Pricing ASICs for Cryptocurrency Mining

Aviv Yaish[1] , **Aviv Zohar**[1]
[1]The Hebrew University of Jerusalem
{aviv.yaish, avivz}@mail.huji.ac.il

Abstract

Cryptocurrencies that are based on Proof-of-Work rely on special purpose hardware (ASICs) to perform mining operations to secure the system. We argue that ASICs have been mispriced by miners and sellers that only consider their expected returns, and that in fact mining hardware should be treated as a bundle of *financial options*, that when exercised, convert electricity to virtual coins. We provide a method of pricing ASICs based on this insight, and compare the prices we derive to actual market prices. Contrary to the widespread belief that ASICs are worth less if the cryptocurrency is highly volatile, we show the opposite effect: volatility significantly increases value. Thus, if a coin's volatility decreases, some miners may leave, affecting security. Finally we construct a portfolio of coins and bonds that provides returns imitating an ASIC, and evaluate its behavior.

1 Introduction

The cryptocurrency boom was heralded in 2008 with the arrival of Bitcoin [Nakamoto, 2008] which introduced the idea of a fully decentralized and distributed currency to the mainstream. Bitcoin's consensus protocol relies primarily on *miners*, who utilize Proof-of-work (PoW) to secure the currency from double spending attacks. Miners in turn are rewarded for their work via a form of computation-based lottery, yielding additional rewards the more they compute on behalf of the system. The ability to earn rewards from mining has led to an arms race in which miners have purchased increasingly efficient hardware that computes Bitcoin's PoW faster and at ever lower costs [Bedford Taylor, 2017]. Today's mining is mostly performed in large industrial scale mining farms hosting many machines, each consisting of ASICs (Application Specific Integrated Circuits) tailor-made for mining. The profits miners derive from their activity are highly volatile as they depend on Bitcoin's fluctuating exchange rate, on the amount of competition from other miners (see Figure 1), and on many other costs. Mining rigs themselves, are purchased in advance, and at significant capital expenditure. These risky returns make mining a high-risk investment and may indirectly hurt the cryptocurrency if fewer miners are there to secure it.

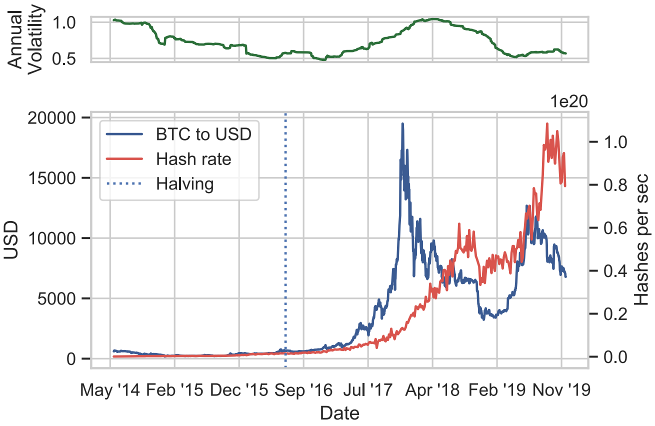


Figure 1: Bitcoin's annual volatility, exchange rate to USD and global hash-rate, as functions of time.

A naïve approach to pricing mining hardware takes into account future *expected* costs and gains. We emphasize, that such approaches, even if they account for future valuations of the currency, and for increases in mining competition, are inherently flawed. We claim that ASICs are functionally equivalent to a bundle of options that allow their owners to exchange electricity for coins at different points in time.

Our main contributions in the paper are thus to correctly model the economics of ASICs and to apply option pricing theory to price them. We thus properly account for risk which significantly affects the value of mining hardware.

We provide an algorithm that computes the value of an ASIC given its performance (power consumption and hash-rate), and market parameters such as the current exchange rate, volatility, electricity prices, the block reward and more.

Finally, we construct an *imitating portfolio* which consists of coins and bonds, and would ideally provide identical returns to an ASIC, and review its performance. Looking back at historical data, we find that our imitating portfolios outperform physical ASICs, even when we account for the fees required for portfolio maintenance.

At first glance it may seem that higher volatility in rewards implies higher risk for miners, which may devalue mining machines, but in fact, we show that mining machines *increase* in value if the cryptocurrency is more volatile, as shown for example in Figure 5. This is because, like with conventional options, if the exchange rate plummets, the losses of miners are bounded (they can always shut off their machines and avoid paying for electricity), but if exchange rates increase steeply their gains can be significant.

Anecdotal evidence suggests mining hardware is usually priced according to its *expected* returns, thus it relies on bitcoin's expected exchange rate, which doesn't take volatility into full consideration, and so does not price in risk. Thus, it is not surprising that our valuation method produces results that are different than actual market prices, as shown in Figure 2.

