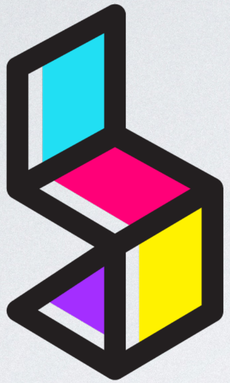


SOME STATISTICS ON BITCOIN VS. BITCOIN CASH

by Nikita Zhavoronkov <nikzh@nikzh.com>

March 24th, 2018

Tokyo, Japan

TECHNICAL DIFFERENCES

			Results in…
Block size limit	1 MB (4 MWU)	32 MB (8 MB soft limit)	Transaction throughput is larger for Bitcoin Cash, different use cases
Difficulty adjustment	Once in 2016 blocks	Each block	Different security models and emission curves
Segregated Witness support	Yes	No	Malleability fix for Bitcoin

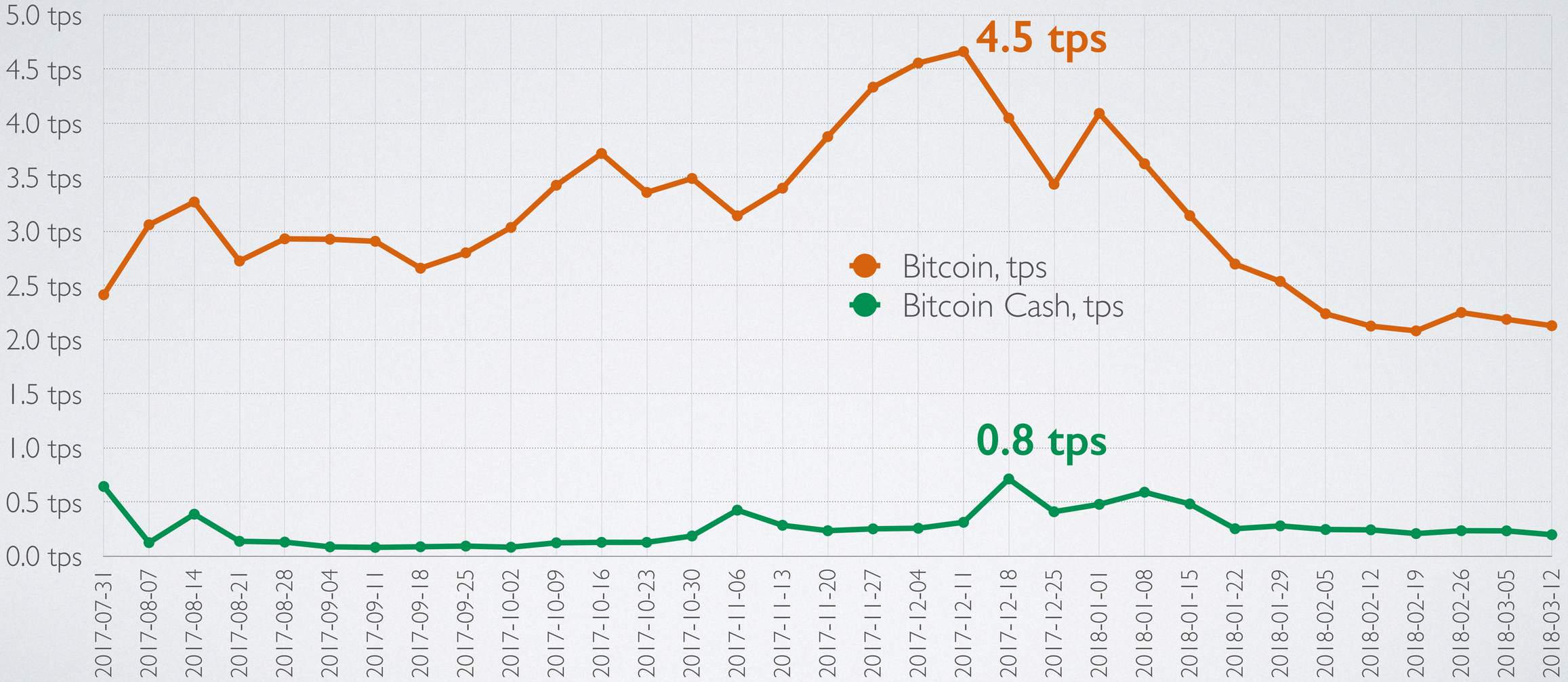
TRANSACTION THROUGHPUT

- The average input count for transactions with 2 outputs (the most common option for ordinary users) is 2 — that is 386 bytes of data;
- That means 1 MB of block data can include only 2.600 transactions;
- Given that blocks are issued once in 10 minutes, 1 MB limits us to 4.33 transactions per second.

