Dynamic Power Control for Rational Cryptocurrency Mining

Sang-Yoon Chang
University of Colorado Colorado Springs
schang2@uccs.edu

Simeon Wuthier
University of Colorado Colorado Springs
swuthier@uccs.edu

ABSTRACT

In blockchain and cryptocurrency, miners participate in a proof-of-work-based distributed consensus protocol to find and generate a valid block, process transactions, and earn the corresponding reward. Because cryptocurrency is designed to adapt to the dynamic miner network size, a miner's participation affects the block difficulty which sets the expected amount of work to find a valid block. We study the dependency between the mining power control and the block difficulty and study a rational miner utilizing such dependency to dynamically control its mining power over a longer horizon than just the impending block. More specifically, we introduce *I-O Mining* strategy where a miner takes advantage of the block difficulty adjustment rule and toggles between mining with full power and power off between the difficulty adjustments. In I-O Mining, the miner influences the block difficulty and mines only when the difficulty is low, gaming and violating the design integrity of the mining protocol for its profit gain. We analyze the I-O Mining's incentive/profit gain over the static-mining strategies and its negative impact on the rest of the blockchain mining network in the block/transaction scalability. Our results show that I-O Mining becomes even more effective and profitable as there are greater competitions for mining and the reward and the cost difference becomes smaller, which are the trends in cryptocurrencies.

CCS CONCEPTS

• **Networks** → *Network algorithms*; • **Computing methodologies** → *Distributed computing methodologies.*

ACM Reference Format:
Sang-Yoon Chang and Simeon Wuthier. 2020. Dynamic Power Control for Rational Cryptocurrency Mining. In *3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems (CryBlock'20), September 25, 2020, London, United Kingdom.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3410699.3413797

1 INTRODUCTION

Blockchain constructs a distributed, immutable, and verifiable ledger and is the driving technology enabling cryptocurrencies to process financial transactions without relying on a centralized authority in a permissionless environment, e.g., Bitcoin and Ethereum. Underlying blockchain is the distributed consensus protocol so that all nodes agree on the transactions on the ledger without relying on a trusted third party. The most popular consensus protocol is based on proof of work (PoW). The miners participate in the PoW consensus protocol to process the transactions and are financially incentivized to do so by the block rewards, which are winnings from solving the probabilistic PoW computational puzzles and finding valid blocks. Since the block reward includes new currencies, the consensus participants generate new currencies via PoW and the consensus protocol participation is therefore called *mining*, similarly to that for extracting valuable minerals such as gold. The distributed consensus protocol is designed to be fair with respect to the miner's computational power, i.e., the greater the computational power the more likely the miner will find a valid PoW/block and earn the corresponding reward.

Because cryptocurrencies operate in a permissionless environment without pre-established trust or identity control, any node can join as a miner as long as it is capable of computing the hash-based PoW puzzle and is connected to the network. To adapt to the varying size and the power capabilities of the mining network (e.g., the miners dynamically joining and leaving the network), the consensus protocol adopts an automatic difficulty control which adapts the block difficulty level according to the overall network's mining power. If the miner network power (the aggregate hash rate) increases, the block difficulty increases accordingly so that the overall block generation rate is fixed in expectation (e.g., once every 10 minutes for Bitcoin).

The inter-dependency between the mining power and the consensus/block difficulty yields an opportunity for a sophisticated and rational miner to more intelligently control its mining power than simply choosing to either continue or discontinue its mining. The rational miner can control the mining power to influence the block difficulty. We introduce a dynamic strategy called *I-O Mining* (where the name of I-O comes from the power symbol on the power switch) providing an energy-efficient mining to mine only when the difficulty level is low. We analyze I-O Mining in the power-constrained regime (it is also incentive-compatible if the constraint is on energy as opposed to power, as discussed in Section 3) and analyze its incentive compatibility over the static strategies of mining with full power and mining with no power (the latter corresponding to no mining).

Contributions. We make the following four contributions in this paper. First, we model the dependency between mining power and consensus difficulty to analyze the miner's dynamic power control. Second, we introduce I-O Mining, a dynamic rational miner strategy. Third, we analyze the incentive of I-O Mining for energy-constrained miner (always greater reward gain than static mining) and for power-constrained miner. For the power-constrained miner, I-O mining i) yields greater reward gain than the static full-power mining in some regions and ii) is profitable with positive net profit even in some other regions where the electricity cost would have exceeded the block reward if the static full-power mining strategy

CryBlock'20, September 25, 2020, London, United Kingdom

ACM ISBN 978-1-4503-8079-9/20/09…$15.00
https://doi.org/10.1145/3410699.3413797

had been used, both of which regions occur in the lifetime of any miner. Fourth, we analyze the negative impact of I-O Mining in the blockchain scalability.

