ORIGINAL ARTICLE

Trading under the proof-of-stake protocol – A continuous-time control approach

Wenpin Tang | David D. Yao

Department of Industrial Engineering and Operations Research, Columbia University, New York, USA

Correspondence
Wenpin Tang, Department of Industrial Engineering and Operations Research, Columbia University.
Email: wt2319@columbia.edu

Abstract

We develop a continuous-time control approach to optimal trading in a Proof-of-Stake (PoS) blockchain, formulated as a consumption-investment problem that aims to strike the optimal balance between a participant's (or agent's) utility from holding/trading stakes and utility from consumption. We present solutions via dynamic programming and the Hamilton–Jacobi–Bellman (HJB) equations. When the utility functions are linear or convex, we derive close-form solutions and show that the bang-bang strategy is optimal (i.e., always buy or sell at full capacity). Furthermore, we bring out the explicit connection between the rate of return in trading/holding stakes and the participant's risk-adjusted valuation of the stakes. In particular, we show when a participant is risk-neutral or risk-seeking, corresponding to the risk-adjusted valuation being a martingale or a sub-martingale, the optimal strategy must be to either buy all the time, sell all the time, or first buy then sell, and with both buying and selling executed at full capacity. We also propose a risk-control version of the consumption-investment problem; and for a special case, the "stake-parity" problem, we show a mean-reverting strategy is optimal.

KEYWORDS
consumption-investment, cryptocurrency, continuous-time control, dynamic programming, HJB equations, Proof of Stake (PoS) protocol, risk control

1 | INTRODUCTION

As a digital exchange vehicle, blockchain technology has been successfully deployed in many applications including cryptocurrency Nakamoto (2008), healthcare Donovan (2019), supply chain Chod et al. (2020), electoral voting Wood (2018), and non-fungible tokens Wang et al. (2021). A blockchain is a growing chain of accounting records, called blocks, which are jointly maintained by participants of the system using cryptography. Consider for instance Bitcoin – a peer-to-peer decentralized payment system. In contrast to traditional payment processing networks, Bitcoin provides a permissionless environment in which everyone is free to participate. At the core of Bitcoin is the consensus protocol known as *Proof of Work* (PoW), in which "miners" compete with each other by solving a hashing puzzle so as to validate an ever-growing log of transactions (the "longest chain") to update a distributed ledger; and the miner who solves the puzzle first receives a reward (a number of coins). Thus, while the competition is open to all participants, the chance of winning is proportional to a miner's computing power.

Despite its popularity, the PoW protocol has some obvious drawbacks. Competition among miners has led to exploding levels of energy consumption in Bitcoin mining, (Mora et al., 2018; Platt et al., 2021). Alsabah and Capponi (2020); Arnosti and Weinberg (2022); Chiu and Koeppl (2017) pointed out that PoW mining will lead to centralization, violating the core tenet of decentralization. To solve the problem of energy efficiency, King and Nadal (2012); Wood (2014) introduced another consensus protocol – *Proof of Stake* (PoS), which is a bidding mechanism to select a miner to validate the new block. Participants who choose to join the bidding process are required to commit certain stakes (coins they own), and the winning probability is proportional to the stakes committed. Hence, a participant in a PoS blockchain is a "bidder", and only the winning bidder becomes the miner who does the validation. As yet the PoS protocol has not been as popular as PoW. However, it is catching up quickly, and blockchain developers have strong incentives to switch from a PoW to a PoS ecosystem. A prominent case in this direction is Ethereum 2.0, where two parallel chains – *Mainnet* (PoW) and *Beacon Chain* (PoS) are expected soon to merge into one unified PoS blockchain Duggan and Powell (2022).

There has been an active stream of recent studies on PoS in the research literature; and here we briefly mention several that relate closely to our study. In Saleh (2021) it is shown that the PoS protocol is "without waste" from an economic standpoint. Issues of stability and decentralization of the PoS protocol are examined in Roşu and Saleh (2021); Tang (2022). Specifically, it is shown in Roşu and Saleh (2021) that for large owners of initial wealth in a PoS system their shares of the total wealth will remain stable in the long run (i.e., proportions to the total wealth will remain constant), and hence the rich-get-richer phenomenon will not happen. Tang (2022) further extends this to medium and small participants, and reveals a phase transition in share stability among those different types of participants. In Roşu and Saleh (2021); Tang and Yao (2022), various aspects of the consumption-investment problem in PoS are examined, and certain conditions are identified under which a participant may have no incentive to trade with others. This leads to the complementing question, given a participant does prefer to trade, what is the optimal trading strategy?

Motivated by the above question, the objective of our study here is to develop a continuous-time control approach to optimal trading in a PoS blockchain. While the control (or game) approach has been proposed in previous studies Bertucci et al. (2020, 2022); Li et al. (2019), they are all for the PoW protocol. To the best of our knowledge, ours is the first control model developed for optimal trading under the PoS protocol.

Here is an overview of our main results. We first formulate the *consumption-investment problem*, which aims to strike a balance between a participant's utility from holding/trading stakes and utility from consumption. It takes the form of a deterministic control problem with the real-time trading strategy being the control variable. We start with a detailed analysis on a special case that we call the "stake-hoarding" problem (Proposition 3.1), where we bring out the possible scenario of monopoly. We then solve the general consumption-investment problem via dynamic programming and the Hamilton–Jacobi–Bellman (HJB) equations (Theorem 3.4).

When the utility functions are linear or convex, more explicit solutions can be obtained, and we show that the bang–bang control is optimal, that is, always buy or sell at full capacity (Propositions 4.1 and 4.3). Along with the optimal trading strategy, we are also able to bring out the explicit connection between the rate of return in trading/holding stakes and the participant's risk-adjusted valuation of the stakes. In other words, the participant's risk sensitivity is explicitly accounted for in the trading strategy. In particular, when a participant is risk-neutral or risk-seeking, corresponding to the risk-adjusted valuation being a martingale or a sub-martingale, the optimal strategy must be either buy all the time, sell all the time, or first buy then sell (with both buying and selling executed at full capacity).

Finally, we propose a risk control version of the consumption-investment problem, by adding a penalty term to control the level of stake holding so as to reduce the level of concentration risk (Theorem 5.1). A special case is a "stake-parity" problem, where the participant's holding is controlled at a level that tries to track the system-wide average. We show that the "mean-reverting" strategy is the optimal solution to the stake-parity problem (Proposition 5.2).

The rest of the paper is organized as follows. Section 2 details the formulation of the consumption-investment problem under the PoS protocol. Section 3 presents the optimal solution to the problem, and Section 4 focuses on the special case of linear and convex utility functions. Section 5 presents extensions to risk-control objectives. Concluding remarks are summarized in Section 6.

2 | MODEL FORMULATION

This section introduces the problem of trading under the PoS protocol in continuous time, and formulate a control model to solve the problem. First, collected below are some conventions that will be used throughout this paper.

- $\mathbb{R}$ denotes the set of real numbers, and $\mathbb{R}_+$ denotes the set of nonnegative real numbers.
- For $x, y \in \mathbb{R}$, $x \wedge y$ denotes the smaller number of x and y; $x \vee y$ denotes the larger number of x and y.
- The symbol $x = o(y)$ means $\frac{x}{y}$ decays towards zero as $y \to \infty$.
- For a random variable X, $\mathbb{E}(X)$ denotes the expectation of X.
- Let Ω be a subset of $\mathbb{R}$. A function $f \in C^k(\Omega)$ if it is k-time continuously differentiable in Ω.
- For $f \in C^1([0, T])$, $f'(t)$ denotes the derivative of f. For $f \in C^1([0, T] \times \Omega)$, $\partial_t f$ (resp. $\partial_x f$) denotes the partial derivative of f with respect to t (resp. x).

Time is continuous, indexed by $t \in [0, T]$, for a fixed $T > 0$ representing the length of a finite horizon. Let $\{N(t), 0 \le t \le T\}$ (with $N(0) := N$) denote the process of the total volume of stakes, which are issued over time by the PoS protocol, and can be either deterministic or stochastic. For

ease of presentation, we consider a deterministic process $N(t)$, which is increasing in time and sufficiently smooth, with the derivative $N'(t)$ representing the instantaneous rate of "reward" – additional stakes (or "coins") injected into the system specified (exogenously) by the PoS protocol. For instance, we will consider below, as a special case, the process $N(t)$ of a polynomial form:

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

Then, $N'_\alpha(t) = \alpha(N^{\frac{1}{\alpha}} + t)^{\alpha-1}$, and $N''_\alpha(t) = \alpha(\alpha - 1)(N^{\frac{1}{\alpha}} + t)^{\alpha-2}$, so the parametric family (1) covers different rewarding schemes according to the values of α.

- For $0 < \alpha < 1$, we have $N''_\alpha(t) < 0$ so the process $N_\alpha(t)$ corresponds to a decreasing reward (e.g., Bitcoin);
- For $\alpha = 1$, the process $N_1(t) = N + t$ gives a rate one constant reward (e.g., Blackcoin);
- For $\alpha > 1$, we get $N''_\alpha(t) > 0$ and hence, the process $N_\alpha(t)$ amounts to an increasing reward (e.g., EOS).

Let $K \geq 2$ denote the total number of participants in the system, who are indexed by $k \in [K] := \{1, \dots, K\}$. For each participant k, let $\{X_k(t), 0 \leq t \leq T\}$ (with $X_k(0) = x_k$) denote the process of the number of stakes that participant k holds, with $X_k(t) \geq 0$ and $\sum_{k=1}^K X_k(t) = N(t)$ for all $t \in [0, T]$. In the (discrete-time) PoS protocol, in each round of the bidding process, individual participants commit stakes so as to be selected to validate the block and receive a reward; and the winning probability is $X_k(t)/N(t)$ for participant k, that is, proportional to the number of stakes committed. (For instance, each round in Ethereum takes about 10 s, corresponding to the block-generation time Buterin (2014).) 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 bidding during any given time interval $[t, t + \Delta t]$. In each round participant k gets either some stake(s) or nothing; so the average total number of stakes k will get over the M rounds is (by law of large numbers when M is large),

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

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

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

$$X'_k(t) = \nu_k(t) + \frac{N'(t)}{N(t)} X_k(t) \quad \text{for } 0 \leq t \leq \tau_k \wedge T := \mathcal{T}_k, \tag{2}$$

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 participant runs out of stakes, or gets all available stakes:

- If $\mathcal{T}_k = \tau_k$, then participant k liquidates all his stakes by time τ_k, and $X_k(\mathcal{T}_k) = 0$;
- If $\mathcal{T}_k = \max_{j \neq k} \tau_j$, then participant k gets all issued stakes by time $\max_{j \neq k} \tau_j$, and hence $X_k(\mathcal{T}_k) = N(\mathcal{T}_k)$.

