Exploring Miner Evolution in Bitcoin Network

Luqin Wang[1] and Yong Liu[2]

[1] Department of Computer Science and Engineering
[2] Department of Electrical and Computer Engineering
NYU Polytechnic School of Engineering

Abstract. In recent years, Bitcoin, a peer-to-peer network based crypto digital currency, has attracted a lot of attentions from the media, the academia, and the general public. A user in Bitcoin network can create Bitcoins by packing and verifying new transactions in the network using their computation power. Driven by the price surge of Bitcoin, users are increasingly investing on expensive specialized hardware for Bitcoin mining. To obtain steady payouts, users also pool their computation resources to conduct pool mining. In this paper, we study the evolution of Bitcoin miners by analyzing the complete transaction blockchain. We characterize how the productivity, computation power and transaction activity of miners evolve over time. We also conduct an in-depth study on the largest mining pool F2Pool. We show how it grows over time and how computation power is distributed among its miners. Finally, we build a simple economic model to explain the evolution of Bitcoin miners.

Keywords: Bitcoin, Measurement, Network Analysis

1 Introduction

Bitcoin [1] is known as *the first decentralized digital currency in the world* [2]. Unlike any traditional currency issued and regulated by a sovereign bank, Bitcoin is not controlled by any institution or country. It circulates globally without boundary and is free from financial regulation systems due to its decentralized P2P accounting and transaction design. Debuted in 2009 and after five years' development, Bitcoin exchange price has raised from nothing to over $100 per coin through mid 2013, surged to its peak at $1,242 on Nov. 29, and is wobbling between $350 and $600 in today's market. Till September 2014, the market capitalization of Bitcoin has increased to around 6 billion US dollars; and the Bitcoin network runs over 60,000 transactions daily. Along with Bitcoin network's capitalization and volume, more and more derivative services are developed and legalized. Exchange markets, i.e., Coinbase [3] and Bitstamp [4], allow users to buy and sell Bitcoins using regular currencies globally. Online merchants, e.g., Dell and Overstock, are now accepting Bitcoin as a payment method. Paypal also adopts Bitcoin and starts to open its API to a few mainstream Bitcoin exchange websites. Governments of several countries, such as Canada and Thailand, have approved fully-legal Bitcoin exchange and issued tax guidance on Bitcoin transactions. Different from a regular currency, there is no central bank or authority who decides how many Bitcoins to be issued and distributed. According to the Bitcoin protocol, there are only a finite amount of Bitcoins. In addition to buying Bitcoins from others, the only way for a user to acquire Bitcoins is to contribute her computation resources to pack and verify new transactions. We call this process *Bitcoin mining* and users who participate in mining as *Bitcoin miners*. The Bitcoin protocol is designed so that new Bitcoins are mined at a steady rate until all Bitcoins are mined. The surge of Bitcoin price motivates Bitcoin miners to invest on more and more powerful hardware for faster mining. Due to the dramatic growth in both the number of Bitcoin miners and the computation power of their hardware, it has become increasingly difficult to mine Bitcoins. For an individual miner, even with powerful hardware, it now takes a very long time for her to get Bitcoins if she does mining by herself, the so called *solo mining*. Similar to pooling money to buy lottery, more and more miners choose to pool their computation resources to mine Bitcoins together, the so called *pool mining*. Pool mining gives individual miners more steady payouts than solo mining.

Bitcoin network is a P2P system that peers can obtain direct financial incentives by contributing their computation resources. While the Bitcoin price is constantly driven by various economic, politic and legal factors, we are interested in finding out how Bitcoin price evolution drives the miners' mining behaviors. Towards this goal, we conduct a measurement study on the evolution of Bitcoin miners by analyzing the complete transaction blockchain of the Bitcoin network from its very first transaction in 2009 to March 2014. We first characterize how the productivity, computation power and transaction activity of miners evolve over time. We then conduct an in-depth study on the largest mining pool F2Pool [5]. We characterize how it grows and how the computation power is distributed among its heterogeneous members. Finally, we build a simple economic model which explains the evolution of miners by considering the Bitcoin price and the computation race between miners.