2 SYSTEM MODEL & BACKGROUND

2.1 Rational and Uncooperative Miner

We consider a miner which is *rational* (driven by its self interest in reward profit) and *uncooperative* (willing and capable to diverge from the agreed consensus protocol to game the protocol). In other words, the rational miner choose the mining strategy which is the most aligned to its incentive, i.e., the chosen strategy yields greater reward incentives than the other strategies. This is a relevant mining model because it captures and supports the typical miners driven by self interests and reward profits. In our model, therefore, an alternative mining strategy to the honest protocol compliance (such as our proposed I-O Mining) will only be utilized when it provides greater incentives and reward than honest mining. If the mining yields unfair advantage to the miner, then it negatively undermines the rewards of the other honestly behaving and protocol-compliant miners. Because of the negative impact on the others, such mining strategy also aligns with the malicious threat model (focusing on the destructive impact on other miners rather than the subject miner's self interest) including those used in related work in Section 6.

Honest mining corresponds to following the protocol and more specifically consistently mining, as opposed to selectively mining for gaming the mining process, in our case. This honest mining strategy serves as the backup mining strategy for the rational miner and will be chosen if the alternative mining strategy is not as profitable as honest mining. Honest mining corresponds to the optimal mining strategy in a one-shot static game, i.e., if only considering the current mining round and not the future rounds, then the miner will mine in that round with its full power as long as the mining is profitable in that round (the expected reward for that round is greater than the expected power cost).

2.2 Cryptocurrency Mining Model

We model the most popular cryptocurrencies for our work, such as Bitcoin and Ethereum[1]. The distributed consensus protocol is based on PoW measuring fairness in computational power (i.e., the more the power and the greater the hash rate the larger the probability of winning the block and the larger the expected reward).

PoW is a random process based on finding the input/preimage of the hash function used for the PoW algorithm, and the miners rely on brute-force search trying different nonces, which is a part of the hash function input. Finding a block via brute force is a Poisson process [12], which makes the block arrival memoryless (e.g., the probability of finding a block remains constant regardless of how long the miner has been trying). Blockchain relies on the one-way property of the hash function and the corresponding randomness of PoW brute-forcing for security.

We call between the blocks as *rounds* so that, in each round, the miners use different block headers which are dependent on the current block. We also define *adjustment periods* (or simply *periods*) which is the time-length between the block-difficulty adjustment; this adjustment period is defined by the protocol and fixed in the number of rounds, e.g., 2016 rounds for Bitcoin. Both rounds and adjustment periods (discretized in rounds) are random in physical time, e.g., in seconds, because of the aforementioned random mining process of finding the block.

The blockchain consensus protocol automatically and adaptively controls the block difficulty according to the current state in the mining network's computational power, e.g., if there are more miners and consequently greater overall hash rate and mining efforts, then the block difficulty increases. The difficulty control is inversely proportional to the total miner's power (measured by the time it took the miners to find the block as a network). In other words, the difficulty of the impending period is determined by the time duration of the previous period.

We also assume that the mining hardware is designed for specific coins, e.g., the mining-dedicated ASICs are designed for specific function and algorithm computations, disabling coin hopping (discussed in Section 6) in many real-world mining implementations.

To put these in to real-world implementation perspectives and provide an example, in Bitcoin, the period is 2016 rounds and, in expectation, each round takes 10 minutes and each period takes 2 weeks. Bitcoin is designed to keep these time durations constant despite the advancing technology and the varying number of participating miners. To achieve such design, Bitcoin adjusts the block difficulty so that the mining threshold increases if the last period was less than 2 weeks and decreases it if it was longer than 2 weeks, and the amount of the difficulty adjustment is according to the difference of the period duration and the targeted 2-week duration.

2.3 System Model Parameters: α, τ, T, ${}^{n}T$, U, R, C, and c

This section builds on Section 2.2 and defines the relevant parameters for our model and analyses. We focus only on the parameters which are needed for our analyses for simpler presentation, and the parameters are either controlled by or dependent on the mining strategy. For example, we normalize our reward-related variables by the reward amount so that a reward of 1 indicates the full reward amount (comprised of the block's new currency and the transaction fees) regardless of its absolute amount.

