}{i+j-2\ell}\binom{i+j-2\ell}{i-\ell} \\ &= \sum_{\ell=0}^{i-x} \frac{x2^x}{2\ell+x}\binom{2\ell+x}{\ell} \frac{j-i}{i+j-2\ell-2x}\binom{i+j-2\ell-2x}{i-\ell-x} \\ &= 2^x\sum_{\ell=0}^{i-x} \frac{x}{2\ell+x}\binom{2\ell+x}{\ell} \frac{j-i}{2(i-x-\ell)+j-i}\binom{2(i-x-\ell)+j-i}{i-x-\ell} \\ &= \frac{2^x(x+j-i)}{i+j-x}\binom{i+j-x}{j} \end{aligned} \tag{45}$$

where again, the third equality follows from Identity (5.63) on page 202 of Graham et al [8]. A similar argument shows further that when $j < i$, we have for $j \geq x$,

$$d_x(i,j) = \frac{2^x(x+i-j)}{i+j-x}\binom{i+j-x}{j} \tag{46}$$

meaning we can conclude that for $x \geq 0$,

$$d_x(i,j) = \frac{2^x(x+|i-j|)}{i+j-x}\binom{i+j-x}{j}. \tag{47}$$

This establishes (31), as well as the proof of Theorem 2.2. $\diamondsuit$

2.3 Calculating the Laplace transforms of the transition functions

It is also possible to express the Laplace transforms of the transition functions of $\{X(t); t \geq 0\}$ in closed-form, if we further assume that $X(0) = (0,0)$ with probability one. Recall that for each state $(i,j) \in S$, the transition function $p_{(i,j)} : [0,\infty) \to [0,1]$ is defined as

$$p_{(i,j)}(t) := \mathbb{P}(X(t) = (i,j) \mid X(0) = (0,0)), \quad t \geq 0 \tag{48}$$

and associated with $p_{(i,j)}$ is its Laplace transform $\pi_{(i,j)}$, which is defined on $\mathbb{C}_+$ as

$$\pi_{(i,j)}(\alpha) := \int_0^\infty e^{-\alpha t} p_{(i,j)}(t)dt, \quad \alpha \in \mathbb{C}. \tag{49}$$

These transforms can be evaluated with the random-product technique as well, thanks to Theorem 2.3. This theorem was first given in [2] for the case where $\alpha > 0$, and later extended to $\mathbb{C}_+$ in [4].

Theorem 2.3 *Each Laplace transform $\pi_{(i,j)}$, for $(i,j) \in S$, satisfies*

$$\pi_{(i,j)}(\alpha) = \pi_{(0,0)}(\alpha) w_{(i,j)}(\alpha), \quad \alpha \in \mathbb{C}_+ \tag{50}$$

where $w_{(0,0)}(\alpha) = 1$ on $\mathbb{C}_+$, and for each state $(i,j) \neq (0,0)$,

$$w_{(i,j)}(\alpha) := \mathbb{E}_{(i,j)}\left[\mathbf{1}(\tilde{\eta}_{(0,0)} < \infty) e^{-\alpha \tilde{\tau}_{(0,0)}} \prod_{\ell=1}^{\tilde{\eta}_{(0,0)}} \frac{q(\tilde{X}_\ell, \tilde{X}_{\ell-1})}{\tilde{q}(\tilde{X}_{\ell-1}, \tilde{X}_\ell)}\right], \quad \alpha \in \mathbb{C}_+. \tag{51}$$

Using Theorem 2.3, we can make use of another lattice path counting procedure to establish the following result.

Theorem 2.4 *The Laplace-Stieltjes transforms of this CTMC is as follows: for $(i,j) \neq (0,0)$,*

$$\pi_{(i,j)}(\alpha) = \pi_{(0,0)}(\alpha) \sum_{x=0}^{\min(i,j)} d_x(i,j) \frac{\lambda_1^i \lambda_2^j}{(\lambda_1+\lambda_2+\alpha)^x (\lambda_1+\lambda_2+\mu+\alpha)^{i+j-x}}. \tag{52}$$

Furthermore,

$$\pi_{(0,0)}(\alpha) = \frac{(\mu+\alpha)\left[1 - \frac{2\lambda_1}{\lambda_1+\lambda_2+\alpha}\phi_1(\mu+\alpha)\right]}{\alpha\mu\left[1 + \frac{\lambda_1+\lambda_2+\alpha}{\mu} - \frac{2\lambda_1\phi_1(\mu+\alpha)}{\mu}\right]}. \tag{53}$$

Proof This argument is analogous to the argument we use to establish Theorem 2.2. First, we calculate the Laplace transform $\pi_{(0,0)}$, and once that has been found we then show how to express every other Laplace transform $\pi_{(i,j)}$, for $(i,j) \neq (0,0)$, in terms of $\pi_{(0,0)}$. Observe first that for each $\alpha \in \mathbb{C}_+$ (see e.g. Corollary 2.1 of [4])

$$\pi_{(0,0)}(\alpha) = \frac{1}{(\lambda_1 + \lambda_2 + \alpha)\left(1 - \mathbb{E}_{(0,0)}\left[e^{-\alpha \tau_{(0,0)}}\right]\right)}. \tag{54}$$

Plugging (9) into (54) and simplifying yields, after some algebra, (53).

