Bitcoin Suisse | Decrypt

August 6, 2019 | Season 1 Episode 3

Exploring the Coinbase

The Bitcoin blockchain continues to increase in strength. Its hashrate and mining difficulty have recently reached all-time highs. But what are the incentives to secure a public blockchain? And how does network growth affect decentralization?

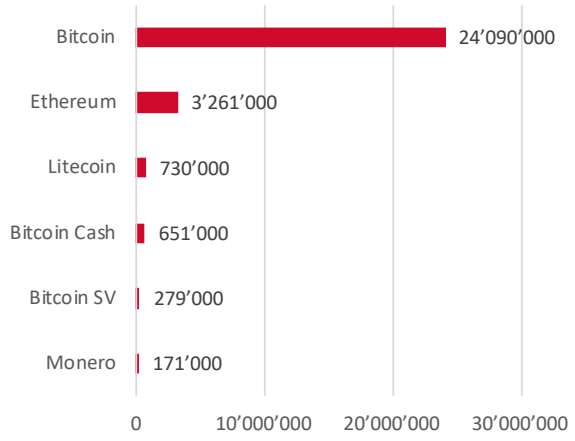
Written by Dr. Raffael Huber from Bitcoin Suisse Research
and Demelza Kelso Hays and Mark J. Valek from incrementum

In the last episode of Bitcoin Suisse Decrypt, we introduced the *blockchain trilemma*, which describes the trade-offs between security, decentralization, and scalability. Of the three, blockchain security is unarguably essential for a network which captures hundreds of billions of dollars in value. As such, the incentives to participate in the network and to help secure it need to be game-theoretically sound. The underlying blockchain protocol must ensure that rational actors benefit more from honest behavior than from operating maliciously. Hence, a potential monetary gain e.g. from double-spending coins should never exceed the costs of the attack.

> *"In order to have a decentralised database, you need to have security. In order to have security, you need to have incentives."*
> *– Vitalik Buterin*

But security is not free. To incentivize participation and thus strengthen the network, most public blockchains pay out a block reward to miners (in proof of work) or to validators/forgers (their equivalent in proof of stake). In Bitcoin, every block includes a *coinbase transaction*, which rewards the miner with an amount of Bitcoin (currently 12.5 BTC) for their work. Ultimately, **the block reward is the price that a decentralized cryptocurrency system pays to miners to secure and propagate the blockchain**. A comparison of mining rewards in large market cap blockchains is shown in Illustration 1.

Illustration 1: Estimate of total daily miner rewards in USD for large market cap blockchains in August 2019.



Source: bitinfocharts.com, Bitcoin Suisse Research.

At more than $24 million per day, Bitcoin pays its miners by far the most, more than seven times as much as Ethereum currently does. For cryptocurrencies that employ the same mining algorithms, the ratio between the two total daily reward amounts also gives an indication of the relative hash rate between the chains. For example, the ratio of rewards for Bitcoin and its fork Bitcoin Cash sits at 2.70%, and the current relative hashrate over the last seven days at 2.71%.[1]

Block rewards are not static, though. For Bitcoin and its forks, the block reward halves every 210'000 blocks – also called the "halvening". The next reward halving for Bitcoin is expected in May 2020,[2] when the block reward will be reduced from 12.5 BTC to 6.25 BTC. Litecoin had its own halvening event just yesterday, going from 25 LTC to 12.5 LTC per block. Ethereum reduced block rewards from 3 to 2 ETH per block (the "thirdening") at the end of February during its last protocol upgrade, the Constantinople hard fork.[3] Such reductions in inflation have previously been associated with price increases in the time periods leading up to them. The most recent example is again Litecoin, which rose almost 400% from January 1 to June 22 and even outperformed Bitcoin (roughly +300% during that time).

In terms of overall chain security, Bitcoin has achieved another all-time high "proof of work equivalent days" in July.[4] This is a measure which describes the time required to rewrite the entire blockchain with 100% of the available hash power. For Bitcoin, more than a year of mining at full capacity would be necessary to rewrite the chain. As such, Bitcoin's network security is stronger than ever.

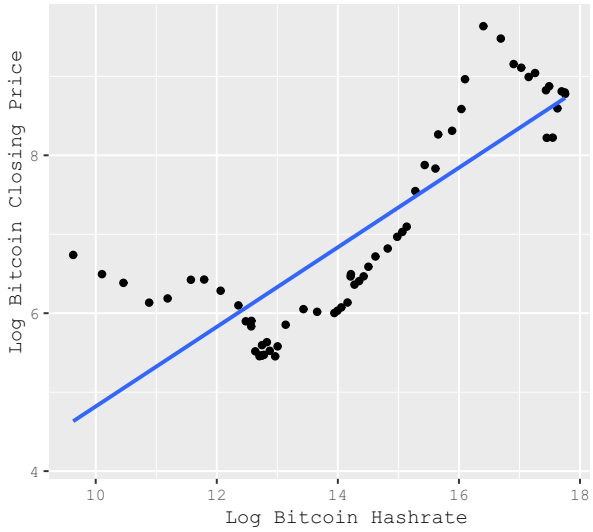
Decentralization and Bitcoin's Proof of Work