The miner has a computational power of α which is normalized with respect to the entire mining network's power. By the design of PoW (computationally fair regardless of the number of accounts/public keys), the attacker's expected reward is also α, normalized by the block reward amount in that round, if all of the miners behave honestly. Since the miner has α power, the rest of the miner network has $1 - \alpha$ power.

We study the case where the attacker may not utilize its full power capability. Given its power capability of α, the miner can use a τ fraction of the power capability, i.e., the miner uses $\tau\alpha$ power. Before this research paper and a few prior work [2, 16], it has been believed that the miner will use all of its power capability to maximize the reward (which is that of honest mining and $\tau = 1$) as long as the mining process is profitable (yielding greater block rewards than the electricity costs). While α is given after installing the hardwares and setting up the mining rigs, τ is fully controllable at any

[1] Ethereum plans to transition to a hybrid consensus between PoW and proof-of-stake (PoS) but its research and development, preceding implementation and deployment, are ongoing [1].

given time since it indicates how much of the power capability the miner will use. We call the mining strategy *dynamic* if the miner varies and actively controls τ across rounds/blocks, i.e., a dynamic miner varies τ across rounds (while a static miner does not) and is motivated to do so because of the dependency between the previous round and the current round from the automatic block-difficulty control by the consensus protocol.

We denote the round duration for round i (the amount of time for mining block i) as T_i, e.g., $T_0 = 0$ corresponds to the genesis block and if there has been x blocks mined in the ledger so far, then $\sum_{i=0}^{x} T_i$ determines how long it took for the ledger to grow x-block long beyond the zeroth genesis block (which block sets up mining and consensus protocol but does not involve mining). There are n rounds for a period (one period equals n consecutive rounds) where n is a positive integer pre-determined and agreed by the protocol, and the period duration for period j is ${}^nT = \sum_{i=n(j-1)+1}^{nj} T_i$ and the targeted period duration by the consensus protocol is ${}^cT$. While ${}^nT$ is random (because each of the T_i is random), ${}^cT$ is constant and pre-determined by the protocol, e.g., ${}^cT = 2$ weeks in Bitcoin (i.e., Bitcoin is designed to produce blocks every two weeks on average). If the miners all behave honestly, $\mathrm{E}[{}^nT] = {}^cT$ averaged over the periods of the blockchain ledger/history. (The block difficulty of that period, also very relevant to our model, does not require an additional variable because it is simply inversely proportional to ${}^nT$ by the automatic difficulty control in the consensus protocol design as described in Section 2.2. In other words, if block difficulty is denoted with D, then $D = \frac{b}{{}^nT}$ where b is a protocol-given constant.)

The miner's objective is to increase its reward profit rate, which is equal to the expected block reward per time minus the power cost consumed for running the PoW mining. We denote this rate utility function (U) as the difference between the expected block reward (R) and the power cost of mining (C), i.e., $U = R - C$. If the miners behave honestly, $R = \alpha$ by the design of PoW (computationally fair). We measure U, R, C per period (which is n number of rounds) while α, c are per round, because our dynamic mining strategy changes its control for every period as opposed to for every round. To quantify the cost of mining with respect to the miner's computational power, we introduce c which is the ratio between the cost C and the reward R given that the miners comply to the protocol and use their full power, i.e., $C = c \cdot R = c \cdot n\alpha$ if $\tau = 1$. In other words, assuming honest mining, c indicates the fraction of the reward which is used for the electricity/power cost while $1 - c$ indicates the fraction of the reward corresponding to the gross profit. c is constant given α. Thus, the utility function in expectation assuming honest mining is: $U = R(1 - c)$.

To recap, while α is given from the miner's capability (e.g., the investment amount for setting up the mining facilities and capabilities) and c is given from the electricity cost of the mining setup/hardware, τ is fully controllable by the attacker and determines T_i (and thus ${}^nT$), R and C. The consensus protocol provides the fixed n and ${}^cT$.

2.4 Power Cost Model: C

While c is fixed and is defined given $\tau = 1$ (assuming the miner will use all of its power for mining), the power cost C depends on the miner's processing utilization for the PoW hash rate, τ. Due to its importance in our analyses in Section 4, we establish the power cost model in this section. The power cost C monotonically grows between the power-off of $\tau = 0$ and the full-power of $\tau = 1$, the latter at which the cost reaches its maximum of $C_{\max} = c \cdot \alpha$. In addition, there is a positive *base cost*[2] (which is the power cost when the device is turned on but is otherwise resting) even when there is no mining and $\tau \to 0$, and the power grows linearly with the processing/hash rate from the base cost to $c\tau$.