We set $X_k(t) = X_k(\mathcal{T}_k)$ for $t > \mathcal{T}_k$.

The problem is for each participant k to decide how to trade stakes with others under the PoS protocol. Let $\{P(t), 0 \leq t \leq T\}$ be the price process of each (unit of) stake, which is a stochastic process assumed to be independent of the dynamics in (2). (This assumption has appeared in recent studies (e.g., Roşu and Saleh (2021)), and is somehow a reflection of the reality that the crypto price tends to be affected by market shocks such as macroeconomics, geopolitics, breaking news, and so on much more than by trading activities.) Here, the price $P(t)$ of each stake is measured in terms of an underlying risk-free asset (referred to as "cash" for simplicity); and let $b_k(t)$ denote the (units of) risk-free asset that participant k holds at time t, and let $r > 0$ denote the risk-free (interest) rate. Also note that all K participants are allowed to trade stakes (with cash) only internally among themselves, whereas each participants can only exchange cash with an external source (say, a bank).

The decision for each participant k at t is hence a tuple $(\nu_k(t), b_k(t))$. Let $\{c_k(t), 0 \leq t \leq T\}$ be the process of consumption, or cash flow of participant k, which follows the dynamics below:

$$dc_k(t) = rb_k(t)dt - db_k(t) - P(t)\nu_k(t)dt, \qquad 0 \leq t \leq \mathcal{T}_k; \qquad (C1)$$

with

$$b_k(0) = 0, \quad b_k(t) \geq 0 \text{ for } 0 \leq t \leq \mathcal{T}_k, \quad 0 \leq X_k(t) \leq N(t) \text{ for } 0 \leq t \leq \mathcal{T}_k. \qquad (C2)$$

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

In (C1), if $db_k(t) < 0$, the participant sells the risk-free asset to get cash either for buying stakes, or for consumption; if $db_k(t) > 0$, the participant adds more risk-free asset. Thus, (C1) is a self-financing condition in which $rb_k(t)dt - db_k(t)$ is the net change (in value of the risk-free asset held) used to finance new stakes $P(t)\nu_k(t)dt$ and consumption $dc(t)$. The requirements in (C2) are all in the spirit of disallowing shorting on either the risk free asset $b_k(t)$ or the stakes $X_k(t)$. In some PoS blockchains, there is a minimum requirement for bidding (e.g., 32 ETHs for Ethereum). In this case, we can impose a lower bound on the process $X_k(t)$, to prevent it from falling below this threshold. The analysis will be similar. We also require that the trading strategy be bounded: there is $\bar{\nu}_k > 0$ such that

$$|\nu_k(t)| \leq \bar{\nu}_k. \qquad (C3)$$

The objective of participant k is:

$$\sup_{\{(\nu_k(t), b_k(t))\}} J(\nu_k, b_k) := \mathbb{E}\left\{ \int_0^{\mathcal{T}_k} e^{-\beta_k t}[dc_k(t) + \ell_k(X_k(t))dt] + e^{-\beta_k \mathcal{T}_k}[b_k(\mathcal{T}_k) + h_k(X_k(\mathcal{T}_k))] \right\} \qquad (3)$$

subject to (2), (C1), (C2), (C3),

where $\beta_k > 0$ is a discount factor, a parameter measuring the risk sensitivity of participant k; $\ell_k(\cdot)$ 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 as presented above takes into account some distinct features of PoS blockchains and cryptocurrencies. One notable point is, the utilities ℓ and h in the objective are expressed as functions of the number of stakes $X_k(t)$, as opposed to their total value $P(t)X_k(t)$. To the extent that $P(t)$ is treated as exogenous (as explained above), 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 stakes from their monetary value at any given time. For instance, holding 1 ETH may be equivalent to \$5,000 for one person, and \$500 for another, and neither will be influenced by the ETH market price at the time, which could be say, about \$1,500.

Throughout below, the following conditions will be assumed:

Assumption 2.1.

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

3 | THE CONSUMPTION-INVESTMENT PROBLEM

Here we study the consumption-investment problem for participant k in (3). To lighten notation, omit the subscript k, and write out the problem in full as follows, where (C0) is a repeat of the state dynamics in (2):

$$U(x) := \sup_{\{(\nu(t), b(t))\}} J(\nu, b) := \mathbb{E}\left\{ \int_0^{\mathcal{T}} e^{-\beta t}[dc(t) + \ell(X(t))dt] + e^{-\beta \mathcal{T}}[b(\mathcal{T}) + h(X(\mathcal{T}))] \right\} \quad (4)$$

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

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

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

$$|\nu(t)| \leq \bar{\nu}. \quad (\text{C3})$$

where $\mathcal{T} := \inf\{t > 0 : X(t) = 0 \text{ or } N(t)\} \wedge T$.

Note that the expectation in the objective function is with respect to $P(t)$, which is involved in $dc_k(t)$ via (C1). Denote

$$\widetilde{P}_\beta(t) := e^{-\beta t}\mathbb{E}P(t), \qquad t \in [0, T]. \quad (5)$$

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 (5), we have

$$J(v, b) = -\int_0^{\mathcal{T}} e^{(r-\beta)t} d(e^{-rt} b(t)) + e^{-\beta \mathcal{T}} b(\mathcal{T})$$

$$+ \underbrace{\int_0^{\mathcal{T}} \left[-\widetilde{P}_\beta(t) v(t) + e^{-\beta t} \ell(X(t)) \right] dt + e^{-\beta \mathcal{T}} h(X(\mathcal{T}))}_{J_2(v)}$$

$$= \underbrace{(r - \beta) \int_0^{\mathcal{T}} e^{-\beta t} b(t) dt}_{:=J_1(b)} + J_2(v), \tag{6}$$

where $b(0) = 0$ is used in the last equality. Hence,

$$U(x) := \sup_{\{(v,b)\}} J(v, b) = \sup_b J_1(b) + \sup_v J_2(v). \tag{7}$$

Next, suppose $\beta \geq r$, a condition that will be assumed below (and readily justified as the risk premium associated with the valuation of any stake over the risk-free asset). Then, from the $J_1(b)$ expression in (6), 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. Consequently, the problem in (4) is reduced to

$$U(x) = \sup_v J_2(v) \quad \text{subject to (C0), (C2'), (C3)}, \tag{8}$$

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

In summary, the key fact here is that the objective $U(x)$ is separable in the control variables $(v(t), b(t))$; hence the problem in (4) is decomposed into two optimal control problems, one on the risk-free asset $b(t)$, and the other on the trading of stakes $v(t)$, as specified in (6) and (7). Moreover, under the condition $\beta \geq r$, the consumption-investment problem is reduced to the one in (8), where the objective function $J_2(v)$ – refer to (6) – takes the form of a tradeoff between the utility from holding stakes ($\ell(X(t))$ and $h(X(\mathcal{T}))$) and the dis-utility of reducing consumption ($-\widetilde{P}_\beta(t)v(t)$). Thus, the optimal trading strategy needs to strike a balance between these two opposing terms.

Before we present the optimal solution to the consumption-investment problem in (8), we make a digression to first study a simple degenerate case of $\widetilde{P}_\beta(t) \equiv 0$. This special case removes the tradeoff mentioned above, so the solution becomes a one-sided strategy of always accumulating (or "hoarding") the stakes at full capacity ($\overline{v}$). Yet, as the analysis below will show, there are still some interesting (and subtle) issues involved. More importantly, this special case provides a very accessible path to finding the optimal solution via dynamic programming and the HJB equation.

3.1 | Stake-hoarding

As motivated above, here the problem for participant k is reduced to the following (again, omit the subscript k):

$$U(x) := \sup_{\nu(t)} \int_0^{\mathcal{T}} e^{-\beta t} \ell(X(t))dt + e^{-\beta \mathcal{T}} h(X(\mathcal{T})) \tag{9}$$

$$\text{subject to} \quad (C0), (C2'), (C3).$$

Below, we denote $\nu_*(t)$ for the optimal control process, $X_*(t)$ for the corresponding state process, and $\mathcal{T}_* := \inf\{t > 0 : X_*(t) = N(t)\} \wedge T$ for the exit time.

Proposition 3.1. *Denote*

$$\gamma(t) := \bar{\nu} N(t) \int_0^t \frac{ds}{N(s)} + \frac{xN(t)}{N} \quad \text{for } 0 \le t \le T. \tag{10}$$

We have:

(i) *If* $\bar{\nu} \int_0^T \frac{dt}{N(t)} \le \frac{N-x}{N}$, *then* $\mathcal{T}_* = T$. *The optimal control is* $\nu_*(t) = \bar{\nu}$ *for* $0 \le t \le T$, *the optimal state process is* $X_*(t) = \gamma(t)$ *for* $0 \le t \le T$, *and* $U(x) = e^{-\beta T} h(X_*(T)) + \int_0^T e^{-\beta t} \ell(X_*(t))dt$.

(ii) *If* $\bar{\nu} \int_0^T \frac{dt}{N(t)} > \frac{N-x}{N}$, *set*

$$t_0 := \inf \left\{ t > 0 : \bar{\nu} \int_0^t \frac{ds}{N(s)} = \frac{N-x}{N} \right\} < T.$$

Assume further that

$$h(N(t))' + \ell(N(t)) \le \beta h(N(t)) \quad \text{for all } 0 \le t \le T. \tag{11}$$

Then, $\mathcal{T}_* = t_0$. *The optimal strategy is* $\nu_*(t) = \bar{\nu}$ *for* $0 \le t \le t_0$ *(and* $\nu_*(t) = 0$ *for* $t > t_0$*), the optimal state process is* $X_*(t) = \gamma(t)$ *for* $0 \le t \le t_0$ *(and* $X_*(t) = N(t_0)$ *for* $t > t_0$*), and* $U(x) = e^{-\beta t_0} h(X_*(t_0)) + \int_0^{t_0} e^{-\beta t} \ell(X_*(t))dt$.

Deferring the proof, we first make a few comments on the above proposition. Note that $\gamma(t)$ as specified in (10) is identified as the optimal state process $X_*(t)$, which is the number of stakes given $\nu_*(t) = \bar{\nu}$. It is easy to see that the participant's share of stakes, $X_*(t)/N(t)$, is increasing in t, leading to centralization regardless of how the rewarding scheme is designed (although large rewards may slow down the speed towards concentration). The interesting point of the above theorem is in its part (ii), where the required condition (11) is a technical one, to ensure the optimality of $\nu_*(t) = \bar{\nu}$. The more substantive fact is $\mathcal{T}_* = t_0 < T$, when $X(\mathcal{T}_*) = N(\mathcal{T}_*)$, i.e., the participant has accumulated all stakes available in the system, leading to the extreme situation of monopoly (or "dictatorship"); and this is done before the end of the horizon, ithat is, forcing a pre-matured exit time. See Figure 1 for an illustration.