It remains to establish (52), but to do so it suffices, given Theorem 2.3, to calculate $w_{(i,j)}(\alpha)$ for each state (i,j) satisfying $i \neq j$. Letting the set of paths $\mathcal{C}_n$ be defined as before, we observe that

$$w_{(i,j)}(\alpha) \quad = \quad \sum_{n=1}^{\infty} \sum_{(x_0, x_1, \ldots, x_n) \in \mathcal{C}_n} \prod_{\ell=1}^{n} \frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1}) + \alpha}. \tag{55}$$

Similar to what we saw in the proof of Theorem 2.2, if a feasible step $(x_{\ell-1}, x_\ell)$ is a western transition, then its corresponding term in the product is

$$\frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1}) + \alpha} = \frac{\lambda_1}{\lambda_1 + \lambda_2 + \mu + \alpha} \tag{56}$$

if $x_{\ell-1}$ is not in D_0: if $x_{\ell-1} \in D_0$, then

$$\frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1}) + \alpha} = \frac{\lambda_1}{\lambda_1 + \lambda_2 + \alpha}. \tag{57}$$

Similarly, for transitions to the South, when $x_{\ell-1}$ is not in D_0,

$$\frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1}) + \alpha} = \frac{\lambda_2}{\lambda_1 + \lambda_2 + \mu + \alpha} \tag{58}$$

and when $x_{\ell-1} \in D_0$,

$$\frac{q(x_\ell, x_{\ell-1})}{q(x_{\ell-1}) + \alpha} = \frac{\lambda_2}{\lambda_1 + \lambda_2 + \alpha}. \tag{59}$$

Applying observations (56), (57), (58) and (59) as necessary yields

$$w_{(i,j)}(\alpha) = \sum_{x=0}^{\min(i,j)} d_x(i,j) \frac{\lambda_1^i \lambda_2^j}{(\lambda_1 + \lambda_2 + \alpha)^x (\lambda_1 + \lambda_2 + \mu + \alpha)^{i+j-x}} \tag{60}$$

which implies, due to (47),

$$\pi_{(i,j)}(\alpha) = \pi_{(0,0)}(\alpha) \sum_{x=0}^{\min(i,j)} d_x(i,j) \frac{\lambda_1^i \lambda_2^j}{(\lambda_1 + \lambda_2 + \alpha)^x (\lambda_1 + \lambda_2 + \mu + \alpha)^{i+j-x}} \tag{61}$$

thus proving (52). This completes the proof of Theorem 2.4. $\diamondsuit$

3 When a pool of miners implement a 'selfish-mining' strategy

We now observe what happens when a portion of the pool implements a selfish-mining strategy. In order to model selfish-mining behavior, Göbel et al [7] introduced the CTMC $\{X(t); t \geq 0\}$ whose

state space is given by $S := \{(i,j) : i \geq 0, j \geq 0\}$ and whose generator is given by $\mathbf{Q} := [q(x,y)]_{x,y \in S}$, where the elements of $\mathbf{Q}$ are defined as follows: given possible rates λ_1, λ_2, and μ we define

$$q((i,j),(k,\ell)) = \begin{cases} \lambda_1 & k = i+1, \ell = j; \\ \lambda_2 & k = i, \ell = j+1; \\ \mu & k = \ell = 0 \text{ with } i < j \text{ or } j = i-1, i \geq 2; \end{cases}$$

with all other off-diagonal rates set equal to zero. Just as before, each diagonal element $q(x,x)$, $x \in S$, satisfies $q(x,x) = -q(x)$, where $q(x)$ is the rate corresponding to each exponential sojourn time spent by the CTMC in state x.

3.1 Hitting Times

We can study the behavior of $\{X(t); t \geq 0\}$ by using an approach analogous to the one used in the previous section to study the behavior of the honest-mining CTMC. Just as in Section 2, our first step consists of showing that the Laplace-Stieltjes transforms of $\tau_{(0,0)}$, under each probability measure $\mathbb{P}_{(i,j)}$, can be calculated numerically.

Proposition 3.1 *The law of the hitting time $\tau_{(0,0)}$ under the probability measure $\mathbb{P}_{(i,j)}$ satisfies the following properties.*
(a) For each integer $i \geq 1$, we have

$$\mathbb{E}_{(i,i)}[e^{-\alpha \tau_{(0,0)}}] = \mathbb{E}_{(1,1)}[e^{-\alpha \tau_{(0,0)}}] \tag{62}$$

and

$$\mathbb{E}_{(i+1,i)}[e^{-\alpha \tau_{(0,0)}}] = \mathbb{E}_{(2,1)}[e^{-\alpha \tau_{(0,0)}}]. \tag{63}$$

(b) For each integer $k \geq 1$, and each $(i,j) \in D_k$,

$$\mathbb{E}_{(i,j)}[e^{-\alpha \tau_{(0,0)}}] = \phi_2(\alpha+\mu)^{j-i}\mathbb{E}_{(1,1)}[e^{-\alpha \tau_{(0,0)}}] + \frac{\mu}{\mu+\alpha}(1 - \phi_2(\alpha+\mu)^{j-i}) \tag{64}$$

and moreover,

$$\mathbb{E}_{(i,j)}[\tau_{(0,0)}] = \frac{1-\phi_2(\mu)^{j-i}}{\mu} + \phi_2(\mu)^{j-i}\mathbb{E}_{(1,1)}[\tau_{(0,0)}]. \tag{65}$$

(c) For each integer $k \leq -2$, and each $(i,j) \in D_k$,

$$\mathbb{E}_{(i,j)}[e^{-\alpha \tau_{(0,0)}}] = \phi_1(\alpha)^{i-j-1}\mathbb{E}_{(2,1)}[e^{-\alpha \tau_{(0,0)}}] \tag{66}$$

and moreover,

$$\mathbb{E}_{(i,j)}[\tau_{(0,0)}] = \frac{i-j-1}{\lambda_2 - \lambda_1} + \mathbb{E}_{(2,1)}[\tau_{(0,0)}]. \tag{67}$$

