Smooth Transition from PoW to PoS

Xinyu Zhang
Monash University and CSIRO Data61
Melbourne, Australia
xinyu.zhang1@monash.edu

Runchao Han
BabylonChain Inc.
Melbourne, Australia
runchao.han@babylonchain.io

Tong Cao
The Hong Kong Polytechnic University
Hong Kong, China
tongcaodaniel@gmail.com

Jiangshan Yu
The University of Sydney
Sydney, Australia
J.Yu.Research@gmail.com

ABSTRACT

We develop a method that facilitates a seamless transition from a Proof-of-Work (PoW)-based blockchain to a Proof-of-Stake (PoS)-based blockchain, by leveraging the Minotaur hybrid consensus protocol [CCS'22]. Our research investigates the feasibility of using weight parameters within the Minotaur protocol to encourage miners to maintain or reduce their current mining status during the transition. We build a game-theoretic model to identify the strategies and utilities of the miners and analyse the model using Nash equilibrium. As a result, we suggest a weight parameter of $-1/20 + 1$ for a short transition lasting 4 epochs, and for a longer-term transition spanning 10 epochs, we suggest selecting a weight parameter of $-1/50 + 1$.

CCS CONCEPTS

• **Computer systems organization → Dependable and fault-tolerant systems and networks**; **Distributed architectures**.

KEYWORDS

Blockchain, Consensus, Proof of Work, Proof of Stake, Transition

ACM Reference Format:
Xinyu Zhang, Runchao Han, Tong Cao, and Jiangshan Yu. 2024. Smooth Transition from PoW to PoS. In *The 6th ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI:'24), July 2, 2024, Singapore, Singapore.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3659463.3660017

1 INTRODUCTION

Since the introduction of Bitcoin, blockchain technology has received considerable attention both from academia and industry. The successful attempt of Bitcoin to validate transactions via a decentralised consensus process brought a severe downside: a considerable amount of electricity energy consumption, which translates into a significant level of carbon emissions [5]. According to the estimation of Digiconomist's Bitcoin Energy Consumption Index[1], one bitcoin transaction can take 1,449 KWh to complete, which is equivalent to 50 days of power for the average US household[2]. Consequently, numerous blockchain consensus protocols (e.g., proof-of-stake (PoS)) have been proposed to replace the original Bitcoin proof-of-work (PoW) protocol.

However, the existing blockchain concensus protocols mainly focused on solving the energy consumption problem for new cryptocurrencies. For existing cryptocurrencies which adopt proof-of-work as the main concensus technique, there are several obstacles that prevent them to become more energy efficient. First of all, PoW miners who invested on mining machines may reluctant to perform the transition. For example, Ethereum blockchain moves from the original PoW consensus (Ethash) to a PoS (Casper) recently. The transition reduced energy consumption by 99.98% while the validator network's Herfindahl index becomes 8.6% lower than the miners' prior to the transition. Targeting on the problem, we apply the state-of-the-art hybrid consensus technique, Minotaur [3] to enable a smoother transition from the PoW blockchain to PoS.

In a nutshell, Minotaur introduced a weight parameter $\omega(e)$ such that the probability of the block validator wins the PoS "lottery" is proportional to the so-called virtual stake, which is a weighted combination of work stake (depending on the PoW) and real stake. By gradually adjusting the weight parameter, the PoW chain can eventually become a pure PoS chain. During the transition, the PoW miners can still use their mining machine to gain the share of virtual stake and increase the probability to win the reward, which makes the transition smoother. However, such transition faces another challenge. Since the weight parameter is constantly decreasing, the miners may decide to buy more mining machines such that their expected profit is higher. We addressed the problem by conducting a game-theoretical analysis and experimenting on the plausible choices of the weight parameter. In this work, we showed that by properly setting the weight parameter, the utility gained from purchasing new mining machines during the transition is smaller than the utility gained from keeping the original mining status. Thus, after a certain number of PoS epoch, the miners stop mining eventually, which leads to a pure PoS blockchain.

In the sections that follow, we begin by we introducing two foundational elements of our proposed solution. The first component is the Ouroboros-Praos [2], a PoS protocol that forms the core of the hybrid consensus mechanism known as Minotaur [3]. We then detail the principal concept behind Minotaur. In Section 3, we

BSCI:'24, July 2, 2024, Singapore, Singapore

ACM ISBN 979-8-4007-0638-7/24/07
https://doi.org/10.1145/3659463.3660017

[1] https://digiconomist.net/bitcoin-energy-consumption
[2] https://www.cnet.com/personal-finance/crypto/

define and formalise the models necessary for our analysis. The methodology for selecting the weight parameter is discussed in Section 4. Finally, we conclude with a brief summary of our findings and point out the future works.