The rest of the paper is organized as follows. We review the related work in Section 2. A short survey of Bitcoin network and the mining process is presented in Section 2. We present our methodology of analysis and the characterization results in Section 4 and 5, respectively. The paper is concluded in Section 6.

2 Related Work

Although Bitcoin network has a short history, as a P2P based digital currency system, it has drawn lots of attentions of researchers from different fields. Babaioff et al. [6] studies the incentive for Bitcoin users to disseminate transactions. Decker and Wattenhofer [7] measured and modeled how transactions are propagated in Bitcoin network. Ron and Shamir [8] examined the entire transaction graph of Bitcoin network to study user behaviors. Meiklejohn et al. [9] measured and clustered Bitcoin accounts owned by the same user. Freid and Harrigan [10] explored the limits of user anonymity. Studies in [11], [12] and [13] investigated user privacy in Bitcoin network. Both [14] and [15] discussed the vulnerabilities of Bitcoin network and how powerful adversaries can potentially manipulate mining mechanism. Huang et al. [16] studied how malwares steal users' computation power to mine Bitcoin.

3 Survey of Bitcoin Network

3.1 Account and Transaction

Bitcoin network is a peer-to-peer network without central authority. A Bitcoin account is simply a pair of public/private keys. Account ID is derived from its public key. The private key is used to generate digital signature for authentication. There is no cost to generate a Bitcoin account. So each Bitcoin user can generate as many accounts as she wishes. Transaction is the mechanism for users to transfer Bitcoins to each other. A transaction consists of a set of senders and a set of receivers (denoted by their account IDs), the amount from each sender, and the amount to each receiver. For example, if Alice wants to send 3 Bitcoins (BTCs) to Bob. She might send from two of her accounts: one account A_1 has 1 BTC and another account A_2 has 2 BTCs. Suppose Bob has only one account B_1, thus this transaction is simply: 1 BTC from A_1, 2 BTCs from A_2, and 3 BTCs to B_1. Finally, all senders will sign the transaction with their private keys, and the signed transaction is broadcast to the entire Bitcoin network. Any user who receives this transaction will first verify whether the senders have the amount of BTCs indicated in the transaction. Different from the traditional banking systems, there is no central database to maintain the Bitcoin balance of each account. Instead, the whole Bitcoin network stores and verifies all the transactions using a shared blockchain. Any user can check the balance of any account by backtracking the blockchain to retrieve all transactions associated the account. Invalid transactions will be discarded, and validate ones will be stored in memory to be packed and appended to the blockchain.

3.2 Block and Blockchain

The blockchain is a public ledger shared in the whole Bitcoin network. As the name suggests, the blockchain contains a chain of chronologically ordered blocks, each of which contains transactions within a time window of ten minutes and a generation transaction indicating which account packed this block. Each user downloads and synchronizes a copy of the blockchain in her local machine to verify incoming transactions. All newly confirmed transactions are packed into a new block, which will be broadcast to the whole network. Whenever a user receives a block, she will validate all the transactions in this block using the current blockchain. If any transaction is invalid, she will discard the block. Otherwise, this block will be confirmed and appended to the current blockchain.

3.3 Bitcoin Mining

Bitcoin network depends on the computation resources on users to maintain the integrity of the blockchain. Each user can volunteer to verify and pack new transactions to blocks. While a lot of users are doing the verification and packing work simultaneously, only the newest valid block will be confirmed by all users and appended to the current blockchain. The user (miner) who created this block will get rewarded with some BTCs (the current reward is 25 BTCs/block). To achieve this, a proof-of-work mechanism is introduced. When packing new transactions to a block, a miner first generates a special transaction indicating that the network sends her the mining reward. Along with all other transactions, she repeatedly generates a random number nonce, put them together and runs a hash function. If the hash value is below a target value, the user claims she created the block and broadcasts the block and the nonce. Other users can easily perform the same hash function with the published nonce to verify the block.