(d) The Laplace-Stieltjes transforms $\mathbb{E}_{(1,1)}[e^{-\alpha \tau_{(0,0)}}]$ and $\mathbb{E}_{(2,1)}[e^{-\alpha \tau_{(0,0)}}]$ satisfy the linear system

$$\left[1 - \frac{\lambda_1 \phi_1(\alpha)}{\lambda_1+\lambda_2+\mu+\alpha}\right]\mathbb{E}_{(2,1)}[e^{-\alpha \tau_{(0,0)}}] = \frac{\lambda_2}{\lambda_1+\lambda_2+\mu+\alpha}\mathbb{E}_{(1,1)}[e^{-\alpha \tau_{(0,0)}}] + \frac{\mu}{\lambda_1+\lambda_2+\mu+\alpha} \tag{68}$$

$$\left[1 - \frac{\lambda_2 \phi_2(\alpha+\mu)}{\lambda_1+\lambda_2+\alpha}\right]\mathbb{E}_{(1,1)}[e^{-\alpha \tau_{(0,0)}}] = \frac{\lambda_1}{\lambda_1+\lambda_2+\alpha}\mathbb{E}_{(2,1)}[e^{-\alpha \tau_{(0,0)}}] + \frac{\mu}{\mu+\alpha}\frac{\lambda_2(1-\phi_2(\alpha+\mu))}{\lambda_1+\lambda_2+\alpha}. \tag{69}$$

Moreover, the expected values $\mathbb{E}_{(2,1)}[\tau_{(0,0)}]$ and $\mathbb{E}_{(1,1)}[e^{-\alpha \tau_{(0,0)}}]$ satisfy the linear system

$$(\lambda_2+\mu)\mathbb{E}_{(2,1)}[\tau_{(0,0)}] = \lambda_2 \mathbb{E}_{(1,1)}[\tau_{(0,0)}] + \frac{\lambda_2}{\lambda_2 - \lambda_1} \tag{70}$$

$$\left[1-\frac{\lambda_2\phi_2(\mu)}{\lambda_1+\lambda_2}\right]\mathbb{E}_{(1,1)}[\tau_{(0,0)}]=\frac{\lambda_1}{\lambda_1+\lambda_2}\mathbb{E}_{(2,1)}[\tau_{(0,0)}]+\frac{1}{\lambda_1+\lambda_2}\left[1+\frac{\lambda_2(1-\phi_2(\mu))}{\mu}\right]. \tag{71}$$

(e) The Laplace-Stieltjes transform $\mathbb{E}_{(1,0)}[e^{-\alpha\tau_{(0,0)}}]$ *satisfies*

$$\mathbb{E}_{(1,0)}[e^{-\alpha\tau_{(0,0)}}]=\frac{\lambda_1}{\lambda_1+\lambda_2+\alpha}\phi_1(\alpha)\mathbb{E}_{(2,1)}[e^{-\alpha\tau_{(0,0)}}]+\frac{\lambda_2}{\lambda_1+\lambda_2+\alpha}\mathbb{E}_{(1,1)}[e^{-\alpha\tau_{(0,0)}}] \tag{72}$$

and furthermore,

$$\mathbb{E}_{(1,0)}[\tau_{(0,0)}]=\frac{\lambda_2}{\lambda_2^2-\lambda_1^2}+\frac{\lambda_2}{\lambda_1+\lambda_2}\mathbb{E}_{(1,1)}[\tau_{(0,0)}]+\frac{\lambda_1}{\lambda_1+\lambda_2}\mathbb{E}_{(2,1)}[\tau_{(0,0)}] \tag{73}$$

(f) Finally, the Laplace-Stieltjes transform $\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}]$ *satisfies*

$$\begin{aligned}\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}] &= \frac{\lambda_2}{\lambda_1+\lambda_2+\alpha}\left[\frac{1-\phi_2(\alpha+\mu)}{\mu+\alpha}\right] \\ &+ \frac{\lambda_1^2}{(\lambda_1+\lambda_2+\alpha)^2}\phi_1(\alpha)\mathbb{E}_{(2,1)}[e^{-\alpha\tau_{(0,0)}}] \\ &+ \frac{\lambda_2}{(\lambda_1+\lambda_2+\alpha)}\left[\frac{\lambda_1}{(\lambda_1+\lambda_2+\alpha)}+\phi_2(\alpha+\mu)\right]\mathbb{E}_{(1,1)}[e^{-\alpha\tau_{(0,0)}}]\end{aligned} \tag{74}$$

and similarly,

$$\begin{aligned}\mathbb{E}_{(0,0)}[\tau_{(0,0)}] &= \frac{1}{\lambda_1+\lambda_2}\left[1+\frac{\lambda_1\lambda_2}{\lambda_2^2-\lambda_1^2}+\frac{\lambda_2(1-\phi_2(\mu))}{\mu}\right] \\ &+ \frac{\lambda_2}{\lambda_1+\lambda_2}\left[\frac{\lambda_1}{\lambda_1+\lambda_2}+\phi_2(\mu)\right]\mathbb{E}_{(1,1)}[\tau_{(0,0)}]+\left(\frac{\lambda_1}{\lambda_1+\lambda_2}\right)^2\mathbb{E}_{(2,1)}[\tau_{(0,0)}].\end{aligned} \tag{75}$$

Proof Statements (62) and (63) of Proposition 3.1 can be established using a 'sum-over-paths' approach: again, we omit the details since the result is intuitively obvious, given the structure of the transition diagram. Next, (65) follows from taking derivatives of both sides of (64) and setting $\alpha=0$, and observe from the form of the transition diagram that (64) follows from the argument used to establish (7) of Proposition 2.1.

The next step is to prove (66). Assuming $X(0)=(i,j)\in D_k$ for some $k\geq 2$, we can see from (63) that, under the probability measure $\mathbb{P}_{(i,j)}$, $\tau_{(0,0)}$ is equal in distribution to the convolution of the amount of time it takes an M/M/1 queue with arrival rate λ_1, service rate λ_2 to move from state $i-j-1$ to state 0, and the law of $\tau_{(0,0)}$ under the probability measure $\mathbb{P}_{(2,1)}$. Once this has been observed, (67) quickly follows from (66) by taking derivatives of both sides, and setting $\alpha=0$.

Next, note that (68) and (69) follow from applying a first-step analysis argument, then applying (64) and (66), and an analogous argument can be used to establish (70) and (71). The rest of the statements contained in Proposition 3.1 follow from first-step analysis and substitution in an analogous manner: we omit the details. $\diamondsuit$

3.2 Calculating the stationary distribution

Our next task is to find the stationary distribution $\mathbf{p}$ of this model, which exists when $0<\lambda_1<\lambda_2$ and $\mu>0$. This is done in Theorem 3.1.

