Correct Cryptocurrency ASIC Pricing: Are Miners Overpaying?

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

ABSTRACT

Cryptocurrencies that are based on Proof-of-Work often rely on special purpose hardware (ASICs) to perform mining operations that 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. To prevent this, we suggest a new reward mechanism.

Finally we construct a portfolio of coins and bonds that provides returns imitating an ASIC, and evaluate its behavior: historically, realized revenues of such portfolios have significantly outperformed ASICs, showing that indeed there is a mispricing of hardware, and offering an alternative investment route for would-be miners.

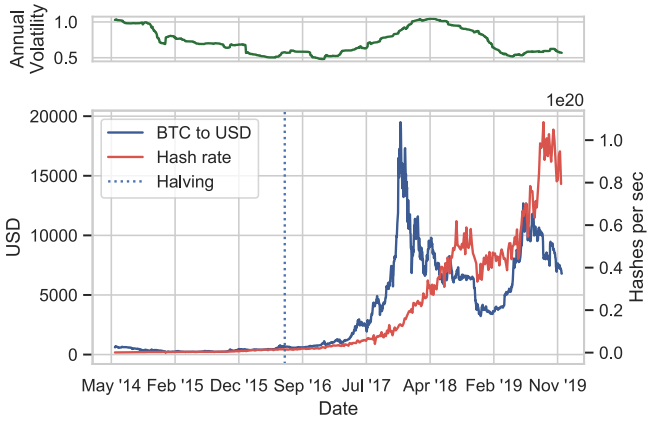


Figure 1: Bitcoin's annual volatility, exchange rate to USD and global hash-rate, as functions of time.

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. To stay competitive, miners purchase mining rigs in advance, and at a significant capital expenditure. These volatile returns make mining a high-risk investment and may indirectly hurt the cryptocurrency if fewer miners are there to secure it.

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 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 out-perform physical ASICs, even when accounting for the fees required for portfolio maintenance.

A novel insight arising from our work is the importance of volatility for miner profitability. At first glance, it may seem that higher volatility in rewards implies a higher risk for miners, which may devalue mining machines, but in fact, we show that said machines *increase* in value if the cryptocurrency is more volatile, as shown for example in Figure 9. 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 without taking volatility into full consideration, thus the inherent risk is ignored. Instead, the hardware's *expected* returns are used;

so, it is not surprising that our valuation method produces results that are different from actual market prices, as shown in Figure 6.

Paper Structure. The remainder of the paper is structured as follows: we begin by reviewing related work, and then present additional background on mining and option pricing in Section 2. We go on to define the precise model for ASICs in Section 3. We present our results on the correct methods for pricing ASICs in Section 4, deferring some of the proofs to Section 6. We then employ our theoretical results to perform an empirical evaluation using real-world price data in Section 5. We conclude with a discussion on the implication of our results in Section 7.

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, 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 its 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; Salimitari et al. 2017; Schrijvers 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; Hanke 2016; Suresh et al. 2018] attempt to improve mining performance, thereby also increasing mining hardware value, but do not directly analyze said value.

2 PRELIMINARIES

2.1 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 included 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 expect small and constant returns from mining over time, and our model will rely on this fact.

2.2 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 and not an obligation, the buyer need not exercise it if deemed unprofitable. Specifically, it might be the case that by the date of expiry the underlying asset's price is lower than the strike price, thus it is preferable to buy the underlying asset directly and discard the option.

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.

3 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 φ, and the cost of electricity as 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.

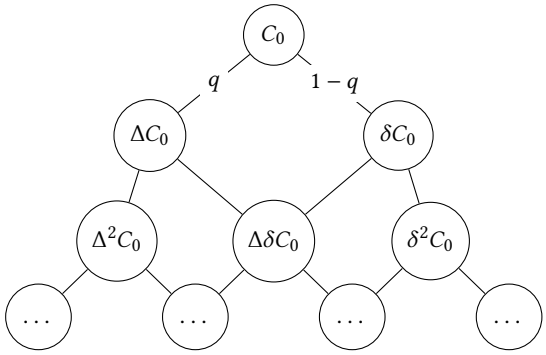


Figure 2: Coin's exchange rate as a multiplicative random walk, with a start value of C_0, a q probability to increase by a factor of Δ, and a $1-q$ probability to decrease by δ.

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 C_t, the probability for its value to rise to ΔC_t in the next turn by q, and to fall to δC_t in the next turn by $1-q$, resulting in the price tree shown in Figure 2.

While it may seem simplistic to assume that the price at every time unit can either increase or decrease by a factor, using sufficiently small time intervals yields a highly granular price model for longer periods. Indeed, this distribution is commonly used in finance to model the value of assets such as currencies and stocks.

Denote the annual interest rate in the economy as $\eta > 0$, and let $r = 1 + \eta$. We assume $0 < \delta < 1 < r < \Delta$, 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 $V(\cdot)$.
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.

In addition, we will create portfolios holding combinations of the above assets, and denote a portfolio's value by $\Phi(\cdot)$.

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 $h \cdot \varphi \cdot e_t$, and in return receive the partial reward of $\frac{h}{H(t)+h} \cdot b_t \cdot C_t$.

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:

$$V(t,t,C_t) \triangleq \max\left(\frac{h}{H(t)+h} b_t C_t - h\varphi e_t, 0\right) \tag{1}$$

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; this will be demonstrated by Example 1. We shall denote the value of the t-th opportunity in relation to some time $k \le t$, where the coin's exchange rate at k is C_k as $V(t,k,C_k)$.

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 $t \le s$:

$$V_{ASIC}(s,t,C_t) = \sum_{t=s}^{\infty} M(t-s) \cdot V(t,t,C_t) \tag{2}$$

Reception Delay. A method for evaluating an ASIC's price could allow us to estimate the potential decrease in price associated with receiving hardware farther in the future.

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 is:

$$V_{ASIC}(s',t,C_t) - V_{ASIC}(s,t,C_t) \tag{3}$$

Example 1. *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 Bitcoin (henceforth denoted as BTC or ₿), and will require* \$250 *worth of electricity. To simplify the example, let the multiplicative interest-rate r be* 1.

For this toy example, assume bitcoin's value starts at \$400 *today, and will either double or halve tomorrow with equal probability, giving an expected exchange-rate of* $\frac{1}{2} \cdot \$200 + \frac{1}{2} \cdot \$800 = \$500$.

At a \$200 *rate, activating the ASIC will result in a loss of* \$50, *as* \$250 *is paid and only* \$200 *is received; thus, rational agents will not activate the ASIC, and will lose nothing. On the other hand, if the rate increases to* \$800, *it is possible to earn* $\$800 - \$250 = \$550$ *by turning the hardware on. In total, the expected return is* $\frac{1}{2} \cdot \$0 + \frac{1}{2} \cdot \$550 = \$275$.

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 $\$183\frac{1}{3}$, *as will be shown later.*

To show why \$275 *is* incorrect, *note that this price creates an* arbitrage *opportunity. Assume there is at least one rational buyer for the opportunity, willing to pay* \$275. *If so, that buyer will surely prefer purchasing it for the lower price of* \$274! *We can sell the opportunity for the lower price* without *actually owning it, all the while promising the buyer that no matter the world state the same exact profits will be earned. Essentially, we are performing a short on the opportunity.*

As summarized in Table 1, to fulfill the promise we will do the following: immediately upon selling the opportunity we will borrow

#	Step	Cash	Debt	Coins	Opportunities
0	Start of day.	\$0	\$0	0	0
1	Sell opportunity.	\$274	\$0	0	−1
2	Borrow $\$183\frac{1}{3}$.	$\$457\frac{1}{3}$	$\$183\frac{1}{3}$	0	−1
3	Buy $\frac{11}{12}$ coins.	$\$90\frac{2}{3}$	$\$183\frac{1}{3}$	$\frac{11}{12}$	−1

Table 1: Balance of all assets on the first day of Example 1. Regarding step #1: when selling the opportunity we have a −1 quantity of it, essentially performing a short (selling it without actually owning it).