The following corollary illustrates further this extreme phenomenon, with the polynomial family $N_\alpha(t)$ defined by (1), and with a long time horizon ($T \to \infty$).

FIGURE 1 Optimal stake trading: concentration and monopoly. [Color figure can be viewed at wileyonlinelibrary.com]
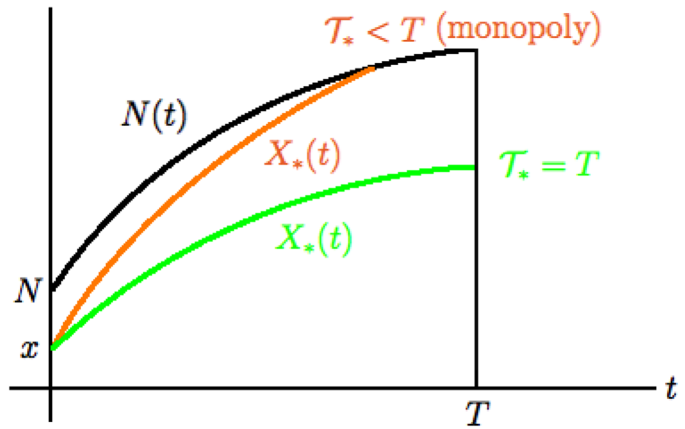
Corollary 3.2. *Let $(N_\alpha(t), 0 \le t \le T)$ be defined by (1), $(X_{\alpha,*}(t), 0 \le t \le T)$ be the optimal state process defined by (10) corresponding to $N_\alpha(t)$, and $\mathcal{T}_{\alpha,*} := \inf\{t > 0 : X_{\alpha,*}(t) = N_\alpha(t)\}$ be the exit time. Assume that the condition (11) holds for $N_\alpha(t)$. Then, as $T \to \infty$, we have*

(i) *For $\alpha > 1$,*
- *if $\bar{\nu} \le (\alpha - 1)(N - x)N^{-\frac{1}{\alpha}}$, then $X_{\alpha,*}(t) < N_\alpha(t)$ for all t. Moreover,*

$$\lim_{t \to \infty} \frac{X_{\alpha,*}(t)}{N_\alpha(t)} = \frac{\bar{\nu}}{\alpha - 1} N^{\frac{1-\alpha}{\alpha}} + \frac{x}{N}. \tag{12}$$

- *if $\bar{\nu} > (\alpha - 1)(N - x)N^{-\frac{1}{\alpha}}$, then $\mathcal{T}_{\alpha,*} < \infty$.*

(ii) *For $\alpha \le 1$, we have $\mathcal{T}_{\alpha,*} < \infty$.*

Proof. Note that

$$\int_0^T \frac{dt}{N_\alpha(t)} = \begin{cases} \frac{1}{1-\alpha}\left((T + N^{\frac{1}{\alpha}})^{1-\alpha} - N^{\frac{1-\alpha}{\alpha}}\right) & \text{for } \alpha \ne 1 \\ \log(1 + T/N) & \text{for } \alpha = 1. \end{cases} \tag{13}$$

As $T \to \infty$, the dominant term in $\frac{1}{1-\alpha}((T + N^{\frac{1}{\alpha}})^{1-\alpha} - N^{\frac{1-\alpha}{\alpha}})$ is $\frac{1}{\alpha-1}N^{\frac{1-\alpha}{\alpha}}$ if $\alpha > 1$, and is $\frac{1}{1-\alpha}T^{1-\alpha}$ if $\alpha < 1$; and the dominant term in $\log(1 + T/N)$ is $\log T$. It then suffices to compare $\bar{\nu} \int_0^T \frac{dt}{N_\alpha(t)}$ to $\frac{N-x}{N}$, and the rest of the corollary is immediate. $\square$

This corollary shows a sharp phase transition towards monopoly in terms of the rewarding schemes. For $\alpha > 1$ (increasing reward), there is a threshold for $\bar{\nu}$, only above which monopoly may occur, and below which the share of stakes increases towards the value on the right side of (12). For $\alpha \le 1$ (constant or decreasing reward), monopoly always occurs. Thus, these results have practical implications in the design of the PoS protocol. For instance, if/when certain participants have large capacities, adopting a suitable increasing reward scheme will counter the effect of concentration.

Now, returning to the proof of Proposition 3.1, we use the standard machinery of dynamic programming and the HJB equation. Consider the following problem, where $V(t, x)$ is the "value-to-go" function, for $0 \le t \le T$ and $0 \le x \le N(t)$:

$$V(t, x) := \max_{\{\nu(s), s \ge t\}} \int_t^{\mathcal{T}} e^{-\beta s} \ell(X(s)) ds + e^{-\beta \mathcal{T}} h(X(\mathcal{T}))$$

$$\text{subject to } X'(s) = \nu(s) + \frac{N'(s)}{N(s)} X(s), \ X(t) = x,$$

$$0 \le X(s) \le N(s),$$

$$|\nu(s)| \le \bar{\nu}.$$

Clearly, the solution to the above problem concerning $V(t, x)$, for all $t \in [0, T]$ and $x \in [0, N(t)]$, will yield the desired solution to $U(x)$ in (9), since $U(x) = V(0, x)$. The following lemma identifies an HJB equation (with terminal and boundary conditions), to which. $V(t, x)$ is a solution.

Lemma 3.3. *Let $Q := \{(t, x) : 0 \le t < T, 0 < x < N(t)\}$. Then V is the (unique) viscosity solution to the following HJB equation:*

$$\begin{cases} \partial_t v + e^{-\beta t} \ell(x) + \frac{x N'(t)}{N(t)} \partial_x v + \sup_{|\nu| \le \bar{\nu}} \{\nu \, \partial_x v\} = 0 & (t, x) \in Q, \\ v(T, x) = e^{-\beta T} h(x), \\ v(t, 0) = e^{-\beta t} h(0), \ v(t, N(t)) = e^{-\beta t} h(N(t)). \end{cases} \tag{14}$$

Proof. Write the HJB equation as $\partial_t v + H(t, x, \partial_x v) = 0$, where

$$H(t, x, p) := e^{-\beta t} \ell(x) + \frac{x N'(t)}{N(t)} p + \sup_{|\nu| \le \bar{\nu}} \{\nu p\}.$$

The fact that V as specified in (14) is a viscosity solution follows a standard dynamic programming argument, see (Fleming and Soner, 2006, Chapter II, Section 7).

Moreover, from the conditions in Assumption 2.1, we have,

$$|H(t, x, p) - H(s, y, q)| \le C(|t - s| + |x - y| + |p - q| + |x - y||p| + |t - s||p|), \tag{15}$$

for $0 \le s, t \le T$ and $0 \le x, y \le N(t)$, and for some $C > 0$. By (Fleming and Soner, 2006, Chapter II, Corollary 9.1), the HJB equation in (14) has a unique viscosity solution, which then must be none other than V. □

What remains is to pin down the term $\sup_{|\nu| \le \bar{\nu}} \{\nu \, \partial_x v\}$ in the HJB equation, that is, to identify the maximizing ν. Given the intuitive solution that $\nu = \bar{\nu} > 0$ (a "conjecture," so far), the HJB equation in 14 is expected to be

$$\begin{cases} \partial_t v + e^{-\beta t} \ell(x) + \left(\bar{\nu} + \frac{x N'(t)}{N(t)} \right) \partial_x v = 0 \text{ in } Q, \\ v(T, x) = e^{-\beta T} h(x), \\ v(t, 0) = e^{-\beta t} h(0), \ v(t, N(t)) = e^{-\beta t} h(N(t)), \end{cases} \tag{16}$$

which is a transport equation with variable coefficients. Now we solve the transport equation (16) by the method of characteristics. For $0 \leq t \leq T$ and $0 \leq x \leq N(t)$, let $\gamma_{t,x}(s)$ be the solution to the following equation:

$$\gamma'_{t,x}(s) = \bar{\nu} + \frac{N'(s)}{N(s)}\gamma_{t,x}(s), \quad s > t; \qquad \gamma_{t,x}(t) = x. \tag{17}$$

A direct computation yields

$$\gamma_{t,x}(s) = \bar{\nu}N(s)\int_t^s \frac{du}{N(u)} + \frac{xN(s)}{N(t)}, \quad s \geq t. \tag{18}$$

Under the regularity conditions in Assumption 2.1, it is standard that (see, e.g., Ambrosio (2008); Golse (2013))

$$v(t,x) = e^{-\beta \mathcal{T}_{t,x}}h(\gamma_{t,x}(\mathcal{T}_{t,x})) + \int_t^{\mathcal{T}_{t,x}} e^{-\beta s}\ell(\gamma_{t,x}(s))ds, \tag{19}$$

where $\mathcal{T}_{t,x} := \inf\{s > t : \gamma_{t,x}(s) = N(s)\} \wedge T$. We will next show that $v(t,x)$ given by (19) indeed solves the HJB equation (14), which then proves Proposition 3.1.

Proof of Proposition 3.1. From the expression of $\gamma_{t,x}(s)$ in (18), we have

$$\partial_x\gamma_{t,x}(s) = \frac{N(s)}{N(t)} > 0 \quad \text{and} \quad \partial_x\mathcal{T}_{t,x} \leq 0. \tag{20}$$

Note that $\gamma_{t,x}(s)/N(s)$ is increasing in s. There are two cases.

Case 1: If $\gamma_{t,x}(T)/N(T) \leq 1$, then $\mathcal{T}_{t,x} = T$ and hence, $v(t,x) = e^{-\beta T}h(\gamma_{t,x}(T)) + \int_t^T e^{-\beta s}\ell(\gamma_{t,x}(s))ds$. By the regularity conditions in Assumption 2.1, we get

$$\partial_x v = e^{-\beta T}\frac{N(T)}{N(t)}h'(\gamma_{t,x}(T)) + \int_t^T e^{-\beta s}\frac{N(s)}{N(t)}\ell'(\gamma_{t,x}(s))ds \geq 0,$$

where the non-negativity follows from the fact that $N(t) > 0$ and ℓ, h are increasing.