2 BUILDING BLOCKS

2.1 Ouroboros Praos

Network Model. The Ouroboros-Praos [2] protocol assumes semi-synchronised network, in which the time is divide into discrete units called slots. A sequence of consecutive R slots are grouped together to form an epoch, where the epochs are independent of each other (i.e., there is no overlapping of slots between two adjacent epochs). At the beginning of the epoch e_j for $j \geq 2$, the stake distribution, denoted as $\mathbb{S}_j$, will be drawn from the most recent block with the time stamp up to $(j-2)R$ as reflected by the local chain of the stakeholder. The stake distribution remains static for the entire epoch.

Key Pairs. Each stakeholder U_i in the system holds three pairs of keys with distinct functionalities.

(1) VRF Keys $(sk_i^{\mathsf{VRF}}, pk_i^{\mathsf{VRF}})$. The pair of the VRF keys is used to generate/verify the VRF output y and the proof π.
(2) Block Keys $(sk_i^{\mathsf{KES}}, pk_i^{\mathsf{KES}})$. The pair of the block keys is used to generate/verify the signature of the block if U_i is the block proposer.
(3) Transaction keys $sk_i^{\mathsf{DSIG}}, pk_i^{\mathsf{DSIG}}$. The pair of transaction keys is used to generate/verify the signature of the transaction initiated by U_i.

PoS Threshold. Assume the stake of U_i is s_i and the total stake in the system is α_S. Then, the relative stake of U_i is defined as $\beta_i = s_i/\alpha_S$. Suppose the VRF has output length ℓ (in bits), the threshold of U_i is defined as $T_i = 2^\ell \cdot P_i$ where $P_i = 1-(1-f)^{\beta_i}$ for the active slot coefficient f. Generally speaking, the threshold decides the probability of a stakeholder to be elected as the block proposer. Since the output $y \in [0, 2^\ell]$ of the VRF is uniformly random, then the larger relative stake β_i results in higher probability of $y < T_i$.

Simplified Protocol Description. We simplify the protocol execution of Ouroboros-Praos as follows.[3]

- **Initialisation.** The protocol is initialised with a genesis block which consists of the initial stake distribution $\mathbb{S}_0$ (defined in Equation 1) and a random string η_0:

$$\mathbb{S}_0 = \Big((U_1, pk_1^{\mathsf{VRF}}, pk_1^{\mathsf{KES}}, pk_1^{\mathsf{DSIG}}, s_1^0), \ldots, (U_n, pk_n^{\mathsf{VRF}}, pk_n^{\mathsf{KES}}, pk_n^{\mathsf{DSIG}}, s_n^0)\Big) \quad (1)$$

- **Chain Extension.** For each new epoch e, U_i defines the stake distribution $\mathbb{S}_e$ (as described in Network Model) and a new randomness η_e that is the output of a hash function (modelled as a random oracle) on input the concatenation of VRF values recorded in the blocks of the prior epoch. U_i decides if it is the block proposer by computing the VRF output y and the corresponding proof π. If $y < T_i^e$, then U_i propose a new block $B = (st, d, sl_e^j, B_\pi, \sigma)$, where st denotes the internal state (i.e., the hash output of the leading block in the longest chain), $d \in \{0,1\}^*$ denotes a set of transactions, sl_e^j denotes the current time slot for $1 \leq j \leq R$, $B_\pi = (U_i, y, \pi)$ denotes the VRF output and corresponding proof, and the signature σ is the signature on message (st, d, sl_e^j, B_π) generated by block keys of U_i. Next, U_i appends the block B to the longest chain C and broadcasts the updated chain to the network.

[3]The description aims to provide a high-level overview of the protocol execution. It omits the selection of the longest chain, the validation of previous blocks, block pruning, and signing transactions.

2.2 Minotaur

We apply Minotaur consensus protocol [3] as the backbone of our approach in order to enable a smooth transition from the PoW-based blockchain to the PoS-based blockchain. Minotaur protocol involves two types of participants, PoW miners and PoS stakeholders, where the relation among the sets of miners and stakeholders can be arbitrary. In a nutshell, the mining of blocks in Minotaur follows the PoS "lottery" mechanism, however, the threshold of each system user depends on *virtual stake* which fuses the real stake and work stake. Hence, alongside the PoS blocks in the main chain, there are PoW blocks (or endorser blocks) that are mined by those who have computing powers according to the rules in PoW chain. Note that the only functionality of PoW blocks is to determine the work stake fairly. Thus, PoW blocks will not carry any transactions in the system. We describe the protocol of Minotaur which uses Ouroboros-Praos [2] as the building block as follows.[4]

Minotaur Protocol in Combination of Ouroboros-Praos.

