Pricing of Mining ASIC and Its Implication to the High Volatility of Cryptocurrency Prices*

Yoshinori Hashimoto[†] Shunya Noda[‡]

First Draft: April 8, 2019; Current Draft: April 10, 2019

Abstract

Mining application-specific integrated circuit (ASIC) is an essential facility for mining in Proof-of-Work (PoW) based blockchain systems. This paper regards ASIC as a financial asset and proposes a theoretical estimate of the pricing of ASIC. We show that the payouts from ASIC can be replicated by an integral of European call options. Hence, the value of ASIC is increasing in the volatility of the cryptocurrency price. Our results imply that miners may prefer to keep the high volatility to maintain the value of their ASIC; thus, they may refuse the proposals and innovations for stabilizing the price. In this sense, the high volatility of the PoW-based cryptocurrency price might be intrinsic.

Keywords: Blockchain, Cryptocurrency, Bitcoin, Volatility, Mining

*We are grateful to Daisuke Adachi and Jun Aoyagi for helpful comments. All remaining errors are our own.

[†] BUIDL, Ltd., Neutrino, 12-10, Sakuragaoka, Shibuya-ku, Tokyo-to, 150-0031, Japan. E-mail: yoshi.h@buidl.jp The opinions expressed in this article are Hashimoto's own and do not reflect the view of BUIDL, Ltd.

[‡] Corresponding Author. Department of Economics, Stanford University, 579 Serra Mall, Stanford, CA 94305-6072, USA. E-mail: shunya.noda@gmail.com Noda has been supported by the Funai Overseas Scholarship and the E. K. Potter fellowship.

1 Introduction

Blockchain is a novel decentralized ledger system, which enables us to keep records in a verifiable and permanent way, in the absence of the trusted central server. It was invented by Nakamoto (2008) to serve as the transaction ledger of cryptocurrency, Bitcoin. Blockchain and cryptocurrency have been attracted the attention of the industry, academia, and the public, and a number of novel applications have been proposed.

The users of a blockchain system must agree on which transactions are legitimate and are added. The Proof-of-Work (PoW) system is a classic consensus mechanism (time stamping scheme), which is invented by Dwork and Naor (1992) and applied to the design of blockchain by Nakamoto (2008). Although various alternatives have been proposed, PoW is the most popular as of 2019.[1] In the PoW system, record-keepers, who extends the record, are called *miners*. To add some additional record (e.g., new transaction data) to the blockchain, a miner must execute a computationally resource-consuming task, called the mining puzzle. This structure guarantees the blockchain system tamper-proofness: it is extremely costly (thus unprofitable) for the attacker to overturn the record. Once a miner solves the current mining puzzle, he adds some additional records to the blockchain and is rewarded with newly created coins and transaction fees. (We do not fully describe how the PoW system works in this short paper. Read Antonopoulos (2014); Narayanan, Bonneau, Felten, Miller, and Goldfeder (2016), for example.)

The probability that a miner successfully creates a new block (and obtains the reward) is proportional to his ability to solve the mining puzzle. For example, in Bitcoin, the mining puzzle is to find a parameter (nonce) with which a function (hash function) returns a number (hash value) smaller than a target value, which is adjusted over time. Here, the ability to solve the mining puzzle is equal to the hash rate: the speed to compute hash values. To achieve high-efficiency, miners naturally want to use the facility that is customized to solving mining puzzles. Such a facility is called *mining application-specific integrated circuit* (ASIC). Compared with all-purpose CPU or GPU, ASIC has much

[1] In April 2019, Bitcoin, Ethereum, Ripple, Litecoin, and Bitcoin Cash are the five largest cryptocurrencies by market capitalization. Among them, Bitcoin, Ethereum, Litecoin, and Bitcoin Cash are using the PoW system, while Ethereum is planning to switch to another consensus mechanism.

better performance.[2] Accordingly, working as a miner is virtually equivalent to running ASIC.[3] Once a miner made a long-term investment for ASIC, he can run it or pause it (when the reward for mining is lower than the variable cost, e.g., electricity cost) any time.

Miners play a crucial role for the blockchain system. To analyze the properties of PoW-based blockchain systems, we need to shed light on miners' complex profit structure and incentives for making long-term investments (i.e., to buy ASIC).

