

Correct Cryptocurrency ASIC Pricing: Are Miners Overpaying?

Aviv Yaish ✉ 

The Hebrew University, Israel

Aviv Zohar ✉ 

The Hebrew University, Israel

Abstract

Cryptocurrencies that are based on Proof-of-Work (PoW) often rely on special purpose hardware to perform so-called *mining* operations that secure the system, with miners receiving freshly minted tokens as a reward for their work. A notable example of such a cryptocurrency is Bitcoin, which is primarily mined using application specific integrated circuit (ASIC) based machines. Due to the supposed profitability of cryptocurrency mining, such hardware has been in great demand in recent years, in spite of high associated costs like electricity.

In this work, we show that because mining rewards are given in the mined cryptocurrency, while expenses are usually paid in some fiat currency such as the United States Dollar (USD), cryptocurrency mining is in fact a bundle of *financial options*. When exercised, each option converts electricity to tokens.

We provide a method of pricing mining hardware based on this insight, and prove that any other price creates arbitrage. Our method shows that contrary to the popular belief that mining hardware is worth less if the cryptocurrency is highly volatile, the opposite effect is true: volatility *increases* value. Thus, if a coin's volatility decreases, some miners may leave, affecting security.

We compare the prices produced by our method to prices obtained from popular tools currently used by miners and show that the latter only consider the expected returns from mining, while neglecting to account for the inherent risk in mining, which is due to the high exchange-rate volatility of cryptocurrencies.

Finally, we show that the returns made from mining can be imitated by trading in bonds and coins, and create such imitating investment portfolios. Historically, realized revenues of these portfolios have *outperformed* mining, showing that indeed hardware is mispriced.

2012 ACM Subject Classification Applied computing → Digital cash; Security and privacy → Economics of security and privacy

Keywords and phrases Cryptocurrency, Blockchain, Proof of Work, Economics

Digital Object Identifier [10.4230/LIPIcs.AFT.2023.2](https://doi.org/10.4230/LIPIcs.AFT.2023.2)

Related Version See the full version of the paper for proofs and additional details.

Full Version: <https://doi.org/10.48550/arXiv.2002.11064> [90]

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

1 Introduction

The cryptocurrency boom was heralded by the arrival of Bitcoin [56], which introduced the idea of a decentralized currency to the mainstream. Bitcoin relies on pseudonymous users called *miners* to operate the cryptocurrency's ledger in a decentralized manner. In particular, a computationally-heavy mechanism called PoW is used to achieve consensus between miners on the system's state and secure it from various attacks [72].

Miners are rewarded for their work via a form of computation based lottery, yielding additional rewards the more they compute on behalf of the system. These mining rewards have led to an arms-race in which miners purchase increasingly efficient and performant

hardware [6]. Today’s Bitcoin mining is mostly performed in industrial-scale mining “farms” hosting ASICs tailor-made for mining [61].

To stay competitive, miners buy mining rigs in advance at a significant capital expenditure, and they go to great lengths to keep their hardware’s electricity cost at a minimum [61]. Thus, miners turn off their machines if it is unprofitable to mine [58, 68, 46, 42], and even transport hardware between remote locations on a seasonal basis to save on electricity [62, 18, 40].

The profits derived from mining are highly volatile as they depend on the erratic exchange-rate of the cryptocurrency received as reward (see Figure 1) and on the level of competition from other miners. These factors make mining a risky investment and may indirectly hurt the cryptocurrency if fewer miners are there to secure it.

Despite the high-risk returns from mining, mining calculators utilize basic techniques to evaluate the price of mining hardware. These naïve approaches revolve around a metric called the *hashprice*, which assumes that the currency’s exchange-rate is *constant* and ignore the associated risk.

► **Definition 1 (Hashprice).** *The hashprice of a specific mining machine is the expected profit that it produces per unit of computation, given that the exchange-rate of the mined token and the computational power mining it are constant until the end-of-life of the machine.*

This metric was introduced by the Luxur mining pool [47], and is widely used by the community [54, 67, 26, 60]. Indeed, this metric is used by the top 8 websites which correspond to the keywords *mining calculator* [81, 48, 53, 86, 29, 59, 21, 25, 25], according to the web traffic analyzer *similarweb* [70]. These sites were frequently recommended on mining-related resources [91, 74].

1.1 Our Approach

In contrast to using the expected rewards as captured by the hashprice, we advance a more nuanced approach for evaluating cryptocurrency mining hardware, such as ASICs that accounts for risk attitudes regarding the exchange rate. Risk attitudes are subjective, and hard to measure but are reflected in the exchange rate itself. We utilize tools from financial option pricing to incorporate the market’s risk attitude into the ASIC pricing model.

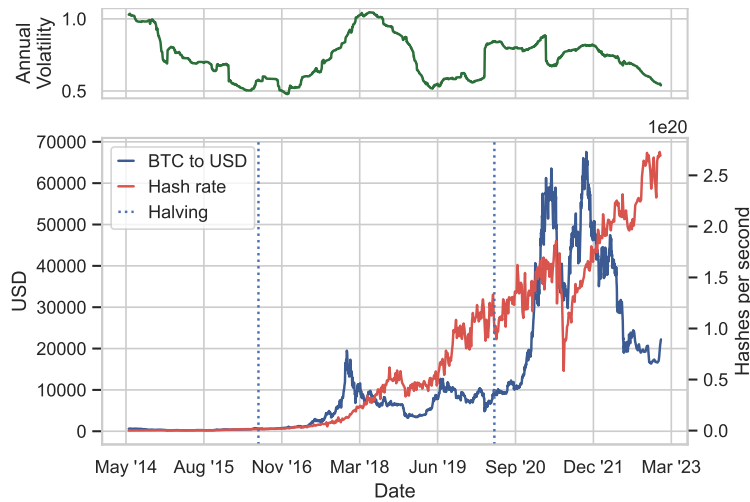
Specifically, we show that using publicly available information about the market (such as the interest-rate) and information about the efficiency of hardware (such as hash rate and power consumption of each device), one can derive a *correct* price for the hardware. This price is correct in the sense that any other price creates *arbitrage* and thus allows market forces to earn a risk-free profit.

Then, we construct an investment portfolio of tokens and bonds which *imitates* an ASIC and provides the same profits as a given mining machine. This portfolio has the same price as the correct price of the machine which it imitates. We empirically evaluate such imitating portfolios over historical data and show that they earn more than the corresponding ASICs, while costing less.

To obtain the correct price and an imitating portfolio which has an equal cost, we prove ASICs are equivalent to a bundle of *financial options* that allow their owners to exchange electricity for coins at different points in time. Then, we present algorithms which compute the correct hardware cost and the corresponding imitating portfolio.

Summary of Contributions

- **An economic model for PoW cryptocurrency mining.** We model mining while accounting for the inherent risk due to the volatile exchange-rate of cryptocurrencies. At



■ **Figure 1** Bitcoin's exchange rate, annual volatility and global hash-rate, as functions of time.

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. This is because 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.

- **An algorithm for pricing cryptocurrency mining hardware.** Using our model, we provide an algorithm that computes the price of an ASIC given its specifications and market parameters, without relying on subjective measures like a miner's risk preference or the expected exchange-rate of the mined cryptocurrency. We prove that any other price creates arbitrage.
- **The effects of risk and delay on the price of mining hardware.** We quantify the impact of the volatility of Bitcoin's exchange-rate and the delays miners frequently face when ordering new hardware on the value of mining machines.
- **Imitating portfolios for mining hardware.** We construct an *imitating portfolio* consisting of coins and bonds, which ideally provides the same returns as a specific ASIC.
- **Empirical evaluation.** We make a three-way comparison between historical hardware prices, the correct prices obtained by our results, and the costs of the corresponding imitating portfolios. Historically, our portfolios earn *more* than ASICs while costing less, even when considering trading fees. These results imply that ASICs are overpriced.

1.2 Motivating Example

To motivate our work, we show in Example 2 that the hashprice metric (given in Definition 1) is flawed. Furthermore, we show that more complex hardware pricing methods such as using the expected profit of a mining machine produce incorrect prices that create arbitrage opportunities.

► **Example 2.** A vendor offers the option of using its ASIC tomorrow to mine a single block. 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. For simplicity, let the interest rate be 1.

■ **Table 1** Balance of all assets on the first day of Example 2. In step #1, after selling the opportunity we have a -1 quantity of it, essentially performing a short on it.

#	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

Assume bitcoin's value starts at \$400 today, and will either double or halve tomorrow with equal probability. Note that per the definition of the hashrate metric (see Definition 1), the price of the option is $\$400 - \$250 = \$150$. Furthermore, this price does not depend on the exchange-rate's random walk, but rather solely on its current value.

A more complex method to evaluate the price of the option would be to use its expected profits. 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 exchange 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 it does not take exchange-rate volatility into account. We later show that the correct price is in fact $\$183\frac{1}{3}$.

To show why both \$150 and \$275 are *incorrect*, note that these prices create arbitrage opportunities. We proceed by constructing a trading strategy that capitalizes on the arbitrage created by the latter price, and note that a similar strategy can be used for the former. 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.

To fulfill the promise we do the following: immediately upon selling the opportunity we borrow $\$183\frac{1}{3}$ from the bank, giving us a total of $\$183\frac{1}{3} + \$274 = \$457\frac{1}{3}$. We buy $\frac{11}{12}$, which under the current exchange-rate are worth $\frac{11}{12} \cdot \$400 = \$366\frac{2}{3}$. After this, we remain with a profit of $\$457\frac{1}{3} - \$366\frac{2}{3} = \$90\frac{2}{3}$, which we pocket as a profit. This is summarized in Table 1.

If bitcoin's value goes up, our rational buyer will want to turn on the (imaginary) ASIC and receive the promised $\text{฿}1$ reward in exchange for the \$250 activation fee, which is paid to us. We use the fee to pay back the loan, leaving us with $\$250 - \$183\frac{1}{3} = \$66\frac{2}{3}$, exactly enough to buy $\frac{1}{12}$, that together with our existing $\frac{11}{12}$ 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. The balances throughout the day are 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 $\text{฿}1$ ($= \$200$) 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 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 started with no money, we made a riskless profit of $\$90\frac{2}{3}$ due to the *incorrect* pricing of the ASIC. In Section 4, we show how to correctly price it, and prove that when using our method no arbitrage opportunities arise.

■ **Table 2** Balance of all assets on the second day of Example 2, 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.	$\$90\frac{2}{3}$	$\$183\frac{1}{3}$	$\frac{11}{12}$	-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 3** Asset balance on the second day, if the exchange-rate has halved. Rational buyers will not activate the ASIC for a loss, thus there is a 0 amount of the opportunity at step #0.

#	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

Organization

This paper is structured as follows: we present additional background on cryptocurrencies and option theory in Section 2. We go on to define a mining model in Section 3, and present our methods for correctly pricing ASICs in Section 4, deferring most proofs to Appendix A. We then employ our methods to perform an empirical evaluation using real-world data in Section 5. We go over related work in Section 6 and conclude with a discussion on the implication of our results and future work in Section 7.

2 Background

We now go over preliminary details necessary for our work. We begin by describing in Section 2.1 the mechanisms which underlie PoW cryptocurrencies, and by reviewing the economical considerations made by real-world miners in Section 2.2. We finish by giving a brief overview of option theory in Section 2.3.

