Volatility and Welfare in a Crypto Economy*

Fahad Saleh†

McGill University, Desautels

October 1, 2018

Abstract

Proof-of-Work (PoW) blockchains possess at least two undesirable characteristics: exceptional price volatility and welfare impairment. Exceptional price volatility arises because PoW implements a passive monetary policy that fails to modulate cryptocurrency demand shocks. Welfare impairment arises because PoW compensates those updating the blockchain through seigniorage while facilitating free-entry among them. This paper theoretically formalizes the aforementioned points and also examines an alternative blockchain mechanism, Proof-of-Burn (PoB), that induces arbitrarily low volatility with arbitrarily enhanced welfare. PoB implements an active monetary policy that modulates cryptocurrency demand shocks. Further, PoB employs a similar incentive structure as PoW but induces welfare gains by supporting cryptocurrency prices with blockchain updating expenses. This paper demonstrates that PoB maintains desirable PoW-characteristics such as free-entry and a deflationary monetary policy but does so without inducing undesirable PoW-characteristics such as exceptional volatility and welfare losses.

Keywords: Cryptocurrency, Volatility, Stable Coin, Welfare, Proof-of-Burn, Proof-of-Work, Blockchain, Bitcoin, Ethereum, FinTech

JEL Classification: E50, G12

*I am especially grateful to Franz Hinzen for extensive discussions. I also thank Farshid Abdi, Joel Hasbrouck, Gur Huberman, Kose John, Tianzan Pang, Max Raskin, Jacob Sagi, Rangarajan Sundaram and David Yermack for valuable comments. All errors are my own. Email: fahad.saleh@mcgill.ca

†McGill University - Desautels Faculty of Management, 1001 Sherbrooke St. West, Montreal, Quebec H3A 1G5, Canada. Email: fahad.saleh@mcgill.ca.

1 Introduction

A permissionless blockchain constitutes an electronic ledger with free entry for updaters. The ledger records transactions in discrete chunks referenced as blocks with the blocks being chained together in an approximately temporal order to form the ledger. The permissionless nature of the blockchain necessitates an updating mechanism that theoretically allows any agent to update the ledger. For this purpose, most major permissionless blockchains employ a mechanism known as Proof-of-Work (PoW). This paper examines that mechanism's volatility and welfare properties and demonstrates the economic inefficiency of PoW. This paper also examines an alternative mechanism, Proof-of-Burn (PoB), and demonstrates that PoB dominates PoW. Thus, this paper provides economic guidance for blockchain design.

Per Nakamoto (2008), PoW "involves scanning for a value" that when evaluated by a special pre-specified function, known as a hash function, produces a sufficiently small output. "When [an agent, known as a miner,] finds [such a value], it broadcasts the [associated] block" to the network thereby updating the ledger. The described exercise requires non-trivial computational power and therefore involves a non-trivial cost. Recognizing that such a cost may deter agents from updating the ledger, Nakamoto (2008) specifies an explicit countervailing incentive: "the first transaction in a block is a special transaction that starts a new coin [or new coins] owned by the creator of the block." The referenced "new coin" constitutes the unit of account for blockchain transactions; this unit of account is known as a cryptocurrency. Nakamoto (2008) specifies the difficulty of finding a valid PoW value be "determined by... targeting an average number of blocks per hour" so that PoW induces a passive monetary policy that fails to react to exogenous cryptocurrency demand shocks.

That monetary policy contributes to the exceptional cryptocurrency volatility documented by Yermack (2014). A positive (negative) demand shock creates upward (down-

ward) price pressure which, ceteris paribus, increases (decreases) mining incentives. A commensurate increase (decrease) in mining activity would increase (decrease) the cryptocurrency supply's growth rate which would counteract the initial demand shock and thereby modulate cryptocurrency volatility. However, such a phenomenon does not obtain because Nakamoto (2008) specifies the difficulty of finding a valid PoW value adjust to maintain a pre-specified expected cryptocurrency supply growth rate. PoW shifts the cryptocurrency supply curve in response to cryptocurrency demand shocks to target an expected cryptocurrency supply growth rate; this supply adjustment magnifies the demand shock's effect on prices.

PoW's economic design also possesses negative welfare implications. Miners receive compensation through newly created cryptocurrency which dilutes the existing cryptocurrency stock thereby imposing a welfare loss upon cryptocurrency holders. These welfare losses represent an economy-wide welfare loss because the blockchain's permissionless nature implies that miners face competition so that miner welfare gains do not off-set household welfare losses.

This paper's first contribution is to formaly demonstrate the aforementioned economic deficiencies of PoW blockchains. This paper models an infinite horizon endowment economy with over-lapping generations of households. Households possess risk-averse preferences and earn income when young but not old. As such, households desire to save for old-age consumption; a cryptocurrency serves as the vehicle for that saving and obtains non-negative endogenous value for that reason. The model also possesses a continuum of risk-neutral miners that may participate in the blockchain's updating process. Conditional upon participating, a miner selects an energy level to expend in the PoW updating process. Miners receive compensation via newly created cryptocurrencies based on the number of valid PoW values found. Each miner faces idiosyncratic risk arising from the number of valid PoW values found, but the cryptocurrency supply evolves with a pre-specified growth rate. This paper demonstrates that any such

monetary policy may be implemented via PoW in equilibrium and that such equilibria always result in exceptional volatility and economy-wide welfare losses.

This paper also studies an alternative mechanism for permissionless blockchains, Proof-of-Burn (PoB). PoB, introduced by Iain Stewart,[1] preserves PoW's reward of new cryptocurrency units for an agent updating the ledger but replaces PoW's computational cost with a different "expensive" task that does not require "real resources [be expended] in the real economy." Stewart's original implementation set the expensive task as "'burning' a tranche of bitcoins [by] sending them to an address which is unspendable." This paper examines a variant of Stewart's PoB in which an agent must surrender ("burn") a quantity of numeraire, hereafter referenced as the burn-rate, to update the ledger.[2] The surrendered quantity accumulates within an account that supports the cryptocurrency in the sense that cryptocurrency holders may retire holdings in exchange for withdrawing account funds in proportion to the number of cryptocurrency units retired.

Unlike PoW, PoB implements an active monetary policy. Positive cryptocurrency demand shocks create upward price pressure. That pressure increases incentives for agents to update the ledger which increases cryptocurrency supply thereby counteracting the upward price pressure. Similarly, negative cryptocurrency demand shocks create downward price pressure. That pressure increases incentives for agents to retire cryptocurrency holdings which reduces the cryptocurrency supply thereby counteracting the downward price pressure. As PoB counteracts price pressure resulting from cryptocurrency demand shocks, PoB induces low cryptocurrency volatility.

PoB also improves welfare relative to PoW and a traditional economic setting. PoB achieves such an improvement not only by removing PoW's expenditure of real resources but also by employing burned resources to support the cryptocurrency. That support

[1] See https://bitcointalk.org/index.php?topic=131139.0

[2] In practice, the numeraire may be substituted for an existing stable currency such as the US Dollar.

provides agents insurance during economic contractions and thereby improves welfare.

This paper's second contribution is to provide the first formal economic analysis of PoB and to establish that PoB dominates PoW both in terms of cryptocurrency volatility reduction and welfare improvement. I demonstrate that PoB both reduces conditional cryptocurrency volatility finitely and induces arbitrarily low cryptocurrency volatility asymptotically. I also demonstrate that PoB can be designed to pareto-dominate PoW and to produce infinitely higher cumulative welfare asymptotically. My results thus highlight that cryptocurrencies may be more viable than otherwise believed.

Related Literature

This paper relates to a large body of research on PoW economics. Eyal and Sirer (2014), Nayak, Kumar, Miller, and Shi (2015), Carlsten, Kalodner, Weinberg, and Narayanan (2016), Biais, Bisiere, Bouvard, and Casamatta (2018) and Cong, He, and Li (2018) study PoW mining strategies. Easley, O'Hara, and Basu (2017) and Huberman, Leshno, and Moallemi (2017) examine congestion and optimal design of PoW blockchains. Pagnotta and Buraschi (2018) study the determinants of cryptocurrency prices within a PoW setting.

This paper also relates to several other literatures. Akin to Fernández-Villaverde and Sanches (2016), Jermann (2018) and Schilling and Uhlig (2018), this paper conducts a monetary analysis of cryptocurrencies. Akin to Routledge and Zetlin-Jones (2018) and Saleh (2018), this paper provides economic guidance for blockchain design.

The remainder of this paper is organized as follows. Section 2 formally states the economic setting and establishes both existence and uniqueness of equilibria for both PoW and PoB mechanisms. Section 3 considers PoB with a constant burn-rate and demonstrates that such a PoB mechanism dominates any PoW mechanism in the sense of generating both lower volatility and higher welfare. Section 4 relaxes the constant burn-rate restriction and demonstrates the existence of a PoB mechanism that pareto dominates a given PoW mechanism and the existence of a PoB mechanism that produces

infinitely more cumulative welfare than a given PoW mechanism. Section 5 demonstrates that the results hold under an alternate PoW model. Section 6 concludes.

2 Model

This paper models an infinite horizon economy that evolves in discrete time. Overlapping generations of households populate the economy. These households live for two periods and possess log utility. Households born in period t receive an exogenous endowment, y_t, when young and no endowment when old. Assumption 1 characterizes the endowment process. Agents trade solely through a cryptocurrency, and households employ this cryptocurrency to facilitate consumption in old age. The time-t cryptocurrency price, P_t, arises endogenously, and households behave as price-takers.

Assumption 1. *Endowment Process*

$\log(y_{t+1}) = \log(y_t) + \varepsilon_{t+1},\ \varepsilon_{t+1} \sim IID(0, \sigma^2)$

I examine three settings: a PoW setting, a traditional setting and a PoB setting. These settings involve different incentive structures, so I discuss these settings separately in subsequent sub-sections.

2.1 Proof-of-Work (PoW)

PoW dates back to Dwork and Naor (1992). Later, Nakamoto (2008) popularized the concept. PoW's precise technical details extend beyond the scope of this paper, but the interested reader may consult Narayanan, Bonneau, Felten, Miller, and Goldfeder (2016) or Biais et al. (2018) for details.