According to Nakamoto's protocol [1], the total number of BTCs that can be mined is 21 million and the last BTC to be mined is in block #6,929,999 near year 2140. By default, a new block is created approximately every ten minutes, no matter how much aggregate computation power is in the network. To control the new block creation speed, a *difficulty value* is introduced. The target value for block hash calculation is inversely proportional to the difficulty value. As a result, the higher the difficulty value, the more hash calculations each miner has to conduct to find a hash value below the target. As detailed in [17], at a given difficulty value D, for a miner with computation power of H hashes per second, the expected time for the miner to generate a new valid block is:

$$E[T] = \frac{D \times 2^{32}}{H} seconds. \tag{1}$$

The difficulty value is updated every $2,016$ blocks based on the speed at which the past $2,016$ blocks were generated. The difficulty value is stored in each block. Knowing how many BTCs are generated in the whole network in one day, given the difficulty value, we can also calculate the total hash rate of the system.

Solo and Pool Mining In the early days of Bitcoin, miners mined blocks individually. We call this approach *solo mining*. The advantage of solo mining is whenever a block is created by the miner, she gets all the rewards. However, as more and more computation resources are injected to the Bitcoin network, the difficulty value has to be increased significantly to control the new block creation speed. Now it takes a powerful miner years to create a block. Pool mining is a way for miners to pool their resources together to obtain steady payouts. A pool assigns a lower difficulty value to each of its members. It becomes easier for each miner in the pool to solve the hash problem and prove their work. Each pool miner submits her own hash values under the pool target value (called shares) to the pool for verification. If a share is under the network target value, a block is claimed by the pool and pool operator will distribute the reward to every pool miners. The most popular payout approach for pool mining is pay-per-share, in which miners are rewarded proportionally to the number of shares they submitted to the pool. With pool mining, the expected payout for a minor is the same as solo mining, but the variance of payout is largely reduced.

4 Methodology

4.1 Data Collection

As described in Section 3, all transactions in Bitcoin network are stored in the blockchain. When a user wants to make a transfer, she must first connect to the Bitcoin network and synchronize with the current blockchain. We ran the Bitcoin client in our local machine to get the latest blockchain. After collecting the blockchain, we parsed it to blocks and transactions. Each block has its hash value, height (block id), hash value of the previous block, generation time (in UTC timestamp), the amount of new BTCs created, target difficulty, nonce, and all transactions in the block. For each transaction, inputs include the previous transaction hashes of the senders and the associated signature scripts; outputs include the receiver account IDs and their corresponding amounts. We use the previous transaction hash to retrieve the transaction history and the balance of each sender by iteratively backtracking the blockchain. We synchronized the complete blockchain in March 2014 and parsed the data. The raw data includes all blocks and transactions from 2009/01/03 (the very first Bitcoin block created) to 2014/03/11. We retrieved 290,089 blocks and 34,646,076 transactions. We then parsed all blocks and transactions field-by-sfield and stored all the parsed information into a MYSQL database.

4.2 Solo Miner Analysis

Pool mining only started on 16th December 2010 [18]. All previous miners were solo miners. After the introduction of pool mining, each pool also uses one unique ID to mine Bitcoins. We first treat each unique Bitcoin ID who successfully created a block as a solo miner. As a result, we treat pools as solo miners for now. Using block timestamps, we count the number of BTCs mined by miners each month in the network. Also, using Bitcoin exchange market data we calculate the monthly USD (we assume BTCs were exchanged to USD at market price immediately after they were mined) generated in the network. Moreover, we also obtain the distribution of how many BTCs each miner mined over time.

Besides the earnings, we can also estimate the aggregate computation power of all miners. With a given difficulty value of D, if N blocks were mined in a day, based on (1), the aggregate daily hash rate of the whole Bitcoin network can be estimated as:

$$H_{total} = \frac{N \times D \times 2^{32}}{86,400} \tag{2}$$

Similarly, we can estimate a miner's daily hash rate by replacing N with the number of blocks the miner mined in a day.

We are also interested in whether the miners cashed out their mined BTCs after mining. However, it is hard to collect IDs of all Bitcoin exchange markets so as to track all transactions between the miners and the exchange markets. Instead, we track for each miner the interval between the time when she mined some new BTCs and the time when her next transaction was issued. This time interval serves as a lower bound for her cash out lag.