Case 2: If $\gamma_{t,x}(T)/N(T) > 1$, then $\mathcal{T}_{t,x} < T$, and hence $v(t,x) = e^{-\beta \mathcal{T}_{t,x}}h(N(\mathcal{T}_{t,x})) + \int_t^{\mathcal{T}_{t,x}} e^{-\beta s}\ell(\gamma_{t,x}(s))ds$. As a result,

$$\partial_x v = -\beta e^{-\beta \mathcal{T}_{t,x}}(\partial_x\mathcal{T}_{t,x})h(N(\mathcal{T}_{t,x})) + e^{-\beta \mathcal{T}_{t,x}}(\partial_x\mathcal{T}_{t,x})(h\circ N)'(\mathcal{T}_{t,x})$$

$$+ \int_t^{\mathcal{T}_{t,x}} e^{-\beta s}\frac{N(s)}{N(t)}\ell'(\gamma_{t,x}(s))ds + e^{-\beta \mathcal{T}_{t,x}}(\partial_x\mathcal{T}_{t,x})\ell(N(\mathcal{T}_{t,x}))$$

$$= \int_t^{\mathcal{T}_{t,x}} e^{-\beta s}\frac{N(s)}{N(t)}\ell'(\gamma_{t,x}(s))ds$$

$$- e^{-\beta \mathcal{T}_{t,x}}\underbrace{(\partial_x\mathcal{T}_{t,x})}_{\leq 0 \text{ by } (20)}\underbrace{(-\ell\circ N - (h\circ N)' + \beta h\circ N)}_{\geq 0 \text{ by } (11)}(\mathcal{T}_{t,x})$$

$$\geq 0.$$

So, in both cases, we have $\partial_x v(t, x) \geq 0$. Thus, $v(t, x)$ defined by (19) is a classical solution and hence, a viscosity solution to the HJB equation in (14). By Lemma 3.3, we conclude $V(t, x) = v(t, x)$, and the optimal control is $v_*(s) = \overline{v}$ for $s \geq t$. Specializing to $t = 0$ yields the results in Proposition 3.1 (and $\gamma(t)$ defined by (10) is just $\gamma_{0,x}(t)$). □

3.2 | Main theorem and proof

We are now ready to present the main result of this section, the optimal solution to $U(x)$ in (8) and hence to $U(x)$ in (4).

Theorem 3.4. *Assume that $r \leq \beta$, and $\widetilde{P}_\beta(t)$ in (5) satisfies the Lipschitz condition:*

$$|\widetilde{P}_\beta(t) - \widetilde{P}_\beta(s)| \leq C|t - s| \quad \text{for some } C > 0. \tag{21}$$

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

$$\begin{cases} \partial_t v + e^{-\beta t}\ell(x) + \frac{xN'(t)}{N(t)}\partial_x v + \sup_{|v| \leq \overline{v}}\{v(\partial_x v - \widetilde{P}_\beta(t))\} = 0 & \text{in } Q, \\ v(T, x) = e^{-\beta T}h(x), \\ v(t, 0) = e^{-\beta t}h(0), \quad v(t, N(t)) = e^{-\beta t}h(N(t)). \end{cases} \tag{22}$$

Moreover, the optimal strategy is $b_*(t) = 0$ and $v_*(t) = v_*(t, X_*(t))$ for $0 \leq t \leq \mathcal{T}_*$, where $v_*(t, x)$ achieves the supremum in (22), and $X_*(t)$ solves $X_*'(t) = v_*(t, X_*(t)) + \frac{N'(t)}{N(t)}X_*(t)$ with $X_*(0) = x$, and $\mathcal{T}_* := \inf\{t > 0 : X_*(t) = 0 \text{ or } N(t)\} \wedge T$.

Proof. Similar to the dynamic programming/HJB approach that proves Lemma 3.3 and Proposition 3.1 above, here we consider

$$V_2(t, x) := \max_{v(s)} \int_t^{\mathcal{T}} (-\widetilde{P}_\beta(s)v(s) + e^{-\beta s}\ell(X(s))ds + e^{-\beta\mathcal{T}}h(X(\mathcal{T}))$$

$$\text{subject to } X'(s) = v(s) + \frac{N'(s)}{N(s)}X(s), \, X(t) = x,$$

$$0 \leq X(s) \leq N(s),$$

$$|v(s)| \leq \overline{v},$$

so that $U(x) = V_2(0, x)$. By the same dynamic programming argument as above, V_2 solves in the viscosity sense the HJB equation in (22), which can be expressed as $\partial_t v + H(t, x, \partial_x v) = 0$, with

$$H(t, x, p) := e^{-\beta t}\ell(x) + \frac{xN'(t)}{N(t)}p + \sup_{|v| \leq \overline{v}}\{v(p - \widetilde{P}_\beta(t))\}.$$

It is readily checked that under Assumption 2.1 and the Liptschiz condition in (21), the inequality in (15) holds. Thus, V_2 as identified above is the unique viscosity to the HJB equation in (22). The rest of the theorem is straightforward. □

Comparing the HJB equations in (14) and in (22), we see the nonlinear term changes from $\sup_{|\nu|\leq\overline{\nu}}\{\nu\partial_x v\}$ in the stake-hoarding problem, to $\sup_{|\nu|\leq\overline{\nu}}\{\nu(\partial_x v - \widetilde{P}_\beta(t))\}$ in the stake-trading problem, the latter being the general consumption-investment problem. The more general HJB equation in (22) does not have a closed-form solution, and neither does the optimal trading strategy $\nu_*(t)$. This calls for numerical methods; see, for example, Osher and Shu (1991), Souganidis (1985).

4 | LINEAR AND CONVEX UTILITIES

4.1 | Linear utility

Consider the special case of 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 (22), and then derive the optimal strategy $\nu_*(t)$ (in terms of $\widetilde{P}_\beta(t)$).

To start with, the HJB equation in (22) now specializes to the following, with $Q := \{(t, x) : 0 \leq t < T, 0 < x < N(t)\}$ (as before, refer to Lemma 3.3):

$$\begin{cases} \partial_t v + \ell e^{-\beta t} x + \frac{xN'(t)}{N(t)}\partial_x v + \sup_{|\nu|\leq\overline{\nu}}\{\nu(\partial_x v - \widetilde{P}_\beta(t))\} = 0 & (t, x) \in Q, \\ v(T, x) = hx, \\ v(t, 0) = 0, \ v(t, N(t)) = hN(t). \end{cases} \tag{23}$$

For the nonlinear term $\sup_{|\nu|\leq\overline{\nu}}\{\nu(\partial_x v - \widetilde{P}_\beta(t))\}$, we have $\nu_*(t, x) = \overline{\nu}$ if $\partial_x v(t, x) \geq \widetilde{P}_\beta(t)$, and $\nu_*(t, x) = \overline{\nu}$ if $\partial_x v(t, x) < \widetilde{P}_\beta(t)$.

Next, presuming that $\partial_x v \geq \widetilde{P}_\beta(t)$, and ignoring the boundary conditions, the HJB equation in (23) becomes

$$\partial_t v + \ell e^{-\beta t} x - \overline{\nu}\widetilde{P}_\beta(t) + \left(\overline{\nu} + \frac{xN'(t)}{N(t)}\right)\partial_x v = 0, \quad v(T, x) = hx,$$

which has the (classical) solution

$$v^+(t, x) := he^{-\beta T}\gamma_{t,x}^+(T) + \int_t^T \left[\ell e^{-\beta s}\gamma_{t,x}^+(s) - \overline{\nu}\widetilde{P}_\beta(s)\right]ds, \tag{24}$$

where

$$\gamma_{t,x}^+(s) := \overline{\nu}N(s)\int_t^s \frac{du}{N(u)} + \frac{xN(s)}{N(t)}, \quad s \in [t, T]. \tag{25}$$

Similarly, presuming that $\partial_x v < \widetilde{P}_\beta(t)$ and neglecting the boundary conditions turns the HJB equation in (22) into the following form:

$$\partial_t v + \ell e^{-\beta t} x + \overline{\nu}\widetilde{P}_\beta(t) + \left(-\overline{\nu} + \frac{xN'(t)}{N(t)}\right)\partial_x v = 0, \quad v(T, x) = hx,$$

which has the solution

$$v^-(t, x) := he^{-\beta T}\gamma_{t,x}^-(T) + \int_t^T \left[\ell e^{-\beta s}\gamma_{t,x}^-(s) + \overline{\nu}\widetilde{P}_\beta(s)\right]ds, \tag{26}$$

where

$$\gamma_{t,x}^-(s) := -\overline{\nu}N(s)\int_t^s \frac{du}{N(u)} + \frac{xN(s)}{N(t)}, \quad s \in [t, T]. \tag{27}$$

The key observation is that

$$\partial_x v^+(t, x) = \partial_x v^-(t, x) = \underbrace{\frac{1}{N(t)}\left(he^{-\beta T}N(T) + \ell\int_t^T e^{-\beta s}N(s)ds\right)}_{:=\Psi(t)}; \tag{28}$$

and $\Psi(t)$, notably independent of x, is decreasing in $t \in [0, T]$:

$$\Psi(0) = he^{-\beta T}\frac{N(T)}{N} + \frac{\ell}{N}\int_0^T e^{-\beta t}N(t)dt \;\downarrow(\geq)\; \Psi(t) \;\downarrow(\geq)\; \Psi(T) = he^{-\beta T}. \tag{29}$$

This suggests that $\nu_*(t) = \overline{\nu}$ (buy all the time) if $\sup_{[0,T]}\widetilde{P}_\beta(t) \leq \Psi(T)$; and $\nu_*(t) = -\overline{\nu}$ (sell all the time) if $\inf_{[0,T]}\widetilde{P}_\beta(t) \geq \Psi(0)$. Various other scenarios are also possible, such as first buy then sell, or first sell then buy, and so forth.

The following proposition classifies all possible optimal strategies corresponding to $\widetilde{P}_\beta(t)$ as specified above, which we will comment on later.

Proposition 4.1. *Let $\ell(x) = \ell x$ and $h(x) = hx$ with $\ell, h > 0$, and $N(t)$ satisfy Assumption 2.1 (i). Assume that $\widetilde{P}_\beta(t)$ satisfies the Lipschitz condition in (21), and that $\overline{\nu}$ satisfies the following:*

$$\overline{\nu}\int_0^T \frac{dt}{N(t)} \leq \frac{x}{N} \wedge \frac{N - x}{N}. \tag{30}$$

Then, the following results hold:

(i) *Suppose $\widetilde{P}_\beta(t)$ stays constant, that is, 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 $0 \leq t \leq T$. That is, the participant sells at all time at full capacity.*
   (b) *If $P(0) \leq \Psi(T)$, then $\nu_*(t) = \overline{\nu}$. That is, the participant purchases at all time at full capacity.*
   (c) *If $\Psi(T) < P(0) < \Psi(0)$, then*

$$\nu_*(t) = \begin{cases} \overline{\nu} & \text{for } t \leq t_0, \\ -\overline{\nu} & \text{for } t > t_0, \end{cases}$$

   where t_0 is the unique point in $[0, T]$ such that $P(0) = \Psi(t_0)$ with $\Psi(t)$ defined in (28). That is, the participant first buys and after some time sells, both at full capacity.