2.1.1 Households

$$\max_{c_t^t, c_{t+1}^t, m_t^t} \log c_t^t + \mathbb{E}_t[\log c_{t+1}^t]$$

$$s.t.$$

$$\begin{aligned} c_t^t + P_t m_t^t &\leqslant y_t \\ c_{t+1}^t &\leqslant P_{t+1} m_t^t \\ c_t^t, c_{t+1}^t &\geqslant 0 \end{aligned} \tag{1}$$

Problem 1 states the household problem in a PoW setting. A household born in period t selects consumption when young, c_t^t, and consumption when old, c_{t+1}^t. That household also selects a cryptocurrency holding, m_t^t, when young to facilitate consumption in old age.

2.1.2 Miners

$$\max_{h_t^i \geqslant 0} P_t R_t h_t^i - \frac{\alpha}{2}(h_t^i)^2 - \beta \tag{2}$$

Within each period, there exists a continuum of zero-measure risk-neutral miners that each live for only one period. Miner i may access a hashing technology if she incurs a cost of $\beta > 0$. This hashing technology enables a miner to execute arbitrarily many hashes. Each hash produces a valid PoW value with some probability, and each valid PoW value yields the associated miner new units of cryptocurrency, hereafter referenced as a block reward.

Miner i selects $\chi_t^i \in \{0, 1\}$ at the beginning of period t with $\chi_t^i = 1$ corresponding to acquiring hashing technology and $\chi_t^i = 0$ corresponding to not acquiring hashing technology. A miner receives no utility if she does not acquire hashing technology, and a miner makes the hashing technology acquisition decision to maximize her utility. Miner i also selects $h_t^i \geqslant 0$ at the beginning of period t with h_t^i corresponding to her chosen hash-rate if $\chi_t^i = 1$. Problem 2 states Miner i's problem if she acquires hashing

technology with R_t denoting the expected block reward from a single hash. Akin to Pagnotta and Buraschi (2018), I assume quadratic hashing costs with $\alpha > 0$.

2.1.3 Equilibrium

Definition 2.1. PoW Equilibrium

A PoW equilibrium is a household allocation $\{(c_t^t, c_{t+1}^t, m_t^t)\}_{t=1}^{\infty}$, an allocation c_1^0 for the initial old, a price sequence, $\{P_t\}_{t=1}^{\infty}$, a miner hashing acquisition decision set, $\{\chi_t^i\}_{t\in\mathbb{N},i\in[0,\infty)}$, a hash-rate set, $\{h_t^i\}_{t\in\mathbb{N},i\in[0,\infty)}$, and an expected block reward sequence, $\{R_t\}_{t=1}^{\infty}$, given an endowment process, $\{y_t\}_{t=1}^{\infty}$, a pre-specified currency supply growth rate, $\{g_t\}_{t=1}^{\infty} \subseteq [0,\infty)$, an initial money supply, $M_0 > 0$, and an initial endowment, $y_0 > 0$ such that:

(i) $\forall t \geqslant 1 : (c_t^t, c_{t+1}^t, m_t^t)$ solves Problem 1

(ii) c_1^0 solves $\max\limits_{c_1^0 \geqslant 0} \log c_1^0 \; s.t. \; c_1^0 \leqslant P_1 M_0$

(iii) $\forall i, t : h_t^i$ solves Problem 2

(iv) $\forall t : \max\limits_{h_t^i \geqslant 0} P_t R_t h_t^i - \frac{\alpha}{2}(h_t^i)^2 - \beta = 0$

(v) $\forall t : M_t \equiv M_0 \prod\limits_{k=1}^{t} e^{g_k} = M_0 + \sum\limits_{k=0}^{t} R_k \int\limits_0^{\infty} h_k^i \chi_k^i di$

(vi) $\forall t : M_t \equiv M_0 \prod\limits_{k=1}^{t} e^{g_k} = m_t^t$

Definition 2.1 defines a PoW equilibrium. Definitions 2.1 (i) and (ii) require that households maximize utility. Definitions 2.1 (iii) requires that a miner maximizes utility if she acquires the hashing technology. Definition 2.1 (iv) constitutes a free-entry condition which reflects the permissionless blockchain setting. Definition 2.1 (v) asserts

that the cryptocurrency supply evolves with a pre-specified growth rate.[3] Definition 2.1 (vi) asserts that the cryptocurrency market must clear.

Condition 1.

$\forall t : \exists N_t \geqslant 0 : \forall i : \chi_t^i = \mathcal{I}_{i \leqslant N_t}$

I consider only equilibria that satisfy Condition 1. This condition imposes sufficient regularity to ensure coherence of Definition 2.1. Condition 1 does not inhibit any economic analysis as it precludes only equilibria that differ exclusively on a semantic dimension.

Proposition 2.1. *PoW Equilibrium Existence and Uniqueness*

There exists a PoW equilibrium satisfying Condition 1. There are no other PoW equilibria that satisfy Condition 1. The following conditions characterize the unique equilirbium.

(A) $\forall t \geqslant 1 : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_{t+1}}{2} e^{-g_{t+1}}, m_t^t = M_0 \prod_{k=1}^{t} e^{g_k}$

(B) $c_1^0 = \frac{y_1}{2} e^{-g_1}$

(C) $\forall i, t : h_t^i = \sqrt{\frac{2\beta}{\alpha}}$

(D) $\forall t : R_t = \frac{2M_0 \prod_{k=1}^{t} e^{g_k}}{y_t} \sqrt{2\alpha\beta}$

[3]Miners being infinitesimal and hash trials being independent yields that a pre-specified currency supply growth rate equates with a deterministic monetary policy. As such, within this section, I model PoW as having a deterministic monetary policy without loss of generality. I relax the assumption of infinitesimal miners in Section 5 which induces a stochastic monetary policy. That relaxation reduces tractability but strengthens my results.

(E) $\forall t : N_t = \frac{y_t}{4\beta}(1 - e^{-g_t})$

(F) $\forall t : P_t = \frac{\frac{y_t}{t}}{2M_0 \prod_{k=1}^{t} e^{g_k}}$

Proposition 2.1 establishes existence and uniqueness of a PoW equilibrium. Thus, there exists a unique expected block reward sequence that induces any particular PoW cryptocurrency monetary policy. In turn, that cryptocurrency monetary policy implies unique economic allocations and prices.

2.2 Traditional Setting

Definition 2.2. Traditional Economic Equilibrium

A Traditional Economic Equilibrium is a PoW Equilibrium that satisfies Condition 1 and $\forall t : g_t = 0$.

Corollary 2.2. *No Miners in a Traditional Economic Equilibrium*

A Traditional Economic Equilibrium involves no mining, i.e. $\forall t : N_t = 0$.

A traditional economic equilibrium may be understood as a special case of the PoW equilibrium defined in Section 2.1 because holding the cryptocurrency supply constant induces a standard equilibrium without mining. Definition 2.2 and Corollary 2.2 formalizes this assertion.

2.3 Proof-of-Burn (PoB)

PoB, introduced by Iain Stewart, possesses various implementations (e.g. Counterparty[4] and Slimcoin[5]). This paper does not model any of those implementations exactly but nonetheless considers a PoB-variant with a similar spirit.

[4]See https://counterparty.io/why-proof-of-burn/
[5]See http://slimco.in/proof-of-burn-eli5/

$$\max_{c_t^t, c_{t+1}^t, m_t^t, \tilde{m}_t^t, m_{t+1}^t, \tilde{m}_{t+1}^t} \log c_t^t + \mathbb{E}_t[\log c_{t+1}^t]$$

$$s.t.$$

$$\begin{aligned} c_t^t + P_t m_t^t + B_t \tilde{m}_t^t &\leqslant y_t \\ c_{t+1}^t &\leqslant P_{t+1} m_{t+1}^t + F_{t+1} \tilde{m}_{t+1}^t \\ c_t^t, c_{t+1}^t, \tilde{m}_t^t, \tilde{m}_{t+1}^t &\geqslant 0 \\ m_{t+1}^t + \tilde{m}_{t+1}^t &\leqslant m_t^t + \tilde{m}_t^t \end{aligned} \tag{3}$$

Problem 3 states the household problem in a PoB setting. Problem 3 differs from Problem 1 for two reasons. First, PoB enables households to update the blockchain and thereby earn new cryptocurrency units by surrendering ("burning") a pre-specified numeraire quantity. B_t denotes the time-t burn-rate while $\tilde{m}_t^t$ denotes the units of cryptocurrency that a young household acquires through updating the blockchain in period t. Second, PoB deposits all surrendered numeraire into an account that supports the cryptocurrency by enabling cryptocurrency holders to retire holdings in exchange for the pro-rata account value. F_t, hereafter referenced as the cryptocurrency's time-t fundamental value, equates with the time-t pro-rata account value while $\tilde{m}_{t+1}^t$ denotes the cryptocurrency amount retired by old households at time $t+1$.

Definition 2.3. PoB Equilibrium

A PoB equilibrium is a household allocation $\{(c_t^t, c_{t+1}^t, m_t^t, \tilde{m}_t^t, m_{t+1}^t, \tilde{m}_{t+1}^t)\}_{t=1}^{\infty}$, an allocation $(c_1^0, m_1^0, \tilde{m}_1^0)$ for the initial old, a price sequence, $\{P_t\}_{t=1}^{\infty}$, a fundamental value sequence, $\{F_t\}_{t=1}^{\infty}$, and a cryptocurrency supply, $\{M_t\}_{t=1}^{\infty}$, given an endowment process, $\{y_t\}_{t=1}^{\infty}$, a weakly-increasing burn-rate sequence, $\{B_t\}_{t=1}^{\infty}$, an initial money supply, $M_0 > 0$, an initial endowment, $y_0 > 0$, and an initial fundamental value, $F_0 \in (0, B_1)$ such that[6]:

[6]I assume $F_0 > 0$ for exposition. The main results hold for $F_0 = 0$. Moreover, no result depends on the level of F_0.