4.3 Pool Miner Analysis

To study how Bitcoin mining pool evolves, we collect pool data from our database. We choose miner IDs with top hash rates in the network and manually classify them. Most of these IDs belong to well-known mining pools according to Blockchain.info, an online Bitcoin statistics website. To analyze pool mining behaviors, we choose F2Pool, a China-based mining pool whose payout rule is clear and the payout transactions are easy to obtain. In our data up to March 2014, F2pool ranked the 7th in terms of the total hash rate in the network. According to the newest statistics in [19], in September 2014, F2Pool grows to the largest mining pool, having over 25% of the overall computation power.

We query transactions having F2Pool's Bitcoin ID and classify them as input or output. For transactions having F2Pool ID as the only receiver, we identify whether they are block generation transactions. For a transaction having it as the only sender, we validate whether the transaction is used to distribute payouts to pool miners. Pools have different approaches to send payouts to pool miners. The simplest way is that the pool sends out payouts to all pool miners in one transaction immediately after each block is created. However, none of the ten pools we checked use this approach. Some pools use a binary tree like iterative payout approach which pays one pool miner and transfer the remaining balance to a new ID at each iteration. And some pools randomly choose a number of miners to pay in one transaction and transfer the remaining balance to a new ID, and then distribute the remaining balance in subsequent transactions. When F2Pool mines a block, it will send out the payouts in the next day. It used to send out payouts to all members using a single transaction, but changed to two transactions recently. Knowing the payout mechanism, we can calcualte how many BTCs each pool miner earns each day using pool payout transactions.

4.4 Simple Economic Model for Miners

To become a miner, a user first needs to invest on hardware, ranging from regular computers in early days, to graphics card, GPUs, and specially designed ASIC chips, and incur the *capital cost*. After she joins the network for mining, she needs to pay the bill for electricity, air conditioning, housing and maintenance etc., and incur the *operational cost*. Since miners are driven by profits derived from the mined Bitcoins, the economic question is *whether and how soon their revenues can cover their capital and operational costs?* We build a simple economic model. For a hardware with hash rate H, based on (1), assume the hardware works 24 hours per day, the expected number of BTCs it can mine daily is:

$$N(t, H) = \frac{H \times 86,400}{D(t) \times 2^{32}} R, \tag{3}$$

where $D(t)$ is the difficulty value in day t, R is the number of BTCs rewarded for each block. If the hardware's power consumption is $P\ kw$, and the electricity price is $\eta(t)$ per kwh, the daily electricity bill is $24P\eta$. Given the Bitcoin exchange price of $\rho(t)$ in day t, if we only consider electricity operational cost, the daily profit rate $r(t)$ for the hardware with hash rate H and power consumption P is:

$$r(t, H, P) = N(t, H)\rho(t) - 24P\eta(t). \tag{4}$$

Obviously, a miner prefers places with low electricity price $\eta(t)$, and will shut down her hardware whenever the profit rate becomes negative. Based on (3) and (4), to maintain a positive profit rate, the hardware's computation-over-power efficiency should satisfy:

$$\frac{H}{P} > K\frac{\eta(t)D(t)}{R\rho(t)}, \tag{5}$$

where K is a constant. As $D(t)$ increases, hardware with low computation-over-power efficiency will be quickly kicked out of the mining game.

To obtain high profit rate, minors should go for specialized mining hardware with high computation-over-power efficiency. Those hardware come at high prices, though. If the miner purchased a piece of expensive hardware at day t_0 with price C, the time τ it takes her to recover the capital cost should satisfy:

$$\int_{t_0}^{t_0+\tau} r(t, H, P) \times I[r(t, H, P)]dt = C, \tag{6}$$

where $I[x]$ is the indicator function which equals to 1 if $x > 0$, and 0 otherwise.