#	Step	Cash	Debt	Coins	Opportunities
0	Start of day.	$\$90\frac{2}{3}$	$\$183\frac{1}{3}$	$\frac{11}{12}$	−1
1	Get activation fee.	$\$340\frac{2}{3}$	$\$183\frac{1}{3}$	$\frac{11}{12}$	−1
2	Pay loan back.	$\$157\frac{1}{3}$	\$0	$\frac{11}{12}$	−1
3	Buy $\frac{1}{12}$ coins.	$\$90\frac{2}{3}$	\$0	1	−1
4	Pay buyer 1 coin.	$\$90\frac{2}{3}$	\$0	0	0

Table 2: Balance of all assets on the second day of Example 1, if the exchange-rate has doubled. Regarding step #4: giving the buyer 1 coin covers the short on the opportunity.

#	Step	Cash	Debt	Coins	Opportunities
0	Start of day.	$\$90\frac{2}{3}$	$\$183\frac{1}{3}$	$\frac{11}{12}$	0
1	Sell all coins.	\$274	$\$183\frac{1}{3}$	0	0
2	Pay loan back.	$\$90\frac{2}{3}$	\$0	0	0

Table 3: Balance of all assets on the second day of Example 1, if the exchange-rate has halved. Note that there is a 0 amount of the opportunity at the start of the day because a rational buyer will not choose to activate the ASIC, thus our short on the opportunity is closed.

$\$183\frac{1}{3}$ from the bank, giving us a total of $\$183\frac{1}{3} + \$274 = \$457\frac{1}{3}$. We will buy $\frac{11}{12}$ BTC, which under the current exchange-rate are worth $\frac{11}{12} \cdot \$400 = \$366\frac{2}{3}$. After this, we remain with $\$457\frac{1}{3} - \$366\frac{2}{3} = \$90\frac{2}{3}$, which we will pocket as a profit.

If the value of bitcoin goes up, our rational buyer will want to turn on the (imaginary) ASIC and receive the promised 1 BTC reward in exchange for the \$250 activation fee, which is paid to us. We will use the fee to pay back the loan, leaving us with $\$250 - \$183\frac{1}{3} = \$66\frac{2}{3}$, exactly enough to buy $\frac{1}{12}$ BTC, that together with our existing $\frac{11}{12}$ BTC can be given to the buyer as the mining reward, thus covering our short. Note we have also paid back all debt, while our pocketed $\$90\frac{2}{3}$ profit was untouched, as shown in Table 2.

On the other hand, if the value goes down, the rational buyer will not want to pay the activation fee as it is more expensive than the 1 BTC (= \$200) profit; even if the buyer is interested in receiving a single bitcoin, buying it on the free market is cheaper than activating the ASIC. So, we have covered our short without having to pay the mining reward. We will still need to repay our $\$183\frac{1}{3}$ debt, and luckily our coins are worth exactly $\frac{11}{12} \cdot \$200 = \$183\frac{1}{3}$. Again, we keep our pocketed profit. Table 3 presents all changes in our holdings.

Although we have started with no money, we have made a riskless profit of $\$90\frac{2}{3}$ due to the incorrect *pricing of the ASIC. In the rest of the paper we show how to correctly price it, and prove that when using our method no arbitrage opportunities arise.*

4 RESULTS

In this section we tackle the problem presented in the previous example more generally – 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 a mining opportunity, a portfolio of mining opportunities and coins is constructed and purchased at at turn $t-1$. The portfolio is crafted to yield identical valuations at turn t regardless of the change in the exchange-rate (we do this in Claim 1), and as such is termed a *risk-free* portfolio. Thus, its exact value at turn $t-1$ will be known by properly discounting and accounting for the interest rate (We show this in Claim 2).

We consider a portfolio that consists of the t-th mining opportunity and a short on (a yet to be chosen amount of) a_{t-1} coins, thus its value at turn $t-1$ is:

$$\Phi(t-1) = V(t, t-1, C_{t-1}) - a_{t-1}C_{t-1} \tag{4}$$

And at turn t:

$$\Phi(t) = V(t, t, C_t) - a_{t-1}C_t \tag{5}$$

Claim 1. *A portfolio holding the t'th mining opportunity and a short on the following amount of coins:*

$$a_{t-1} = \frac{V(t, t, \Delta C_{t-1}) - V(t, t, \delta C_{t-1})}{C_{t-1}(\Delta - \delta)}$$

Is a risk free-portfolio for the single turn between time $t-1, t$, and its value in all possible states at t is:

$$\Phi(t) = V(t, t, \Delta C_{t-1}) - a_{t-1}\Delta C_{t-1}$$

The proof is given in Section 6; its main idea is that there is one degree of freedom (choosing the short amount, a_{t-1}) and we must satisfy an equation equating the value of the portfolio in both possible world states, yielding the same return in both.

Now that we have a risk-free portfolio, we proceed to evaluate its return, and use it to price the mining opportunity.

Claim 2. *If no arbitrage opportunities exist, the multiplicative return of holding the risk-free portfolio constructed in Claim 1 between turns $t-1$ and t is equal to the risk-free rate.*

The proof is given in Section 6; briefly, every other possible return is examined and shown to contradict the no-arbitrage assumption. Just as in Example 1, we can make a risk-free profit whenever such arbitrage opportunities arise.

We then end up with the following expression for pricing the mining opportunity:

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

$$V(t, t-1, C_{t-1}) = \frac{V(t, t, \Delta C_{t-1})}{r} + \\ + \frac{V(t, t, \Delta C_{t-1}) - V(t, t, \delta C_{t-1})}{\Delta - \delta}\left(1 - \frac{\Delta}{r}\right)$$

In the above expression, all factors are known and can be calculated at time $t-1$.

The proof is given in Section 6. It consists of using the return of the portfolio together with its values at turns $t-1$ and t to extract the value of the opportunity at $t-1$.

For the sake of completeness, let us revisit the scenario in Example 1 and derive the *correct* price for the opportunity, as implied by Corollary 1.

Example 2. *Surprisingly, the price given by Corollary 1 for the mining opportunity presented in Example 1 is even lower than the naïve estimate.*

The immediate value of the mining opportunity if the exchange rate has gone up is:

$$V(1,1,800) = \max(1 \cdot 800 - 250, 0) = \$550 \tag{6}$$

And for the down state it is:

$$V(1,1,200) = \max(1 \cdot 200 - 250, 0) = \$0 \tag{7}$$

When using the above with Corollary 1 we can obtain the value of the opportunity at turn 0*:*

$$V(1,0,400) = \frac{550}{1} + \frac{550-0}{2-\frac{1}{2}}\left(1-\frac{2}{1}\right) = \$183\frac{1}{3}$$

As the proof for Claim 2 shows, any price different than this one, for example the naïve price, creates an arbitrage opportunity.

4.1 Pricing Relative to an Arbitrary Time

By extending the previous method, it is possible to evaluate the t-th opportunity relative to any previous point in time k, as shown in Algorithm 1.