1.1 Related Work

Several papers explore economic and game theoretic models of mining, but most focus on the willingness of new miners to enter the market based on expected returns, and usually consider equilibria in a single shot interaction, e.g., [Arnosti and Weinberg, 2018; Dimitri, 2017]. [Dwivedi *et al.*, 2019] consider a myopic Nash equilibrium in a dynamic game model of the bitcoin market. Other works such as [Hayes, 2014; Hayes, 2017] look at mining dynamics in an economic setting where different cryptocurrencies (altcoins) co-exist. An analysis of mining in a model where miner rewards are based only on transaction fees and block rewards are negligible is carried out in [Tsabary and Eyal, 2018]. An equilibrium of miners in a bounded horizon setting is explored in [Fiat *et al.*, 2019] and [Goren and Spiegelman, 2019]. Both show that miners may in fact gain by turning ASICs on and off repeatedly, taking advantage of difficulty adjustments. An economic analysis of the security aspects of Bitcoin is performed by [Budish, 2018], arguing that when the currency is under attack, the value of Bitcoin drops and mining hardware loses value. Unlike our work, in all of the above the risk inherent in exchange-rate fluctuations and their affect on ASIC pricing is not addressed.

Mining pools, which are coalitions of miners who perform PoW together in order to get a steadier revenue-flow, are very popular [Gervais *et al.*, 2014]; thus, risk-aversion is believed to be widespread among miners. Pools were examined from an economic perspective by [Rosenfeld, 2011; Schrijvers *et al.*, 2017; Salimitari *et al.*, 2017], but those again neglected risk. An analysis that does take risk into consideration appears in [Athey *et al.*, 2016], where the price of bitcoin (and not the price of ASICs) is modeled based on user adoption and friction due to exchange rate uncertainty.

Lastly, works in the vein of [Anish Dev, 2014; Suresh *et al.*, 2018; Hanke, 2016] attempt to improve mining performance, thereby also increasing mining hardware value, but do not directly analyze said value.

1.2 Additional Details on Mining

In Bitcoin, a block is considered valid only if its hash, interpreted as a number, is under some target value. The hash function used is SHA-256, as standardized by NIST. Currently, the best known method for finding a low hash is to simply try many different pre-images by brute force.

The target value is automatically set by the protocol in order to adjust the difficulty of creating blocks to keep the creation rate constant even when more computational power is added to the network. Thus, the probability that a single miner will create a block decreases if more hash-rate is competing against it.

To encourage the creation of valid blocks, i.e. *mining*, even in the face of the ever-mounting computational effort required, Bitcoin rewards miners by allowing the creator of a block to add a *coinbase* transaction to it. This transaction creates money out of "thin-air" and transfers it to an address specified by the miner, in addition to other fees collected from each of the transactions in the block.

Single miners do not expect to find a block often, thus the majority of bitcoin mining is done in mining pools, where miners split rewards from blocks they find jointly. For this reason, miners can indeed expect small and constant returns from mining over time.

1.3 Option Pricing

A European *call-option* is a form of contract involving two parties and an underlying asset. By purchasing a call-option, the buyer receives from the seller the right to buy the asset at some agreed-upon price, the *strike price*, at an agreed-upon future date, the *expiration date*. As this is a right, not an obligation, the buyer need not exercise it if deemed unprofitable.

In 1973, Black and Scholes have published what is now called the Black-Scholes model of option valuation [Black and Scholes, 1973], a seminal work using the *no-arbitrage* argument, which argues that options should be priced such that no arbitrage possibility involving the underlying asset exists.

Using option pricing as a foundation, various financial decisions have been cast as options, for example the decision of whether to delay or abandon a project [Dixit and Pindyck, 1994], and even valuing patents and patent protected research and development projects [Schwartz, 2004]. This technique is called *real option valuation* and it underlies this work.

2 The Model

Our model divides time into discrete mining opportunities (*turns*). The model assumes a miner can either activate its hardware or leave it off for the whole duration of a single turn t. If the ASIC has a hash-rate of h hashes-per-second and the total hash-rate active on the network excluding the ASIC is $H(t)$, activation of the ASIC allows the miner to receive a fraction $\frac{h}{H(t)+h}$ of the block-reward, which is b^t coins. This is a highly accurate approximation of the reward a participant in a mining pool would receive [Rosenfeld, 2011].

Denote the ASIC's efficiency, measured in the Watt-hours required for the computation of a single mining opportunity, as e, and the cost of electricity as p_e^t, measured in dollars per Watt-hour. To model hardware failures, assume the ASIC "decays" gradually. We model this via a mortality distribution: let $M(t)$ be the fraction of ASICs that "remains" after t time units. Following [Cox *et al.*, 1979], we model the change in Bitcoin's exchange rate as a multiplicative random walk. We denote the Bitcoin-to-USD exchange rate at turn t by p_c^t, the probability for its value to rise to Δp_c^t in the next turn by q, and to fall to $\frac{1}{\delta} p_c^t$ in the next turn by $1-q$. While it may seem simplistic to assume that the price at every time unit can either go up by a factor or decrease by a factor, using sufficiently small time intervals yields a highly granular price model for longer periods. Denote the annual interest rate in the economy as $\eta > 0$, and let $r = 1 + \eta$. We assume $\frac{1}{\delta} < 1 < r < \Delta$, otherwise, risk-less arbitrage opportunities emerge, which our model assumes do not exist.

