Mining Power Misestimation in PoW Blockchain

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

Abstract—In blockchain and cryptocurrency, a miner’s estimation of its computational power capability (relative to the overall mining network’s) is critical since it is used for profit estimation and mining control. We study the impact on the miner’s power estimation in the presence of other rational miners, such as those launching selfish mining and block withholding. Such rational mining underestimates the total network proof-of-work rate and thus overestimates the miner’s relative power. This paper introduces the novel mining power misestimation problem and analyzes its impact. Our analyses show that the incorrect estimation of the mining power yields the profit overestimation and drives the miner to actively mine when the actual expected profit is negative and that the problem/impact grows as there are greater rational miners withholding or delaying blocks. This paper informs the blockchain communities of the mining power misestimation and discusses the potential countermeasures for future work.

Index Terms—Blockchain, Cryptocurrency, Proof of Work (PoW), Mining, Selfish mining, Block withholding attack.

I. INTRODUCTION & BACKGROUND

Cryptocurrencies such as Bitcoin and Ethereum govern and process financial transactions in a decentralized environment without relying on a trusted intermediary such as a bank. Blockchain is the enabling technology for cryptocurrency and constructs a distributed ledger with irrevocable and verifiable transactions in a permissionless environment. The permissionless blockchain forgoes the pre-established trust or identity control, such as those provided by the public key infrastructure (PKI) for the Internet or other traditional networking applications, and enables the anonymity and censorship resistance in the transactions. Underlying blockchain is a distributed consensus protocol so that all participants agree on the ledger and the recent block (including the latest transactions) in a permissionless and decentralized environment. The most popular protocol for achieving such consensus is based on proof of work (PoW), which has the participants called miners execute computations to solve a hash-function-based puzzle and present the solution as proofs of their computational work. PoW is random (as long as the one-way property of the hash function holds, miners rely on brute force search for finding the valid solution) and statistically fair in computational power (the greater the computational power of a miner the greater the chance that it will find a solution). It is also a race between the participating miners, as the first miner to find the solution produces the valid block and earns the corresponding reward.

Such financial reward provides the incentives for mining and the basis for blockchain security (more specifically the irrevocability and the integrity of blockchain transactions), and the greater the participants’ computational power the more secure the blockchain. For example, the seminal Bitcoin paper [20] introduces the aforementioned PoW-based consensus protocol and defeats double-spending threats (based on selected transaction revocation) if the attacking miner does not control the majority of the computational power (51% attack). Because it becomes increasingly challenging to meet such attack requirement of computational power, the security increases as the mining network grows.

Past research work in blockchain security identified more sophisticated threats which are feasible even without compromising the majority of the network’s computational power. These threats are based on withholding blocks (delaying or discarding the found block) - including selfish mining, block withholding, and their variants - so that the miners gain an unfair reward advantage over the protocol-complying honest miners. These threats became increasingly sophisticated (often combined with other threats or through evolution of the threat mechanism itself) and are now known to provide multiple threat strategies which are incentive compatible for rational mining, i.e., yielding greater reward than protocol-complying honest mining. While often considered in the security context (because they violate the agreed protocol and undermine and sabotages other honest miners), the threats based on withholding blocks are actually more relevant and applicable than the traditional malicious-and-irrational threat model because a rational profit-driven miner will launch such threats to increase its profit as long as it is willing to diverge from the consensus protocol. Section II-A describes these threats for rational mining in greater details.

We investigate a previously unknown impact of such withholding mining strategies which are destructive to the other miners. In contrast to the prior literature focusing on the mining competition at the time (skewing the probability of winning for the block/reward which are being mined), we focus on its destructive impact on the miners in computational power misestimation (which can affect the mining operational decision for the future blocks). Such misestimation is critical to the miner operation because the computational power is used for making critical mining operation decisions, including when to stop the mining operation and which mining strategy to choose in case of a rational miner capable of changing its strategy from the set protocol. In this paper, we focus on a miner naturally aging and increasingly becoming less competitive in the mining and deciding on when to stop the mining operation since it is no longer profitable.

The rest of the paper is organized as follows. Section II identifies the causes of mining power misestimation, including the relevant rational mining strategies, while Section III
models the cryptocurrency mining and analyzes the impact of power misestimation. We then discuss about the potential countermeasure directions for future work in Section IV and conclude our paper in Section V.