Algorithm 1: MiningOpportunityValue

Output: value of t-th opportunity at turn k.
for $C_t \in \{\Delta^{t-k}\cdot C_k, \Delta^{t-k-1}\cdot\delta\cdot C_k, \ldots, \delta^{t-k}\cdot C_k\}$ **do**
  $V(t,t,C_t) \leftarrow h \cdot \max\left(\frac{b_t \cdot C_t}{H(t)+h} - \varphi \cdot e_t, 0\right)$
end
for $\tau \in t-1, \ldots, k$ **do**
  for $C_\tau \in \{\Delta^\tau \cdot C_k, \Delta^{\tau-1}\cdot\delta\cdot C_k, \ldots, \Delta\cdot\delta^{\tau-1}C_k, \delta^\tau \cdot C_k\}$ **do**
    $a_\tau \leftarrow \frac{V(t,\tau+1,\Delta\cdot C_\tau) - V(t,\tau+1,\delta\cdot C_\tau)}{C_\tau\cdot(\Delta-\delta)}$
    $\Phi(\tau+1) \leftarrow V(t,\tau+1,\Delta\cdot C_\tau) - a_\tau\cdot\Delta\cdot C_\tau$
    $V(t,\tau,C_\tau) \leftarrow a_\tau\cdot C_\tau + \frac{\Phi(\tau+1)}{r}$
  end
end
return $V(t,k,C_k)$

The idea behind the algorithm is to apply the same methods of Section 4 on every possible world-state, starting from turn t and going back, one step at a time, until reaching k. We will now proceed to explain the method in depth:

The random-walk describing the coin's exchange rate for the period between turns k and t forms a tree with root C_k and leaves $\Delta^\tau\delta^{t-k-\tau}C_k$, for every $\tau \in [0, t-k]$.

The leaves represent the trivial cases for evaluation, each one of them corresponds to a possible world state at turn t and as the opportunity expires at that turn, its value can be calculated directly from the definition given in Equation 1.

Proceeding inductively, let $\tau \in [k, t-1]$. We will want to evaluate the opportunity at one of the vertices of the $(\tau-k)$-th level, assume it is C_τ. Note it points to exactly two vertices from level $(\tau-k+1)$, specifically $\Delta C_\tau, \delta C_\tau$. The method laid down in Section 4 suggests that given that the opportunity values for these two vertices have already been calculated, the opportunity's value at C_τ's world-state can be obtained. Claim 3 covers this case.

Claim 3. *Let $\tau < t$. Given that the opportunity's valuations at $\tau+1$ are known, it is possible to evaluate $V(t,\tau,C_\tau)$, which is equal to:*

$$V(t,\tau,C_\tau) = \frac{V(t,\tau+1,\Delta C_\tau)}{r} + \\ + \frac{V(t,\tau+1,\Delta C_\tau) - V(t,\tau+1,\delta C_\tau)}{\Delta-\delta}\left(1-\frac{\Delta}{r}\right)$$

The proof is given in Section 6; the result is achieved by using the valuations at $\tau+1$ to create a risk-free portfolio at turn τ that holds the t-th opportunity. The return of the portfolio at $\tau+1$ can then be used to retrieve the value of the opportunity, similarly to Corollary 1.

By applying Claim 3 on every vertex of the current level and continuing in a dynamic manner to previous levels, it is possible to reach our goal and finally derive the value at the root of the tree, which corresponds to turn k.

Deriving a formula for the mining opportunity's value. 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. *The value of the t-th mining opportunity at to turn $k < t$ is:*

$$V(t,k,C_k) = \sum_{\tau=\tau_0}^{t-k} \frac{\binom{t-k}{\tau}\gamma_\uparrow^\tau}{\left(-\gamma_\downarrow\right)^{k+\tau-t}} V\left(t,t,\Delta^\tau\delta^{t-k-\tau}C_k\right)$$

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

$$\tau_0 = \left\lceil \frac{\log\left(\left(\frac{b_t\delta^{t-k}C_k}{H(t)+h}\right)^{-1}\varphi e_t\right)}{\log\left(\frac{\Delta}{\delta}\right)} \right\rceil$$

The proof is given in Section 6. It involves recursively applying Claim 3 on $V(t,k,C_k)$ until reaching a sum that only includes values of immediate opportunities. Then, the sum is shortened by looking only at opportunities that have a value that is greater than 0.

Example 3. *Assume that bitcoin's exchange-rate can either double or halve with an equal probability, with the random walk starting from a value of* \$200 *at turn* 0*. Extending the walk to two turns produces the recombining tree depicted in Figure 3.*

Assume the vendor from Example 1 offers you the option of using its ASIC at the second turn for 10 minutes, under the same conditions as before. By following Algorithm 1, the value of the opportunity at each state can be calculated, as shown in Figure 4. The algorithm proceeds as follows:

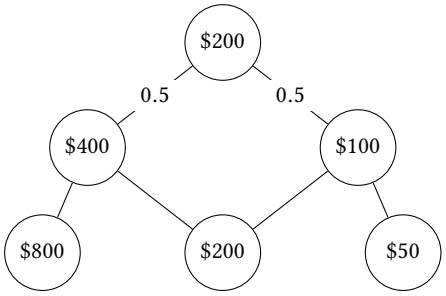


Figure 3: Example 3's equiprobable two turn random walk.

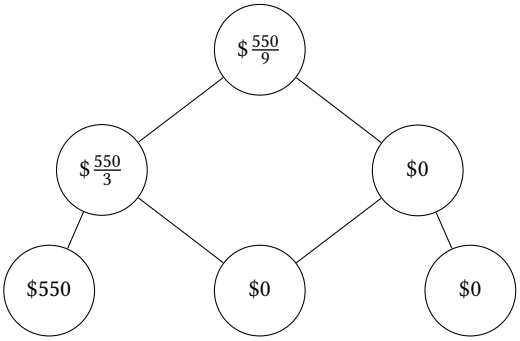


Figure 4: The value of Example 3's mining opportunity at each state, according to Algorithm 1.

We start from the leaves and evaluate the immediate value of the opportunity at each one. At the leaf where the exchange-rate is \$800*, the opportunity is worth* \$550*. On the other hand, if the rate is either* \$200 *or* \$50*, the opportunity is worth* \$0*. We have determined the value of the opportunity at all possible states of turn 2.*

Now, by using Claim 3 on each of the two possible states at turn 1*, we get that the value of the opportunity can be either* $\$\frac{550}{3}$ *(if the exchange rate is* \$400*) or* \$0 *(if it is* \$100*).*

Finally, we take one step back and look at turn 0*. By employing Claim 3 again together with our previous results, we find that the opportunity is worth* $\$\frac{550}{9}$ *at the first turn.*

4.2 Imitating Portfolio

Buying physical mining hardware can sometimes entail difficulties: cooling, storing and maintaining it is costly, and receiving ordered ASICs promptly requires paying a hefty premium when there is high demand.

Imitating an ASIC's revenue using a portfolio that does not include the ASIC might be better – it can start to produce revenue immediately, without waiting, and avoids the aforementioned expenses. We show such a portfolio can be constructed using coins and bonds.

The portfolio will imitate the t-th opportunity between turns $\tau, \tau+1$, for $\tau < t$. Denote by $\overline{a}_\tau, B_\tau$ the respective amount of coins and risk-free bonds in the imitating portfolio at time τ. Thus, the portfolio's value at time τ is:

$$\overline{\Phi}(\tau) = B_\tau + \overline{a}_\tau C_\tau \tag{8}$$

And, at $\tau+1$ it is

$$\overline{\Phi}(\tau+1) = rB_\tau + \overline{a}_\tau C_{\tau+1} \tag{9}$$

Claim 4. *Assuming there are no fees for trading bonds and coins, a portfolio can be constructed at turn τ to be worth exactly the same as the t-th mining-opportunity in all possible world-states at turn $\tau+1$: $\overline{\Phi}(\tau+1) = V(t, \tau+1, C_{\tau+1})$. The portfolio is obtained by setting:*

$$\overline{a}_\tau = \frac{V(t, \tau+1, \Delta C_\tau) - V(t, \tau+1, \delta C_\tau)}{C_\tau(\Delta - \delta)}$$

$$B_\tau = \frac{\Delta V(t, \tau+1, \delta C_\tau) - \delta V(t, \tau+1, \Delta C_\tau)}{r(\Delta - \delta)}$$

The proof is given in Section 6, and is similar to the proof of Claim 1.

