Marcel Thum

The Economic Cost of Bitcoin Mining

Marcel Thum
ifo Institute and Technical University Dresden

Until recently, Bitcoins were mostly a topic for computer nerds. This has changed dramatically. Nowadays, Bitcoins and other crypto currencies are widely discussed as part of general payment systems and as speculative investments. The economic literature on crypto currencies has grown substantially. Yermack (2013), for instance, investigates the extent to which Bitcoins fulfill the usual criteria of monetary currencies. Another important research topic is the need for the regulation of crypto currencies (ifo Schnelldienst 2017). The exponential growth and subsequent crash of Bitcoin prices has led to greater debate over speculative bubbles in crypto currencies. However, the social costs of crypto currencies have been largely neglected in the academic and public debate. Some proponents of crypto currencies still paint an idyllic scene of a decentralized currency created by 'volunteers' as if Bitcoin mining was done for the common good only. Nothing could be more misleading. While central banks can create cash at almost no cost – printing a bank note uses up very few resources – this is not true of a virtual currency like Bitcoins. Although Bitcoins have only been in existence for a few years, they have cost society over 5 billion US dollars.

To understand their social cost, a brief and admittedly sketchy description of the process of Bitcoin mining might be helpful.[1] In the following, all aspects regarding the trading of Bitcoins – for purposes of payment or speculation – are completely ignored, as the social costs of crypto currencies are generated in the mining process, i.e. in the production of new Bitcoins. How do new Bitcoins enter the world? Ultimately Bitcoins are just a text file or a chain of linked text files. Every transfer of a Bitcoin from one person to another is irrevocably written into this text file ('blockchain'). To safeguard the text file against manipulation, a checksum ('hash') has to be generated. Calculating this checksum is a complex task requiring significant computing resources. Nowadays thousands of highly specialized server farms, distributed across the world, compete to be the first to come up with the next valid checksum. The Bitcoin system is designed in a way that the complexity of calculating the checksum increases when the global computing capacity increases. On average, the blockchain is amended every ten minutes; hence, Bitcoin miners around the globe have to generate six new checksums per hour.[2]

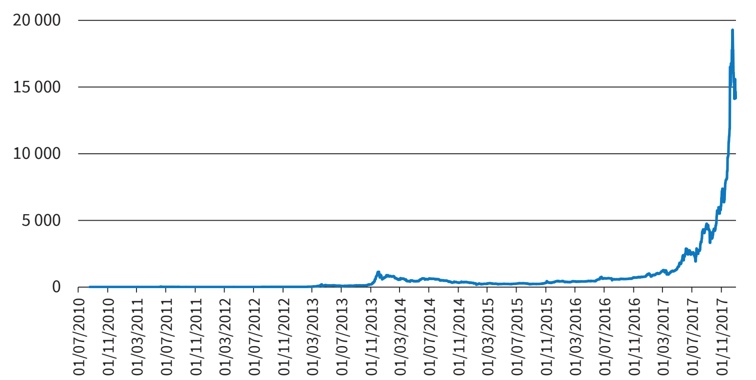
What are the incentives for miners – i.e. all those who try to find a new checksum – to invest time, energy and capital (high-powered server farms) into this stochastic search process? The first miner, who succeeds in generating a new valid checksum and therefore in amending the blockchain, is remunerated with Bitcoins. All other miners who also invested resources in the search for the new checksum go away empty-handed. The remuneration of successful miners falls over time. For the first 210,000 blocks the remuneration was 50 Bitcoins per new block, then it fell to 25 Bitcoins per block for the next 210,000 blocks and so on. Whenever 210,000 blocks have been added, the remuneration is halved.

The social costs of global Bitcoin mining can be estimated by employing standard economic theory. The competitive process among the miners resembles a rent-seeking contest.[3] In a rent-seeking contest, all competitors have to invest real resources to stand a chance of obtaining a prize. (In standard market competition, by contrast, only those firms who stay in business have to incur costs in production.) Ultimately, rent seeking is a wasteful process as the efforts made by the losing parties were in vain. Tullock's model of rent seeking shows that total efforts increase with the number of competitors and that – with free entry – the

Figure 1

Bitcoin Prices

US dollars



Source: https://blockchain.info.

[1] A more detailed description can be found in Velde (2013) and Kroll *et al.* (2013), where topics like the security of crypto currencies and fraud are also discussed.

[2] The checksum for the new blockchain will only be valid if the checksum is under a certain threshold. This threshold is regularly adjusted so that – given the global computing capacity of all Bitcoin miners – six blocks are added per hour on average.

[3] The seminal paper is Tullock (1967). For a survey of rent seeking, see Nitzan (1994).

Table 1

Present Value Costs of Bitcoin Mining (in billions of US dollars)

Discount factor	2%	4%	6%
Present value of mining costs	5.123	5.267	5.417

Source: Author's own calculations.

total expenditure equals the prize. The prize, which the miners are competing for, is the current value of the Bitcoins that are paid out as remuneration for the successful discovery of a new checksum. The Tullock model implies that the costs of Bitcoin mining can be approximated through the value of newly minted Bitcoins. Whatever the development of Bitcoin prices, at each point in time the costs of mining correspond to the value of new Bitcoins, which are paid out as remuneration for successful mining. Each single miner can try to reduce his or her costs, for example, by locating the server farms in regions with low energy costs like Iceland. However, this does not affect the overall outcome, as lower energy costs are completely offset by additional computer operations and the entry of new competitors. (A sketch of the formal model is provided in the Box 1.)

