Chapter 7

Trading and wealth evolution in the Proof of Stake protocol

Wenpin Tang[1]

A blockchain is a digit ledger allowing the secure transfer of assets in a distributed network without an intermediary, hence, achieving decentralisation. As the Internet is a technology to facilitate the digit flow of information, the blockchain is a technology to facilitate the digit exchange of value. Blockchain technology has shown great potential, with a wide range of applications including cryptocurrency [1,2], healthcare [3,4], supply chain [5,6], and non-fungible tokens [7,8]. See Part 2 of this book for other applications of the blockchain. Recently, a large number of financial institutions seek to launch crypto exchanges in the stock market [9].

The core of a blockchain is the consensus protocol, which specifies a set of rules for the participants (miners or validators) to agree on an ever-growing log of transactions so as to form a distributed ledger. There are two major blockchain protocols, *Proof of Work* (PoW [1]) and *Proof of Stake* (PoS [2,10]):

- In the PoW protocol, miners compete with each other by solving a hashing puzzle. The miner who solves the puzzle first receives a reward (a number of coins) and whose work validates a new block's addition to the blockchain. Hence, while the competition is open to everyone, the chance of winning is proportional to a miner's computing power. The PoW coins include Bitcoin and Dogecoin.
- In the PoS protocol, there is a bidding mechanism to select a miner to do the work of validating a new block. Participants who choose to join the bidding are required to commit some stakes (coins they own), and the winning probability is proportional to the number of stakes committed. The PoS coins include Ethereum and BNB.

As of July 15, 2023, `Cryptoslate` lists 326 PoW coins with a total \$628B (51%) market capitalisation, and 248 PoS coins with a total \$321B (26%) market capitalisation. One major pitfall of the PoW protocol is that competition among the miners has led to exploding levels of energy consumption, and hence raised the issue of sustainability [11,12]. Refs. [13–15] also discussed the drawbacks of the PoW

[1]Department of Industrial Engineering and Operations Research, Columbia University, USA

blockchain from economic perspectives. These concerns have created a strong incentive among blockchain practitioners to switch from the PoW to the PoS ecosystem, as was pioneered by Ethereum 2.0 in September 2022 [16].

In this chapter, we present recent research on the PoS protocol, with a focus on its wealth evolution. There are three major components in the PoS ecosystem:

(a) *User–miner interface*: The users seek to get their transactions settled and published on the blockchain by the miners. Since each block has a maximum capacity, most blockchains adopt a 'pay your bid' auction, in which the users bid to have the miners include their transactions in the blockchain. (In general, the more a user bids, the more likely her transaction will be settled shortly.) The activity of the user–miner interface relies on the blockchain adoption, and the problem is to design a good transaction fee mechanism, e.g., satisfying some incentive-compatible conditions.

(b) *Built-in PoS protocol*: Each miner selects a set of transactions from the mempool (according to the bids mentioned in (a)) and includes them into a block. As explained earlier, the miners then commit their stakes in a PoS election, and the elected miner gains the right to add the new block to the blockchain. In return, the elected miner will receive transaction fees from the users, and block rewards from the blockchain. The PoS protocol may have additional hard-coded rules, e.g., the longest chain. The key issue is the security level facing to various attacks.

(c) *Speculation and trading*: As the blockchain is a digit exchange vehicle, there is a cryptocurrency (crypto) attached to it. Along with the increasing blockchain adoption, crypto has become a new financial instrument. This leads to the crypto trading. The trading parties are the miners and the investors (i.e., the crypto market). The investors may be the blockchain users who trade the crypto for use, or the speculators who seek profit from crypto holdings. The problem is to understand the trading strategy and wealth evolution of the participants in the crypto market.

See Figure 7.1 for an illustration of the aforementioned components in the PoS ecosystem. Here we concentrate on part (c). Refer to [17–19] for discussions related to part (a), and [20–23] for developments in part (b).

As the readers may have observed, the miners play a particularly important role in the blockchain ecosystem: they manage the user–miner interface (in part (a)); they maintain the blockchain (in part (b)); they provide liquidity in the crypto trading (in part (c)). For the miners, they can commit their stakes to participate in the PoS mining process, trade their stakes on the crypto market for instantaneous profit, or a combination of the two. The most obvious questions are how the miner allocates her stakes between PoS mining and trading (called a *strategy*), and what is her wealth evolution. The former question is concerned with the miner's optimal strategy, while the latter studies the level of decentralisation in the PoS economy. Being more specific, we ask:

1. Does the PoS protocol lead to centralisation or the rich-get-richer phenomenon (assuming no trading)? This question is related to the PoS protocol design.

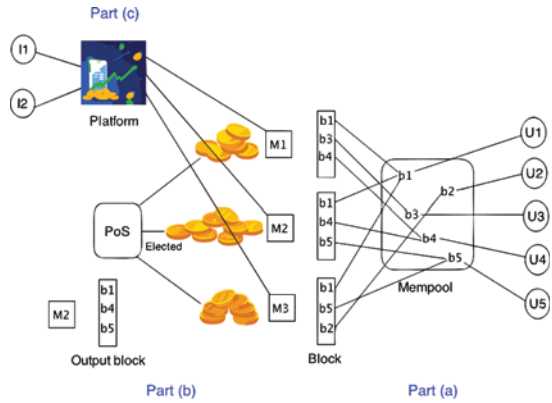


Figure 7.1 Miner–user–investor activities in the PoS protocol

2. For each individual miner, what is her best strategy? This question asks for a miner's trading incentive in the PoS protocol.
3. What is the wealth evolution of the whole (miner) population if each miner follows the best response to the others? This question is concerned with the miner's collective behaviour in a PoS trading environment.

We will answer these questions in the following sections. The remainder of the paper is organized as follows. In Section 7.1, we study the question (1), which hinges on a Pólya urn representation of the PoS election/protocol. Our main finding is that a large miner's shares are stable over the time, while those of a small miner can be much more fluctuated. As a consequence, the PoS protocol alone will lead to neither centralisation, nor decentralisation. In Section 7.2, we allow for trading in the PoS protocol, and provide a sufficient condition under which the miners have no incentive to trade. To address the question (2), we formulate and solve an optimal control problem in Section 7.3. The optimal control framework also allows us to analyse the question (3) via a mean field model in Section 7.4. Numerical experiments show that allowing trading in the PoS protocol does lead to decentralisation, which manifests the market power. In Section 7.5, we conclude with a few open problems and future directions. We emphasise that each PoS blockchain may have specific rules (e.g., block validity, the longest chain rule, etc.), and we will not take these blockchain-specific rules into account. Our analysis applies to the generic PoS protocol which will be defined accordingly.

7.1 Stability of the PoS protocol

We consider the question (1) in this section. Recall that the miners who choose to join the PoS election are required to commit their coins, and the winning probability is

proportional to the number of coins committed. To study the PoS protocol itself, we assume in this section that no trading is allowed, and all the miners will participate in the PoS mining process. Hence, the number of coins committed by each miner is equal to that she owns. At first glance, the miner who owns the largest number of coins is more likely to win the PoS election, which will in turn generate more and more coins for her. This is called the rich-get-richer phenomenon, which fundamentally violates the decentralised nature of any blockchain. We will show that the wealth evolution of a PoS miner depends on the reward type and her coin possession level.

Now we describe formally the PoS protocol without trading. Time is discrete, indexed by $t \in \{0, 1, \ldots\}$. Let K be the number of miners, and $N \in \mathbb{R}_+$ be the number of initial coins in the PoS blockchain. The miners are indexed by $[K] := \{1, \ldots, K\}$, and miner k's initial coins are $n_{k,0}$ with $\sum_{k=1}^{K} n_{k,0} = N$. We define the *share* as the fraction of coins each miner owns. So the initial shares $(\pi_{k,0},\ k \in [K])$ are given by

$$\pi_{k,0} := \frac{n_{k,0}}{N}, \quad k \in [K]. \tag{7.1}$$

Similarly, denote by $n_{k,t}$ the number of coins owned by miner k at time t, and the corresponding share is

$$\pi_{k,t} := \frac{n_{k,t}}{N_t}, \quad k \in [K], \quad \text{with} \quad N_t := \sum_{k=1}^{K} n_{k,t}. \tag{7.2}$$

Here N_t is the total number of coins at time t, with $N_0 = N$. We shall often refer to N_t as the 'volume of coins', or simply 'volume'.

At time t, miner k is selected at random with probability $\pi_{k,t-1}$. Once selected, the miner receives a deterministic reward of $R_t \in \mathbb{R}_+$ coins (which may include transaction fees and block rewards). Denote by $S_{k,t}$ the random event that miner k is selected at time t. So the number of coins owned by each miner evolves as

$$n_{k,t} = n_{k,t-1} + R_t 1_{S_{k,t}}, \quad k \in [K]. \tag{7.3}$$

Note that the volume satisfies $N_t = N_{t-1} + R_t$. Combining (7.2) and (7.3) yields a recursion of the shares:

$$\pi_{k,t} = \frac{N_{t-1}}{N_t}\pi_{k,t-1} + \frac{R_t}{N_t}1_{S_{k,t}}, \quad k \in [K]. \tag{7.4}$$

which is a (time-dependent) Pólya urn model [24].

We consider the long-time evolution of the shares $(\pi_{k,t},\ k \in [K])$. Let $\mathscr{F}_t$ be the filtration generated by the random events $(S_{k,r} : k \in [K], r \le t)$. Observe that for each $k \in [K]$, the process $(\pi_{k,t},\ t \ge 0)$ is an $\mathscr{F}_t$-martingale. By the martingale convergence theorem (see [25, Theorem 4.2.11]),

$$(\pi_{1,t}, \ldots, \pi_{K,t}) \longrightarrow (\pi_{1,\infty}, \ldots, \pi_{K,\infty}) \quad \text{as } t \to \infty \text{ with probability 1}, \tag{7.5}$$

where $(\pi_{1,\infty}, \ldots, \pi_{K,\infty})$ is some random probability distribution on $[K]$.

To quantify the wealth evolution of miner k, there are two obvious metrics:

$$|\pi_{k,t} - \pi_{k,0}| \text{ (difference)} \quad \text{and} \quad \frac{\pi_{k,t}}{\pi_{k,0}} \text{ (ratio)}. \tag{7.6}$$

If $|\pi_{k,t} - \pi_{k,0}|$ is close to 0, or $\frac{\pi_{k,t}}{\pi_{k,0}}$ is close to 1 (as t is large), we say that the share $\pi_{k,t}$ is *stable* or *concentrated*. This is the desired case as it implies that the PoS protocol will not lead to centralisation. Note that if $\pi_{k,t}$ is of constant order, there is no difference in considering $|\pi_{k,t} - \pi_{k,0}|$ or $\pi_{k,t}/\pi_{k,0}$. However, when $\pi_{k,t}$ is small, the two metrics may exhibit different results: $|\pi_{k,t} - \pi_{k,0}|$ is (trivially) close to 0 $(0 - 0)$, while $\pi_{k,t}/\pi_{k,0}$ is indeterminate $(0/0)$.