II. MINING POWER MISESTIMATION CAUSES

We study the mining power misestimation in this paper. The mining power misestimation is caused by the rational mining strategies based on withholding blocks. We review such strategies and the previous research introducing or analyzing them in Section II-A and describe how they cause the mining power misestimation in Section II-B.

A. Related Work in Rational Mining Strategies

Prior research studies in blockchain security and incentives introduced rational mining strategies based on withholding blocks where the self-profit-driven miners aim to gain reward advantages by withholding the block and delaying the time of its announcement. For example, selfish mining [11], [17] withholds blocks so that the miner gets a head-start in mining the next block and only announces the block when there is another block getting propagated. Although limited in practicality by itself [21], selfish mining becomes incentive compatible and provides unfair reward gains over the honest strategy of protocol compliance when combined with the followings: the networking-based Eclipse attack [21], the exploitation of uncle rewards in Ethereum [22], the bribery attack to help win the fork race [13], or the projected future fee/subsidy composition of Bitcoin (as the transaction fees become the dominating source for block rewards) [4].

Other withholding-based mining threats involve compromising the mining pools where an attacker becomes a member of the victim mining pool but does not follow the mining protocol [23], [9]. Joining and compromising pools are generally easy because of the permissionless property (lacking the control and trust in identities) of many cryptocurrency applications, e.g., Eligius lost 300 BTC in 2014 due to such compromise. In the compromised mining pools, withholding blocks becomes the Nash equilibrium for rational miners with more sophisticated control of when to announce the withheld blocks than selfish mining [16], [7]. More specifically, rational miners can either only announce the withheld blocks when there is a third-party block getting propagated to cause a fork [16] or make use of all the withheld blocks to exploit uncle rewards (e.g., Ethereum) [7]. These mining threats are incentive compatible to the rational miners and delay the block announcement until there is another block propagation to cause forks. The miners can also further advance these strategies for greater reward gains by using dynamic strategies in power control [13] or in block-withholding timing [14] or by withholding the shares (also called partial proof of works and designed to estimate the pool members’ mining contributions for dividing the reward within the pool) [5]. In contrast to the initial block withholding threat [23] being subjected to the Miner’s Dilemma (establishing that launching attacks against one another results in the tragedy of commons and incentivizing cooperation) [10], the more recent advanced threats forgo the Miner’s Dilemma [16], [7], [13], [14], [5].

B. Rational Mining Causes Mining Power Misestimation

The witholding-based mining strategies in Section II-A are applicable to rational miners driven by their self interests. In addition to undermining and sabotaging the mining operations of the other honest, protocol-complying miners (which is why they have been studied in the context of security and fits well with the malicious threat model), the strategies are applicable to all of the miners who are profit-driven as long as they are uncooperative and willing to diverge from the set protocol.

The withholding-based mining strategies in Section II-A, including selfish mining but except for the original block-withholding attack [23], wait until another block is found to cause intentional forks, which is an event where multiple blocks are found before completing the broadcasting propagation. Such forks cause a partition in the blockchain network, a peer-to-peer-networking-based racing between the two partitions, and the discarding of the losing block. Because they cause forks, the withholding-based mining strategies do not actually contribute to the growth of the ledger and the transaction scalability/rate, e.g., the ledger will have the same length/number of blocks with or without the withholding miners. While the actual ledger growth remains the same regardless of the presence of the withholding miners, they still mine to earn credits for mining (via the intra-pool shares) and divide the finite reward by the entire mining network; in fact, the strategy yields more reward advantage than have they mined honestly, as described in Section II-A. Because a miner’s power estimation takes into account how often the miner finds a block and how often a block is found by the entire network (lacking the consideration for the rational withholding-based mining strategies), the rational withholding-based miners skew the miner’s mining power estimation to overestimate the power relative to the entire network’s. This results in a critical misestimation of the miner reward because the reward is expected to be proportional to the mining power (relative to the overall network’s mining power) by the design of the PoW consensus protocol.

III. MINING POWER MISESTIMATION IMPACT

As discussed in Section II-B, the rational mining strategies based on witholding blocks cause other miners to misestimate their powers to overestimation; the estimated power is greater than the actual relative power to the network’s. In this section, we model the mining operation and analyze the power overestimation impact. More specifically, our analyses show that the miners relying on the flawed power estimation to control its mining operation will mine even when it is not profitable, and such regions for incentive-misaligned/erroneous control increase as there are more rational miners withholding blocks.