Definition 1 (The no-arbitrage assumption) *The free market adjusts asset prices such that it is impossible to outpace market gains without exposure to more risk. If such an arbitrage opportunity arises, market forces would quickly use it until a pricing equilibrium is found, thus closing the opportunity.*

We mainly deal with the following types of assets:

i. The underlying cryptocurrency.

ii. A mining opportunity, denoting its value as $V_{opp}(\cdot)$.

iii. A risk-free asset. An asset with a future return which is independent of the state of the world that is reached. Its multiplicative return is denoted as the *risk-free rate*. An example of such an asset is a government-issued bond, the value of which is denoted by B.

We assume that all these assets are traded with sufficient liquidity, a clearly defined price and that it is possible to hold a "short" position on each one of them (owing the asset to another party, equivalent to holding a negative amount of it).

Pricing a Single Immediate Mining Opportunity

Owning an ASIC gives the owner an option to activate it for each of the mining opportunities available during its lifetime; thus an ASIC's value is exactly the sum of the values of all these opportunities. Therefore, by pricing a single opportunity we can price an ASIC.

An opportunity is similar to a European call option - an ASIC's owner has the option of paying the electricity cost of activating the ASIC for the duration of the opportunity (or, in option terminology, pay the strike price), which is $h \cdot e \cdot p_e^t$, and in return receive the partial reward of $\frac{h}{H(t)+h} b^t p_c^t$. This opportunity can never be worth strictly less than zero, as a miner is not obliged to turn on its ASIC. In total, the value at time t of the t-th mining opportunity is:

$$V_{opp}\left(t, t, p_c^t\right) \triangleq \max\left(\frac{h}{H(t)+h} b^t p_c^t - hep_e^t, 0\right) \quad (1)$$

This is the *immediate* value of an opportunity offered by the ASIC. But, pricing a future opportunity is trickier, as the future exchange-rate is unknown. We shall denote the value of the t-th opportunity in relation to some time $k \leq t$, where the coin's exchange rate at k is p_c^k as $V_{opp}\left(t, k, p_c^k\right)$.

Total ASIC Value Assuming we have successfully evaluated ASIC activation for a single turn, we can proceed to calculate the value of an "entire" ASIC received at time s relative to $t \leq s$:

$$V_{ASIC}\left(s, t, p_c^t\right) = \sum_{T=s}^{\infty} M(T-s) V_{opp}\left(T, t, p_c^t\right) \quad (2)$$

Reception Delay Often, ASIC manufacturers are backlogged and either deliver ASICs to customers in the "far" future, or charge a premium for early deliveries. Assuming ASICs do not decay while in transit, the loss of receiving the ASIC at time s' instead of s relative to t is:

$$V_{ASIC}\left(s', t, p_c^t\right) - V_{ASIC}\left(s, t, p_c^t\right) \quad (3)$$

Example 1 *In a no-interest economy, a vendor offers the option of using its ASIC tomorrow for a single round. The vendor assures that if the ASIC is turned on, it will earn exactly 1 BTC (bitcoin), and will require* $\$250$ *worth of electricity.*

For this toy example, let us assume that bitcoin's value, which starts at $\$400$ *today, will either double or halve, each with equal probability of* $\frac{1}{2}$*, giving an expected exchange-rate of* $\frac{\$200+\$800}{2} = \$500$. *At a* $\$200$ *rate, activating the ASIC will result in a loss, and so a miner can earn* $\$800 - \$250 = \$550$ *only if the price increases, yielding an expected return of* $\$275$. *It is tempting to say that this is the correct price for the option, but such considerations do not take risk into account. In fact, the correct price for the mining opportunity is* $\$183.3$ *as will be shown later.*

On the other hand, assume bitcoin's random walk has a starting value of $\$400$*, but can rise to* $\$6200$ *with probability* 0.05 *and go down to* $\$200$ *with the complementary probability; the expected exchange-rate remains* $\$500$*, but the option is much* riskier - *if it is priced above* $\$0$*, money will be lost* $\%95$ *of the time. The same naïve argument from before suggests a price of* $0.05 \cdot (6200 - 250) + 0.95 \cdot 0 = \$297.5$. *According to our results, the correct price in this case is* $\$198.3$.

