Telematics and Informatics 34 (2017) 1308–1321

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin

Adam S. Hayes

University of Wisconsin-Madison, 8128 William H. Sewell Social Sciences Building, 1180 Observatory Drive, Madison, WI 53706-1393, United States

ARTICLE INFO

Article history:
Received 7 December 2015
Received in revised form 13 April 2016
Accepted 5 May 2016
Available online 13 May 2016

Keywords:
Bitcoin
Cryptocurrencies
Digital currencies
Blockchain
Asset pricing
Altcoins

ABSTRACT

This paper aims to identify the likely determinants for cryptocurrency value formation, including for that of bitcoin. Due to Bitcoin's growing popular appeal and merchant acceptance, it has become increasingly important to try to understand the factors that influence its value formation. Presently, the value of all bitcoins in existence represent approximately $7 billion, and more than $60 million of notional value changes hands each day. Having grown rapidly over the past few years, there is now a developing but vibrant marketplace for bitcoin, and a recognition of digital currencies as an emerging asset class. Not only is there a listed and over-the-counter market for bitcoin and other digital currencies, but also an emergent derivatives market. As such, the ability to value bitcoin and related cryptocurrencies is becoming critical to its establishment as a legitimate financial asset.

Using cross-sectional empirical data examining 66 of the most widely used cryptocurrencies, a regression model was estimated that points to three main drivers of cryptocurrency value: the level of competition in the network of producers, the rate of unit production, and the difficulty of algorithm used to "mine" for the cryptocurrency. These amount to relative differences in the cost of production of one digital currency over another at the margin, pointing to differences in relative cost of production – electricity goes in, cryptocurrency comes out. Using that as a starting point, a no-arbitrage situation is established for Bitcoin-like cryptocurrencies followed by the formalization of a cost of production model to determine the fair value of a bitcoin.

1. Introduction

Due to Bitcoin's growing popular appeal and merchant acceptance, it has become increasingly important to try to understand the factors that influence its value formation.[1] Presently, the value of all bitcoins in existence represent approximately $7 billion, and more than $60 million of notional value changes hands each day. Having grown rapidly over the past few years, there is now a developing but vibrant marketplace for bitcoin, and a recognition of digital currencies as an emerging asset class. Not only is there a listed and over-the-counter market for bitcoin and other digital currencies, but also an emergent derivatives market. As such, the ability to value bitcoin and related cryptocurrencies is becoming critical to its establishment as a legitimate financial asset. This topic is not only of general importance to the fields of finance and economics, but also intersects with computer science, information systems, and applied cryptography.

E-mail address: hayes2@me.com

[1] For convention, Bitcoin with a capital 'B' represents the network and protocol while bitcoin with a small 'b' represents individual units of bitcoin, the digital currency.

http://dx.doi.org/10.1016/j.tele.2016.05.005
0736-5853/

The future of Bitcoin or other digital currency platforms can be potentially disruptive to traditional or legacy financial systems. It effectively disintermediates monetary transactions from the banking sector and monetary authority, and instead establishes trust using only technology. It can provide access to financial services to the un- and under-banked, allow for extremely low cost money transfers and remittances across state borders, and serve as a store of value against volatile national currencies – to name just a few benefits.

It is important then to ask the question: Why do bitcoins have value? Determining the economic value of an otherwise intangible, digital entity without any central authority to confer value upon it is a novel pursuit and warrants exploration.

However, price fluctuations of bitcoin versus national currencies such as the U.S. dollar, euro or Chinese yuan, have been extremely volatile over the past few years. This extreme price volatility produces a lot of noise which makes meaningful analysis difficult.

Fortunately, there is an active and fairly liquid market for various altcoin–bitcoin trading pairs, an altcoin being one of many alternative digital currencies based on the original open source Bitcoin code. By looking at bitcoin-denominated relative prices and removing the external dollar, euro, yuan, etc. exchange rates, much of the noise and price volatility can be removed, making for a much better analysis of the data. Comparing how the variations in several shared attributes of cryptocurrencies affects their relative prices with bitcoin, factors that influence value formation can be identified.

This paper describes a cross-sectional data analysis of 66 cryptocurrencies in such a manner using objective factors shared by each one of them. It then compares the production of bitcoin compared to other Bitcoin-like digital currencies, and finally produces a model to consistently value bitcoin. The findings indicate that relative value formation occurs in production at the margin, much like traditional commodities, and that bitcoins' value is derived from its cost of production.

1.1. A brief overview of Bitcoin

Bitcoin is the first and most popular of what has become known as *cryptocurrencies,* digital monetary and payment systems that exist online via decentralized, distributed networks that employ a shared ledger data technology known as *blockchain* coupled with secure encryption.

The low-level technical specifications of the Bitcoin and altcoin protocols are beyond the scope of this paper, however some key points must be understood before going any further, under the assumption that many readers have little to no prior knowledge of this topic. Taking Bitcoin as the generalized digital currency example, one can then extend those concepts to the greater universe of cryptocurrencies. This overview is purposefully brief and meant only to clarify some points that will be referred to in this paper.

Bitcoin is an open source software-based online payment system that emerged in 2008–2009. Payments are recorded in a shared public ledger, known as the blockchain, using its own unit of account, which is also called bitcoin, symbolically represented as either BTC or XBT.

Transactions occur over a peer-to-peer network without a central repository or single administrator – it is a truly decentralized virtual currency where nodes in its network are essentially anonymous. New bitcoins are created as a reward for transaction processing work in which users offer their computing power to verify and record payments into the public ledger. Also known as "mining", individuals or firms engage in this activity in exchange for the chance to earn newly created blocks of bitcoins.

Mining is a necessary component of a cryptocurrency network that is open to the public and which does not censor participants from transacting in it. This purposefully resource-intensive validation activity is meant to deter anonymous participants from acting badly and undermining the system. In other words, the protocol operates under the assumption that any and all nodes will be controlled by fraudsters and thieves, and preempts efforts to scam or steal by making it insurmountably expensive to exploit or attack the network.

Mining is carried out by specialized hardware which has a certain amount of computational power, measured in *hashes* per second. Hashes can be thought of somewhat analogous to the processing power of a CPU microchip, which is measured in hertz for defining how many individual computations can be achieved per second. The aggregate Bitcoin network has a cumulative computational power additive of all the mining effort employed around the world. For every one GigaHash per second ($1\ GH/s = 10^9$ hashes) any individual miner puts online, for example, that amount will be added to the overall network power.

Mining is quite competitive, in the sense that somebody mining with more computational power, or with greater efficiency, has a better chance of finding new bitcoins than somebody with less. Computational effort in cryptocurrency production is often referred to as alternatively *hashpower*, *hashing power*, *mining effort*, or *hashrate*. A hash is simply a single iteration of an algorithm used in cryptography, known as a hash function.

Besides mining, bitcoins can be obtained in exchange for national currencies such as dollars, euros, etc., for other altcoins, or in exchange for products and services. Users can send and receive bitcoins electronically using freely available 'wallet' software on a personal computer, mobile device, or a web application.

2. Survey of relevant literature

There is a small but emerging academic literature regarding the valuation of cryptocurrencies, with most emphasis surrounding Bitcoin itself. Much of the economic study undertaken has attempted to address the "moneyness" of bitcoin or

whether it is more analogous to a fiat versus commodity money, like a 'digital gold' (Gertchev, 2013; Harwick, 2014; Bergstra, 2014).