(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 $0 \leq t \leq T$. That is, the participant sells all the time at full capacity.*
   (b) *If $\widetilde{P}_\beta(T) \leq \Psi(T)$, then $\nu_*(t) = \overline{\nu}$. That is, the participant purchases all the time at full capacity.*

(c) *If $P(0) < \Psi(0)$ and $\widetilde{P}_\beta(T) > \Psi(T)$, then*

$$\nu_*(t) = \begin{cases} \overline{\nu} & \text{for } t \leq t_0, \\ -\overline{\nu} & \text{for } t > t_0, \end{cases}$$

where t_0 is the unique point of intersection of $\widetilde{P}_\beta(t)$ and $\Psi(t)$ on $[0, T]$. That is, the participant first buys and after some time sells, both at full capacity.

(iii) *Suppose that $\widetilde{P}_\beta(t)$ is decreasing in $t \in [0, T]$.*

    (a) *If $P(0) \geq \Psi(0)$, then the participant first sells, and may then buy, and so on, always (buy or sell) 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 participant first buys, and may then sell, and so on, always (buy or sell) at full capacity, according to the crossings of $\widetilde{P}_\beta(t)$ and $\Psi(t)$ in $[0, T]$.*

Proof. Recall that $X_*(t)$ is the state process (number of stakes) corresponding to the optimal strategy $\nu_*(t)$, which, as stipulated in the rest of the proposition, will be equal to either $\overline{\nu}$ or $-\overline{\nu}$. The condition in (30) then ensures that $0 \leq X_*(t) \leq N(t)$ for all $t \in [0, T]$, so $\mathcal{T}_* = T$ (i.e., there will no forced early exit).

Thus, it suffices to find the optimal strategy $\nu_*(t)$ from

$$\sup_{|\nu| \leq \overline{\nu}} \{\nu[\partial_x \upsilon - \widetilde{P}_\beta(t)]\} = \sup_{|\nu| \leq \overline{\nu}} \{\nu[\Psi(t) - \widetilde{P}_\beta(t)]\}.$$

(i) and (ii). Since $\Psi(t)$ is decreasing and $\widetilde{P}(t)$ is either constant or increasing, $\Psi(t) - P(t)$ is decreasing. Hence, we have the following cases (for both (i) and (ii)).

(a) If $\widetilde{P}(0) = P(0) \geq \Psi(0)$, then $\widetilde{P}(t) \geq \Psi(t)$ for all $t \in [0, T]$; hence, $\nu_*(t) = -\overline{\nu}$, and $U(x) = \upsilon^-(0, x)$.

(b) Similarly, if $P(0) \leq \Psi(T)$, then $\widetilde{P}(t) \leq \Psi(t)$ for all $t \in [0, T]$; hence, $\nu_*(t) = \overline{\nu}$, and $U(x) = \upsilon^+(0, x)$.

(c) Otherwise, there will be a unique point for $\Psi(t) - P(t)$ (which is decreasing in t) to cross 0 from above, and let $t_0 \in [0, T]$ denote the crossing point.

This implies that $\nu_*(t) = \overline{\nu}$ for $t \leq t_0$, and $\nu_*(t) = -\overline{\nu}$ for $t > t_0$; and

$$U(x) = \upsilon^+(0, x) - \upsilon^+(t_0, \gamma_{0,x}^+(t_0)) + \upsilon^-(t_0, \gamma_{0,x}^+(t_0)).$$

Part (iii) is similarly argued, the only complication is that $\Psi(t) - P(t)$ is now non-monotone, and hence, there will be multiple points when it crosses 0. □

Several remarks are in order. First note that the condition in (30) 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. This condition may well be removed, but then we would expect another condition similar to the one in (11) to guarantee the optimality of a strategy when an early exit occurs.

Second, $\widetilde{P}_\beta(t) = \mathbb{E}[e^{-\beta t}P(t)]$ combines β, which measures the participant's sensitivity towards risk, with the stake price $P(t)$. Thus, the monotone properties of $\widetilde{P}_\beta(t)$, which classify the three parts (i)-(iii) in Proposition 4.1, naturally connect to martingale pricing: $\widetilde{P}_\beta(t)$ being a constant in
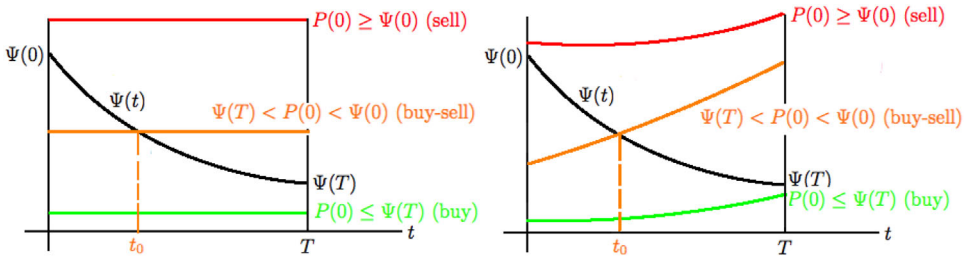
FIGURE 2 Optimal stake trading with linear $\ell(\cdot), h(\cdot)$ when $\widetilde{P}_\beta(t)$ is constant (left) and $\widetilde{P}_\beta(t)$ is increasing (right). [Color figure can be viewed at wileyonlinelibrary.com]

(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 $\Psi(t) = \partial_x v^+(t, x) = \partial_x v^-(t, x)$ represents the rate of return of the participant's utility (from holding of stakes, 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 participant's risk-adjusted stake price (or, valuation) $\widetilde{P}_\beta(t)$: if $\Psi(t) \geq$ (resp. $<$)$\widetilde{P}_\beta(t)$, then the participant will buy (resp. sell) stakes.

Specifically, following (i) and (ii) of Proposition 4.1, for a constant or an increasing $\widetilde{P}_\beta(t)$ (corresponding to a risk-neutral or risk-seeking participant), 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 2 for an illustration.

4.2 | A special case

In part (iii) of Proposition 4.1, 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 is more model structure. Consider, for instance, when $P(t)$ follows a geometric Brownian motion (GBM):

$$\frac{dP(t)}{P(t)} = \mu dt + \sigma dB_t, \quad \text{or} \quad P(t) = P(0)e^{(\mu - \sigma^2/2)t + \sigma B_t}; \quad t \in [0, T], \tag{31}$$

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 $\{P(t)\}$. From the second equation in (31), we have $\mathbb{E}P(t) = P(0)e^{\mu t}$; hence, $\widetilde{P}_\beta(t) = P(0)e^{-(\beta-\mu)t}$. Then, a decreasing $\widetilde{P}_\beta(t)$ corresponds to $\beta > \mu$. From (28), we can derive

$$\Psi'(t) = -\frac{N'(t)}{N(t)}\Psi(t) - \ell e^{-\beta t},$$

and hence,

$$\left(\Psi(t) - \widetilde{P}_\beta(t)\right)' = -\frac{N'(t)}{N(t)}\Psi(t) - \ell e^{-\beta t} + (\beta - \mu)P(0)e^{-(\beta-\mu)t}. \tag{32}$$

Let $\Psi_\alpha(t)$ denote $\Psi(t)$ for $N(t) = N_\alpha(t)$ defined by (1). 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 4.2. *Suppose the assumptions in Proposition 4.1 hold, with $N(t) = N_\alpha(t)$ and $\{P(t)\}$ specified by (31) with $\beta > \mu$. As $N \to \infty$, we have the following results:*

- *If for some $\varepsilon > 0$,*

$$P(0) > \frac{1}{\beta - \mu}\left(\frac{\alpha h e^{-\mu T}(N^{\frac{1}{\alpha}} + T)^\alpha}{N^{1 + \frac{1}{\alpha}}} + \frac{\alpha \ell \beta^{-1}}{N^{\frac{1}{\alpha}}} + \ell\right) + \frac{\varepsilon}{N^{\frac{1}{\alpha}}}, \tag{33}$$

  then $\Psi_\alpha(t) - \widetilde{P}_\beta(t)$ is increasing on $[0, T]$.
- *If for some $\varepsilon > 0$,*

$$P(0) < \frac{1}{\beta - \mu}\left(\frac{\alpha h e^{-\beta T}}{N^{\frac{1}{\alpha}} + T} + \ell e^{-\mu T}\right) - \frac{\varepsilon}{N^{\frac{1}{\alpha}}}, \tag{34}$$

  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 (33) holds, or $P(0) > \Psi_\alpha(0)$ and (34) holds, then $v_*(t) = -\overline{v}$ for all t. That is, the participant sells all the time at full capacity.*
(b) *If $\Psi_\alpha(0) \leq P(0) < e^{(\beta - \mu)T}\Psi_\alpha(T)$ and (33) holds, then $v_*(t) = -\overline{v}$ for $t \leq t_0$ and $v_*(t) = \overline{v}$ for $t > t_0$, where t_0 is the unique point of intersection of $\widetilde{P}_\beta(t)$ and $\Psi_\alpha(t)$ on $[0, T]$. That is, the participant first sells (before t_0) and then buys (after t_0), both at full capacity.*
(c) *If $e^{(\beta - \mu)T}\Psi_\alpha(T) \leq P(0) < \Psi_\alpha(0)$ and (34) holds, then $v_*(t) = \overline{v}$ for $t \leq t_0$ and $v_*(t) = -\overline{v}$ for $t > t_0$, where t_0 is the unique point of intersection of $\widetilde{P}_\beta(t)$ and $\Psi_\alpha(t)$ on $[0, T]$. That is, the participant first buys (before t_0) and then sells (after t_0), both at full capacity.*
(d) *If $P(0) < e^{(\beta - \mu)T}\Psi_\alpha(T)$ and (34) holds, or $P(0) < \Psi_\alpha(0)$ and (33) holds, then $v_*(t) = v$ for all t. That is, the participant buys all the time at full capacity.*