3 Results

Let us tackle the problem presented in the previous example in a more general case - pricing the t-th mining opportunity in relation to turn $t-1$. To do so, we shall borrow a technique from option-pricing theory (as in [Black and Scholes, 1973] and [Cox *et al.*, 1979]) where in order to price one asset, a portfolio of different assets is constructed such that the value of the portfolio at turn $t-1$ will be easy to calculate. Then, by using financial arguments we will derive the value of the asset, in our case the t-th mining opportunity.

According to the model, there are only two possible world states: one where the coin's exchange-rate has gone up relative to $t-1$ and is now Δp_c^{t-1}, and the other where it went down and is $\frac{1}{\delta} p_c^{t-1}$, thus p_c^t can be either. Denote the immediate value of the mining opportunity in the up state as:

$$V_{opp}\left(t, t, \Delta p_c^{t-1}\right) = \max\left(\frac{h \cdot b^t \Delta p_c^{t-1}}{H(t)+h} - hep_e^t, 0\right) \quad (4)$$

And of the down state as:

$$V_{opp}\left(t, t, \frac{1}{\delta} p_c^{t-1}\right) = \max\left(\frac{h \cdot b^t \frac{1}{\delta} p_c^{t-1}}{H(t)+h} - hep_e^t, 0\right) \quad (5)$$

Construct the portfolio to hold the t-th mining opportunity and a short on (a yet to be chosen amount of) c^{t-1} coins, thus its value at turn $t-1$ is:

$$\Phi(t-1) \triangleq V_{opp}\left(t, t-1, p_c^{t-1}\right) - c^{t-1} p_c^{t-1} \quad (6)$$

And at turn t is:

$$\Phi\left(t\right) = V_{opp}\left(t, t, p_c^t\right) - c^{t-1} p_c^t \tag{7}$$

The main difficulty is that at $t-1$ we do not yet know the realization of p_c^t. Given that t is in the future, this model assumes that there is some estimation for $H\left(t\right)$; Section 4 elaborates on the way such estimates were made.

Claim 1 *Shorting* $c^{t-1} = \frac{V_{opp}\left(t,t,\Delta p_c^{t-1}\right) - V_{opp}\left(t,t,\frac{1}{\delta} p_c^{t-1}\right)}{p_c^{t-1}\left(\Delta - \frac{1}{\delta}\right)}$ *coins produces a risk free-portfolio for a single turn, specifically the final turn before the mining opportunity.*

A proof is given in the full version of the paper; its main idea is that there is one degree of freedom (choosing the short amount) and we must satisfy an equation equating the value of the portfolio in both possible world states, yielding the same returns in both.

Denote the return from holding the portfolio between $t-1$ and t as $\rho\left(t\right) \triangleq \frac{\Phi(t)}{\Phi(t-1)}$. By finding a precise value for the return of the portfolio, we could extract $\Phi\left(t-1\right)$ and thus also $V_{opp}\left(t, t-1, p_c^{t-1}\right)$.

Claim 2 *If no arbitrage opportunities exist, the return is exactly the risk-free rate:* $\rho\left(t\right) = r$.

A proof is given in the full version of the paper; briefly, every other possible return is examined and shown to contradict the no-arbitrage assumption.

Corollary 1 *The value of the* t*-th opportunity at* $t-1$ *is:*

$$V_{opp}\left(t, t-1, p_c^{t-1}\right) = \frac{V_{opp}\left(t, t, \Delta p_c^{t-1}\right)}{r} + \\ \frac{V_{opp}\left(t, t, \Delta p_c^{t-1}\right) - V_{opp}\left(t, t, \frac{1}{\delta} p_c^{t-1}\right)}{\Delta - \frac{1}{\delta}} \left(1 - \frac{\Delta}{r}\right) \tag{8}$$

In the above expression, all factors are known and can be calculated at time $t-1$. *Specifically,* $V_{opp}\left(t, t, \Delta p_c^{t-1}\right)$ *and* $V_{opp}\left(t, t, \frac{1}{\delta} p_c^{t-1}\right)$ *are given by Eq. 4, 5.*

Example 2 *Following up on Example 1, Equation 8 gives a concrete price for the mining opportunity presented there, assuming the equal-probability random walk. It is even less than the naïve lower estimate given:*

$$V_{opp}\left(1, 0, 400\right) = \frac{550}{1} + \frac{550 - 0}{2 - \frac{1}{2}}\left(1 - \frac{2}{1}\right) \approx 183.3$$

3.1 Pricing Relative to an Arbitrary Time

By extending the previous method, it is possible to evaluate the opportunity relative to any point in time $k \leq t$.

Assume $k < T$. The random-walk describing the period between these turns forms a tree τ with root p_c^k and leaves $\Delta^t \left(\frac{1}{\delta}\right)^{T-k-t} p_c^k$, for every $t \in [0, T-k]$.