First, assume that $R_t \equiv R$ (constant reward), where the limiting $(\pi_{1,\infty}, \ldots, \pi_{K,\infty})$ can be identified. Let $\Gamma(z) := \int_0^\infty x^{z-1}e^{-x}dx$ be the Gamma function. Recall that the Dirichlet distribution with parameters $(a_1, \ldots, a_K)$, which we denote by $\mathrm{Dir}(a_1, \ldots, a_K)$, has support on the standard simplex $\{(x_1, \ldots, x_K) \in \mathbb{R}_+^K : \sum_{k=1}^K x_k = 1\}$ and has density:

$$f(x_1, \ldots, x_K) = \frac{\Gamma\left(\sum_{k=1}^K a_k\right)}{\prod_{k=1}^K \Gamma(a_k)} \prod_{k=1}^K x_k^{a_k - 1}. \tag{7.7}$$

The following theorem elucidates the wealth evolution of a PoS miner with a constant reward.

Theorem 1. *[26,27] Assume that the coin reward is $R_t \equiv R > 0$. Then the miner shares have a limiting distribution*

$$(\pi_{1,\infty}, \ldots, \pi_{K,\infty}) \stackrel{d}{=} Dir\left(\frac{n_{1,0}}{R}, \ldots, \frac{n_{K,0}}{R}\right). \tag{7.8}$$

Moreover,

(i) For $n_{k,0} = f(N)$ such that $f(N) \to \infty$ as $N \to \infty$, we have for each $\varepsilon > 0$ and for each $t \geq 1$ or $t = \infty$:

$$\mathbb{P}(|\pi_{k,t} - \pi_{k,0}| > \varepsilon) \to 0 \quad \textit{and} \quad \mathbb{P}\left(\left|\frac{\pi_{k,t}}{\pi_{k,0}} - 1\right| > \varepsilon\right) \to 0, \quad \textit{as } N \to \infty. \tag{7.9}$$

(ii) For $n_{k,0} = \Theta(1)$, we have for each $\varepsilon > 0$, $\mathbb{P}(|\pi_{k,\infty} - \pi_{k,0}| > \varepsilon) \to 0$ as $N \to \infty$, and the convergence in distribution:

$$\frac{\pi_{k,\infty}}{\pi_{k,0}} \xrightarrow{d} \frac{R}{n_{k,0}}\gamma\left(\frac{n_{k,0}}{R}\right), \quad \textit{as } N \to \infty, \tag{7.10}$$

where $\gamma\left(\frac{n_{k,0}}{R}\right)$ is a Gamma random variable with density $x^{\frac{n_{k,0}}{R}-1}e^{-x}1_{x>0}/\,\Gamma\left(\frac{n_{k,0}}{R}\right)$.

Let us make a few comments. The theorem reveals a *phase transition* of shares in the long run between large and small miners. Part (i) shows that for large miners, their shares are stable (which holds not only for extremely large miners with initial coins $n_{k,0} = \Theta(N)$ but for less rich large miners with $n_{k,0} \gg 1$, $n_{k,0} = o(N)$). Consequently, the PoS protocol with constant reward will lead to neither centralisation, nor decentralisation. On the other hand, the evolution of shares for small miners has a different limiting behaviour. Part (ii) shows that a small miner's share is volatile in

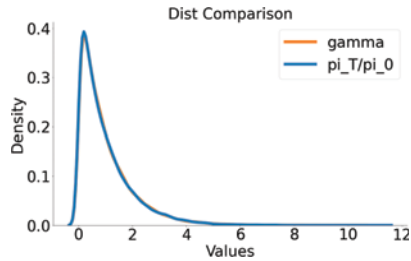


Figure 7.2 Constant reward: instability of $\pi_{k,t}/\pi_{k,0}$ for small miners. Blue curve: histogram of $\pi_{k,50,000}/\pi_{k,0}$ with $n_{k,0} = R = 1$ and $N = 100$. Orange curve: Gamma distribution.

such a way that the ratio $\pi_{k,\infty}/\pi_{k,0}$ is close to a gamma distribution independent of the initial coin offerings, and hence $\mathrm{Var}(\pi_{k,\infty}/\pi_{k,0}) \approx \frac{1}{n_{k,0}}$. For instance, if $n_{k,0} = R = 1$ the limiting distribution of the ratio $\pi_{k,\infty}/\pi_{k,0}$ reduces to the exponential distribution with parameter 1. (See Figure 7.2 for an illustration of this approximation.) In this case, we have

$$\mathbb{P}\left(\frac{\pi_{k,\infty}}{\pi_{k,0}} > \theta\right) \approx e^{-\theta} \quad \text{as } N \to \infty.$$

Thus, with probability $e^{-2} \approx 0.135$ a small miner's share will double, and with probability $1 - e^{-0.5} \approx 0.393$, this miner's share will be halved.

Next we consider the wealth evolution of a PoS miner with a decreasing reward. Though the limiting $(\pi_{1,\infty}, \ldots, \pi_{K,\infty})$ is not explicit, we can still characterise a miner's share stability in terms of her coin possession level.

Theorem 2. *[27] Assume that the coin reward is R_t with $R_t \geq R_{t+1}$ for each $t \geq 0$.*

1. *If R_t is bounded away from 0, i.e., $\lim_{t\geq 0} R_t = \underline{R} > 0$, then*
   (i) For $n_{k,0} = f(N)$ such that $f(N) \to \infty$ as $N \to \infty$, we have for each $\varepsilon > 0$ and each $t \geq 1$ or $t = \infty$:
   $$\mathbb{P}\left(\left|\frac{\pi_{k,t}}{\pi_{k,0}} - 1\right| > \varepsilon\right) \to 0, \quad \text{as } N \to \infty. \tag{7.11}$$
   (ii) For $n_{k,0} = \Theta(1)$, we have $\mathrm{Var}\left(\frac{\pi_{k,\infty}}{\pi_{k,0}}\right) = \Theta(1)$. Moreover, there is $c > 0$ independent of N such that for $\varepsilon > 0$ sufficiently small:
   $$\mathbb{P}\left(\left|\frac{\pi_{k,\infty}}{\pi_{k,0}} - 1\right| > \varepsilon\right) \geq c. \tag{7.12}$$
2. *If $R_t = \Theta(t^{-\alpha})$ for $\alpha > 0$, then for each $\varepsilon > 0$ and each $t \geq 1$ or $t = \infty$:*
   $$\mathbb{P}\left(\left|\frac{\pi_{k,t}}{\pi_{k,0}} - 1\right| > \varepsilon\right) \to 0, \quad \text{as } N \to \infty. \tag{7.13}$$

The theorem distinguishes two ways that the reward function decreases, leading to different phase transition results. Part (1) assumes that the reward function decreases to a nonzero value. In this case, the threshold to identify large and small miners is $n_{k,0} = \Theta(1)$, which is the same as that of the PoS protocol with a constant reward. This may not be surprising, since the underlying dynamics is not much different from the one with a constant reward. For large miners, the ratio $\pi_{k,\infty}/\pi_{k,0}$ is close to 1; while for small miners there is the *anti-concentration* bound (7.12), indicating that the evolution of a small miner's share is no longer stable, and may be volatile. Part (2) considers a fast decreasing reward $R_t = \Theta(t^{-\alpha})$ for $\alpha > 0$. In this case, there is no phase transition, and the ratio $\pi_{k,\infty}/\pi_{k,0}$ concentrates at 1 for every miner.

To conclude this section, we present the results of the wealth evolution of a PoS miner with an increasing reward.

Theorem 3. *[27] Assume that the coin reward $R_t = \rho N_{t-1}^{\gamma}$ for some $\rho > 0$ and $\gamma > 0$.*

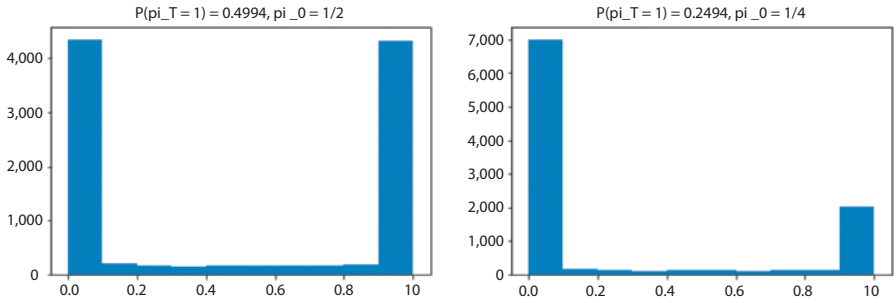
1. *If $\gamma > 1$, then $\pi_{k,\infty} \in \{0, 1\}$ almost surely with*
$$\mathbb{P}(\pi_{k,\infty} = 1) = \pi_{k,0}, \quad \mathbb{P}(\pi_{k,\infty} = 0) = 1 - \pi_{k,0} \tag{7.14}$$
2. *If $\gamma < 1$, then*
   (i) For $n_{k,0} = f(N)$ such that $f(N)/N^{\gamma} \to \infty$ as $N \to \infty$, we have for each $\varepsilon > 0$ and each $t \geq 1$ or $t = \infty$:
   $$\mathbb{P}\left(\left|\frac{\pi_{k,t}}{\pi_{k,0}} - 1\right| > \varepsilon\right) \to 0 \quad \text{as } N \to \infty. \tag{7.15}$$
   (ii) For $n_{k,0} = \Theta(N^{\gamma})$, we have $Var\left(\frac{\pi_{k,\infty}}{\pi_{k,0}}\right) = \Theta(1)$. Moreover, there exists $c > 0$ independent of N such that for $\varepsilon > 0$ sufficiently small:
   $$\mathbb{P}\left(\left|\frac{\pi_{k,\infty}}{\pi_{k,0}} - 1\right| > \varepsilon\right) \geq c. \tag{7.16}$$
   For $n_{k,0} = o(N^{\gamma})$, we have $Var\left(\frac{\pi_{k,\infty}}{\pi_{k,0}}\right) \to \infty$ as $N \to \infty$.