TRANSACTION THROUGHPUT

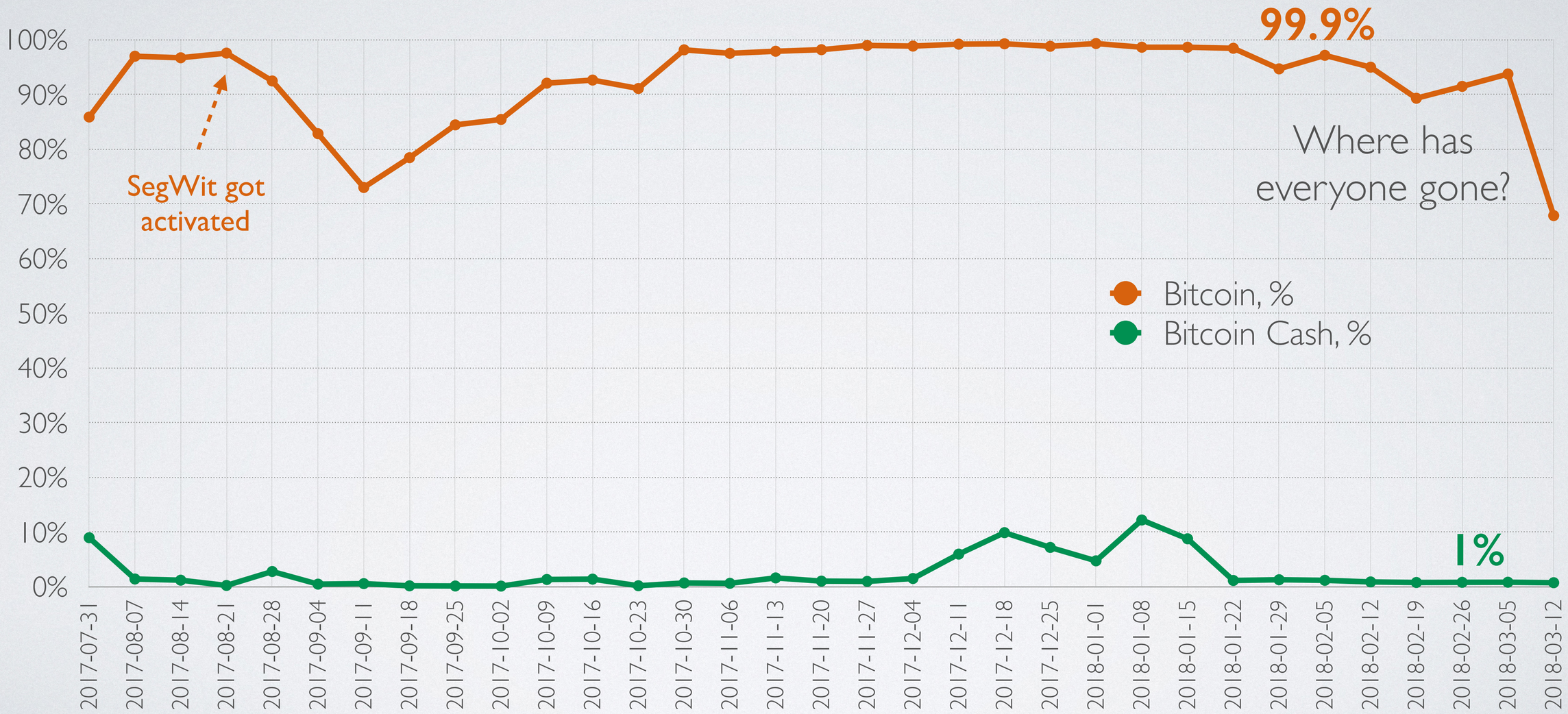
	Throughput	**Required storage**
1 MB blocks	4⅓ tps	144 MB per day
8 MB blocks	34⅔ tps	1.1 GB per day
32 MB blocks	138⅔ tps	4.6 GB per day
VISA	24.000 tps (peak)	N/A
5.5 GB blocks	24.000 tps	792 GB per day