- **Initialisation.** Define a weight parameter $\omega(e)$ that can be hard coded in the genesis block. The PoS threshold of each user U_i is determined proportional to its relative *virtual stake* which is defined as follows. Suppose U_i has relative mining power β_i^W and relative stake distribution β_i^S, then its relative virtual stake is $\beta_i^V = \omega(e)\beta_i^W + (1-\omega(e))\beta_i^S$. The corresponding PoS threshold of U_i is defined as $T_i = 2^\ell \cdot P_i$ where ℓ is the output length of the VRF and $P_i = 1-(1-f)^{\beta_i^V}$.
- **PoW mining.** In slot sl_e^j for $1 \leq j \leq R$, a miner U_i mines the PoW block if $H(pk_i, sl_e^j, h, mr, nonce) < T_e$, where pk_i is the public key of U_i, sl_e^j is current slot, h is the hash of the last confirmed *PoS block* that is no earlier than $sl_e^j - sl_{re}$ (i.e., sl_{re} is the recency parameter), mr is the Merkle root of the payload, and T_e is the mining target in epoch e. If U_i solves the PoW puzzle, and the PoW block is referenced by the future PoS block (i.e., in epoch $e+2$), U_i will obtain the reward in the form of the work stake which can be used to propose the main chain block in PoS block producing procedure.
- **PoS mining.** Following the Ouroboros-Praos process, while the only difference is that the threshold for each PoS stakeholder is determined by its virtual stake defined previously.

Proof of Fungible Work and Stake. The security of Minotaur [3] is guaranteed as long as the honest players in the system control a majority of the combined resources. The notion is captured by proof of fungible work and stake, which is defined as follows.

[4]Minotaur can also be initialised with Ouroboros [4] or Ouroboros-Genesis [1], we refer the readers to [3, Section 6] for more details.

Definition 1 (Fungibility of resources [3]). *For a time window W where $|W| = 2R$, let β_s^W be the maximum fraction of adversarial stake in W, where the maximum is taken over all views of all honest players across all slots in W; and let β_w^W be the maximum fraction of adversarial mining power over all slots in W. For $\theta = 1/2 - 2\sigma$ where $\sigma \in (0, 1)$, we say the adversary $\mathcal{A}$ is $(\theta, 2R, \omega(e))$-bounded if for any time window W with at most $2R$ slots, we have $\omega(e) \cdot \beta_w^W + (1 - \omega(e)) \cdot \beta_s^W \leq \theta$. We say a blockchain protocol achieves fungibility of work and stake if it is secure against such an adversary.*

It is shown that Minotaur (constructed with Ouroboros-Praos) [3, Section 6.3] satisfies persistence and liveness with overwhelming probability under the following assumptions:

(1) Honest stakeholders are always online (or at least online at the beginning of the epoch).
(2) Honest miners who mined PoW blocks in epoch e will stay online in epoch $e + 2$ (or at least online at the beginning of the epoch $e + 2$).
(3) When an honest party join the protocol, its initial chain provided by the environment should match an honest party's chain which was active in the previous slot.

Note that the original security proof in Minotaur is for static weight parameters. However, the authors gave a proof sketch shows that the security also holds for dynamic weight parameters $\omega(e)$ as long as the difference of ω between two adjacent epochs is sufficiently small. We exploit the dynamic weight parameter to enable the smooth transition from PoW to PoS.

3 MODEL

3.1 Mining Model

Participants. We assume there are totally n rational miners in the Minotaur protocol [3], who will always try to maximise the expected profit during the game. We denote the players as U such that $|U| = n$. In the beginning of the game, there are three types of players:

(1) A player $U_i \in U_S$ does not have mining power but holds a portion of real stakes to participate in the PoS block generation process.
(2) A miner $U_i \in U_W$ has mining power but none of the real stakes.
(3) A miner-stakeholder $U_i \in U_{SW}$ has both mining machines and real stakes.

Evidently, $|U_S| + |U_W| + |U_{SW}| = n$. The role of the player is not fixed. That is, the players will change its role if the expected profit of the certain role is higher than its current role.