It is possible to calculate the values at each of the leaves, corresponding to the immediate values. Then, the method described at Subsection 3 can be used at each of the $T-k$ vertices at the $T-k-1$ level to derive the value at those world states. It is possible to continue in this manner until finally a value at the first turn is derived, as shown in Algorithm 1.

Algorithm 1: MiningOpportunityValue

```
Output: value of $T$-th opportunity relative to turn $k$.
for $p_c^T \in \{p_c : p_c \in \tau, height(p_c) = T - k\}$ do
    $V_{opp}\left(T, T, p_c^T\right) \leftarrow h \max\left(\frac{b^T p_c^T}{H(T)+h} - e p_e^T, 0\right)$
end
for $t \in T-1, \ldots, k$ do
    for $p_c^t \in \{p_c : height(p_c) = t - k, p_c \in \tau\}$ do
        $c^t \leftarrow \frac{V_{opp}\left(T,t+1,\Delta p_c^t\right) - V_{opp}\left(T,t+1,\frac{1}{\delta} p_c^t\right)}{p_c^t\left(\Delta - \frac{1}{\delta}\right)}$
        $\Phi\left(t+1\right) \leftarrow V_{opp}\left(T, t+1, \Delta p_c^t\right) - c^t \Delta p_c^t$
        $V_{opp}\left(T, t, p_c^t\right) \leftarrow c^t p_c^t + \frac{\Phi(t+1)}{r}$
    end
end
return $V_{opp}\left(T, k, p_c^k\right)$
```

Formula Looking closely at the algorithm and performing the necessary substitutions, one is able to derive an expression for the value of the T-th mining opportunity.

Theorem 1 *If the global hash-rate is exogenous, then:*

$$V_{opp}\left(T, k, p_c^k\right) = \\ = \sum_{t=0}^{T-k} \frac{\binom{T-k}{t} \gamma_{\uparrow}^t}{\left(-\gamma_{\downarrow}\right)^{k+t-T}} V_{opp}\left(T, T, \Delta^t \left(\frac{1}{\delta}\right)^{T-k-t} p_c^k\right)$$

Where $\gamma_{\downarrow} = \frac{1 - \frac{\Delta}{r+1}}{\Delta - \frac{1}{\delta}}$, *and* $\gamma_{\uparrow} = \gamma_{\downarrow} + \frac{1}{r+1}$.

A proof is given in the full version of the paper.

3.2 Imitating Portfolio

Sometimes receiving ordered ASICs promptly entails paying a hefty premium. Imitating an ASIC's revenue using a portfolio that does not include the ASIC might be better – starting to produce revenue immediately, without waiting. We show such a portfolio can be constructed using coins and bonds.

We will start by imitating the t-th mining opportunity. Denote by c^{t-1}, B^{t-1} the respective amount of coins and risk-free bonds in the portfolio at time $t-1$. Thus, the portfolio's value at time $t-1$ is $\Phi\left(t-1\right) = B^{t-1} + c^{t-1} p_c^{t-1}$, and at t it is $\Phi\left(t\right) = r B^t + c^{t-1} p_c^t$.

Theorem 2 *Assuming there are no fees for trading bonds and coins, at turn* $t-1$*, a portfolio can be constructed to be worth exactly the same as the* t*-th mining-opportunity in all possible world-states:* $\Phi\left(t\right) = V_{opp}\left(t, t, p_c^t\right)$. *The portfolio is obtained by setting* $c^{t-1} = \frac{V_{opp}\left(t,t,\Delta p_c^{t-1}\right) - V_{opp}\left(t,t,\frac{1}{\delta} p_c^{t-1}\right)}{p_c^{t-1}\left(\Delta - \frac{1}{\delta}\right)}$, $B^{t-1} = \frac{\Delta V_{opp}\left(t,t,\frac{1}{\delta} p_c^{t-1}\right) - \frac{1}{\delta} V_{opp}\left(t,t,\Delta p_c^{t-1}\right)}{r\left(\Delta - \frac{1}{\delta}\right)}$.

Proof and construction are given in the full version, and are similar to the proofs of Claims 1 and 2.

Remark 1 *Like before, this can be extended to multiple time periods, as shown in the full paper. After the initial construction of the portfolio, adjustments need to be made at every time-step, costing additional fees; these are included in the empirical evaluation.*

4 Empirical Evaluation

We now turn to employ our analysis on real world data, deriving prices for an ASIC, specifically the Bitmain Antminer S9, and comparing them to historical market prices.

ASIC prices and specifications (hash-rate and power consumption) are taken from Amazon. We assumed ASICs have a 2-year expected lifetime; in fact, hash-rate considerations usually imply that their profits vanish even faster.