Theorem 3.1 *The stationary distribution* $\mathbf{p}$ *of* $\{X(t);t\geq 0\}$ *satisfies the following properties:*
(a) the long-run fraction of time $p_{(0,0)}$ *satisfies*

$$p_{(0,0)} = \frac{1}{(\lambda_1+\lambda_2)\mathbb{E}_{(0,0)}[\tau_{(0,0)}]} \tag{76}$$

where $\mathbb{E}_{(0,0)}[\tau_{(0,0)}]$ can be calculated using Proposition 3.1.
(b) For each integer $k \geq 1$, and each state $(i,j) \in D_k$, we have

$$p_{(i,j)} = \sum_{\ell=0}^{i} \frac{j-i}{i+j-2\ell} \binom{i+j-2\ell}{j-\ell} \frac{\lambda_1^{i-\ell}\lambda_2^{j-\ell}}{(\lambda_1+\lambda_2+\mu)^{i+j-2\ell}} p_{(\ell,\ell)}. \tag{77}$$

(c) For each integer $k \leq -2$, and each state $(i,j) \in D_k$, we have

$$p_{(i,j)} = \sum_{\ell=0}^{j} \frac{i-j-1}{i+j-2\ell-1} \binom{i+j-2\ell-1}{j-\ell} \frac{\lambda_1^{i-1-\ell}\lambda_2^{j-\ell}}{(\lambda_1+\lambda_2)^{i+j-2\ell-1}} p_{(\ell+1,\ell)}. \tag{78}$$

(d) Next,

$$p_{(1,0)} = \frac{\lambda_1}{\lambda_1+\lambda_2} p_{(0,0)} \tag{79}$$

and for each integer $\ell \geq 1$,

$$\begin{aligned} p_{(\ell+1,\ell)} &= \frac{\lambda_2}{\lambda_1+\lambda_2+\mu} \sum_{k=0}^{\ell-1} \frac{1}{2\ell-2k-l} \binom{2\ell-2k-1}{\ell-1-k} \frac{\lambda_1^{\ell-k}\lambda_2^{\ell-1-k}}{(\lambda_1+\lambda_2)^{2\ell-2k-1}} p_{(k+1,k)} \\ &+ \frac{\lambda_1}{\lambda_1+\lambda_2+\mu} p_{(\ell,\ell)}. \end{aligned} \tag{80}$$

(e) Finally, for each integer $\ell \geq 1$,

$$\begin{aligned} p_{(\ell,\ell)} &= \frac{\lambda_1}{\lambda_1+\lambda_2} \sum_{k=0}^{\ell-1} \frac{1}{2\ell-1-2k} \binom{2\ell-1-2k}{\ell-k} \frac{\lambda_1^{\ell-1-k}\lambda_2^{\ell-k}}{(\lambda_1+\lambda_2+\mu)^{2\ell-1-2k}} p_{(k,k)} \\ &+ \frac{\lambda_2}{\lambda_1+\lambda_2} p_{(\ell,\ell-1)}. \end{aligned} \tag{81}$$

From Theorem 3.1, we can see that in order to calculate, for example, $p_{(i,j)}$ for $i < j$, we first need to find $p_{(0,0)}$, then use the recursions given in Theorem 3.1 to find $p_{(1,0)}$, $p_{(1,1)}$, $p_{(2,1)}$, $p_{(2,2)}$, etc., up to $p_{(i,i)}$.

Proof Statement (76) is obvious, but we state it formally within Theorem 3.1 to remind readers that Proposition 3.1 can be used to compute $p_{(0,0)}$.

Our next task is to use Theorem 2.1, where state $(0,0)$ is used as the reference point, to establish both (77) and (78). Consider first the case where $(i,j) \in D_k$ for some integer $k \geq 1$, meaning $i < j$. Setting

$$\tilde{\eta}_{D_0} := \inf\{n \geq 1 : \tilde{X}_n \in D_i\}$$

we can apply the strong Markov property at the stopping time $\tilde{\eta}_{D_0}$ to express $w_{(i,j)}$ as follows:

$$\begin{aligned} w_{(i,j)} &= \sum_{\ell=0}^{i} \mathbb{E}_{(i,j)} \left[\mathbf{1}(\tilde{\eta}_{D_0} < \infty, \tilde{X}_{\tilde{\eta}_{D_{0,i}}} = (\ell,\ell)) \prod_{k=1}^{\tilde{\eta}_{D_0}} \frac{q(\tilde{X}_k, \tilde{X}_{k-1})}{\tilde{q}(\tilde{X}_{k-1}, \tilde{X}_k)} \mathbf{1}(\tilde{\eta}_{(0,0)} < \infty) \prod_{k=\tilde{\eta}_{D_0}+1}^{\tilde{\eta}_{(0,0)}} \frac{q(\tilde{X}_k, \tilde{X}_{k-1})}{\tilde{q}(\tilde{X}_{k-1}, \tilde{X}_k)} \right] \\ &= \sum_{\ell=0}^{i} w_{(\ell,\ell)} \mathbb{E}_{(i,j)} \left[\mathbf{1}(\tilde{\eta}_{D_0} < \infty, \tilde{X}_{\tilde{\eta}_{D_0}} = (\ell,\ell)) \prod_{k=1}^{\tilde{\eta}_{D_0}} \frac{q(\tilde{X}_k, \tilde{X}_{k-1})}{\tilde{q}(\tilde{X}_{k-1}, \tilde{X}_k)} \right]. \end{aligned} \tag{82}$$

The next step is to simplify, for each integer $\ell \in \{0, 1, \ldots, i\}$, the expected value

$$\mathbb{E}_{(i,j)} \left[\mathbf{1}(\tilde{\eta}_{D_0} < \infty, \tilde{X}_{\tilde{\eta}_{D_0}} = (\ell,\ell)) \prod_{k=1}^{\tilde{\eta}_{D_0}} \frac{q(\tilde{X}_k, \tilde{X}_{k-1})}{\tilde{q}(\tilde{X}_{k-1}, \tilde{X}_k)} \right]. \tag{83}$$