2.1 Cryptocurrencies

Bitcoin and other similar tokens let users exchange funds by creating *transactions* [36] that are collected in *blocks* in a decentralized manner by pseudonymous users called *miners*, who are allowed to freely join or leave the system. The creation of blocks is called *mining*. To enforce some chronological order on transactions, each block must point to a preceding one, with the resulting data-structure often referred to as a *blockchain*. Thus, a blockchain is in essence a decentralized ledger of transactions, where blocks should ideally be mined one after the other.

Proof-of-Work

Bitcoin relies on a mechanism called PoW to ensure miners invest some expected amount of effort to create blocks, thus preventing miners from maliciously retroactively changing the

ledger to their benefit [88]. This is enforced by requiring blocks to have a cryptographic hash [50] which is lower than some *target* value (when this hash is interpreted as a number). The hash function used in Bitcoin is *SHA256* [30]. Currently, the best known method for finding a low SHA256 hash is to try many different inputs by brute force [50]. Thus, the performance of mining hardware is measured by its *hash-rate*, the amount of hash calculations it can perform per unit of time. The mining target value is set by the mechanism to keep block creation rate roughly constant even when computational power is added to the network [89]. The specific mechanism overseeing this is called the *difficulty-adjustment algorithm (DAA)*. Thus, the probability that a single miner will create a block decreases if more hash-rate is competing against it.

In our work, we focus on Bitcoin. Historical data shows that Bitcoin’s hash-rate was consistently more than 100 times higher than the combined power of other popular cryptocurrencies [8]. This allows us to avoid considerations such as “coin-hopping” (wherein miners switch between mining different cryptocurrencies), similarly to other papers [32, 89, 72, 37, 79]. Indeed, previous research shows that such behavior is rare in practice [51].

Mining Incentives

To encourage mining even in the face of the ever-mounting computational effort required, Bitcoin and similar cryptocurrencies reward the creator of each block with a *block reward*. As the size of blocks is limited, users can incentivize miners to prefer their transaction over others by paying a *transaction fee* to the first miner that includes it in a block. Transaction fees have roughly amounted to 1.5% of Bitcoin mining profits over the past year [16].

Single miners do not expect to find a block often, and so the majority of bitcoin mining is done in mining *pools* [85, 69, 76], where miners mine cooperatively and split rewards amongst themselves according to their relative contribution. Thus, small and constant returns can be expected by miners who take part in pools.

2.2 Real-World Considerations of Miners

Cryptocurrency exchange-rates and electricity costs are important considerations for miners [61, 33, 57, 84]. This is affirmed by large-scale miners, who claim to respond to market changes by turning mining rigs on and off “at a minute’s notice” and “in real-time” [68, 46, 58]. Indeed, historical data indicates that miners rapidly turn hardware on and off, going as far as using old and inefficient hardware when the current rates deem it profitable [42]. On the other end of the spectrum, large-scale miners are not afraid of shutting hardware down for prolonged periods of time to move it to remote areas with cheap electricity [62, 18, 40].

Such behavior is facilitated by hardware and software vendors, who create products that are designed to rapidly switch between multiple low-power modes according to market conditions [10, 75, 42, 23, 22].

Even amateur miners use such optimizations by adopting after-market software that adds similar functionality to hardware which doesn’t have it by default [74, 12, 3, 15, 82, 13, 83, 24].

2.3 Financial Options

A European *call-option* is a 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 a specific future date, the *expiration date*. As this is a right and not an obligation, the buyer need not exercise it if deemed unprofitable. For

example, if by the date of expiry the underlying asset's price is lower than the strike price, it is preferable to buy the underlying asset directly and to discard the option.

In 1973, the Black-Scholes method for option valuation was proposed by [9], a seminal work in the field of option theory, and was later expanded upon by Merton [52]. Both rely on the *no-arbitrage* principle 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 [14, 78, 77, 27], for example the decision of whether to delay or abandon a project. This technique is called *real option valuation*.

Techniques from real option theory are introduced as needed throughout Section 4, with the required modifications for our setting. Further exploration of the topic is beyond the scope of this paper, but can be found in classic texts such as [19].

3 Model

We now describe an accurate model which accounts for the considerations made by real-world miners (see Section 2.2).

3.1 Mining Model

We divide time into discrete mining *opportunities* (or *turns*), and 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 R_t coins. This is a highly accurate approximation of the rewards earned by mining, as explained previously in Section 2.

Denote the ASIC's efficiency, measured in the Kilowatt-hours (kWhs) required for the computation of a mining opportunity, as φ , and the cost of electricity as e_t dollars per kWh.

To model hardware failures, we assume the ASIC “decays” gradually according to a mortality distribution: let $M(t)$ be the fraction of the ASIC that “remains” after t time units. For example, M can be a complementary cumulative density function (CDF) of some distribution [49]; let F be the CDF, then the complementary CDF is defined to be $1 - F$.

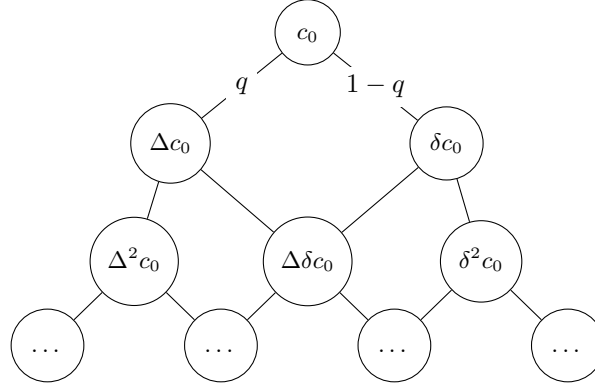
3.2 Financial Model

In our financial model of the world, for simplicity we call the mined cryptocurrency “Bitcoin”, and refer to the fiat currency in which mining expenses are paid for as the USD, but both can be replaced by any other similar cryptocurrency and fiat currency.

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 a binomial price tree. A general form of such a tree is depicted in Figure 2.

While it may seem simplistic to assume that the price at every step can either increase or decrease by a factor, using sufficiently small steps yields a granular price model. Indeed, this distribution is commonly used in finance to model the value of assets such as currencies and stocks [14, 64]. Note that the length of each step of the exchange-rate's random walk does not have to coincide with the length of a mining opportunity. As we focus on evaluating a single mining opportunity, we use arbitrarily small steps to achieve a high granularity.

Denote the economy's annual multiplicative risk-free rate as r . We assume $0 < \delta < 1 < r < \Delta$, otherwise, riskless arbitrage opportunities emerge, which we assume to not exist.



■ **Figure 2** A 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 .

This assumption is crystallized in Definition 3.

► **Definition 3** (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 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 the *risk-free rate*. An example of such an asset is a government-issued bond, the value of which is denoted by B .

We also create portfolios holding combinations of the above assets, and denote their values by $\Phi(\cdot)$. We assume that assets are traded with sufficient liquidity, a clearly defined price and that it is possible to hold a “short” position on each one (owing the asset to another party, equivalent to holding a negative amount of it).

4 Theoretical Results

In this section, we derive the main results that allow us to evaluate the price of a mining machine, with all proofs given in Appendix A.

4.1 Pricing an ASIC

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

► **Definition 4** (The value of the t -th mining opportunity, at turn k). *Let $k \leq t$. Given that the coin's exchange rate at k is c_k , we shall denote the value of the t -th opportunity at time k as $V(t, k, c_k)$.*

Some parameters (such as h) are left out of the notation for brevity.

Recall Example 2, which has demonstrated that it is hard to evaluate a future mining opportunity, e.g. calculate $V(t, k, c_k)$ when $k < t$, as the future exchange-rate is unknown. Specifically, that example examined a very basic case: $V(1, 0, \$400)$. Thus, we take a step back and attempt to evaluate something easier, starting with each option's "immediate" value, which we soon define, and use a series of theorems and claims to evaluate a future option's value relative to arbitrary points in time, thereby giving the tools to calculate $V(t, k, c_k)$.

Total ASIC Value

Assuming we have successfully evaluated ASIC activation for a single turn, we can evaluate an "entire" ASIC received at time s , relative to time $t \leq s$:

$$V_{ASIC}(s, t, c_t) \stackrel{\text{def}}{=} \sum_{\tau=s}^{\infty} M(\tau - s) \cdot V(\tau, t, c_t) \quad (1)$$

Reception Delay

A method for evaluating ASIC prices 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 orders in the far future, or charge a premium for early deliveries. Assuming ASICs do not decay while in transit, the loss of receiving an ASIC at time s' instead of s is:

$$V_{ASIC}(s', t, c_t) - V_{ASIC}(s, t, c_t) \quad (2)$$

4.2 Pricing the Current Mining Opportunity

We begin by evaluating the t -th opportunity relative to turn t . Following Definition 4, this is notated by $V(t, t, c_t)$. At turn t , we know everything required to calculate the value of the t -th mining opportunity, as the biggest cause of uncertainty, the cryptocurrency's exchange rate c_t , is given. Thus, we call $V(t, t, c_t)$ the *immediate* value of the t -th mining opportunity.

Immediate Value of a Single Opportunity

At the t -th mining opportunity, an ASIC's owner has the option of paying the electricity cost of activating the ASIC for the duration of the opportunity, which under our model is $h \cdot \varphi \cdot e_t$, and in return receive the partial reward of $\frac{h}{H(t)+h} \cdot R_t \cdot c_t$. This opportunity can never be worth strictly less than zero, as a miner is not obliged to turn on its ASIC, and indeed a rational miner will not do so if it incurs a loss.

In total, the value at time t of the t -th mining opportunity is:

$$V(t, t, c_t) \stackrel{\text{def}}{=} \max \left(\frac{h}{H(t)+h} R_t c_t - h \varphi e_t, 0 \right) \quad (3)$$

Shutdown Price

Immediately arising from Equation (3) is that if the cost of turning on the ASIC exceeds the profits, meaning that $\frac{h}{H(t)+h} R_t c_t \leq h \varphi e_t$, then no miner will turn it on, as paying the activation cost to buy the mined cryptocurrency on the free market is a better deal than actually using the hardware. This corresponds with the behavior of actual miners, as described in Section 2.2.

4.3 Pricing the Next Mining Opportunity

We now tackle the problem presented in the previous section more generally – pricing the t -th mining opportunity in relation to turn $t - 1$. We do so by modifying techniques from option-pricing theory (as in [9, 28]). Specifically, to price this mining opportunity, we construct a portfolio of mining opportunities and coins at turn $t - 1$.

The portfolio is crafted to yield identical valuations at turn t regardless of the change in the exchange-rate (see Claim 5). Thus, it is termed a *risk-free* portfolio. Its exact value at $t - 1$ can be known by discounting and accounting for the risk-free rate (see Theorem 6).

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:

$$\Phi(t-1) = V(t, t-1, c_{t-1}) - a_{t-1}c_{t-1} \quad (4)$$

And, its value at turn t is:

$$\Phi(t) = V(t, t, c_t) - a_{t-1}c_t \quad (5)$$

▷ **Claim 5.** A portfolio holding the t 'th mining opportunity and a short on a_{t-1} coins, where: $a_{t-1} = \frac{V(t, t, \Delta c_{t-1}) - V(t, t, \delta c_{t-1})}{c_{t-1}(\Delta - \delta)}$, is a risk free-portfolio for the turn between $t - 1$, t . The portfolio's value in all possible states at t is: $\Phi(t) = V(t, t, \Delta c_{t-1}) - a_{t-1}\Delta c_{t-1}$.

Appendix A contains a formal proof. The main idea is that there is one degree of freedom (choosing the short amount, a_{t-1}) which must satisfy an equation equating the value of the portfolio in both possible world states.