(i) $\forall t : (c_t^t, c_{t+1}^t, m_t^t, \tilde{m}_t^t, m_{t+1}^t, \tilde{m}_{t+1}^t)$ solves Problem 3

(ii) $(c_1^0, m_1^0, \tilde{m}_1^0)$ solves $\max_{c_1^0, m_1^0, \tilde{m}_1^0} \log c_1^0 \; s.t. \; c_1^0 \leqslant P_1 m_1^0 + F_1 \tilde{m}_1^0, \; m_1^0 + \tilde{m}_1^0 \leqslant M_0, \; c_1^0, \tilde{m}_1^0 \geqslant 0$

(iii) $\forall t : F_{t+1} = \frac{F_t M_t + (M_{t+1} - M_t) B_{t+1}}{M_{t+1}} \mathcal{I}_{M_{t+1} > M_t} + F_t \mathcal{I}_{M_{t+1} \leqslant M_t}$

(iv) $\forall t : M_t = m_t^t + \tilde{m}_t^t$

(v) $\forall t : M_{t+1} - M_t = \tilde{m}_{t+1}^{t+1} - \tilde{m}_t^{t+1}$

Definition 2.3 defines a PoB equilibrium. Definitions 2.3 (i) and (ii) require that households maximize utility. Definition 2.3 (iii) describes the evolution of cryptocurrency fundamental value. Definition 2.3 (iv) asserts that the cryptocurrency market must clear. Definition 2.3 (v) provides a law of motion for the cryptocurrency supply.

Proposition 2.3. *PoB Equilibrium Existence and Uniqueness*
There exists a PoB equilibrium. There are no other PoB equilibria. The following conditions characterize the unqiue equilibrium.

(A) $\forall t : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_{t+1}}{2} \frac{B_{t+1} \mathcal{I}_{y_{t+1} > 2M_t B_{t+1}} + F_t \mathcal{I}_{y_{t+1} < 2M_t F_t}}{P_t}, m_t^t = M_{t-1} \mathcal{I}_{y_t \geqslant 2M_{t-1} F_{t-1}} + \frac{y_t}{2F_{t-1}} \mathcal{I}_{y_t < 2M_{t-1} F_{t-1}}, \tilde{m}_t^t = (\frac{y_t}{2B_t} - M_{t-1}) \mathcal{I}_{y_t > 2M_{t-1} B_t}, \tilde{m}_{t+1}^t = (M_t - \frac{y_{t+1}}{2F_t}) \mathcal{I}_{y_{t+1} < 2M_t F_t}, m_{t+1}^t = \frac{y_{t+1}}{2F_t} \mathcal{I}_{y_{t+1} < 2M_t F_t} + M_t \mathcal{I}_{y_{t+1} \geqslant 2M_t F_t}$

(B) $\forall t : P_{t+1} = \min\{\max\{\frac{y_{t+1}}{2M_t}, F_t\}, B_{t+1}\}$

(C) $\forall t : F_{t+1} = \frac{F_t M_t + (\frac{y_{t+1}}{2B_{t+1}} - M_t) B_{t+1}}{\frac{y_{t+1}}{2B_{t+1}}} \mathcal{I}_{y_{t+1} > 2M_t B_{t+1}} + F_t \mathcal{I}_{y_{t+1} \leqslant 2M_t B_{t+1}}$

(D) $\forall t : M_{t+1} = M_t \mathcal{I}_{\frac{y_{t+1}}{2M_t} \in (F_t, B_{t+1})} + \frac{y_{t+1}}{2B_{t+1}} \mathcal{I}_{y_{t+1} \geqslant 2M_t B_{t+1}} + \frac{y_{t+1}}{2F_t} \mathcal{I}_{y_{t+1} \leqslant 2M_t F_t}$

Proposition 2.3 establishes existence and uniqueness of a PoB equilibrium. Thus, any PoB mechanism, defined by the burn-rate sequence, possesses unambiguous economic implications.

3 Main Results

This section provides the paper's main results. Section 3.1 demonstrates that PoB induces lower volatility than PoW and the traditional economic equilibrium. Section 3.2 demonstrates that PoB improves welfare relative to PoW and the traditional economic equilibrium.

Condition 2. *Constant Burn-Rate*

$\forall t : B_t = B > \frac{y_0}{2M_0} > F_0$

For exposition, I impose Condition 2 throughout this section. The burn-rate sequence constitutes a PoB design parameter, so this section's results understate PoB's advantages. Section 4 attests to that assertion.

Hereafter, I employ the superscript PoW to denote PoW-equilibrium objects; the superscript PoB, PoB-equilibrium objects; the superscript $Trad$, traditional-economic-equilibrium objects. Any objects discussed without a superscript correspond to equations that hold under all equilibria.

3.1 Volatility

$$P_t = \frac{y_t}{2M_t} \tag{4}$$

Equation 4 highlights that a cryptocurrency's price increases in transaction volume and decreases in supply. Accordingly, prices may remain stable despite transaction volume fluctuations if cryptocurrency supply adjusts appropriately.

$$Var_t[r_{t,t+1}] = Var_t[\log \frac{y_{t+1}}{y_t}] + Var_t[\log \frac{M_{t+1}}{M_t}] - 2\, Cov_t[\log \frac{y_{t+1}}{y_t}, \log \frac{M_{t+1}}{M_t}] \tag{5}$$

Proposition 3.1. *Reduced Volatility*

$\forall t : vol_t(r^{PoB}_{t,t+1}) \leqslant vol_t(r^{PoW}_{t,t+1})$ *and* $vol_t(r^{PoB}_{t,t+1}) \leqslant vol_t(r^{Trad}_{t,t+1})$

Equation 5 decomposes the time-t conditional variance of one-day-ahead log-returns, $r_{t,t+1}$ and asserts that $Var_t[r_{t,t+1}]$ decreases in $Cov_t[\log \frac{y_{t+1}}{y_t}, \log \frac{M_{t+1}}{M_t}]$. This observation suggests that a positive (negative) correlation between transaction volume and the cryptocurrency supply modulates (magnifies) return volatility. PoW implements a passive monetary policy and thus induces no correlation between the cryptocurrency supply and transaction volume; PoB, in contrast, implements an active monetary policy and induces a positive correlation between the cryptocurrency supply and transaction volume. As such, PoB modulates return volatility whereas PoW neither magnifies nor modulates return volatility. Proposition 3.1 formalizes the aforementioned intuition.

$$\forall t : F_t \leqslant P_t \leqslant B \tag{6}$$

Since households may acquire a newly created cryptocurrency unit by paying B units of numeraire, no-arbitrage implies that cryptocurrency prices cannot exceed B. Moreover, since households may retire cryptocurrency units for fundamental value, no-arbitrage also implies that cryptocurrency prices cannot fall below fundamental value. Then, as indicated by Equation 6, cryptocurrency prices must lie between fundamental value and the burn-rate.

Lemma 3.2. *Fundamental Value*

$F_t \geqslant B \frac{M_t^{PoB} - M_0}{M_t^{PoB}}$

Proposition 3.3. *Asymptotic Price*

$\lim_{t\to\infty} F_t = B$ *so that* $\lim_{t\to\infty} P_t^{PoB} = B$ *almost surely*

Proposition 3.4. *Zero Volatility*

$\lim_{t\to\infty} vol(r^{PoB}_{t,t+1}) = 0$ *and* $\lim_{t\to\infty} vol_t(r^{PoB}_{t,t+1}) = 0$ *almost surely so that* $\lim_{t\to\infty}\{vol_t(r^{PoW}_{t,t+1}) -$

$vol_t(r^{PoB}_{t,t+1})\} = \sup_{t\in\mathbb{N}} \{vol_t(r^{PoW}_{t,t+1}) - vol_t(r^{PoB}_{t,t+1})\}$ *almost surely and* $\lim_{t\to\infty}\{vol_t(r^{Trad}_{t,t+1}) - vol_t(r^{PoB}_{t,t+1})\} = \sup_{t\in\mathbb{N}} \{vol_t(r^{Trad}_{t,t+1}) - vol_t(r^{PoB}_{t,t+1})\}$.

PoB requires that real value support all newly issued cryptocurrency so that cryptocurrency creation augments fundamental value despite decreasing transaction value. Lemma 3.2 formalizes that assertion and implies that fundamental value approaches the burn rate as cryptocurrency creation grows. That insight, coupled with Equation 6, suggests that cryptocurrency prices approach the burn rate asymptotically. Proposition 3.3 formalizes that intuition. Proposition 3.4 extends the result by demonstrating that conditional and unconditional PoB-cryptocurrency volatility becomes arbitrarily small over time.

3.2 Welfare

Definition 3.1. Cumulative Welfare

$\forall T : W_T \equiv \mathbb{E}[\sum_{t=1}^{T} \{\log c_t^t + \log c_t^{t-1}\}]$

Lemma 3.5. *Cumulative Welfare*

$\forall T : W_T = 2T \log \frac{y_0}{2} + \mathbb{E}[\log \frac{M_0}{M_T}]$

Definition 3.1 defines W_T, cumulative welfare for the first T periods, as the expected utility over those periods. Lemma 3.5 evaluates the aforementioned definition and demonstrates that cumulative welfare differs only on the dimension of monetary policy.

Proposition 3.6. *(PoW) Blockchain With Waste*

$\forall T : W_T^{Trad} \geqslant W_T^{PoW}$

Cryptocurrency supply growth imposes a welfare loss upon households. Within a PoW economy, miners benefit from that welfare loss. Permissionless blockchains, however, facilitate free entry of miners; this fact implies that miners obtain no utility in equilibrium so that household welfare losses constitute economy-wide welfare losses. Proposition 3.6 formalizes that assertion and clarifies the notion of "waste" referenced in Saleh (2018) as economically relevant.