Bitcoin's programming code is open source. This means that anyone can modify Bitcoin's rules and start a new cryptocurrency. Since Bitcoin's secret recipe is not patented, trademarked, or otherwise protected by intellectual property contracts, critics of Bitcoin argue that Bitcoin is not scarce because forking Bitcoin and creating Bitcoin 2.0 takes only a few minutes. This is a common misconception. Bitcoin is not considered scarce because there are only 21 million Bitcoin. Rather, Bitcoin is scarce because there are approximately six million specialized computers[5] consuming an estimated 63 terawatt hours (TWh) of electricity per year that secure Bitcoin against a double-spend attack.[6]

This week Bitcoin's hashrate reached an all-time high of almost 79 Exahashs per second (EH/s).[7] When Bitcoin hit its all-time price of $19'891 in December of 2017, its hashrate was only 15 EH/s, meaning that it has become 400% more difficult to double-spend Bitcoin. Buying equipment and energy to produce Bitcoin's hashrate requires scarce resources, and anyone that wants to create a new Bitcoin must find a way to incentivize people to invest capital and labor into securing that coin instead of Bitcoin.

The cost of mining Bitcoin has a positive correlation coefficient with the price of Bitcoin of 0.829.

Illustration 2: Correlation of monthly price of Bitcoin and hashrate from 2013–2019



Source: Blockchain.info, Incrementum AG.

Miners are price takers, which means they will sell Bitcoin for the going price on the free market. Their revenue is a variable function based on the number of Bitcoins sold multiplied by the price of Bitcoin on the market. However, the costs of mining are both variable and fixed. The variable costs of mining are the costs that are dependent on the number of Bitcoin mined. For example, mining

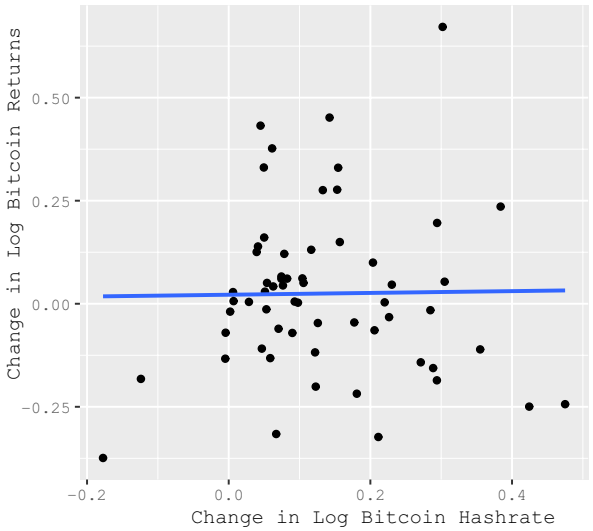
1. https://fork.lol/
2. https://www.bitcoinblockhalf.com/
3. https://media.consensys.net/the-thirdening-what-you-need-to-know-df96599ad857
4. http://bitcoin.sipa.be/index.html
5. If we assume the market consists of all Antminer S9s, then Bitcoin's current hashrate of 77.5 EH/s divided by an Antminer S9's hashrate of 13.5 TH/s equals approximately 5.74 million specialized computers.
6. https://cbeci.org/
7. https://www.blockchain.com/de/charts/hash-rate

more Bitcoin means a higher electricity cost. The fixed costs include buying mining equipment, installing an electricity generator, and renting or buying a warehouse. **Whenever a business has fixed costs, there are economies of scale.** Economies of scale mean that larger businesses are more profitable on average than smaller businesses. The miners try to spread out the start-up costs of the mining rigs and racks over as many Bitcoin as possible. In economic terms, the marginal cost of producing another Bitcoin is decreasing. Economies of scale encourage centralization, which runs perpendicular to the decentralized ethos associated with cryptocurrencies and the blockchain technology.

However, there is a second and even more centralizing force that steers Bitcoin mining. Cheap supplies of electricity are located in specific geographic areas because of infrastructure, regulations, and natural resources. Most miners are in China because of coal and hydropower, and there is an emerging trend of miners going to Texas for cheap natural gas. As miners scour the earth for the cheapest source of electricity, the arbitrage opportunity of low electricity costs will decrease. Therefore, many mining projects will fail leaving only a few large mining companies located near sources of cheap electricity.

Despite the strong correlation between Bitcoin's hashrate and price, the relationship is not causal, and is, therefore, not a good predictor of short-term price movements. Plotting the growth rate in return versus the growth rate in hashrate (Illustration 3) makes the positive linear relationship disappear. This is because the hashrate seen on the Bitcoin blockchain today is often the result of mining investment decisions taken between nine months to a year prior.

Illustration 3: Rate of change of monthly price of Bitcoin and hashrate from 2013–2019.



Source: Blockchain.info, Incrementum AG.

Bitcoin Suisse AG
CH-6300 Zug
bitcoinsuisse.com

in collaboration with

incrementum