Scheduler. The system proceeds in epochs, where at the beginning of each epoch, the scheduler asks the players to choose its actions. Let α_W^{e-2} be the total mining power at epoch $e - 2$ and α_S^e be the total stake of epoch e. Note that when $e < 2$, the mining power distribution is calculated from the original PoW chain. Then, for $U_i \in U_S$ with (real) stake s_i^e, its wining probability is proportional to $(1 - \omega(e)) \cdot \frac{s_i^e}{\alpha_S^e}$. For $U_i \in U_W$ with mining power w_i^{e-2}, its winning probability is proportional to $\omega(e) \cdot \frac{w_i^{e-2}}{\alpha_W^{e-2}}$. Similarly, for $U_i \in U_{SW}$ with mining power w_i^{e-2} and stakes s_k^e, its winning probability is proportional to $\omega(e) \cdot \frac{w_k^{e-2}}{\alpha_W^{e-2}} + (1 - \omega(e)) \frac{s_i^e}{\alpha_S^e}$. It is obvious that $\alpha_S^e = \sum_{i \in U_S \cup U_{SW}} s_i^e$ and $\alpha_W^{e-2} = \sum_{i \in U_W \cup U_{SW}} w_i^{e-2}$.

In addition to choose the PoS winner, the scheduler also chooses the PoW winner for the current epoch according to players' mining power distribution of the current epoch. In other words, for $U_i \in U_W \cup U_{SW}$, the probability of producing a PoW block is proportional to $\frac{w_i^e}{\alpha_W^e}$.

3.2 Game-Theoretic Model

Let us denote the duration of each epoch as t_e. The game starts (at epoch $e = 0$) when the PoW chain changes the underlying consensus protocol to Minotaur [3], and the game ends when no PoW miners willing to participate in mining (i.e., the system becomes a pure PoS chain). Hence, the game is a finite game, which implies that the one-time cost during the game is not negligible.

Assumptions. To simplify the analysis, we make the following assumptions of the game.

(1) The real value of a coin is constant, and we denote the block generation reward r. Note that we do not take into account the transaction fees since typically, the transaction fees do not change participants' revenue significantly.
(2) The duration of each epoch t_e is constant, which can be achieved by adjusting the difficulty parameter of Minotaur.
(3) There is no racing of blocks during the game. The assumption is reasonable since our target is to analyse the maximum profits gained by players. If there is a race, then the expected profits of players decreases (i.e., they may mine blocks that are eventually discarded).
(4) The number of blocks (both PoW blocks and PoS blocks) produced during each epoch e is constant.
(5) Different PoW miners may have different run-time costs (e.g., the electricity costs), but we assume the cost does not change throughout the game.
(6) All players can choose to purchase additional mining powers with a universal one-time cost c_o (e.g., fees for purchasing the new mining machine) which adds a unit amount of power to the system. The newly purchased mining powers effect immediately.

Strategies of players. During the game, the players can choose from the following two actions at the beginning of each epoch:

(1) S_{add} - $U_i \in U$ purchases new mining power to the system.
(2) S_{keep} - $U_i \in U$ keeps its current mining status.

Note that we assume the players do not change their strategies during an epoch (or a state). This is owning to the weight parameter which influences their profit does not change during an epoch.

Utility. Let us denote the mining cost by c_i, which is the cost incurred by player $U_i \in \{U_W \cup U_{SW}\}$ for investing unit amount of power for each time slot. During the transition, the players may add new mining power to the system. We assume the one-time cost (e.g., buying equipment) for adding unit amount of power is c_o, which is universal to all players. Therefore, for adding n_i unit amount of powers to the system, the incurred cost is $n_i c_o + n_i c_i + w_i c_i = n_i c_o + (n_i + w_i) c_i$, where w_i is the existing mining power held by

U_i. Furthermore, we define the difficulty parameter of the Minotaur protocol [3] as λ (assume the block generation rate of PoS and PoW blocks is the same for simplicity). Then, the expected profit Π_i^e of players when every one kept their mining status as follows:

(1) For players $U_i \in U_S$, $\Pi_i^e = (1-\omega(e))\frac{s_i^e}{\alpha_S^e} \cdot r \cdot \frac{t_e}{\lambda}$;
(2) For players $U_i \in U_W$, $\Pi_i^e = \omega(e)\frac{w_i^{e-2}}{\alpha_W^{e-2}} \cdot r \cdot \frac{t_e}{\lambda} - w_i^e c_i t_e$;
(3) For players $U_i \in U_{SW}$, $\Pi_i^e = \left(\omega(e)\frac{w_i^{e-2}}{\alpha_W^{e-2}} + (1-\omega(e))\frac{s_i^e}{\alpha_S^e}\right) \cdot r \cdot \frac{t_e}{\lambda} - w_i^e c_i t_e$.

