De-Coding Crypto

Weekly Analysis

The difficulty drop in context

November 13, 2019

In this week's issue, we focus on the 'difficulty drop', and whether we are yet approaching the risk cases for a loss of miner confidence. We also look at the legal situation of cryptocurrency in Russia moving forward.

Written by Joseph Edwards, Head of Research at Enigma Securities.

Our Market View

May you live in interesting times. A strange week for cryptocurrency - most high-cap coins are down by a decent amount, including even some Chinacoins, but it hasn't felt that way. Volatility overall has been on the low side, and while we hoped that we would have a clearer view on direction or at least on timing of the next break, it hasn't come through. We no longer hold a generally bullish bias short-term; we tend to think that we will mostly likely see a drop soon into the $8000-$8500 range, and that we need to see performance in that area before forming any further medium-term bias.

Please direct all queries about this week's research to jedwards@enigma-securities.io.

Market Snapshot

Major

Ticker	Price	7D	1M	6M	12M	Cap
BTC	8717.37	-6.45%	4.68%	20.10%	58.54%	157.3B
ETH	185.993	-2.07%	0.01%	-20.55%	7.86%	20.19B
XRP	0.27036	-9.77%	-7.11%	-27.31%	-44.39%	11.71B
BCH	284.128	-5.65%	24.72%	-20.58%	-27.13%	5.15B
LTC	60.3748	-3.92%	6.45%	-30.25%	45.62%	3.84B
EOS	3.42792	-4.32%	8.57%	-41.91%	-23.85%	3.52B

Selected

Ticker	Price	7D	1M	6M	12M	Cap
LINK	2.99409	12.35%	18.45%	29.45%	29.45%	1.09B
NEO	12.8242	15.32%	72.67%	7.09%	2.17%	0.90B
ONT	0.9179	2.11%	42.82%	3.06%	75.92%	0.64B

The difficulty drop in context

By far the most common enquiry we received over the course of last week was about the difficulty rate adjustment last week, and the implications for hash rate momentum going forward. We have talked about hash rate a couple of times in recent editions of the newsletter - most extensively on 30th October - and, to sum up the key points from those newsletters:

1. Hash rate is seen as a symbol of miner confidence; a decline in overall hash rate implies a loss of confidence to the market in general.
2. Such a loss of confidence has tended to contribute heavily to downwards price movements, since it implies that miners don't expect price to keep up with baselines for production cost in the near-term.
3. There is always the threat of a downwards cascade in those scenarios - the price falls enough to make mining unprofitable, more mining machines are turned off thus driving down hash rate further, and so on.

We did not explicitly talk about difficulty in those newsletters. To briefly explain what difficulty is, Bitcoin is designed to have an essentially flat rate of block creation speed and therefore issuance; to that end, as the network gains more and more processing power, the difficulty of the problems being solved at each step are automatically adjusted in order to ensure that blocks continue to be mined at that rate of approximately once every 10 minutes.

Difficulty in essence is hence a simple function of hash rate - it adjusts once every 2016 blocks (once every fortnight, give or take - 6 blocks per hour * 24 hours * 14 days = 2016 blocks) to reflect hash rate over the last two weeks.

As an absolute measurement, it is hence less useful than hash rate; while hash rate is noisy enough that measurements over even a single day are generally not enough to make any long-term prognostications on, measurements like 7-day moving average are generally considered to usually give a reliable picture.

Why, then, are we talking about difficulty at all? This weekend's difficulty adjustment saw a widely-reported drop in difficulty - implying a drop in hash rate - and a significant one at that:

Date	Difficulty	Change
01/09/2019	1.08E+13	5.78%
13/09/2019	1.19E+13	10.38%
26/09/2019	1.28E+13	7.31%
10/10/2019	1.30E+13	1.95%
23/10/2019	1.37E+13	5.25%
08/11/2019	1.27E+13	-7.10%

Data via blockchain.com.