Proof. Note that $\frac{N'_\alpha(t)}{N_\alpha(t)} = \alpha(N^{\frac{1}{\alpha}} + t)^{-1}$, and

$$\int_t^T e^{-\beta s} N_\alpha(s) ds = e^{\beta N^{\frac{1}{\alpha}}} \beta^{-\alpha - 1}\left(\Gamma(\alpha + 1, \beta(N^{\frac{1}{\alpha}} + t)) - \Gamma(\alpha + 1, \beta(N^{\frac{1}{\alpha}} + T))\right),$$

where $\Gamma(a, x) := \int_x^\infty t^{a-1} e^{-t} dt$ is the incomplete Gamma function. As $N \to \infty$, we have

$$\int_t^T e^{-\beta s} N_\alpha(s) ds = \beta^{-1}\left(e^{-\beta t} N_\alpha(t) - e^{-\beta T} N_\alpha(T)\right) + o(N),$$

which together with (28) and (32) implies that

$$
\left(\Psi_\alpha(t) - \widetilde{P}_\beta(t)\right)' = -\frac{\alpha}{N^{\frac{1}{\alpha}} + t}\left[\frac{he^{-\beta T}N_\alpha(T)}{N_\alpha(t)} + \ell\beta^{-1}\left(e^{-\beta t} - e^{-\beta T}\frac{N_\alpha(T)}{N_\alpha(t)}\right) + o(1)\right]
$$
$$
- \ell e^{-\beta t} + (\beta - \mu)P(0)e^{-(\beta-\mu)t}. \tag{35}
$$

Multiplying the RHS of (35) by $e^{(\beta-\mu)t}$, we get

$$
-\frac{\alpha}{N^{\frac{1}{\alpha}} + t}\left[\frac{he^{-\beta(t-T)-\mu t}N_\alpha(T)}{N_\alpha(t)} + \ell\beta^{-1}\left(e^{-\mu t} - e^{-\beta(t-T)-\mu t}\frac{N_\alpha(T)}{N_\alpha(t)}\right) + o(1)\right]
$$
$$
- \ell e^{-\mu t} + (\beta - \mu)P(0).
$$

Clearly, the sum of all the terms above is lower bounded by

$$
-\left(\frac{\alpha he^{-\mu T}N_\alpha(T)}{N^{1+\frac{1}{\alpha}}} + \alpha\ell\beta^{-1}N^{-\frac{1}{\alpha}} + \ell\right) + (\beta - \mu)P(0) \overset{(33)}{>} 0,
$$

which implies that $\inf_{[0,T]}(\Psi_\alpha(t) - \widetilde{P}_\beta(t))' > 0$, and hence, $\Psi_\alpha(t) - \widetilde{P}_\beta(t)$ is increasing.

Moreover, the term is upper bounded by

$$
-\left(\frac{\alpha he^{-\beta T}}{N^{\frac{1}{\alpha}} + T} + \ell e^{-\mu T}\right) + (\beta - \mu)P(0) \overset{(34)}{<} 0,
$$

which implies that $\sup_{[0,T]}(\Psi_\alpha(t) - \widetilde{P}_\beta(t))' < 0$, and hence, $\Psi_\alpha(t) - \widetilde{P}_\beta(t)$ is decreasing.

(a) If $P(0) > e^{(\beta-\mu)T}\Psi_\alpha(T)$ and (33) holds, then $\Psi_\alpha(T) < \widetilde{P}_\beta(T)$ and $\Psi_\alpha(t) - \widetilde{P}_\beta(t)$ is increasing. If $P(0) > \Psi_\alpha(0)$ and (34) holds, then $\Psi_\alpha(0) < \widetilde{P}_\beta(0)$ and $\Psi_\alpha(t) - \widetilde{P}_\beta(t)$ is decreasing. In both cases, we have $\Psi_\alpha(t) - \widetilde{P}_\beta(t) < 0$ for all t.

(b) (c) (d) follow the same argument as (a). □

See Figure 3 for an illustration of the results in the above proposition. Also note that the connection to the participant's risk sensitivity as remarked at the end of Section 4.1 can also be made more explicit when the price process $P(t)$ follows the GBM model in (31), for which we have $\widetilde{P}_\beta(t) = P(0)e^{-(\beta-\mu)t}$. Then, the three cases in Proposition 4.1 correspond to $\beta = \mu$ (martingale), $\beta < \mu$ (sub-martingale), and $\beta > \mu$ (super-martingale). According to the three ranges of β, they can be viewed as representing the participant as risk-neutral, risk-seeking and risk-averse.

4.3 | Convex utility

It is possible to extend the above results to more general, non-linear utility functions $\ell(\cdot)$ and $h(\cdot)$, by following the same approach as above that leads to $v^+(t, x)$ and $v^-(t, x)$ in (24) and (26).

Specifically, considering the two cases of $\partial_x v \geq \widetilde{P}_\beta(t)$, and $\partial_x v < \widetilde{P}_\beta(t)$, we can derive

$$
v^+(t, x) := e^{-\beta T}h\left(\gamma^+_{t,x}(T)\right) + \int_t^T \left[e^{-\beta s}\ell\left(\gamma^+_{t,x}(s)\right) - \overline{\nu}\widetilde{P}_\beta(s)\right]ds, \tag{36}
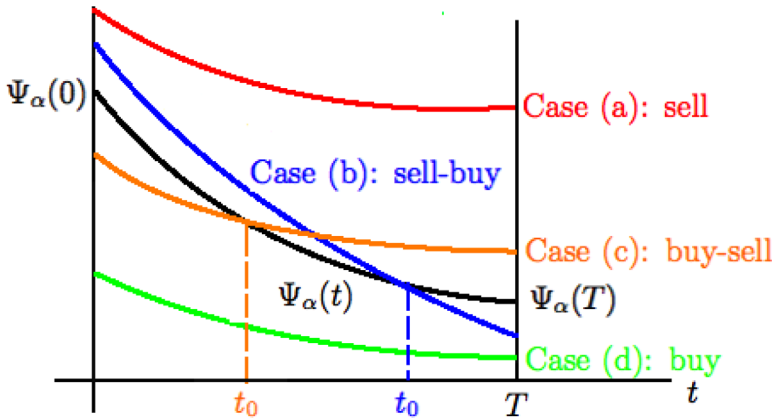$$

FIGURE 3 Optimal stake trading with linear $\ell(\cdot), h(\cdot)$ when $\widetilde{P}_\beta(t) = P(0)e^{(\mu-\beta)t}$ and $N(t) = N_\alpha(t)$.. [Color figure can be viewed at wileyonlinelibrary.com]

$$v^-(t,x) := e^{-\beta T}h\left(\gamma^-_{t,x}(T)\right) + \int_t^T \left[e^{-\beta s}\ell\left(\gamma^-_{t,x}(s)\right) + \overline{\nu}\widetilde{P}_\beta(s)\right]ds; \tag{37}$$

whereas $\gamma^+_{t,x}$ and $\gamma^-_{t,x}$ remain the same as in (25) and (27).

The Ψ function in (28) now splits into two functions: for $(t,x) \in Q := \{(t,x) : 0 \le t < T, 0 < x < N(t)\}$, we have

$$\partial_x v^+(t,x) = \underbrace{\frac{1}{N(t)}\left(e^{-\beta T}N(T)h'\left(\gamma^+_{t,x}(T)\right) + \int_t^T e^{-\beta s}N(s)\ell'\left(\gamma^+_{t,x}(s)\right)ds\right)}_{:=\Psi^+(t,x)}, \tag{38}$$

and

$$\partial_x v^-(t,x) = \underbrace{\frac{1}{N(t)}\left(e^{-\beta T}N(T)h'\left(\gamma^-_{t,x}(T)\right) + \int_t^T e^{-\beta s}N(s)\ell'\left(\gamma^-_{t,x}(s)\right)ds\right)}_{:=\Psi^-(t,x)}. \tag{39}$$

Note that both Ψ^+ and Ψ^- depend on x (as well as on t), via $\gamma^+_{t,x}$ and $\gamma^-_{t,x}$. This dependence makes it necessary to take a closer look at $\gamma^+_{t,x}$ and $\gamma^-_{t,x}$, since the $x = x(t)$ involved in both depends on the control ν *before* (and up to) t. We have the following cases: for $s \ge t$,

$$\text{if } x = \gamma^+_{0,x}(t), \text{ then } \gamma^+_+(s) := \gamma^+_{t,x}(s) = \left(\overline{\nu}\int_t^s \frac{du}{N(u)} + \overline{\nu}\int_0^t \frac{du}{N(u)} + \frac{x}{N}\right)N(s), \tag{40}$$

$$\text{if } x = \gamma^-_{0,x}(t), \text{ then } \gamma^-_-(s) := \gamma^-_{t,x}(s) = \left(-\overline{\nu}\int_t^s \frac{du}{N(u)} - \overline{\nu}\int_0^t \frac{du}{N(u)} + \frac{x}{N}\right)N(s). \tag{41}$$

In other words, γ^+_+ corresponds to $\nu = \overline{\nu}$ both before and after t, whereas γ^-_- corresponds to $\nu = -\overline{\nu}$ both before and after t. The other two cases are similar:

$$\text{if } x = \gamma^+_{0,x}(t), \text{ then } \gamma^-_+(s) := \gamma^-_{t,x}(s) = \left(-\overline{\nu}\int_t^s \frac{du}{N(u)} + \overline{\nu}\int_0^t \frac{du}{N(u)} + \frac{x}{N}\right)N(s), \tag{42}$$

if $x = \gamma_{0,x}^-(t)$, then $\gamma_{\mp}^\pm(s) := \gamma_{t,x}^+(s) = \left(\overline{\nu} \int_t^s \frac{du}{N(u)} - \overline{\nu} \int_0^t \frac{du}{N(u)} + \frac{x}{N} \right) N(s);$ (43)

where γ_+^- corresponds to $\nu = \overline{\nu}$ before (and up to) t and $\nu = -\overline{\nu}$ after t, and γ_-^+ corresponds to the other way around.

Substituting these four cases into Ψ^+ and Ψ^- in (38) and (39) further splits the latter two into four cases:

$$\Psi_+^+(t) := \Psi^+(t, \gamma_{0,x}^+(t)), \quad \Psi_-^-(t) := \Psi^-(t, \gamma_{0,x}^-(t));$$ (44)

$$\Psi_+^-(t) := \Psi^-(t, \gamma_{0,x}^+(t)), \quad \Psi_-^+(t) := \Psi^+(t, \gamma_{0,x}^-(t)).$$ (45)

All four are now functions of t only, as x has been replaced by either $\gamma_{0,x}^+(t)$ or $\gamma_{0,x}^-(t)$.

Clearly, from (40) to (43) above, we have

$$\partial_t \gamma_+^+(s) = \partial_t \gamma_-^-(s) = 0, \quad \partial_t \gamma_+^-(s) = \frac{2\overline{\nu} N(s)}{N(t)} > 0, \quad \partial_t \gamma_-^+(s) = -\frac{2\overline{\nu} N(s)}{N(t)} < 0.$$ (46)

Now, suppose $\ell(\cdot)$ and $h(\cdot)$ are both smooth, *convex* (and increasing) functions. Hence, $\ell'(\cdot) \geq 0$ and $h'(\cdot) \geq 0$, and both are increasing functions. Then, it is readily verified:

(i) Both $\Psi_+^+(t)$ and $\Psi_-^-(t)$ are decreasing in $t \in [0, T]$, and so is $\Psi_-^+(t)$; whereas $\Psi_+^-(t)$ could be both increasing and decreasing (i.e., non-monotone).
(ii) Furthermore, $\Psi_+^+(t) \geq \Psi_-^-(t)$ for all $t \in [0, T]$.