The expected profit Π_i^e of the player $U_i \in U$ when deciding to purchase n_i^e amount of power at epoch e is defined as follows:

(1) If U_i was originally in U_S, $\Pi_i^e = (1-\omega(e))\frac{s_i^e}{\alpha_S^e} \cdot r \cdot \frac{t_e}{\lambda} - n_i^e c_o - n_i^e c_i t_e$;
(2) If U_i was originally in U_W, $\Pi_i^e = \omega(e)\frac{w_i^{e-2}}{\alpha_W^{e-2}} \cdot r \cdot \frac{t_e}{\lambda} - n_i^e c_o - (n_i^e + w_i^e)c_i t_e$;
(3) If U_i was originally in U_{SW}, $\Pi_i^e = \left(\omega(e)\frac{w_i^{e-2}}{\alpha_W^{e-2}} + (1-\omega(e))\frac{s_i^e}{\alpha_S^e}\right) \cdot r \cdot \frac{t_e}{\lambda} - n_i^e c_o - (n_i^e + w_i^e)c_i t_e$.

4 ANALYSIS

Recall that our target is to analyse the choice of weight parameter $\omega(e)$ in order to encourage the smooth transition from the PoW chain to the PoS chain. Therefore, we are interested in the expected profit per epoch of mining PoW blocks under different strategies. This allows us to ignore the profit gained by the PoS mining since as long as the payoff of PoW mining decreases to 0, there is no incentive for PoW miners to keep mining on the PoW blocks (but they can still enjoy the reward from the PoS mining). In the following analysis, we will assume that adopting S_{keep} achieves Nash equilibrium. Then, we explore different weight parameters so that our assumption holds. Thus, under the certain choice of $\omega(e)$, if the player U_i chooses the strategy S_{add} while all other players choose S_{keep}, its utility decreases.

4.1 PoW Utility for Each Strategy

We first analyse the conditions for a specific strategy to be the dominant strategy by comparing its utility to other strategies given the same choice of the other players. Consequently, we consider two strategies $S_{\mathsf{add}}, S_{\mathsf{keep}}$ for players $U_i \in U$. We say S_1 is more profitable than S_2 if the utility by playing the strategy S_1 is larger than the utility by playing S_2. Before we perform the analysis, let us assume the weight parameter $\omega(e) \in [0,1]$ is a discrete linear function of e which is decreasing. That is, for $e \in \{0,1,\ldots,k\}$, $\omega(e) = a \cdot e + b$ for $a < 0$ and $b = -a \cdot k$. Hence, we can write $\omega(e) = a(e-k)$. Furthermore, we can derive the relation between a and k. We know that $a \le 0$ and $0 \le a(e-k) \le 1$. Since $e \in [0,k]$, the inequalities imply that $a \ge -\frac{1}{k}$. In other words, a is bounded by $-\frac{1}{k} \le a \le 0$.

Stakeholders. For stakeholders $U_i \in U_S$, it can either add new mining power or keep the current mining status. Suppose at epoch $e_0 \in [0,k]$, the stakeholder purchases n_i unit mining power. Then, the total expected utility of PoW mining for U_i is:

$$\Pi_i^{\mathsf{add}} = \sum_{e=e_0+2}^{k}\left(\omega(e)\frac{n_i}{\alpha_W + n_i} \cdot r \cdot \frac{t_e}{\lambda}\right) - n_i c_o - (k - e_0 + 1)(n_i c_i t_e). \tag{2}$$

On the other hand, if the stakeholder $U_i \in U_S$ keeps the current mining status, then they utility of PoW mining is 0.

PoW Miners and Miner-Stakeholders. Since we only consider the utility for PoW mining, we can analyse the two types of roles at the same time. Suppose $U_i \in U_S \cup U_{SW}$ holds (existing) mining power w_i, and the player purchases n_i unit of mining power at epoch $e_0 \in [0,k]$. Then, the expected total utility of PoW mining for U_i is:

$$\Pi_i^{\mathsf{add}} = \sum_{e=0}^{e_0+1}\left(\omega(e)\frac{w_i}{\alpha_W} \cdot r \cdot \frac{t_e}{\lambda}\right) + \sum_{e=e_0+2}^{k}\left(\omega(e)\frac{w_i + n_i}{\alpha_W + n_i} \cdot r \cdot \frac{t_e}{\lambda}\right) - n_i c_o - ((k+1)w_i + (k - e_0 + 1)n_i)c_i t_e. \tag{3}$$

Correspondingly, if the player U_i choose to keep the existing mining status, the total utility of PoW mining is

$$\Pi_i^{\mathsf{keep}} = \sum_{e=0}^{k}\left(\omega(e)\frac{w_i}{\alpha_w} \cdot r \cdot \frac{t_e}{\lambda} - w_i c_i t_e\right) \tag{4}$$

4.2 Analysis of the Weight Parameter

In order to claim that the dominant strategy is S_{keep}, we need to consider the following two conditions:

- Condition 1. For $U_i \in U_S$, $\Pi_i^{\mathsf{add}} < 0$;
- Condition 2. For $U_i \in U_W \cup U_{SW}$, $D_i = \Pi_i^{\mathsf{add}} - \Pi_i^{\mathsf{keep}} < 0$.

