Game of Hashes

A study on the driving forces of the Bitcoin price

Executive Summary:

In the period between December 2017 and December 2018, the price of Bitcoin reached an all-time record of almost 20'000 USD and a minimum price of about 3'200 USD. In this short study, we analyze and explain some of the driving forces that negatively influenced the price of Bitcoin during the last quarter of 2018. Our purpose is to understand some of the mechanisms behind the price fluctuations of cryptocurrencies. Since many of the technical factors that alter the price of cryptocurrencies, such as forks or moves in the mining hash power, can be foreseen by observing social media and metrics in the network—like the fees paid to the miners, or the block time—we argue that active management of cryptocurrency portfolios might be able to anticipate some of the future (positive or negative) sharp moves in the price of cryptocurrencies.

Date:

December 2018

Authors:

José Parra Moyano

Prof. Karl Schmedders, PhD

Disclaimer

The Content is for informational purposes only, you should not construe any such information or other material as legal, tax, investment, financial, or other advice. Nothing contained here constitutes a solicitation, recommendation, endorsement, or offer by the authors, or any third party service provider to buy or sell any cryptocurrency or other financial instruments in this or in in any other jurisdiction.

All Content on this file is information of a general nature and does not address the circumstances of any particular individual or entity. Nothing in the document constitutes professional and/or financial advice, nor does any information on the document constitute a comprehensive or complete statement of the matters discussed or the law relating thereto. The authors are not a fiduciary by virtue of any person's use of or access to the document or Content.

You alone assume the sole responsibility of evaluating the merits and risks associated with the use of any information or other Content on the document before making any decisions based on such information or other Content. In exchange for using the document, you agree not to hold the authors, its affiliates or any third party service provider liable for any possible claim for damages arising from any decision you make based on information or other Content made available to you through the document.

Introduction

In order to analyze the development of the Bitcoin price, we first introduce and explain various technical concepts that are necessary to understand the explanation. We start introducing mining in "Proof of Work" protocols and the role of hash power in the probability of writing valid blocks. We continue by introducing forks, which are changes in the original protocol that yield new currencies. Only after introducing these concepts we analyze and explain the development of the Bitcoin price in the last quarter of 2018.

Understanding Proof of Work Mining

Bitcoin is a currency that is created by computers, which are commonly referred as "miners". Miners follow the Bitcoin protocol, which is the set of rules that defines how new bitcoins are created and how bitcoin transactions are validated. New bitcoins are created whenever a miner writes a valid block. A block is a piece of information (that can be understood as an entry in an accounting ledger), which refers to the history of all previous valid transactions by means of a cryptographic hash and adds information about new transactions. A valid block confirms the new transactions made by bitcoin users. A valid block is a block that respects the rules of the Bitcoin protocol. Valid blocks are created in a random manner, such that miners need to write and test many versions of a block until they find one that is valid. Once a miner finds a valid version of a block, the block is added to the blockchain and the mining process starts again. [1]

In order to write versions of a block, miners use computational power –hash power– which is what is required to write versions of a block. The higher the hash power that a miner devotes to writing versions of a block, the higher its probability of writing a valid block and of earning the new bitcoins that the valid block contains. As already stated, mining is a random process. The probability of a miner writing a valid block depends not only on its hash power, but also on the networks' "difficulty". The difficulty is a parameter that is adapted every 2016 blocks, such that on average, a miner of the network finds a block every 10 minutes. Nowadays hash power can be rented online.

Understanding Forks

The Bitcoin protocol is open and can be replicated and altered by any miner. When miners disagree about the mechanics of a currency (block size, block reward, average mining time, etc.) they can slightly alter the protocol and create a "fork" to accommodate the cryptocurrency to their needs. A fork is a change in the protocol of the original currency. Forks yield new currencies. [2]

A famous and successful fork that occurred to Bitcoin was the Bitcoin Fork of August 2017. As of August 1st, 2017, a different version of the Bitcoin protocol was released under the name of Bitcoin Cash [3]. This has resulted in the coexistence of two similar but independent cryptocurrencies: Bitcoin and Bitcoin Cash. While forks are neither good nor bad, miners of the original currency need to decide by the time of the fork which currency they are going to mine, since mining of both currencies with the same piece of hardware is not possible. In other words, miners need to decide which protocol to follow and for which currency they are going to try to write valid blocks. A consequence of forks is that they split the total existing hash power of the original currency (which is just the sum of the hash power of all the miners mining the original currency), since supporters of the forked currency stop mining the original currency.