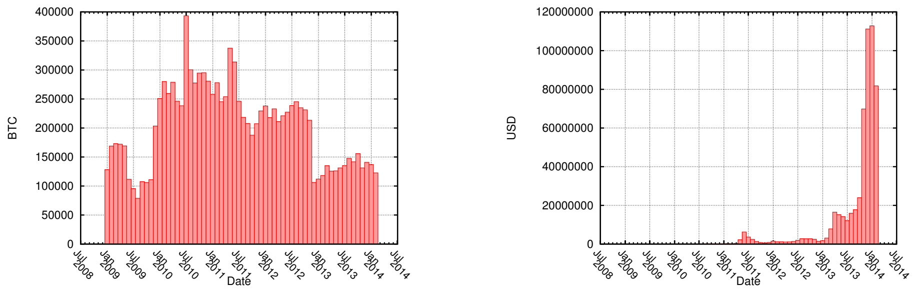
4.5 Limit of Computation Race

According to (4), miners are highly incentivized to increase their computation power to obtain higher profit margin. The Bitcoin network has witnessed exponential computation power growth in the past few years. But at the same time, the number of Bitcoins that can be mined each day is deliberately set to a fix value. If the Bitcoin price is kept flat, the total mining profit that miners can obtain from the network is a constant. All miners are essentially playing a zero-sum computation race game: each miner increases her computation power, then the total computation power in the network increases; consequently the system increases the difficulty value $D(t)$ to maintain a steady Bitcoin creation speed, which in turn reduces the Bitcoin mining rate of individual miners, according to (3). This is a unfortunate and unavoidable *tragedy-of-common* phenomena that has been observed in the Bitcoin network. Such a race will automatically end when the profit margin hits zero. We can predict the equilibrium point by extrapolating on our simple economic model in the previous section. Namely, let ξ_0 be the highest computation-over-power efficiency (in unit of hash-per-second/kilowatt) that the future computation technology can achieve, η_0 be the lowest electricity price in the world, and ρ_0 be the steady state exchange price of Bitcoin, then we can immediately calculate the maximum sustainable computation power $\mathcal{H}$ in the whole Bitcoin network as:

$$\frac{\mathcal{H}}{\xi_0}\eta_0 = 6R\rho_0, \quad \Rightarrow \quad \mathcal{H} = \frac{6R\xi_0\rho_0}{\eta_0}, \tag{7}$$

where the left-hand side of the first equation is the minimum electricity charge for one-hour mining with the most efficient mining hardware, and the right-hand side of the first equation is the expected hourly total payout in the whole network at the target mining rate of one block every ten minutes. If the total computation power goes above $\mathcal{H}$, the expected profit margins of all miners become negative, some of them will start to drop out the mining race, which in turn brings back the profit margin to positive. So far we ignored the capital cost and other operational costs. Therefore (7) gives us an upper bound on the maximum sustainable computation power at any fixed Bitcoin price ρ_0, given the highest feasible computation efficiency ξ_0 and the lowest electricity price η_0.

5 Characterization Results



(a) (b)

Fig. 1: (a) Monthly BTCs Generated, (b) Monthly USD Generated

Figure 1a plots the total Bitcoins generated each month. In 2009, the numbers are not stable because the Bitcoin client was newly released and the size of the network was relatively small. In December 2012, the reward R for each block was reduced from 50 BTCs to 25 BTCs, resulting in the number of BTCs was reduced by half in the latter months. Figure 1b shows how much USD are generated monthly according to the daily Bitcoin to USD exchange price.

5.1 Solo Miners

Figure 2 illustrates the distribution of solo miners' annually earnings. Before August 2010, there is no market data and the estimation of BTC value is \$0. The earnings in latter years are tremendously greater than in the earlier years due to the exchange price went up rapidly. In addition, top miners became more and more powerful and were responsible for the most blocks created. Similar to (3), we estimate the hash rate of each solo miner based on the number of blocks she created. Figure 3 shows the minimum, maximum and mean hash rate of solo miners together with the system regulated difficulty value in logarithm scale. It shows that the computation power are evenly distributed among miners at the the early stage, then become highly skewed with a small number of very powerful miners as the Bitcoin network evolves. As will be studied next, those top miners are indeed mining pools.