PRACTICAL THROUGHPUT



2017-08 **2018-03**

BLOCKCHAIN SATURATION



2017-08 **2018-03**

TRANSACTION THROUGHPUT

Two remarks:

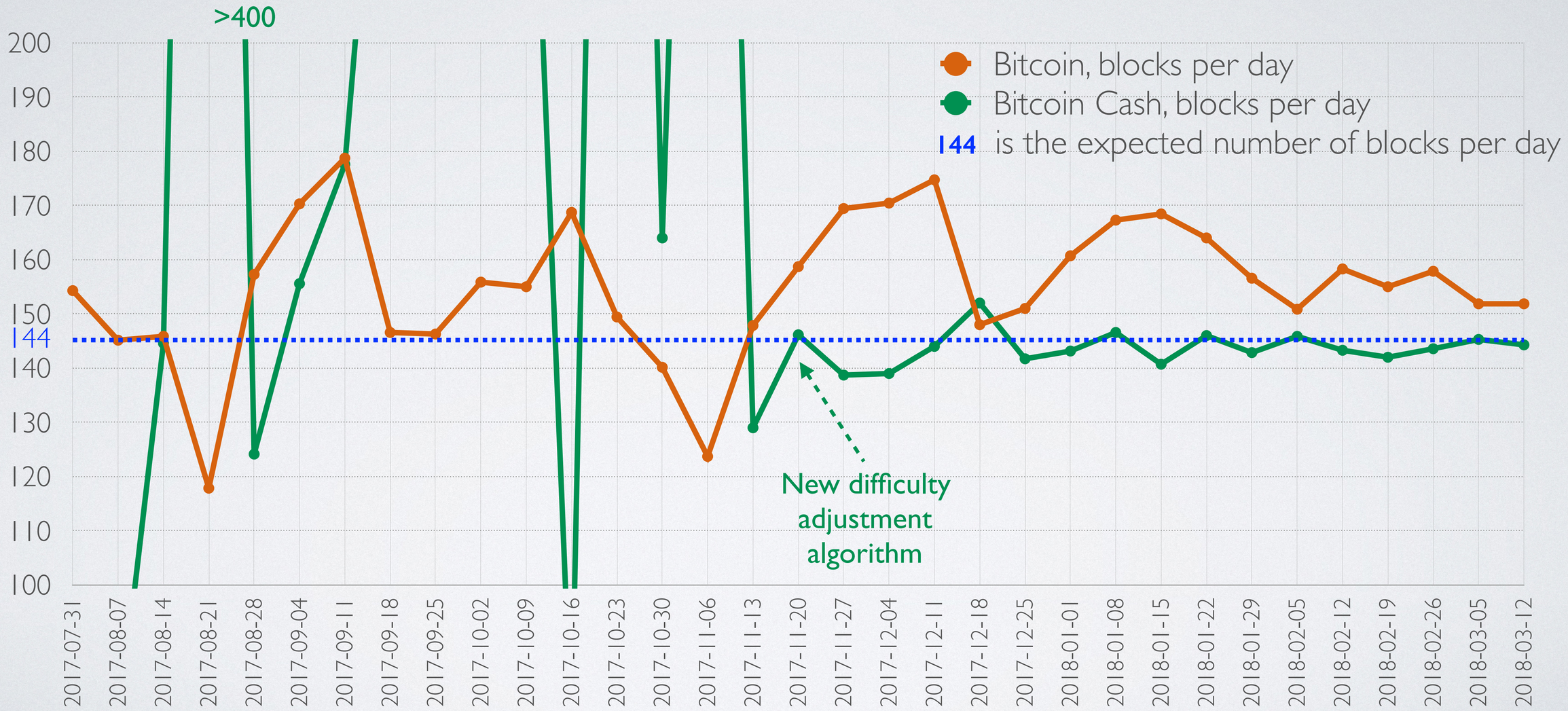
- Difficulty adjustment algorithm affects the average time between blocks, thus the throughput;
- SegWit replaced 1 MB block size limit with 4 MWU (weight unit) block weight limit.