Hash power plays a crucial role in the success or failure of forks. Cryptocurrencies that are "backed" by a relatively high hash power are less prone to double-spending-attacks than cryptocurrencies that are "backed" by a relatively low hash power. A double-spending-attack is an attack in which miners succeed in writing blocks that spend coins that were previously spent. A fork which attracts a very low proportion of the hash power of the original cryptocurrency is vulnerable to attacks since miners of the original currency have so much relative hash power that they could temporarily join the forked currency and use their relatively high hash power to commit double-spending-attacks. Figure 1 illustrates the hash power distribution of an original and a forked currency, as well as a double-spending-attack from some supporters of the original currency to the forked currency. In Figure 1 the red column in the second diagram represents supporters of the original currency that temporarily

mine the forked currency to conduct double-spending-attacks and undermine the credibility and use of the forked currency.

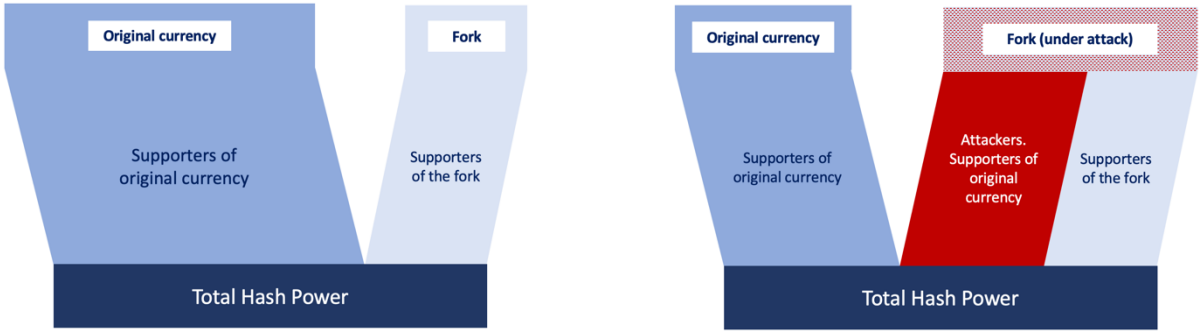

Figure 1: Illustration of hash power distribution and of a double-spending-attack (in red).

Another crucial factor for the success of a fork is the price of its currency immediately after the fork. Since the forked currency and the original currency share their past (they are the same currency until they are forked) all the holders of the original currency are also holders of the forked currency. As a matter of an example: if Alice held one bitcoin on July 31st and made no transaction in the next 48 hours, on August 2nd, after the Bitcoin Cash fork, she would hold one bitcoin and also one bitcoin cash. If Alice and her peers start selling one of both cryptocurrencies, they are signaling on which cryptocurrency they place higher trust, and therefore, the price of the original and forked currency right after the fork are a very good indicator for the survival of the currencies after the fork.

The Bitcoin Cash SV Fork and its Impact on the Bitcoin Price

On November 15th, 2018 Bitcoin Cash was forked in two currencies, namely Bitcoin Cash SV ("SV" standing for "Satoshi's Version"), and Bitcoin Cash ABC ("ABC" standing for "Adjustable Blocksize Cap"). Both versions vary in the implementation of some attributes of the currency and their supporters have fought roughly in terms of price, hash power, and media statements to become the "original" Bitcoin Cash. Bitcoin Cash ABC has been backed by more hash power and is nowadays referred by miners and exchanges as "Bitcoin Cash", whereas Bitcoin Cash SV has kept its versioned name and is currently traded at lower rates than Bitcoin Cash (ABC) [4].

Ahead of the Bitcoin Cash ABC and SV Fork, supporters of both versions started a fight to defend the currency they considered most adequate. This fight did not only involve miners of Bitcoin Cash, but also miners of Bitcoin, and created two factions that have operated furiously in the market to establish the version of Bitcoin Cash that they were backing. This had consequences for both Bitcoin Cash and Bitcoin Cash SV, but also for Bitcoin [5].

First, on November 14th, 2018, two influencers in the Bitcoin community, Craig Wrigh and Jihan Wu, communicated in social media channels that they would sell bitcoin to rent hash power from miners in order to support their respective favorite Bitcoin Cash version and buy the currencies themselves to keep the prices of the forked currencies relatively high [6]. These threats became effective and later that day the price of Bitcoin fell dramatically. Well informed bitcoin holders also sold Bitcoin for fiat currencies or stable coins on that date, which lowered the price of Bitcoin even more [7]. The average price of Bitcoin in the month previous to these statements (October 13th to November 13th) fluctuated between 6259USD and 6634USD, with an average price of 6436USD and a Standard Deviation of 88USD around the mean.