Yermack (2013) looks at bitcoin's moneyness and points out weaknesses in bitcoin as a currency. He claims that bitcoin (and all cryptocurrencies by association) have no intrinsic value. I consider the potential that while its characteristics are intangible and the labor employed to mine for them is computational rather than human or mechanical, a bitcoin does indeed have an intrinsic value, albeit virtual, which cannot be directly compared to tangible intrinsic value possessed by gold, for example. I don't disagree with the premise that bitcoin and its cousins are not *money* in the strict sense and that many issues stand in the way of it moving toward mass acceptance and appeal. Yermack makes a valid point that the price volatility of bitcoin as expressed in dollars is quite high and that its dollar price may vary significantly among the various exchanges. He mentions that this can cause problems when trying to analyze price data.

For this paper, I have used bitcoin rather than dollars as the denomination for the various cryptocurrency prices. One can then transpose all prices to dollars using a current dollar-bitcoin exchange rate if they chose. Hence, in my analysis a bitcoin is always worth 1 BTC, and all other cryptocurrencies are expressed in decimal form as x.xxxxxxxx BTC. It is worth noting that for many cryptocurrencies there only exists pairwise trading on exchanges between itself and bitcoin (or to a lesser extent another cryptocurrency); there are far less altcoin-dollar trading pairs than altcoin-bitcoin pairs. Attempts thus far at valuation, or determining sources of value, have focused almost entirely on bitcoin without consideration to the scope of alternative cryptocurrencies and altcoins.

Hanley (2013) proposes that the value of bitcoin floats against other currencies as a pure market valuation with no fundamental value to support it. Woo et al. (2013) suggest that bitcoin may have some fair value due to its money-like properties as a medium of exchange and a store of value, but without any other underlying basis.

Jenssen (2014) identifies the "proof-of-work" feature of the mining protocol – the fact that mining is resource-intensive – implying there may be some sort of computer-labor power source of value. Jenssen also argues, however, that the observed market price of bitcoin in dollars is due to the traditional determinant of demand given a limited supply. The fact that there will only ever be 21 million bitcoins as a bounded limit on eventual supply could very well be a red herring; since each bitcoin is divisible to eight decimal places and that number of decimal places can be theoretically increased. There is nothing to prevent the functional unit from being a nano-bitcoin, for example. Although dealing with leading zeros might be cumbersome, it is not prohibitive. With traditional money, there is no effective way to have the functional unit as a fraction of a cent. This paper shows that what is more important as a source of value seems to be the rate of unit formation.

Van Alstyne (2014) considers a source of bitcoin value to be the technological value in solving the so-called double spend problem. While this breakthrough has certainly allowed for the viability of bitcoin, it does not in and of itself make for value. For why then would other cryptocurrencies, which have the same or similar protocols underlying them, have disparate relative values?

Bouoiyour and Selmi (2014) attempt to describe bitcoin value by regressing its market price against a number of independent variables including those such as the market price of gold, occurrences of the word 'bitcoin' in Google searches, the velocity of bitcoin measured by transaction data, and so on. Largely, the variables when regressed were not statistically significant at the 5% or better level of significance. Lags on the price of bitcoin itself were found to carry some weight, but that can be an artefact of the time-series analysis. Seemingly, only the regression on lagged Google search results were significant at the 1% level. While this finding is interesting, it shows that many variables which may be hypothesized to confer value actually do not. In an 18-variable multiple regression the R^2 value they obtained was a moderate 0.46, indicating that some other variables must account for over half of bitcoin's dollar value. Because cryptocurrencies are nascent and still highly speculative and volatile, using time series analysis can be misleading and prone to misinterpretation over the short life time of its existence.

Polasik et al. (2014) concludes that bitcoin price formation is the result primarily of its popularity and the transactional needs of its users. They, too, utilized Google search results and found this variable to be highly significant, while the number of transactions (a proxy for velocity) was found not to be. I argue that use of Google search results is not a good metric and that the found correlation might be spurious. In the period when these studies took place, the dollar price of bitcoin was rising rapidly. This rapid price increase caused increasing media attention and word-of-mouth introducing it to more and more people who subsequently searched the internet to gain more information. The people actively mining for or transacting in bitcoin, I surmise, would not need to repeatedly input the word 'bitcoin' as a Google search term, rather people looking at it for the first time, or to investigate it to a greater degree would utilize such a search.

Zhang and Song (2014) looks at alternative cryptocurrencies (altcoins) in conjunction with bitcoin, however they only consider three such altcoins (litecoin, dogecoin and reddcoin). Their work is largely descriptive, but lays the groundwork for future research on cryptocurrencies in general and in the framework of micro- and macroeconomics.

Halaburda and Gandal (2014) analyze the competition among a small number of cryptocurrencies in the marketplace and competition between four online exchanges. They found that arbitrage opportunities, for the most part, do not exist. The small sample size makes their findings a bit incomplete; they also relate cryptocurrency prices to the dollar instead of using bitcoin as the base for comparison. Due to a number of frictions in transactions between cryptocurrencies and national fiat money, markets tend to be more efficient and less volatile when looking at cryptocurrencies relative to a bitcoin base.[5] This transactional friction and the noise it creates may also be why it was found that gross trading opportunities were much greater across exchanges than within exchanges – where conversions to and from fiat currencies are required.

Garcia et al. (2014) asserts that the cost of production via mining could matter in coming up with a fundamental value for bitcoins insofar as it represents a lower bound. This paper will elaborate on that general idea and formalize it to identify a cost of production model for bitcoin. Doing so can identify theoretical break-even levels in market price, electricity cost, mining energy efficiency, and mining difficulty for individual miners – and may be extended to impute averages for the aggregate network.

While it may be tempting to objectify these results to impute a true intrinsic value for bitcoin, I would caution against making such a leap. Even if the models developed in this paper can theoretically determine an intrinsic value, extreme volatility and frequent market price fluctuations in the few years since bitcoin has been around could make identifying such an intrinsic value meaningless in application. There is also the matter of subjective components of value formation which are more difficult to quantify.

3. Assumptions and hypotheses

I will continue to use Bitcoin as the generic example to elaborate on the more general case of cryptocurrencies. There are a few fundamental variables that have been hard-wired into the Bitcoin protocol at its inception. As most altcoins share a common Bitcoin lineage, the majority of cryptocurrencies also have the same set of built-in variables. The numerical values of these variables vary from one digital currency to the next, and are baked-in at the time that they are created.

These variables include:

1- The total number of "coins" ever to be created. For Bitcoin, this value will be 21,000,000 and no more. I refer to this variable as *Total Money Supply*.
2- Each "block" found by mining will contain a specified number of units. A block of bitcoins initially contained 50 BTC, currently it stands at 25 BTC per block, and that amount will continue to be halved over time, approximately every four years. [2] I refer to this variable representing the number of coins in a block the *Block Reward*.
3- A block of coins will be found by mining over the same interval, on average, regardless of the magnitude of mining effort. Bitcoin blocks will be found, on average, once every 10 min. I refer to this variable as *Block Time*.
4- The network will check to ensure that the specified Block Time as been achieved on average over some number of blocks previously mined. In the case of Bitcoin, after 2016 blocks have been found, the system will check and see if the actual average time in creating blocks was greater or less than 10 min. If it was less than 10 min, the system will increase the marginal difficulty in finding new blocks so that the 10 min average will be restored. This I call the *Difficulty Retarget*.
5- The underlying mining *Algorithm* is the cryptologic hash function used as the basis for the protocol. Bitcoin uses what is known as SHA-256d. Many altcoins use this same method, while others use a related function called Scrypt. The inner workings of the algorithms used are beyond the scope of this paper.
6- The *Difficulty* variable is exogenous and describes how hard (in computational power) it is to find a new block given a fixed level of hashpower. Because of the Difficulty Retarget mechanism, the difficulty will adjust up or down as aggregate mining effort is employed or removed from the network.
7- The market *Price* is the observable price on exchanges where altcoin/BTC trading pairs are listed.