Claim 5. *At turn τ, a portfolio constructed as in Claim 4 is worth exactly the same as the t-th mining-opportunity:*

$$\overline{\Phi}(\tau) = V(t, \tau, C_\tau)$$

The proof is given in Section 6; it relies on showing that at turn τ the risk-free portfolio of Claim 3 is equal in value to B_τ. Then, algebraic manipulations are made on the definitions of both the risk-free portfolio and the portfolio of Claim 4 to conclude that the claim holds.

Combining Claims 4 and 5 immediately gives the following:

Corollary 2. *The portfolio constructed in Claim 4 is an imitating portfolio for the t-th mining opportunity between turns τ, $\tau+1$, meaning the portfolio is equal in value to the opportunity at both turns.*

Similarly to Section 4.1, the imitating portfolio can be evaluated at multiple time periods by dynamically moving backwards in time. The portfolio can change between turns, costing additional fees to perform the necessary adjustments; these are included in the empirical evaluation performed in Section 5.

Note that under the assumption that there are no fees, Claims 4 and 5 imply that at turn $\tau+1$, selling the imitating portfolio for turns $\tau, \tau+1$ generates enough money to buy the imitating portfolio for turns $\tau+1, \tau+2$, meaning that after the initial investment is made, no new influx of funds is required to adjust the portfolio between turns. In addition, the initial purchase of the portfolio costs exactly the same as the opportunity that it imitates.

Let us proceed by demonstrating how to use these results to construct an imitating portfolio:

Example 4. *Figure 5 shows the portfolios imitating the mining opportunity offered in Example 3 for all possible world states. The portfolios were constructed in the following manner:*

First, evaluate the opportunity's value at all the states, as in Example 3. Next, apply Claim 4 on each possible state at turn 1*. The imitating portfolio for the state where the exchange-rate equals* \$400 *is comprised of* $\frac{550-0}{400\cdot(2-0.5)} = \frac{11}{12}$ *coins, and* $\frac{2\cdot 0-0.5\cdot 550}{1\cdot(2-0.5)} = -\$\frac{550}{3}$ *worth of bonds. On the other hand, if the exchange-rate is* \$100 *then the portfolio has* $\frac{0-0}{100\cdot(2-0.5)} = 0$ *coins and* $\frac{2\cdot 0-0.5\cdot 0}{1\cdot(2-0.5)} = 0$ *bonds.*

Now, we will construct an imitating portfolio for the first state; it will hold $\frac{\frac{550}{3}-0}{200\cdot(2-0.5)} = \frac{11}{18}$ *coins, and bonds valued at* $\frac{2\cdot 0-0.5\cdot\frac{550}{3}}{1\cdot(2-0.5)} = -\$\frac{550}{9}$.

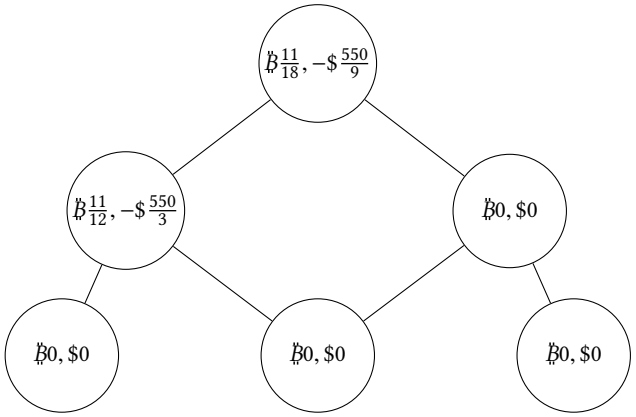


Figure 5: The imitating portfolio for each state of Example 4. The portfolio is represented as a tuple, where the left number (prefixed by ₿) is the amount of coins, and the right number is the bonds' value in USD (prefixed by $). The portfolios should always be sold on the last turn, thus all final portfolios hold no assets.

To show that these portfolios are indeed imitating, we will analyze their returns on the final turn. If an imitating portfolio is sold on the final turn, by construction its return should equal the one given by the actual mining opportunity.

If the exchange-rate is \$800*, the portfolio we constructed is worth* $800 \cdot \frac{11}{12} - \frac{550}{3} = \$550$*, thus selling it produces exactly the same profits as the opportunity at this state. If the exchange-rate is* \$200*, look at the two possible cases: if the previous turn's exchange-rate was* \$400*, our portfolio is comprised of* $\frac{11}{12}$ *coins and bonds worth* $-\$\frac{550}{3}$*, thus selling the portfolio results in a profit of* $400 \cdot \frac{11}{12} - \frac{550}{3} = \$0$*, again equal to the opportunity's. Conversely, if the previous rate was* \$100*, our portfolio holds no assets, so there is nothing to sell - and as before, the profit is* \$0*, the same as the opportunity's.*

5 EMPIRICAL EVALUATION

We now turn to employ our analysis on real world data, deriving prices for an ASIC, specifically the Bitmain Antminer S9, a single hardware platform that has dominated the ASIC market for an extended period of time, and has lately been replaced. We compare these prices 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.

For the following evaluations, 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 trading 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 Δ, δ*.* The estimation of the random-walk's multiplicative factors is outside the scope of this paper, and was done using the same method presented in [Cox et al. 1979].

Denote the annual volatility of the coin's exchange-rate by σ, and by n the actual ("calendar") time until the mining opportunity to evaluate. Assuming that there are t turns until n, the multiplicative factors are:

$$\Delta = \exp\left(\sigma\sqrt{\frac{n}{t}}\right) \tag{10}$$

$$\delta = \exp\left(-\sigma\sqrt{\frac{n}{t}}\right) \tag{11}$$

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

Value Comparison. Figure 6 compares ASIC valuations obtained by our method to the 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.

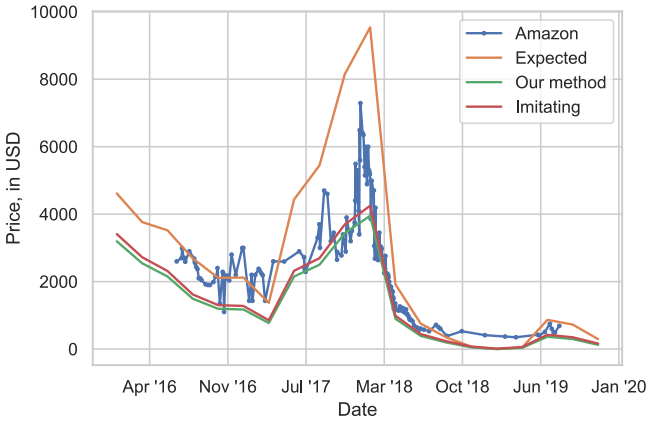


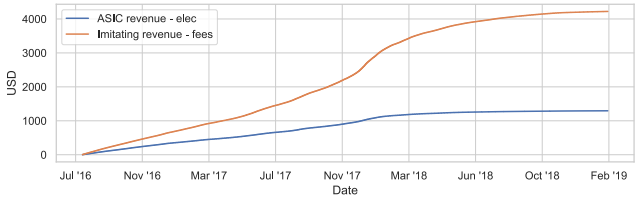
Figure 6: ASIC value according to different valuation methods.

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.