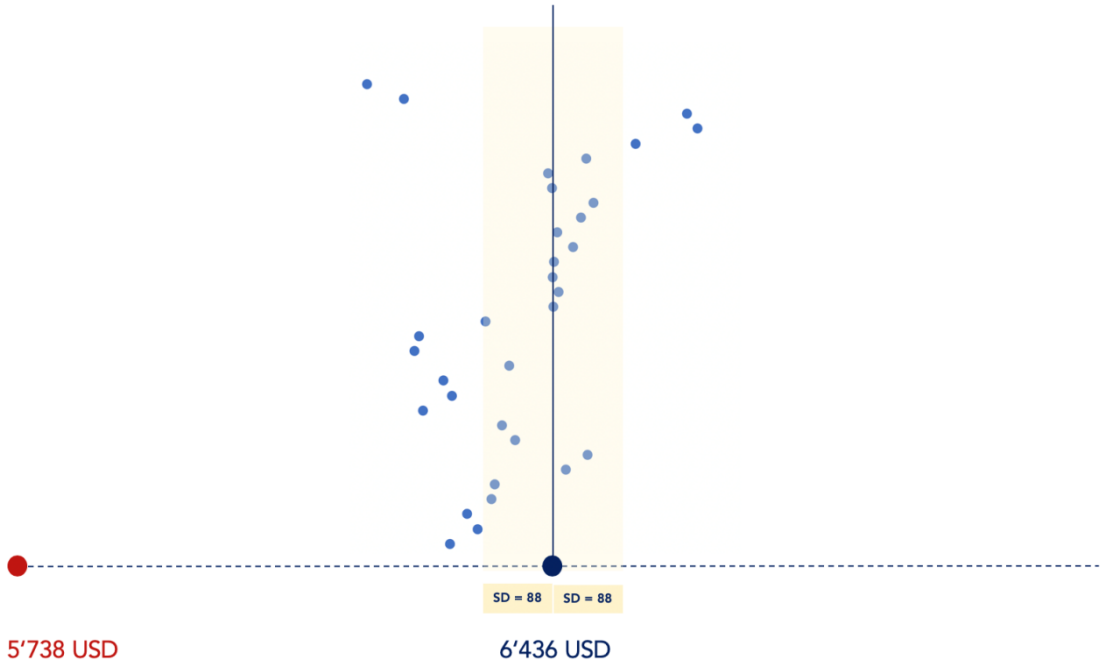

Figure 2: Daily average Bitcoin price and standard deviation between October 13th and November 14th.

On the 24 hours that followed the statements by Craig Wright and Jihan Wu, the price of Bitcoin dropped to 5738USD, which represents a 22% value loss of Bitcoin in 24 hours and a distance from the monthly average of 7.9 standard deviations (an "eight sigma event") [8]. These quantities are represented in Figure 2, where the daily average Bitcoin prices are depicted along the vertical axis in blue, the average price for the observed period is represented in blue at the center of the horizontal axis, and the Bitcoin average price for the end of November 14th is represented in red on the left edge of the horizontal axis.[1]