By endowing a cryptocurrency with a steady and known rate of unit formation, it cannot be influenced by any central authority. It is important to note that by employing more computational power (e.g. mining hardware) to the network, it may temporarily increase the likelihood that the individual miner with the most power will be most productive; however, the network will check the Difficulty Retarget and adjust the Difficulty accordingly to restore the Block Time. Therefore, if hypothetically somebody were to put online the most powerful new technology, say many Peta-Hashes/second (1,000,000 s GH/s) of computational power, once the network detects that the average time between block creation was too low it would adjust the difficulty up accordingly, rendering that new technology merely adequate, and also rendering every other miner's technology inferior or even obsolete.

In devising new and alternative cryptocurrencies, the creator of a new 'coin' need only look at the open source computer code, copy it, and change one or more of the above variables to suit their liking. Thus, there are is a diverse universe of altcoins: some that have only a '1' Difficulty Retarget instead of Bitcoin's '2016'; some which set the Total Money Supply to either a small handful, or any other number including up to an infinite amount; some set the Block Reward to a fraction of a coin per block while others issue many thousands of coins per block. Virtually any configuration conceivable is possible, and many have been tried out as altcoins already.

Because there are active markets on the internet, exchange ratios and prices for each of these altcoins is known and are tradeable in real-time and across a number of platforms. The open source nature of the underlying code also makes finding the values for the above variables easy to obtain.

The fact that there are altcoins with all sorts of various configurations makes it a rich data set with which to inquire into what factors may be determinants of value on to them.

[2] The block reward for Bitcoin will decrease to 12.5 bitcoins per block in the summer of 2016.

The more aggregate computational power employed in mining for a cryptocurrency, the higher the value. I make this assertion for a number of reasons. First, the more mining power there is, the more acceptance for that 'coin' can be inferred – since mining also serves to verify transactions, the amount of mining power in use is a proxy for overall use and acceptance of that altcoin.

A cryptocurrency with no acceptance or usage will have neither value nor computational power directed at it. Second, a rational miner, motivated by profit, would only seek to employ mining resources to a profitable pursuit. Therefore, if the marginal cost of mining exceeded the marginal product of mining, that miner would redeploy his resources elsewhere, removing the computational power from the network of that altcoin and into another. (Marginal cost refers to the additional cost a producer would incur in making one additional unit, and the marginal product the income from making that unit). Third, the computational power is a proxy for the mining difficulty since the more network power employed, the greater the difficulty will become in order to maintain the pre-programmed Block Time. Therefore, difficulty can be used as an indirect proxy of aggregate mining power.

There is the possibility that the causal relationship between price and computational power is reversed, or bidirectional. It is certainly plausible that computational power will be deployed to where it is already profitable to do so (e.g. prices are already high). To check this, a Granger causality test was run on price and aggregate hashpower. The results strongly indicate that causality runs one-way from mining effort to price and not the other way.

H1. The amount of mining (computational) power devoted to finding a 'coin' is positively correlated to altcoin value.

Extending the law of diminishing marginal utility, the more readily something is available, and the more rapid that pace of availability, the lower the value; in other words, the faster the rate of unit formation, the lower the price. If an altcoin is configured such that it produces an abundance of units per block, and/or blocks are found in rapid succession, it will negatively impact the value of those units. On the other hand, scarcity per block would tend to lead to greater perceived value. This hypothesis takes into account the variables of Block Reward and Block Time.

H2. The rate of 'coins' found per minute is negatively correlated to altcoin value.

Since there is an exogenous future limit to the money supply, the closer the percentage of units that have been mined compared to what is still left to be found will increase its scarcity and confer value. This can be computed by dividing the number of coins found So far to date by Total Money Supply. This can be used to measure relative scarcity.

H3. The percentage of coins mined thus far compared to that which is left to be mined before the Total Money Supply is reached is positively correlated to altcoin value.

The Scrypt system for mining was put into use with cryptocurrencies in an effort to improve upon the SHA-256d protocol which preceded it (which Bitcoin is based on). Specifically, Scrypt was employed as a solution to prevent specialized hardware from brute-force efforts to out-mine others for bitcoins. As a result, scrypt altcoins require more computing effort per unit, on average, than the equivalent coin using SHA-256d. The relative hardness of the algorithm confers relative value.

H4. Altcoins based on the scrypt algorithm will be more valuable than SHA-256d, all else equal.

In other words, the longer a cryptocurrency has been around and used, the more value it will have. This is because in a competitive environment, such as that in altcoins, the 'losers' will simply cease to exist. Therefore, the longer a cryptocurrency has persisted, the more valuable it should be. All cryptocurrencies have a 'genesis' date which is easy to ascertain.

H5. The longevity of the cryptocurrency is positively related to altcoin value.

4. Empirical results of regression analysis

A least-squares (OLS) multiple regression was estimated using cross-sectional data from 66 of the most widely used and actively traded altcoins at the time of this study with the following specification:

$$\ln(PRICE) = \beta 1 + \beta 2 \ln(GH/s) + \beta 3 \ln(COINS\_PER\_MIN) + \beta 4(\%COINS\_MINED) + \beta 5(ALGO) + \beta 6(DAYS\_SINCE) + e$$

where:

ln(PRICE) is the natural logarithm of the observed bitcoin-denominated market price on September 18, 2014.
ln(GH/s) is the natural logarithm of the computational power in GigaHashes per second.
ln(COINS_PER_MIN) is the natural logarithm of the number of coins found per minute, on average which is computed by dividing Block Reward and Time Between Blocks.
%COINS_MINED is the percentage of coins that have been mined thus far compared to the total that can ever be found.
ALGO is a dummy variable for which algorithm is employed, taking on the value of '0' if SHA-256 and '1' if scrypt.
DAYS_SINCE is the number of calendar days from inception of the cryptocurrency through September 18, 2014.

The resulting regression output produced *Model A*:

$$\ln(PRICE) = -9.68^{***} + 0.67\ln(GH/S)^{**} - 0.98\ln(COINS\_PER\_MIN)^{***} - 0.57(\%COINS\_MINED) + 7.43(ALGO)^{***} + 0.00067(DAYS\_SINCE)$$

R^2 = 0.844, Adjusted R^2 = 0.830, F-statistic = 63.71
t-statistics are indicated according to each explanatory variable. *** indicates p < 0.001, ** indicates p < 0.005

The R^2 from this regression is quite high, suggesting that approximately 84.4% of the variation in relative cryptocurrency prices are determined by the variables in the model.

Hypothesis H1 is supported in that the coefficient is positive as expected *a priori* (prices increase as computational power increases), and the t-statistic indicates that it is highly statistically significant that computational power influences price.

Hypothesis H2 is supported in that the coefficient is negative as expected *a priori* (prices decrease as the rate of coin production per minute increases), and the t-statistic indicates that it is highly statistically significant that coins produced per minute influences price.

Hypothesis H3 is *not* supported in that the sign of the coefficient is unexpected, and also the t-statistic indicates that percentage of coins mined is not statistically significant. One possible reason for this result is that while the total number of coins is determined at the inception of a cryptocurrency, the 'coins' themselves are divisible down to 8 decimal places by default, and that number of decimal places can be increased, potentially without limit. Therefore, it may be the case that an absolute Total Money Supply may not actually be a limiting factor since once that ceiling is reached, the units can simply be divided and subdivided. For example, 1 BTC is actually 1.00000000 BTC, and there is nothing preventing 0.00000001 BTC from having useful value (except perhaps that it is cumbersome).

Hypothesis H4 is supported in that the coefficient is positive as expected *a priori* that scrypt altcoins are more valuable than SHA-256, on average, and the t-statistic indicates that it is highly statistically significant that scrypt as opposed to SHA-256 influences price.