For instance, for $\Psi_+^+(t)$ in (i), consider

$$\partial_t \Psi_+^+(t) = e^{-\beta T} N(T) \left(\frac{h''(\gamma_+^+(T)) \partial_t \gamma_+^+(T)}{N(t)} - \frac{h'(\gamma_+^+(T)) N'(t)}{N^2(t)} \right)$$

$$- \frac{N'(t)}{N^2(t)} \int_t^T e^{-\beta s} N(s) \ell'(\gamma_+^+(s)) ds - e^{-\beta t} \ell'(\gamma_+^+(t))$$

$$+ \frac{1}{N(t)} \int_t^T e^{-\beta s} N(s) \ell''(\gamma_+^+(s)) \partial_t \gamma_+^+(s) ds \quad \leq 0,$$ (47)

where ≤ 0 follows from $\partial_t \gamma_+^+(\cdot) = 0$ in both the first and last terms on the RHS. The other two cases, $\partial_t \Psi_-^-(t) \leq 0$ and $\partial_t \Psi_-^+(t) \leq 0$, are similarly verified.

As in the case of linear utility, the properties above can be used to compare against $\widetilde{P}_\beta(t)$ to identify the optimal trading strategy. Consider the case of $\widetilde{P}_\beta(t)$ being a constant, $\widetilde{P}_\beta(t) = P(0)$ for all $t \in [0, T]$, as in part (i) of Proposition 4.1. If $\Psi_+^+(t) \geq \Psi_-^-(t) \geq P(0)$ for all $t \in [0, t]$, then the optimal strategy is to buy all the time and at rate $\overline{\nu}$. If $P(0) \geq \Psi_+^+(t) > \Psi_-^-(t)$ for all $t \in [0, t]$, then it is optimal to sell all the time, at full capacity.

On the other hand, since Ψ_-^+ corresponds to sell first (before t) and then buy, this clearly cannot be optimal, as it is impossible for $\Psi_-^+ \leq P(0)$ before t and $\Psi_-^+ \geq P(0)$ after t, since Ψ_-^+ is decreasing in t. Similarly, Ψ_+^- corresponds to buy first (before t) and then sell, which can be optimal provided if $\Psi_+^-(t)$ is decreasing in t.

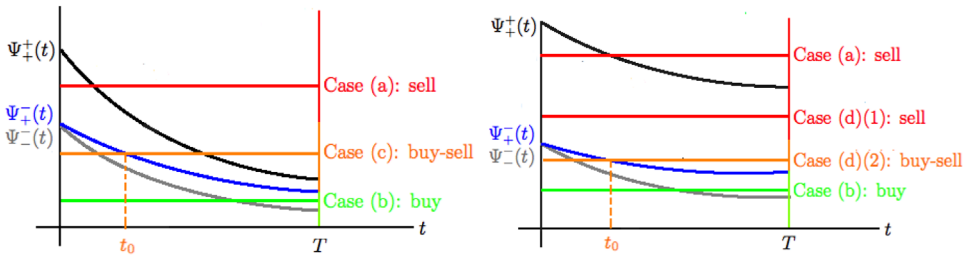The details are stated in the following proposition; and see Figure 4 for an illustration.

FIGURE 4 Optimal stake trading with convex $\ell(\cdot), h(\cdot)$ when $\widetilde{P}_\beta(t)$ is constant, and $\Psi_+^+(T) < \Psi^-(0, x)$ (left) and $\Psi_+^+(T) > \Psi^-(0, x)$ (right). [Color figure can be viewed at wileyonlinelibrary.com]

Proposition 4.3. *Assume that $\ell(\cdot)$ and $h(\cdot)$ are twice continuously differentiable, convex, and satisfy the conditions in Assumption 2.1. Assume that $\widetilde{P}_\beta(t)$ stays constant, that is, $\widetilde{P}_\beta(t) = P(0)$ for all $t \in [0, T]$. Further assume the condition (30), and that $t \to \Psi_+^-(t)$ is decreasing then*

(a) *If $P(0) \geq \Psi_+^+(T) \vee \Psi^-(0, x)$, then $\nu_*(t) = -\bar{\nu}$ for all $0 \leq t \leq T$. That is, the participant sells at all time at full capacity.*

(b) *If $P(0) \leq \Psi_+^-(T)$, then $\nu_*(t) = \bar{\nu}$ for all $0 \leq t \leq T$. That is, the participant buys at all time at full capacity.*

(c) *If $\Psi_+^+(T) < \Psi^-(0, x)$ and $\Psi_+^+(T) < P(0) < \Psi^-(0, x)$, then*

$$\nu_*(t) = \begin{cases} \bar{\nu} & \text{for } t \leq t_0, \\ -\bar{\nu} & \text{for } t > t_0, \end{cases}$$

where t_0 is the unique point in $[0, T]$ such that $\Psi_+^-(t) = P(0)$. That is, the participant first buys and after some time sells, both at full capacity.

(d) *If $\Psi^-(0, x) < \Psi_+^+(T)$, then*
   (1) *if $\Psi^-(0, x) < P(0) < \Psi_+^+(T)$, then $\nu_*(t) = -\bar{\nu}$ for all $0 \leq t \leq T$. That is, the participant sells at all time at full capacity.*
   (2) *if $\Psi_+^-(T) < P(0) \leq \Psi^-(0, x)$, then then*

$$\nu_*(t) = \begin{cases} \bar{\nu} & \text{for } t \leq t_0, \\ -\bar{\nu} & \text{for } t > t_0, \end{cases}$$

where t_0 is the unique point in $[0, T]$ such that $\Psi_+^-(t) = P(0)$. That is, the participant first buys and after some time sells, both at full capacity.

5 | EXTENSION: RISK CONTROL

In the previous sections, we have focused on profit seeking objectives in which a participant's utility increases with getting more stakes, or consuming more. In the modern finance literature, Markowitz Markowitz (1959) pioneered the idea of balancing return and risk in any investment, which is particularly relevant for cryptocurrency trading, which often involves substantial volatility. In this spirit, here we add to the utility objective two "cost" terms that penalize the deviation of participant k's holding of stakes from the average of all others. The idea is, to extent this

deviation measures risk (analogous to the variance in the Markowitz model), it should be the price to be paid for the utility (in holding stakes) that k wants to maximize. (The same idea has been used in Guo et al. (2022) in the context of stochastic games.) Specifically, the deviation of participant k's holding from the average all others can be expressed as $|X_k(t) - \frac{N(t)}{K}|$, taking into account $N(t) = \sum_{k=1}^{K} X_k(t)$. Hence, the new objective function is:

$$U(x) := \sup_{\{v(t), b(t)\}} J(v, b) := \mathbb{E}\left\{ \int_0^{\mathcal{T}} e^{-\beta t}(dc(t) + \ell(X(t))dt) + e^{-\beta \mathcal{T}}(b(\mathcal{T}) + h(X(\mathcal{T}))) \right.$$

$$\left. - \int_0^{\mathcal{T}} e^{-\delta t} g\left(X(t) - \frac{N(t)}{K}\right) dt - e^{-\delta \mathcal{T}} q\left(X(\mathcal{T}) - \frac{N(\mathcal{T})}{K}\right) \right\} \tag{48}$$

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

$$dc(t) + db(t) - rb(t)dt + P(t)v(t)dt = 0, \tag{C1}$$

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

$$|v(t)| \leq \bar{v}, \tag{C3}$$

where $\delta > 0$ is a discount factor (which may or may not be equal to β), and $g : \mathbb{R} \to \mathbb{R}_+$ and $q : \mathbb{R} \to \mathbb{R}_+$ are symmetric, and increasing on $\mathbb{R}_+$ (a typical example is $g(x) = gx^2$ and $q(x) = qx^2$ with $g, q > 0$).

The theorem below follows the same argument as Theorem 3.4.

Theorem 5.1. *Let the assumptions in Theorem 3.4 hold for the problem (48). Assume that $g, q \in C^1(\mathbb{R})$ are symmetric, and increasing on $\mathbb{R}_+$. Then $U(x) = v(0, x)$ where $v(t, x)$ is the unique viscosity solution to the following HJB equation:*

$$\begin{cases} \partial_t v + e^{-\beta t} \ell(x) - e^{-\delta t} g\left(x - \frac{N(t)}{K}\right) + \frac{xN'(t)}{N(t)} \partial_x v + \sup_{|v| \leq \bar{v}} \{v(\partial_x v - \widetilde{P}_\beta(t))\} = 0 & in \ Q, \\ v(T, x) = e^{-\beta T} h(x) - e^{-\delta T} q\left(x - \frac{N(T)}{K}\right), \\ v(t, 0) = e^{-\beta t} h(0) - e^{-\delta t} q\left(\frac{N(t)}{K}\right), \ v(t, N(t)) = e^{-\beta t} h(N(t)) - e^{-\delta t} q\left(\frac{(K-1)N(t)}{K}\right). \end{cases} \tag{49}$$

Moreover, the optimal strategy is $b_*(t) = 0$ and $v_*(t) = v_*(t, X_*(t))$ for $0 \leq t \leq \mathcal{T}_*$ (if it exists), where $v_*(t, x)$ achieves the supremum in (22), and $X_*(t)$ solves $X'_*(t) = v_*(t, X_*(t)) + \frac{N'(t)}{N(t)} X_*(t)$ with $X_*(0) = x$, and $\mathcal{T}_* := \inf\{t > 0 : X_*(t) = 0 \text{ or } N(t)\} \wedge T$.

In general, the HJB equation (49) does not have a closed-form solution even when ℓ, h are linear, and g, q are quadratic. Again it requires numerical methods to solve the HJB equation, and then find the optimal strategy v_*. Nevertheless, there is one exception where the participant is only concerned with the risk entailed by the stakes. The objective is to solve the stake parity problem:

$$U(x) := \inf_{\nu(t)} J(\nu) := \int_0^{\mathcal{T}} e^{-\delta t} g\left(X(t) - \frac{N(t)}{K}\right) dt + e^{-\delta \mathcal{T}} q\left(X(\mathcal{T}) - \frac{N(\mathcal{T})}{K}\right) \tag{50}$$

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

$$b(0) = 0, \ b(t) \geq 0 \text{ and } 0 \leq X(t) \leq N(t), \tag{C2'}$$

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

Since g, h attain the minimum at 0, if $x \geq N/K$, then the participant sells at full capacity until hitting the average $N(t)/K$; if if $x < N/K$, then the participant purchases at full capacity until hitting the average $N(t)/K$. We record this simple fact in the following proposition.