The theorem considers two increasing reward schemes: a geometric reward and a sub-geometric one. Part (1) assumes a geometric reward and shows that with probability one, all the shares will eventually go to one miner in such a way that

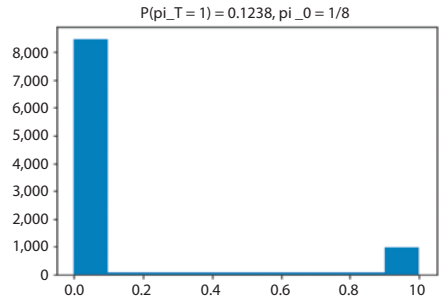
$$\mathbb{P}(\pi_k = 1 \text{ and } \pi_j = 0 \text{ for all } j \neq k) = \pi_{k,0}, \quad k \in [K].$$

We call this *chaotic centralisation* because the underlying dynamics will lead to the dictatorship, with the dictator being selected in a random manner. (See Figure 7.3 for an illustration of chaotic centralisation.) Part (2) considers a polynomial reward $R_t = \Theta(t^{\frac{1}{1-\gamma}})$ for $\gamma < 1$. In this case, there is a phase transition in the stability of $\pi_{k,t}/\pi_{k,0}$, with the threshold $n_{k,0} = \Theta(N^{\gamma})$.

We also mention that it is possible to study the wealth evolution in the PoS protocol with infinite population ($K = \infty$), see [27, Section 3].



(a) $\pi_{k,0} = \frac{1}{2}$ (b) $\pi_{k,0} = \frac{1}{4}$



(c) $\pi_{k,0} = \frac{1}{8}$

Figure 7.3 Increasing reward: chaotic centralisation. Histogram of $\pi_{k,5000}$ with $\rho = 0.001$, $\gamma = 1.1$, $N = 1{,}000$ and $\pi_{k,0} \in \{1/2, 1/4, 1/8\}$.

7.2 Participation and PoS trading

We consider the question (2) in this section and provide conditions under which no miner will have incentive to trade (so Theorems 1– 3 continue to hold). So far, we have not considered the possibility of allowing the miners to trade coins (among themselves). In the new setting of allowing trading, we need to modify the problem formulation presented in Section 7.1. First, for each $k \in [K]$, let $\nu_{k,t}$ be the number of coins that miner k will trade at time t. Then, instead of (7.3), the number of coins $n_{k,t}$ evolves as

$$n_{k,t} = \underbrace{n_{k,t-1} + R_t 1_{S_{k,t}}}_{n'_{k,t}} + \nu_{k,t}, \tag{7.17}$$

i.e., $n'_{k,t}$ denotes the number of coins miner k owns in between time $t-1$ and t, excluding those traded in period t. Note that $\nu_{k,t}$ will be up to miner k to decide, as opposed to the random event $S_{k,t}$ which is exogenous; in particular, $\nu_{k,t}$ can be negative

(as well as positive or zero). We will elaborate more on this below, but note that $\nu_{k,t}$ will be constrained such that after the updating in (7.17) $n_{k,t}$ will remain nonnegative.

Let $\{P_t,\, t \geq 0\}$ be the price process of each (unit of) coin, which is a stochastic process assumed to be independent of the randomness induced by the PoS selection (specifically, the process $\{S_{k,t}\}$). Hence, we augment the filtration $\{\mathscr{F}_t\}_{t\geq 0}$ with that of the exogenous price process $\{P_t,\, t \geq 0\}$ to a new filtration denoted $\{\mathscr{G}_t\}_{t\geq 0}$. This assumption need not be so far off, as the crypto's price tends to be affected by market shocks (such as macroeconomics, geopolitics, and breaking news) much more than by trading activities.

Let $b_{k,t}$ denote (units of) the risk-free asset that miner k holds at time t, and $r_{\text{free}} > 0$ the risk-free (interest) rate. As we are mainly concerned with the effect of exchanging coins to each individual, we allow miners to trade coins only internally among themselves, but not risk-free assets between them. Hence, each miner has to trade risk-free asset with a third-party instead of trading that with another bidder.

The decision for each miner k at t is a tuple, $(\nu_{k,t}, b_{k,t})$. Moreover, there is a terminal time, denoted $T_k \geq 1$, by which time miner k has to sell all assets, including both any risk-free asset and any coins owned at that time. T_k can either be deterministic or random. In the latter case, assume it has a finite expectation and is either adapted to $\{\mathscr{G}_t\}_{t\geq 0}$, or independent of all other randomness (in which case augment $\{\mathscr{G}_t\}$ accordingly). We also allow miner k to liquidate prior to T_k at a stopping time τ_k relative to $\{\mathscr{G}_t\}_{t\geq 0}$. Thus, miner k will also decide at which time τ_k to stop and exit. Abuse τ_k for the minimum of τ_k and T_k.

Let $c_{k,t}$ denote the (free) cash flow (or, 'consumption') of miner k at time t, i.e.,

$$c_{k,t} = (1 + r_{\text{free}})b_{k,t-1} - b_{k,t} - \nu_{k,t}P_t, \quad \forall 1 \leq t < \tau_k; \tag{C1}$$

with

$$b_{k,0} = 0,\ b_{k,t} \geq 0, \quad 0 \leq n_{k,t} = n'_{k,t} + \nu_{k,t} \leq N_t, \quad \forall 1 \leq t < \tau_k; \tag{C2}$$

and

$$c_{k,\tau_k} = (1 + r_{\text{free}})b_{k,\tau_k-1} + n'_{k,\tau_k}P_{\tau_k}, \quad \text{and } \nu_{k,\tau_k} = b_{k,\tau_k} = 0. \tag{C3}$$

The equation in (C1) is a budget constraint, which defines what's available for 'consumption' in period t. The requirements in (C2) are all in the spirit of disallowing shorting, on both the free asset $b_{k,t}$ and the traded coins $\nu_{k,t}$. In particular, the latter is constrained such that $\nu_{k,t} \geq -n'_{k,t}$, i.e., miner k cannot sell more than what's in possession at t; it also ensures that no miner can own a number of coins beyond the total volume ($n_{k,t} \leq N_t$). (C3) specifies how the assets are liquidated at the exit time τ_k: both ν_{k,τ_k} and b_{k,τ_k} will be set at zero, and all remaining coins n'_{k,τ_k} liquidated (cashed out at P_{τ_k} per unit).

Denote by τ_k and $(\nu, b) := \{(\nu_{k,t}, b_{k,t}),\ 1 \le t \le \tau_k\}$ miner k's decision (process) or 'strategy'. The objective of miner k is to solve the consumption–investment problem:

$$U_k^* := \max_{\tau_k,(\nu,b)} U_k := \max_{\tau_k,(\nu,b)} \mathbb{E}\left(\sum_{t=1}^{\tau_k} \delta_k^t c_{k,t}\right), \quad \text{subject to (C1), (C2), and (C3);} \tag{7.18}$$

where $\delta_k \in (0, 1]$ is a discount factor, a given parameter measuring the risk sensitivity of miner k.

We need to introduce two more processes that are related and central to understanding the PoS protocol in the presence of trading. The first one is $\{M_t,\ t \ge 1\}$, where $M_t := N_t P_t$ denotes the market value of the coins at time t. The second one is $\{\Pi_{k,t},\ t \ge 0\}$, for each bidder k, defined as follows:

$$\Pi_{k,0} := n_{k,0} P_0, \quad \text{and} \quad \Pi_{k,t} := \delta_k^t n'_{k,t} P_t - \sum_{j=1}^{t-1} \delta_k^j \nu_{k,j} P_j, \quad t \ge 1; \tag{7.19}$$

where $n'_{k,t+1}$ follows (7.17). The process $\{\Pi_{k,t}\}$ connects to the utility U_k in (7.18). To see this, summing up both sides of (C1) and (C3) over t (along with $b_{k,0} = 0$ in (C2)), we get

$$\sum_{t \le \tau_k} \delta_k^t c_{k,t} = \sum_{t \le \tau_k} \delta_k^t c_{k,t} = \delta_k^{\tau_k} n'_{\tau_k} P_{\tau_k} - \sum_{t=1}^{\tau_k - 1} \delta_k^t \nu_{k,t} P_t + \sum_{t=1}^{\tau_k - 1} \delta_k^t \left[(1 + r_{\text{free}})\delta_k - 1\right] b_{k,t}. \tag{7.20}$$

Observe that the first two terms on the right-hand side are equal to Π_{k,τ_k}, so we can rewrite the above as follows, emphasizing the exit time τ_k and the strategy (ν, b),

$$U_k(\tau_k, \nu, b) = \mathbb{E}\left[\Pi_{k,\tau_k}(\nu)\right] + \mathbb{E}\left(\sum_{t=1}^{\tau_k - 1} \delta_k^t \left[(1 + r_{\text{free}})\delta_k - 1\right] b_{k,t}\right); \tag{7.21}$$

hence, the right-hand side above is *separable*: the first term depends on (ν) only while the second term, the summation, on (b) only. Moreover, the second term is ≤ 0 provided $(1 + r_{\text{free}})\delta_k \le 1$, along with b being non-negative, part of the feasibility in (C2). In this case, we will have $U_k \le \mathbb{E}(\Pi_{k,\tau_k}(\nu))$, which implies $U_k^* \le \max_{\tau_k,\nu} \mathbb{E}(\Pi_{k,\tau_k}(\nu))$, with equality holding when $b_{k,t} = 0$ for all $t = 1, \ldots, \tau_k$.

We are ready to present the result of the utility maximisation problem in (7.18). Two strategies are singled out: the *'buy-out' strategy*, in which miner k buys up all coins available at time 1, and then participate in the PoS mining process until the end; and the *'non-participation' strategy*, in which miner k turns all $n_{k,0}$ coins into cash, and then never participates in either PoS mining or trading for all $t \ge 1$. Note that the non-participation strategy is executed at $\tau_k = 0$; as such, it complements the feasible class, which is for $\tau_k \ge 1$ and presumes participation. The buy-out strategy clearly belongs to the feasible class.

Theorem 4 (Buy-out strategy versus non-participation). *[26,28] Assume the following two conditions:*

$$\text{(a)}\ \ \delta_k(1+r_{free}) \le 1 \quad \text{and} \quad \text{(b)}\ \ \mathbb{E}(M_{t+1}\,|\,\mathscr{G}_t) = (1+r_{cryp})M_t. \tag{7.22}$$

Then with condition (a), the maximal utility U_k^* is achieved by setting $b_{k,t} = 0$ for all $t = 1, \ldots, T_k$; i.e., $U_k^* = \max_v \mathbb{E}(\Pi_{k,T_k})$. In addition, all three parts of the following will hold.