Hypothesis H5 is *not* supported by the regression output, although the sign of the coefficient is positive which was expected *a priori*, the number of days since inception is not statistically significant. One possible reason for this result is that the vast majority of altcoins are less than two years old, which hasn't given the market enough time for competition to weed out the losers and reward the winners.

Removing the independent variables that were not statistically significant in *Model A,* a new regression was estimated to produce *Model B*, which had the following output:

$$\ln(PRICE) = -9.53^{***} + 0.69\ln(GH/S)^{***} - 0.98\ln(COINS\_PER\_MIN)^{***} + 7.46(ALGO)^{***}$$

R^2 = 0.843, Adjusted R^2 = 0.835, F-statistic = 111.04
t-statistics according to each explanatory variable and full regression output for Model B available in the Appendix.
*** indicates p < 0.001.

Model B represents a more parsimonious output with a very similar R^2 compared to *Model A*, while improving the F-statistic and slightly improving the t-statistics for each explanatory variable. The model was checked for consistency with the assumptions of a linear regression, and exhibits normality of residuals, does not exhibit heteroscedasticity, collinearity, or other common regression errors.

Model B infers that holding all else constant:

- given a 1% increase in aggregate GH/s output, the price will rise by approximately 0.69%.
- given a 1% increase in coins produced per minute, the price will fall by approximately 0.98%.
- given that the altcoin uses the scrypt protocol, the price will be higher by approximately 7.46% compared to it's SHA-256 counterpart., all else equal.

I would argue that in either of these regression models the intercept term has no valid economic interpretation.

The above model can be useful in a number of ways. It specifies the factors that influence relative prices across a wide variety of cryptocurrencies that exist, inclusive of Bitcoin, and without the noise generated by price volatility with exchange rates against national currencies. Using these findings, pricing existing or newly created cryptocurrencies can be undertaken with some greater degree of confidence.

It shows that more than 84% of relative value formation can be explained by the three variables: computational power (which is a proxy for mining difficulty), rate of coin production, and the relative hardness of the mining algorithm employed. This suggests that relative rates of production for given level of mining effort are paramount. For a given level of hashpower, increasing the difficulty will yield less units, and thus the relative cost of production. Similarly, reducing the block reward or employing a more rigorous mining algorithm will yield fewer units. In other words, this suggests that differences in the relative cost of production on the margin drive value formation for cryptocurrencies.

Using Model B, it is possible, in theory, to create an altcoin of high value simply by increasing its cost of production: choosing scrypt (or another even more difficult protocol) and reducing the coins produced per minute to some minuscule

amount – this can be accomplished by increasing the Block Time and simultaneously reducing the Block Reward. Once that is achieved, the hard part is getting the computational power (and thus the mining difficulty) of the network up – and that is largely out of the control of the altcoin creator.

One important implication is that the total money supply, or ultimate number of units to ever be created is not a driving factor in value creation, rather it is the rate of unit creation that matters.

Of course, there are other subjective factors in determining the market price not included in the model, but which are yet to be identified. At any given point in time, any individual cryptocurrency may trade above or below its modelled value, the same as any other asset. There is likely to be a speculative premium, as well as the tendency to hoard mined coins which will play an additional role in value formation, but which is more difficulty to quantify and measure

5. The decision to mine for altcoins

There exists theoretically efficient mobility of capital (easily using the same piece of equipment for one purpose versus another) in switching mining effort from that of one coin to another; all one has to do is change the settings for the software or hardware to point the miner's hashing power towards mining another coin. Once those coins are mined and accumulated, they may be exchanged for bitcoin on any number of online exchanges.

Today, due to path-dependency bitcoin is the stable equilibrium digital currency, and, for the most part, anybody wishing to transact in the real economy with a digital currency needs to use bitcoin. In other words, even if bitcoin is not the optimal cryptocurrency available, because of its history and widespread adoption, it doesn't matter that there are better alternatives – much like how VHS won out over the technologically superior Betamax video tapes. If obtaining bitcoins is the ultimate goal, a rational cryptocurrency miner would only direct mining effort at an altcoin if it provided for greater profitability than mining bitcoin directly over some period of time. What tends to happen is that any opportunities for excess returns are short-lived as competition drives all profit rates down to at least that of the cost of mining for bitcoin itself.

This apparent efficiency in removing opportunities to earn excess profits in mining seems to be the result of two forces: 1) competition of capital, as it is mobilized to mine for the more profitable coin it raises the aggregate network hashing power in that coin, causing the difficulty to subsequently increase. As the difficulty increases, profitability falls per unit of mining effort; and 2) the market exchange rate will change as mining participants actively produce and then sell relatively 'over-priced' coins.

Thus, both the bitcoin-denominated exchange price and the current difficulty of mining for the cryptocurrency in question relative to bitcoin's difficulty determines if there is an arbitrage opportunity, and acting on either variable will serve to eliminate that opportunity (arbitrage meaning the ability to simultaneously buy something at one price and sell it for a higher price, generating a riskless profit).

The baseline for profitability, then, or the regulating level of daily production, is the own-rate of return for bitcoin mining, measured in expected bitcoins per day per unit of mining power. For simplicity, I peg the level of hashing power at a standard 1000 GigaHashes/sec (GH/s) of mining power (or equivalently 1 TeraHash/sec (TH/s)). In practice, the actual hashing power of a miner is likely to deviate more or less from 1000 GH/s, however this level tends to be a good standard of measure under current circumstances.

The rate of bitcoin creation at the time of writing this paper is approximately 0.0003 BTC/day for every 1 TH/s of mining effort employed.[3]

The expected number of bitcoins expected to be produced per day can be calculated as follows:

$$BTC/day* = \left(\frac{\beta\rho \cdot \mathrm{sec}_{hr}}{\delta \cdot 2^{32}}\right) hr_{day} \tag{1}$$

where BTC/day* is the expected level of daily bitcoin production when mining bitcoin directly, β is the block reward (expressed in units of BTC/block), ρ is the hashing power employed by a miner, and δ is the difficulty (expressed in units of GH/block) The constant $\mathrm{sec}_{\mathrm{hr}}$ is the number of seconds in an hour, or 3600. The constant $\mathrm{hr}_{\mathrm{day}}$ is the number of hours in a day, or 24. The constant 2^{32} relates to the normalized probability of a single hash solving a block, and is an attribute of the mining algorithm.

The constants, which normalize the dimensional space for daily time and for the mining algorithm, can be summarized by the variable θ, which would equal:

$$\theta = 24\ \mathrm{hr}_{\mathrm{day}} \cdot 3600\ \mathrm{sec}_{\mathrm{hr}}/2^{32} = 0.00002012.$$

Eq. (1) can thus be rewritten:

$$BTC/day^{*} = \left(\frac{\beta\rho}{\delta}\right)\theta \tag{2}$$

The only inputs needed therefore are β, ρ and δ. For this analysis, the hashing power, ρ, will be pegged to a fixed standard rate of 1000 GH/s of hashing power.

[3] Given an observed difficulty value for Bitcoin of 166,851,513,283 and a block reward of 25 BTC per block.

An arbitrage opportunity exists when mining for any other cryptocurrency with the same amount of hashing power would produce a greater expected level of BTC/day than BTC/day*. To generalize Eq. (1) to account for any other altcoin, we simply introduce the current exchange rate of the altcoin/BTC pair, ε, holding the difficulty for bitcoin mining constant. Specifically, the market bid of the exchange rate is the price that matters since an arbitrageur would only be concerned with selling the altcoin to buy BTC.