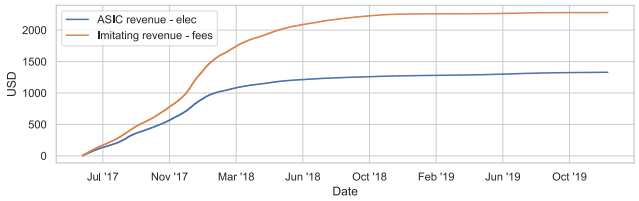
Figure 7 compares the *realized* revenue obtained from investing \$1,000 in an imitating portfolio with an equivalent investment in

real mining hardware that is received and activated *immediately* after the investment was made, which is far from the typical case as usually miners wait a long time to receive hardware. The revenue for both is after deducting all maintenance costs, meaning electricity for ASICs and cryptocurrency and bond trading fees for the portfolio. The imitating portfolio allows each mining opportunity 25 portfolio adjustments, which empirically produces accurate results.

Figure 8 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 7: 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 9 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.

As can be seen, our method gives higher prices for ASICs if the annual volatility is higher. For example, an ASIC bought on June 2019 could have cost %16 more if the volatility was at its historical peak.

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 10.

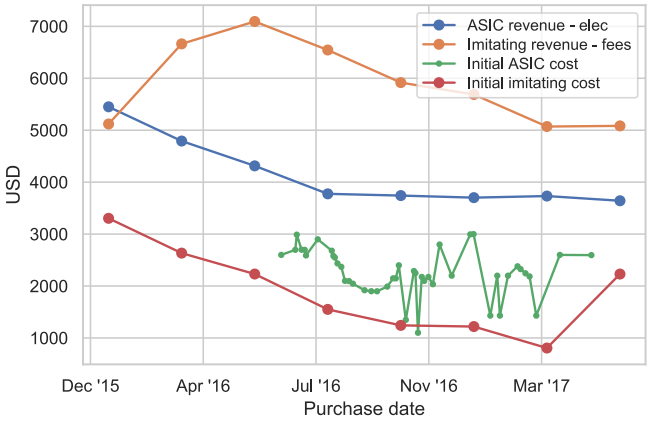


Figure 8: Realized revenue (minus maintenance costs) and initial cost for a 2-year operation of an ASIC and the corresponding imitating portfolio, as functions of the purchase date. An ASIC's initial cost is its Amazon price, and the portfolio's is the initial sum of money required for buying the portfolio.

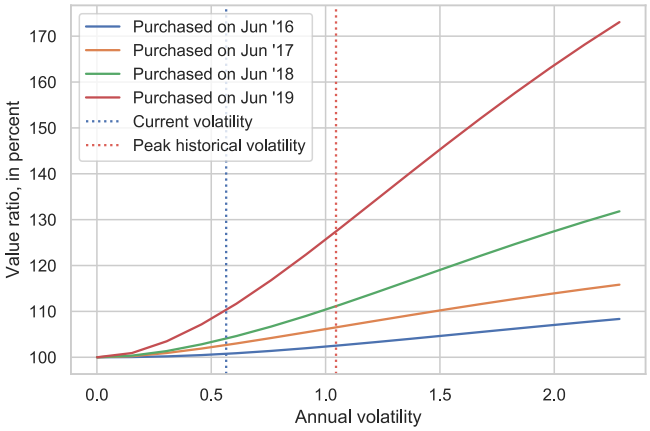


Figure 9: The increase in an ASIC's value, in percent, as a function of volatility.

6 PROOFS

Proof of Claim 1. There are only two possible future world states: one where the coin's exchange-rate will up relative to $t-1$ and will be ΔC_{t-1}, and the other where it will go down to δC_{t-1}. Denote the immediate value of the mining opportunity in the up state as:

$$V(t, t, \Delta C_{t-1}) = \max\left(\frac{hb_t \Delta C_{t-1}}{H(t)+h} - h\varphi e_t, 0\right) \tag{12}$$

And of the down state as:

$$V(t, t, \delta C_{t-1}) = \max\left(\frac{hb_t \delta C_{t-1}}{H(t)+h} - h\varphi e_t, 0\right) \tag{13}$$

Given that t is in the future, our model assumes that there is some estimation for $H(t)$; Section 5 elaborates on the way such estimates were made. Thus, the sole difficulty in evaluating $\Phi(t)$ is

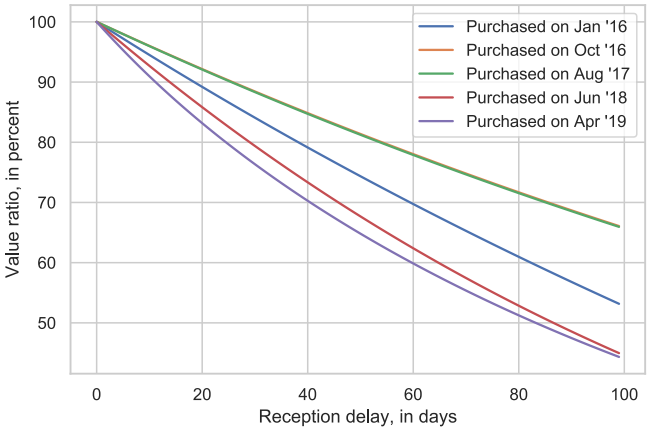


Figure 10: The decrease in an ASIC's value, in percent, as a function of delay.

that although at $t-1$ we know what the value of C_{t-1} is, we do not yet know the realization of C_t. To circumvent this, we will construct the portfolio such that its value at t will be the same no matter if C_t is equal to ΔC_{t-1} or δC_{t-1}, yielding a risk-free portfolio.

The portfolio's value at the up-state is:

$$\Phi(t) = V(t, t, \Delta C_{t-1}) - a_{t-1}\Delta C_{t-1} \tag{14}$$

And, at the down-state:

$$\Phi(t) = V(t, t, \delta C_{t-1}) - a_{t-1}\delta C_{t-1} \tag{15}$$

So, we require that the following property would hold:

$$V(t, t, \Delta C_{t-1}) - a_{t-1}\Delta C_{t-1} = V(t, t, \delta C_{t-1}) - a_{t-1}\delta C_{t-1} \tag{16}$$

Everything but a_{t-1} is known, thus it is possible to derive a_{t-1} by isolating it, producing the following short amount:

$$a_{t-1} = \frac{V(t, t, \Delta C_{t-1}) - V(t, t, \delta C_{t-1})}{C_{t-1}(\Delta - \delta)} \tag{17}$$

Note that there is no probability in the equation, meaning that this shorting strategy is not dependent on the probability of an upward or downward change in the coin's price.

From Equations 14, 15, 16 we get that by performing this short, our portfolio's value at turn t is equal to:

$$\Phi(t) = V(t, t, \Delta C_{t-1}) - a_{t-1}\Delta C_{t-1} \tag{18}$$

The equation holds in all possible world state, so the portfolio is indeed risk-free. By substituting for the short amount the following explicit form is obtained:

$$\Phi(t) = V(t, t, \Delta C_{t-1}) - \frac{V(t, t, \Delta C_{t-1}) - V(t, t, \delta C_{t-1})}{\Delta - \delta}\Delta \tag{19}$$

□

Proof of Claim 2. The proof mainly relies on the no-arbitrage assumption. First, we will define the multiplicative return of our portfolio between $t-1$ and t as:

$$\rho(t) \triangleq \frac{\Phi(t)}{\Phi(t-1)} \tag{20}$$

Thus, we want to prove that $\rho(t) = r$. Assume by contradiction that $\rho(t) \neq r$. We will now show how to make risk-free profit in every world state by dividing to cases:

Case 1. If $\Phi(t-1) > 0$.

Make a further sub-division to two sub-cases:

Case 1.a. If $\rho(t) > r$.

It is possible to "make money out of nothing" by borrowing enough money at the risk-free rate to buy the portfolio at time $t-1$, and selling it after a single turn.

Buying the portfolio is simply purchasing the mining opportunity and shorting the coins as specified by the portfolio, and selling it is the "reverse" - selling the opportunity and delivering the shorted asset. A reminder: shorting an asset means borrowing it and immediately selling it, thus the same asset should be returned to the loaner.