Our first contribution is to derive a formula that gives a theoretical estimate of the value of ASIC. We regard ASIC as a financial asset and show that the payouts from ASIC is equal to the payouts of a portfolio that is an integral of European call options. This is because (i) the reward for mining is paid in the mined cryptocurrency, and (ii) miners can pause mining any time if the reward is too low because of the low cryptocurrency price. Applying the Black–Scholes formula to evaluate the period-0 value of such European call options, we obtain the period-0 value of ASIC.

We also obtain an implication for the high volatility of cryptocurrency prices. Several studies have shown that the blockchain system is a promising way to mitigate asymmetric information problems appeared in traditional markets (Cong and He (2019); Aoyagi and Adachi (2019)). However, the price of cryptocurrencies has been very volatile, and this fact is one of the important reasons why cryptocurrencies are inconvenient to use as a transaction scheme.

To stabilize the price, previous studies have proposed various policy suggestions for it (e.g., Iwamura, Kitamura, Matsumoto, and Saito (2014); Saito and Iwamura (2018)). However, the value of ASIC is increasing in the volatility of the cryptocurrency price because miners can pause their ASIC at any time when the cryptocurrency price is low. Since miners, who already own and run ASIC, have the voting right to accept/reject proposed changes in the cryptocurrency protocol, the proposals for reducing the volatility

[2] In an article of Bitcoin Market Journal, Walters (2019) says "*While it is still possible to mine altcoins with a GPU (or even a CPU) these days, bitcoin and most others have gone beyond accessibility for home miners. In 2018, most mining is done using powerful ASIC (application-specific integrated circuit) rigs that have been created specifically for mining.*"

[3] The performance ratio of ASIC to GPU/CPU are different across mining puzzles. According to Yap (2018), ASIC is many thousands of times faster than GPU for the mining puzzle used in Bitcoin and Bitcoin Cash (SHA256), while it is only two to three times faster for the one used in Ethereum (Ethash).

might be rejected because such changes do not benefit miners. In this sense, the high volatility of the cryptocurrency price might be intrinsic and persistent. To our knowledge, this is the first paper to point out the incentive conflict between users and miners.

2 Asset Pricing

Consider a continuous-time environment in which there is one cryptocurrency that is based on a PoW system. We assume that the markets of the risk-free asset and cryptocurrency are thick enough that it is possible to buy and sell these assets at any time without changes. This assumption is satisfied for several popular cryptocurrencies, e.g., Bitcoin. Let $S(t)$ be the price of the cryptocurrency. We denote the annual interest rate (from the risk-free asset) by r. As in the standard Black–Scholes–Merton model,[4] we assume that $S(t)$ follows a geometric Brownian motion:

$$\begin{aligned} dS(t) &= \mu S(t) + \sigma S(t) dW(t), \\ S(0) &= S. \end{aligned}$$

We assume that ASIC is necessary for mining and useless for the other purposes. This assumption is realistic in that (i) it is virtually impossible to mine cryptocurrencies profitably with all-purpose CPU or GPU, and (ii) each type of ASIC is customized to solve a specific mining puzzle and cannot be repurposed.[5] We assume that the lifespan of ASIC is T period. For simplicity, we assume that T is deterministic.

At each moment, a miner chooses whether to run or pause ASIC. If a miner decides to pause ASIC, his instantaneous payoff is zero. If a miner chooses to run ASIC, he has to pay a variable cost of e (e.g., electricity cost), but he has a chance to create a new block and get rewarded. We assume that the miner's instantaneous expected reward is $D(t)M(t)S(t)$, where $D(t)$ denotes the Poisson intensity that a new block is found by the miner (which is proportional to the target value of the mining puzzle) at time t, and $M(t)$ denotes the amount of coins awarded for the new block creator. We assume that both

[4] Black and Scholes (1973); Merton (1973).

[5] For example, Wilmoth (2018) states "*Unlike GPU chips, which can be repurposed when mining ceases to be profitable, ASIC chips are programmed exclusively for a single application.*" in an article of CCN.

$D(t)$ and $M(t)$ are deterministic.