A. Model: Computational Power and Operational Cost

The subject of our mining estimation and control is a legitimate miner following the protocol (including the timely
submission of the blocks) and contributes to the consensus with computational power of $\beta$. The miner coexists with other miners withholding blocks whose aggregate computational power is $\alpha$. $\alpha$ and $\beta$ are normalized by the entire blockchain network’s power, and $0 \leq \alpha + \beta \leq 1$ because the legitimate miner contributing $\beta$ is mutually exclusive with the other withholding miners. $1 - \alpha$ includes the legitimate miner along with others not withholding blocks and corresponds to the actual computations finding the block. $\alpha$ corresponds to the computational power for withholding, as opposed to the computational power budget of a miner or a pool capable of withholding blocks$. Previous research in Section II-A include the investigation of a miner capable of both the protocol-compliant/non-withholding mining and block-withholding mining. The optimization between the two strategies result in the hybrid approach between the two splitting the power resources and a dynamic control strategy, as opposed to just choosing either of the strategies.

Fig. 1: Mining power misestimation impact: $(c, \alpha)$-region showing the three regions depending on the miner’s decision to mine and the profitability with $U$.

$$c = \frac{1}{\alpha} \cdot \frac{1}{1 - \alpha}$$

Fig. 2: Mining power misestimation impact: the fraction of time mining with negative profit (due to power and profit overestimation) vs. the aggregate withholding power.

$\beta$ is the focus of the previous research, including those described in Section II-A. The target pool of block withholding attack which has been the focus of the previous research, including those described in Section II-A.

B. Computational Power Overestimation and Its Impact

Even though a legitimate miner’s actual computational power is $\beta$, the miner estimates its power to be $\frac{\beta}{1 - \alpha}$ since the overall hash rate measured from the blockchain using how quickly the block gets found is $1 - \alpha$. Because PoW is computationally fair, the miner expects to earn according to the perceived power estimation ($\frac{\beta}{1 - \alpha}$ fraction of block reward). Since $1 - \alpha < 1$, the estimated power (and correspondingly the estimated reward) is greater than the actual, i.e., $\frac{\beta}{1 - \alpha} > \beta$.

A miner has a profit, which is the reward minus the cost. The miner’s actual profit in expectation, $U$ is $U = \beta(1 - c)$ while its estimated profit, $\tilde{U}$ is $\tilde{U} = \beta - \beta c$, skewed from power overestimation. If $\alpha = 0$ (no withholding miners),
then $U = \tilde{U}$. As the mining rig gets older, the miner will mine until the perceived profit is positive, i.e., $\tilde{U} = \frac{\beta}{\alpha - \lambda} - \beta c > 0$, which yields $c < \frac{1}{\alpha - \lambda}$. Since the cost outweighs the actual expected reward at $c > 1$ while $\frac{1}{\alpha - \lambda} > 1$, the power overestimation introduces a $c$-region where the miner decides to mine (incorrectly estimating a positive profit) while it actually yields negative profit if $U < 0$. The cost outweighs the expected reward and yields $U < 0$ when $1 < c < \frac{1}{\alpha - \lambda}$.

Figure 1 presents the $(c, \alpha)$-regions depending on the miner decision and the expected profit. In the region where the rational miner decides to mine but experiences negative profit ($U < 0$) due to power overestimation, the damage/profit ($U$) is proportional to $\beta$ and the greater the miner’s actual power capability the greater the loss/negative in profit. Also, the range of $c$ for such region increases as there are greater withholding miners (increasing $\alpha$). The device ages with increasing $c$ (compared to the other miners’ competition) from left to right in Figure 1.

Figure 2 assumes that $c$ grows linearly in time starting from the initial cost of $c = 0.685$ [8] and shows the fraction of time which a miner spends mining within negative profitability, i.e., $U < 0$, due to the power and the profit overestimation. The miner stops mining if it estimates negative profit, i.e., $\tilde{U} < 0$. As there are greater withholding miners and $\alpha$ increases, the fraction of time which a miner spends mining with negative profitability ($U < 0$) increases. $\alpha$ can become larger if the self-profit-driven miners assume rational strategies because the Nash equilibrium is to launch the withholding attacks with the advanced strategies as described in Section II-A.