Eq. (3) indicates how many bitcoins would be obtained on average *indirectly* by mining for an altcoin instead:

$$BTC/day_{altcoin=}\left(\frac{\beta_{altcoin}\rho}{\delta_{altcoin}}\right)\theta\cdot\varepsilon \tag{3}$$

Under the no-arbitrage assumption that BTC/day* will be given as the own-rate of return for BTC, Eq. (3) can be re-arranged to solve for a theoretical equilibrium market price (of the bid) of the altcoin, holding the altcoin's difficulty constant[4]:

$$\varepsilon^{*}=\frac{(BTC/day^{*})}{\left(\frac{\beta_{altcoin}\rho}{\delta_{altcoin}}\right)\theta} \tag{4}$$

If the altcoin's difficulty remains the same, there is a market opportunity for an arbitrageur to sell the relatively overpriced cryptocurrency until it reaches ε* when exchanged for bitcoin on the market.

If, instead, the market price is held constant at ε*, the difficulty can be thought of as relatively 'undervalued' and directing mining effort to that coin will produce excess profitability by subsequently exchanging those mined coins for bitcoin at price ε*. Employing more mining power will necessarily increase the difficulty of that coin over time, so the arbitrage opportunity only exists until the difficulty is normalized and equilibrium is restored.

$$\delta^{*}=\left(\frac{\varepsilon\beta_{altcoin}\rho}{BTC/day^{*}}\right)\theta \tag{5}$$

Because the outcomes from Eqs. (4) and (5) can be worked on by many different agents at the same time – mining difficulty in an altcoin will rise at the same time that units of the altcoin are sold in the market – observed arbitrage opportunities tend to be short-lived.

An example is useful here. A hypothetical individual miner has enough hashing power to earn 1 BTC/day*, on average. Alternatively, her same mining equipment could produce an expected 33,000 XYZ Coin per day, where XYZ Coin is a hypothetical altcoin that is traded against BTC on one or more exchanges. If the market bid is 0.00003996 BTC, she can exchange her XYZ and get in return: $33{,}000 \times 0.00003996 = 1.32$ BTC/day$_{altcoin}$, making XYZ Coin mining right now 32% more profitable than mining bitcoin directly.

As she and other miners continue to mine and subsequently sell their XYZ Coin, the market price in XYZ/BTC will fall as bids are cleared. The addition of new mining power in the XYZ network will also tend to make its difficulty rise, making it a more costly and less attractive alternative. It is worth noting that since there will tend to be orders of magnitude more mining effort directed at mining bitcoin than any altcoin at a given moment, while the new hashing power added to XYZ Coin may be a significant amount to XYZ Coin, the effort being removed from aggregate bitcoin mining is likely to be inconsequential and have no effect on bitcoin difficulty.

6. A cost of production model for valuing a bitcoin

As I have shown, the decision to mine for bitcoin comes down to its profitability given its relative cost of production; the regression results from above show that this is the predominant factor in forming its value. A rational agent would not undertake production of bitcoins if they incurred a real ongoing loss in doing so.

Bitcoin mining employs computational effort which requires the consumption of electricity to function, which must be paid for. This computational effort is directed at mining bitcoin, in competition with many other miners who presumably are also motivated by profit, on average. The more powerful the mining effort (the higher the hash-rate), the more likely it is to successfully mine bitcoins during a given interval (typically measured per day) for a given level of mining difficulty.

Therefore, success in finding bitcoins depends not only on the hashing power, but also on the difficulty level of the algorithm at the time that mining is undertaken. The difficulty specifies how hard it is to find a bitcoin during some interval, the higher the difficulty the more computational effort will be required to mine bitcoins at the same rate as with a lower difficulty setting. The Bitcoin network automatically adjusts the difficulty variable so that one block of bitcoins is found, on average, every ten minutes. As more aggregate computational effort is added to mining bitcoins, the time between blocks will tend to decrease below ten minutes, the result being that the network will adjust the difficulty upwards to maintain the set ten minute interval accommodating the excess mining effort. Likewise, if mining effort is removed from the network, the length between blocks would grow longer than ten minutes and the network will adjust the difficulty downwards to restore the ten minute interval.

[4] A no-arbitrage assumption simply means that under optimal conditions no opportunities for riskless profit can ever exist since they will be immediately identified and eliminated.

Each unit of mining effort has a fixed sunk cost involved in the purchase, transportation and installation of the mining hardware. It also has a variable, or ongoing cost which is the direct expense of electricity consumption. Each unit of hashing power consumes a specific amount of electricity based on its efficiency, which has a real-world cost for the miner. Because miners cannot generally pay for their electricity cost in bitcoin, they must refer to the currency price of a bitcoin to measure profitability given a real monetary cost of electricity.

It seems to be the case that the marginal cost of bitcoin production matters in value formation. Instead of approaching bitcoin as a digital money or currency, it is perhaps more appropriate to consider it a virtual commodity with a competitive market among producers.

The important variables in forming the decision to mine are: [1] the cost of electricity, measured in cents per kilowatt-hour; [2] the energy consumption per unit of mining effort, measured in watts per GH/s (or Joules per GH), a function of the cost of electricity and energy efficiency; [3] the monetary price of bitcoin in the market; and [4] the difficulty of the bitcoin algorithm. (The block reward also matters, but this value changes only after much longer intervals, approximately once every 4 years.)

An individual would undertake mining if the marginal cost per day (here, the cost of electricity consumption) were less than or equal to the marginal product (here, the number of bitcoins found per day on average multiplied by the dollar price of bitcoin). If bitcoin production is a competitive commodity market, albeit a virtual one, then we would theoretically expect marginal cost to equal marginal product – which would also equal selling price.

The main cost in bitcoin mining is the energy consumption which is needed to facilitate the computational labor employed in mining. (Other, much smaller, costs that do exist such as internet service, hardware maintenance, computer cables etc., can be regarded as negligible.)

The actual observed market price is determined by the supply and demand for bitcoin at any given moment, while the cost of production might set a lower bound in value around which miners will decide to produce or not. While this lower bound could represent an intrinsic value, the actual observed price may deviate from that expected value for long periods of time, or may never converge to it.

Of course, there are likely to be many subjective motivations for bitcoin mining beyond the objective components elaborated in this paper. Individual decision makers may operate regardless of cost if they believe that there is enough speculative potential to the upside. Bitcoin mining may draw in those who find the features of anonymity and lack of governmental oversight attractive. Some miners may decide to hoard some or all of their lot and not regularly engage in offering mined bitcoins in the open market, a sort of bitcoin 'fetishism'. Some miners may be subject to an opportunity cost whereby it would be more profitable to expend the same electrical capacity for some other pursuit. Subjective rationales for mining may induce some individuals to make the decision to produce at a marginal loss for prolonged periods of time. The speculative and money-like properties of bitcoin, as a means of exchange and a potential store of value, add a subjective portion to any objective attempt at forming an intrinsic value. New and innovative uses of the Bitcoin network for non-bitcoin specific applications are also likely to add value for mining.

The objective decision to mine for bitcoins can be modelled. The necessary inputs are the dollar price of electricity, the energy consumption per unit of mining power, the dollar price of bitcoin, and the expected production of bitcoins per day which is based in part on the mining difficulty.[5]

Recall the model for determining the expected number of cryptocurrency coins to be mined per day on average given the difficulty and block reward (number of coins issued per successful mining attempt) per unit of hashing power, Eq. (1):

$$BTC/day^{*} = \left(\frac{\beta\rho \cdot \sec_{hr}}{\delta \cdot 2^{32}}\right) hr_{day}$$

The cost of mining per day, E_{day} can be expressed as:

$$E_{day} = (\rho/1000)(\$/kW\,h \cdot W\ per\ GH/s \cdot hr_{day}) \tag{6}$$

where E_{day} is the dollar cost per day for a producer, ρ is the hashpower employed by a producer, the $/kW h is the dollar price per kilowatt-hour, and W per GH/s is the energy consumption efficiency of the producer's hardware.