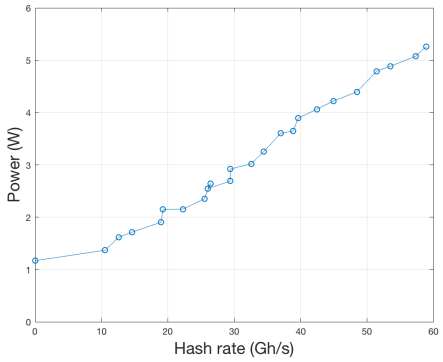

Figure 1: Power vs. hash rate in our ASIC mining experiment

To validate our power cost model, Figure 1 shows our experimental result on ASIC hardware for Bitcoin mining (GekkoScience NewPac based on Bitmain's BM 1387 ASIC chip). The hash rate is controlled by the clock frequency (the hash rate increases with the frequency) and the power was computed from measuring both the current and the voltage of the ASIC mining hardware. The computational power increases with the hash rate. From the base power cost in our measurement at 1.168 Watt, increasing the hash rate monotonically increases the power until reaching the maximum at 5.261 Watt achieving $59 \cdot 10^9$ hash computations per second. Our power model informed by our measurements corroborates with the general power model characterizing processing and power relations, e.g., [3, 14, 17].

3 DYNAMIC I-O MINING

We describe I-O Mining in this section and analyze it later in Section 4, including the incentive compatibility (greater reward than full-power mining or no mining). I-O Mining is an energy-efficient mining strategy where the miner alternates and switches back and forth between mining with full power of $\tau = 1$ in one period (power off or "I") and inactivity/no mining of $\tau = 0$ in the adjacent period (corresponding to the power off or "O"). The name of the scheme comes from the use of I-O for indicating power on and off statuses on a power switch, which symbol is ⏻. The miner will always choose $\Delta\tau = \pm 1$ for every period transition, and only one of those values are viable per transition (e.g., if $\tau = 1$, then $\Delta\tau \neq 1$ and $\Delta\tau = -1$ because $0 \leq \tau + \Delta\tau \leq 1$). Therefore, in I-O Mining, the miner chooses $\Delta\tau = -1$ to transition from the I state ($\tau = 1$) to the O state ($\tau = 0$) and chooses $\Delta\tau = -1$ for the transition in the reverse direction.

[2]The base cost is platform-dependent and can be as large as 60% for laptops, 48% for single-board computers (e.g., Raspberry Pi), and 3.5% for power-efficient embedded platforms [3].

I-O Mining leverages the fact that the miner contributes to the mining (and the overall network's hash rate) and therefore affects the period duration. The rational miner can control the computational power it uses for one period to influence the period duration (shift the distribution) and therefore the block difficulty of the upcoming period (which is inversely proportional to the aforementioned period duration the miner influenced). Given a finite energy constraint, I-O Mining maximizes the reward because it maximally shifts the difficulty to be the lowest/easiest and then consumes energy only in those periods.

However, unless our aim is to reduce the energy use (e.g., green computing), a more typical miner is supported by an electricity infrastructure with practically unlimited energy but a finite-bound cost in power (cost per energy use). In such case with unlimited energy but finite power cost, the miner will be interested in maximizing the utility U over time. Therefore, we investigate the incentive of the I-O mining strategy in a power-limited regime (with limited power cost and limited computational power/hash rate but infinite energy), e.g., the miner has no externally influenced, foreseeable time/energy limit in participating in mining.

4 I-O MINING ANALYSES

We build on our system model in Section 2 and analyze I-O Mining in this section. We analyze the effect, superiority over honest mining (no gaming), and profitability of I-O Mining. In this section, we achieve the following significant results. First, we identify the region/condition where I-O Mining outperforms $\tau = 1$. Second, we quantify the reward-profit gain. Third, we study when I-O Mining is profitable (greater reward than cost and therefore better than disabling mining altogether) and show that it is profitable even in some cases where the electricity cost would have exceeded the expected reward if the miner had adopted honest mining, i.e., $c > 1$.

4.1 τ Control and Effect

Dynamic miner controls τ to control the hash rate and the power of the miner. The miner's τ affects the expected period duration, $\mathrm{E}[{}^{n}T]$ and the block difficulty for the next period (inversely proportional to the previous ${}^{n}T$). Since the block difficulty for the upcoming period is only dependent on the last period (and not the periods before), we investigate the effect by changing the miner's control parameter by $\Delta\tau$ in the upcoming period. In other words, the miner changes from τ to $\tau+\Delta\tau$ between the periods where $0 \leq \tau+\Delta\tau \leq 1$.