Proposition 3.7. *PoB Monetary Policy*

$\forall \delta > 0$: *There exists a PoB mechanism such that* $\lim_{T \to \infty} \{\log M_T^{Trad} - \mathbb{E}[\log M_T^{PoB}]\} = \delta$

Proposition 3.8. *PoB Welfare Gain*

$\forall \delta > 0$: *There exists a PoB mechanism such that* $\lim_{T \to \infty} \{W_T^{PoB} - W_T^{Trad}\} = \delta$ *and* $\lim_{T \to \infty} \{W_T^{PoB} - W_T^{PoW}\} \geqslant \delta$ *for any PoW mechanism.*

Proposition 3.7 asserts that PoB induces an asymptotically smaller cryptocurrency supply than a traditional economic equilibrium. By setting the burn-rate appropriately, that gap may be made arbitrarily large. That fact, coupled with Proposition 3.6, yields Proposition 3.8 which asserts that PoB enhances welfare by an arbitrary margin relative to a traditional economic equilibirum and PoW.

4 Time-Varying Burn-Rates

This section strengthens the insights of Section 3 by allowing for time-varying burn-rates. Section 4.1 demonstrates the existence of a PoB mechanism that pareto-dominates any particular PoW mechanism. Section 4.2 establishes the existence of a PoB mechanism that induces asymptotically arbitrarily low volatility and asymptotically infinitely better welfare than any particular PoW mechanism.

4.1 Pareto Dominance

Proposition 4.1. *Pareto Dominance*

For every PoW mechanism, there exists a PoB mechanism that pareto-dominates the PoW mechanism

Per Section 3.2, PoW induces economy-wide welfare losses. Households that face cryptocurrency supply increases when old incur those welfare losses. PoB, however, may be designed to impose arbitrarily smaller welfare losses on those same households and then pass the associated welfare onto future generations. Thus, there exists a PoB mechanism that pareto dominates any particular PoW mechanism. Proposition 4.1 formalizes this assertion.

4.2 Volatility and Welfare

A burn-rate functions as a price ceiling. A price ceiling contributes to lower volatility by restricting the range of prices but reduces welfare by limiting the extent that households benefit from economic growth. This sub-section considers PoB mechanisms that dynamically adjust burn-rates so that these mechanisms achieve both arbitrarily low volatility and arbitrarily large welfare gains.

$$\tilde{B}_n \equiv \frac{y_0}{2M_0} \prod_{t=1}^{n} e^{\frac{\lambda}{t^\gamma}} \tag{7}$$

$$\tau_n \equiv \inf\{t \in \mathbb{N} : F_t \geqslant \tilde{B}_{n-1}\} \tag{8}$$

$$N(t) \equiv \sup\{\{0\} \bigcup \{n \in \mathbb{N}_+ : \tau_n < t\}\} \tag{9}$$

Proposition 4.2. *Zero Volatility with Infinitely Better Welfare*

There exists a continuum of PoB mechanisms indexed by $\lambda > 0$ *and* $\gamma \in (0, 1]$ *such that* $\lim_{t\to\infty} vol_t(r^{PoB}_{t,t+1}) = 0$ *almost surely and* $\lim_{T\to\infty} \{W^{PoB}_T - W^{Trad}_T\} = \infty$

Equation 7 defines a sequence of increasing burn-rates indexed by $\lambda > 0$ and $\gamma \in (0, 1]$. I prescribe the PoB dynamically adjusting burn-rates by $B_t \equiv \tilde{B}_{N(t)+1}$ with $\tilde{B}_n$ being defined by Equation 7, τ_n being defined by Equation 8 and $N(t)$ being defined by Equation 9. Proposition 4.2 demonstrates that a PoB mechanism defined as such induces zero volatility and infinitely more welfare than a traditional economic equilibrium asymptotically.

Proposition 4.2 offers only asymptotic analysis. As such, I conduct simulations to compare PoB mechanisms with time-varying burn-rates in finite samples. I calibrate parameters based on Bitcoin, and I simulate 1000 paths for 50 years with ε_t assumed to follow a normal distribution.

	γ				
λ	0.01	0.02	0.03	0.04	0.05
0.1	(0.37, 0.38)	(0.36, 0.38)	(0.36, 0.37)	(0.35, 0.37)	(0.35, 0.36)
0.2	(0.50, 0.52)	(0.50, 0.51)	(0.49, 0.51)	(0.49, 0.50)	(0.48, 0.50)
0.3	(0.59, 0.60)	(0.59, 0.59)	(0.58, 0.59)	(0.58, 0.59)	(0.57, 0.58)
0.4	(0.64, 0.65)	(0.64, 0.65)	(0.63, 0.64)	(0.63, 0.64)	(0.63, 0.64)
0.5	(0.67, 0.68)	(0.67, 0.68)	(0.67, 0.68)	(0.67, 0.67)	(0.66, 0.67)

Table 1: Annualized Volatility

Table 1 provides confidence intervals for mean annualized sample volatility across various PoB mechanisms. PoW produces an annualized volatility of 80% with the selected parameters whereas all studied PoB mechanisms produce annualized volatilities statistically lower than 70%. In general, lower λ and higher γ produce lower volatilities.

Table 2 provides confidence intervals for cumulative welfare over a traditional economic equilibrium for various PoB mechanisms. All studied PoB mechanisms produce cumulative welfare statistically higher than a traditional economic equilibrium. In gen-

	γ				
λ	0.01	0.02	0.03	0.04	0.05
0.1	(3.48, 4.11)	(3.41, 4.04)	(3.34, 3.97)	(3.26, 3.90)	(3.19, 3.83)
0.2	(5.13, 5.74)	(5.07, 5.68)	(5.00, 5.61)	(4.94, 5.55)	(4.88, 5.49)
0.3	(5.73, 6.32)	(5.69, 6.28)	(5.65, 6.24)	(5.61, 6.20)	(5.56, 6.16)
0.4	(5.87, 6.45)	(5.87, 6.44)	(5.84, 6.42)	(5.82, 6.40)	(5.79, 6.37)
0.5	(5.81, 6.37)	(5.80, 6.36)	(5.79, 6.36)	(5.79, 6.35)	(5.78, 6.34)

Table 2: Cumulative Welfare

eral, intermediate λ and lower γ produce higher welfare.

5 Extension: A More Realistic PoW Mechanism

Section 2 models miners as infinitesimal which, due to independence of hash trials, yields a deterministic PoW monetary policy. This section relaxes that assumption which then generates a stochastic PoW monetary policy that strengthens this paper's main results. Section 5.1 states the new model and demonstrates existence of a stochastic PoW equilibrium; Section 5.2 provides associated results.

5.1 Model

As within Section 2, Problem 1 states the household problem. Different than Section 2, I assume there exist infinitely many unit-measure miners, indexed by $i \in \mathbb{N}$.

$$\max_{h_t^i \geqslant 0} \mathbb{E}[P_t | y_t, M_{t-1}] R_t h_t^i - \frac{\alpha}{2}(h_t^i)^2 - \beta \tag{10}$$

Problem 10 states Miner i's problem if Miner i acquires hashing technology. As in Section 2, Miner i possesses risk-neutral preferences and faces quadratic hashing costs. Different from Section 2, Miner i acts based on expected prices because, even with fundamental economic uncertainty resolved (i.e. y_t realizes at the beginning of period t), prices remain uncertain due to unresolved uncertainty about the cryptocurrency

supply.[7] Miner i also selects $\chi_t^i \in [0,1]$ with χ_t^i corresponding to the probability that Miner i acquires hashing technology.

Definition 5.1. Stochastic PoW Equilibrium

A stochastic PoW equilibrium is a household allocation $\{(c_t^t, c_{t+1}^t, m_t^t)\}_{t=1}^{\infty}$, an allocation c_1^0 for the initial old, a price sequence, $\{P_t\}_{t=1}^{\infty}$, a miner hashing acquisition decision set, $\{\chi_t^i\}_{t\in\mathbb{N},i\in\mathbb{N}}$, a hash-rate set, $\{h_t^i\}_{t\in\mathbb{N},i\in\mathbb{N}}$, a block reward sequence, $\{\tilde{R}_t\}_{t=1}^{\infty}$, and a hash trial success probability sequence, $\{\pi_t\}_{t=1}^{\infty}$,given an endowment process, $\{y_t\}_{t=1}^{\infty}$, a pre-specified currency supply growth rate, $\{g_t\}_{t=1}^{\infty} \subseteq [0,\infty)$, an initial money supply, $M_0 > 0$, and an initial endowment, $y_0 > 0$ such that:

(i) $\forall t \geqslant 1 : (c_t^t, c_{t+1}^t, m_t^t)$ solves Problem 1

(ii) c_1^0 solves $\max_{c_1^0 \geqslant 0} \log c_1^0 \; s.t. \; c_1^0 \leqslant P_1 M_0$

(iii) $\forall i,t : h_t^i$ solves Problem 10

(iv) $\forall t : \max_{h_t^i \geqslant 0} \mathbb{E}[P_t|y_t, M_{t-1}]\pi_t \tilde{R}_t h_t^i - \frac{\alpha}{2}(h_t^i)^2 - \beta = 0$

(v) $\forall t : \mathbb{E}[M_t|y_t, M_{t-1}] = M_{t-1}e^{g_t}$ with $M_t \equiv M_{t-1} + \tilde{R}_t(\sum_i \sum_h \mathcal{I}_{i,h,t})$

(vi) $\forall t : M_t = m_t^t$

Definition 5.1 states the stochastic PoW equilibrium definition. These conditions constitute a generalization of Definition 2.1. This definition explicitly decomposes the expected block reward, R_t, into component parts: $R_t = \tilde{R}_t \pi_t$. $\mathcal{I}_{i,h,t}$ denotes an indicator that equals 1 if and only if Miner i acquires hashing technology in period t and her hth hash produces a valid PoW solution.

Condition 3.

$\forall t : \exists N_t \geqslant 0 : \forall i : \chi_t^i = \mathcal{I}_{i \leqslant \lfloor N_t \rfloor} + (N_t - \lfloor N_t \rfloor)\mathcal{I}_{i=\lfloor N_t \rfloor + 1}$

[7] Miner i's problem within this section constitutes a generalization of that from Section 2 because $P_t = \mathbb{E}[P_t|y_t, M_{t-1}]$ within Section 2.

I consider only equilibria that satisfy Condition 3. Condition 3 serves a similar role as Condition 1 in Section 2.

Proposition 5.1. *Stochastic PoW Equilibrium Existence*

There exists a Stochastic PoW equilibrium satisfying Condition 3 and the following conditions.