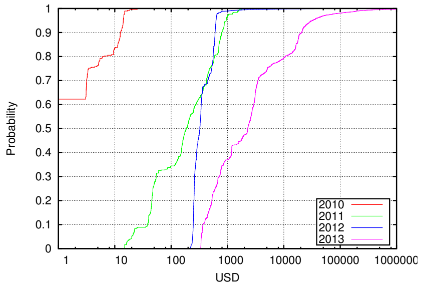


Fig. 2: CDF of Miners' Annually Earning

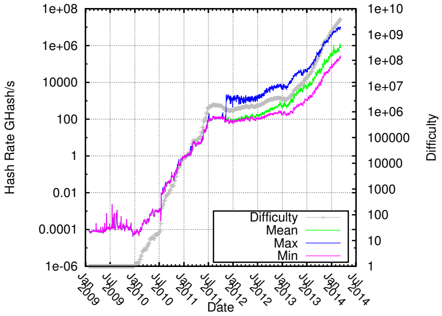


Fig. 3: Bitcoin Network Hash Rate

	Frozen Ratio	Transfer Lag
2009	66.36%	138 Days
2010	20.13%	102 Days
2011	1.89%	19 Days
2012	0.49%	7 Days
2013	0.96%	1.5 Days

Fig. 4: Fraction of Frozen Miners and Average Transfer Lag of Active Miners

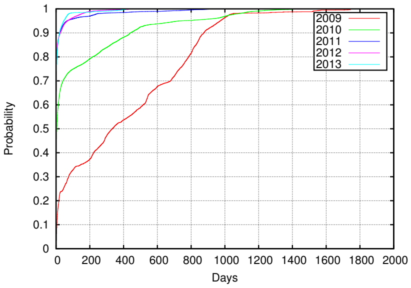
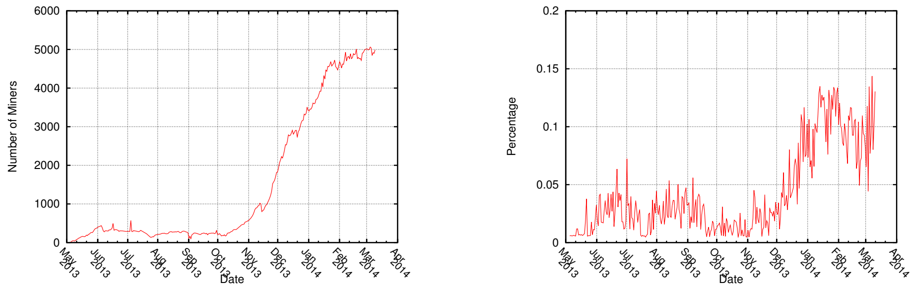


Fig. 5: Transfer Lag Distribution

We now examine how fast miners transfer out mined Bitcoins. We measure the time lag between a miner claimed a block and her next transaction. If a miner has no subsequent transaction in our trace, we tag the minor as frozen. For active miners, we calculate the average and distribution of their transfer lags. As shown in Figure 4, a large fraction of early miners were frozen and never touched their mined Bitcoins, even after the Bitcoin price surge in 2013. Our conjecture is that those early miners were casual early adopters of Bitcoin as a fun technology, and they were not motivated by the potential financial value of Bitcoin. When Bitcoin became valuable, they might have, unfortunately, lost their account IDs, so that couldn't cash out. This suggests that lots of Bitcoins mined in the first two years might have been lost permanently! Things changed completely in 2011, not surprisingly, this is in sync with the value increase of Bitcoin. Not only almost all miners are active, the lag for transfer gets shorter and shorter. The slight increase in frozen ratio from 2012 to 2013 is due to the artifact that our trace ends in March 2014. Figure 5 further illustrates the decrease trend of transfer lags as time evolves. This suggests that later miners were explicitly driven by profits and diligently transferred out mined Bitcoins.