Before the miner changes its hash rate by $\Delta\tau$, the consensus protocol adjusts the block difficulty so that $\mathrm{E}[{}^{n}T] = {}^{c}T$ for the round if the miner kept its hash rate power of τ (no change and $\Delta\tau = 0$). However, the miner changing its hash rate by $\Delta\tau$ affects the actual period duration to become:

$$\mathrm{E}[{}^{n}T] = {}^{c}T\frac{1-\alpha+\alpha\tau}{1-\alpha+\alpha(\tau+\Delta\tau)} \tag{1}$$

If $\Delta\tau > 0$, then the period duration decreases and, if $\Delta\tau < 0$, then the period duration increases in expectation. (At the end of this period, the block difficulty gets adjusted by $\left(\frac{1-\alpha+\alpha\tau}{1-\alpha+\alpha(\tau+\Delta\tau)}\right)^{-1}$ so that, in the next period, $\mathrm{E}[{}^{n}T] = {}^{c}T$ if the total mining power remains the same at $1-\alpha+\alpha(\tau+\Delta\tau)$.)

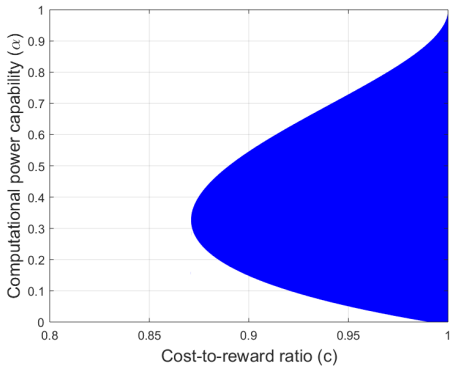

Figure 2: (c, α)-region for I-O Mining

While the miner reward is $R = \alpha\tau$, the expected power cost, C monotonically increases with ${}^{n}T$ and therefore decreasing τ by $\Delta\tau$ reduces both the reward and the cost.

4.2 Superiority: Comparison with Static $\tau = 1$

In this section, we compare I-O Mining and the static mining of $\tau = 1$, which corresponds to honest mining with no gaming. In the next section of Section 4.3, we study the profitability and compare it with the no-mining case of $\tau = 0$.

The utility of the static mining of $\tau = 1$ is the following:

$$U_{\tau=1} = R_{\tau=1} - C_{\tau=1} = n\alpha(1-c) \tag{2}$$

where the miner is expected to earn block rewards of $n\alpha$ and consume nc for the electricity cost in each period.

The utility of the I-O Mining is the weighted average between the I-state mining (yielding R_I and C_I) and the O-state mining (yielding R_O and C_O);

$$\begin{aligned} U_{\mathrm{IO}} &= \frac{\mathrm{E}[{}^{n}T]\Big|_{\Delta\tau=1}(R_I - C_I) + \mathrm{E}[{}^{n}T]\Big|_{\Delta\tau=-1}(R_O - C_O)}{\mathrm{E}[{}^{n}T]\Big|_{\Delta\tau=1} + \mathrm{E}[{}^{n}T]\Big|_{\Delta\tau=-1}} \\ &= \frac{{}^{c}T(1-\alpha)\cdot n\alpha\left[1-c(1-\alpha)\right]}{{}^{c}T(1-\alpha)+\frac{{}^{c}T}{1-\alpha}} \\ &= \frac{(1-\alpha)^2\cdot n\alpha\left[1-c(1-\alpha)\right]}{(1-\alpha)^2+1} \end{aligned} \tag{3}$$

where $\mathrm{E}[{}^{n}T]\Big|_{\Delta\tau=1} = {}^{c}T(1-\alpha)$ and $\mathrm{E}[{}^{n}T]\Big|_{\Delta\tau=-1} = \frac{{}^{c}T}{1-\alpha}$ from Equation 1; $R_I = n\alpha$ (by computational fairness) and $C_O = c\alpha\mathrm{E}[{}^{n}T]\Big|_{\Delta\tau=1}$ (reducing the energy cost); and $R_O = C_O = 0$ since power off.

The reward-profit gain for I-O Mining over the static strategy of always-full-power mining is $U_{IO} - U_{\tau=1}$, i.e., the difference between Equation 3 and Equation 2. The exact values for I-O Mining's gain over the static $\tau = 1$ depends on the miner setup, including its computational power capability (α) and the cost-to-reward ratio (c), and the period duration in the number of blocks/rounds (n).