That 7% drop is, by percentage, the fourth-biggest drop since 2014. Simply put, difficulty has historically very rarely reduced, because even when the market suffers from leaner times and there is possibly even an outflow of smaller miners on account of no longer being profitable, the eternal upwards march of technology and per-unit processing has kept hash rates up. Here are all the drops in difficulty since 2017:

Date	Difficulty	Change
03/07/2017	7.09E+11	-0.43%
25/08/2017	8.88E+11	-3.80%
11/11/2017	1.36E+12	-6.09%
25/11/2017	1.35E+12	-1.28%
18/07/2018	5.18E+12	-3.45%
19/10/2018	7.18E+12	-3.65%
17/11/2018	6.65E+12	-7.39%
04/12/2018	5.65E+12	-15.13%
19/12/2018	5.11E+12	-9.56%
29/01/2019	5.81E+12	-1.18%
11/03/2019	6.07E+12	-0.05%
22/04/2019	6.35E+12	-0.63%
15/06/2019	7.41E+12	-0.67%
24/07/2019	9.01E+12	-0.56%
08/11/2019	1.27E+13	-7.10%

Difficulty dropping is not unknown, but it is concerning, particularly given the parallels to 2018 (which saw the three biggest drops, and with them a complete collapse of price) - as we have talked about, this is the single metric that we are keeping the closest eye on, because it is capable of casting the single biggest shadow of any vaguely predictable event over the market at large for Q4 2019 as a whole.

This clearly redoubles our focus, but we do not believe that the first apocalyptic horseman is here yet, and our view comes from looking at the data across both periods. Remember: hash rate is estimated from the speed at which the network solves a given block, and there can be significant variance on that. You can see this at essentially any time by looking at the chain; here is a randomly-chosen 2-hour streak from Monday:

Height	Hash	Mined	Miner	Size
603287	0..ee2bd1f6758148f1a4b58f6c8c0de52537606ab...	10 minutes	Poolin	769,752 bytes
603286	0..4c08aeb5c24d0e79b0b18c8d9defc291b902d2...	15 minutes	Poolin	1,185,124 bytes
603285	0..b868ec35ea977449e92b8223c5bcca74d1375c...	23 minutes	AntPool	1,216,798 bytes
603284	0..3ab0e332300e4779249e0186ab7413a44aa5ab...	36 minutes	~~Unknown~~	403,181 bytes
603283	0..a16cd1ac861c3c13ec497d9992ba4521d2b7e47...	37 minutes	Bitcoin.com	1,170,807 bytes
603282	0..1ee0868e9c268d996624a724644b663e78edb...	39 minutes	~~Unknown~~	1,211,529 bytes
603281	0..b680e814a2c0e044e15c06968f3cb537ec5456...	53 minutes	ViaBTC	1,184,030 bytes
603280	0..c047353cb5826a5f9b358b5bf4079305e1ccf8...	54 minutes	BTC.TOP	1,247,974 bytes
603279	0..16008a56b1b787cadeaa74df1a49e86fe01b7f51...	1 hour	F2Pool	1,327,009 bytes
603278	0..a26708875e016ce0a345f354260ba22b8054ed...	1 hour	Unknown	1,281,084 bytes
603277	0..1544d453e0e3f22edf87228c2f1b23c37779748...	1 hour	BTC.com	1,236,082 bytes
603276	0..30bd3fc0d4dfe3d0fb1305257c0f0099abc9e8a...	1 hour	AntPool	1,226,070 bytes