BITCOIN ENJOYS ADDITIONAL SPACE

- Because the hashrate in Bitcoin is constantly increasing, and the difficulty readjusts only once in 2016 blocks (~2 weeks), Bitcoin miners find blocks more frequently than the target 10 minutes;

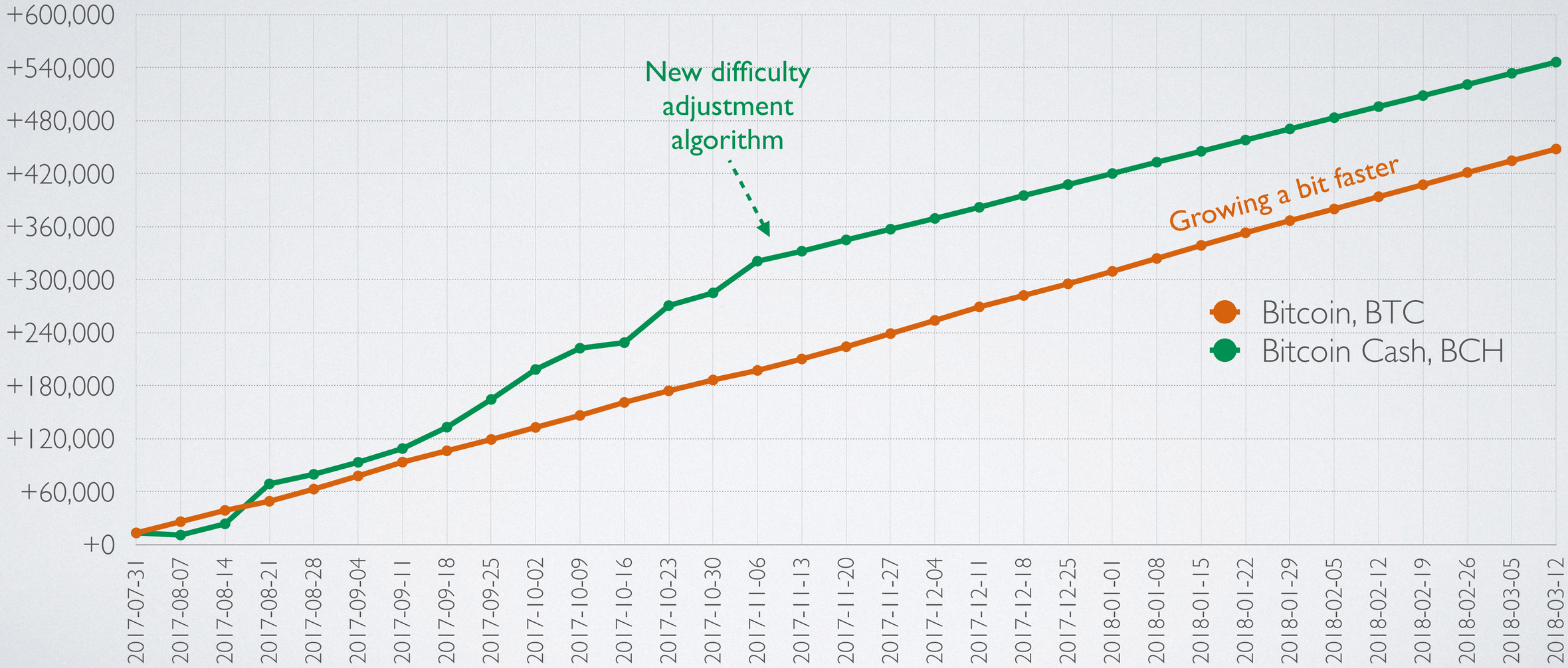
- That leads to the fact that the 'real' tps limit is ~20% more than theoretical. So far the Bitcoin blockchain has been increasing not for 1 MB each 10 minutes, but for 1.2 MB.