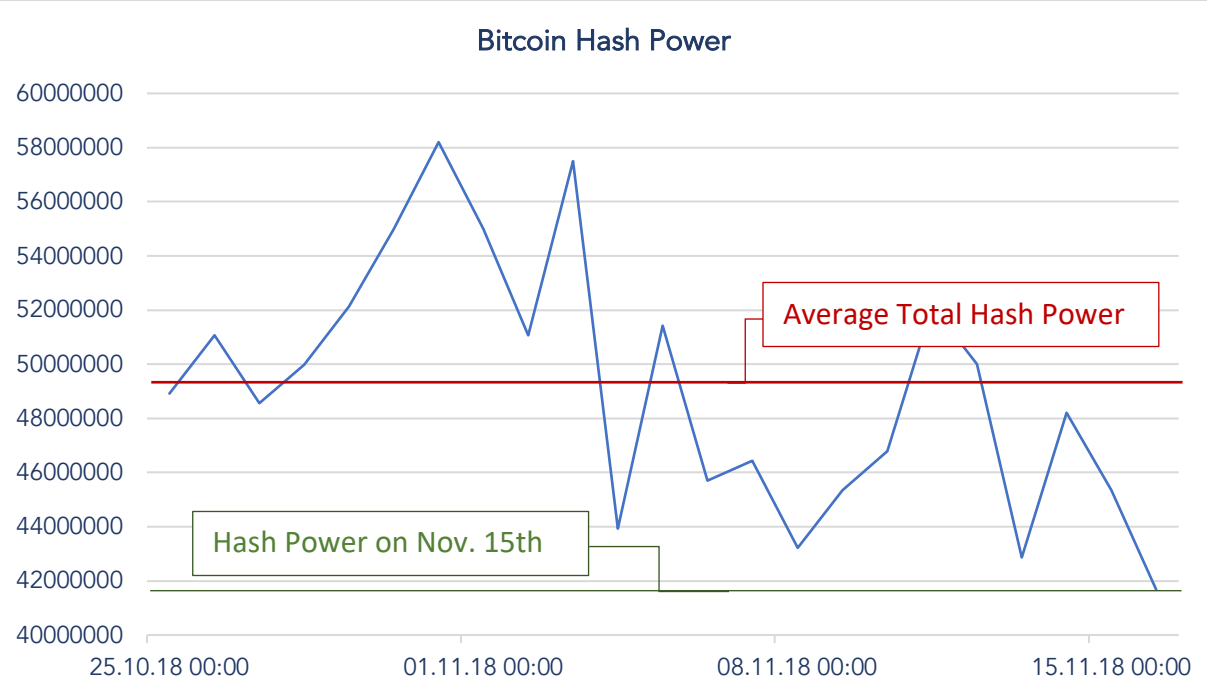

Figure 3: Total hash power of the Bitcoin network between October 25th and November 15th.

Second, hash power of Bitcoin was effectively moved to either ABC or SV, lowering the efficiency and performance of Bitcoin despite the drop in Difficulty, due to higher block times. The lower price of Bitcoin also forced the miners mining at the edge of their benefit

[1] It is worth noting that the Bitcoin Fork of August 2017 was different form the Bitcoin Cash Fork of November 2018, since in the former one there were only two currencies competing for the highest price and highest hash rate, namely Bitcoin and Bitcoin Cash, whereas in the latter one there were the two currencies involved in the fork and a third one (Bitcoin) which was massively sold to influence the price of the forked currencies. In August 2017 there was no "third" cryptocurrency with enough market capitalization, such that if sold, it could influence the price of the forked currencies. Bitcoin was the "forked" currency in August 2017 and the "third" currency in November 2018, and therefore these two forks influenced its price in different directions.

to stop mining Bitcoin in order to avoid incurring losses. A consequence of this was that miners who remained mining Bitcoin needed, on average, a higher time to write a valid block.

The average block time (time required for any miner to write the next valid block) during the 6 months previous to the fork was 584 seconds. The average block time during the 2016 blocks after the fork[2] was 703 seconds, and therefore 20% higher than during the previous 6 months. In terms of performance, longer block times represent a drawback for users aiming to make transactions, since more time is required to validate transactions. In order to prevent these high transaction times, users pay higher transaction fees to incentivize miners to validate their transactions, which makes transactions in Bitcoin more expensive and therefore less attractive than transactions in other currencies [9]. The average daily sum of transaction fees paid in Bitcoin between June 27th and November 13th was 21 bitcoin with a standard deviation from the mean of 5 bitcoins. The transaction fees paid on November 14th and 15th respectively were 26 and 39 Bitcoin, which reflects the higher cost of making payments in Bitcoin [9]. Figure 4 depicts these numbers. As a result, users willing to use a cryptocurrency to make a transaction have had reasons to not use Bitcoin for their purposes, but other currencies instead.