(A) $\forall t \geqslant 1 : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_{t+1}}{2}\frac{M_t}{M_{t+1}}, m_t^t = M_t$

(B) $c_1^0 = \frac{y_1}{2}\frac{M_0}{M_1}$

(C) $\forall i, t : h_t^i = \sqrt{\frac{2\beta}{\alpha}}$

(D) $\forall t : \tilde{R}_t = \frac{4M_{t-1}e^{g_t}}{y_t}\sqrt{2\alpha\beta}$

(E) $\forall t : N_t = \frac{y_t}{8\beta\pi_t}(1 - e^{-g_t})$

(F) $\forall t : P_t = \frac{y_t}{2M_t}$

Proposition 5.1 asserts existence of a Stochastic PoW equilibrium. Due to the non-constructive nature of the associated proof, I do not provide closed-form expressions for all equilibrium objects.

5.2 Results

Proposition 5.2. *Reduced Volatility II*

$\forall t : vol_t(r_{t,t+1}^{PoB}) \leqslant vol_t(r_{t,t+1}^{PoW}) \leqslant vol_t(r_{t,t+1}^{SPoW})$

By construction, hash trial outcomes exhibit independence from all else. Then, since hash trial outcomes constitute the only cryptocurrency supply source of uncertainty, the PoW model within this section induces additional return volatility relative to that from Section 2. Then, following results from Section 3, PoB induces lower return volatility relative to this section's PoW mechanism. Proposition 5.2 formalizes that assertion with the superscript $SPoW$ denoting a stochastic PoW object.

Proposition 5.3. *(PoW) Blockchain With Waste II*

$\forall T : W_T^{Trad} \geqslant W_T^{SPoW}$

Corollary 5.4. *PoB Welfare Gain*

$\forall \delta > 0$: *There exists a PoB mechanism such that* $\lim_{T \to \infty} \{W_T^{PoB} - W_T^{SPoW}\} \geqslant \delta$ *for any Stochastic PoW mechanism.*

The new setting maintains the permissionless nature of the blockchain. Thus, mining remains competitive, and miners earn no utility in equilibrium. Nonetheless, mining imposes a welfare loss upon households via a seigniorage tax so that a stochastic PoW imposes an economy-wide welfare loss relative to both traditional and PoB settings. Proposition 5.3 and Corollary 5.4 formalize these assertions. Corollary 5.4 follows from Propositions 3.8 and 5.3 and therefore requires no independent proof.

6 Conclusion

This paper provides a formal economic critique of PoW. I demonstrate that PoW induces exceptional volatility and impairs aggregate welfare. These points augment the list of PoW concerns beyond those raised by Carlsten et al. (2016), Budish (2018) and Saleh (2018).

This paper also examines an alternative mechanism, PoB. I provide the first formal economic analysis of that mechanism and find that PoB reduces volatility and increases

welfare relative to PoW. PoB also reduces volatility and increases welfare relative to a traditional benchmark. Thus, this paper highlights that cryptocurrencies may be more viable than otherwise believed.

References

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta. 2018. The Blockchain Folk Theorem. *Working Paper* .

Budish, E. 2018. The Economic Limits of Bitcoin and the Blockchain. *NBER Working Paper* .

Carlsten, M., H. Kalodner, S. M. Weinberg, and A. Narayanan. 2016. On the Instability of Bitcoin Without the Block Reward. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* pp. 154–167.

Cong, L. W., Z. He, and J. Li. 2018. Decentralized mining in centralized pools. *Working Paper* .

Dwork, C., and M. Naor. 1992. Pricing via processing or combatting junk mail. *In 12th Annual International Cryptology Conference* pp. 139–147.

Easley, D., M. O'Hara, and S. Basu. 2017. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Working Paper* .

Eyal, I., and E. G. Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *Eighteenth International Conference on Financial Cryptography and Data Security (FC'14)*.

Fernández-Villaverde, J., and D. Sanches. 2016. Can Currency Competition Work? *NBER Working Paper* .

Huberman, G., J. D. Leshno, and C. Moallemi. 2017. Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *Working Paper* .

Jermann, U. 2018. Bitcoin and Cagan's Model of Hyperinflation. *Working Paper* .

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. *www.cryptovest.co.uk* .

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and cryptocurrency technologies*. Princeton University Press.

Nayak, K., S. Kumar, A. Miller, and E. Shi. 2015. Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. Cryptology ePrint Archive, Report 2015/796. http://eprint.iacr.org/2015/796.

Pagnotta, E., and A. Buraschi. 2018. An equilibrium valuation of bitcoin and decentralized network assets. *Working paper* .

Routledge, B. R., and A. Zetlin-Jones. 2018. Currency Stability Using Blockchain Technology. *Working Paper* .

Saleh, F. 2018. Blockchain Without Waste: Proof-of-Stake. *Working Paper* .

Schilling, L., and H. Uhlig. 2018. Some Simple Bitcoin Economics. *NBER Working Paper* .

Yermack, D. 2014. Is Bitcoin a Real Currency? An economic appraisal. *NBER Working Paper* .

Appendices

A Proofs

Lemma A.1. *Non-Real Limit*

Let $S_t \equiv \log \frac{y_t}{y_0} = \sum_{k=1}^{t} \varepsilon_k$.

Then, $\mathbb{P}(\limsup_{t\to\infty} S_t \in \{-\infty, \infty\}) = \mathbb{P}(\liminf_{t\to\infty} S_t \in \{-\infty, \infty\}) = 1$

Proof.

By the Hewitt-Savage zero-one Law, $\forall a \in \mathbb{R} : \mathbb{P}(\limsup_{t\to\infty} S_t \in [a, a + \frac{\sigma}{2}]) \in \{0, 1\}$. Then, $\forall a \in \mathbb{R} : \mathbb{P}(\limsup_{t\to\infty} S_t \in [a, a + \frac{\sigma}{2}]) \leqslant \mathbb{P}(\varepsilon_1 \in [-\frac{1}{2}, \frac{1}{2}]) < 1$ so that $\forall a \in \mathbb{R} : \mathbb{P}(\limsup_{t\to\infty} S_t \in [a, a + \frac{\sigma}{2}]) = 0$ which in turn implies $\forall M \in \mathbb{R} : \mathbb{P}(\limsup_{t\to\infty} S_t \in [-M, M]) = 0$. Then, $\mathbb{P}(\limsup_{t\to\infty} S_t \in \{-\infty, \infty\}) = 1 - \mathbb{P}(\limsup_{t\to\infty} S_t \in \mathbb{R}) = 1 - \lim_{M\to\infty} \mathbb{P}(\limsup_{t\to\infty} S_t \in [-M, M]) = 1$

$\mathbb{P}(\liminf_{t\to\infty} S_t \in \{-\infty, \infty\}) = 1$ follows from a similar argument. □

Lemma A.2. *Unbounded Range*

Let $S_t \equiv \log \frac{y_t}{y_0} = \sum_{k=1}^{t} \varepsilon_k$.

Then, $\limsup_{t\to\infty} S_t = \infty$ *almost surely and* $\liminf_{t\to\infty} S_t = -\infty$ *almost surely*

Proof.

$\mathbb{P}(\limsup_{t\to\infty} S_t = -\infty) \leqslant 1 - \mathbb{P}(\limsup_{t\to\infty} \frac{S_t}{\sqrt{t}} > 0) \leqslant 1 - \mathbb{P}(\bigcap_{t=1}^{\infty} \bigcup_{i=t}^{\infty} \frac{S_i}{\sqrt{i}} \geqslant 1) = 1 - \liminf_{t\to\infty} \mathbb{P}(\bigcup_{i=t}^{\infty} \frac{S_i}{\sqrt{i}} \geqslant 1) \leqslant 1 - \liminf_{t\to\infty} \mathbb{P}(\frac{S_t}{\sqrt{t}} \geqslant 1) < 1$. The Hewitt-Savage zero-one law then implies that $\mathbb{P}(\limsup_{t\to\infty} S_t = -\infty) = 0$ almost surely so that Lemma A.1 yields $\limsup_{t\to\infty} S_t = \infty$ as desired. A similar argument implies that $\liminf_{t\to\infty} S_t = -\infty$

□

Corollary A.3. *Unbounded Endowment*

$\limsup_{t\to\infty} y_t = \infty$ *and* $\liminf_{t\to\infty} y_t = 0$

Proof.

$y_t = y_0 e^{S_t}$ with $S_t \equiv \sum_{k=1}^{t} \varepsilon_k$ so that result follows immediately from Lemma A.2. □

Lemma A.4. *Fundamental Value Upper Bound*

$\forall t : B_{t+1} \geqslant B_t \implies \forall t : B_{t+1} \geqslant F_t$

Proof.

The base case, $t = 0$, holds by assumption. Then, by Definition 2.3(*iii*):

$$
\begin{aligned}
& F_{t+1} \\
&= \tfrac{F_t M_t + (M_{t+1} - M_t) B_{t+1}}{M_{t+1}} \mathcal{I}_{M_{t+1} > M_t} + F_t \mathcal{I}_{M_{t+1} \leqslant M_t} \\
&\leqslant \tfrac{B_{t+1} M_t + (M_{t+1} - M_t) B_{t+1}}{M_{t+1}} \mathcal{I}_{M_{t+1} > M_t} + B_{t+1} \mathcal{I}_{M_{t+1} \leqslant M_t} \\
&= B_{t+1} \\
&\leqslant B_{t+2}
\end{aligned}
$$

□

Lemma A.5. *Weakly Increasing Fundamental Value*

$\forall t : B_{t+1} \geqslant B_t \implies \forall t : F_{t+1} \geqslant F_t$

Proof.