BLOCK COUNT



2017-08 **2018-03**

EMISSION CURVE

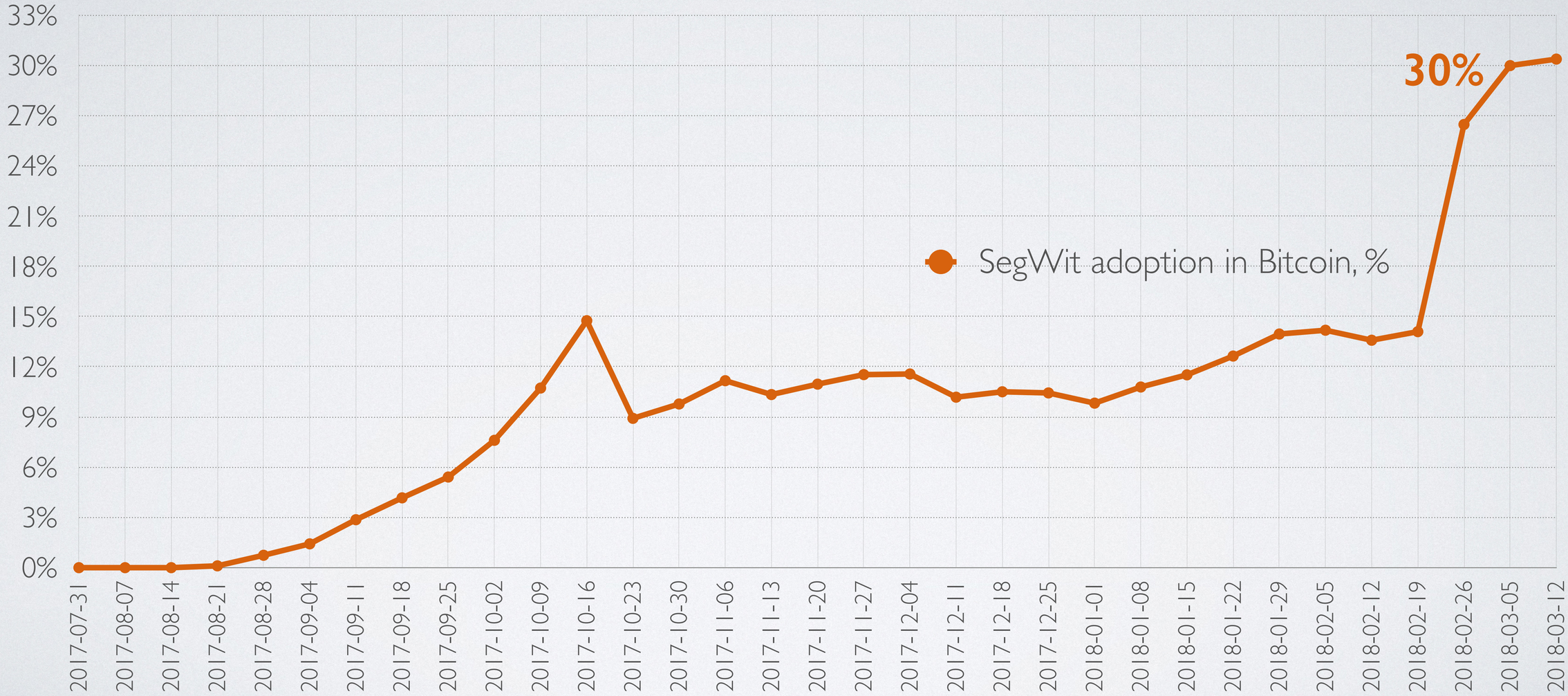


2017-08 **2018-03**

BITCOIN ENJOYS ADDITIONAL SPACE

- But there is a reverse side to the coin…
- Hashrate may decrease (e.g. due to a huge price drop), leading to the decrease of throughput;
- Plausible scenario is a downwards spiral: price drops — hashrate drops — throughput decreases until the next readjustment in 2 weeks — fees skyrocket — markets panic (“my transaction to the exchange is stuck, they’re robbing me!”) — price drops even more — …