According to established microeconomic theory, the marginal product of mining should theoretically equal its marginal cost in a competitive market, which should also equal its selling price.[6] Because of this theoretical equivalence, and since cost per day is expressed in $/day and production in BTC/day, the $/BTC price level is simply the ratio of (cost/day) divided by (BTC/-day). This objective price of production level, P*, serves as a logical lower bound for the market price, below which a miner would operate at a marginal loss and presumably remove them self from the network. P* is expressed in dollars per bitcoin, given the difficulty and cost of production:

$$P^{*} = \frac{E_{day}}{BTC/day^{*}} \tag{7}$$

[5] For illustrative purposes only, the US dollar is the currency used to price bitcoin. In reality, there are bitcoin miners worldwide, notably in Russia, Europe, and China who will buy electricity in their own regional currency and at their local rate. The same analysis can be made with any other national currency.

[6] A mathematical proof of the concept that marginal cost (mc) = marginal product (mp) = selling price can be found in any number of intermediate microeconomics textbooks. (e.g. Case and Fair, 2006).

Eq. (7) allows one to calculate a fair value, P*, for bitcoins. Note that P* is a function of mining difficulty and the block reward in the denominator. Given an observed market price (P) and a known difficulty, one can solve for the break-even electricity cost per kilowatt-hour:

$$\$/kW\ h^* = \left(\frac{P(BTC/day^*)}{hr_{day}}\right) W\ per\ GH/s \tag{8}$$

Given a known cost of production and observed market price, one can solve for a break-even level of mining difficulty:

$$\delta^* = \left(\frac{\beta\rho \cdot hr_{day} \cdot \sec_{hr}}{2^{32} E_{day}}\right) P \tag{9}$$

And, to solve for a break-even hardware energy efficiency, we can again rearrange terms given a market price, cost of electricity per kilowatt-hour, and difficulty:

$$WperGH/s^* = \left(\frac{P(BTC/day^*)}{\$/kW\ h \cdot hr_{day}}\right) \tag{10}$$

6.1. Discussion of the cost of production valuation model

These equations are useful in application as well an in theory. It informs miners objectively as to which price they should undertake or else give up mining. It also informs miners when to stop or start mining given changes in difficulty and electricity costs. Furthermore, looking at market prices for a given difficulty and known average electricity cost, the average energy efficiency of mining for the entire network can be imputed. Non-miner participants such as traders can produce an expected price given knowledge of the input variables.

It is useful to consider a hypothetical example:

Assume that the average electricity cost for the world is approximately 13 cents per kilowatt-hour and the average energy efficiency of mining hardware currently deployed is 0.40 W per GH/s (equivalently Joules per GH/s). Using Eq. (6), the average cost per day for a 1 TH/s mining rig would be approximately: (0.13·24·0.40) · (1000 /1000) = $1.248/day.

Eq. (1) predicts the number of bitcoins that the same 1 TH/s of mining power can find in a day with a difficulty of 166,851,513,283 is approximately 0.000301 BTC/day.

Because these two values (marginal cost and marginal product) are expected to be theoretically equivalent, to express them in dimensional space of $/BTC we simply take the ratio given by Eq. (7): (1.248 $/day)/(0.00301 BTC/day) = $414.62/BTC.

This is surprisingly close to the current observed market value of around $420 per BTC.[7]

It is worth noting that very small margins exist for a variable to change and make mining for bitcoin no longer worthwhile for the average producer: for example electricity costs only need rise by a fraction of a cent or the difficulty by 1%. Because of this, mining is a very competitive pursuit.

As real-world mining hardware efficiency increases, which is a likely result of competition, the break-even price for bitcoin producers will tend to decrease. Low cost producers will compete in the marketplace by offering their product at lower and lower prices. Mining hardware energy efficiency has already increased greatly since its early days. A research study found that the average mining efficiency over the period 2010–2013 was a substantial 500 W per GH/s (Garcia et al., 2014). Today, the best dedicated mining rigs available for purchase have somewhere around 0.15 W per GH/s energy efficiency. The *average* energy efficiency right now across the mining network, which is the value which regulates the marginal cost, seems to be around 0.40 W per GH/s.

This speaks to the rapid pace of technological advancement produced over the past few years and months in mining energy efficiency. The Bitcoin mining network is vast in size and scope and it is likely that some miners are at work with hardware that is older and less efficient than the best available.

Fig. 1, below, illustrates how rapidly the energy efficiency of mining hardware for Bitcoin has improved over time. The rate of technological progress in this case has actually exceeded that predicted by Moore's Law, which is the observation that over the history of computing hardware, the number of transistors in a dense integrated circuit, and therefore its processing power, has doubled approximately every two years.

Bitcoin mining, unlike traditional commodity production, has the unique feature of a regular difficulty adjustment in order to maintain a steady rate of unit production over time – specifically, a block of bitcoins will be mined on average once every ten minutes, regardless of aggregate mining power. Unlike most produced commodities where the supply can change to accommodate fluctuations in demand, the supply of bitcoin is hardwired at its steady rate with the difficulty setting adjusting up and down to maintain that linear rate of production through time. In other words, the elasticity of supply is manifest in changes in the mining difficulty.

[7] As of April, 2016.

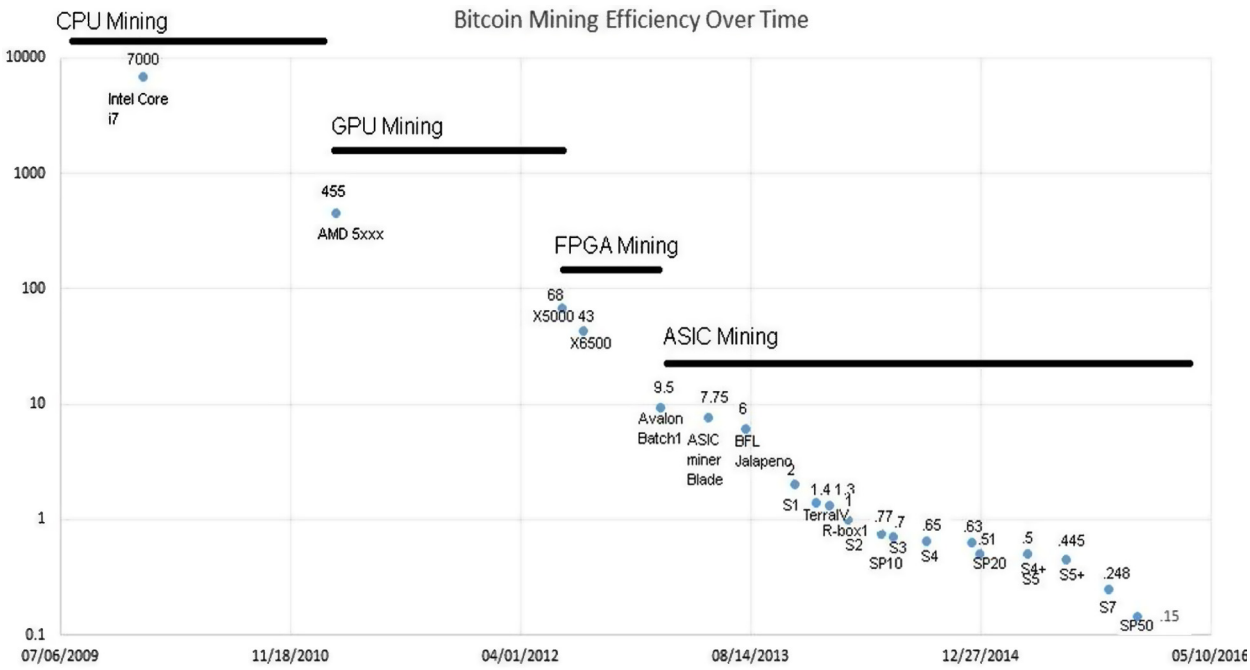


Fig. 1. *Bitcoin mining energy efficiency over time.* The *y*-axis represents bitcoin mining energy efficiency in units of Watts per GH/s on a logarithmic scale. The *x*-axis represents time, beginning with the introduction of Bitcoin in 2009. Mining technology regimes are indicated as well.