Borrowing at the risk-free rate means that there is interest to be paid for the loan, but as this case assumes that the return of the portfolio is higher, a profit has been made even after taking interest into account, a contradiction to the no-arbitrage assumption.

Case 1.b. If $\rho(t) < r$.

Risk-less profit can be made by shorting the portfolio and investing the resulting money in a risk-free instrument at time $t-1$, and by returning the short at the next turn.

Shorting the portfolio entails shorting the mining opportunity and buying the coins, as specified by the portfolio. Returning this short is simply returning the mining opportunity and selling the coins.

By the current case's assumption, the return on the coins and risk-free investment is large enough make a profit, even after delivering the short, and we have reached a contradiction.

Case 2. If $\Phi(t-1) = 0$.

$\rho(t)$ is undefined, thus a split to different cases than before is required:

Case 2.a. If $\Phi(t) > 0$.

Buy the portfolio at turn $t-1$. According to the assumption of the current case, at $t-1$ the portfolio is priced at 0, meaning that shorting the required number of coins as specified in Claim 1 produces exactly enough money to buy the mining opportunity. By selling the portfolio after a single turn, a risk-less profit can be made, as according to our assumptions: $\Phi(t) > 0 = \Phi(t-1)$.

Case 2.b. If $\Phi(t) < 0$.

Short the portfolio at turn $t-1$ and return it after a single turn. Combining this case's assumptions we get:

$$\Phi(t-1) = 0 > \Phi(t) \tag{21}$$

After a single turn the portfolio has made a loss; thus the short has made a profit, which is again risk-less.

Case 2.c. If $\Phi(t) = 0$.

From our assumptions we get:

$$\Phi(t) = 0 = r\Phi(t-1) \tag{22}$$

Case 3. If $\Phi(t-1) < 0$.

Proceeding as in *Case 1.*:

Case 3.a. If $\rho(t) > r$.

Borrow enough money at the risk-free rate to short the portfolio (this costs money in the current world state). After a single turn,

return the short, receive $-\Phi(t)$, and pay back $-r\Phi(t-1)$ to repay the loan.

As $r > 1$, we get that $\rho(t) > r > 1$, thus from our assumption that $\Phi(t-1) < 0$ and from the return's definition in Equation 20:

$$\Phi(t) = \rho(t)\Phi(t-1) < r\Phi(t-1) < \Phi(t-1) < 0 \tag{23}$$

Conversely:

$$-\Phi(t) = -\rho(t)\Phi(t-1) > -r\Phi(t-1) > -\Phi(t-1) > 0 \tag{24}$$

Meaning that a risk-less profit has been made.

Case 3.b. If $0 \leq \rho(t) < r$.

Buy the portfolio at the first turn. As the portfolio cost is negative, buying it generates money; invest it at the risk-free rate for a single turn.

At the next turn, sell the portfolio. This costs a positive amount, according to the current world state, specifically $-\Phi(t)$. From the assumptions and the definition of the return as given by Equation 20:

$$r\Phi(t-1) < \rho(t)\Phi(t-1) = \Phi(t) \leq 0 \tag{25}$$

So:

$$-r\Phi(t-1) > -\rho(t)\Phi(t-1) = -\Phi(t) \geq 0 \tag{26}$$

$-\Phi(t)$ was lost by selling the portfolio, but the risk-free investment is worth $-r\Phi(t-1)$, enough to make a profit even after selling.

Case 3.c. If $\rho(t) < 0$.

As before, by buying the portfolio at the beginning, money is earned, and it can be invested at the risk-free rate. By the next turn, the portfolio is already worth a positive amount of money, thus selling it earns even more money. So, a risk-free profit was made.

All in all, if the return of the portfolio is not exactly the risk-free rate, there is an arbitrage opportunity and it is possible to make a sure profit in every world state, in contradiction to the no-arbitrage assumption; thus, the return has to equal the risk-free rate. □

Proof of Corollary 1. According to Claim 2:

$$\Phi(t) = r\Phi(t-1) \tag{27}$$

Rearranging we get:

$$\Phi(t-1) = \frac{\Phi(t)}{r} \tag{28}$$

Substituting by the definition of $\Phi(t-1)$ given in Equation 4:

$$V(t, t-1, C_{t-1}) - a_{t-1}C_{t-1} = \frac{\Phi(t)}{r} \tag{29}$$

We are interested in $V(t, t-1, C_{t-1})$, so we will isolate it:

$$V(t, t-1, C_{t-1}) = a_{t-1}C_{t-1} + \frac{\Phi(t)}{r} \tag{30}$$

By using Equation 18 to substitute for $\Phi(t)$:

$$V(t, t-1, C_{t-1}) = a_{t-1}C_{t-1} + \\ + \frac{1}{r}\left(V(t, t, \Delta C_{t-1}) - a_{t-1}\Delta C_{t-1}\right) \tag{31}$$

Slightly rearranging:

$$V(t, t-1, C_{t-1}) = a_{t-1}C_{t-1}\left(1 - \frac{\Delta}{r}\right) + \frac{V(t, t, \Delta C_{t-1})}{r} \tag{32}$$

Finally, substituting for a_{t-1} as given in Claim 1, an explicit form is reached:

$$V(t, t-1, C_{t-1}) = \frac{V(t, t, \Delta C_{t-1})}{r} + \\ \frac{V(t, t, \Delta C_{t-1}) - V(t, t, \delta C_{t-1})}{\Delta - \delta}\left(1 - \frac{\Delta}{r}\right) \tag{33}$$

Note that all factors are known and can be calculated at time $t-1$. Specifically, $V(t, t, \Delta C_{t-1})$ and $V(t, t, \delta C_{t-1})$ can be obtained by substituting for the correct exchange-rate in the definition given in Equation 1. □

Proof of Claim 3. At turn τ it seems the uncertainty regarding the coin's exchange rate at turn t is larger because there are $t - \tau + 1$ possible "final" future values instead of only 2, as shown in Figure 2 for the case where $t = 2$.

But, luckily, we are given $V(t, \tau+1, \Delta C_\tau), V(t, \tau+1, \delta C_\tau)$. We will use both values to construct a risk-free portfolio such that its value at $\tau+1$ will be the same no matter if the exchange-rate will go up or down. Similarly to Claim 1, it will hold the t-th opportunity, and a short on a_τ coins.

At turn $\tau + 1$ the portfolio's value is defined by:

$$\Phi(\tau) = V(t, \tau, C_\tau) - a_\tau C_\tau \tag{34}$$

And at $\tau + 1$ it is:

$$\Phi(\tau+1) = V(t, \tau+1, C_{\tau+1}) - a_\tau C_{\tau+1} \tag{35}$$

If the coin's exchange-rate has moved upwards between $\tau, \tau+1$, the portfolio will be worth:

$$\Phi(\tau+1) = V(t, \tau+1, \Delta C_\tau) - a_\tau \Delta C_\tau \tag{36}$$

Similarly for the down-state:

$$\Phi(\tau+1) = V(t, \tau+1, \delta C_\tau) - a_\tau \delta C_\tau \tag{37}$$

So, to make it risk-free the following property should hold:

$$V(t, \tau+1, \Delta C_\tau) - a_\tau \Delta C_\tau = V(t, \tau+1, \delta C_\tau) - a_\tau \delta C_\tau \tag{38}$$

Solving for a_τ gives the following short:

$$a_\tau = \frac{V(t, \tau+1, \Delta C_\tau) - V(t, \tau+1, \delta C_\tau)}{C_\tau(\Delta - \delta)} \tag{39}$$