The annual interest rate in the economy was set to 2%, and electricity cost to $\$0.035$, consistent with reported prices that large miners pay. We assume that mining pool fees are 2%, and bond and BTC-to-USD exchange fees are 1% each. The BTC-to-USD exchange rate and global hash-rate were taken from blockchain.com. Volatility was evaluated according to all historical data points starting at 2013 and ending at the value estimation date, and future global hash-rate growth was evaluated according to the 2 year window preceding the estimation date. Volatility is the standard deviation of log-returns, and the hash-rate's growth was assumed to be exponential (which fits historical data well according to the literature [Bowden *et al.*, 2018]). Estimation of $\Delta, \frac{1}{\delta}$ is done according to the annual volatility, as in [Cox *et al.*, 1979], and is elaborated upon in the full version of the paper.

All code used to generate our results is available at <Removed due to blind review>.

Value Comparison

Figure 2 compares ASIC valuations obtained by our method to historical Amazon prices of Bitmain's Antminer S9, and to a naïve evaluation method anecdotally used by miners. In addition, the total cost of an imitating portfolio, including the average-case fees paid for all necessary adjustments, is shown (labeled ”Imitating”).

The naïve evaluation method assumes that the future BTC-USD exchange-rate will continue its recent rate of growth (labeled “Expected” in the figure). This corresponds to an evaluation that ignores risk and uses only expected values, as shown in Example 1.

The figure shows that Amazon prices for hardware are closer to the value obtained using the fixed-growth assumption, and are higher than our estimate, suggesting that they do not fully account for risk.

Revenue Comparison

An imitating portfolio's accuracy increases with the granularity of its time-steps. On the other hand, portfolio adjustments which are made at every such step potentially increase its cost.

Figure 3 compares the *realized* revenue obtained from investing $\$1,000$ in an imitating portfolio with an equivalent investment in real mining hardware that is received and activated *immediately* after the investment was made, which is far from the typical case. The revenue for both is after deducting all maintenance costs, meaning electricity for ASICs and cryptocurrency and bond exchange fees for the portfolio. The imitating portfolio allows each mining opportunity 25 portfolio adjustments, which empirically produces accurate results.

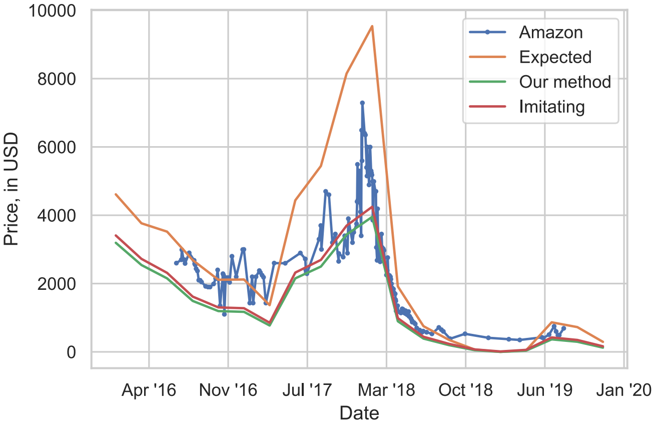
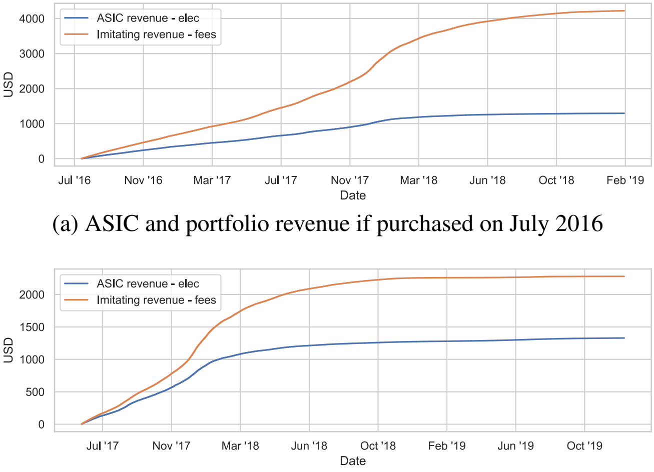


Figure 2: ASIC value according to different valuation methods.

Figure 4 aggregates realized revenue and initial costs of ASICs and the corresponding imitating portfolios, constructed according to our method. As before, the revenue for both is after deducting all maintenance costs. The figure shows that in recent history imitating portfolios produce higher revenues than ASICs. The reason our imitating portfolio's revenue is not exactly the same as an ASIC's is that there is a gap between the realized and projected growth rates of the network's total mining power.



(a) ASIC and portfolio revenue if purchased on July 2016

(b) ASIC and portfolio revenue if purchased on June 2017

Figure 3: Realized revenues (minus maintenance costs) of an ASIC and the corresponding imitating portfolio bought for an initial sum of $1000 and received at the same time, as functions of time.