Proposition 5.2. *Assume that* $g, q \in C^1(\mathbb{R})$ *are symmetric, and increasing on* $\mathbb{R}_+$ *for the stake parity problem (50). Let* $\gamma_+(t)$ *be defined by (10), and*

$$\gamma_-(t) := -\bar{\nu} N(t) \int_0^t \frac{ds}{N(s)} + \frac{xN(t)}{N} \quad \text{for } 0 \leq t \leq T, \tag{51}$$

and

$$t_\pm := \inf \left\{ t > 0 : \bar{\nu} \int_0^t \frac{ds}{N(s)} = \pm \left(\frac{1}{K} - \frac{x}{N}\right) \right\}. \tag{52}$$

Then, the following results hold.

(i) *If* $x > N(\frac{1}{K} + \bar{\nu} \int_0^T \frac{dt}{N(t)})$, *then the optimal strategy is* $\nu_*(t) = -\bar{\nu}$ *for all* $0 \leq t \leq T$, *and* $U(x) = \int_0^T e^{-\delta t} g(\gamma_-(t) - \frac{N(t)}{K}) dt + e^{-\delta T} q(\gamma_-(T) - \frac{N(T)}{K})$.

(ii) *If* $\frac{N}{K} < x \leq N(\frac{1}{K} + \bar{\nu} \int_0^T \frac{dt}{N(t)})$, *then the optimal strategy is*

$$\nu_*(t) = \begin{cases} -\bar{\nu} & \text{for } t \leq t_-, \\ 0 & \text{for } t > t_-, \end{cases}$$

and $U(x) = \int_0^{t_-} e^{-\beta t} g(\gamma_-(t) - \frac{N(t)}{K}) dt + \frac{g(0)}{\delta}(e^{-\delta t_-} - e^{-\delta T}) + e^{-\delta T} q(0)$.

(iii) *If* $N(\frac{1}{K} - \bar{\nu} \int_0^T \frac{dt}{N(t)}) \leq x < \frac{N}{K}$, *then the optimal strategy is*

$$\nu_*(t) = \begin{cases} \bar{\nu} & \text{for } t \leq t_-, \\ 0 & \text{for } t > t_-, \end{cases}$$

and $U(x) = \int_0^{t_+} e^{-\beta t} g(\gamma_-(t) - \frac{N(t)}{K}) dt + \frac{g(0)}{\delta}(e^{-\delta t_-} - e^{-\delta T}) + e^{-\delta T} q(0)$.

(iv) *If* $x < N(\frac{1}{K} - \bar{\nu} \int_0^T \frac{dt}{N(t)})$, *the the optimal strategy is* $\nu_*(t) = \bar{\nu}$ *for all* $0 \leq t \leq T$, *and* $U(x) = \int_0^T e^{-\delta t} g(\gamma_+(t) - \frac{N(t)}{K}) dt + e^{-\delta T} q(\gamma_+(T) - \frac{N(T)}{K})$.

Proof. (i) If $x > N(\frac{1}{K} + \bar{\nu}\int_0^T \frac{dt}{N(t)})$, we have $\gamma_-(t) > N(t)/K$ for all $0 \le t \le T$. By a comparison argument, we get $X(t) \ge \gamma_-(t)$ for all $0 \le t \le T$ given any feasible strategy $\nu(t)$. Since g, q are increasing on $\mathbb{R}_+$, we obtain

$$\int_0^T e^{-\delta t} g\left(X(t) - \frac{N(t)}{K}\right) dt + e^{-\delta T} q\left(X(T) - \frac{N(T)}{K}\right)$$
$$\ge \int_0^T e^{-\delta t} g\left(\gamma_-(t) - \frac{N(t)}{K}\right) dt + e^{-\delta T} q\left(\gamma_-(T) - \frac{N(T)}{K}\right),$$

which yields the desired result.

(ii) If $\frac{N}{K} < x \le N(\frac{1}{K} + \bar{\nu}\int_0^T \frac{dt}{N(t)})$, we have $\gamma_-(t) > N(t)/K$ for $0 \le t < t_-$ and $\gamma_-(t_-) = N(t_-)/K$. Again by the comparison argument, $X(t) \ge \gamma_-(t)$ for $0 \le t \le t_-$ given any strategy. Thus,

$$\int_0^T e^{-\delta t} g\left(X(t) - \frac{N(t)}{K}\right) dt + e^{-\delta T} q\left(X(T) - \frac{N(T)}{K}\right)$$
$$= \int_0^{t_-} e^{-\delta t} g\left(X(t) - \frac{N(t)}{K}\right) dt + \int_{t_-}^T e^{-\delta t} g\left(X(t) - \frac{N(t)}{K}\right) dt + e^{-\delta T} q\left(X(T) - \frac{N(T)}{K}\right)$$
$$\ge \int_0^{t_-} e^{-\delta t} g\left(\gamma_-(t) - \frac{N(t)}{K}\right) dt + g(0)\int_{t_-}^T e^{-\delta t} dt + e^{\delta T} g(0),$$

which permits to conclude.

(iii) and (iv) follow the same argument as (1) and (2). □

6 | CONCLUSION

We have developed in this paper a continuous-time control approach to the optimal trading under the PoS protocol, formulated as a consumption-investment problem. We present general solutions to the optimal control via dynamic programming and the HJB equations, and in the case of linear and utility functions, close-form solutions in the form of bang-bang controls. Furthermore, we bring out the explicit connections between the rate of return in trading/holding stakes and the participant's risk-adjusted valuation of the stakes, such that the participant's risk sensitivity is explicitly accounted for in the trading strategy. We have also studied a risk-control version of the consumption-investment problem, and for a special case, the "stake-parity" problem, we show a mean-reverting strategy is the optimal solution.

While our focus here is entirely on an individual participant's trading strategy in a PoS protocol, it is possible to study the interactions among the participants, and formulate the problem of trading in a PoS protocol as a game (deterministic or stochastic), and to study issues such as equilibrium, social welfare, and the inclusion of a trusted third party (or market maker). This will be our focus of a follow-up paper.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID

Wenpin Tang https://orcid.org/0000-0001-7228-1954

REFERENCES

Alsabah, H., & Capponi, A. (2020). Pitfalls of Bitcoin's Proof-of-Work: R&D arms race and mining centralization. SSRN:3273982.

Ambrosio, L. (2008). Transport equation and Cauchy problem for non-smooth vector fields. In *Calculus of variations and nonlinear partial differential equations*, volume 1927 of *Lecture Notes in Mathematics* (pp. 1–41). Springer.

Arnosti, N., & Weinberg, S. M. (2022). Bitcoin: A natural oligopoly. *Management Science*, *68*(7), 4755–4771.

Bertucci, C., Bertucci, L., Lasry, J.-M., & Lions, P.-L. (2020). Mean field game approach to Bitcoin mining. arXiv:2004.08167.

Bertucci, C., Bertucci, L., Lasry, J.-M., & Lions, P.-L. (2022). How resilient is the Bitcoin protocol? SSRN:3907822.

Buterin, V. (2014). Toward a 12-second block time. https://blog.ethereum.org/2014/07/11/toward-a-12-second-block-time

Chiu, J., & Koeppl, T. V. (2017). The economics of cryptocurrencies–Bitcoin and beyond. SSRN:3048124.

Chod, J., Trichakis, N., Tsoukalas, G., Aspegren, H., & Weber, M. (2020). On the financing benefits of supply chain transparency and blockchain adoption. *Management Science*, *66*(10), 4378–4396.

Donovan, F. (2019). Healthcare blockchain could save industry $100b annually by 2025. *HIT Infrastructure*. https://hitinfrastructure.com/news/healthcare-blockchain-could-save-industry-100b-annually-by-2025

Duggan, W., & Powell, F. What is Ethereum 2.0? understanding the merge. Avalialbe at https://www.forbes.com/uk/advisor/investing/cryptocurrency/what-is-ethereum-2/, year=2022

Fleming, W. H., & Soner, H. M. (2006). *Controlled Markov processes and viscosity solutions* (2nd ed.)., volume 25 of *Stochastic Modelling and Applied Probability*. Springer.

Golse, F. (2013). Mean field kinetic equations. http://www.cmls.polytechnique.fr/perso/golse/M2/PolyKinetic.pdf

Guo, X., Tang, W., & Xu, R. (2022). A class of stochastic games and moving free boundary problems. *SIAM Journal on Control and Optimization*, *60*(2), 758–785.

King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. https://decred.org/research/king2012.pdf

Li, Z., Reppen, A. M., & Sircar, R. (2019). A mean field games model for cryptocurrency mining. arXiv:1912.01952.

Markowitz, H. M. (1959). *Portfolio selection: Efficient diversification of investments*. Cowles Foundation for Research, Monograph 16. John Wiley & Sons, Inc.

Mora, C., Rollins, R. L., Taladay, K., Kantar, M. B., Chock, M. K., Shimada, M., & Franklin, E. C. (2018). Bitcoin emissions alone could push global warming above 2 c. *Nature Climate Chang*, *8*(11), 931–933.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Osher, S., & Shu, C. W. (1991). High-order essentially nonoscillatory schemes for Hamilton-Jacobi equations. *SIAM Journal on Numerical Analysis*, *28*(4), 907–922.

Platt, M., Sedlmeir, J., Platt, D., Tasca, P., Xu, J., Vadgama, N., & Ibañez, J. I. (2021). Energy footprint of blockchain consensus mechanisms beyond proof-of-work. arXiv:2109.03667.

Roşu, I., & Saleh, F. (2021). Evolution of shares in a proof-of-stake cryptocurrency. *Management Science*, *67*(2), 661–672.

Saleh, F. (2021). Blockchain without waste: Proof-of-stake. *The Review of Financial Studies*, *34*(3), 1156–1190.

Souganidis, P. E. (1985). Approximation schemes for viscosity solutions of {H}amilton-{J}acobi equations. *Journal of Differential Equations*, *59*(1), 1–43.

Tang, W. (2022). Stability of shares in the Proof of Stake protocol – concentration and phase transitions. arXiv:2206.02227.

Tang, W., & Yao, D. D. (2022). Polynomial voting rules. arXiv:2206.10105.

Wang, Q., Li, R., Wang, Q., & Chen, S. (2021). Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv:2105.07447.

Wood, A. (2018). West Virginia secretary of state reports successful blockchain voting in 2018 midterm elections. https://cointelegraph.com/news/west-virginia-secretary-of-state-reports-successful-blockchain-voting-in-2018-midterm-elections

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, *151*, 1–32.