Comparing the two yields the region where I-O Mining outperforms mining with full power.

Theorem 1. *A miner is incentivized to launch I-O Mining over full-power mining if* $\alpha^3 - 2\alpha^2 + \alpha + 1 - \frac{1}{c} > 0$.

Proof. Using Equation 2 and Equation 3, $U_{IO} - U_{\tau=1} > 0$ yields $\alpha^3 - 2\alpha^2 + \alpha + 1 - \frac{1}{c} > 0$. □

Theorem 1 provides a (c, α)-region where I-O Mining outperforms the static mining of $\tau = 1$. As a corollary, I-O Mining is more relevant (reward gain over full-power mining) when c is closer to 1, i.e., the electricity cost is closer to the reward, not leaving much profit. More specifically, if $c < 0.871$, then I-O Mining is always suboptimal compared to full-power mining. Figure 2 shows the (c, α)-region where I-O Mining outperforms honest mining.

4.3 Profitability: Comparison with Static $\tau = 0$

We investigate the profitability of I-O Mining where mining is *profitable* if it yields greater utility function than that when there is no mining and power is off (in which case, the utility function is zero since there is no reward and no cost). For the static mining of $\tau = 1$, using Equation 2, $U_{\tau=1} > U_{\tau=0} = 0 \iff c < 1$, which is also intuitive by the definition of c.

For I-O Mining, we establish that the upper bound for the cost-to-reward ratio, given $\tau = 1$, c is even greater than one.

Theorem 2. *I-O Mining is profitable if* $c < \frac{1}{1-\alpha}$.

Proof. Using Equation 3, $U_{\mathrm{IO}} > 0$ yields $c < \frac{1}{1-\alpha}$. □

Theorem 2 provides an upper bound for c to make I-O Mining profitable (positive profit gain over no mining), and the upper bound is greater than or equal to one, i.e., $\frac{1}{1-\alpha} \geq 1$ (equality holds when $\alpha = 0$). This theorem is significant since it establishes that I-O Mining is incentivized over not mining even if the cost-to-reward ratio is greater than one (i.e., the electricity cost would have been greater than the expected reward if the static full-power mining had been used), because the miner manipulates the block difficulty in order to mine in an energy-efficient manner and decrease the expected duration for mining.

4.4 Negative Impact on Overall Blockchain

I-O Mining hinders the transaction scalability and reduces the block generation rate of the overall blockchain network than the static honest mining (no gaming), even though the strategy can increase the subject miner's own reward.

Theorem 3. *I-O Mining yields smaller overall block generation rate than honest mining with full power.*

Proof. The expected period duration in Equation 1 is convex with respect to $\Delta\tau$. Jensen's Inequality yields that I-O Mining takes longer to produce the same number of blocks than the static-mining case where $\tau = 0.5$ and $\Delta\tau = 0$ (static mining using half the power capability) in expectation. The static-mining case where $\tau = 0.5$ and $\Delta\tau = 0$ takes longer to produce blocks than the static-mining case of $\tau = 1$ and $\Delta\tau = 0$ (honest mining with full power) in expectation. □

5 PRACTICALITY OF I-O MINING

In Section 4, we show that I-O Mining is better than the static strategy of $\tau = 1$ (honest mining and no gaming) and is profitable (better than the static strategy of $\tau = 0$). Theorem 1 provides that I-O Mining is more relevant (greater incentives than $\tau = 1$) as c grows larger, and Theorem 2 yields that I-O Mining is profitable even when $c > 1$ and up to $c < \frac{1}{1-\alpha}$. Therefore, I-O Mining becomes increasingly practically relevant (i.e., the miner will launch I-O Mining over either $\tau = 1$ or $\tau = 0$) as the cost-to-reward ratio c (given the ordinary mining of $\tau = 1$) increases.

In mining in practice, c generally increases with time in the lifetime of a miner as there are increasing competitions and technological advancements, increasing the block difficulty and the per-miner computational effort. Therefore, once setting up the miner, c generally increases until the miner eventually becomes outdated and no longer competitive compared to the overall miner network. Furthermore, cryptocurrencies decrease the block rewards to limit the new currencies to provide a stable currency and avoid the risk of hyperinflation; e.g., Bitcoin has a scheduled plan for such implementation to decrease the new Bitcoins to circulation and, more specifically, halves new currency in its amount every 210,000 blocks (or 4 years) until it reaches 21 million BTC cap (no more new currency afterward); such decrease in block reward increases c in the lifetime of a miner. As c increases, our work provides a region when the profit-seeking miner will switch to I-O Mining for maximizing its reward in Theorem 1. As c increases, I-O Mining also prolongs the profitability and therefore the validity/use of the mining setup in Theorem 2 before permanently shutting down the miner (equivalent to $\tau = 0$).