We use Bitcoin[5] as an example for our analysis of transitions from PoW-based blockchain to PoS-based blockchain. According to our research, the current Bitcoin block reward is 6.25 BTC ($\approx 104,420.65$ USD[6]). Hence, we set $r = 104,420.65$. The average total mining power consumed for mining Bitcoin is around 88 TWh per year (i.e., 10045.66 MWh per hour), while the electricity cost for 1 MWh is 50 USD.[7] Hence, we set $\alpha_W = 10045.66$ MWh (per hour) and $c_i = 50$ since the electricity cost dominates the total costs in PoW mining. Furthermore, we adopt the epoch duration of Ouroboros[8], which is 5 days (i.e., 120 hours). Hence, we set $t_e = 120$. We set the PoW block generation time $\frac{1}{\lambda}$ as 10 minutes as in Bitcoin and the (average) unit cost for adding 1 MWh mining power to the PoW chain is $c_o = 523$ USD. Table 1 summarises the estimated values for the parameters.

4.2.1 The Choice of e_0. Now we argue the choice of e_0 (i.e., the epoch to purchase new mining power) such that the profit is maximised for rational players. That is, the players will add the new mining power if and only if the expected utility gained from the new mining power is greater than 0.

Theorem 1. *For all rational players $U_i \in U$, adding new mining power at the beginning of the game (i.e., at the epoch 0) is more profitable than adding new mining power later.*

[5] https://bitcoin.org/en/
[6] Current BTC price (18 December 2022) is 16707.3 USD
[7] https://cointelegraph.com/news/bitcoin-mining-would-cost-less-than-0-5-of-global-energy-if-btc-hits-2m-arcane
[8] https://cardano.org/ouroboros/

Parameter	Notation	Value
Block reward	r	104,420.65 USD
Average total mining power	α_W	12557 MWh (per hour)
Electricity cost per MWh	c_i	50 USD
Epoch duration	t_e	120 hours
PoW block rate	$1/\lambda$	1/6 hours
One-time cost per MWh	c_o	523 USD

Table 1: Value Estimation of the Parameters.

Proof. Let us first consider $U_i \in U_S$. For $e_0 \in [0, k-1]$, we set $e_0' = e_0 + 1$. Then, the expected utility gained from adding n_i unit amount of power at epoch e_0 is:

$$\Pi_{i,e_0}^{\text{add}} = \sum_{e=e_0+2}^{k} \left(\omega(e)\frac{n_i}{\alpha_W + n_i} \cdot r \cdot \frac{t_e}{\lambda}\right) - n_i c_o - (k - e_0 + 1)(n_i c_i t_e). \tag{5}$$

The expected utility gained from adding n_i unit amount of power at epoch e_0' is:

$$\Pi_{i,e_0'}^{\text{add}} = \sum_{e=e_0+3}^{k} \left(\omega(e)\frac{n_i}{\alpha_W + n_i} \cdot r \cdot \frac{t_e}{\lambda}\right) - n_i c_o - (k - e_0)(n_i c_i t_e). \tag{6}$$

Subtracting Equation 6 from Equation 5, we obtain the difference

$$D_i = \omega(e_0 + 2)\frac{n_i}{\alpha_W + n_i} \cdot r \cdot \frac{t_e}{\lambda} - n_i c_i t_e \tag{7}$$

Note that D_i is eventually the profit of adding n_i unit amount of power at epoch e_0 regardless of the one-time cost. Since the player U_i is rational, if $D_i < 0$, then the mining cost alone is larger than the expected revenue of the newly added power to the system. Hence, there is no incentive for U_i to purchase the power. Furthermore, as $\omega(e)$ is a decreasing function, for next epoch, the reward gained from PoW mining is strictly smaller than the current epoch while the mining cost remain unchanged. The player will only lose the money in this case. Evidently, purchasing power at epoch e_0 is more beneficial than doing so at epoch $e_0 + 1$, which implies that the maximum profit is possible when $U_i \in U_S$ purchases new mining power at epoch 0.