By Proposition 2.3(*iii*):

$$
\begin{aligned}
& F_{t+1} \\
&= \tfrac{F_t M_t + (M_{t+1} - M_t) B_{t+1}}{M_{t+1}} \mathcal{I}_{M_{t+1} > M_t} + F_t \mathcal{I}_{M_{t+1} \leqslant M_t} \\
&\geqslant \tfrac{F_t M_t + (M_{t+1} - M_t) F_t}{M_{t+1}} \mathcal{I}_{M_{t+1} > M_t} + F_t \mathcal{I}_{M_{t+1} \leqslant M_t} \\
&= F_t
\end{aligned}
$$

The second line follows from Lemma A.4. □

Lemma A.6. *Lower Bound on Fundamental Value*

If $\forall t : t \geqslant X \implies B_{t+1} = B$ *then* $\forall t : t \geqslant X \implies F_t \geqslant B \frac{M_t^{PoB} - M_X^{PoB}}{M_t^{PoB}}$

Proof.

I proceed by induction. The base case, $t = X$, follows by construction. Moreover, by Definition 2.3(*iii*):

$$
\begin{aligned}
&F_{t+1} \\
&= \frac{F_t M_t^{PoB} + (M_{t+1}^{PoB} - M_t^{PoB}) B_{t+1}}{M_{t+1}^{PoB}} \mathcal{I}_{M_{t+1}^{PoB} > M_t^{PoB}} + F_t \mathcal{I}_{M_{t+1}^{PoB} \leqslant M_t^{PoB}} \\
&\geqslant B \frac{M_{t+1}^{PoB} - M_X^{PoB}}{M_{t+1}^{PoB}} \mathcal{I}_{M_{t+1}^{PoB} > M_t^{PoB}} + B \frac{M_t^{PoB} - M_X^{PoB}}{M_t^{PoB}} \mathcal{I}_{M_{t+1}^{PoB} \leqslant M_t^{PoB}} \\
&\geqslant B \frac{M_{t+1}^{PoB} - M_X^{PoB}}{M_{t+1}^{PoB}}
\end{aligned}
$$

□

Proposition 2.1 *PoW Equilibrium Existence and Uniqueness*

There exists a PoW equilibrium satisfying Condition 1. There are no other PoW equilibria that satisfy Condition 1. This following conditions characterize the unique equilibrium.

(A) $\forall t \geqslant 1 : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_{t+1}}{2} e^{-g_{t+1}}, m_t^t = M_0 \prod_{k=1}^{t} e^{g_k}$

(B) $c_1^0 = \frac{y_1}{2} e^{-g_1}$

(C) $\forall i, t : h_t^i = \sqrt{\frac{2\beta}{\alpha}}$

(D) $\forall t : R_t = \frac{2M_0 \prod_{k=1}^{t} e^{g_k}}{y_t} \sqrt{2\alpha\beta}$

(E) $\forall t : N_t = \frac{y_t}{4\beta}(1 - e^{-g_t})$

(F) $\forall t : P_t = \frac{y_t}{2M_0 \prod_{k=1}^{t} e^{g_k}}$

Proof.

By standard calculus, the conditions for a PoW equilibrium may be re-written as:

(a) $\forall t \geqslant 1 : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_t}{2}\frac{P_{t+1}}{P_t}, m_t^t = \frac{y_t}{2P_t}$

(b) $c_1^0 = P_1 M_0$

(c) $\forall i, t : h_t^i = \frac{P_t R_t}{\alpha}$

(d) $\forall t : \frac{P_t^2 R_t^2}{2\alpha} - \beta = 0$

(e) $\forall t : M_t \equiv M_0 \prod_{k=1}^{t} e^{g_k} = M_0 + \frac{1}{\alpha}\sum_{k=0}^{t} P_k R_k^2 N_k$

(f) $\forall t : M_t = m_t^t$

(a), (b) and (f) equate with $\forall t \geqslant 1 : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_{t+1}}{2}e^{-g_{t+1}}, m_t^t = M_0 \prod_{k=1}^{t} e^{g_k}, P_t = \frac{y_t}{2M_0 \prod_{k=1}^{t} e^{g_k}}, c_1^0 = \frac{y_1}{2}e^{-g_1}$ so that allocations and prices are uniquely determined. Then, (c) and (d) are satisfied uniquely by $\forall i, t : R_t = \frac{2M_0 \prod_{k=1}^{t} e^{g_k}}{y_t}\sqrt{2\alpha\beta}, h_t^i = \sqrt{\frac{2\beta}{\alpha}}$. As such, demonstrating existence and uniqueness of a PoW equilibrium requires demonstrating only that there exists a unique sequence of non-negative entrant measures, $\{N_t\}_{t=1}^{\infty}$ such that the following condition holds:

(*) $\forall t : M_0 \prod_{k=1}^{t} e^{g_k} = M_0 + 4\beta \sum_{k=0}^{t} \frac{M_0 \prod_{j=1}^{k} e^{g_j}}{y_k} N_k$

The desired conclusion follows by induction. Explicitly, $\forall t : N_t = y_t \frac{1-e^{-g_t}}{4\beta} \geqslant 0$.

□

Proposition 2.3 *PoB Equilibrium Existence and Uniqueness*

There exists a PoB equilibrium. There are no other PoB equilibria. The following conditions characterize the unique equilibrium.

(A) $\forall t : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_{t+1}}{2}\frac{B_{t+1}\mathcal{I}_{y_{t+1}>2M_tB_{t+1}}+F_t\mathcal{I}_{y_{t+1}<2M_tF_t}}{P_t}, m_t^t = M_{t-1}\mathcal{I}_{y_t\geqslant 2M_{t-1}F_{t-1}} + \frac{y_t}{2F_{t-1}}\mathcal{I}_{y_t<2M_{t-1}F_{t-1}}, \tilde{m}_t^t = (\frac{y_t}{2B_t}-M_{t-1})\mathcal{I}_{y_t>2M_{t-1}B_t}, \tilde{m}_{t+1}^t = (M_t-\frac{y_{t+1}}{2F_t})\mathcal{I}_{y_{t+1}<2M_tF_t}, m_{t+1}^t = \frac{y_{t+1}}{2F_t}\mathcal{I}_{y_{t+1}<2M_tF_t} + M_t\mathcal{I}_{y_{t+1}\geqslant 2M_tF_t}$

(B) $\forall t : P_{t+1} = \min\{\max\{\frac{y_{t+1}}{2M_t}, F_t\}, B_{t+1}\}$

(C) $\forall t : F_{t+1} = \frac{F_tM_t+(\frac{y_{t+1}}{2B_{t+1}}-M_t)B_{t+1}}{\frac{y_{t+1}}{2B_{t+1}}}\mathcal{I}_{y_{t+1}>2M_tB_{t+1}} + F_t\mathcal{I}_{y_{t+1}\leqslant 2M_tB_{t+1}}$

(D) $\forall t : M_{t+1} = M_t\mathcal{I}_{\frac{y_{t+1}}{2M_t}\in(F_t,B_{t+1})} + \frac{y_{t+1}}{2B_{t+1}}\mathcal{I}_{y_{t+1}\geqslant 2M_tB_{t+1}} + \frac{y_{t+1}}{2F_t}\mathcal{I}_{y_{t+1}\leqslant 2M_tF_t}$

Proof.

$\forall t : F_t < B_t$ holds for all equilibria. $F_1 < B_1$ holds by the assumption that $F_0 < B_1$, Definition 2.3 (iii) and no-arbitrage. Given $F_t < B_t$, I demonstrate that period t allocations, cryptocurrency supply, fundamental values and prices are unique, and these quantities coupled with Definition 2.3 (iii) and no-arbitrage ensure $F_{t+1} < B_{t+1}$. Thus, without loss of generality, I impose $\forall t : F_t < B_t$ for the remainder of the proof.

Under no-arbitrage, the conditions for a PoB equilibrium may be re-written as:

(a) $\forall t \geqslant 1 : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_{t+1}}{2}\frac{P_{t+1}}{P_t}, m_t^t + \tilde{m}_t^t = \frac{y_t}{2P_t}, m_t^t + \tilde{m}_t^t = m_{t+1}^t + \tilde{m}_{t+1}^t, P_t < B_t \implies \tilde{m}_t^t = 0, P_{t+1} > F_{t+1} \implies \tilde{m}_{t+1}^t = 0$

(b) $c_1^0 = P_1M_0, P_1 > F_1 \implies \tilde{m}_1^0 = 0$

(c) $\forall t : F_{t+1} = \frac{F_tM_t+(M_{t+1}-M_t)B_{t+1}}{M_{t+1}}\mathcal{I}_{M_{t+1}>M_t} + F_t\mathcal{I}_{M_{t+1}\leqslant M_t}$

(d) $\forall t : M_t = m_t^t + \tilde{m}_t^t$

(e) $\forall t : M_{t+1} - M_t = \tilde{m}_{t+1}^{t+1} - \tilde{m}_t^{t+1}$

Under no-arbitrage, $\forall t : P_t = \frac{y_t}{2(m_t^t+\tilde{m}_t^t)}, P_t < B_t \implies \tilde{m}_t^t = 0, P_{t+1} > F_{t+1} \implies \tilde{m}_{t+1}^t = 0$ (from (a) and (b)), (d) and (e) yield $\forall t : \frac{y_{t+1}}{2M_t} \in (F_t, B_{t+1}) \implies M_{t+1} = M_t, \frac{y_{t+1}}{2M_t} > B_{t+1} \implies \tilde{m}_{t+1}^{t+1} = \frac{y_{t+1}}{2B_{t+1}} - M_t, P_{t+1} = B_{t+1}, \frac{y_{t+1}}{2M_t} < F_t \implies \tilde{m}_t^{t+1} =$

$M_t - \frac{y_{t+1}}{2F_t}, P_{t+1} = F_t$. Then, any PoB equilibrium must provide the following allocations and prices, fundamental values and cryptocurrency supply:

(A) $\forall t : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_{t+1}}{2}\frac{B_{t+1}\mathcal{I}_{y_{t+1}>2M_tB_{t+1}} + F_t\mathcal{I}_{y_{t+1}<2M_tF_t}}{P_t}, m_t^t = M_{t-1}\mathcal{I}_{y_t \geqslant 2M_{t-1}F_{t-1}} + \frac{y_t}{2F_{t-1}}\mathcal{I}_{y_t<2M_{t-1}F_{t-1}}, \tilde{m}_t^t = (\frac{y_t}{2B_t} - M_{t-1})\mathcal{I}_{y_t>2M_{t-1}B_t}, \tilde{m}_{t+1}^t = (M_t - \frac{y_{t+1}}{2F_t})\mathcal{I}_{y_{t+1}<2M_tF_t}, m_{t+1}^t = \frac{y_{t+1}}{2F_t}\mathcal{I}_{y_{t+1}<2M_tF_t} + M_t\mathcal{I}_{y_{t+1}\geqslant 2M_tF_t}$