We now evaluate the return of the portfolio, and use it to price the mining opportunity.

► **Theorem 6.** *If no arbitrage opportunities exist, the multiplicative return of holding the portfolio constructed in Claim 5 between turns $t - 1$ and t is equal to the risk-free rate.*

The proof (given in Appendix A) shows that every other return contradicts the no-arbitrage assumption. As in Example 2, we can make a risk-free profit whenever such arbitrage opportunities arise.

We now reach an expression for the opportunity's price:

► **Corollary 7.** *The value of the t -th opportunity at $t - 1$ is:*

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

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

We provide a proof in Appendix A. 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 $t - 1$.

In Example 8, we revisit Example 2 and apply Corollary 7 to it.

► **Example 8.** Surprisingly, the price of the opportunity shown in Example 2 is lower than the naïve estimate. The opportunity's immediate value if the exchange-rate has gone up is:

$$V(1, 1, 800) = \max(1 \cdot 800 - 250, 0) = \$550$$

And, for the down state it is:

$$V(1, 1, 200) = \max(1 \cdot 200 - 250, 0) = \$0$$

By plugging the above into Corollary 7 we obtain the correct value of the opportunity at turn 0:

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

According to Theorem 6, any other price creates arbitrage.

4.4 Pricing Relative to an Arbitrary Time

Algorithm 1 extends the previous method to evaluate the t -th opportunity relative to any previous point in time k . The idea behind the algorithm is to apply the same methods of Section 4.3 on every possible world-state, starting from turn t and going back, one step at a time, until reaching k . We now proceed to explain the method in depth.

■ Algorithm 1 MiningOpportunityValue

Input : t - the mining opportunity to evaluate.
 k - the turn to evaluate relative to.
 c_k - coin's exchange-rate at turn k .

Output: value of t -th opportunity at turn k .

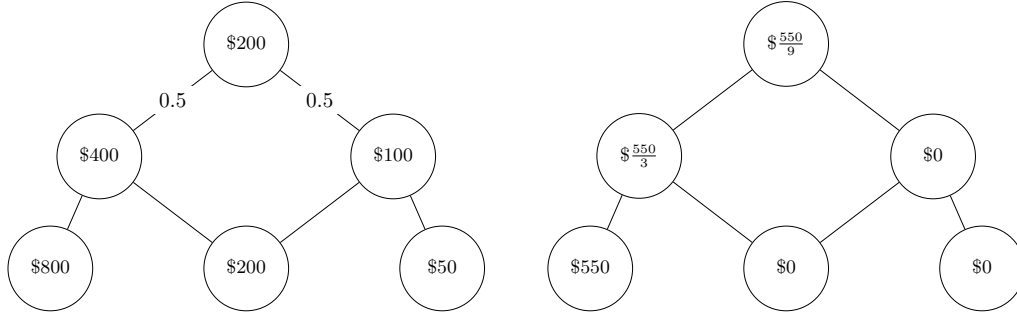
for $c_t \in \{\Delta^{t-k} \cdot c_k, \Delta^{t-k-1} \cdot \delta \cdot c_k, \dots, \delta^{t-k} \cdot c_k\}$ **do**
 $V(t, t, c_t) \leftarrow h \cdot \max\left(\frac{R_t \cdot c_t}{H(t)+h} - \varphi \cdot e_t, 0\right)$
end
for $\tau \in t-1, \dots, k$ **do**
 for $c_\tau \in \{\Delta^\tau c_k, \Delta^{\tau-1} \delta c_k, \dots, \Delta \delta^{\tau-1} c_k, \delta^\tau c_k\}$ **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 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 corresponds to a possible world state at turn t . As the opportunity expires at that turn, its value can be calculated directly from the definition given in Equation (3).

Proceeding inductively, let $\tau \in [k, t-1]$. We shall evaluate the opportunity at one of the vertices of the $(\tau-k)$ -th level, assume it is c_τ . It points to two vertices from level $\tau-k+1$, specifically $\Delta c_\tau, \delta c_\tau$. Section 4.3 suggests that if the opportunity values for these two vertices are already calculated, the opportunity's value at c_τ 's world-state can be obtained. Claim 9 covers this case.

▷ **Claim 9.** 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:

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



(a) Example 11's equiprobable two turn random walk, with a starting exchange-rate of \$200 per BTC. (b) The value of Example 11's mining opportunity at each possible world state, according to Algorithm 1.

■ **Figure 3** Visual depictions of the possible states for Example 11's exchange-rate random walk, and the corresponding mining opportunity values and imitating portfolios.

The proof is given in Appendix A. It uses 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 7.

By applying Claim 9 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 .

A formula for a mining opportunity's value

Careful mathematical reasoning can be applied to Algorithm 1 to derive a formula for the value of the t -th opportunity:

► **Theorem 10.** Let $\gamma_{\downarrow} = \frac{1 - \frac{\Delta}{r}}{\Delta - \delta}$, $\gamma_{\uparrow} = \gamma_{\downarrow} + \frac{1}{r}$, $\tau_0 = \left\lceil \frac{\log\left(\frac{(H(t)+h)\varphi e_t}{R_t \delta^{t-k} c_k}\right)}{\log\left(\frac{\Delta}{\delta}\right)} \right\rceil$. The value of the t -th mining opportunity at turn $k < t$ is:

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

The proof is given in Appendix A. By recursively applying Claim 9 on $V(t, k, c_k)$, a sum that only includes values of immediate opportunities is reached; this sum is shortened by ignoring opportunities with zero value. By Theorem 6, the value which is obtained is the only one which does not violate the no-arbitrage principle.

Example 11 shows how to use Theorem 10 in a complex setting.

► **Example 11.** Assume that bitcoin's exchange-rate at turn 0 is \$200, and can either double or halve with equal probability. Extending the walk to two turns produces the tree in Figure 3a.

Furthermore, assume the vendor from Example 2 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 3b. The algorithm proceeds as follows:

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 9 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 9 again together with our previous results, we find that the opportunity is worth $\$ \frac{550}{9}$ at the first turn.

4.5 Imitating Portfolio

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

Imitating an ASIC's revenue using purely financial means (e.g., an investment portfolio of tokens) might be better – it can start to produce revenue immediately without waiting, and avoids the aforementioned expenses. In Theorem 12, we show construct such a portfolio using coins and bonds.

► **Theorem 12.** *At turn τ , it is possible to construct an imitating portfolio for the t -th mining opportunity which is comprised of tokens and bonds. If this portfolio is properly adjusted at each turn until reaching time t , it can be sold to produce the same profits as the imitated mining opportunity.*

The proof relies on a series of claims, which we go over now. The portfolio we construct imitates the t -th opportunity between turns $\tau, \tau + 1$, for $\tau < t$. Denote by $\bar{a}_\tau, B_\tau$ 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:

$$\bar{\Phi}(\tau) = B_\tau + \bar{a}_\tau \cdot c_\tau \quad (6)$$

And, at $\tau + 1$ it is

$$\bar{\Phi}(\tau + 1) = r \cdot B_\tau + \bar{a}_\tau \cdot c_{\tau+1} \quad (7)$$

► **Claim 13.** If 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 world-states of turn $\tau + 1$: $\bar{\Phi}(\tau + 1) = V(t, \tau + 1, c_{\tau+1})$. This portfolio is comprised of $\bar{a}_\tau$ tokens and B_τ risk-free bonds, where:

$$\begin{aligned} \bar{a}_\tau &= \frac{V(t, \tau + 1, \Delta \cdot c_\tau) - V(t, \tau + 1, \delta \cdot c_\tau)}{c_\tau \cdot (\Delta - \delta)} \\ B_\tau &= \frac{\Delta \cdot V(t, \tau + 1, \delta \cdot c_\tau) - \delta \cdot V(t, \tau + 1, \Delta \cdot c_\tau)}{r \cdot (\Delta - \delta)} \end{aligned}$$

The proof is similar to that of Claim 5, see Appendix A for details.

► **Claim 14.** At turn τ , the portfolio constructed in Claim 13 is equal in value to the t -th mining opportunity: $\bar{\Phi}(\tau) = V(t, \tau, c_\tau)$.

The proof is given in Appendix A. It relies on showing that at turn τ the risk-free portfolio of Claim 9 is equal in value to B_τ . Finally, the claim is reached by applying algebraic manipulations to the definitions of the risk-free portfolio and the portfolio of Claim 13.

We finish the proof of Theorem 12 by combining Claims 13 and 14.

► **Corollary 15.** *The portfolio of Claim 13 is an imitating portfolio for the t -th mining opportunity between turns $\tau, \tau + 1$, meaning the portfolio is equal in value to the opportunity at both turns. Additionally, if there are no fees, selling the imitating portfolio for turns $\tau, \tau + 1$ at turn $\tau + 1$ generates enough money to buy the imitating portfolio for $\tau + 1, \tau + 2$. Thus, after the initial investment is made, no influx of funds is required to adjust the portfolio between turns, meaning that the initial purchase of the portfolio costs exactly the same as the opportunity that it imitates.*

Like in Section 4.4, the imitating portfolio can be evaluated at multiple time periods by dynamically moving backwards in time. Algorithm 2 provides an algorithmic construction of such a portfolio. If the portfolio changes between turns, the necessary adjustments cost additional fees; these are included in the empirical evaluation given in Section 5.

■ **Algorithm 2** ImitateMiningOpportunity

Input : t - the mining opportunity to imitate.
 k - the turn to at which to create the portfolio.
 c_k - coin's exchange-rate at turn k .

Output: an imitating portfolio for the t -th opportunity relative to turn k .

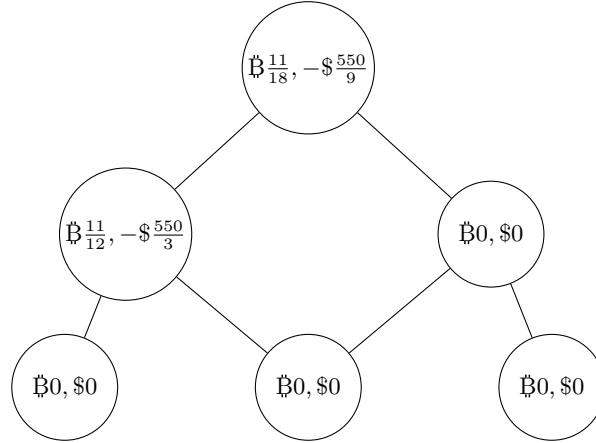
$\bar{a}_t \leftarrow 0$
 $B_t \leftarrow 0$
for $c_t \in \{\Delta^{t-k} \cdot c_k, \Delta^{t-k-1} \cdot \delta \cdot c_k, \dots, \delta^{t-k} \cdot c_k\}$ **do**
 $V(t, t, c_t) \leftarrow h \cdot \max\left(\frac{R_t \cdot c_t}{H(t)+h} - \varphi \cdot e_t, 0\right)$
end
for $\tau \in t-1, \dots, k$ **do**
 for $c_\tau \in \{\Delta^\tau c_k, \Delta^{\tau-1} \delta c_k, \dots, \Delta \delta^{\tau-1} c_k, \delta^\tau c_k\}$ **do**
 $\bar{a}_\tau \leftarrow \frac{V(t, \tau+1, \Delta \cdot c_\tau) - V(t, \tau+1, \delta \cdot c_\tau)}{c_\tau \cdot (\Delta - \delta)}$
 $B_\tau \leftarrow \frac{\Delta \cdot V(t, \tau+1, \delta \cdot c_\tau) - \delta \cdot V(t, \tau+1, \Delta \cdot c_\tau)}{r \cdot (\Delta - \delta)}$
 $\bar{\Phi}(\tau) \leftarrow B_\tau + \bar{a}_\tau c_\tau$
 $V(t, \tau, c_\tau) \leftarrow \bar{\Phi}(\tau)$
 end
end
return $\{(\bar{a}_\tau, B_\tau) \mid \tau \in k, \dots, t\}$

In Example 16, we construct an imitating portfolio using the results of Section 4.5.