In exactly the same manner as in the proof for Claim 2, the return of the portfolio at turn $\tau + 1$ is equal to r:

$$\Phi(\tau+1) = r\Phi(\tau) \tag{40}$$

Thus, by employing similar reasoning to Corollary 1 it is possible to derive the result:

$$V(t, \tau, C_\tau) = \frac{V(t, \tau+1, \Delta C_\tau)}{r} + \\ + \frac{V(t, \tau+1, \Delta C_\tau) - V(t, \tau+1, \delta C_\tau)}{\Delta - \delta}\left(1 - \frac{\Delta}{r}\right) \tag{41}$$

□

Proof for Theorem 1. Let $k < t$. We will start by applying Claim 3 on $V(t, k, C_k)$:

$$V(t, k, C_k) = \frac{V(t, k+1, \Delta C_k)}{r} + \\ + \frac{V(t, k+1, \Delta C_k) - V(t, k+1, \delta C_k)}{\Delta - \delta}\left(1 - \frac{\Delta}{r}\right) \tag{42}$$

Note that $V(t,k+1,\Delta C_k)$ appears in multiple places, by gathering all occurrences we get:

$$V(t,\tau,C_\tau) = \left(\frac{1-\frac{\Delta}{r}}{\Delta-\delta}+\frac{1}{r}\right)V(t,\tau+1,\Delta C_\tau) - \left(\frac{1-\frac{\Delta}{r}}{\Delta-\delta}\right)V(t,\tau+1,\delta C_\tau) \tag{43}$$

Denote $\gamma_\downarrow = \frac{1-\frac{\Delta}{r}}{\Delta-\delta}$, and $\gamma_\uparrow = \gamma_\downarrow + \frac{1}{r}$. So:

$$V(t,k,C_k) = \gamma_\uparrow V(t,k+1,\Delta C_k) - \gamma_\downarrow V(t,k+1,\delta C_k) \tag{44}$$

The opportunity's value is now represented as a recursive formula. Let us repeat the previous steps recursively on $V(t,k+1,\Delta C_k)$ and $V(t,k+1,\delta C_k)$:

$$V(t,k,C_k) = \gamma_\uparrow\left(\gamma_\uparrow V\left(t,k+2,\Delta^2 C_k\right) - \gamma_\downarrow V(t,k+2,\delta\Delta C_k)\right) - \gamma_\downarrow\left(\gamma_\uparrow V(t,k+2,\Delta\delta C_k) - \gamma_\downarrow V\left(t,k+2,\delta^2 C_k\right)\right) \tag{45}$$

Note that $V(t,k+2,\delta\Delta C_k)$ and $V(t,k+2,\Delta\delta C_k)$ are equal, so:

$$V(t,k,C_k) = \gamma_\uparrow^2 V\left(t,k+2,\Delta^2 C_k\right) - 2\gamma_\uparrow\gamma_\downarrow V(t,k+2,\Delta\delta C_k) + \gamma_\downarrow^2 V\left(t,k+2,\delta^2 C_k\right) \tag{46}$$

We can inductively continue with the recursion until reaching the exercise time of the opportunity, resulting in:

$$V(t,k,C_k) = = \sum_{\tau=0}^{t-k}\binom{t-k}{\tau}\gamma_\uparrow^\tau\left(-\gamma_\downarrow\right)^{t-k-\tau}V\left(t,t,\Delta^\tau\delta^{t-k-\tau}C_k\right) \tag{47}$$

Slightly rearranging:

$$V(t,k,C_k) = \sum_{\tau=0}^{t-k}\frac{\binom{t-k}{\tau}\gamma_\uparrow^\tau}{\left(-\gamma_\downarrow\right)^{k+\tau-t}}V\left(t,t,\Delta^\tau\delta^{t-k-\tau}C_k\right) \tag{48}$$

Note that the sum potentially goes over states where the opportunity's value is equal to zero, which is unnecessary. This can be avoided by starting the summation only from τ where:

$$V\left(t,t,\Delta^\tau\delta^{t-k-\tau}C_k\right) > 0 \tag{49}$$

By the definition given in Equation 1 this is the same as requiring:

$$\max\left(\frac{hb_t\Delta^\tau\delta^{t-k-\tau}C_k}{H(t)+h} - h\varphi e_t, 0\right) > 0 \tag{50}$$

As the opportunity's value is strictly greater than 0, the max can be dropped, resulting in:

$$\frac{b_t\delta^{t-k}C_k}{H(t)+h}\left(\frac{\Delta}{\delta}\right)^\tau > \varphi e_t \tag{51}$$

By isolating τ we can find the minimal turn where this condition is held. First, let us isolate $\frac{\Delta}{\delta}$:

$$\left(\frac{\Delta}{\delta}\right)^\tau > \frac{\varphi e_t}{\left(\frac{b_t\delta^{t-k}C_k}{H(t)+h}\right)} = \left(\frac{b_t\delta^{t-k}C_k}{H(t)+h}\right)^{-1}\cdot\varphi e_t \tag{52}$$

Now, take the logarithm of both sides:

$$\tau\cdot\log\left(\frac{\Delta}{\delta}\right) > \log\left(\left(\frac{b_t\delta^{t-k}C_k}{H(t)+h}\right)^{-1}\varphi e_t\right) \tag{53}$$

Finally, we can isolate τ:

$$\tau > \frac{\log\left(\left(\frac{b_t\delta^{t-k}C_k}{H(t)+h}\right)^{-1}\varphi e_t\right)}{\log\left(\frac{\Delta}{\delta}\right)} \tag{54}$$

So, the minimal turn for which the opportunity's value is greater than 0 is:

$$\tau_0 \triangleq \left\lceil\frac{\log\left(\left(\frac{b_t\delta^{t-k}C_k}{H(t)+h}\right)^{-1}\varphi e_t\right)}{\log\left(\frac{\Delta}{\delta}\right)}\right\rceil \tag{55}$$

Starting the summation from τ_0 gives the following equation:

$$V(t,k,C_k) = \sum_{\tau=\tau_0}^{t-k}\frac{\binom{t-k}{\tau}\gamma_\uparrow^\tau}{\left(-\gamma_\downarrow\right)^{k+\tau-t}}V\left(t,t,\Delta^\tau\delta^{t-k-\tau}C_k\right) \tag{56}$$

As noted before, thanks to summing only strictly positive values it is possible to drop the max, resulting in the following equation:

$$V(t,k,C_k) = \sum_{\tau=\tau_0}^{t-k}\frac{\binom{t-k}{\tau}\left(\gamma_\uparrow\right)^\tau h}{\left(-\gamma_\downarrow\right)^{k+\tau-t}}\left(\frac{b_tC_k\delta^{t-k}}{H(t)+h}\left(\frac{\Delta}{\delta}\right)^\tau - \varphi e_t\right) \tag{57}$$

□

Proof of Claim 4. This is done similarly to the proof of Claim 1. We want the portfolio to be worth the same as the underlying asset in the next turn, no matter the realization of the coin's exchange-rate.