As energy efficiency increases, the difficulty adjustment acts as a stabilizing mechanism, increasing the cost of production; as more aggregate mining power is brought on line, the mining difficulty increases. For example, if a mining rig can find 1 BTC/day on average with today's difficulty, the same rig can expect to produce less per day when the difficulty increases 10% or 20% etc. If miners are not able to supply enough new coins to meet an influx of new demand, the market price can see increases while the cost of production remains largely the same. This would induce miners to increase their mining efforts which would then cause the difficulty to increase, raising the cost of production until presumably a new breakeven level is reached. This mechanism tends to counteract the downward tendency caused by increasing energy efficiency.

Fig. 2, below, illustrates the relative change in mining efficiency compared to changes in mining difficulty over time. The left y-axis represents the inverse of the mining difficulty on a logarithmic scale, and is denoted by the dark blue line on the chart. The right y-axis is the mining efficiency, measured in joules per GH, and is denoted by the orange line. The x-axis is time from Bitcoin's origin in 2009 to the present.

Initially, when bitcoin mining was only accomplished via a computer's central processor, or CPU, there were not many individuals involved with bitcoin mining, and the difficulty was very low. At the same time, mining was very inefficient. A computer's processor is designed to do many tasks such as run software and applications. It was discovered that a computer's graphics processor (GPU) was much better at solving the cryptographic algorithm used to mine for cryptocurrencies, and the difficulty grew rapidly as more mining power suddenly came on line. In Fig. 2, the darker shaded areas indicate periods where the network size (i.e. difficulty) was increasing at a faster pace than technological change in mining efficiency. Lighter-shaded areas indicate periods where technological change has outpaced the growth of the network. GPU mining, while more efficient that CPU mining, was still not ideal. Video cards are designed for computer graphics and optimized for application such as gaming or design. As a result, mining with a GPU is not optimized for cryptocurrency mining. Furthermore, the manufacturers of graphics cards (and of CPUs for that matter) do not concern themselves with increasing the efficiency of their products to mine for cryptocurrencies. These manufacturers typically produce newer, better GPU hardware only when they can improve their primary functionality. Therefore, there is no induced technological change to make these devices more efficient at mining even when the network size and mining difficulty is growing rapidly.

This all, however, changed with the introduction of application-specific integrated circuits, or ASICs, designed with the sole purpose to solve the encryption underlying cryptocurrencies. As a result, we begin to see marginal cost and marginal product begin to converge in mid- to late-2013 as they made their way to producers worldwide. Since then, there has been evidence of induced technological change, evidenced by the continued convergence of network size and mining efficiency since.

It is important to note that in the pre-ASIC period of bitcoin mining, the cost of production model outlined above would not hold. The capacity utilization of a CPU or GPU to mine for bitcoin is simply not efficient enough. One would not expect marginal cost to converge to marginal product when the hardware being used is not subject to competition. An apt comparison is that with ASICs it is like mining for gold with a pick and shovel – specifically made for such an activity – and when mining with CPUs/GPUs is like mining for gold with a shoe.

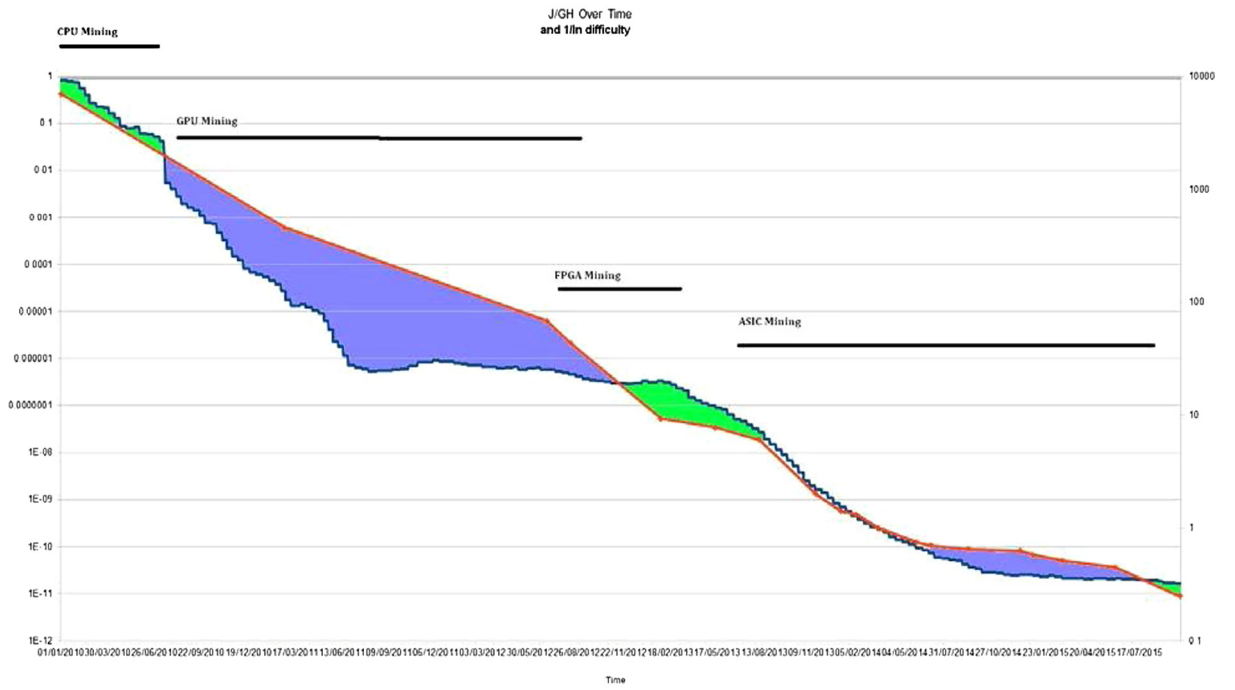


Fig. 2. *Bitcoin mining difficulty vs. mining energy efficiency over time.* The left-hand *y*-axis represents the inverse of the mining difficulty for Bitcoin (1/difficulty) on a logarithmic scale. The right-hand *y*-axis represents bitcoin mining energy efficiency in units of Watts per GH/s on a logarithmic scale. The *x*-axis represents time, beginning with the introduction of Bitcoin in 2009. Mining technology regimes are indicated as well.

While a shoe is not meant to mine for gold, one could conceivably collect some dirt in the shoe and find gold by happenstance. Just as the picks and shovels used for gold mining were induced to adapt and change, becoming steam shovels and later industrial mining operations, so too has bitcoin mining in the ASIC age seen such technological progress and consolidation due to competition.

One insight that could have sizable consequences for the cost of production of bitcoin relates to the block reward amount and how changes in this variable will impact BTC/day production. When Bitcoin was launched, each block mined was composed of 50 bitcoins. That amount is set to halve every four years, and in 2012 the block reward became 25. The block reward will again halve to 12.5 bitcoins per block, expected mid-Summer, 2016, and will again in the year 2020, and so on. If we refer back to the illustrative example above and substitute a 12.5 BTC block reward for the current 25, the expected BTC*/-day' becomes half of 0.00301, or 0.001505 per 1 TH/s. Using the hypothetical example above and given this new BTC*/day', the break-even price for a bitcoin would increase suddenly to $829.24, holding all else constant.[8] If the market price of bitcoin does not increase in turn, it will suggest that the breakeven efficiency has also increased at a more or less equivalent rate. This could have the effect of eliminating all but the most efficient producers all at once.