Recall that starting in state (i,j), the tilde process can only make transitions to the West or to the South until it reaches state (ℓ,ℓ). While the process is above D_0, transitions to the West have corresponding product term

$$\frac{q(x_k,x_{k-1})}{q(x_{k-1})} = \frac{\lambda_1}{\lambda_1+\lambda_2+\mu}, \tag{84}$$

while transitions to the South have corresponding product term

$$\frac{q(x_k,x_{k-1})}{q(x_{k-1})} = \frac{\lambda_2}{\lambda_1+\lambda_2+\mu}. \tag{85}$$

Moreover, in order for $\{\tilde{X}_n\}_{n\geq 0}$ to move from state (i,j) to state (ℓ,ℓ), it must make exactly $i-\ell$ Western transitions, and exactly $j-\ell$ Southern transitions. Define $\mathcal{C}_{i+j-2\ell}$ to be the set of all paths of the form $(x_0,x_1,\ldots,x_{i+j-2\ell})$, where $x_0=(i,j), x_{i+j-2\ell}=(\ell,\ell)$, and for each $k=1,\ldots,i+j-2\ell-1, x_k\notin D_{0,i}$. Then,

$$\begin{aligned}
&\mathbb{E}_{(i,j)}\left[\mathbf{1}(\tilde{\eta}_{D_0}<\infty,\tilde{X}_{\tilde{\eta}_{D_0}}=(\ell,\ell))\prod_{k=1}^{\tilde{\eta}_{D_0}}\frac{q(\tilde{X}_k,\tilde{X}_{k-1})}{\tilde{q}(\tilde{X}_{k-1},\tilde{X}_k)}\right]\\
&= \sum_{x_0,\ldots,x_{i+j-2\ell}\in C_{i+j-2\ell}}\prod_{k=1}^{i+j-2\ell}\frac{q(\tilde{x}_k,\tilde{x}_{k-1})}{q(x_{k-1})}
\end{aligned} \tag{86}$$

and for each path $(x_0,x_1,\ldots,x_{i+j-2\ell})\in C_{i+j-2\ell}$, each term in its corresponding product has to take one of two values found in (84) and (85). Note too that the number of paths in $\mathcal{C}_{i+j-2\ell}$ is simply $d_0(i-\ell,j-\ell)$, which has been derived previously. Thus,

$$\begin{aligned}
w_{(i,j)} &= \sum_{\ell=0}^{i} w_{(\ell,\ell)}\mathbb{E}_{(i,j)}\left[\mathbf{1}(\tilde{\eta}_{D_0}<\infty,\tilde{X}_{\tilde{\eta}_{D_0}}=(\ell,\ell))\prod_{k=1}^{\tilde{\eta}_{D_0}}\frac{q(\tilde{X}_k,\tilde{X}_{k-1})}{\tilde{q}(\tilde{X}_{k-1},\tilde{X}_k)}\right]\\
&= \sum_{\ell=0}^{i}\frac{j-i}{i+j-2\ell}\binom{i+j-2\ell}{j-\ell}\frac{\lambda_1^{i-\ell}\lambda_2^{j-\ell}}{(\lambda_1+\lambda_2+\mu)^{i+j-2\ell}}w_{(\ell,\ell)}
\end{aligned} \tag{87}$$

and after multiplying both sides by $p_{(0,0)}$, we have

$$p_{(i,j)} = \sum_{\ell=0}^{i}\frac{j-i}{i+j-2\ell}\binom{i+j-2\ell}{j-\ell}\frac{\lambda_1^{i-\ell}\lambda_2^{j-\ell}}{(\lambda_1+\lambda_2+\mu)^{i+j-2\ell}}p_{(\ell,\ell)} \tag{88}$$

which establishes (77). A similar argument can be used to establish (78) for the case where state $(i,j)\in D_k$ for some integer $k\leq -2$: in that case, we need to keep track of how $\{\tilde{X}_n\}_{n\geq 0}$ first reaches the set D_{-1} when it starts in state (i,j).

It remains to establish (79), (80), and (81). Recall that since $(0,0)$ is the reference node, $w_{(0,0)}=1$. Next, a simple first-step analysis argument shows that

$$w_{(1,0)} = \frac{\lambda_1}{\lambda_1+\lambda_2}w_{(0,0)} = \frac{\lambda_1}{\lambda_1+\lambda_2} \tag{89}$$

and multiplying both sides of (89) by $p_{(0,0)}$ yields (79).

We can show that the remaining $w_{(\ell,\ell)}$ and $w_{(\ell,\ell+1)}$ terms, for $\ell\geq 1$, satisfy a simple recursion. Using first-step analysis, combined with (77) gives

$$\begin{aligned}
w_{(\ell,\ell)} &= \frac{\lambda_1}{\lambda_1+\lambda_2}w_{(\ell-1,\ell)} + \frac{\lambda_2}{\lambda_1+\lambda_2}w_{(\ell,\ell-1)}\\
&= \frac{\lambda_1}{\lambda_1+\lambda_2}\sum_{k=0}^{\ell-1}\frac{1}{2\ell-1-2k}\binom{2\ell-1-2k}{\ell-k}\frac{\lambda_1^{\ell-1-k}\lambda_2^{\ell-k}}{(\lambda_1+\lambda_2+\mu)^{2\ell-1-2k}}w_{(k,k)}\\
&+ \frac{\lambda_2}{\lambda_1+\lambda_2}w_{(\ell,\ell-1)}
\end{aligned} \tag{90}$$

and similarly, using first-step analysis combined with (78) gives

$$\begin{aligned} w_{(\ell+1,\ell)} &= \frac{\lambda_1}{\lambda_1+\lambda_2+\mu} w_{(\ell,\ell)} + \frac{\lambda_2}{\lambda_1+\lambda_2+\mu} w_{(\ell+1,\ell-1)} \\ &= \frac{\lambda_2}{\lambda_1+\lambda_2+\mu} \sum_{k=0}^{\ell-1} \frac{1}{2\ell-2k-l} \binom{2\ell-2k-1}{\ell-1-k} \frac{\lambda_1^{\ell-k}\lambda_2^{\ell-1-k}}{(\lambda_1+\lambda_2)^{2\ell-2k-1}} w_{(k+1,k)} \\ &+ \frac{\lambda_1}{\lambda_1+\lambda_2+\mu} w_{(\ell,\ell)} \end{aligned} \tag{91}$$