(B) $\forall t : P_{t+1} = \min\{\max\{\frac{y_{t+1}}{2M_t}, F_t\}, B_{t+1}\}$

(C) $\forall t : F_{t+1} = \frac{F_tM_t + (\frac{y_{t+1}}{2B_{t+1}} - M_t)B_{t+1}}{\frac{y_{t+1}}{2B_{t+1}}}\mathcal{I}_{y_{t+1}>2M_tB_{t+1}} + F_t\mathcal{I}_{y_{t+1}\leqslant 2M_tB_{t+1}}$

(D) $\forall t : M_{t+1} = M_t\mathcal{I}_{\frac{y_{t+1}}{2M_t}\in(F_t,B_{t+1})} + \frac{y_{t+1}}{2B_{t+1}}\mathcal{I}_{y_{t+1}\geqslant 2M_tB_{t+1}} + \frac{y_{t+1}}{2F_t}\mathcal{I}_{y_{t+1}\leqslant 2M_tF_t}$

Conditions (A) - (D) provide unique recursive representations for any equilibrium thereby ensuring uniqueness contingent upon demonstrating existence. Existence follows by direct verification that these explicit expressions satisfy PoB equilibrium definition given by (a) - (e). □

Proposition 3.1 *Reduced Volatility*

$\forall t : vol_t(r_{t,t+1}^{PoB}) \leqslant vol_t(r_{t,t+1}^{PoW})$ *and* $vol_t(r_{t,t+1}^{PoB}) \leqslant vol_t(r_{t,t+1}^{Trad})$

Proof.

$\forall t : vol_t(r_{t,t+1}^{PoB}) \leqslant \sqrt{E_t[(r_{t,t+1}^{PoB})^2]} \leqslant \sqrt{E_t[\varepsilon_{t+1}^2]} = \sigma = vol_t(r_{t,t+1}^{PoW}) = vol_t(r_{t,t+1}^{Trad})$ as desired. □

Lemma 3.2 *Fundamental Value*

$\forall t : F_t \geqslant B\frac{M_t^{PoB} - M_0}{M_t^{PoB}}$

Proof.

This result follows from Lemma A.6 with $X = 0$. □

Proposition 3.3 *Asymptotic Price*

$\lim_{t\to\infty} F_t = B$ *so that* $\lim_{t\to\infty} P_t^{PoB} = B$ *almost surely*

Proof.

Proposition 2.3 implies $\forall t : M_t^{PoB} = \frac{y_t}{2P_t^{PoB}} \geqslant \frac{y_t}{2B}$. Then, by Corollary A.3, $\limsup_{t\to\infty} M_t^{PoB} = \infty$ so that Lemmas A.5 and 3.2 yield $\lim_{t\to\infty} F_t = \limsup_{t\to\infty} F_t \geqslant B$. In turn, Lemma A.4 implies $\lim_{t\to\infty} F_t = B$ as desired. Application of the Squeeze Theorem to Equation 6 completes the proof. □

Proposition 3.4 *Zero Volatility*

$\lim_{t\to\infty} vol(r_{t,t+1}^{PoB}) = 0$ *and* $\lim_{t\to\infty} vol_t(r_{t,t+1}^{PoB}) = 0$ *almost surely so that* $\lim_{t\to\infty}\{vol_t(r_{t,t+1}^{PoW}) - vol_t(r_{t,t+1}^{PoB})\} = \sup_{t\in\mathbb{N}}\{vol_t(r_{t,t+1}^{PoW}) - vol_t(r_{t,t+1}^{PoB})\}$ *almost surely and* $\lim_{t\to\infty}\{vol_t(r_{t,t+1}^{Trad}) - vol_t(r_{t,t+1}^{PoB})\} = \sup_{t\in\mathbb{N}}\{vol_t(r_{t,t+1}^{Trad}) - vol_t(r_{t,t+1}^{PoB})\}$.

Proof.

$\lim_{t\to\infty} vol(r_{t,t+1}^{PoB}) = 0$ follows from Proposition 3.3 and the Bounded Convergence Theorem. That result, the Law of Total Variance and the Bounded Convergence Thereom imply $\lim_{t\to\infty} vol_t(r_{t,t+1}^{PoB}) = 0$ almost surely. Finally, $\sup_{t\in\mathbb{N}}\{vol_t(r_{t,t+1}^{PoW}) - vol_t(r_{t,t+1}^{PoB})\} \leqslant \sup_{t\in\mathbb{N}} vol_t(r_{t,t+1}^{PoW}) = \sigma = \lim_{t\to\infty}\{vol_t(r_{t,t+1}^{PoW}) - vol_t(r_{t,t+1}^{PoB})\}$ and $\sup_{t\in\mathbb{N}}\{vol_t(r_{t,t+1}^{Trad}) - vol_t(r_{t,t+1}^{PoB})\} \leqslant \sup_{t\in\mathbb{N}} vol_t(r_{t,t+1}^{Trad}) = \sigma = \lim_{t\to\infty}\{vol_t(r_{t,t+1}^{Trad}) - vol_t(r_{t,t+1}^{PoB})\}$ as desired. □

Lemma 3.5 *Cumulative Welfare*

$\forall T : W_T = 2T \log\frac{y_0}{2} + \mathbb{E}[\log\frac{M_0}{M_T}]$

Proof.

By Definition 3.1 and Proposition 2.1,

$\forall T : W_T = \mathbb{E}[\sum_{t=1}^{T}\{\log c_t^t + \log c_t^{t-1}\}] = \mathbb{E}[\sum_{t=1}^{T}\{\log \frac{y_t}{2} + \log P_t M_{t-1}\}] = 2\sum_{t=1}^{T}\mathbb{E}[\log \frac{y_t}{2}] + \mathbb{E}[\sum_{t=1}^{T}\log \frac{M_{t-1}}{M_t}] = 2T \log \frac{y_0}{2} + \mathbb{E}[\log \frac{M_0}{M_T}]$ as desired. □

Proposition 3.6 *(PoW) Blockchain With Waste*

$\forall T : W_T^{Trad} \geqslant W_T^{PoW}$

Proof.

By Lemma 3.5,

$\forall T : W_T^{Trad} - W_T^{PoW} = \mathbb{E}[\log \frac{M_T^{PoW}}{M_T^{Trad}}] = \sum_{t=1}^{T} g_t \geqslant 0$ as desired. □

Proposition 3.7 *PoB Monetary Policy*

$\forall \delta > 0$: *There exists a PoB mechanism such that* $\lim_{t\to\infty}\{\log M_T^{Trad} - \mathbb{E}[\log M_T^{PoB}]\} = \delta$

Proof.

Let the PoB mechanism be characterized by $B \equiv \frac{y_0}{2M_0}e^{\delta}$. Then, via the Bounded Convergence Theorem and Proposition 3.3:

$\lim_{T\to\infty}\{\log M_T^{Trad} - \mathbb{E}[\log M_T^{PoB}]\} = \lim_{T\to\infty}\{\mathbb{E}[\log P_T^{PoB}] - \mathbb{E}[\log \frac{y_T}{2M_0}]\} = \log B - \log \frac{y_0}{2M_0} = \delta$ as desired. □

Proposition 3.8 *PoB Welfare Gain*

$\forall \delta > 0$: *There exists a PoB mechanism such that* $\lim_{T\to\infty}\{W_T^{PoB} - W_T^{Trad}\} = \delta$ *and* $\lim_{T\to\infty}\{W_T^{PoB} - W_T^{PoW}\} \geqslant \delta$ *for any PoW mechanism.*

Proof.

For each $\delta > 0$, let the PoB mechanism be that considered by Proposition 3.7. Then,

$\lim_{T\to\infty}\{W_T^{PoB} - W_T^{Trad}\} = \lim_{T\to\infty}\{\log M_T^{Trad} - \mathbb{E}[\log M_T^{PoB}]\} = \delta$

Moreover, for any PoW mechanism,

$\lim_{T\to\infty}\{W_T^{PoB} - W_T^{PoW}\} = \lim_{T\to\infty}\{W_T^{PoB} - W_T^{Trad}\} + \lim_{T\to\infty}\{W_T^{Trad} - W_T^{PoW}\} = \delta + \sum_{t=1}^{\infty} g_t \geqslant \delta$

as desired. □

Proposition 4.1 *Pareto Dominance*

For every PoW mechanism, there exists a PoB mechanism that pareto-dominates the PoW mechanism.

Proof.

I proceed by constructing a PoB mechanism that pareto dominates a given PoW mechanism. A sequence of burn-rates, $\{B_t\}_{t=1}^{\infty}$, characterize a PoB mechanism; I construct this sequence inductively and then demonstrate pareto dominance.