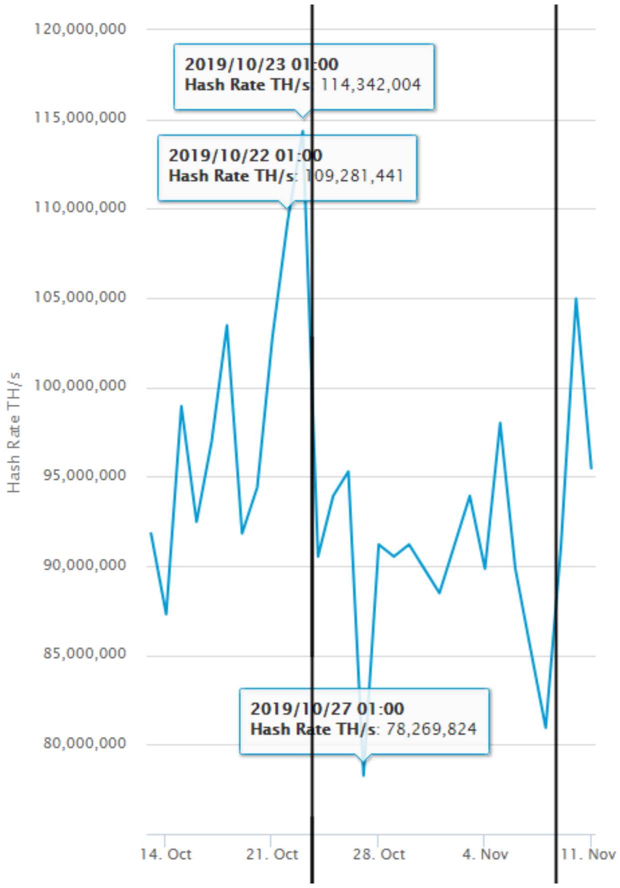
1 hour
4 minutes
1 hour

The expected rate is 12 blocks every 2 hours; the sample delivers on that. Yet, within even this very small sample, we see 4 blocks mined in the former hour, and 8 in the latter; additionally, we see a 4-minute span with 3 solutions (603282, 603283, 603284), to the point that the latter of the three blocks (603284) has a tiny fraction of the usual transaction count/total volume of a 'normal' block:

Block	Txs	TxVol (BTC)
603282	2726	8654
603283	2283	2283
603284	203	196
603285	2685	5131
603286	2624	3854

Data via blockchain.com.

While this all evens out over time, there is enough variance that even data across an entire day (144 blocks) tends to be extremely noisy, which is why we always look at the moving average. However, in this case, the daily data is useful, because it showcases that the magnitude of the adjustment was in part a question of that variance on both ends (with the lines providing an approximation of when difficulty was changed for both periods, and therefore on what periods it was calculated):



Credit: blockchain.com.

The two weeks previous to the most recent period saw a number of days (particularly the 22nd and 23rd of October) that seem more likely to have given aberrantly high readings than anything else, without many steep lows. By contrast, the most recent period saw no real highs, and an aberrant low on the 27th.

It seems likely that there was a small overall decline in hash rate over the 2-week period. However, the 7% headline figure, and the manner in which it invites comparisons to 2018, seems to us to represent an overstatement - going, as it did, from an ATH that may have partially been fueled by a short-term real increase in processing power (as new rigs came online while old rigs enjoyed the last dregs of cheap excess electricity from hydroelectric plants in 2019) to an extreme and non-sustained low followed by period with few 'good' days to boost the overall mean back up.

A continued sustained drop in the next week or two would cause serious concern, particularly with price struggling to break back above $9000, but the evidence is not there for that as of yet. Daily data has hash rate back above 100 XH/s and the 7-day MA has been fairly stable over the last two weeks; it would take a concerted period of significantly lower hash rate estimates to suggest that a 2018-like loss of confidence from (non-retail) miners is coming.

Russia and cryptocurrency: the legal perspective

By Alina Kisilevich

By the end of 2021, The Ministry of Internal Affairs of the Russian Federation together with Rosfinmonitoring, the General Prosecutor's Office, the Investigative Committee, the Ministry of Justice, The Federal Security Service, the Federal Customs Service and the Federal Security Service with the participation of the Supreme Court of the Russian Federation must prepare proposals on seizure of cryptocurrency. This decision is explained by the fact that the growing popularity of virtual assets is also followed by an increase in financial crimes with their use. However, the main problems are its legal difficulties and technical impossibility.

To begin with, having no clear law that would address the status of cryptocurrency within the country, for Russian authorities to be able to seize cryptocurrency it should be first recognized at the legislative level as either a goods or a cash equivalent, which will, legally speaking, mean overall legalization of crypto in the country.

This may be disadvantageous to the Central Bank of the Russian Federation and its money monopoly. However, this is not completely impossible, because from the point of view of international law there are some already existing precedents for the confiscation of cryptocurrency by a court ruling in the absence of regulation of cryptocurrency at the legislative level.

At the international level, it is necessary to develop a definition of the legal status of virtual assets, as well as common standards for defining procedures related to their implementation and seizure. At the same time, an appeal to such a precedent is not very likely for the country because for Russia the building of legislation in the field of cryptocurrency regulation is of particular importance at the moment.

Further, when it comes to the technical difficulties of such proposal, cryptocurrency holders store their virtual assets either in their own virtual wallet or in the cryptocurrency exchange. In case of the exchange, it is more or less clear, theoretically speaking, law enforcement agencies can write an official request to the representative with a request to block the funds of a particular client or, alternatively, transfer them to a special account.

As for the wallet, it is accompanied by the anonymous status of the owner, so the security services first must prove that the specific wallet belongs to this exact person, and then they will need an access to a private digital key, i.e. password, that not only the owners of the wallet themselves know, but more that they do not have any legally binding obligation to disclose such information.