We have the following "microfoundation" for the above specification. In the Hashcash system (which is one of the most popular PoW systems and used in Bitcoin), a mining attempt resembles one draw of a lottery: for each mining attempt, a random number (hash value) is returned. A new block is created if a miner successfully finds a hash value smaller than the target value. Therefore, once the target value is fixed, the probability to win a new block is also determined. We define it as $D(t)$. Taking a continuous limit, it reduces to a Poisson intensity.

A miner runs ASIC if and only if the expected reward exceeds the running cost; i.e., $D(t)M(t)S(t) - e > 0$. Accordingly, the value of an ASIC at time 0 is

$$\begin{aligned} V &= \mathbb{E}_0 \left[\int_0^T \left[D(t)M(t)S(t) - e \right]_+ dt \right] \\ &= \mathbb{E}_0 \left[\int_0^T \left[S(t) - \frac{e}{D(t)M(t)} \right]_+ D(t)M(t) dt \right]. \end{aligned}$$

Recall that $[S(t) - (D(t)M(t))^{-1}e]_+$ is the payout of the European call option whose strike price is $(D(t)M(t))^{-1}e$ and expiration date is t. Holding such call options for $D(t)M(t)$ units for each $t \in [0, T]$, we can replicate the payout sequence from ASIC.

It is well-known that the European call options can be replicated from the base asset (the cryptocurrency) and risk-free asset (Black and Scholes (1973); Merton (1973)). Assuming that there is no arbitrage, the price of the call option must coincide the cost of making such a portfolio. Let $C(t)$ be the period-0 price of the European call option whose strike price is $(D(t)M(t))^{-1}e$ and expiration date is t. Then, by the Black-Scholes formula, we have

$$C(t) = S \cdot N(d_1) - \frac{e}{D(t)M(t)} \cdot \exp(-rt) \cdot N(d_2),$$

where N is the cumulative distribution function of the standard normal distribution, and

$$\begin{aligned} d_1 &= \frac{\log\left(S \cdot \dfrac{D(t)N(t)}{e}\right) + (r + \frac{1}{2}\sigma^2)t}{\sigma\sqrt{t}}, \\ d_2 &= d_1 - \sigma\sqrt{t}. \end{aligned}$$

Accordingly, the period-0 value of ASIC is

$$V = \int_0^T C(t)M(t)D(t)dt.$$

3 Economic Implications

3.1 Comparative Statics

Trivially, the value of ASIC is increasing in the reward $M(t)$ and the inverse difficulty $D(t)$. ASIC is equivalent to the portfolio that comprises a sequence of call options. The value of call options is increasing in the period-0 base-asset (cryptocurrency) price S and decreasing in the volatility of the base asset σ. However, somewhat surprisingly, it is independent of the drift rate μ. The value of ASIC inherits all of these comparative statics. Accordingly, miners do not care about whether the cryptocurrency is in uptrend or downtrend, but the volatility of the price is crucial for whether to make a long-term investment.

3.2 Intrinsic Instability

A number of papers have reported and studied the high volatility of cryptocurrency prices. See, for example, Dwyer (2015), Kristoufek (2015), Ciaian, Rajcaniova, and Kancs (2016), and Hu, Parlour, and Rajan (2018). It is also reported that the high volatility is one of the biggest barriers to the cryptocurrency's value as a currency.[6]

[6] For example, according to the survey conducted by Meter (2018), "*enthusiasts and skeptics alike agree volatility is the biggest issue surrounding cryptocurrency – almost 90 percent worry about volatility. Of those who own cryptocurrencies, 60 percent cited volatility as the most inconvenient aspect of using cryptocurrency.*"

Our result indicates that miners, who have already made significant investments for ASIC, may incur a large loss if the price of the cryptocurrency becomes less volatile. In Bitcoin, miners have the voting right to accept/reject the suggestions for chaining the core Bitcoin technology. Furthermore, their voting rights are proportional to the hash power they own.[7] Following Bitcoin, many other cryptocurrencies adopts similar policies. The proposal for reducing the volatility might be rejected by miners because it does not benefit them.

It should also be noted that, in PoW systems, miners intrinsically have the right to decide the structure of the blockchain because they can always select which block to extend. This point was already pointed out by the original Bitcoin white paper:

> *They [Miners] vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them.* (Nakamoto (2008), p.8)

Hence, it might be difficult to switch to another voting rule.