5.2 Pool Mining

Figure 6a shows the evolution of the number of miners in F2Pool. We can see that from May to October 2013, the number of pool miners is relatively stable. This is due to the stable Bitcoin price around $120 in that period. Figure 6b plots the ratio between F2Pool's computation power over that of the whole network. The ratio is also relatively stable from from May to October 2013. Starting from



(a) (b)

Fig. 6: (a) F2Pool Miner Growth, (b) F2Pool Computation Share

November 2013, motivated by the price surge of Bitcoin, the number of miners increased more than ten times till March 2014. As illustrated in Figure 6b, F2Pool's computation share also increases dramatically. This indicates that more miners chose to join pool mining in the face of increasingly tense competition between minors. In Figure 7, we estimates the mean and median hash rate of F2Pool miners, and how much computation power is controlled by the top 10% powerful pool miners. The mean is larger than the median and the top 10% miners dominate the computation power of the pool. This is because the hash rates of the top pool miners are significantly larger than the low-end miners. Since the earning of a minor in a pool is proportional to her hash rate, the earning distribution among miners in a mining pool conforms to the power law wealth distribution in the real world.

5.3 Economic Considerations

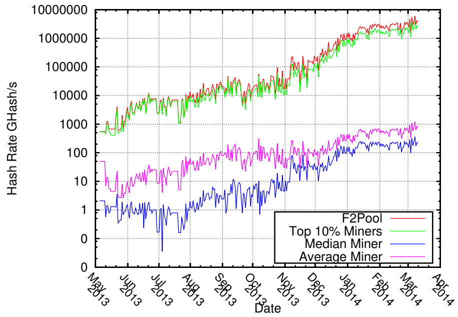
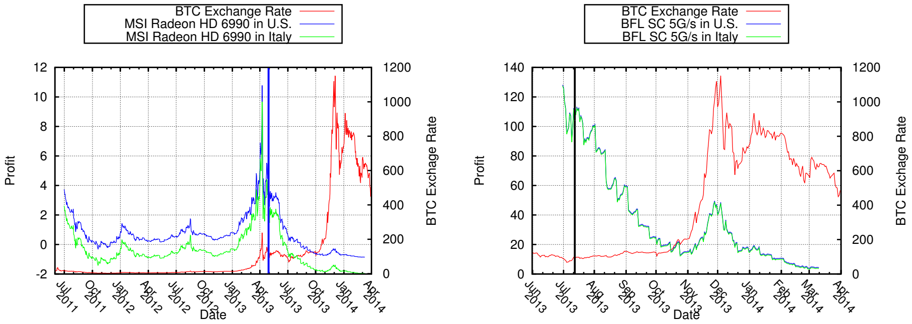


Fig. 7: F2Pool Miner Hash Rate vs. Pool Hash Rate

Curious in knowing whether miners can get their investment back, we choose two mining hardwares released in 2011 and 2013 respectively. The first one is MSI Radeon HD 6990 graphics card with 750 MHash/s and 410 Watt. The price for this card at release was $699. From 2010, mainstream miners started to use graphics cards to do mining instead of CPUs. We set a starting date on 07/01/2011. We calculate the card's profit rate according to (4) using the real Bitcoin price and electricity prices in US and Italy respectively. As shown in Figure 8a, this card generates positive profits in US, breaks even (earns $699 back) on 2013/04/30, and continues to make money till September 2013. Then the daily profit becomes negative even though the Bitcoin price kept increasing. This is because as more minors joined the system, the difficulty value increased at a faster pace than the Bitcoin price. According to (5), the card's computation-over-power efficiency can no longer sustain a positive profit rate. Meanwhile, due to higher electricity price (see Table 1), mining in Italy seldom gets positive profit. There is no way for the miner to recover her capital cost. In late 2012 and early 2013, powerful ASIC mining hardware started to occupy the mining market. We estimate BFL SC 5G/s mining cube, a 5,000 MHash/sec and 30 Watt ASIC chip for just $274. We find that if it were purchased on 2013/07/01, no matter in US or Italy, it would have broken even with less than one month. The major reason is that the computation-over-power efficiency of this new card is about one hundred times higher than MSI Radeon HD 6990 graphics card.



(a) Graphics Card in 2011

(b) ASCI Card in 2013

Fig. 8: Daily Mining Profit Rate and Break-even Time.