► **Example 16.** Recall Example 11, we revisit it and construct imitating portfolios for each of the example's states. These portfolios are summarized in Figure 4. Portfolios are comprised of holdings in coins and bonds, thus we represent them as tuples where the left item is the amount of coins, and the right one is the bonds' value in USD. Portfolios are sold on the last turn, so all final portfolios hold no assets. The portfolios are constructed like so.

First, evaluate the opportunity's price at all states. Next, apply Claim 13 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. Finally, the portfolio for the first state has $\frac{\frac{550}{3} - 0}{200(2-0.5)} = \frac{11}{18}$ coins and $\frac{2 \cdot 0 - \frac{1}{2} \cdot \frac{550}{3}}{1 \cdot (2-0.5)} = -\frac{550}{9}$ bonds.

To show that these portfolios are indeed imitating, we analyze their returns on the final



■ **Figure 4** Imitating portfolios for each possible world-state of Example 16, per Algorithm 2.

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 , so 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 gives 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, equal to the opportunity's.

5 Empirical Evaluation

We now employ our methods on real world data, deriving prices for the *Bitmain Antminer S9*, an ASIC which has dominated the market for an extended period of time, and constitutes around 33% of the currently active hash-rate on Bitcoin [42, 84].

5.1 Parameters

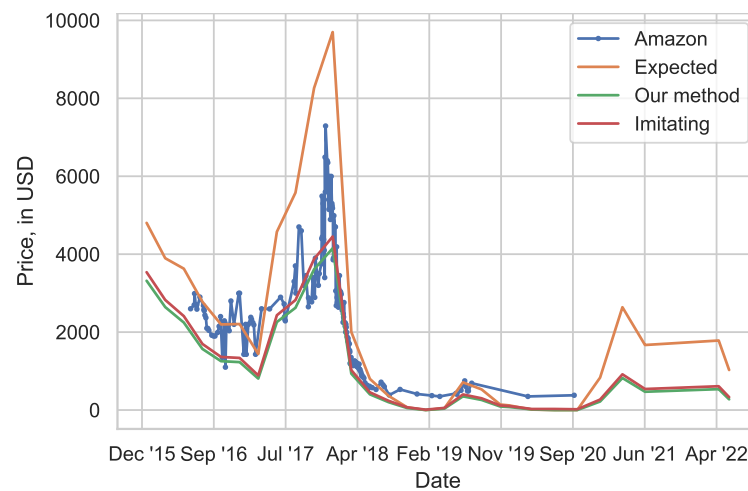
The parameters which are used throughout this section were obtained from real-world data, and were set to the following values:

ASIC price and specifications

We compare our prices to historical market prices which were obtained from the manufacturer's Amazon page. We took hardware specification from [80], and assumed ASICs last 2 years on average. In fact, hash-rate considerations imply that their profits vanish even faster.

Mining and imitation fees

In our evaluation, we compare between ASICs and their corresponding imitating portfolios. If there were multiple options for relevant parameters, we always chose the ones that make the imitating portfolios' job harder:



■ **Figure 5** ASIC prices according to different valuation methods, as functions of time, including the costs associated with the corresponding imitating portfolios.

- *Electricity fees* were set to \$0.035 per kWh, lower than the average rates paid by industrial users and miners in the US [35, 1].
- *Mining pool fees* were set to 2%. Large pools (consistently comprising at least 40% of Bitcoin’s hash-rate over the past year) have asked for 2.5% [38, 16, 87].
- *Trading fees* for bonds and BTC-to-USD were set to 1%, more than fees offered by large companies. For example, Coinbase asks for 0.6% at most [20].

Exchange rate, hashrate and interest rate

The historical BTC-to-USD exchange-rate and global hashrate were taken from blockchain.com. Annual volatility, defined as the standard deviation of log-returns, and future global hash-rate growth (which we assumed to be exponential in accordance with the literature [11]) were evaluated using data starting at 2013 and ending at the estimation date. The economy’s annual risk-free rate was set to 2%.

5.2 Results

We now go over the results of our empirical evaluation.

Official Prices Do Not Account For Risk

We obtain the correct prices for the Antminer S9 by using Algorithm 1 with parameters corresponding to various points in time.

Figure 5 compares prices given by our method to Bitmain’s official Amazon prices, and to a naïve evaluation method anecdotally used by miners (labeled “Expected”), which assumes the future BTC-USD exchange-rate will continue its recent rate of growth. This naïve method ignores risk and uses only expected values, as in Example 2. The official prices are closer to the naïve price, suggesting that *they do not fully account for risk*.

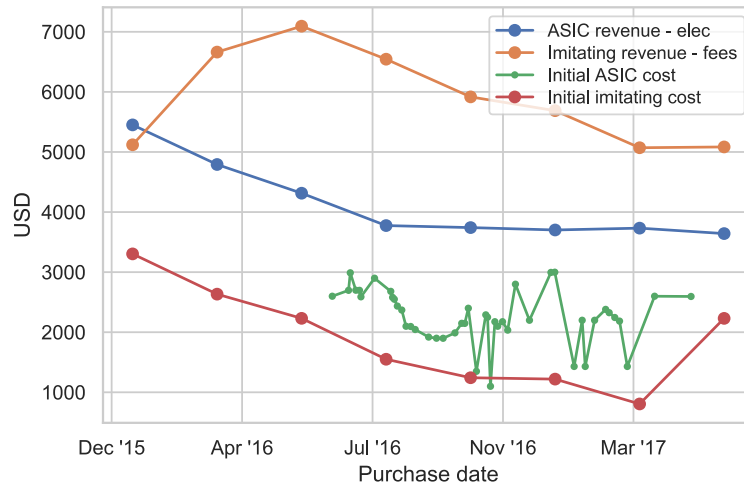


Figure 6 Realized revenue (after expenses) and initial cost for a 2-year operation of an ASIC and its corresponding imitating portfolio. An ASIC's initial cost is its Amazon price, and its expenses are the electricity it consumes. The portfolio's initial cost is the cost of buying it, and its expenses are the trading fees required for maintaining it over 2 years.

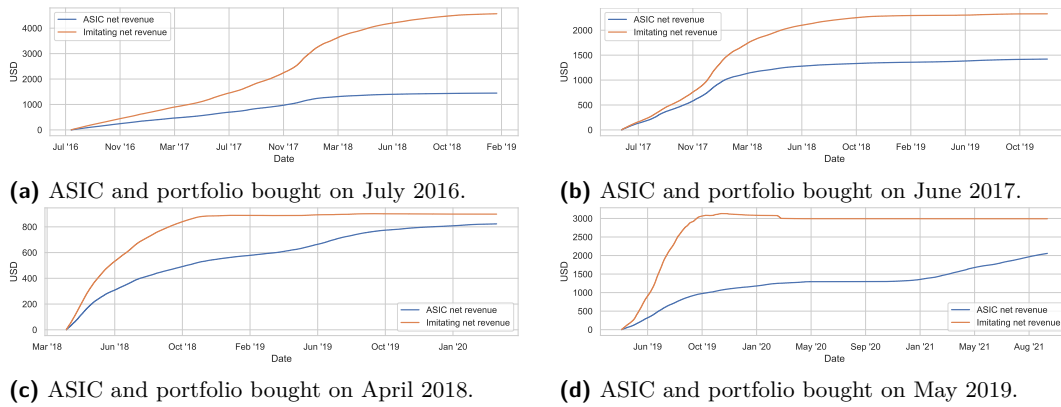


Figure 7 Realized revenue (after expenses) of an ASIC and its imitating portfolio, each bought for \$1000 at different points in time.

Imitating Portfolios

We now utilize Algorithm 2 to produce imitating portfolios for the Antminer S9. These portfolios are benchmarked and compared to the actual hardware using the realized exchange-rates and hash-rates to evaluate the returns made by each.

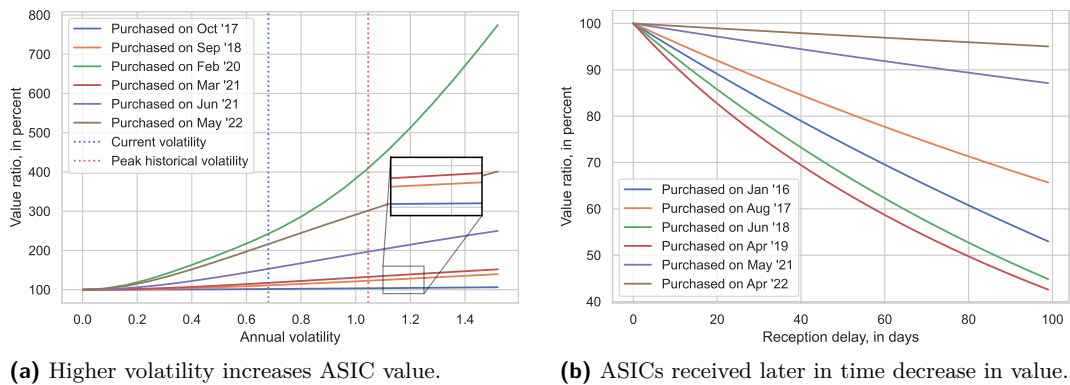
When evaluated on recent data, our imitating portfolios earned more than the equivalent ASICs, while costing less to buy and maintain, meaning ASICs are overpriced.

Figure 6 aggregates *realized* revenues and initial costs of ASICs and the corresponding imitating portfolios. We assume ASICs are received and activated *immediately* after purchase, which is far from typical as usually miners wait a long time to receive hardware. The revenue for both is *after* deducting all expenses (electricity for ASICs, and trading fees for portfolios).

Similarly, Figure 7 compares the realized revenue (after expenses) obtained from investing \$1000 in an imitating portfolio with an equal investment in real mining hardware.

Our imitating portfolio's revenue is not equal to an ASIC's because of a gap between

2:18 Correct Cryptocurrency ASIC Pricing: Are Miners Overpaying?



■ **Figure 8** The effects of volatility and delay on hardware value.

the realized and projected growth rates of the network's total hash-rate. Also, a portfolio's accuracy increases with the granularity of its time-steps, while the adjustments made at every step might increase its cost. We used 25 steps per mining opportunity, which empirically produces accurate results.

To provide an additional angle on these results, we show in Figure 5 both the correct prices of mining hardware over time, and the total cost of the corresponding imitating portfolios, including the average-case fees paid for all necessary adjustments. Although an imitating portfolio is more expensive when compared to the correct price, it still costs less than the official price.

Volatility Increases Value

Figure 8a depicts our evaluation of ASIC prices as a function of volatility, where each line represents a different purchase date. Bitcoin's annual volatility, as estimated on September 9th, 2021, and its peak annual volatility, which occurred in the year preceding April 29th, 2018, are depicted as vertical lines.

Our method gives higher prices for ASICs when volatility is higher. For example, an ASIC bought on June 2021 could cost 20% more if the volatility was at its historical peak.