IV. POTENTIAL COUNTERMEASURES DISCUSSION

While the previous researchers focus on the unfair reward performances, we identify another critical impact of the withholding-based rational mining strategies, which challenges the integrity of the PoW design in that the incentives (critical for securing the transaction integrity) are misaligned with the actual protocol design (particularly with the timely block submissions). In this section, we describe the promising countermeasure directions against the withholding mining threats to facilitate future research and development to prevent or mitigate the misestimation of the mining power.

1) Mining Pool Reward Control: Controlling the reward distribution within a mining pool is an effective preventive measure against the more sophisticated withholding threats based on compromising a victim pool. Bag and Sakurai propose “special reward” for the block submissions [1] to distinguish between block submissions and share submissions (different weights), and Sarker et al. builds on such special reward to prevent the block withholding threats while controlling the special-reward to minimize the reward variance [24]. Such approach is not only effective but of low implementation overhead since it only requires changes on the mining pool managers and is backward-compatible to the existing mining pool implementations.

2) Advancing Designs for Share: A share is used to better estimate the mining contribution and reward split within a mining pool and corresponds to solving the same PoW computational puzzle for the blocks but only with easier difficulty (providing more PoW samples for better estimation). Similar in purpose to the oblivious transfer protocols and building on commit-and-reveal approach, oblivious share deprives the miner of the knowledge of whether it is a block or a share until it submits them [23], [12]. The attacker therefore cannot dynamically adopt the withholding-based threats which require distinguishing the share and the block before submission. While effective against the withholding-based attacks, such approach requires a protocol change (an additional exchange between the mining pool manager and the miners) and is not backward compatible (does not work with the existing system unless the protocol change/update is made) [16], [18], causing protocol/communication overheads and limiting its practicality in implementation and deployment. Another form of share control is via timestamping the shares to enforce the shares to be submitted in the order of their finding for validity [6]. Such mechanism can disincentivize the withholding attacks since it can be used to detect the delay in the block submissions.

3) Behavior-Based Detection: The withholding-based threats result in abnormal reward behaviors, such as the decreased block occurrence rate compared to the expected rate. Such abnormal behavior can be sensed and measured for detection. While we identify behavior-based detection as promising, we do not recommend relying on identity-based detection and mitigation/blacklisting mechanisms, since the identity control is absent by design of the permissionless blockchains and it is cheap for the attacker to generate multiple identities/accounts (Sybil attacks).

4) One Unified Mining Pool: A radical solution to defend against the compromise-based block withholding attack and its variants (but not against selfish mining) is to have one mining pool only so that all miners join a single pool, eliminating the notion of sabotaging/victimizing a pool. A useful platform for this can be distributed mining pools, e.g., SmartPool [19] and P2Pool, which eliminates the centralized mining pool manager and replaces it with a distributed protocol. However, despite such desirable properties, it is difficult to enforce the miners to mine at the designated pool, especially with the existing miners having already joined a pool.

5) Distributed Consensus Protocol Using Different Fairness Metric: An active research problem is to design the next-generation secure distributed consensus protocol in permissionless blockchain, such as a protocol based on proof of stake (PoS) [2], [3], [15] which is fair with respect to the stake/deposit amount in its consensus. By using a different metrics to measure fairness (in splitting the reward between the competing miners), we can de-couple the incentive and the cost of running the consensus computation/protocol. (In contrast, the distributed protocols for permissioned blockchains relying on the trust in registration and identities, such as that based on Practical Byzantine Fault Tolerance (PBFT), will present challenges to integrate them in the permissionless environments for cryptocurrencies.)
V. CONCLUSION

This paper introduces the mining power misestimation problem in permissionless and PoW-based blockchain due to the rational miners’ withholding blocks and selfish mining. While such rational mining strategies have been previously discussed to provide unfair reward advantages to the rational miner subject, we investigate a new impact of such rational mining in the power overestimation to the other miners. Overestimating the mining power, relative to the total network’s, causes a miner to make errors in its profit estimation and consequently on its mining operation decisions, such as mining when the actual expected profit is negative. Such erroneous region for mining control increases as there is an increase in the miners withholding blocks and delaying their announcements. This paper focuses on the problem, cause, and the impact of mining power overestimation and identifies potential countermeasures for future work.

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.

REFERENCES