6 RELATED WORK IN BLOCKCHAIN MINING

Previous literature in blockchain investigates the incentive compatibility of the PoW distributed consensus protocol. In the seminal Bitcoin paper, Nakamoto designs the PoW-based consensus protocol to be incentive compatible (so that the rational attacker's strategy reduces to protocol compliance) as long as the rational miner's computational power is less than 50% the network's [12]. If not, the miner compromising majority of the network's computational power can launch the 51% attack and can revoke transactions for double spending. The mining incentives driving participation are therefore critical in reducing the security risk because greater participation in the consensus protocol increases the barrier for attack feasibility. Since the seminal Bitcoin paper, other mining strategies has emerged which violate the PoW protocol and are incentive compatible (earning greater reward profits). These strategies are based on withholding/controlling the timing of the blocks, including selfish mining [5, 6] and block withholding [4, 6, 8, 10, 13]. Ongoing research includes lightweight and deployable countermeasures to these strategies, e.g., [13, 15], and the next-generation consensus protocols informed by these strategies, e.g., [1].

Particularly relevant to our work studying the PoW mining incentives are those investigating the impact of the adaptive difficulty for mining. Although the mining protocol is generally designed to be robust against a mining attacker with respect to the dynamic difficulty [7], the coin-flipping attack switches between two coins so that the going back and forth enables the miner to mine both coins when they have lower difficulty [11]. Such strategy, however, assumes that the attacking miner can choose different coins, which is generally not supported by the mining hardwares, especially those based on application-specific integrated circuits (ASIC's) which boast significantly larger power and hash rates than GPU's or CPU's. Barring few exceptions (e.g., a mining hardware can be used between Bitcoin and Bitcoin Cash [9]), the mining hardwares

are designed and fabricated for specific coins (and often for specific pools) and therefore support specific/fixed coin. Our work therefore does not require or consider coin-hopping capabilities (which can involve hardware-based switching and engineering expertise), in contrast to these previous research.

Other researchers investigate the emerging mining strategies and the incentive issues of the current consensus protocols as the block reward transitions to only variable transaction-fees (as opposed to also including the base fees that generate new currencies) [2, 16]. The variance of the block reward amount incentivizes the attackers to selectively mine the blocks in time (e.g., there are "mining gaps" when the attackers decide not to mine). Although related, our work is orthogonal to these issues since I-O Mining maximizes the reward advantage given the block reward amount, e.g., our analyses normalizes the reward with respect to the block reward amount. Also, while these prior work analyzes the strategy within a round (transaction fees vary in time within a round), our work focuses on the inter-rounds across blocks where the dependency across the rounds exist due to the difficulty control. The decrease in the base fees (for generating new currencies), however, would actually further motivate I-O Mining because it can reduce the gap between the reward and the power cost, as investigated in Section 4.

7 CONCLUSION & FUTURE WORK

This paper studies dynamic mining for rational miners in PoW blockchain. I-O Mining toggles between the I-state (mining with full power) and O-state (power off) in order to be energy-efficient by taking advantage of the dependency across blocks arising from the block-difficulty adaptation of the cryptocurrency protocol. The absence of mining in the O-state lowers the block difficulty and therefore makes the mining in the I-state that much more efficient. Our results indicate that I-O Mining can also be power-efficient (yield greater profit per time given unlimited electrical energy supply) and outperform the static full-power mining (which has been known to be incentive compatible until our work). I-O Mining is especially effective when the mining setup is generally low in gross profit (i.e., the cost is relatively high compared to the earnings from the block reward) and can prolong the use and the profitability of the mining equipment, including some mining rounds where the electricity cost would have exceeded the block reward if the miner had used static full-power mining (protocol compliance with no gaming). I-O Mining introduces a strategy gaming the blockchain mining, violating the design integrity of blockchain/cryptocurrency, and hindering the transaction scalability.