The Effect of Volatility

As intuitively explained in Section 1, Bitcoin's volatility starkly affects miner revenue, and thus also should affect an ASIC's price. Figure 5 depicts our method's evaluation of ASIC prices as functions of volatility, where each line represents a different purchase date. Bitcoin's annual volatility, as estimated on December 21st, 2019, and its peak annual volatility, which occurred in the year preceding April 29th, 2018, are depicted as vertical lines.

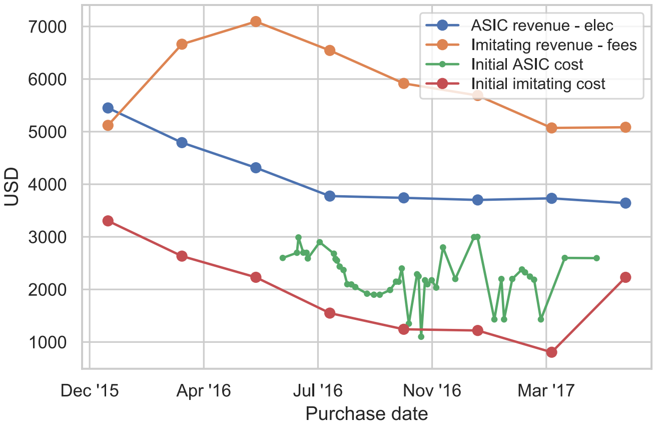


Figure 4: Realized revenue (minus maintenance costs) and initial cost for a 2-year operation of an ASIC and the corresponding imitating portfolio, as functions of purchase date. An ASIC's initial cost is its Amazon price, and the portfolio's is the initial sum of money required for buying the portfolio.

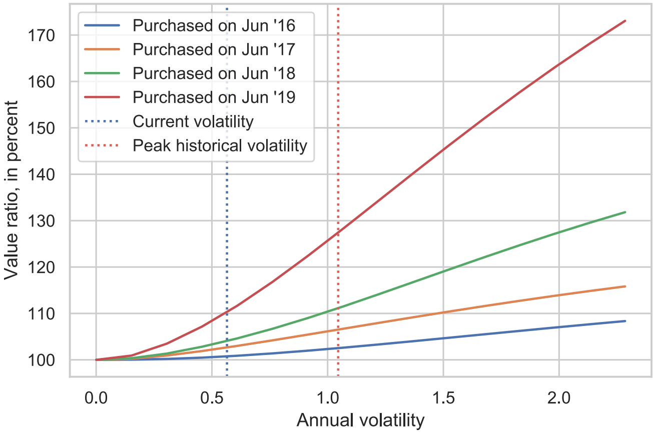


Figure 5: The increase in an ASIC's value, in percent, as a function of volatility.

The Effect of Reception Delay

Applying Equation 3 on historical data from specific periods of Bitcoin's short-term history, we learn that even a brief delay in the reception of an ASIC can severely decrease its value; for example, a month's delay can decrease value by 30%, as seen in Figure 6.

5 Conclusions and Future Work

In this paper we argued that widespread notions regarding ASIC prices and their dependence on cryptocurrency volatility are flawed and require a different analysis. We have presented a method of ASIC valuation, and have shown mining hardware can be imitated using bonds and the underlying cryptocurrencies.

Our evaluation shows that a decrease in Bitcoin's volatility negatively affects the value of mining hardware, while at the same time making imitating portfolios cheaper to maintain (smaller adjustments are needed); combined, both negate the financial incentives put in place to encourage mining. Popular opinion holds that as Bitcoin becomes more widely used, its volatility will decrease. As Bitcoin's security relies on miner participation, lower miner revenues hurt security and undermine Bitcoin's usage as a currency.

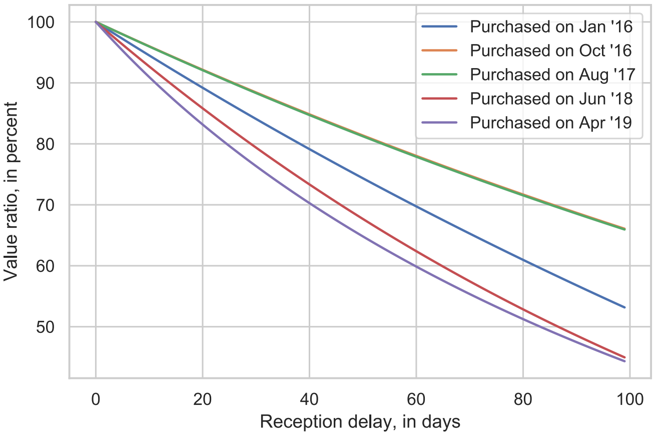


Figure 6: The decrease in an ASIC's value, in percent, as a function of delay.

Future Work To address the security risk inherent in lower volatility, one possibility is artificially increasing volatility. This can be done by adopting a random block-reward mechanism: If for example, the block reward is made to follow a random walk, the returns of miners become more volatile which will increase miner participation. By determining rewards randomly post-hoc, miners cannot foresee future profits; but, according to the analysis presented in this work, miners can know that they have the *potential* to earn more.