- *(i) If $\delta_k(1+r_{cryp}) \le 1$, then any feasible strategy will provide no greater utility for miner k than the non-participation strategy, i.e., $U_k^* \le n_{k,0}P_0$.*
- *(ii) If $\delta_k(1+r_{cryp}) \ge 1$, then any feasible strategy will provide no greater utility for miner k than the buy-out strategy. In this case, miner k will buy all available coins at time 1, and participate in the PoS mining process until the terminal time T_k.*
- *(iii) If $\delta_k(1+r_{cryp}) = 1$, then miner k is indifferent between the non-participation and the buy-out strategy with any exit time, both of which will provide no less utility than any feasible strategy. All strategies achieve the same utility (which is $\Pi_{k,0} = n_0 P_{k,0}$).*

Moreover, when $\delta_k = \delta := (1+r_{cryp})^{-1}$ for all k, no miner will have any incentive to trade. Consequently, the long-term behaviour of $\pi_{k,t}$ characterised in Theorems 1–3 will hold.

In what remains of this section, we make a few remarks on Theorem 4, in particular, to motivate and explain its required conditions. First, the rate r_{cryp}, which is determined by condition (b), is the (expected) rate of return of each coin, i.e., it is the counterpart of r_{free}, the rate for the risk-free asset. For all practical purpose, we can assume $r_{\text{crpt}} \ge r_{\text{free}}$, even though this is not assumed in the theorem. When this relation holds, condition (a) will become superfluous in cases (i) and (iii).

Second, the factor δ_k in the utility objective in (7.18) plays a key role in characterizing phase transitions in terms of $\delta_k(1+r_{\text{cryp}})$. In case (i), the inequality $\delta_k \le 1/(1+r_{\text{cryp}})$ implies miner k is seriously risk-averse; and this is reflected in k's non-participation strategy. In case (ii), the inequality holds in the opposite direction, implying miner k is lightly risk-averse or even a risk taker. Accordingly, k's strategy is to aggressively sweep up all the available coins to reach monopoly and participate (but not trade) until the terminal time. In case (iii), the inequality becomes an equality $\delta_k = 1/(1+r_{\text{cryp}})$, and $(\Pi_{k,t})$ becomes a martingale. Thus, miner k is indifferent between non-participation and participation, and, in the latter case, indifferent to all (feasible) strategies, including the buy-out (and the no-trading) strategy. Indeed, the equality $\delta_k = 1/(1+r_{\text{cryp}})$ is both necessary and sufficient for the no-trading strategy.

Next, we emphasise that the two conditions in (7.22) play very different roles. Condition (b) makes $(\Pi_{k,t})$ a super- or sub-martingale or a martingale, according to miner k's risk sensitivity as specified by the inequalities and equality applied to δ_k in the three cases. Yet, to solve the maximisation problem in (7.18), $(\Pi_{k,t})$ needs to be connected to the utility; and this is the role played by condition (a), under

which, it is necessary (for optimality) to set $b_{k,t} = 0$ for all $t \geq 1$, and applicable to all three cases. In this sense, condition (a) alone solves half of the maximisation problem, the $b_{k,t}$ half of the strategy. In fact, it is more than half, as the optimal ν strategy is only needed in the sub-martingale case; and, even there, condition (a) pins down the fact that to participate (even without trading) is better than non-participation.

Theorem 4 is easily extended to the case where the rates $r_{\text{cryp}}(t)$ and $r_{\text{free}}(t)$ may vary over the time. In this case, it suffices to modify the conditions in case (i) to $\left(1 + \sup_{t<T_k} r_{\text{cryp}}(t)\right) \delta_k \leq 1$ and $\left(1 + \sup_{t<T_k} r_{\text{free}}(t)\right) \delta_k \leq 1$; the conditions in case (ii) to $\left(1 + \inf_{t<T_k} r_{\text{cryp}}(t)\right) \delta_k \geq 1$ and $\left(1 + \sup_{t<T_k} r_{\text{free}}(t)\right) \delta_k \leq 1$; and the conditions in case (iii) to $\delta_k = (1 + r_{\text{cryp}})^{-1}$ and $\sup_{t<T_k} r_{\text{free}}(t) \leq r_{\text{cryp}}$, with r_{cryp} being constant. Then, Theorem 4 will continue to hold.

Finally, the last part of the theorem considers the wealth evolution of a homogenous miner population. It is also worth considering the wealth evolution of a heterogeneous miner population (e.g., with different risk sensitivity, holding periods, etc.) See [29] for a study on the reward effect on the wealth distribution of the miners with different coin holding horizons.

7.3 PoS trading with volume constraint – a continuous-time control setup

We continue to consider the question (2) in this section. As shown in Theorem 4, the miner's strategy is either not to participate (in both PoS mining and trading) or to sweep up all available coins immediately. The latter, being a market manipulation, rarely occurs in practice due to regulation. One way to prohibit the 'buy-out' strategy is to limit the number of coins that can be traded at a time. This motivates the study of the PoS trading with volume constraint.

To simplify the analysis, we adopt a continuous-time control approach. Time is continuous, indexed by $t \in [0, T]$, for a fixed $T > 0$ representing the length of a finite horizon. Let $\{N(t),\ 0 \leq t \leq T\}$ (with $N(0) := N$) denote the process of the volume of coins, which is increasing in time and sufficiently smooth. So the derivative $N'(t)$ represents the instantaneous rate of 'reward' by the PoS protocol. For instance, we will consider below, as a special case, the process $N(t)$ of a polynomial form:

$$N_\alpha(t) = (N^{\frac{1}{\alpha}} + t)^\alpha, \quad t \geq 0. \tag{7.23}$$

The parametric family (7.23) covers different rewarding schemes according to the values of α: for $0 < \alpha < 1$, the process $N_\alpha(t)$ corresponds to a decreasing reward; for $\alpha = 1$, the process $N_1(t) = N + t$ gives a rate one constant reward; for $\alpha > 1$, the process $N_\alpha(t)$ amounts to an increasing reward.

Let $K \geq 2$ be the number of miners, who are indexed by $k \in [K] := \{1, \ldots, K\}$. For each miner k, let $\{X_k(t),\ 0 \leq t \leq T\}$ (with $X_k(0) = x_k$) denote the process of the number of coins that miner k holds, with $X_k(t) \geq 0$ and $\sum_{k=1}^K X_k(t) = N(t)$ for all $t \in [0, T]$. For our continuous-time PoS model here, in which the time required

for each round of voting is 'infinitesimal', imagine there are M rounds of election during any given time interval $[t, t+\Delta t]$. (Each round in Ethereum takes about 10 s, corresponding to the block-generation time [30].) In each round miner k gets either some coin(s) or nothing, so the average total number of coins k will get over the M rounds is (by law of large numbers when M is large),

$$\underbrace{\frac{X_k(t)}{N(t)}\frac{N'(t)\Delta t}{M}}_{\text{average number of coins in each round}} \times \underbrace{M}_{\text{number of rounds}} = \frac{X_k(t)}{N(t)}N'(t)\Delta t.$$

Hence, replacing Δt by the infinitesimal dt, we know miner k will receive (on average) $\frac{X_k(t)}{N(t)}N'(t)dt$ coins, where $\frac{X_k(t)}{N(t)}$ is k's winning probability, and $N'(t)dt$ is the reward issued by the blockchain in $[t, t+dt]$.

The miners are allowed to trade (buy or sell) their coins. Miner k will buy $\nu_k(t)dt$ coins in $[t, t+dt]$ if $\nu_k(t) > 0$, and sell $-\nu_k(t)dt$ coins if $\nu_k(t) < 0$. This leads to the following dynamics of miner k's coins under trading:

$$X_k'(t) = \nu_k(t) + \frac{N'(t)}{N(t)}X_k(t) \quad \text{for } 0 \le t \le \tau_k \wedge T := \mathscr{T}_k, \tag{7.24}$$

where $\tau_k := \inf\{t > 0 : X_k(t) = 0\}$ is the first time at which the process $X_k(t)$ reaches zero. It is reasonable to stop the trading process if a miner runs out of coins or gets all available coins: if $\mathscr{T}_k = \tau_k$, then miner k liquidates all his coins by time τ_k, and $X_k(\mathscr{T}_k) = 0$; if $\mathscr{T}_k = \max_{j\neq k}\tau_j$, then miner k gets all issued coins by time $\max_{j\neq k}\tau_j$, and, hence, $X_k(\mathscr{T}_k) = N(\mathscr{T}_k)$. We set $X_k(t) = X_k(\mathscr{T}_k)$ for $t > \mathscr{T}_k$.

The problem is for each miner k to decide how to trade coins with others under the PoS protocol. Similar to Section 7.2, let $\{P(t),\ 0 \le t \le T\}$ be the price process of each (unit of) coin, which is a stochastic process assumed to be independent of the dynamics in (7.24). Let $b_k(t)$ denote the (units of) risk-free asset that miner k holds at time t, and let $r > 0$ denote the risk-free (interest) rate. Recall that all K miners are allowed to trade coins only internally among themselves, whereas each miner can only exchange cash with an external source (say, a bank).

Let $\{c_k(t),\ 0 \le t \le T\}$ be the process of consumption, or cash flow of miner k, which follows the dynamics below:

$$dc_k(t) = rb_k(t)dt - db_k(t) - P(t)\nu_k(t)dt, \quad 0 \le t \le \mathscr{T}_k; \tag{C1}$$

with

$$b_k(0) = 0, \quad b_k(t) \ge 0 \text{ for } 0 \le t \le \mathscr{T}_k, \quad 0 \le X_k(t) \le N(t) \text{ for } 0 \le t \le \mathscr{T}_k. \tag{C2}$$

Set $b_k(t) = b_k(\mathscr{T}_k)$ and $\nu_k(t) = 0$ for $t > \mathscr{T}_k$. The conditions (C1)–(C2) are the continuous analogue to those in Section 7.2. We also require that the trading strategy be bounded: there is $\overline{\nu}_k > 0$ such that

$$|\nu_k(t)| \le \overline{\nu}_k. \tag{C3}$$

The objective of miner k is:

$$\sup_{\{(\nu_k(t),b_k(t))\}} J(\nu_k, b_k) := \mathbb{E}\Big\{ \int_0^{\mathscr{T}_k} e^{-\beta_k t}\,[dc_k(t) + \ell_k(X_k(t))dt] + e^{-\beta_k \mathscr{T}_k}\,[b_k(\mathscr{T}_k) + h_k(X_k(\mathscr{T}_k))] \Big\} \tag{7.25}$$

subject to (7.24), (C1), (C2), *and* (C3),

where $\beta_k > 0$ is a discount factor; $\ell_k(\,\cdot\,)$ and $h_k(\,\cdot\,)$ are two utility functions representing, respectively, the running profit and the terminal profit.