Multiplying both sides of (90) and (91) by $p_{(0,0)}$ yields (81) and (80), respectively, which proves Theorem 3.1. $\diamondsuit$

3.3 Calculating the Laplace transforms of the transition functions

Not surprisingly, we can also calculate the Laplace transform $\pi_{(i,j)}$ associated with each transition function $p_{(i,j)}(t)$, if we further assume that $X(0) = (0,0)$. Theorem 3.2 shows how to calculate these transforms: since the proof of Theorem 3.2 is similar to the proof of Theorem 3.1 in a way analogous to how the proof of Theorem 2.4 is similar to the proof of Theorem 2.2, in the interest of saving space we omit the details of the proof.

Theorem 3.2 *Suppose $X(0) = (0,0)$ with probability one. Then the Laplace transforms $\pi_{(i,j)}$ of the transition functions satisfy the following properties.*
(a) First,

$$\pi_{(0,0)}(\alpha) = \frac{1}{(\lambda_1+\lambda_2+\alpha)\left(1-\mathbb{E}_{(0,0)}\left[e^{-\alpha\tau_{(0,0)}}\right]\right)} \tag{92}$$

where $\mathbb{E}_{(0,0)}[e^{-\alpha\tau_{(0,0)}}]$ can be calculated using Proposition 3.1.
(b) For each integer $k \geq 1$, and each $(i,j) \in D_k$,

$$\pi_{(i,j)}(\alpha) = \sum_{\ell=0}^{i} \frac{j-i}{i+j-2\ell} \binom{i+j-2\ell}{j-\ell} \frac{\lambda_1^{i-\ell}\lambda_2^{j-\ell}}{(\lambda_1+\lambda_2+\mu+\alpha)^{i+j-2\ell}} \pi_{(\ell,\ell)}(\alpha). \tag{93}$$

(c) For each integer $k \leq -2$, and each $(i,j) \in D_k$,

$$\pi_{(i,j)}(\alpha) = \sum_{\ell=0}^{j} \frac{i-j-1}{i+j-2\ell-1} \binom{i+j-2\ell-1}{j-\ell} \frac{\lambda_1^{i-1-\ell}\lambda_2^{j-\ell}}{(\lambda_1+\lambda_2+\alpha)^{i+j-2\ell-1}} \pi_{(\ell+1,\ell)}(\alpha). \tag{94}$$

(d) Next,

$$\pi_{(1,0)}(\alpha) = \frac{\lambda_1}{\lambda_1+\lambda_2+\alpha} \pi_{(0,0)}(\alpha) \tag{95}$$

and for each $\ell \geq 1$,

$$\begin{aligned} \pi_{(\ell+1,\ell)}(\alpha) &= \frac{\lambda_2}{\lambda_1+\lambda_2+\mu+\alpha} \sum_{k=0}^{\ell-1} \frac{1}{2\ell-2k-1} \binom{2\ell-2k-1}{\ell-1-k} \frac{\lambda_1^{\ell-k}\lambda_2^{\ell-1-k}}{(\lambda_1+\lambda_2+\alpha)^{2\ell-2k-1}} \pi_{(k+1,k)}(\alpha) \\ &+ \frac{\lambda_1}{\lambda_1+\lambda_2+\mu+\alpha} \pi_{(\ell,\ell)}(\alpha). \end{aligned} \tag{96}$$

(e) Finally, for each integer $\ell \geq 1$,

$$\begin{aligned} \pi_{(\ell,\ell)}(\alpha) &= \frac{\lambda_1}{\lambda_1+\lambda_2+\alpha} \sum_{k=0}^{\ell-1} \frac{1}{2\ell-1-2k} \binom{2\ell-1-2k}{\ell-k} \frac{\lambda_1^{\ell-1-k}\lambda_2^{\ell-k}}{(\lambda_1+\lambda_2+\mu+\alpha)^{2\ell-1-2\ell}} \pi_{(k,k)}(\alpha) \\ &+ \frac{\lambda_2}{\lambda_1+\lambda_2+\alpha} \pi_{(\ell,\ell-1)}(\alpha). \end{aligned} \tag{97}$$

4 Extensions and Future Work

The methods we used in this paper can also be used to analyze other similar models. For instance, suppose that the greedy miners would like to use a different strategy that is similar to Selfish Mining, except that once their lead is reduced to m, $m > 1$ they will publish all their blocks. The generator of this new CTMC is given by $\mathbf{Q}$ where the elements of $\mathbf{Q}$ are

$$q((i,j),(k,\ell)) = \begin{cases} \lambda_1 & k = i+1, \ell = j; \\ \lambda_2 & k = i, \ell = j+1; \\ \mu & k = \ell = 0 \text{ with } i < j \text{ or } j = i - m, i \geq m+1 \end{cases}$$

and all other rates are equal to zero. Using this CTMC we have the following theorem which can be proved using similar techniques as those in Section 3 so we omit the proof.