Now we consider $U_i \in U_W \cup U_{SW}$. Similarly, we set $e_0' = e_0 + 1$ for any $e_0 \in [0, k-1]$. The expected utility gained from adding n_i unit amount of power at epoch e_0 is:

$$\Pi_i^{\text{add}} = \sum_{e=0}^{e_0+1} \left(\omega(e)\frac{w_i}{\alpha_W} \cdot r \cdot \frac{t_e}{\lambda}\right) + \sum_{e=e_0+2}^{k} \left(\omega(e)\frac{w_i + n_i}{\alpha_W + n_i} \cdot r \cdot \frac{t_e}{\lambda}\right) - n_i c_o - ((k+1)w_i + (k - e_0 + 1)n_i)c_i t_e. \tag{8}$$

The expected utility gained from adding n_i unit amount of power at epoch e_0' is:

$$\Pi_i^{\text{add}} = \sum_{e=0}^{e_0+2} \left(\omega(e)\frac{w_i}{\alpha_W} \cdot r \cdot \frac{t_e}{\lambda}\right) + \sum_{e=e_0+3}^{k} \left(\omega(e)\frac{w_i + n_i}{\alpha_W + n_i} \cdot r \cdot \frac{t_e}{\lambda}\right) - n_i c_o - ((k+1)w_i + (k - e_0)n_i)c_i t_e. \tag{9}$$

Subtracting Equation 9 from Equation 8, we obtain the difference

$$D_i = \omega(e_0 + 2) \cdot r \left(\frac{w_i + n_i}{\alpha_W + n_i} - \frac{w_i}{\alpha_W}\right) \cdot \frac{t_e}{\lambda} - n_i c_i t_e \tag{10}$$

We first observe that $\omega(e_0+2) \cdot r \left(\frac{w_i+n_i}{\alpha_W+n_i} - \frac{w_i}{\alpha_W}\right) \cdot \frac{t_e}{\lambda}$ is the expected revenue increase for adding n_i unit amount of power at epoch e_0 while the $n_i c_i t_e$ is the corresponding cost increase. For a rational player $U_i \in U_W \cup U_{SW}$, it will always keep $D_i > 0$, since otherwise, the expected increase in revenue will be smaller than increase of the cost, which gives U_i no incentive to purchase the mining power. Similar as in previous case, $\omega(e)$ is a strict decreasing function. Hence, for the next epoch, the expected revenue increase in PoW mining will be smaller than the current epoch and the mining cost remains unchanged. Hence, purchasing power at epoch e_0 is more beneficial than doing so at epoch $e_0 + 1$, which implies that the maximum profit is possible when $U_i \in U_W \cup U_{SW}$ purchases new mining power at epoch 0. □

4.2.2 Weight Parameter Threshold for PoW Mining. Although the weight parameter may decrease to 0, but the rational miners may stop mining as soon as the weight parameter decreases to a certain threshold so that the expected utility from PoW mining is not a positive value. Note that the threshold does not depend on the choice of k and a. Let us define the utility of PoW mining for $U_i \in U_W \cup U_{SW}$ as follows:

$$\Pi_i = \omega(e) \cdot \frac{w_i}{\alpha_W} \cdot r \cdot \frac{t_e}{\lambda} - w_i c_i t_e \tag{11}$$

The threshold is $\min_{e \in [0,k]} \omega(e)$ such that $\omega(e) \cdot \frac{w_i}{\alpha_W} \cdot r \cdot \frac{t_e}{\lambda} \leq w_i c_i t_e$. We experiment on different choice of w_i, including Foundry USA (with mining power distribution 28.10%), Braiins Pool (with mining power distribution 5.48%), and KuCoinPool (with mining power distribution 0.24%)[9] and the result is shown in Figure 1.

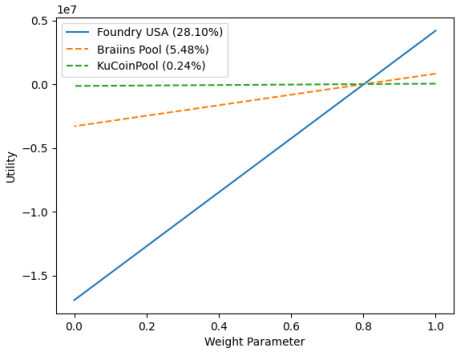


Figure 1: Threshold of Weight Parameter

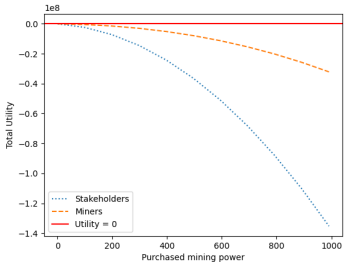
Figure 1 shows that when weight parameter decreases to 0.8, PoW mining brings no profit for miners. In the following analysis, we assume the rational players will stop mining as soon as the weight parameter $\omega(e) \leq 0.8$.

[9] https://btc.com/stats/pool

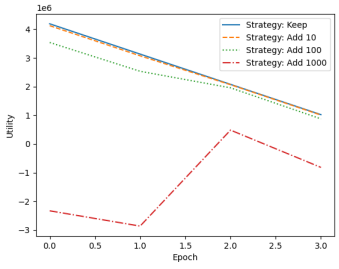
4.2.3 Choice of $\omega(e)$. As the expected utility is maximised at epoch 0, we assume the rational players $U_i \in U$ only purchase the mining power at the beginning of the game. We now find the good parameter choice for $\omega(e) = a(e-k)$ such that keeping the current mining status achieves the Nash equilibrium.