7. Conclusions

Beginning with a cross-sectional analysis to define the causes of relative value formation among cryptocurrencies, it was found that relative differences in costs of production on the margin are the main determinants. By looking at bitcoin-denominated relative prices, which are available on a number of online cryptocurrency exchanges, the high degree of price volatility found in the dollar-bitcoin exchange rate was eliminated. Cross-sectional analysis also was able to remove a number of other issues found in time-series analysis including any chance of non-stationary data or a small time horizon for the data set.

Next, using the regression results as a facilitator, a series of related equations were formalized to calculate how many units of a cryptocurrency a producer with a fixed amount of hashing power could expect to find, on average. Because Bitcoin is the stable equilibrium digital currency, even if some other altcoins are better or have various interesting features that Bitcoin lacks, it will be very difficult to dislodge. Therefore, the ultimate goal of any cryptocurrency producer operating in the real economy will to obtain bitcoins.

Given efficient mobility of capital, a cryptocurrency producer will only mine for an altcoin if there is a greater profitability in that than using their equipment to mine for bitcoin directly. When these cases occur, markets tend to efficiently correct arbitrage opportunities ensuring that no altcoin is more profitable to produce than mining for bitcoin directly.

[8] The change in block reward will have no impact on difficulty. Rather, less BTC/day will be found given the same difficulty.

Finally, a cost of production model is put forward to establish break-even values for a bitcoin producer. Extrapolating that model to account of the average or regulating values for the aggregate Bitcoin mining network, the cost of production model can closely approximate the market price for bitcoins versus dollars.

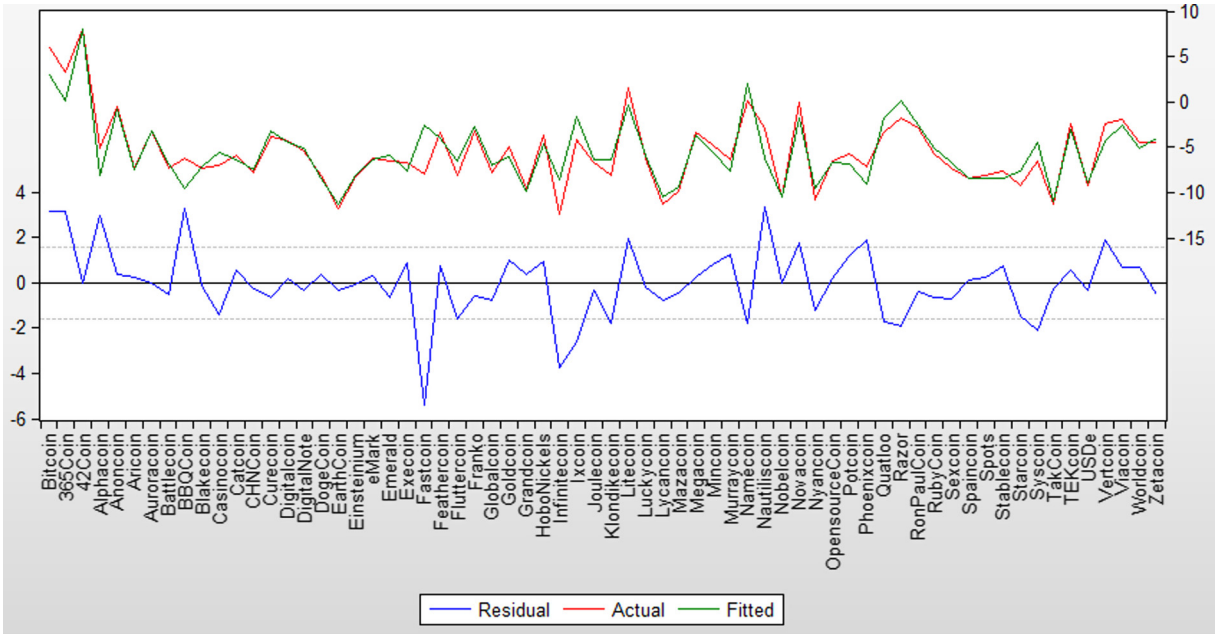
The implications are that cost of production drives value and anything that serves to reduce the cost of bitcoin production will tend to have a negative influence on its price. Increased mining hardware energy efficiency, lower worldwide electricity prices, or lower mining difficulty will all reduce the marginal cost of production. As mining efficiency increases due to technological progress, it lowers the cost of production and puts a negative pressure on the price. At the same time, the additional hashing power added to the global mining network will tend to increase the mining difficulty, and positively influence the price. The question will be which factor will outpace the other: technological progress (energy efficiency) or the size of the mining network (difficulty). A further implication is that when the Bitcoin block reward halves, it will effectively increase the cost of production overnight.

Appendix A

Dependent Variable: LOG(_PRICE)
Method: Least Squares
Date: 05/12/16 Time: 14:03
Sample: 1 66
Included observations: 66

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	−9.526966	0.779882	−12.21591	0.0000
LOG(GH_S_HASHPOWER)	0.685330	0.064390	10.64349	0.0000
LOG(COINS_PM)	−0.983477	0.061908	−15.88620	0.0000
TYPE="Scrypt"	7.461170	0.875470	8.522473	0.0000

R-squared	0.843083	Mean dependent var	−5.493893
Adjusted R-squared	0.835491	S.D. dependent var	3.888541
S.E. of regression	1.577183	Akaike info criterion	3.807849
Sum squared resid	154.2253	Schwarz criterion	3.940555
Log likelihood	−121.6590	Hannan-Quinn criter.	3.860287
F-statistic	111.0381	Durbin-Watson stat	1.929522
Prob(F-statistic)	0.000000		



References

*Additional data collected from the following web sites: coinmarketcap.com, coinwarz.com, cryptsy.com, bitcoinwisdom.com, and blockchain.info.

Bergstra, Jan Aldert, 2014. Bitcoin: Not a Currency-Like Informational Commodity. Informatics Institute, University of Amsterdam.
Bouoiyour, Jamal, Selmi, Refk, 2014. What Bitcoin Looks Like? No 58091. University Library of Munich, Germany.
Case, K.E., Fair, R.C., 2006. Principles of Microeconomics. Pearson Education.
Garcia, David et al, 2014. The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy. J. R. Soc. Interface 11 (99), 20140623.
Gertchev, Nikolay, 2013. The Moneyness of Bitcoin, <www.mises.org>.
Halaburda, Hanna, Gandal, Neil, 2014. Competition in the Cryptocurrency Market Available at SSRN 2506463.
Hanley, Brian P., 2013. The False Premises and Promises of Bitcoin arXiv preprint arXiv: 1312.2048.
Harwick, Cameron, 2014. Crypto-Currency and the Problem of Intermediation Available at SSRN 2523771.
Jenssen, T., 2014. Why Bitcoins Have Value, and Why Governments Are Sceptical Available at cryptolibrary.org.
Polasik, Michal et al, 2014. Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry Available at SSRN 2516754.
Van Alstyne, Marshall, 2014. Why bitcoin has value. Commun. ACM 57 (5), 30–32.
Woo, David et al, 2013. Bitcoin: A First Assessment FX and Rates.
Yermack, David, 2013. Is Bitcoin a Real Currency? No w19747. National Bureau of Economic Research.
Zhang, Yiteng, Song, Guangyan, 2014. Economics of Competing Crypto Currencies: Monetary Policy, Miner Reward and Historical Evolution.

Further reading

Nakamoto, Satoshi, 2008. Bitcoin: a peer-to-peer electronic cash system. Whitepaper 8 (2015), 28 (Consulted).