While generally following Merton's consumption–investment framework, our formulation takes into account some distinct features of the PoS blockchain. One notable point is the utilities ℓ and h are expressed as functions of the number of coins $X_k(t)$, as opposed to their value $P(t)X_k(t)$. To the extent that $P(t)$ is treated as exogenous, this difference may seem to be trivial. Yet, it is a reflection of the more substantial fact that crypto-participants tend to mentally decouple the utility of holding coins from their monetary value at any given time.

Throughout below, the following conditions will be assumed:

Assumption 5.

(i) $N : [0, T] \to \mathbb{R}_+$ *is increasing with* $N(0) = N > 0$, *and* $N \in \mathscr{C}^2([0, T])$.
(ii) $\ell : \mathbb{R}_+ \to \mathbb{R}_+$ *is increasing and* $\ell \in \mathscr{C}^1(\mathbb{R}_+)$.
(iii) $h : \mathbb{R}_+ \to \mathbb{R}_+$ *is increasing and* $h \in \mathscr{C}^1(\mathbb{R}_+)$.

To lighten notation, omit the subscript k, and write

$$U(x) := \sup_{\{(\nu(t),b(t))\}} J(\nu, b) := \mathbb{E}\Big\{ \int_0^{\mathscr{T}} e^{-\beta t}\,[dc(t) + \ell(X(t))dt] + e^{-\beta \mathscr{T}}\,[b(\mathscr{T}) + h(X(\mathscr{T}))] \Big\} \tag{7.26}$$

$$\text{subject to} \quad X'(t) = \nu(t) + \frac{N'(t)}{N(t)} X(t),\ X(0) = x, \tag{C0}$$

$$dc(t) = rb(t)dt - db(t) - P(t)\nu(t)dt, \tag{C1}$$

$$b(0) = 0,\ b(t) \geq 0 \text{ and } 0 \leq X(t) \leq N(t), \tag{C2}$$

$$|\nu(t)| \leq \overline{\nu}. \tag{C3}$$

Let

$$\widetilde{P}_\beta(t) := e^{-\beta t}\mathbb{E}P(t), \quad t \in [0, T]. \tag{7.27}$$

Substituting the constraint (C1) into the objective function, and taking into account $rb(t)dt - db(t) = -e^{rt}d(e^{-rt}b(t))$, along with (7.42), we have

$$\begin{aligned} J(\nu, b) &= (r-\beta)\int_0^{\mathscr{T}} e^{-\beta t}b(t)dt \\ &\quad + \int_0^{\mathscr{T}} [-\widetilde{P}_\beta(t)\nu(t) + e^{-\beta t}\ell(X(t)]dt + e^{-\beta\mathscr{T}}h(X(\mathscr{T})) \\ &:= J_1(b) + J_2(\nu). \end{aligned} \tag{7.28}$$

Hence,

$$U(x) := \sup_{\{(\nu,b)\}} J(\nu, b) = \sup_b J_1(b) + \sup_\nu J_2(\nu). \tag{7.29}$$

Suppose $\beta \geq r$, which is analogue to (7.22)(a) in the discrete setting. Then, from the $J_1(b)$ expression in (7.28), and taking into account $b(t) \geq 0$ as constrained in (C2), we have $\sup_b J_1(b) = 0$ with the optimality binding at $b_*(t) = 0$ for all t. Therefore, the problem in (7.26) reduces to

$$U(x) = \sup_\nu J_2(\nu) \quad \text{subject to (C0), (C2'), and (C3),} \tag{7.30}$$

where (C2') is (C2) without the constraints on $b(\,\cdot\,)$. The problem (7.26) can then be solved by dynamic programming and the Hamilton–Jacobi–Bellman (HJB) equations. The result is stated as follows.

Theorem 5. *[31] Assume that $r \leq \beta$, and $\widetilde{P}_\beta(t)$ in* (7.42) *satisfies the Lipschitz condition:*

$$|\widetilde{P}_\beta(t) - \widetilde{P}_\beta(s)| \leq C|t-s| \quad \textit{for some } C > 0. \tag{7.31}$$

Then, $U(x) = v(0,x)$ where $v(t,x)$ is the unique viscosity solution to the following HJB equation, where $Q := \{(t,x) : 0 \leq t < T,\ 0 < x < N(t)\}$:

$$\begin{cases} \partial_t v + e^{-\beta t}\ell(x) + \frac{xN'(t)}{N(t)}\partial_x v + \sup_{|\nu|\leq\overline{\nu}}\{\nu(\partial_x v - \widetilde{P}_\beta(t))\} = 0 \quad \textit{in } Q, \\ v(T,x) = e^{-\beta T}h(x), \\ v(t,0) = e^{-\beta t}h(0),\ v(t,N(t)) = e^{-\beta t}h(N(t)). \end{cases} \tag{7.32}$$

Moreover, the optimal strategy is $b_*(t) = 0$ and $\nu_*(t) = \nu_*(t, X_*(t))$ for $0 \leq t \leq \mathscr{T}_*$, where $\nu_*(t,x)$ achieves the supremum in (7.32)*, and $X_*(t)$ solves $X_*'(t) = \nu_*(t, X_*(t)) + \frac{N'(t)}{N(t)}X_*(t)$ with $X_*(0) = x$, and $\mathscr{T}_* := \inf\{t > 0 : X_*(t) = 0 \text{ or } N(t)\} \wedge T$.*

Now specialise to linear utility $\ell(x) = \ell x$ and $h(x) = hx$, for some given (positive) constants ℓ and h. In this case, we can derive a closed-form solution to the HJB equation in (7.32), and then derive the optimal strategy $\nu_*(t)$ (in terms of $\widetilde{P}_\beta(t)$). Let

$$\Psi(t) := \frac{1}{N(t)}\left(he^{-\beta T}N(T) + \ell\int_t^T e^{-\beta s}N(s)ds\right). \tag{7.33}$$

The following corollary classifies all possible optimal strategies (of the miner).

Corollary 1. *[31] Let $\ell(x) = \ell x$ and $h(x) = hx$ with $\ell, h > 0$, and $N(t)$ satisfy Assumption 5 (i). Assume that $\widetilde{P}_\beta(t)$ satisfies the Lipschitz condition in* (7.31) *and that $\overline{\nu}$ satisfies:*

$$\overline{\nu} \int_0^T \frac{dt}{N(t)} \leq \frac{x}{N} \wedge \frac{N-x}{N}. \tag{7.34}$$

Then, the following results hold:

(i) *Suppose $\widetilde{P}_\beta(t)$ stays constant, i.e., for all $t \in [0,T]$, $\widetilde{P}(t) = \widetilde{P}(0) = P(0)$.*
  (a) *If $P(0) \geq \Psi(0)$, then $\nu_*(t) = -\overline{\nu}$ for all $0 \leq t \leq T$.*
  (b) *If $P(0) \leq \Psi(T)$, then $\nu_*(t) = \overline{\nu}$.*
  (c) *If $\Psi(T) < P(0) < \Psi(0)$, then $\nu_*(t) = \overline{\nu}$ for $t \leq t_0$, and $-\overline{\nu}$ for $t > t_0$, where t_0 is the unique point in $[0,T]$ such that $P(0) = \Psi(t_0)$ with $\Psi(t)$ defined in* (7.33).

(ii) *Suppose that $\widetilde{P}_\beta(t)$ is increasing in $t \in [0,T]$.*
  (a) *If $P(0) \geq \Psi(0)$, then $\nu_*(t) = -\overline{\nu}$ for all $0 \leq t \leq T$.*
  (b) *If $\widetilde{P}_\beta(T) \leq \Psi(T)$, then $\nu_*(t) = \overline{\nu}$.*
  (c) *If $P(0) < \Psi(0)$ and $\widetilde{P}_\beta(T) > \Psi(T)$, then $\nu_*(t) = \overline{\nu}$ for $t \leq t_0$, and $-\overline{\nu}$ for $t > t_0$, where t_0 is the unique point of intersection of $\widetilde{P}_\beta(t)$ and $\Psi(t)$ on $[0,T]$.*

(iii) *Suppose that $\widetilde{P}_\beta(t)$ is decreasing in $t \in [0,T]$.*
  (a) *If $P(0) \geq \Psi(0)$, then the miner first sells, and may then buy, etc., always at full capacity, according to the crossings of $\widetilde{P}_\beta(t)$ and $\Psi(t)$ in $[0,T]$.*
  (b) *If $P(0) < \Psi(0)$, then the miner first buys, and may then sell, etc., always at full capacity, according to the crossings of $\widetilde{P}_\beta(t)$ and $\Psi(t)$ in $[0,T]$.*

Several remarks are in order. First note that the condition in (7.34) is to guarantee the constraint (C2') not activated prior to T, that is, to exclude the possibility of monopoly/dictatorship that will trigger a forced early exit. Second, the monotone properties of $\widetilde{P}_\beta(t)$, which classify the three parts (i)–(iii) in the corollary naturally connect to martingale pricing: $\widetilde{P}_\beta(t)$ being a constant in (i) makes the process $e^{-\beta t}P(t)$ a martingale, whereas $\widetilde{P}_\beta(t)$ increasing or decreasing, respectively in (ii) and (iii), makes $e^{-\beta t}P(t)$ a sub-martingale or a super-martingale. On the other hand, the function $\Psi(t)$ represents the rate of return of the miner's utility (from holding of coins, x); and interestingly, in the linear utility case, this return rate is independent of x while decreasing in t. Thus, the trading strategy is completely determined by comparing this return rate $\Psi(t)$ with the miner's risk-adjusted coin price $\widetilde{P}_\beta(t)$: if $\Psi(t) \geq$ (resp. $<$) $\widetilde{P}_\beta(t)$, then the miner will buy (resp. sell) coins.

Specifically, following (i) and (ii) of Corollary 1, for a constant or an increasing $\widetilde{P}_\beta(t)$ (corresponding to a risk-neutral or risk-seeking miner), there are only three possible optimal strategies: buy all the time, sell all the time, or first buy then sell. (The first-buy-then-sell strategy echoes the general investment practice that an early investment pays off in a later day.) See Figure 7.4 for an illustration.