Of note is the increase in value for hardware bought on February 2020. This can be explained by the crash in global hashrate experienced at the beginning of 2021 (see Figure 1). The combination of high volatility and low hashrate means that it is profitable to turn on hardware which might not be the most efficient or powerful (equivalently, the hardware's shutdown price is lower).

Reception Delay Decreases Value

By applying Equation (2) on historical data, we learn that a delay in the reception of an ASIC can severely lower its value, with a month's delay decreasing value by 30%, as seen in Figure 8b.

6 Related Work

To the best of our knowledge, our work is the first to evaluate the price of mining hardware, and to show that mining hardware can be imitated by purely financial means.

Economic Models of Mining

Other works have attempted to model the economics of mining without evaluating hardware prices, but most of these have not addressed the risk inherent in exchange-rate fluctuations and their affect on the economics of mining. For example [44, 45, 55], examine mining revenue in an economic setting where different cryptocurrencies co-exist. Several papers explore single-token economic 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. [4, 31], or works such as [71], which consider a myopic Nash equilibrium in a game model of the bitcoin market. An equilibrium of miners in a bounded horizon setting is explored in [34, 39], both show that miners may gain by turning their hardware on and off repeatedly, thereby taking advantage of difficulty adjustments.

Some tried accounting for risk, for example [5], where the price of bitcoin (but not of mining hardware) is based on user adoption and friction due to exchange-rate uncertainty, or [7] which focuses on estimating hashrate allocation between multiple tokens by using miner risk-preference to estimate their expected revenue, which our method shows can give an incorrect result.

Concurrently and independently of our work, [43] consider mining hardware as an option, but present a simpler model that lacks several factors inherent to the mining market such as: changing electricity costs, hardware decay and delivery delays. Our work also adds an empirical evaluation of the model compared to historical data and an analysis of the performance of imitating portfolios.

Economic Models of Cryptocurrency Security

An analysis of Bitcoin's security in a model where miner rewards are based on transaction fees and block-rewards are negligible is carried out in [79]. An economic analysis of the security of Bitcoin is performed by [17], arguing that when the currency is under attack, its value drops, causing mining hardware to lose value. In [88], it is shown that a malicious mining strategy strictly dominates the honest one in Ethereum-like cryptocurrencies, meaning that attacking the cryptocurrency is riskless when compared to the "honest" mining protocol, but can earn more profits.

Improving Mining Performance and Mining Pools

Some works attempted to improve the performance of mining machines [2, 41, 73], thus also increasing profits. But, these do not analyze the value of mining hardware.

A different approach is for so-called "solo" miners to operate as part of mining pools, which are coalitions of miners who mine together to get a steadier revenue-flow. Indeed, most mining is performed by pools [85]; thus, risk-aversion is believed to be widespread among miners. The economics of pools were examined by [63, 66, 65], which again neglected risk.

7 Conclusion

In this paper we show that widespread notions regarding ASIC prices and their dependence on subjective measures like projected expected exchange-rates are flawed. Instead, we present a method for *correctly* pricing mining hardware, and show ASICs can be *imitated* using bonds and tokens.

Popular opinion holds that as Bitcoin becomes more widely used, its volatility will decrease. Our evaluation shows that a decrease in volatility negatively affects the value of

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. As Bitcoin's security relies on miner participation, lower mining revenues hurt security and undermine Bitcoin's usage as a currency.

Future Work

The security risk inherent in lower volatility can be addressed by adopting random reward mechanisms to artificially increase volatility: if rewards are made to follow a random walk, the returns of miners become more volatile, thus increasing potential profits and miner participation. To prevent miners from foreseeing future profits and stopping mining, rewards should be determined post-hoc.

We 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 additions could allow using our results to estimate the global-hash rate as dependent on the reward and difficulty adjustment mechanisms of a coin and its competitors, potentially helping to design better ones that avoid pitfalls like selfish-mining and "hash-wars". Hash-rate could also be analyzed in relation to a coin's exchange-rate, which are correlated according to anecdotal evidence, see Figure 1.

References

- 1 U.S. Energy Information Administration. Electric power monthly, 2022. URL: https://web.archive.org/web/20220818154159/https://www.eia.gov/electricity/monthly/epm_table_grapher.php?t=epmt_5_6_a.
- 2 J. Anish Dev. Bitcoin mining acceleration and performance quantification. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–6, San Francisco, CA, USA, May 2014. IEEE. doi:10.1109/CCECE.2014.6900989.
- 3 Antpool. Antminertool manual, 2020. URL: <https://web.archive.org/web/20201111172854/https://www.antpool.com/download/tools/002-BulkManagement-en.pdf>.
- 4 Nick Arnosti and S. Matthew Weinberg. Bitcoin: A Natural Oligopoly. *Management Science*, 68(7):4755–4771, 2022. arXiv:<https://doi.org/10.1287/mnsc.2021.4095>, doi:10.1287/mnsc.2021.4095.
- 5 Susan Athey, Ivo Parashkevov, Vishnu Sarukkai, and Jing Xia. Bitcoin pricing, adoption, and usage: Theory and evidence, 2016.
- 6 M. Bedford Taylor. The evolution of bitcoin hardware. *Computer*, 50(9):58–66, 2017. doi:10.1109/MC.2017.3571056.
- 7 George Bissias, Brian N. Levine, and David Thibodeau. Using economic risk to model miner hash rate allocation in cryptocurrencies. In Joaquin Garcia-Alfaro, Jordi Herrera-Joancomartí, Giovanni Livraga, and Ruben Rios, editors, *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pages 155–172, Cham, 2018. Springer International Publishing.
- 8 BitInfoCharts. Bitcoin, ethereum, dogecoin, xrp, ethereum classic, litecoin, monero, bitcoin cash, zcash, bitcoin gold hashrate historical chart, 2022. URL: <https://web.archive.org/web/20220522122528/https://bitinfocharts.com/comparison/hashrate-btc-eth-doge-xrp-etc-ltc-xmr-bch-zec-btg.html#3y>.
- 9 Fischer Black and Myron Scholes. The pricing of options and corporate liabilities. *Journal of political economy*, 81(3):637–654, 1973. doi:10.1086/260062.

- 10 Blockstream. Instant energy demand from the bitcoin network, 2021. URL: <https://web.archive.org/web/20210824180952/https://blockstream.com/energy/>.
- 11 R. Bowden, H. P. Keeler, A. E. Krzesinski, and P. G. Taylor. Modeling and analysis of block arrival times in the bitcoin blockchain. *Stochastic Models*, 36(4):602–637, 2020. [arXiv:https://doi.org/10.1080/15326349.2020.1786404](https://doi.org/10.1080/15326349.2020.1786404), doi:10.1080/15326349.2020.1786404.
- 12 braiins. Braiins os & braiins os+ custom asic firmware: optimize performance & efficiency, 2018. URL: <https://web.archive.org/web/20210812132518/https://bitcointalk.org/index.php?topic=5036844.0>.
- 13 BRAIINS. Autotuning mining firmware, 2022. URL: <https://web.archive.org/web/20220425034423/https://braiins.com/os/plus>.
- 14 Luiz E Brandão, James S Dyer, and Warren J Hahn. Using binomial decision trees to solve real-option valuation problems. *Decision Analysis*, 2(2):69–88, 2005. doi:10.1287/deca.1050.0040.
- 15 BTC.com. Using btc tools to do miners’ batch management, 2019. URL: <https://web.archive.org/web/20201129045355/https://help.pool.btc.com/hc/en-us/articles/360020105012-Miners-Batch-Management>.
- 16 BTC.com. Pool stats, 2022. URL: https://web.archive.org/web/20220820062646/https://btc.com/stats/pool?pool_mode=year.
- 17 Eric Budish. The economic limits of bitcoin and the blockchain. Working Paper 24717, National Bureau of Economic Research, June 2018. URL: <http://www.nber.org/papers/w24717>, doi:10.3386/w24717.
- 18 Scott Chipolina. Bitcoin’s hash rate drops as china’s rainy season ends, 2020. URL: <https://web.archive.org/web/20211117210216/https://decrypt.co/46601/bitcoin-hash-rate-drop-attributed-to-chinese-rainy-season>.
- 19 John H Cochrane. *Asset pricing: Revised edition*. Princeton university press, Princeton, NJ, USA, 2009.
- 20 Coinbase. What are the fees on coinbase pro?, 2022. URL: <https://web.archive.org/web/20220406132137/https://help.coinbase.com/en/pro/trading-and-funding/trading-rules-and-fees/fees>.
- 21 CoinWarz. Bitcoin mining calculator, 2022. URL: <https://web.archive.org/web/20220514110643/https://www.coinwarz.com/mining/bitcoin/calculator>.
- 22 Bitmain Technologies Holding Company. S19 server installation guide, 2020. URL: <https://web.archive.org/web/20220520122512/https://file12.bitmain.com/shop-product-s3/firmware/4e25b493-58d5-4986-8cff-52006dda2038/2022/01/19/17/S19ServerManual.pdf>.
- 23 Bitmain Technologies Holding Company. Difference between low power mode and low power enhanced mode, 2022. URL: <https://web.archive.org/web/20220309092700/https://support.bitmain.com/hc/en-us/articles/360019738593-Difference-between-Low-Power-Mode-and-Low-Power-Enhanced-Mode>.
- 24 Bitmain Technologies Holding Company. Recommended antminer monitor and management tools (apminertool & btc tool), 2022. URL: <https://web.archive.org/web/20220309090337/https://support.bitmain.com/hc/en-us/articles/360023257293-Recommended-Antminer-monitor-and-management-tools-APMinerTool-BTC-Tool->.
- 25 BRAIINS Bitcoin Mining Company. Bitcoin mining profitability calculator, 2022. URL: <https://web.archive.org/web/20220714050553/https://insights.braiins.com/en/profitability-calculator/>.
- 26 BRAIINS Mining Company. Mining insights, 2022. URL: <https://web.archive.org/web/20220818165736/https://insights.braiins.com/en/>.
- 27 Tom Copeland and Vladimir Antikarov. *Real options*. Texere New York, New York, NY, USA, 2001.
- 28 John C Cox, Stephen A Ross, and Mark Rubinstein. Option pricing: A simplified approach. *Journal of financial Economics*, 7(3):229–263, 1979. doi:10.1016/0304-405x(79)90015-1.