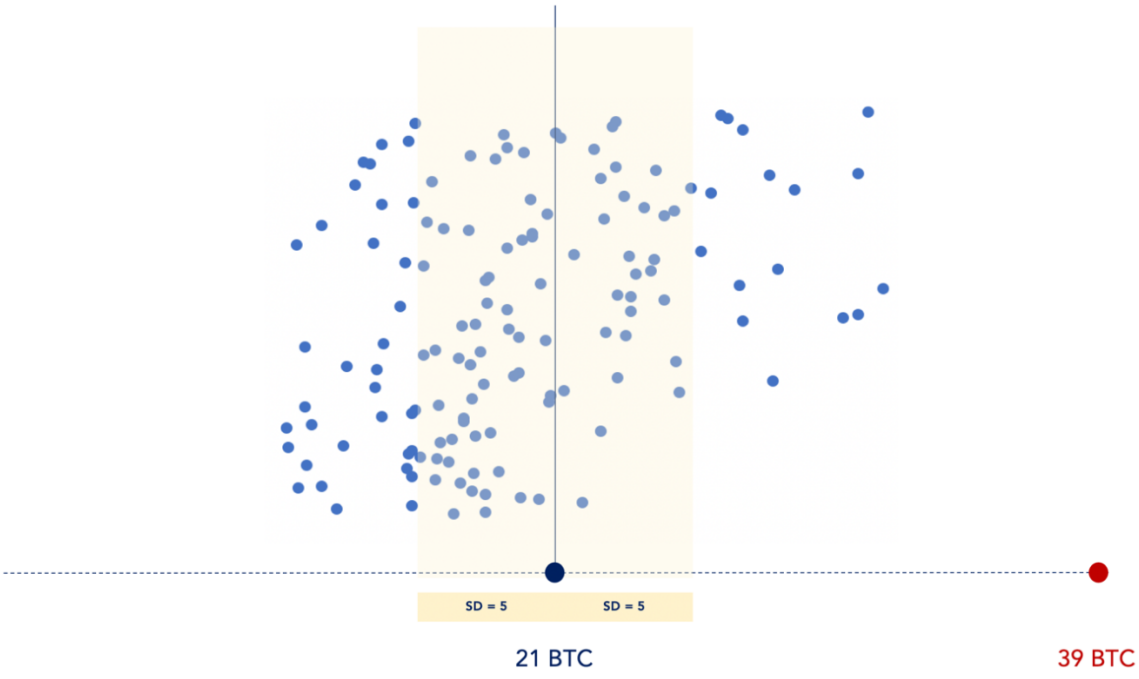

Figure 4: Daily miner's fees comparison.

[2] The Difficulty level of the Bitcoin network during these 2016 was constant at $5{,}9*10^{11}$.

Third, stop-loss orders were activated, yielding a devaluation spiral ("fire sales") in Bitcoin that has resulted in the price drop that we know already.

Average Block time before the fork	Average Block time after the fork
584 seconds	**703 seconds**

Conclusion

While understanding all the forces that drive the price of cryptocurrencies is a difficult if not impossible task, we have analyzed some of the key reasons for the decline in the price of bitcoin during November 14th and 15th. Our aim is to understand some of these fundamentals and in order to anticipate –or at least explain– sharp moves in the prices of cryptocurrencies.

We have shown how the Bitcoin Cash SV Fork influenced the price of Bitcoin, due to the fact that supporters of both Bitcoin Cash versions sold bitcoin on November 14th to rent mining power and support their favorite Bitcoin Cash version. Well informed investors anticipated this move and also sold Bitcoin to minimize losses. Due to these moves, less hash power remained mining bitcoin, which increased the block time by as much as 20%, lowering the performance of the network, and making it less attractive for users to make payments in Bitcoin. All these forces have had an impact on the negative price development of Bitcoin during November 2018.

The information about the Bitcoin Cash Fork was available to investors and portfolio managers prior to the price drop. This information combined with a solid understanding of the impact of hash power on the performance of cryptocurrencies helped well informed investors who could minimize the losses. Due this kind of moves, which are not rare in the cryptocurrency space, active portfolio management might yield better results than passive portfolio management.

Sources

[1] Andreas M. Antonopoulos, Mastering Bitcoin, Unlocking Digital Cryptocurrencies, O'Reilyy Media 2014.

[2] https://en.bitcoin.it/wiki/Hardfork, last accessed on December 23rd.

[3] https://en.wikipedia.org/wiki/Bitcoin_Cash, last accessed on December 23rd.

[4] https://www.investopedia.com/news/all-about-bitcoin-cash-hard-fork/, last accessed on December 26th.

[5] https://www.marketwatch.com/story/what-you-need-to-know-about-the-bitcoin-cash-hard-fork-2018-11-13, last accessed on December 26th.

[6] https://ethereumworldnews.com/how-the-bitcoin-cash-bch-hash-war-is-affecting-bitcoin-btc/, last accessed on December 26th

[7] https://breakermag.com/the-bitcoin-cash-hash-war-by-the-numbers/, last accessed on December 26th

[8] https://coinmarketcap.com, last accessed on December 24th

[9] https://btc.com, last accessed on December 23rd