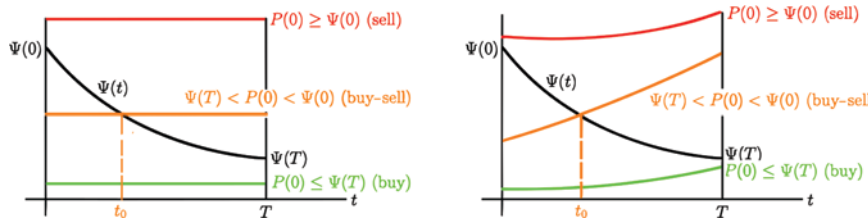


Figure 7.4 Optimal trading with linear $\ell(\cdot), h(\cdot)$ when $\widetilde{P}_\beta(t)$ is constant (left) and $\widetilde{P}_\beta(t)$ is increasing (right)

In part (iii) of Corollary 1, when $\widetilde{P}_\beta(t)$ is decreasing in t, like $\Psi(t)$, the multiple crossings between the two decreasing functions can be further pinned down when there's more model structure. Consider, for instance, when $P(t)$ follows a geometric Brownian motion (GBM):

$$\frac{dP(t)}{P(t)} = \mu dt + \sigma dB_t, \quad \text{or} \quad P(t) = P(0)e^{(\mu-\sigma^2/2)t+\sigma B_t}; \quad t \in [0,T], \tag{7.35}$$

where $\{B_t\}$ denotes the standard Brownian motion; and $\mu > 0$ and $\sigma > 0$ are the two parameters of the GBM model, representing the rate of return and the volatility of $\{P(t)\}$. The following proposition gives the conditions under which $\Psi_\alpha(t) - \widetilde{P}_\beta(t)$ is monotone in the regime $N \to \infty$, and optimal strategies are derived accordingly.

Proposition 1. *[31] Suppose the assumptions in Proposition 1 hold, with $N(t) = N_\alpha(t)$ and $\{P(t)\}$ specified by* (7.35) *with $\beta > \mu$. As $N \to \infty$, we have the following results:*

1. *If for some $\varepsilon > 0$, $P(0) > \frac{1}{\beta-\mu}\left(\frac{\alpha h e^{-\mu T}(N^{\frac{1}{\alpha}}+T)^\alpha}{N^{1+\frac{1}{\alpha}}} + \frac{\alpha\ell\beta^{-1}}{N^{\frac{1}{\alpha}}} + \ell\right) + \frac{\varepsilon}{N^{\frac{1}{\alpha}}}$, then $\Psi_\alpha(t) - \widetilde{P}_\beta(t)$ is increasing on $[0,T]$.*
2. *If for some $\varepsilon > 0$, $P(0) < \frac{1}{\beta-\mu}\left(\frac{\alpha h e^{-\beta T}}{N^{\frac{1}{\alpha}}+T} + \ell e^{-\mu T}\right) - \frac{\varepsilon}{N^{\frac{1}{\alpha}}}$, then $\Psi_\alpha(t) - \widetilde{P}_\beta(t)$ is decreasing on $[0,T]$.*

Consequently, we have:

(a) If $P(0) > e^{(\beta-\mu)T}\Psi_\alpha(T)$ and (1) holds, or $P(0) > \Psi_\alpha(0)$ and (2) holds, then $\nu_*(t) = -\overline{\nu}$ for all t.

(b) If $\Psi_\alpha(0) \le P(0) < e^{(\beta-\mu)T}\Psi_\alpha(T)$ and (1) holds, then $\nu_*(t) = -\overline{\nu}$ for $t \le t_0$ and $\nu_*(t) = \overline{\nu}$ for $t > t_0$, where t_0 is the unique point of intersection of $\widetilde{P}_\beta(t)$ and $\Psi_\alpha(t)$ on $[0,T]$.

(c) If $e^{(\beta-\mu)T}\Psi_\alpha(T) \le P(0) < \Psi_\alpha(0)$ and (2) holds, then $\nu_*(t) = \overline{\nu}$ for $t \le t_0$ and $\nu_*(t) = -\overline{\nu}$ for $t > t_0$, where t_0 is the unique point of intersection of $\widetilde{P}_\beta(t)$ and $\Psi_\alpha(t)$ on $[0,T]$.

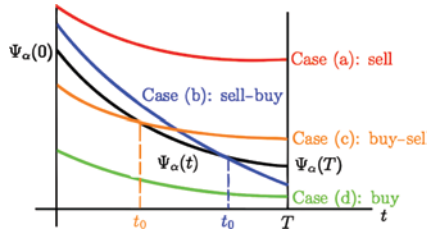


Figure 7.5 *Optimal trading with linear $\ell(\cdot), h(\cdot)$ when $\widetilde{P}_\beta(t) = P(0)e^{(\mu-\beta)t}$ and $N(t) = N_\alpha(t)$*

(d) *If $P(0) < e^{(\beta-\mu)T}\Psi_\alpha(T)$ and (2) holds, or $P(0) < \Psi_\alpha(0)$ and (1) holds, then $\nu_*(t) = \nu$ for all t.*

See Figure 7.5 for an illustration of all four possible strategies.

7.4 PoS trading – a mean field model

We consider the question (3) in this section. In the previous sections, we study the optimal strategy for each individual miner, assuming that all other miners will 'cooperate' with her (except that no shorting is allowed). This assumption seems to be too optimistic. As mentioned in part (c) in the introduction, there are also investors or speculators participating in the PoS trading.

- In Sections 7.2–7.3, the price process (of each coin) is assumed to be exogenous. In the presence of investors and in view of their speculative nature, it is necessary to incorporate the market impact into the price formation.
- Interaction and competition among the miners and investors should play a role in each miner's decision. Thus, it is natural to formulate the PoS trading as a game building on the continuous-time control setting in Section 7.3.

With an exchange platform (e.g., Coinbase) for miner–investor tradings, we can define a notion of *equilibrium trading strategy* for a typical miner. This leads to the wealth evolution of the whole (miner) population from a mean field perspective. Refer to [32–34] for discussions on the game theoretical analysis of the PoW protocol. We would like to point out that the material in this section is preliminary (and novel), so there are many research problems in modelling, theory, and applications.

Recall that $\{N(t),\ 0 \le t \le T\}$ is the process of the volume of coins issued by the PoS blockchain. There are K miners, indexed by $k \in [K]$. For each miner k, $\{X_k(t),\ 0 \le t \le T\}$ (with $X_k(0) = x_k$) denotes the process of the number of coins that miner k holds, and $\{\nu_k(t),\ 0 \le t \le T\}$ denotes miner k's trading strategy.

Let $\{Z(t),\ t \ge 0\}$ (with $Z(0) = z$) be the process of the number of coins that investors possess, with $X_k(t), Z(t) \ge 0$ and

$$\sum_{k=1}^{K} X_k(t) + Z(t) = N(t), \quad \text{for } 0 \le t \le T. \tag{7.36}$$

So there are only $N(t) - Z(t)$ coins committed in the PoS election. The dynamics of miner k's coin under trading is:

$$X_k'(t) = \nu_k(t) + \frac{N'(t)}{N(t) - Z(t)} X_k(t) \quad \text{for} \quad 0 \le t \le \tau_k \wedge T := \mathscr{T}_k, \tag{7.37}$$

where $\tau_k := \inf\{t > 0 : X_k(t) = 0\}$. We set $X_k(t) = X_k(\mathscr{T}_k)$ for $t > \mathscr{T}_k$. If we take $Z(t) \equiv 0$ (no investors), the dynamics (7.37) reduces to (7.24). Equations (7.36)–(7.37) imply that $\sum_{k=1}^K \nu_k(t) + Z'(t) = 0$, which can be viewed as a clearing house condition. It simply yields

$$Z(t) = Z(0) - \int_0^t \sum_{k=1}^K \nu_k(s) ds. \tag{7.38}$$

Central to each miner's decision is the price process $\{P(t),\ t \ge 0\}$ of each (unit) of coin. The modern trading theory postulates a market impact structure underlying the price. That is, the asset price is affected by the trading volume. For ease of presentation, we adopt the linear price impact, i.e., the Almgren–Chriss model [35]:

$$P(t) = P(0) + \sigma B(t) - \eta(Z(t) - Z(0)), \tag{7.39}$$

where $\{B(t),\ t \ge 0\}$ is the standard Brownian motion, $\sigma > 0$ is the volatility, and $\eta > 0$ is the market impact parameter. Refer to [36, Chapter 3] for background, and [37–39] for other market impact models.

Recall that $b_k(t)$ is the (units of) risk-free asset that miner k holds at time t, and r is the risk-free rate. Here, all K miners and investors can trade coins on the exchange platform, whereas each miner can only exchange cash with an external source. For each miner k, the process of consumption $\{c_k(t),\ 0 \le t \le T\}$ evolves as

$$dc_k(t) = rb_k(t)dt - db_k(t) - P(t)\nu_k(t)dt - N'(t) L\left(\frac{\nu_k(t)}{N'(t)}\right) dt, \quad 0 \le t \le \mathscr{T}_k, \tag{C1}$$

where $L(\cdot)$ is an even function, increasing on $\mathbb{R}_+$, strictly convex and asymptotically super-linear. Compared to (C1) in Section 7.3, the additional term $-N'(t) L\left(\frac{\nu_k(t)}{N'(t)}\right)$ stands for the transaction cost which depends not only on the traded volume $\nu_k(t)dt$ but also the total volume $N'(t)dt$ (see [36, p. 43, (3.3)]). The quadratic cost $L(x) = \rho|x|^2$ with $\rho > 0$ corresponds to the original Almgren–Chriss model, which we will mostly stick to. We also impose the no shorting constraint:

$$b_k(0) = 0, \quad b_k(t) \ge 0 \text{ for } 0 \le t \le \mathscr{T}_k, \quad 0 \le X_k(t) \le N(t) \text{ for } 0 \le t \le \mathscr{T}_k. \tag{C2}$$

Set $b_k(t) = b_k(\mathscr{T}_k)$ and $\nu_k(t) = 0$ for $t > \mathscr{T}_k$.

Miner's strategy if $Z(\cdot)$ is known. It is easy to see from (7.39) that the price $P(t)$ (up to noise) only depends on the investor holdings $Z(t)$, or equivalently all the

miners' holdings $\sum_{k=1}^{K} X_k(t)$. Here, suppose that each miner k 'knows' the number of coins that the investors hold. As in (7.25), the objective of miner k is:

$$\sup_{\{(\nu_k(t),b_k(t))\}} J(\nu_k, b_k) := \mathbb{E}\Big\{ \int_0^{\mathscr{T}_k} e^{-\beta_k t}\,[dc_k(t) + \ell_k(X_k(t))dt] + e^{-\beta_k \mathscr{T}_k}\,[b_k(\mathscr{T}_k) + h_k(X_k(\mathscr{T}_k))] \Big\} \tag{7.40}$$

subject to (7.37), (7.39), (C1), *and* (C2).