Experts say that legal mechanism of cryptocurrency seizure will not affect neither digital currency market nor its prices. The decision, if implemented fully, will only affect citizens who break the law so they wouldn't be able to conceal digital assets. Such initiative is being considered in the long run which means the situation might shift. One of the possible paths in order to avoid volatility, the state can create its own cryptocurrency exchange and cryptocurrency with a stable exchange rate in order to keep the funds seized.

What we're reading

Coinbase Will Now Reward Users for Holding This Cryptocurrency (Coindesk): We'll save you a click here - it's Tezos (XTZ), which experienced an enormous short-term increase in price on this news, going from $0.94 to a peak over $1.30 over the course of the next day, and has settled back towards $1.19 at the time of writing. Staking and similar mechanisms (e.g. positive interest rates for holding stablecoins) have been and will most likely continue to be a growing trend for exchanges over the last few months, but this is only the second time that we have noticed a major price movement on such an announcement (TRX's Binance staking announcement in September being the first). It is an important trend given several major altcoins - including ETH - are making moves towards a PoS (proof-of-stake) system as a replacement for mining in 2020.

Avalon Bitcoin Miner Maker Canaan Posts $13 Million Q3 Profit in New Filing (Coindesk): General consensus has been positive on this news; we are a little more cautious. Revenue was higher than the previous three quarters combined, but still below Q2 2018. While it is above Q3 2018, if we take the listed change in market share (15.3% in 2018 -> 21.9% in 2019) to be roughly accurate, it would imply in the median a small contraction in the total market in the respective quarters - concerning given that between an exploding hash rate and the sheer proportional increase in power and efficiency of 2019's new products (and the implications for older staple rigs finally being pushed out of the market), we would tend to expect a decent overall increase in sales across the market even being further removed from the warmth of the 2017 boom. We are at this point extremely worried about what the details of the Bitmain IPO may show when published..

Chinese Police Hold MicroBT CEO Allegedly Over Dispute With Bitmain (Cointelegraph): Speaking of Bitmain...Zuoxing Yang was the designer of the original Antminer models that still hold a massive share of the mining markets. MicroBT have reportedly cut into Bitmain's market share of new products significantly over the last year or so; it seems likely that this was the culmination of some movement behind the scenes. Implications going forward are hard to say as of yet, but it's clear that Bitmain will not be allowing themselves to go down quietly if that possibility was on the agenda

Bakkt Bitcoin Futures Daily Trading Volume Hits New Record - $15M (Cointelegraph): The important part of this swell is that while the headline ATH happened on (downwards) price movement), volumes were up this week on last in a climate of very low volatility overall; it bodes well for the future of Bakkt products, with a possibility (albeit still very small) that the market might make it to the Bakkt options launch on December 9th with said event actually underpriced rather than neutral (our current expectation) or overpriced (as it was for the first Bakkt launch in September). We additionally note that on the same day as their record trading, Bakkt also announced it had gotten the go-ahead to start extending their custody solutions to marquee cryptocurrency firms.

XRP/USD price in shambles: The not so Swell Ripple conference (FXStreet): Speaking of Swell, as far as we can see, this was the big chance for XRP to finally break above $0.30 medium-term, a level that it has stubbornly stuck at since August, even after the China rally a couple of weeks ago brought essentially all of his compatriots higher. It did briefly do so, but never threatened any higher than $0.31, and quickly fell back to $0.27 at the time of writing. Our view on XRP long-term gets more bearish by the day, and short-term we are concerned that, even given how little XRP has moved upwards recently (which would seem to point to it as a candidate for a correction), the current range of $0.26-$0.29 may still be unsustainably high.

China's State-Run Media: Bitcoin Is Blockchain's First Success (Cointelegraph): The actual article is fairly negative on Bitcoin, regurgitating most of the classic Western media critiques (waste of energy, black market transactions, volatility, and so on), but a Xinhua mention is always worth noting. Some 'Chinacoins' appear to have moved upwards significantly in the day following the news (most notably NEO and ONT), but the rule remains: news from China is generally overhyped and rarely ends up significantly moving Western markets. The notion that the Xi Jinping announcement was an exception rather than a rule-changer has so far largely played out.

Until next week – thank you for reading.

ENIGMA SECURITIES

http://www.Enigma-Securities.io

Owned by Makor

New York
Park Avenue, 6th Floor 430

London
Gossard House 7/8 Savile Row

Paris
Rue Saint-Honoré 336

Tel Aviv
Menachem Begin 11 Ramat Gan

Singapore
Robinson Road 160

Geneva
Rue De La Croix-D'Or 27

Gibraltar
,World Trade Center, 6 Bayside Road