If the exchange-rate has went up, the portfolio's value is:

$$\overline{\Phi}(\tau+1) = rB_\tau + \overline{a}_\tau\Delta C_\tau \tag{58}$$

If it went down, the value is:

$$\overline{\Phi}(\tau+1) = rB_\tau + \overline{a}_\tau\delta C_\tau \tag{59}$$

So, to find the correct values for $B_\tau, \overline{a}_\tau$ we will need to solve the following system of linear equations:

$$\Delta C_\tau\overline{a}_\tau + rB_\tau = V(t,\tau+1,\Delta C_\tau) \tag{60}$$

$$\delta C_\tau\overline{a}_\tau + rB_\tau = V(t,\tau+1,\delta C_\tau) \tag{61}$$

The only solution is:

$$\overline{a}_\tau = \frac{V(t,\tau+1,\Delta C_\tau) - V(t,\tau+1,\delta C_\tau)}{C_\tau(\Delta-\delta)} \tag{62}$$

$$B_\tau = \frac{\Delta V(t,\tau+1,\delta C_\tau) - \delta V(t,\tau+1,\Delta C_\tau)}{r(\Delta-\delta)} \tag{63}$$

□

Proof of Claim 5. According to Claim 4 and the definition given in Equation 9, the value of the portfolio at time $\tau+1$ is:

$$\overline{\Phi}(\tau+1) = rB_\tau + \overline{a}_\tau C_{\tau+1} = V(t,\tau+1,C_{\tau+1}) \tag{64}$$

Recall that the risk-free portfolio constructed in Claim 3 has the following value at $\tau + 1$:

$$\Phi(\tau + 1) = V(t, \tau + 1, C_{\tau+1}) - a_\tau C_{\tau+1} \tag{65}$$

By isolating the opportunity's value we get:

$$V(t, \tau + 1, C_{\tau+1}) = \Phi(\tau + 1) + a_\tau C_{\tau+1} \tag{66}$$

Thus, by substituting the above in Equation 64:

$$\overline{\Phi}(\tau + 1) = rB_\tau + \overline{a}_\tau C_{\tau+1} = \Phi(\tau + 1) + a_\tau C_{\tau+1} \tag{67}$$

Note that the amount of coins in both the portfolio of Claim 4 and the risk-free portfolio of Claim 3 is identical:

$$\overline{a}_\tau = \frac{V(t, \tau + 1, \Delta C_\tau) - V(t, \tau + 1, \delta C_\tau)}{C_\tau(\Delta - \delta)} = a_\tau \tag{68}$$

So both can be eliminated from Equation 67, resulting in:

$$rB_\tau = \Phi(\tau + 1) \tag{69}$$

As the proof of Claim 3 shows, specifically Equation 40, the return of risk-free portfolio is equal to the risk-free rate:

$$rB_\tau = r\Phi(\tau) \tag{70}$$

From the assumption that $r \neq 0$, it is possible to divide by it:

$$B_\tau = \Phi(\tau) \tag{71}$$

This equality can be used to replace B_τ in Equation 8, giving:

$$\overline{\Phi}(\tau) = \Phi(\tau) + \overline{a}_\tau C_\tau \tag{72}$$

Substituting for $\Phi(\tau)$ by using Equation 34:

$$\overline{\Phi}(\tau) = V(t, \tau, C_\tau) - a_\tau C_\tau + \overline{a}_\tau C_\tau \tag{73}$$

Finally, from Equation 68: $\overline{a}_\tau C_\tau - a_\tau C_\tau = 0$. We can deduce:

$$\overline{\Phi}(\tau) = V(t, \tau, C_\tau) \tag{74}$$

□

7 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.

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 thus increasing miner profits and, as a consequence, 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.

These two additions could allow using our model to estimate cryptocurrency parameters such as the global-hash rate (and thus, security relative to other coins) as dependent on the reward and difficulty adjustment mechanisms of the coin and its competitors, potentially helping to design better ones that avoid pitfalls like oscillations and "hash-wars". Additionally, the hash-rate could be analyzed in relation to the coin's exchange-rate and electricity price. As anecdotal evidence shows (see Figure 1), there is a correlation between these parameters.

ACKNOWLEDGMENTS

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

REFERENCES

J. Anish Dev. 2014. Bitcoin mining acceleration and performance quantification. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*. 1–6. https://doi.org/10.1109/CCECE.2014.6900989

Nick Arnosti and S. Matthew Weinberg. 2018. Bitcoin: A Natural Oligopoly. *arXiv e-prints*, Article arXiv:1811.08572 (Nov. 2018), arXiv:1811.08572 pages. arXiv:cs.CR/1811.08572

Susan Athey, Ivo Parashkevov, Vishnu Sarukkai, and Jing Xia. 2016. Bitcoin Pricing, Adoption, and Usage: Theory and Evidence.

M. Bedford Taylor. 2017. The Evolution of Bitcoin Hardware. *Computer* 50, 9 (2017), 58–66. https://doi.org/10.1109/MC.2017.3571056

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

R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor. 2018. Block arrivals in the Bitcoin blockchain. *ArXiv e-prints* (Jan. 2018). arXiv:cs.CR/1801.07447

Eric Budish. 2018. *The Economic Limits of Bitcoin and the Blockchain.* Working Paper 24717. National Bureau of Economic Research. https://doi.org/10.3386/w24717

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

Nicola Dimitri. 2017. Bitcoin Mining as a Contest. *Ledger* 2, 0 (2017), 31–37. https://doi.org/10.5195/ledger.2017.96

Avinash K. Dixit and Robert S. Pindyck. 1994. *Investment under Uncertainty.* Number 5474 in Economics Books. Princeton University Press. https://ideas.repec.org/b/pup/pbooks/5474.html

Ashutosh Dwivedi, Gautam Srivastava, and Rajani Singh. 2019. A Game Theoretic Analysis of Resource Mining in Blockchain. (11 2019).

Amos Fiat, Anna Karlin, Elias Koutsoupias, and Christos Papadimitriou. 2019. Energy Equilibria in Proof-of-Work Mining. In *Proceedings of the 2019 ACM Conference on Economics and Computation (EC âĂŹ19)*. Association for Computing Machinery, New York, NY, USA, 489âĂŞ502. https://doi.org/10.1145/3328526.3329630

A. Gervais, G. O. Karame, V. Capkun, and S. Capkun. 2014. Is Bitcoin a Decentralized Currency? *IEEE Security Privacy* 12, 3 (May 2014), 54–60. https://doi.org/10.1109/MSP.2014.49

Guy Goren and Alexander Spiegelman. 2019. Mind the Mining. *arXiv e-prints*, Article arXiv:1902.03899 (Feb 2019), arXiv:1902.03899 pages. arXiv:cs.CR/1902.03899

Timo Hanke. 2016. AsicBoost - A Speedup for Bitcoin Mining. *arXiv e-prints*, Article arXiv:1604.00575 (Apr 2016), arXiv:1604.00575 pages. arXiv:cs.CR/1604.00575

Adam Hayes. 2014. The Decision to Produce Altcoins: Miners' Arbitrage in Cryptocurrency Markets. (12 2014).

Adam S. Hayes. 2017. Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin. *Telematics and Informatics* 34, 7 (2017), 1308 – 1321. https://doi.org/10.1016/j.tele.2016.05.005

Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).

M. Rosenfeld. 2011. Analysis of Bitcoin Pooled Mining Reward Systems. *ArXiv e-prints* (Dec. 2011). arXiv:cs.DC/1112.4980

M. Salimitari, M. Chatterjee, M. Yuksel, and E. Pasiliao. 2017. Profit Maximization for Bitcoin Pool Mining: A Prospect Theoretic Approach. In *2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC)*. 267–274. https://doi.org/10.1109/CIC.2017.00043

Okke Schrijvers, Joseph Bonneau, Dan Boneh, and Tim Roughgarden. 2017. Incentive Compatibility of Bitcoin Mining Pool Reward Functions. In *Financial Cryptography and Data Security*, Jens Grossklags and Bart Preneel (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 477–498.

Eduardo S. Schwartz. 2004. Patents and R&D as Real Options. *Economic Notes* 33, 1 (2004), 23–54. https://doi.org/10.1111/j.0391-5026.2004.00124.x arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.0391-5026.2004.00124.x

Vikram B Suresh, Sudhir K Satpathy, and Sanu K Mathew. 2018. Optimized SHA-256 datapath for energy-efficient high-performance Bitcoin mining. US Patent 10,142,098.

Itay Tsabary and Ittay Eyal. 2018. The Gap Game. *arXiv e-prints*, Article arXiv:1805.05288 (May 2018), arXiv:1805.05288 pages. arXiv:cs.CR/1805.05288