With $\{B_t\}_{t=1}^{T}$ fixed, I define $\nu_{T+1} \in m\mathcal{F}_T$ by $\nu_{T+1} \equiv \mathbb{E}_T[\max\{\varepsilon_{T+1}, \log\frac{F_T}{P_T^{PoB}}\}] > 0$. Then, I select $B'_{T+1}, B_{T+1} \in m\mathcal{F}_{\mathcal{T}}$ such that $G_T(B'_{T+1}) \equiv \mathbb{E}_T[\min\{\max\{\varepsilon_{T+1}, \log\frac{F_T}{P_T^{PoB}}\}, \log\frac{B'_{T+1}}{P_T^{PoB}}\}] = \frac{\nu_{T+1}}{2}$ and $B_{T+1} \equiv \max\{B_T, B'_{T+1}\}$. G_T constitutes a continuous and increasing (random) function such that $\lim_{x\to P_T^{PoB+}} G_T(x) \leqslant 0$ and $\lim_{x\to\infty} G_T(x) = \nu_{T+1}$ with continuity following from the Conditional Monotone Convergence Theorem; these properties ensure the existence of B'_{T+1} and B_{T+1}. Then, letting W^t denote the expected utility of a household born in period t:

$W^{t,PoB} - W^{t,PoW} = \mathbb{E}[\log\frac{M_t^{PoB}}{M_{t+1}^{PoB}}] - \mathbb{E}[\log\frac{M_t^{PoW}}{M_{t+1}^{PoW}}] = \mathbb{E}[\log\frac{P_{t+1}^{PoB}}{P_t^{PoB}}] + g_{t+1} = \mathbb{E}[G_t(B_{t+1})] + g_{t+1} \geqslant \mathbb{E}[G_t(B'_{t+1})] + g_{t+1} > 0$

This result completes the proof because miners receive no utility in any equilibria. □

Proposition 4.2 *Zero Volatility with Infinitely Better Welfare*

There exists a continuum of PoB equilibria indexed by $\lambda > 0$ and $\gamma \in (0, 1]$ such that $\lim_{t\to\infty} vol_t(r_{t,t+1}^{PoB}) = 0$ almost surely and $\lim_{T\to\infty}\{W_T^{PoB} - W_T^{Trad}\} = \infty$

Proof.

I define $N \equiv \sup\{\{0\} \bigcup \{n \in \mathbb{N}_+ : \tau_n < \infty\}\}$.

Then, $\forall n \in \mathbb{N}$:

$\mathbb{P}(N = n)$

$= \mathbb{P}(N = n, \tau_{n+1} = \infty)$

$\leqslant \mathbb{P}(N = n, \limsup_{t\to\infty} F_t \leqslant \tilde{B}_n)$

$\leqslant \mathbb{P}(N = n, \limsup_{t\to\infty} \tilde{B}_{n+1}(\frac{M_t - M_{\tau_n}}{M_t}) \leqslant \tilde{B}_n)$

$\leqslant \mathbb{P}(N = n, \limsup_{t\to\infty} \tilde{B}_{n+1}(1 - \frac{2\ \tilde{B}_{n+1}\ M_{\tau_n}}{y_t}) \leqslant \tilde{B}_n)$

$= 0$

Thus, $\mathbb{P}(N = \infty) = 1$.

Moreover, $\forall n \in \mathbb{N}_+ : N \geqslant n \implies \limsup_{t\to\infty} vol_t(r^{PoB}_{t,t+1}) \leqslant \frac{2\lambda}{n^\gamma}$ so that $\forall \delta > 0 : \mathbb{P}(\limsup_{t\to\infty} vol_t(r^{PoB}_{t,t+1}) \leqslant \delta) \geqslant \mathbb{P}(\limsup_{t\to\infty} vol_t(r^{PoB}_{t,t+1}) \leqslant \delta, N \geqslant \lceil(\frac{2\lambda}{\delta})^{\frac{1}{\gamma}}\rceil) = \mathbb{P}(N \geqslant \lceil(\frac{2\lambda}{\delta})^{\frac{1}{\gamma}}\rceil) =$ 1 which implies $\lim_{t\to\infty} vol_t(r^{PoB}_{t,t+1}) = 0$ almost surely.

Additionally, $\forall n \in \mathbb{N}_+ : \mathbb{P}(\lim_{t\to\infty} F_t \geqslant \tilde{B}_n) \geqslant \mathbb{P}(N \geqslant n+1) = 1$ so that $\lim_{n\to\infty} \tilde{B}_n = \infty$ yields $\lim_{t\to\infty} F_t = \infty$ almost surely. Then, $\liminf_{T\to\infty}\{W^{PoB}_T - W^{Trad}_T\} = \liminf_{T\to\infty} \mathbb{E}[\log \frac{M_0}{M^{PoB}_T}] = \liminf_{T\to\infty} \mathbb{E}[\log P^{PoB}_T] - \log \frac{y_0}{2\ M_0} \geqslant \liminf_{T\to\infty} \mathbb{E}[\log F_T] - \log \frac{y_0}{2\ M_0} = \infty$ with the Monotone Convergence Theorem yielding the last equality. □

Proposition 5.1 *Stochastic PoW Equilibrium Existence*

There exists a Stochastic PoW equilibrium satisfying Condition 3 and the following conditions.

(A) $\forall t \geqslant 1 : c^t_t = \frac{y_t}{2}, c^t_{t+1} = \frac{y_{t+1}}{2}\frac{M_t}{M_{t+1}}, m^t_t = M_t$

(B) $c^0_1 = \frac{y_1}{2}\frac{M_0}{M_1}$

(C) $\forall i,t : h_t^i = \sqrt{\frac{2\beta}{\alpha}}$

(D) $\forall t : \tilde{R}_t = \frac{4M_{t-1}e^{g_t}}{y_t}\sqrt{2\alpha\beta}$

(E) $\forall t : N_t = \frac{y_t}{8\beta\pi_t}(1 - e^{-g_t})$

(F) $\forall t : P_t = \frac{y_t}{2M_t}$

Proof.

By standard calculus, the conditions for a stochastic PoW equilibrium may be re-written as:

(a) $\forall t \geqslant 1 : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_t}{2}\frac{P_{t+1}}{P_t}, m_t^t = \frac{y_t}{2P_t}$

(b) $c_1^0 = P_1 M_0$

(c) $\forall i,t : h_t^i = \frac{\mathbb{E}[P_t|y_t,M_{t-1}]R_t}{\alpha}$

(d) $\forall t : \frac{\mathbb{E}[P_t|y_t,M_{t-1}]^2 R_t^2}{2\alpha} - \beta = 0$

(e) $\forall t : \mathbb{E}\big[M_t|y_t, M_{t-1}\big] = M_{t-1}e^{g_t} = M_{t-1} + \frac{\mathbb{E}[P_t|y_t,M_{t-1}]R_t^2 N_t}{\alpha}$

(f) $\forall t : M_t = m_t^t$

(a), (b) and (f) equate with $\forall t \geqslant 1 : c_t^t = \frac{y_t}{2}, c_{t+1}^t = \frac{y_{t+1}}{2}\frac{M_t}{M_{t+1}}, m_t^t = M_t, P_t = \frac{y_t}{2M_t}, c_1^0 = \frac{y_1}{2}\frac{M_0}{M_1}$ so that allocations and prices are determined uniquely by the cryptocurrency supply. (c), (d) and (e) equate with conditions given below:

(1) $\forall i,t : h_t^i = \sqrt{\frac{2\beta}{\alpha}}$

(2) $\forall t : \mathbb{E}\big[P_t|y_t, M_{t-1}\big]^2 R_t^2 = 2\alpha\beta$

(3) $\forall t : \mathbb{E}[M_t|y_t, M_{t-1}] = M_{t-1}e^{g_t} = M_{t-1} + R_t N_t\sqrt{\frac{2\beta}{\alpha}}$

Let $R_t^* \equiv \frac{4M_{t-1}e^{g_t}}{y_t}\sqrt{2\alpha\beta}$, $N(\pi_t) \equiv \frac{y_t}{8\beta\pi_t}(1 - e^{-g_t})$

and $F(y_t, \pi_t, M_{t-1}) \equiv \frac{y_t^2}{4}(R_t^*)^2\pi_t^2\mathbb{E}[\frac{1}{M_t(\pi_t, M_{t-1})}|y_t, M_{t-1}]^2 - 2\alpha\beta$.

I define $M_t(\pi_t, M_{t-1}) \equiv M_{t-1} + \pi_t R_t^*(\sum_{i=1}^{N_t^\chi}\sum_{h=1}^{\sqrt{\frac{2\beta}{\alpha}}}\mathcal{I}_{i,h,t})$ with $N_t^\chi = \lfloor N(\pi_t)\rfloor + \mathcal{I}_t$ and $\mathcal{I}_t \sim$Bernoulli$(N(\pi_t) - \lfloor N(\pi_t)\rfloor)$ conditionally independent of all else observed as of the beginning of time t.

Then, finding a stochastic sequence $\{\pi_t\}_{t=1}^\infty$ such that $\forall t : F(y_t, \pi_t, M_{t-1}) = 0$ and $\forall t : 0 \leqslant \pi_t \leqslant 1$ suffices to demonstrate existence of an equilibrium because all equilibrium conditions hold with $\tilde{R}_t = R_t^*, N_t = N(\pi_t)$ and $h_t^i = \sqrt{\frac{2\beta}{\alpha}}$. By Jensen's inequality, $F(y_t, \frac{1}{2}, M_{t-1}) \geqslant 0$ whereas $\limsup_{\pi_t \to 0^+} F(y_t, \pi_t, M_{t-1}) < 0$, so continuity of $F(y_t, \pi_t, M_{t-1})$ in the second argument concludes the proof.

□

Proposition 5.2 *Reduced Volatility II*

$\forall t : vol_t(r_{t,t+1}^{PoB}) \leqslant vol_t(r_{t,t+1}^{PoW}) \leqslant vol_t(r_{t,t+1}^{SPoW})$

Proof.

$\forall t : vol_t(r_{t,t+1}^{SPoW}) = \sqrt{Var_t[\log\frac{y_{t+1}}{y_t}] + Var_t[\log\frac{M_{t+1}^{SPoW}}{M_t^{SPoW}}] - 2\,Cov_t[\log\frac{y_{t+1}}{y_t}, \log\frac{M_{t+1}^{SPoW}}{M_t^{SPoW}}]} = \sqrt{Var_t[\log\frac{y_{t+1}}{y_t}] + Var_t[\log\frac{M_{t+1}^{SPoW}}{M_t^{SPoW}}]} \geqslant \sigma = vol_t(r_{t,t+1}^{PoW})$. The remaining inequality follows from Proposition 3.1. □

Proposition 5.3 *(PoW) Blockchain With Waste II*

$\forall T : W_T^{Trad} \geqslant W_T^{SPoW}$

Proof.

By Lemma 3.5,

$\forall T : W_T^{Trad} - W_T^{SPoW} = \mathbb{E}[\log\frac{M_T^{PoW}}{M_T^{Trad}}] \geqslant 0$ as desired. □