4 Conclusion

This paper proves that the payouts from ASIC can be replicated by a portfolio that comprises a (continuum) sequence of European call options. From this result, we derive a formula that gives a theoretical estimate of the value of ASIC. Interestingly, the value of ASIC is increasing in the volatility of the cryptocurrency price. Our result implies that the high volatility of the cryptocurrency price may be intrinsic in the sense that the cause lies in its design philosophy. Technological innovations for stabilizing the price may not be a breakthrough since decision-makers (miners) incur a loss from the volatility reduction.

References

Antonopoulos, A. M. (2014): *Mastering Bitcoin: unlocking digital cryptocurrencies*, O'Reilly Media, Inc.

[7] To be more precise, a proposal is accepted and labeled as *final* after 95% of the miners who have created the last 2016 blocks have supported it (BIP34).

Aoyagi, J. and D. Adachi (2019): "Economic implications of blockchain platforms," Working paper.

BIP34 (2012): "Block v2, Height in Coinbase," An active and implemented Bitcoin Improvement Proposal: https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki, last visited 04/06/2019.

Black, F. and M. Scholes (1973): "The pricing of options and corporate liabilities," *Journal of Political Economy*, 81, 637–654.

Ciaian, P., M. Rajcaniova, and d. Kancs (2016): "The economics of BitCoin price formation," *Applied Economics*, 48, 1799–1815.

Cong, L. W. and Z. He (2019): "Blockchain Disruption and Smart Contracts," *The Review of Financial Studies*, 32, 1754–1797.

Dwork, C. and M. Naor (1992): "Pricing via processing or combatting junk mail," in *Annual International Cryptology Conference – CRYPTO' 92*, Springer, 139–147.

Dwyer, G. P. (2015): "The economics of Bitcoin and similar private digital currencies," *Journal of Financial Stability*, 17, 81 – 91.

Hu, A. S., C. A. Parlour, and U. Rajan (2018): "Cryptocurrencies: Stylized facts on a new investible instrument," Working paper.

Iwamura, M., Y. Kitamura, T. Matsumoto, and K. Saito (2014): "Can we stabilize the price of a cryptocurrency?: Understanding the design of Bitcoin and its potential to compete with central bank money," Working paper.

Kristoufek, L. (2015): "What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis," *PloS one*, 10, e0123923.

Merton, R. C. (1973): "Theory of rational option pricing," *The Bell Journal of Economics and Management*, 4, 141–183.

METER (2018): "New study shows crypto volatility biggest barrier to mainstream adoption: Vast majority would like to use cryptocurrency daily but cite volatility as primary concern," https://www.prnewswire.com/news-releases/new-study-shows-crypto-volatility-biggest-barrier-to-mainstream-adoption-300756698.html, last visited 04/06/2019.

NAKAMOTO, S. (2008): "Bitcoin: A peer-to-peer electronic cash system," The Bitcoin white paper.

NARAYANAN, A., J. BONNEAU, E. FELTEN, A. MILLER, AND S. GOLDFEDER (2016): *Bitcoin and cryptocurrency technologies: A comprehensive introduction*, Princeton University Press.

SAITO, K. AND M. IWAMURA (2018): "How to make a digital currency on a blockchain stable," Working paper.

WALTERS, S. (2019): "Crypto mining: What's most profitable in 2019," https://www.bitcoinmarketjournal.com/crypto-mining-most-profitable/, last visited 04/06/2019.

WILMOTH, J. (2018): "Bitcoin miners are selling old ASICs for scrap metal as price decline hastens obsolescence," In CCN; https://www.ccn.com/bitcoin-miners-are-selling-old-asics-for-scrap-metal-as-price-decline-hastens-obsolescence, last visited 04/06/2019.

YAP, R. (2018): "ASIC resistance is still worth the fight for egalitarian mining, this time with Merkle tree proofs (MTP)," In CryptoSlate; https://cryptoslate.com/asic-resistance-is-still-worth-the-fight-for-egalitarian-mining-this-time-with-merkle-tree-proofs-mtp/, last visited 04/06/2019.