Theorem 4.1 *The stationary distribution* $\mathbf{p}$ *of* $\{X(t) : t \geq 0\}$ *satisfies the following properties: (a) the long-run fraction of time satisfies*

$$p_{(0,0)} = \frac{1}{(\lambda_1 + \lambda_2)\mathbb{E}_{(0,0)}[\tau_{(0,0)}]} \tag{98}$$

where $\mathbb{E}_{(0,0)}[\tau_{(0,0)}]$ *can be computed by first calculating* $\mathbb{E}_{(i,1)}[\tau_{(0,0)}]$*, for* $1 \leq i \leq m+1$*, which can be found by solving a linear system consisting of* $m+1$ *equations and* $m+1$ *unknowns.*
(b) For each integer $\ell \geq 1$*, we have*

$$\begin{aligned} p_{(\ell+m,\ell)} &= \frac{\lambda_2}{\lambda_1+\lambda_2+\mu} \sum_{k=0}^{\ell-1} \frac{1}{2\ell-2k-1} \binom{2\ell-2k-1}{\ell-1-k} \frac{\lambda_1^{\ell-k}\lambda_2^{\ell-k-1}}{(\lambda_1+\lambda_2)^{2\ell-2k-1}} p_{(k+m,k)} \\ &+ \frac{\lambda_1}{\lambda_1+\lambda_2+\mu} p_{(\ell+m-1,\ell)}, \end{aligned} \tag{99}$$

and

$$\begin{aligned} p_{(\ell,\ell)} &= \frac{\lambda_1}{\lambda_1+\lambda_2} \sum_{k=0}^{\ell-1} \frac{1}{2\ell-2k-1} \binom{2\ell-1-2k}{\ell-k} \frac{\lambda_2^{\ell-1-k}\lambda_2^{\ell-k}}{(\lambda_1+\lambda_2+\mu)^{2\ell-1-2k}} p_{(k,k)} \\ &+ \frac{\lambda_2}{\lambda_1+\lambda_2} p_{(\ell,\ell-1)}. \end{aligned} \tag{100}$$

(c) For $k = 1, \ldots, m-1$ *and for each integer* $\ell \geq 1$*, we have,*

$$p_{(\ell+k,\ell)} = \frac{\lambda_1}{\lambda_1+\lambda_2} p_{(\ell+k-1,\ell)} + \frac{\lambda_2}{\lambda_1+\lambda_2} p_{(\ell+k,\ell-1)}. \tag{101}$$

(d) For $k = 1, \ldots, m$*, we have,*

$$p_{(k,0)} = \frac{\lambda_1}{\lambda_1+\lambda_2} p_{(k-1,0)}. \tag{102}$$

(e) Next, for each integer $k \geq 1$ *and each state* $(i,j) \in D_k$*, we have,*

$$p_{(i,j)} = \sum_{\ell=0}^{i} \frac{j-i}{i+j-2\ell} \binom{i+j-2\ell}{j-\ell} \frac{\lambda_1^{i-\ell}\lambda_2^{j-\ell}}{(\lambda_1+\lambda_2+\mu)^{i+j-2\ell}} p_{(\ell,\ell)}. \tag{103}$$

(f) Finally, for each integer $k \leq -(m+1)$*, and each state* $(i,j) \in D_k$

$$p_{(i,j)} = \sum_{\ell=0}^{j} \frac{i-m-j}{i+j-2\ell-m} \binom{i+j-2\ell-m}{j-\ell} \frac{\lambda_1^{i-m-\ell}\lambda_2^{j-\ell}}{(\lambda_1+\lambda_2)^{i+j-2\ell-m}} p_{(\ell+m,\ell)}. \tag{104}$$

Equations (99)-(102) can also be represented in matrix form, which may be useful for computational purposes. We will only consider the case when $m = 2n, n \in \mathbb{N}$, but the case where m is odd can be expressed in a similar manner.

First we define some notation. For each integer $k \geq 0$, and each integer $\ell > k$, define

$$r_{\ell,k} := \frac{\lambda_1}{\lambda_1+\lambda_2}\frac{1}{2\ell-2k-1}\binom{2\ell-1-2k}{\ell-k}\frac{\lambda_2^{\ell-1-k}\lambda_2^{\ell-k}}{(\lambda_1+\lambda_2+\mu)^{2\ell-1-2k}},$$

and

$$s_{\ell,k} := \frac{\lambda_2}{\lambda_1+\lambda_2+\mu}\frac{1}{2\ell-2k-1}\binom{2\ell-2k-1}{\ell-1-k}\frac{\lambda_1^{\ell-k}\lambda_2^{\ell-k-1}}{(\lambda_1+\lambda_2)^{2\ell-2k-1}}.$$

Next, for each integer $0 \leq k \leq n$, we define the diagonal set

$$E_{2n-2k} := \{(2n-2k, 0), (2n-2k-1, 1), \ldots, (n-k, n-k)\}$$

and its corresponding row vector

$$\mathbf{p}_{2n-2k} := [p_{(2n-2k,0)}, p_{(2n-2k-1,1)}, \ldots, p_{(n-k,n-k)}].$$

For each integer $0 \leq k \leq n-1$, we define the diagonal set

$$E_{2n-2k-1} := \{(2n-2k-1, 0), (2n-2k-2, 1), \ldots, (n-k, n-k-1)\}$$

and its corresponding row vector

$$\mathbf{p}_{2n-2k-1} := [p_{(2n-2k-1,0)}, p_{(2n-2k-2,1)}, \ldots, p_{(n-k,n-k-1)}].$$

Similarly, for each integer $k \geq 1$ we define

$$E_{2n+2k} := \{(2n+k, k), (2n+k-1, k+1), \ldots, (n+k, n+k)\}$$

and

$$\mathbf{p}_{2n+2k} := [p_{(2n+k,k)}, p_{(2n+k-1,k+1)}, \ldots, p_{(n+k,n+k)}].$$

Finally, we define

$$E_{2n+2k-1} := \{(2n+k-1, k), (2n+k-2, k+1), \ldots, (n+k, n+k-1)\},$$

and

$$\mathbf{p}_{2n+2k-1} := [p_{(2n+k-1,k)}, p_{(2n+k-2,k+1)}, \ldots, p_{(n+k,n+k-1)}].$$