- 29 CryptoCompare. Bitcoin mining profitability calculator, 2022. URL: <https://web.archive.org/web/20220513095414/https://www.cryptocompare.com/mining/calculator/btc?HashingPower=40&HashingUnit=TH/s&PowerConsumption=1500&CostPerkWh=0.12&MiningPoolFee=1>.
- 30 Quynh H Dang et al. Secure hash standard, 2015. doi:10.6028/nist.fips.180-4.
- 31 Nicola Dimitri. Bitcoin mining as a contest. *Ledger*, 2(0):31–37, 2017. URL: <http://ledger.pitt.edu/ojs/index.php/ledger/article/view/96>, doi:10.5195/ledger.2017.96.
- 32 Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In *International conference on financial cryptography and data security*, volume 61, pages 436–454. Springer, Association for Computing Machinery (ACM), jun 2014. doi:10.1145/3212998.
- 33 Amanda Fabiano. Today @bitcoinbeezy gave a great talk at the @bitmaintech event focusing on how we, as a financing company, evaluate miners., 2022. URL: https://web.archive.org/web/20220726183620/https://twitter.com/_amanda_fab/status/1551999454433132544.
- 34 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. doi:10.1145/3328526.3329630.
- 35 Cambridge Centre for Alternative Finance. Cambridge bitcoin electricity consumption index, 2022. URL: <https://web.archive.org/web/20220818013329/https://ccaf.io/cbeci/index>.
- 36 Yotam Gafni and Aviv Yaish. Greedy transaction fee mechanisms for (non-)myopic miners, 2022. URL: <https://arxiv.org/abs/2210.07793>, doi:10.48550/ARXIV.2210.07793.
- 37 Juan Garay, Aggelos Kiayias, and Nikos Leonardos. The bitcoin backbone protocol: Analysis and applications. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, pages 281–310, Berlin, Heidelberg, 2015. Springer.
- 38 Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gün Sirer. Decentralization in bitcoin and ethereum networks. In Sarah Meiklejohn and Kazue Sako, editors, *Financial Cryptography and Data Security*, pages 439–457, Berlin, Heidelberg, 2018. Springer.
- 39 Guy Goren and Alexander Spiegelman. Mind the mining. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, EC '19, page 475–487, New York, NY, USA, 2019. Association for Computing Machinery. doi:10.1145/3328526.3329566.
- 40 Samuel Haig. Btc hash rate slumps amid seasonal miner migration in china, 2020. URL: <https://cointelegraph.com/news/btc-hash-rate-slumps-amid-seasonal-miner-migration-in-china>.
- 41 Timo Hanke. AsicBoost - A Speedup for Bitcoin Mining, Apr 2016. arXiv:1604.00575.
- 42 Colin Harper and Ethan Vera. Hashrate index 2021 year-end report, 2022. URL: <https://web.archive.org/web/20220113191729/https://blog.hashrateindex.com/content/files/2022/01/Hashrate-Index-2021-Year-End-Report.pdf>.
- 43 Yoshinori Hashimoto and Shunya Noda. Pricing of mining asic and its implication to the high volatility of cryptocurrency prices, 2019. doi:10.2139/ssrn.3368286.
- 44 Adam Hayes. The decision to produce altcoins: Miners' arbitrage in cryptocurrency markets, 12 2014. doi:10.2139/ssrn.2579448.
- 45 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. URL: <http://www.sciencedirect.com/science/article/pii/S0736585315301118>, doi:10.1016/j.tele.2016.05.005.
- 46 Christopher Helman. How this billionaire-backed crypto startup gets paid to not mine bitcoin, 2020. URL: <https://web.archive.org/web/20200524160256/https://www.forbes.com/sites/christopherhelman/2020/05/21/how-this-billionaire-backed-crypto-startup-gets-paid-to-not-mine-bitcoin/#7bdc51b97596>.

- 47 Hashrate Index. Bitcoin hashprice index, 2022. URL: <https://web.archive.org/web/20220714205330/https://data.hashrateindex.com/chart/bitcoin-hashprice-index>.
- 48 Hashrate Index. Profitability calculator, 2022. URL: <https://web.archive.org/web/20220623021224/https://hashrateindex.com/tools/calculator>.
- 49 Harold Jeffreys. *The theory of probability*. OUP Oxford, Oxford, UK, 1998. doi:10.2307/2669965.
- 50 Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, New York, dec 2020. doi:10.1201/9781351133036.
- 51 Sishan Long, Soumya Basu, and Emin Gün Sirer. Measuring miner decentralization in proof-of-work blockchains, 2022. URL: <https://arxiv.org/abs/2203.16058>, doi:10.48550/ARXIV.2203.16058.
- 52 Robert Merton. Theory of rational option pricing. *Bell Journal of Economics*, 4(1):141–183, 1973.
- 53 minerstat. Mining profitability calculator, 2022. URL: <https://web.archive.org/web/20220530152147/https://minerstat.com/mining-calculator>.
- 54 Compass Mining. What is hashprice?, 2021. URL: <https://web.archive.org/web/20211019011808/https://compassmining.io/education/what-is-hashprice/>.
- 55 Michael Mirkin, Yan Ji, Jonathan Pang, Arian Klages-Mundt, Ittay Eyal, and Ari Juels. Bdos: Blockchain denial-of-service. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, CCS '20, page 601–619, New York, NY, USA, 2020. Association for Computing Machinery. doi:10.1145/3372297.3417247.
- 56 Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008. URL: <https://web.archive.org/web/20100704213649/https://bitcoin.org/bitcoin.pdf>.
- 57 John Naughton. As energy prices soar, the bitcoin miners may find they have struck fool's gold, 2022. URL: <https://web.archive.org/web/20220717043121/https://www.theguardian.com/commentisfree/2022/jun/11/as-energy-prices-soar-the-bitcoin-miners-may-find-they-have-struck-fools-gold>.
- 58 Bloomberg News. Bitcoin 'hash crash' rebound points to miners plugging back in, 2021. URL: <https://www.bloomberg.com/news/articles/2021-09-03/bitcoin-hash-crash-rebound-points-to-miners-plugging-back-in>.
- 59 NiceHash. Profitability calculator, 2022. URL: <https://web.archive.org/web/20220519093350/https://www.nicehash.com/profitability-calculator>.
- 60 Lumin Protocol. What is hashprice?, 2022. URL: <https://web.archive.org/web/20220314144723/https://medium.com/lumin-blog/what-is-hashprice-9651cb08b215>.
- 61 Michel Rauchs and Garrick Hileman. *Global Cryptocurrency Benchmarking Study*. Cambridge Centre for Alternative Finance, Cambridge Judge Business School, University of Cambridge, Cambridge, United Kingdom, 2017. URL: <https://EconPapers.repec.org/RePEc:jbs:altfin:201704-gcbs>.
- 62 Jamie Redman. Chinese bitcoin miners migrate north after wet season, 2019. URL: <https://web.archive.org/web/20220427014036/https://news.bitcoin.com/chinese-bitcoin-miners-migrate-north-after-wet-season/>.
- 63 M. Rosenfeld. Analysis of Bitcoin Pooled Mining Reward Systems, December 2011. arXiv:1112.4980.
- 64 Mark Rubinstein. Implied binomial trees. *The journal of finance*, 49(3):771–818, 1994. doi:10.1111/j.1540-6261.1994.tb00079.x.
- 65 M. Salimitari, M. Chatterjee, M. Yuksel, and E. Pasilião. 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, San Francisco, CA, USA, Oct 2017. IEEE. doi:10.1109/CIC.2017.00043.
- 66 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.
- 67 Spencer Sherwood. Why bitcoin asic prices can reach new highs in 2022, 2022. URL: <https://web.archive.org/web/20220127160904/https://miningstore.com/understanding-the-bitcoin-mining-rig-market/why-bitcoin-asic-prices-can-reach-new-highs-in-2022/>.
 - 68 MacKenzie Sigalos. As major winter storm descends on texas, bitcoin miners are helping the power grid brace for impact, 2022. URL: <https://web.archive.org/web/20220203143819/https://www.cnn.com/2022/02/03/winter-storm-descends-on-texas-bitcoin-miners-shut-off-to-protect-ercot.html>.
 - 69 Paulo Silva, David Vavricka, João Barreto, and Miguel Matos. Impact of geo-distribution and mining pools on blockchains: A study of ethereum. In *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 245–252, San Francisco, CA, USA, June 2020. IEEE. doi:10.1109/DSN48063.2020.00041.
 - 70 similarweb. Website traffic - check and analyze any website, 2022. URL: <https://web.archive.org/web/20220818075305/https://www.similarweb.com/>.
 - 71 Rajani Singh, Ashutosh Dhar Dwivedi, Gautam Srivastava, Agnieszka Wiszniewska-Matyskiel, and Xiaochun Cheng. A game theoretic analysis of resource mining in blockchain. *Cluster Computing*, 23(3):2035–2046, 2020. doi:10.1007/s10586-020-03046-w.
 - 72 Yonatan Sompolinsky and Aviv Zohar. Bitcoin’s security model revisited, 2016. arXiv:1605.09193.
 - 73 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.
 - 74 taserz. Asic.to firmware s17+ 95th/s • t17+ 80th/s t17 40w/t • s17/t17 on over 250k asic, 2019. URL: <https://web.archive.org/web/20210812103613/https://bitcointalk.org/index.php?topic=5208500.0>.
 - 75 Layer1 Technologies. Building bitcoin batteries, 2019. URL: <https://web.archive.org/web/20220401125045/https://layer1.com/>.
 - 76 Natkamon Tovanich, Nicolas Soulié, and Petra Isenberg. Visual analytics of bitcoin mining pool evolution: On the road toward stability? In *2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pages 1–5, San Francisco, CA, USA, April 2021. IEEE. doi:10.1109/NTMS49979.2021.9432675.
 - 77 Lenos Trigeorgis et al. *Real options: Managerial flexibility and strategy in resource allocation*. MIT press, Cambridge, MA, USA, 1996.
 - 78 Lenos Trigeorgis and Jeffrey J Reuer. Real options theory in strategic management. *Strategic Management Journal*, 38(1):42–63, 2017.
 - 79 Itay Tsabary and Ittay Eyal. The gap game. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS ’18*, page 713–728, New York, NY, USA, 2018. Association for Computing Machinery. doi:10.1145/3243734.3243737.
 - 80 ASIC Miner Value. Asic miner value, 2021. URL: <https://www.asicminervalue.com/>.
 - 81 ASIC Miner Value. Miners profitability, 2022. URL: <https://web.archive.org/web/20220808050607/https://www.asicminervalue.com/>.
 - 82 Ethan Vera. What is bitcoin mining firmware?, 2020. URL: <https://web.archive.org/web/20220520114305/https://blog.hashrateindex.com/asic-custom-firmware-guide/>.
 - 83 VNISH. Firmware for overclocking and downvolt antminer s17pro s17 s17+, 2022. URL: <https://web.archive.org/web/20220520134308/https://vnish-firmware.com/en/razgon-antminer-s17-s17pro-s17/>.
 - 84 Gian M. Volpicelli. As bitcoin falters, crypto miners brace for a crash, May 2022. URL: <https://web.archive.org/web/20220531110502/https://www.wired.co.uk/article/bitcoin-mining-crisis>.
 - 85 Canhui Wang, Xiaowen Chu, and Yang Qin. Measurement and analysis of the bitcoin networks: A view from mining pools. In *2020 6th International Conference on Big Data Computing and*

- Communications (BIGCOM)*, pages 180–188, San Francisco, CA, USA, 2020. IEEE, IEEE. [arXiv:1902.07549](https://arxiv.org/abs/1902.07549), [doi:10.1109/bigcom51056.2020.00032](https://doi.org/10.1109/bigcom51056.2020.00032).
- 86 whattomine. Crypto coins mining profit calculator, 2022. URL: <https://web.archive.org/web/20220729175135/https://whattomine.com/>.
- 87 Bitcoin Wiki. Comparison of mining pools, 2022. URL: https://web.archive.org/web/20220819173306/https://en.bitcoin.it/wiki/Comparison_of_mining_pools.
- 88 Aviv Yaish, Gilad Stern, and Aviv Zohar. Uncle maker: (time)stamping out the competition in ethereum. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23)*, CCS '23, New York, NY, USA, 2023. Association for Computing Machinery. [doi:10.1145/3576915.3616674](https://doi.org/10.1145/3576915.3616674).
- 89 Aviv Yaish, Saar Tochner, and Aviv Zohar. Blockchain stretching & squeezing: Manipulating time for your best interest. In *Proceedings of the 23rd ACM Conference on Economics and Computation*, EC '22, page 65–88, New York, NY, USA, 2022. Association for Computing Machinery. [doi:10.1145/3490486.3538250](https://doi.org/10.1145/3490486.3538250).
- 90 Aviv Yaish and Aviv Zohar. Pricing asics for cryptocurrency mining, 2023. [arXiv:2002.11064](https://arxiv.org/abs/2002.11064).
- 91 Kristina Zucchi. Is bitcoin mining profitable?, July 2022. URL: <https://web.archive.org/web/20220815040240/https://www.investopedia.com/articles/forex/051115/bitcoin-mining-still-profitable.asp>.