Assuming that all the miners are *interchangeable* (which assumes a homogenous miner population), we drop the subscript 'k' in (7.40), and the objective of a *typical* miner is:

$$U(x) := \sup_{\{(\nu(t),b(t))\}} J(\nu, b) := \mathbb{E}\Big\{ \int_0^{\mathscr{T}} e^{-\beta t}\,[dc(t) + \ell(X(t))dt] + e^{-\beta \mathscr{T}}\,[b(\mathscr{T}) + h(X(\mathscr{T}))] \Big\} \tag{7.41}$$

$$\text{subject to} \quad X'(t) = \nu(t) + \frac{N'(t)}{N(t) - Z(t)} X(t),\ X(0) = x, \tag{C0}$$

$$dc(t) = rb(t)dt - db(t) - P(t)\nu(t)dt - N'(t)\,L\left(\frac{\nu(t)}{N'(t)}\right)dt, \tag{C1}$$

$$b(0) = 0,\ b(t) \geq 0 \text{ and } 0 \leq X(t) \leq N(t), \tag{C2}$$

$$P(t) = P(0) + \sigma B(t) - \eta(Z(t) - Z(0)), \tag{C3}$$

where (C0) is a repeat of the state dynamics in (7.37), and (C3) is the price dynamics in (7.39). Compared to (7.26), the volume constraint $|\nu(t)| \leq \overline{\nu}$ for $\overline{\nu} > 0$ is removed; instead the transaction cost $-N'(t)\,L\left(\frac{\nu(t)}{N'(t)}\right)dt$ is introduced in the budget constraint (C1). This way, the miner's strategy will no longer be a bang–bang control but depend on the specific market impact mechanism.

Let

$$\widetilde{P}_\beta(t) := e^{-\beta t}\mathbb{E}P(t) = e^{-\beta t}\,[P(0) - \eta(Z(t) - Z(0))] \quad \text{and} \quad \widetilde{P}(t) := \widetilde{P}_0(t). \tag{7.42}$$

The same argument as in (7.28) and (7.29) shows that the consumption–investment problem (7.41) is separable:

$$U(x) := \sup_{\{(\nu,b)\}} J(\nu, b) = \sup_b J_1(b) + \sup_\nu J_2(\nu),$$

where $J_1(b) := (r-\beta)\int_0^{\mathscr{T}} e^{-\beta t} b(t)dt$ and

$$J_2(\nu) := \int_0^{\mathscr{T}} \left[-\widetilde{P}_\beta(t)\nu(t) - e^{-\beta t} N'(t) L\left(\frac{\nu(t)}{N'(t)}\right) + e^{-\beta t}\ell(X(t)) \right] dt + e^{-\beta \mathscr{T}} h(X(\mathscr{T})).$$

Again suppose $\beta \geq r$. Then $\sup_b J_1(b) = 0$ with the optimality binding at $b_*(t) = 0$ for all t. So the problem (7.26) is reduced to

$$U(x) = \sup_\nu J_2(\nu) \quad \text{subject to} \quad \text{(C0), (C2')}, \tag{7.43}$$

where (C2') is (C2) without the constraints on $b(\,\cdot\,)$.

Next we argue by dynamic programming, and let

$$\begin{aligned} v(t,x) := \sup_{\{\nu(s), s\geq t\}} \int_t^{\mathscr{T}} & \left[-\widetilde{P}_\beta(s)\nu(s) - e^{-\beta s} N'(s) L\left(\frac{\nu(s)}{N'(s)}\right) + e^{-\beta s}\ell(X(s)) \right] dt \\ & + e^{-\beta \mathscr{T}} h(X(\mathscr{T})) \\ \text{subject to} \quad & X'(s) = \nu(s) + \frac{N'(s)}{N(s) - Z(s)} X(s),\ X(t) = x, \\ & 0 \leq X(s) \leq N(s), \end{aligned}$$

so $U(x) = v(0,x)$. Let $Q := \{(t,x) : 0 \leq t < T,\ 0 < x < N(t)\}$. Under some suitable conditions, v is the unique viscosity solution to the HJB equation:

$$\begin{cases} \partial_t v + e^{-\beta t}\ell(x) + \frac{xN'(t)}{N(t)}\partial_x v \\ \qquad\qquad + \sup_\nu \left\{ \nu(\partial_x v - \widetilde{P}_\beta(t)) - e^{-\beta t} N'(t) L\left(\frac{\nu}{N'(t)}\right) \right\} = 0 \quad \text{in } Q, \\ v(T,x) = e^{-\beta T} h(x), \\ v(t,0) = e^{-\beta t} h(0),\ v(t,N(t)) = e^{-\beta t} h(N(t)). \end{cases}$$

By optimizing $\nu \to \nu(\partial_x v - \widetilde{P}_\beta(t)) - e^{-\beta t} N'(t) L\left(\frac{\nu}{N'(t)}\right)$, we get

$$\nu_* = N'(t)(L')^{-1}\left(e^{\beta t}\partial_x v - \widetilde{P}(t)\right).$$

This yields the following nonlinear PDE:

$$\begin{cases} \partial_t v + e^{-\beta t}\ell(x) + \frac{xN'(t)}{N(t)-Z(t)}\partial_x v \\ \quad + e^{-\beta t} N'(t) \Big\{ (e^{\beta t}\partial_x v - \widetilde{P}(t))(L')^{-1}(e^{\beta t}\partial_x v - \widetilde{P}(t)) \\ \qquad\qquad - L\left((L')^{-1}(e^{\beta t}\partial_x v - \widetilde{P}(t))\right) \Big\} = 0 \quad \text{in } Q, \\ v(T,x) = e^{-\beta T} h(x), \\ v(t,0) = e^{-\beta t} h(0),\ v(t,N(t)) = e^{-\beta t} h(N(t)). \end{cases} \tag{7.44}$$

When $L(x) = \rho x^2$, the PDE (7.44) specialises to

$$\begin{cases} \partial_t v + e^{-\beta t}\ell(x) + \frac{xN'(t)}{N(t)-Z(t)}\partial_x v + \frac{e^{\beta t}N'(t)}{4\rho}(\partial_x v - \widetilde{P}_\beta(t))^2 = 0 \quad \text{in } Q, \\ v(T,x) = e^{-\beta T}h(x), \\ v(t,0) = e^{-\beta t}h(0),\ v(t,N(t)) = e^{-\beta t}h(N(t)), \end{cases} \tag{7.45}$$

with the optimal strategy $\nu_*(t,x) = \frac{N'(t)}{2\rho}\left(e^{\beta t}\partial_x v(t,x) - \widetilde{P}(t)\right)$. To simplify the presentation, we assume the quadratic cost (and (7.45)) from now on.

Mean field strategy. Assume that the distribution of the miners by their coin holdings is approximated by $m_0(x)dx$ at time $t = 0$. The goal is to find an equilibrium trading strategy $\nu^{\text{eq}}(t \mid m_0)$, or simply $\nu^{\text{eq}}(t)$, which can be viewed as the averaged trading strategy among all the miners.

Now let us describe the mean field model.

1. Since there are K miners, by (7.38), the investors' equilibrium holdings are:
$$Z^{\text{eq}}(t) = Z(0) - K\int_0^t \nu^{\text{eq}}(s)ds, \tag{7.46}$$
2. Given $Z^{\text{eq}}(\,\cdot\,)$, the miner's optimal strategy is
$$\nu_*^{\text{eq}}(t,x) = \frac{N'(t)}{2\rho}(e^{\beta t}\partial_x v(t,x) - \widetilde{P}(t)), \tag{7.47}$$
where v is the solution to (7.45) with $Z(t) = Z^{\text{eq}}(t)$.
3. The feedback control of a (typical) miner is $X'(t) = \nu_*^{\text{eq}}(t, X(t)) + \frac{N'(t)}{N(t)-Z^{\text{eq}}(t)}X(t)$. Hence, the density of the miners by their coin holdings solves the continuity equation:
$$\partial_t m + \partial_x\left(\left(\nu_*^{\text{eq}}(t,x) + \frac{xN'(t)}{N(t)-Z^{\text{eq}}(t)}\right)m\right) = 0, \quad m(0,x) = m_0(x). \tag{7.48}$$
4. The equilibrium trading strategy $\nu^{\text{eq}}(t)$ satisfies the fixed point equation:
$$\int \nu_*^{\text{eq}}(t,x)m(t,x)dx = \nu^{\text{eq}}(t). \tag{7.49}$$

If the mean field model (7.46)–(7.49) is well-posed (i.e., has a unique solution), then $m(t,\cdot)$ represents the wealth distribution of the whole miner population at time t. To illustrate, Figure 7.6 shows the wealth evolution of the miners with initial shares uniformly distributed on $x \in [20, 30]$. Observe that the wealth distribution spreads out and shifts to the left over the time, which implies decentralisation of the PoS protocol. While the PoS protocol alone does not lead to decentralisation, allowing trading in the PoS protocol yields decentralisation – this is a manifestation of the market power.

The problem now is to make rigorous such defined mean field model. By injecting (7.47) into (7.49), and then into (7.46), (7.45), and (7.48), we get the mean field game form:

$$\begin{cases} \partial_t v + H(t,x,\partial_x v, \partial_x v(\cdot,\cdot), m(\cdot,\cdot)) = 0, \\ \partial_t m + \partial_p H(t,x,\partial_x v, \partial_x v(\cdot,\cdot), m(\cdot,\cdot)) = 0 = 0, \\ m(t,0) = m_0(x),\ v(T,x) = e^{-\beta T}h(x), \end{cases} \tag{7.50}$$

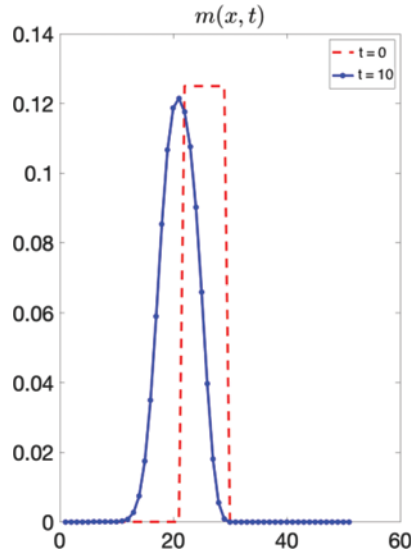


Figure 7.6 Wealth evolution of the whole miner population

with

$$H(t,x,p,Q,m) := e^{-\beta t}\ell(x) + + \frac{e^{\beta t}N'(t)}{4\rho}(p - \widetilde{P}_\beta(t))^2 + \frac{2\rho x N'(t)}{2\rho(N(t) - Z(0)) + K\int_0^t N'(s)\int (e^{\beta s}Q(s,x) - \widetilde{P}(s))m(s,x)dxds}p, \quad (7.51)$$

where

$$\widetilde{P}_\beta(t) = e^{-\beta t}\left[P(0) + \eta K\int_0^t \nu^{\text{eq}}(s)ds\right], \quad (7.52)$$

and $\nu^{\text{eq}}(\,\cdot\,)$ satisfies

$$\frac{N'(t)}{2\rho}\left[e^{\beta t}\int \partial_x v(t,x)m(t,x)dx - P(0) - \eta K\int_0^t \nu^{\text{eq}}(s)ds\right] = \nu^{\text{eq}}(t). \quad (7.53)$$

Combining (7.52) and (7.53), we have that $\widetilde{P}_\beta(t)$ (resp. $\widetilde{P}(t)$) is a function of Q and m (i.e., $\partial_x v(\cdot,\cdot)$ and $m(\cdot,\cdot)$).