We consider the two types of players, the stakeholders $U_i \in U_S$ who do not hold any mining power before the game, and the original PoW miners $U_i \in U_W \cup U_{SW}$ who have PoW mining power before the game. In the analysis, we take the threshold of $\omega(e)$ into account, that is, we set the game starts at epoch 0 and ends as soon as $\omega(e) \leq 0.8$. We experiment on different sets of weight parameters with different choices of a and k.

Our first choice is $k = 20$ and $a = -\frac{1}{20}$. The game has duration of 4 epochs since the weight parameter will decrease to 0.8 at epoch 4, which will cause negative utility for existing miners. Therefore, the rational players will not participate in PoW mining from epoch 4, and the game ends. In Figure 2 (a) we plot the utility gained for adopting the strategy S_{add} under our choice of parameters, while Figure 2 (b) shows the utility gained in each epoch with different strategies adopted by $U_i \in U_W \cup U_{SW}$.



(a)

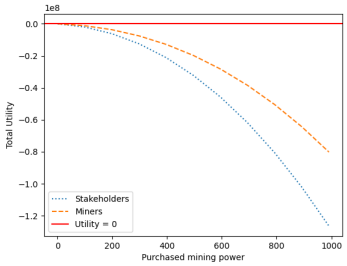


(b)

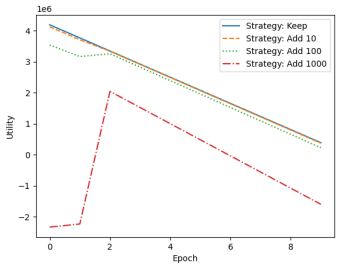
Figure 2: (a) Total Utility Gained by Adopting S_{add}; (2) Different Strategy Comparison for $U_i \in U_W \cup U_{SW}$.

We now experiment on our second choice of parameters, $k = 50$ and $a = -\frac{1}{50}$. The game has duration of 9 epochs. Figure 3 (a) shows that the utility gained from changing the strategy S_{keep} to S_{add} is not profitable for all players $U_i \in U$. Figure 3 (b) shows the utility at each epoch during the game for $U_i \in U_W \cup U_{SW}$ when adopting different strategies.

Specifically, both Figure 2 (a) and Figure 3 (a) showed that $\Pi_i^{\mathsf{add}} - \Pi_i^{\mathsf{keep}} < 0$ for $U_i \in U$. Figure 2 (b) and Figure 3 (b), on the other hand, showed that the expected profit of adopting the strategy S_{keep} is indeed larger than the profit of adopting S_{add}. Furthermore, buying more mining power for $U_i \in U_W \cup U_S$ will not lead to profit increase but only lost more money.



(a)



(b)

Figure 3: (a) Total Utility Gained by Adopting S_{add}; (2) Different Strategy Comparison for $U_i \in U_W \cup U_{SW}$.

5 CONCLUSION

In this work, we proposed a method for smooth transition from PoW-based blockchain to PoS-based blockchain by applying the state-of-art hybrid consensus protocol Minotaur [3]. We explore the possibility of weight parameters in Minotaur such that keeping the current mining status is the dominant strategy during the transition (compare to purchasing more mining power during the game). We propose to choose weight parameter $\omega(e) = -\frac{1}{20} + 1$ for a short period of transition (i.e., the transition lasts for 4 epochs) or $\omega(e) = -\frac{1}{50} + 1$ for a longer period of transition (i.e., the transition lasts for 10 epochs).

5.1 Future Works

In this paper, our primary focus is on developing a theoretical framework to facilitate a smooth transition from Proof of Work (PoW) blockchains to Proof of Stake (PoS) blockchains. The practical implementation of this system and empirical studies on the transition process represent promising directions for future research.

ACKNOWLEDGMENTS

This paper is supported by Australian Research Council (ARC) Discover Project DP220101234.

REFERENCES

[1] Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. 2018. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 913–930.

[2] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. 2018. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 66–98.

[3] Matthias Fitzi, Xuechao Wang, Sreeram Kannan, Aggelos Kiayias, Nikos Leonardos, Pramod Viswanath, and Gerui Wang. 2022. Minotaur: Multi-Resource Blockchain Consensus. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*. Association for Computing Machinery.

[4] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. 2017. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Annual international cryptology conference*. Springer, 357–388.

[5] Christian Stoll, Lena Klaaßen, and Ulrich Gallersdörfer. 2019. The carbon footprint of bitcoin. *Joule* 3, 7 (2019), 1647–1661.