To establish the total costs of Bitcoin mining, we calculate the value of newly minted Bitcoins for each day. This value is obtained by multiplying the daily Bitcoin price (in US dollars) with the number of newly minted Bitcoins. Figure 1 shows the price development of Bitcoins since August 2010. The Bitcoin system was already in place in January 2009. Consistent price data, however, are not available for the initial phase of Bitcoin trading.[4] For days without quotes, the last available price is held constant. Figure 1 shows that the Bitcoin price remained fairly low for a long time and did not start to increase significantly until mid-2016.

As mentioned earlier, miners received 50 Bitcoins for each new block for the first 210,000 blocks that were added to the blockchain. On 28 November 2012, the remuneration fell to 25 Bitcoins. As of 10 July 2016, only 12.5 Bitcoins are paid for the first valid checksum of a new block. Combining remuneration and Bitcoin prices allows us to calculate the value of newly minted Bitcoins for each day up to 31 December

[4] Due to the low Bitcoin prices in the first years of its existence, the starting date for the calculations is almost irrelevant to the outcome.

Box 1

The remuneration of a miner who is successful at time *t* amounts to *R(t)* Bitcoins. At time *t*, this remuneration has a market value of *p(t) · R(t)* where *p* is the Bitcoin price in US dollars. The efforts of a single miner can be expressed by the number of computer operations, with which the miner tries to win the race for the first valid checksum. Let m_i be the number of computer operations of miner *i* in a given period. The probability of successful mining can then be written as $\frac{m_i}{m_i + \sum_{j \neq i} m_j}$ where $\sum_{j \neq i} m_j$ is the total effort of all other miners. The expected profit of miner *i* is

$$(1) \quad E\pi_i = \frac{m_i}{m_i + \sum_{j \neq i} m_j} \cdot p \cdot R - c \cdot m_i - C$$

where *c* stands for the variable cost per computer operation (e.g. energy cost) and *C* for the fixed cost of mining.

Maximising miner *i*'s profit for a given effort of all other miners yields

$$(2) \quad \frac{\partial E\pi_i}{\partial m_i} = \frac{\sum_{j \neq i} m_j}{\left(m_i + \sum_{j \neq i} m_j\right)^2} \cdot p \cdot R - c = 0$$

With a total number of *n* miners in the market, each miner exerts an effort of

$$(3) \quad m_i^* = \frac{n-1}{n^2} \cdot \frac{p \cdot R}{c}$$

in the symmetric equilibrium ($m_i = m_j$). Hence, the expected profit of a representative miner can be written as

$$(4) \quad E\pi_i^* = \frac{p \cdot R}{n^2} - C$$

With free market entry, miners should enter up to the point where all profits are dissipated ($E\pi_i^* = 0$). The number of miners amounts to

$$(5) \quad n^* = \sqrt{\frac{p \cdot R}{C}}$$

It increases in the remuneration and decreases with the fixed cost. The key point here is that as each miner earns zero profits in expectation, the costs of mining have to match the value of newly minted Bitcoins at each point in time.

2017.[5] These values are then discounted to 1 January 2018 and added up. Table 1 shows the present value of the costs of Bitcoin mining at alternative discount rates. At a discount factor of 4 percent, the total costs of Bitcoin mining (in present value terms) amount to 5.3 billion US dollars. As a matter of course, some miners make a profit as they were lucky to be the first with new hashes and the value of remuneration exceeded their costs. These profits, however, are mirrored by the losses of other miners who unsuccessfully installed computing capacity and wasted time, energy and natural resources. The energy consumption alone, which is only one element of total costs, currently amounts to 259 KWh for a single Bitcoin transaction – more than one US household's weekly energy consumption (https://digiconomist.net/bitcoin-sustainability-report-12-2017). Table 1 also shows that the precise level of the discount factor is almost irrelevant to the outcome as the bulk of the social costs of Bitcoin mining were generated last year (2017). In all scenarios, the total costs of Bitcoin mining are in the range of 5 billion US dollars. In addition to the recently debated challenges of a Bitcoin system, like the cyber attacks on Bitcoin exchanges and the risk of a bursting bubble, the Bitcoin system also suffers from a massive waste of resources.

REFERENCES

ifo Schnelldienst (2017), "Kryptowährung Bitcoin: Währungswettbewerb oder Spekulationsobjekt: Welche Konsequenzen sind für das aktuelle Geldsystem zu erwarten?", *ifo Schnelldienst* 22, 3-20.

Kroll, J.A., I.C. Davey and E.W Felten (2013), *The Economics of Bitcoin Mining or, Bitcoin in the Presence of Adversaries*, The Twelfth Workshop on the Economics of Information Security, Washington DC, 11-12 June 2013.

Nitzan, S. (1994), "Modelling Rent-Seeking Contests", *Public Choice* 10, 41-60.

Tullock, G. (1967), "The Welfare Costs of Tariffs, Monopolies, and Theft", *Western Economic Journal* 5, 224-232.

Velde, F.R. (2013), *Bitcoin: A Primer*, Chicago Fed Letter 317, December.

Yermack, D. (2013), *Is Bitcoin a Real Currency? An Economic Appraisal*, NBER Working Paper 19747.

[5] In addition to the remuneration for valid checksums, miners also receive transaction fees. These transaction fees are ignored in the present calculation.