A Proofs

In this section, we prove the theorems and claims used throughout the paper.

A.1 Pricing a Single Mining Opportunity

▷ **Claim 5.** A portfolio holding the t 'th mining opportunity and a short on a_{t-1} coins, where: $a_{t-1} = \frac{V(t, t, \Delta c_{t-1}) - V(t, t, \delta c_{t-1})}{c_{t-1}(\Delta - \delta)}$, is a risk free-portfolio for the turn between $t - 1, t$. The portfolio's value in all possible states at t is: $\Phi(t) = V(t, t, \Delta c_{t-1}) - a_{t-1} \Delta c_{t-1}$.

Proof of Claim 5. 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:

$$V(t, t, \Delta c_{t-1}) = \max \left(\frac{h R_t \Delta c_{t-1}}{H(t) + h} - h \varphi e_t, 0 \right) \quad (8)$$

And of the down state as:

$$V(t, t, \delta c_{t-1}) = \max \left(\frac{h R_t \delta c_{t-1}}{H(t) + h} - h \varphi e_t, 0 \right) \quad (9)$$

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 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 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:

$$\Phi(t) = V(t, t, \Delta c_{t-1}) - a_{t-1} \Delta c_{t-1} \quad (10)$$

And, at the down-state:

$$\Phi(t) = V(t, t, \delta c_{t-1}) - a_{t-1} \delta c_{t-1} \quad (11)$$

So, we require that the following equality will hold:

$$V(t, t, \Delta c_{t-1}) - a_{t-1} \Delta c_{t-1} = V(t, t, \delta c_{t-1}) - a_{t-1} \delta c_{t-1} \quad (12)$$

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

$$a_{t-1} = \frac{V(t, t, \Delta c_{t-1}) - V(t, t, \delta c_{t-1})}{c_{t-1} (\Delta - \delta)} \quad (13)$$

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 (10)–(12) we get that by doing this short, our portfolio's value at turn t is:

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

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:

$$\begin{aligned} \Phi(t) &= \frac{V(t, t, \Delta c_{t-1}) - V(t, t, \delta c_{t-1})}{\Delta - \delta} \Delta \\ &\quad - V(t, t, \Delta c_{t-1}) \end{aligned} \quad (15)$$

◀

► **Theorem 6.** *If no arbitrage opportunities exist, the multiplicative return of holding the portfolio constructed in Claim 5 between turns $t - 1$ and t is equal to the risk-free rate.*

Proof of Theorem 6. The proof mainly relies on the no-arbitrage assumption. First, we define the multiplicative return of our portfolio between $t - 1$ and t as:

$$\rho(t) \stackrel{\text{def}}{=} \frac{\Phi(t)}{\Phi(t-1)} \quad (16)$$

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

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

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

- 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.

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 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.

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

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

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 5 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:

$$\Phi(t) > 0 = \Phi(t - 1) \quad (17)$$

b. If $\Phi(t) < 0$. Short the portfolio at $t - 1$ and return it after a single turn. By combining this case's assumptions:

$$\Phi(t - 1) = 0 > \Phi(t) \quad (18)$$

After one turn the portfolio has made a loss and the short has made a risk-less profit.

c. If $\Phi(t) = 0$. From our assumptions we get:

$$\Phi(t) = 0 = r\Phi(t - 1) \quad (19)$$

3. If $\Phi(t - 1) < 0$. Proceeding as in 1:

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

Borrow enough money at the risk-free rate to short the portfolio (this costs money in the current state). After one turn, return the short, receive $-\Phi(t)$, and pay back $-r\Phi(t - 1)$ to repay the loan.

As $r > 1$, we get that

$$\rho(t) > r > 1 \quad (20)$$

Thus, from our assumption that $\Phi(t - 1) < 0$ and from the return's definition in Equation (16):

$$\begin{aligned} \Phi(t) &= \rho(t) \Phi(t - 1) \\ &< r\Phi(t - 1) \\ &< \Phi(t - 1) \\ &< 0 \end{aligned} \quad (21)$$

We deduce that conversely:

$$\begin{aligned}
-\Phi(t) &= -\rho(t) \Phi(t-1) \\
&> -r\Phi(t-1) \\
&> -\Phi(t-1) \\
&> 0
\end{aligned} \tag{22}$$

Meaning that a risk-less profit has been made.

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 (16):

$$\begin{aligned}
r\Phi(t-1) &< \rho(t) \Phi(t-1) \\
&= \Phi(t) \\
&\leq 0
\end{aligned} \tag{23}$$

So, we deduce:

$$\begin{aligned}
-r\Phi(t-1) &> -\rho(t) \Phi(t-1) \\
&= -\Phi(t) \\
&\geq 0
\end{aligned} \tag{24}$$

$-\Phi(t)$ 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.

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. ◀

► **Corollary 7.** *The value of the t -th opportunity at $t-1$ is:*

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

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

Proof of Corollary 7. According to Theorem 6:

$$\Phi(t) = r\Phi(t-1) \tag{25}$$

By rearranging, we get:

$$\Phi(t-1) = \frac{\Phi(t)}{r} \tag{26}$$

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

$$V(t, t-1, c_{t-1}) - a_{t-1}c_{t-1} = \frac{\Phi(t)}{r} \quad (27)$$

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

$$V(t, t-1, c_{t-1}) = a_{t-1}c_{t-1} + \frac{\Phi(t)}{r} \quad (28)$$

By using Equation (14) to substitute for $\Phi(t)$:

$$\begin{aligned} V(t, t-1, c_{t-1}) &= \frac{1}{r} (V(t, t, \Delta c_{t-1}) - a_{t-1}\Delta c_{t-1}) \\ &\quad + a_{t-1}c_{t-1} \end{aligned} \quad (29)$$

Slightly rearranging:

$$\begin{aligned} V(t, t-1, c_{t-1}) &= a_{t-1}c_{t-1} \left(1 - \frac{\Delta}{r}\right) \\ &\quad + \frac{V(t, t, \Delta c_{t-1})}{r} \end{aligned} \quad (30)$$

Finally, substituting for a_{t-1} as given in Claim 5, an explicit form is reached:

$$\begin{aligned} V(t, t-1, c_{t-1}) &= \frac{V(t, t, \Delta c_{t-1}) - V(t, t, \delta c_{t-1})}{\Delta - \delta} \left(1 - \frac{\Delta}{r}\right) \\ &\quad + \frac{V(t, t, \Delta c_{t-1})}{r} \end{aligned} \quad (31)$$

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 Equation (3). ◀

A.2 Pricing Relative to an Arbitrary Time

▷ **Claim 9.** 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:

$$\begin{aligned} V(t, \tau, c_\tau) &= \frac{V(t, \tau+1, \Delta c_\tau) - V(t, \tau+1, \delta c_\tau)}{\Delta - \delta} \left(1 - \frac{\Delta}{r}\right) \\ &\quad + \frac{V(t, \tau+1, \Delta c_\tau)}{r} \end{aligned}$$

Proof of Claim 9. 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 $V(t, \tau+1, \Delta c_\tau)$ and $V(t, \tau+1, \delta c_\tau)$. We 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 5, 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:

$$\Phi(\tau) = V(t, \tau, c_\tau) - a_\tau c_\tau \quad (32)$$

2:30 Correct Cryptocurrency ASIC Pricing: Are Miners Overpaying?

And at $\tau + 1$ it is:

$$\Phi(\tau + 1) = V(t, \tau + 1, c_{\tau+1}) - a_{\tau} c_{\tau+1} \quad (33)$$

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

$$\Phi(\tau + 1) = V(t, \tau + 1, \Delta c_{\tau}) - a_{\tau} \Delta c_{\tau} \quad (34)$$

Similarly for the down-state:

$$\Phi(\tau + 1) = V(t, \tau + 1, \delta c_{\tau}) - a_{\tau} \delta c_{\tau} \quad (35)$$

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

$$V(t, \tau + 1, \Delta c_{\tau}) - a_{\tau} \Delta c_{\tau} = V(t, \tau + 1, \delta c_{\tau}) - a_{\tau} \delta c_{\tau} \quad (36)$$

Solving for a_{τ} gives the following short:

$$a_{\tau} = \frac{V(t, \tau + 1, \Delta c_{\tau}) - V(t, \tau + 1, \delta c_{\tau})}{c_{\tau} (\Delta - \delta)} \quad (37)$$

Exactly the same as in the proof for Theorem 6, the return of the portfolio at turn $\tau + 1$ is equal to r :

$$\Phi(\tau + 1) = r \Phi(\tau) \quad (38)$$

Thus, by employing similar reasoning to Corollary 7 it is possible to derive the result:

$$\begin{aligned} V(t, \tau, c_{\tau}) &= \frac{V(t, \tau + 1, \Delta c_{\tau}) - V(t, \tau + 1, \delta c_{\tau})}{\Delta - \delta} \left(1 - \frac{\Delta}{r}\right) \\ &\quad + \frac{V(t, \tau + 1, \Delta c_{\tau})}{r} \end{aligned} \quad (39)$$

◀

► **Theorem 10.** Let $\gamma_{\downarrow} = \frac{1 - \frac{\Delta}{r}}{\Delta - \delta}$, $\gamma_{\uparrow} = \gamma_{\downarrow} + \frac{1}{r}$, $\tau_0 = \left\lceil \frac{\log\left(\frac{(H(t)+h)\varphi e_t}{R_t \delta^{t-k} c_k}\right)}{\log\left(\frac{\Delta}{\delta}\right)} \right\rceil$. The value of the t -th mining opportunity at turn $k < t$ is:

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

Proof for Theorem 10. Let $k < t$. We start by applying Claim 9 on $V(t, k, c_k)$:

$$\begin{aligned} V(t, k, c_k) &= \frac{V(t, k + 1, \Delta c_k) - V(t, k + 1, \delta c_k)}{\Delta - \delta} \left(1 - \frac{\Delta}{r}\right) \\ &\quad + \frac{V(t, k + 1, \Delta c_k)}{r} \end{aligned} \quad (40)$$

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

$$\begin{aligned} V(t, \tau, c_{\tau}) &= \left(\frac{1 - \frac{\Delta}{r}}{\Delta - \delta} + \frac{1}{r}\right) V(t, \tau + 1, \Delta c_{\tau}) \\ &\quad - \left(\frac{1 - \frac{\Delta}{r}}{\Delta - \delta}\right) V(t, \tau + 1, \delta c_{\tau}) \end{aligned} \quad (41)$$

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

$$V(t, k, c_k) = \gamma_{\uparrow} V(t, k+1, \Delta c_k) - \gamma_{\downarrow} V(t, k+1, \delta c_k) \quad (42)$$