Our paper informs the blockchain and cryptocurrency research of dynamic rational mining, and we urge the research community to better align the consensus protocol participation incentives. There are multiple potential directions for future research. First, the system model can incorporate other relevant mining factors to analyze their impacts on mining for a greater systems analysis. For example, the model can capture the miner hardware/setup decreasing in competitiveness with respect to time or combine dynamic mining with other rational mining strategies, such as those in Section 6. Second, the dynamic mining analyses can improve, e.g., the Nash equilibrium analysis or generalizing the power control for finer granularity beyond the binary option of on or off. Third, to provide solutions for resolving the rational miners gaming the system, the potential countermeasures can include: a more sophisticated algorithm for adjusting the block difficulty (such as period control or different weight allocations for each blocks), a novel reward distribution scheme, and a chain-level monitoring scheme based on reward/block behavior.

ACKNOWLEDGMENT

This material is based upon work supported by the National Science Foundation under Grant No. 1922410. This research is also supported in part by Colorado State Bill 18-086. We would also like to thank the anonymous reviewers for their helpful feedback.

REFERENCES

[1] V. Buterin, D. Reijsbergen, S. Leonardos, and G. Piliouras, "Incentives in ethereum's hybrid casper protocol," *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2019. [Online]. Available: http://arxiv.org/abs/1903.04205

[2] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the instability of bitcoin without the block reward," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16. New York, NY, USA: ACM, 2016, pp. 154–167. [Online]. Available: http://doi.acm.org/10.1145/2976749.2978408

[3] S.-Y. Chang, S. L. S. Kumar, B. A. N. Tran, S. Viswanathan, Y. Park, and Y.-C. Hu, "Power-positive networking using wireless charging: Protecting energy against battery exhaustion attacks," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '17. New York, NY, USA: ACM, 2017, pp. 52–57. [Online]. Available: http://doi.acm.org/10.1145/3098243.3098265

[4] S.-Y. Chang, Y. Park, S. Wuthier, and C.-W. Chen, "Uncle-block attack: Blockchain mining threat beyond block withholding for rational and uncooperative miners," in *Proceedings of the 17th International Conference on Applied Cryptography and network Security*, ser. ACNS'19, 2019.

[5] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *CoRR*, vol. abs/1311.0243, 2013.

[6] S. Gao, Z. Li, Z. Peng, and B. Xiao, "Power adjusting and bribery racing: Novel mining attacks in the bitcoin system," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS'19. New York, NY, USA: Association for Computing Machinery, 2019, p. 833?850. [Online]. Available: https://doi.org/10.1145/3319535.3354203

[7] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol with chains of variable difficulty," in *Advances in Cryptology – CRYPTO 2017*. Springer International Publishing, 2017, pp. 291–323.

[8] J. Ke, P. Szalachowski, J. Zhou, Q. Xu, and Z. Yang, "Ibwh: An intermittent block withholding attack with optimal mining reward rate," in *Information Security*, Z. Lin, C. Papamanthou, and M. Polychronakis, Eds. Cham: Springer International Publishing, 2019, pp. 3–24.

[9] Y. Kwon, H. Kim, J. Shin, and Y. Kim, "Bitcoin vs. bitcoin cash: Coexistence or downfall of bitcoin cash?" in *2019 2019 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, may 2019, pp. 1290–1306. [Online]. Available: https://doi.ieeecomputersociety.org/10.1109/SP.2019.00075

[10] Y. Kwon, D. Kim, Y. Son, E. Vasserman, and Y. Kim, "Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '17. New York, NY, USA: ACM, 2017, pp. 195–209. [Online]. Available: http://doi.acm.org/10.1145/3133956.3134019

[11] D. Meshkov, A. Chepurnoy, and M. Jansen, "Short paper: Revisiting difficulty control for blockchain systems," 09 2017, pp. 429–436.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[13] M. Rosenfeld, "Analysis of bitcoin pooled mining reward systems," *CoRR*, vol. abs/1112.4980, 2011. [Online]. Available: http://arxiv.org/abs/1112.4980

[14] J. C. SanMiguel and A. Cavallaro, "Energy consumption models for smart camera networks," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 27, no. 12, pp. 2661–2674, Dec 2017.

[15] A. Sarker, S. Wuthier, and S. Chang, "Anti-withholding reward system to secure blockchain mining pools," in *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, 2019, pp. 43–46.

[16] I. Tsabary and I. Eyal, "The gap game," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. New York, NY, USA: ACM, 2018, pp. 713–728. [Online]. Available: http://doi.acm.org/10.1145/3243734.3243737

[17] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in *2015 18th International Conference on Intelligence in Next Generation Networks*, Feb 2015, pp. 184–191.