The system of equations (7.50) is a first-order mean field game with *non-local* and *non-separable* Hamiltonian. It does not seem to have been studied before. One possible idea to prove the wellposedness of (7.50) is to (1) add viscosity terms ($\varepsilon\Delta v$, $\varepsilon\Delta m$) to the equations and study the corresponding second-order mean field games (see [40]); (2) pass to the limit $\varepsilon \to 0$ by vanishing viscosity (see [41,42]). The

analysis of the equations (7.50) may (probably) be very involved, and we leave it open.

7.5 Conclusion

This chapter presents and surveys recent progress on trading and wealth evolution in the PoS protocol under various settings (discrete, continuous, volume constraint, transaction cost, etc.) Below we provide a few open problems and future directions of research.

1. In Section 7.4, we present a mean field model to study the wealth distribution of the miners under the PoS protocol. This leads to a mean field game with non-local and non-separable Hamiltonian. Prove that (7.50) have a (unique) solution.
2. We have seen from Figure 7.6 that the mean field model yields decentralisation. Is it possible to prove a quantitative result to support this observation?
3. In Sections 7.2–7.4, we consider the optimal strategy of the miner assuming that $\delta_k(1 + r_{\text{free}}) \leq 1$ or $\beta \geq r$, i.e., risk-averse. What's the miner's optimal strategy if she is more risk-seeking (such that $\delta_k(1 + r_{\text{free}}) > 1$ or $\beta < r$)?
4. We assume a fixed miner population, i.e., K is fixed. In practice, some existing miners may quit, and some new miners may join at random times. What happens if there is a dynamic miner population (or K is varying over the time)?
5. We assume that the reward R_t is deterministic and is from the blockchain. But in many PoS blockchains (e.g., Ethereum), revenue for the miners comes mostly from the transaction fees. Thus, the 'reward' is from the user–miner interface (part (a)), and the users can also be the investors. What will be the miner's strategy, and the wealth evolution if we take the user–miner connection into account?
6. In Sections 7.2 and 7.4, we consider the wealth evolution of a homogenous population – that is, all the miners solve the same optimisation problem. What are the corresponding results for a heterogeneous miner population (e.g., with different risk sensitivity)?
7. We assume that the miners maximise some objective to find the best strategy. In practice, when people make decisions, they will adopt 'rational' strategy rather than the 'optimal' strategy. This leads to the idea of *bounded rationality* [43], which can be formulated in Bayesian languages. What is the miner's rational strategy?

Acknowledgements

We thank David Yao for collaborations which lead to a large part of the material presented in this chapter. We thank Erhan Bayraktar for pointing out the reference [40] on the mean field game with non-separable Hamiltonian. We also thank Siyao Jiang and Yuhang Wu for help in numerical experiments. This research is supported by

NSF Grants DMS-2113779 and DMS-2206038, and a start-up grant at Columbia University.

References

[1] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. *Decentralized Business Review*. 2008;21260.
[2] Wood G. Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*. 2014;151:1–32.
[3] McGhin T, Choo KKR, Liu CZ, *et al*. Blockchain in healthcare applications: research challenges and opportunities. *Journal of Network and Computer Applications*. 2019;135:62–75.
[4] Tanwar S, Parekh K, and Evans R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*. 2020;50:102407.
[5] Chod J, Trichakis N, Tsoukalas G, *et al*. On the financing benefits of supply chain transparency and blockchain adoption. *Management Science*. 2020;66(10):4378–4396.
[6] Saberi S, Kouhizadeh M, Sarkis J, *et al*. Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*. 2019;57(7):2117–2135.
[7] Dowling M. Is non-fungible token pricing driven by cryptocurrencies? *Finance Research Letters*. 2022;44:102097.
[8] Wang Q, Li R, Wang Q, *et al*. Non-fungible token (NFT): overview, evaluation, opportunities and challenges. 2021. ArXiv:2105.07447.
[9] Mccrank J and Nishant N. Fidelity readies new spot bitcoin ETF filing, report says. 2023. Available at https://www.reuters.com/technology/fidelity-preparing-submit-spot-bitcoin-etf-filing-block-2023-06-27/.
[10] King S and Nadal S. Ppcoin: peer-to-peer crypto-currency with proof-of-stake. 2012. Available at https://decred.org/research/king2012.pdf.
[11] Mora C, Rollins RL, Taladay K, *et al*. Bitcoin emissions alone could push global warming above 2 C. *Nature Climate Change*. 2018;8(11):931–933.
[12] Platt M, Sedlmeir J, Platt D, *et al*. The energy footprint of blockchain consensus mechanisms beyond proof-of-work. In: *IEEE 21st International Conference on Software Quality, Reliability and Security Companion (QRS-C)*; 2021. p. 1135–1144.
[13] Chiu J and Koeppl TV. The economics of cryptocurrency: Bitcoin and beyond. *Canadian Journal of Economics*. 2022;55(4):1762–1798.
[14] Cong LW, He Z, and Li J. Decentralized mining in centralized pools. *The Review of Financial Studies*. 2021;34(3):1191–1235.
[15] Saleh F. Volatility and welfare in a crypto economy. 2019;SSRN:3235467.
[16] Wickens K. 'The Merge' to end cryptocurrency mining on gaming GPUs won't come until 2022. 2021. Available at https://www.pcgamer.com/the-merge-to-end-cryptocurrency-mining-on-gaming-gpus-wont-come-until-2022.

[17] Brown-Cohen J, Narayanan A, Psomas A, *et al*. Formal barriers to longest-chain proof-of-stake protocols. In: *Proceedings of the 2019 ACM Conference on Economics and Computation*; 2019. p. 459–473.
[18] Chung H and Shi E. Foundations of transaction fee mechanism design. In: *Proceedings of the 2023 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. SIAM, Philadelphia, PA; 2023. p. 3856–3899.
[19] Tang W and Yao DD. Transaction fee mechanism for Proof-of-Stake protocol. 2023. ArXiv:2308.13881.
[20] Bagaria V, Dembo A, Kannan S, *et al*. Proof-of-stake longest chain protocols: security vs predictability. 2019. ArXiv:1910.02218.
[21] Daian P, Pass R, and Shi E. Snow white: robustly reconfigurable consensus and applications to provably secure proof of stake. In: *International Conference on Financial Cryptography and Data Security*; 2019. p. 23–41.
[22] Kiayias A, Russell A, David B, *et al*. Ouroboros: a provably secure proof-of-stake blockchain protocol. In: *Annual International Cryptology Conference*; 2017. p. 357–388.
[23] Saleh F. Blockchain without waste: proof-of-stake. *The Review of Financial Studies*. 2021;34(3):1156–1190.
[24] Pemantle R. A survey of random processes with reinforcement. *Probability Surveys*. 2007;4:1–79.
[25] Durrett R. *Probability—Theory and Examples*. Cambridge: Cambridge University Press; 2019.
[26] Roşu I and Saleh F. Evolution of shares in a proof-of-stake cryptocurrency. *Management Science*. 2021;67(2):661–672.
[27] Tang W. Stability of shares in the Proof of Stake protocol – concentration and phase transitions. 2022. ArXiv:2206.02227.
[28] Tang W and Yao DD. Polynomial voting rules. 2022. ArXiv:2206.10105.
[29] John K, Rivera TJ, and Saleh F. Equilibrium staking levels in a proof-of-stake blockchain. 2021. Available at SSRN 3965599.
[30] Buterin V. Toward a 12-Second Block Time. 2014. Available at https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time.
[31] Tang W and Yao DD. Trading under the Proof-of-Stake Protocol—a continuous-time control approach. *Mathematical Finance*. 2023. Available at https://onlinelibrary.wiley.com/doi/10.1111/mafi.12403. arXiv:2207.12581.
[32] Bertucci C, Bertucci L, Lasry JM, *et al*. Mean field game approach to Bitcoin mining. 2020. ArXiv:2004.08167.
[33] Li Z, Reppen AM, and Sircar R. A mean field games model for cryptocurrency mining. 2019. ArXiv:1912.01952.
[34] Prat J and Walter B. An equilibrium model of the market for Bitcoin mining. *Journal of Political Economy*. 2021;129(8):2415–2452.
[35] Almgren R and Chriss N. Optimal execution of portfolio transactions. *Journal of Risk*. 2001;3:5–40.
[36] Guéant O. The financial mathematics of market liquidity. *Chapman & Hall/CRC Financial Mathematics Series*. London: CRC Press; 2016. From optimal execution to market making.

[37] Donier J and Bonart J. A million metaorder analysis of market impact on the Bitcoin. *Market Microstructure and Liquidity*. 2015;1(02):1550008.
[38] Gatheral J and Schied A. Optimal trade execution under geometric Brownian motion in the Almgren and Chriss framework. *International Journal of Theoretical and Applied Finance*. 2011;14(3):353–368.
[39] Tóth B, Lemperiere Y, Deremble C, *et al*. Anomalous price impact and the critical nature of liquidity in financial markets. *Physical Review X*. 2011;1(2):021006.
[40] Ambrose DM. Existence theory for non-separable mean field games in Sobolev spaces. *Indiana University Mathematics Journal*. 2022;71(2):611–647.
[41] Cardaliaguet P, and Graber PJ. Mean field games systems of first order. *ESAIM Control, Optimisation and Calculus of Variations*. 2015;21(3):690–722.
[42] Tang W and Zhang YP. The convergence rate of vanishing viscosity approximations for mean field games. 2023. ArXiv:2303.14560.
[43] Simon HA. Bounded rationality. In: *Utility and Probability*, Palgrave Macmillan: London; 1990. p. 15–18.