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 $V(t, k+1, \delta c_k)$:

$$\begin{aligned} V(t, k, c_k) &= \gamma_{\uparrow} \cdot \left(\gamma_{\uparrow} \cdot V(t, k+2, \Delta^2 c_k) \right. \\ &\quad \left. - \gamma_{\downarrow} \cdot V(t, k+2, \delta \Delta c_k) \right) \\ &\quad - \gamma_{\downarrow} \cdot \left(\gamma_{\uparrow} \cdot V(t, k+2, \Delta \delta c_k) \right. \\ &\quad \left. - \gamma_{\downarrow} \cdot V(t, k+2, \delta^2 c_k) \right) \end{aligned} \quad (43)$$

As $V(t, k+2, \delta \Delta c_k)$ and $V(t, k+2, \Delta \delta c_k)$ are equal:

$$\begin{aligned} V(t, k, c_k) &= \gamma_{\uparrow}^2 \cdot V(t, k+2, \Delta^2 c_k) \\ &\quad - 2 \cdot \gamma_{\uparrow} \cdot \gamma_{\downarrow} V(t, k+2, \Delta \delta c_k) \\ &\quad + \gamma_{\downarrow}^2 \cdot V(t, k+2, \delta^2 c_k) \end{aligned} \quad (44)$$

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

$$V(t, k, c_k) = \sum_{\tau=0}^{t-k} \binom{t-k}{\tau} \gamma_{\uparrow}^{\tau} (-\gamma_{\downarrow})^{t-k-\tau} V(t, t, \Delta^{\tau} \delta^{t-k-\tau} c_k) \quad (45)$$

Slightly rearranging:

$$V(t, k, c_k) = \sum_{\tau=0}^{t-k} \frac{\binom{t-k}{\tau} \gamma_{\uparrow}^{\tau}}{(-\gamma_{\downarrow})^{k+\tau-t}} V(t, t, \Delta^{\tau} \delta^{t-k-\tau} c_k) \quad (46)$$

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

$$V(t, t, \Delta^{\tau} \delta^{t-k-\tau} c_k) > 0 \quad (47)$$

By the definition given in Equation (3), this is the same as requiring:

$$\max \left(\frac{h R_t \Delta^{\tau} \delta^{t-k-\tau} c_k}{H(t) + h} - h \varphi e_t, 0 \right) > 0 \quad (48)$$

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

$$\frac{R_t \delta^{t-k} c_k}{H(t) + h} \left(\frac{\Delta}{\delta} \right)^{\tau} > \varphi e_t \quad (49)$$

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

$$\left(\frac{\Delta}{\delta} \right)^{\tau} > \frac{\varphi e_t}{\left(\frac{R_t \delta^{t-k} c_k}{H(t) + h} \right)} = \left(\frac{R_t \delta^{t-k} c_k}{H(t) + h} \right)^{-1} \cdot \varphi e_t \quad (50)$$

Now, take the logarithm of both sides:

$$\tau \cdot \log\left(\frac{\Delta}{\delta}\right) > \log\left(\left(\frac{R_t \delta^{t-k} c_k}{H(t) + h}\right)^{-1} \varphi e_t\right) \quad (51)$$

Finally, we isolate τ :

$$\tau > \frac{\log\left(\left(\frac{R_t \delta^{t-k} c_k}{H(t) + h}\right)^{-1} \varphi e_t\right)}{\log\left(\frac{\Delta}{\delta}\right)} \quad (52)$$

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

$$\tau_0 \stackrel{\text{def}}{=} \left\lceil \frac{\log\left(\left(\frac{R_t \delta^{t-k} c_k}{H(t) + h}\right)^{-1} \varphi e_t\right)}{\log\left(\frac{\Delta}{\delta}\right)} \right\rceil \quad (53)$$

Starting the summation from τ_0 gives the following equation:

$$V(t, k, c_k) = \sum_{\tau=\tau_0}^{t-k} \frac{\binom{t-k}{\tau} \gamma_{\uparrow}^{\tau}}{(-\gamma_{\downarrow})^{k+\tau-t}} V(t, t, \Delta^{\tau} \delta^{t-k-\tau} c_k) \quad (54)$$

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

$$V(t, k, c_k) = \sum_{\tau=\tau_0}^{t-k} \frac{\binom{t-k}{\tau} (\gamma_{\uparrow})^{\tau} h}{(-\gamma_{\downarrow})^{k+\tau-t}} \left(\frac{R_t c_k \delta^{t-k}}{H(t) + h} \left(\frac{\Delta}{\delta}\right)^{\tau} - \varphi e_t \right) \quad (55)$$

◀

A.3 Imitating Portfolio

► **Theorem 12.** *At turn τ , it is possible to construct an imitating portfolio for the t -th mining opportunity which is comprised of tokens and bonds. If this portfolio is properly adjusted at each turn until reaching time t , it can be sold to produce the same profits as the imitated mining opportunity.*

Proof. The proof proceeds via a series of claims.

▷ **Claim 13.** If 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 world-states of turn $\tau + 1$: $\bar{\Phi}(\tau + 1) = V(t, \tau + 1, c_{\tau+1})$. This portfolio is comprised of $\bar{a}_{\tau}$ tokens and B_{τ} risk-free bonds, where:

$$\begin{aligned} \bar{a}_{\tau} &= \frac{V(t, \tau + 1, \Delta \cdot c_{\tau}) - V(t, \tau + 1, \delta \cdot c_{\tau})}{c_{\tau} \cdot (\Delta - \delta)} \\ B_{\tau} &= \frac{\Delta \cdot V(t, \tau + 1, \delta \cdot c_{\tau}) - \delta \cdot V(t, \tau + 1, \Delta \cdot c_{\tau})}{r \cdot (\Delta - \delta)} \end{aligned}$$

Proof of Claim 13. The proof is similar to that of Claim 5. We want the portfolio to be worth the same as the underlying asset in the next turn, no matter the realization of the exchange-rate.

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

$$\bar{\Phi}(\tau + 1) = rB_\tau + \bar{a}_\tau \Delta c_\tau \quad (56)$$

If it went down, the value is:

$$\bar{\Phi}(\tau + 1) = rB_\tau + \bar{a}_\tau \delta c_\tau \quad (57)$$

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

$$\Delta c_\tau \bar{a}_\tau + rB_\tau = V(t, \tau + 1, \Delta c_\tau) \quad (58)$$

$$\delta c_\tau \bar{a}_\tau + rB_\tau = V(t, \tau + 1, \delta c_\tau) \quad (59)$$

The only solution is:

$$\bar{a}_\tau = \frac{V(t, \tau + 1, \Delta c_\tau) - V(t, \tau + 1, \delta c_\tau)}{c_\tau (\Delta - \delta)} \quad (60)$$

$$B_\tau = \frac{\Delta V(t, \tau + 1, \delta c_\tau) - \delta V(t, \tau + 1, \Delta c_\tau)}{r(\Delta - \delta)} \quad (61)$$

◀

▷ **Claim 14.** At turn τ , the portfolio constructed in Claim 13 is equal in value to the t -th mining opportunity: $\bar{\Phi}(\tau) = V(t, \tau, c_\tau)$.

Proof of Claim 14. According to Claim 13 and the definition given in Equation (7), the value of the portfolio at time $\tau + 1$ is:

$$\bar{\Phi}(\tau + 1) = rB_\tau + \bar{a}_\tau c_{\tau+1} = V(t, \tau + 1, c_{\tau+1}) \quad (62)$$

Recall that the risk-free portfolio constructed in Claim 9 has the following value at $\tau + 1$:

$$\Phi(\tau + 1) = V(t, \tau + 1, c_{\tau+1}) - a_\tau c_{\tau+1} \quad (63)$$

By isolating the opportunity's value we get:

$$V(t, \tau + 1, c_{\tau+1}) = \Phi(\tau + 1) + a_\tau c_{\tau+1} \quad (64)$$

Thus, by substituting the above in Equation (62):

$$\bar{\Phi}(\tau + 1) = rB_\tau + \bar{a}_\tau c_{\tau+1} = \Phi(\tau + 1) + a_\tau c_{\tau+1} \quad (65)$$

Note that the amount of coins in both portfolios of Claims 9 and 13 is identical:

$$\bar{a}_\tau = \frac{V(t, \tau + 1, \Delta c_\tau) - V(t, \tau + 1, \delta c_\tau)}{c_\tau (\Delta - \delta)} = a_\tau \quad (66)$$

So, both can be eliminated from Equation (65), resulting in:

$$rB_\tau = \Phi(\tau + 1) \quad (67)$$

As Equation (38) shows, the return of risk-free portfolio is equal to the risk-free rate:

$$rB_\tau = r\Phi(\tau) \quad (68)$$

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

$$B_\tau = \Phi(\tau) \quad (69)$$

This equality can be used to replace B_τ in Equation (6), giving:

$$\bar{\Phi}(\tau) = \Phi(\tau) + \bar{a}_\tau c_\tau \quad (70)$$

Substituting for $\Phi(\tau)$ by using Equation (32) gives us:

$$\bar{\Phi}(\tau) = V(t, \tau, c_\tau) - a_\tau c_\tau + \bar{a}_\tau c_\tau \quad (71)$$

From Equation (66), we get:

$$\bar{a}_\tau c_\tau - a_\tau c_\tau = 0 \quad (72)$$

Finally, we deduce:

$$\bar{\Phi}(\tau) = V(t, \tau, c_\tau) \quad (73)$$

◀

► **Corollary 15.** *The portfolio of Claim 13 is an imitating portfolio for the t -th mining opportunity between turns $\tau, \tau + 1$, meaning the portfolio is equal in value to the opportunity at both turns. Additionally, if there are no fees, selling the imitating portfolio for turns $\tau, \tau + 1$ at turn $\tau + 1$ generates enough money to buy the imitating portfolio for $\tau + 1, \tau + 2$. Thus, after the initial investment is made, no influx of funds is required to adjust the portfolio between turns, meaning that the initial purchase of the portfolio costs exactly the same as the opportunity that it imitates.*

Now, by applying Corollary 15 at each point in time and dynamically moving backwards until reaching τ , we obtain the imitating portfolio for τ and all possible adjustments which may be required to maintain it until t . At this final step, all tokens and bonds contained in the portfolio should be sold. By Claim 14, the profits made by selling the portfolio are equal to the value of the imitated mining opportunity. ◀

B Glossary

Following is a list of important notations used in the paper.

Symbols

V_{ASIC}	Value of an ASIC, in US dollars.
₿	The symbol for the Bitcoin cryptocurrency.
R	The reward received for mining a block, in tokens.
B	Government issued bonds, yielding the risk-free rate.
c	The value of a single coin, in USD.
δ	The multiplicative factor by which the coin's price can decrease.
$1 - q$	The probability of a decrease in the coin's price.
φ	Kilowatt-hours required for the computation of a single mining opportunity.
e	Price of electricity, in US Dollars per kilowatt-hour.

H	The global hash-rate active on the network, in hashes-per-second.
h	The hash-rate of the ASIC to price, in hashes-per-second.
$\bar{a}$	Amount of coins to hold a long position on.
M	The ASIC's mortality distribution.
V	Value of a mining opportunity, in US dollars.
ρ	Multiplicative return of a portfolio.
Φ	Value of a portfolio, in US dollars.
r	The yearly risk-free rate.
a	Amount of coins to hold a short position on.
Δ	The multiplicative factor by which the coin's price can increase.
q	The probability of an increase in the coin's price.

Acronyms

ASIC	application specific integrated circuit
BTC	Bitcoin
CDF	cumulative density function
DAA	difficulty-adjustment algorithm
kWh	Kilowatt-hour
PoW	Proof-of-Work
USD	United States Dollar