Country	Italy	UK	Belgium	U.S.	Sweden
Average Electricity Price in 2013 (Cent per KWh)	20.56	13.61	11.77	9.33	8.25
Network Margin (THash/s)	473,325	715,031	826,812	1,043,041	1,179,584

Table 1: Sustainable Computation Power under Current Bitcoin Price

Finally, we estimate the computation power upper bound of Bitcoin network according to (7). We use the current Bitcoin price and the average electricity prices in different countries [20] to estimate mining cost. We choose the current best hardware SP35 YUKON ASIC chip, which has 6 THash/s and 3,500 Watt. Table 1 shows as the electricity price varies, the network computation power upper bound can differ by a factor of 2.5. The current Bitcoin network has a computation power of 248,116 THash/s. There is still room for growth. Since in average the network computation power doubles every two months, our conjecture is that the network will saturate in about half year, given that the Bitcoin price and mining hardware efficiency stay still.

6 Conclusion

In this paper we characterized the evolution of Bitcoin miners' productivity, computation power and transaction activity by analyzing the full blockchain in Bitcoin network. We showed how the largest mining pool in Bitcoin grows over time and how computation power is distributed among its miners. We also built a simple economic model that explains the evolution of mining hardware and predicts the limit of the computation race game between miners.

References

1. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. (2008) http://www.bitcoin.org/bitcoin.pdf.
2. bitcoin.org: Frequently asked questions. (https://bitcoin.org/en/faq) Accessed September 10, 2014.
3. Coinbase.com. (https://www.coinbase.com) Accessed September 10, 2014.
4. Bitstamp.com. (https://www.bitstamp.net) Accessed September 10, 2014.
5. F2Pool.com. (https://www.f2pool.com) Accessed September 10, 2014.
6. Babaioff, M., Dobzinski, S., Oren, S., Zohar, A.: On bitcoin and red balloons. In: Proceedings of the 13th ACM Conference on Electronic Commerce, ACM (2012) 56–73
7. Decker, C., Wattenhofer, R.: Information propagation in the bitcoin network. In: Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on, IEEE (2013) 1–10
8. Ron, D., Shamir, A.: Quantitative analysis of the full bitcoin transaction graph. In: Financial Cryptography and Data Security. Springer (2013) 6–24
9. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: Characterizing payments among men with no names. In: Proceedings of the 2013 conference on Internet measurement conference, ACM (2013) 127–140
10. Reid, F., Harrigan, M.: An Analysis of Anonymity in the Bitcoin System. Springer (2013)
11. Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S.: Evaluating user privacy in bitcoin. In: Financial Cryptography and Data Security. Springer (2013) 34–51
12. Ober, M., Katzenbeisser, S., Hamacher, K.: Structure and anonymity of the bitcoin transaction graph. Future internet **5** (2013) 237–250
13. Möser, M.: Anonymity of bitcoin transactions. In: Münster Bitcoin Conference. (2013)
14. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. arXiv preprint arXiv:1311.0243 (2013)
15. Kroll, J.A., Davey, I.C., Felten, E.W.: The economics of bitcoin mining, or bitcoin in the presence of adversaries. In: Proceedings of WEIS. Volume 2013. (2013)
16. Huang, D.Y., Dharmdasani, H., Meiklejohn, S., Dave, V., Grier, C., McCoy, D., Savage, S., Weaver, N., Snoeren, A.C., Levchenko, K.: Botcoin: Monetizing stolen cycles. In: Proceedings of the Network and Distributed System Security Symposium (NDSS). (2014)
17. Bitcoinwiki: Bitcoin difficulty. (https://en.bitcoin.it/wiki/Difficulty) Accessed September 10, 2014.
18. bitcoin.cz: World's first mining pool celebrates 3rd year with 0% fee. (https://mining.bitcoin.cz/news/2013-12-16-pool-celebrates-3rd-anniversary) Accessed September 10, 2014.
19. blockchain.info: An estimation of hashrate distribution amongst the largest mining pools. (https://blockchain.info/pools/) Accessed September 10, 2014.
20. statista.com: Felectricity prices in selected countries in 2013 (in u.s. dollar cents per kilowatt hour). (http://www.statista.com/statistics/263492/electricity-prices-in-selected-countries/) Accessed September 10, 2014.