Next, for each $i, j \in \mathbb{N}$

$$\mathbf{A}_{i,j} := \left[\frac{q(x,y)}{q(y)}\right]_{x\in E_i, y\in E_j}.$$

Further, for each even $i \leq m$, and each even $j > i$, we define $\mathbf{B}_{i,j}$ as

$$\mathbf{B}_{i,j} := \left[b_{x,y}^{(i,j)}\right]_{x\in E_i, y\in E_j}$$

which is a matrix whose only non-zero entry corresponds to the ordered pair (x_{nw}, y_{nw}), where x_{nw} and y_{nw} are the northwestern-most states in E_i and E_j, respectively: this entry in $\mathbf{B}_{i,j}$ is equal to $r_{j/2,i/2}$. Lastly, for each even $i > m$, and each even $j > i$, we define $\mathbf{C}_{i,j}$ as

$$\mathbf{C}_{i,j} := \left[c_{x,y}^{(i,j)}\right]_{x\in E_i, y\in E_j}$$

which is a matrix whose only non-zero entries correspond to the ordered pairs (x_{nw}, y_{nw}) and (x_{se}, y_{se}), where

$$c^{(i,j)}_{(x_{se},y_{se})} = s_{j/2-n,i/2-n}, \quad c^{(i,j)}_{(x_{nw},y_{nw})} = r_{j/2,i/2}.$$

We are now ready to present formulas that allow us to compute $p_{(i,j)}$ for $(i,j) \in \cup_{k=0}^{n} D_{-k}$. For each integer $0 \leq k \leq n-1$

$$\mathbf{p}_{2n-2k} = \mathbf{p}_{2n-2k-1}\mathbf{A}_{2n-2k-1,2n-2k} + \sum_{j=1}^{n-k} \mathbf{p}_{2n-2k-2j}\mathbf{B}_{2n-2k-2j,2n-2k}$$

and

$$\mathbf{p}_{2n-2k-1} = \mathbf{p}_{2n-2k-2}\mathbf{A}_{2n-2k-2,2n-2k-1}.$$

The remaining row vectors can be calculated as follows: for each integer $k \geq 1$

$$\mathbf{p}_{2n+2k-1} = \mathbf{p}_{2n+2k-2}\mathbf{A}_{2n+2k-2,2n+2k-1}$$

and

$$\mathbf{p}_{2n+2k} = \mathbf{p}_{2n+2k-1}\mathbf{A}_{2n+2k-1,2n+2k} + \sum_{j=1}^{n} \mathbf{p}_{2n-2j}\mathbf{B}_{2n-2j,2n+2k} + \sum_{j=1}^{k} \mathbf{p}_{2n+2k-2j}\mathbf{C}_{2n+2k-2j,2n+2k}.$$

References

[1] Bowden, R., Keeler, H.P., Krzesinski, A.E., and Taylor, P.G. (2018). Block arrivals in the Bitcoin blockchain. Preprint accessible through the arXiv at https://arxiv.org/abs/1801.07447

[2] Buckingham, P., and Fralix, B. (2015). Some new insights into Kolmogorov's criterion, with applications to hysteretic queues. *Markov Processes and Related Fields* **21**, 339-368.

[3] Eyal, I., and Sirer, E.G. (2013). Majority is not enough: Bitcoin Mining is Vulnerable. *Financial Cryptography and Data Security*, pp. 436-454. Springer, Berlin.

[4] Fralix, B. (2015) When are two Markov chains similar? *Statistics and Probability Letters* **107**, 199-203.

[5] Fralix, B. (2019). On classes of Bitcoin-inspired infinite-server queueing models. Submitted for publication: preprint available at http://bfralix.people.clemson.edu/preprints.htm

[6] Frolkova, M., and Mandjes, M. (2019). A Bitcoin-inspired infinite-server model with a random fluid limit. *Stochastic Models* **35**, 1-32.

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

[8] Graham, R., Knuth, D., and Patashnik, O. (1994). *Concrete Mathematics*. Addison-Wesley.

[9] He, Q. (2014). *Fundamentals of Matrix-Analytic Methods*. Springer, New York.

[10] Huberman, G., Leshno, J.D., and Moallemi, C. (2019). An Economic Analysis of the Bitcoin Payment System. Draft accessible at https://moallemi.com/ciamac/papers/bitcoin-2017.pdf

[11] Joyner, J. and Fralix, B. (2016). A new look at Markov processes of G/M/1-type. *Stochastic Models* **32**, 253-274.

[12] Kasahara, S. and Kawahara, J. (2019). Effect of Bitcoin fee on transaction-confirmation process *Journal of Industrial and Management Organization* **15**, 365-386.

[13] Kawase, Y. and Kasahara, S. (2017). Transaction-confirmation time for Bitcoin: A Queueing Analytical Approach to Blockchain Mechanism. *Queueing Theory and Network Applications* **LNCS 10591**, 75-88.

[14] Latouche, G., and Ramaswami, V. (1999). *Introduction to Matrix-Analytic Methods in Stochastic Modeling*. ASA-SIAM Publications, Philadelphia, USA.

[15] Li, Q., Ma, J., and Chang, Y. (2018). Blockchain Queue Theory. Preprint accessible on arXiv at https://arxiv.org/abs/1808.01795.

[16] Li, Q., Ma, J., Chang, Y., Ma, F., and Yu, H. (2019). Markov Processes in Blockchain Systems. Preprint accessible on arXiv at https://arxiv.org/abs/1904.03598.

[17] Liu, X., and Fralix, B. (2019). On lattice-path counting and the random-product representation, with applications to the $\mathrm{E}_r/\mathrm{M}/1$ queue and the $\mathrm{M}/\mathrm{E}_r/1$ queue. *Methodology and Computing in Applied Probability*, to appear (article available online)

[18] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Paper available at https://bitcoin.org/bitcoin.pdf

[19] Renault, M. (2007). Four proofs of the ballot theorem. *Mathematics Magazine* **80**, 345-352.

[20] Tschorsch, F., and Scheuermann, B. (2016). Bitcoin and beyond: a technical survey on decentralized digital currencies. *IEEE Communications Surveys and Tutorials* **18**, 2084-2123.