This work has assumed that the global hash-rate is exogenous to the model, a possible extension could be to endogenize this. Miners may purchase hardware as long as it remains profitable to do so. Another interesting extension is to consider mining hardware capable of mining multiple currencies.

Acknowledgments

This research was supported by the Ministry of Science & Technology, Israel.

References

[Anish Dev, 2014] J. Anish Dev. Bitcoin mining acceleration and performance quantification. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–6, May 2014.

[Arnosti and Weinberg, 2018] Nick Arnosti and S. Matthew Weinberg. Bitcoin: A Natural Oligopoly. *arXiv e-prints*, page arXiv:1811.08572, November 2018.

[Athey *et al.*, 2016] Susan Athey, Ivo Parashkevov, Vishnu Sarukkai, and Jing Xia. Bitcoin pricing, adoption, and usage: Theory and evidence. 2016.

[Bedford Taylor, 2017] M. Bedford Taylor. The evolution of bitcoin hardware. *Computer*, 50(9):58–66, 2017.

[Black and Scholes, 1973] Fischer Black and Myron Scholes. The pricing of options and corporate liabilities. *Journal of political economy*, 81(3):637–654, 1973.

[Bowden *et al.*, 2018] R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor. Block arrivals in the Bitcoin blockchain. *ArXiv e-prints*, January 2018.

[Budish, 2018] Eric Budish. The economic limits of bitcoin and the blockchain. Working Paper 24717, National Bureau of Economic Research, June 2018.

[Cox *et al.*, 1979] John C Cox, Stephen A Ross, Mark Rubinstein, et al. Option pricing: A simplified approach. *Journal of financial Economics*, 7(3):229–263, 1979.

[Dimitri, 2017] Nicola Dimitri. Bitcoin mining as a contest. *Ledger*, 2(0):31–37, 2017.

[Dixit and Pindyck, 1994] Avinash K. Dixit and Robert S. Pindyck. *Investment under Uncertainty*. Number 5474 in Economics Books. Princeton University Press, 1994.

[Dwivedi *et al.*, 2019] Ashutosh Dwivedi, Gautam Srivastava, and Rajani Singh. A game theoretic analysis of resource mining in blockchain. 11 2019.

[Fiat *et al.*, 2019] Amos Fiat, Anna Karlin, Elias Koutsoupias, and Christos Papadimitriou. Energy equilibria in proof-of-work mining. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, EC '19, page 489–502, New York, NY, USA, 2019. Association for Computing Machinery.

[Gervais *et al.*, 2014] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun. Is bitcoin a decentralized currency? *IEEE Security Privacy*, 12(3):54–60, May 2014.

[Goren and Spiegelman, 2019] Guy Goren and Alexander Spiegelman. Mind the Mining. *arXiv e-prints*, page arXiv:1902.03899, Feb 2019.

[Hanke, 2016] Timo Hanke. AsicBoost - A Speedup for Bitcoin Mining. *arXiv e-prints*, page arXiv:1604.00575, Apr 2016.

[Hayes, 2014] Adam Hayes. The decision to produce altcoins: Miners' arbitrage in cryptocurrency markets. 12 2014.

[Hayes, 2017] Adam S. Hayes. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics*, 34(7):1308 – 1321, 2017.

[Nakamoto, 2008] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.

[Rosenfeld, 2011] M. Rosenfeld. Analysis of Bitcoin Pooled Mining Reward Systems. *ArXiv e-prints*, December 2011.

[Salimitari *et al.*, 2017] M. Salimitari, M. Chatterjee, M. Yuksel, and E. Pasiliao. Profit maximization for bitcoin pool mining: A prospect theoretic approach. In *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*, pages 267–274, Oct 2017.

[Schrijvers *et al.*, 2017] Okke Schrijvers, Joseph Bonneau, Dan Boneh, and Tim Roughgarden. Incentive compatibility of bitcoin mining pool reward functions. In Jens Grossklags and Bart Preneel, editors, *Financial Cryptography and Data Security*, pages 477–498, Berlin, Heidelberg, 2017. Springer Berlin Heidelberg.

[Schwartz, 2004] Eduardo S. Schwartz. Patents and r&d as real options. *Economic Notes*, 33(1):23–54, 2004.

[Suresh *et al.*, 2018] Vikram B Suresh, Sudhir K Satpathy, and Sanu K Mathew. Optimized sha-256 datapath for energy-efficient high-performance bitcoin mining, November 27 2018. US Patent 10,142,098.

[Tsabary and Eyal, 2018] Itay Tsabary and Ittay Eyal. The Gap Game. *arXiv e-prints*, page arXiv:1805.05288, May 2018.