SEGREGATED WITNESS USAGE



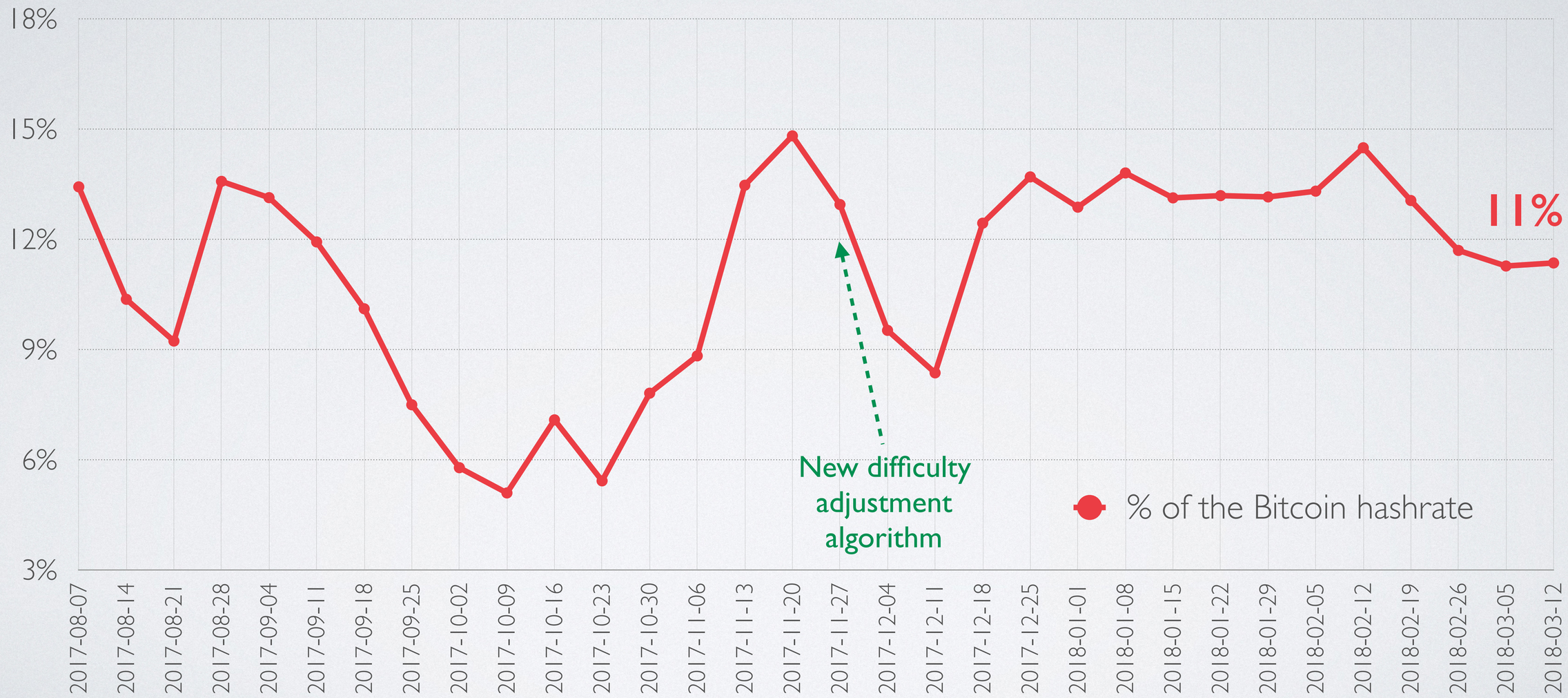
2017-08

2018-03

LET'S GET BACK TO DIFFICULTY

- Ok, everyone knows that Bitcoin's hashrate is much higher than that of Bitcoin Cash;
- That leaves Bitcoin Cash open to a hypothetical 51% attack from Bitcoin miners. Let's see what % of the current Bitcoin miners is needed to attack Bitcoin Cash.

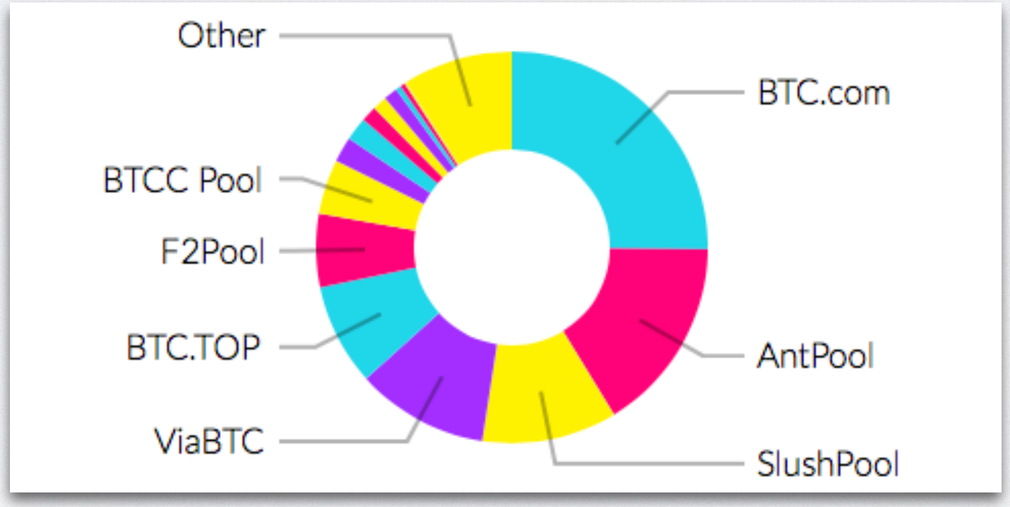
% OF BITCOIN MINERS NEEDED TO 51%-ATTACK BITCOIN CASH



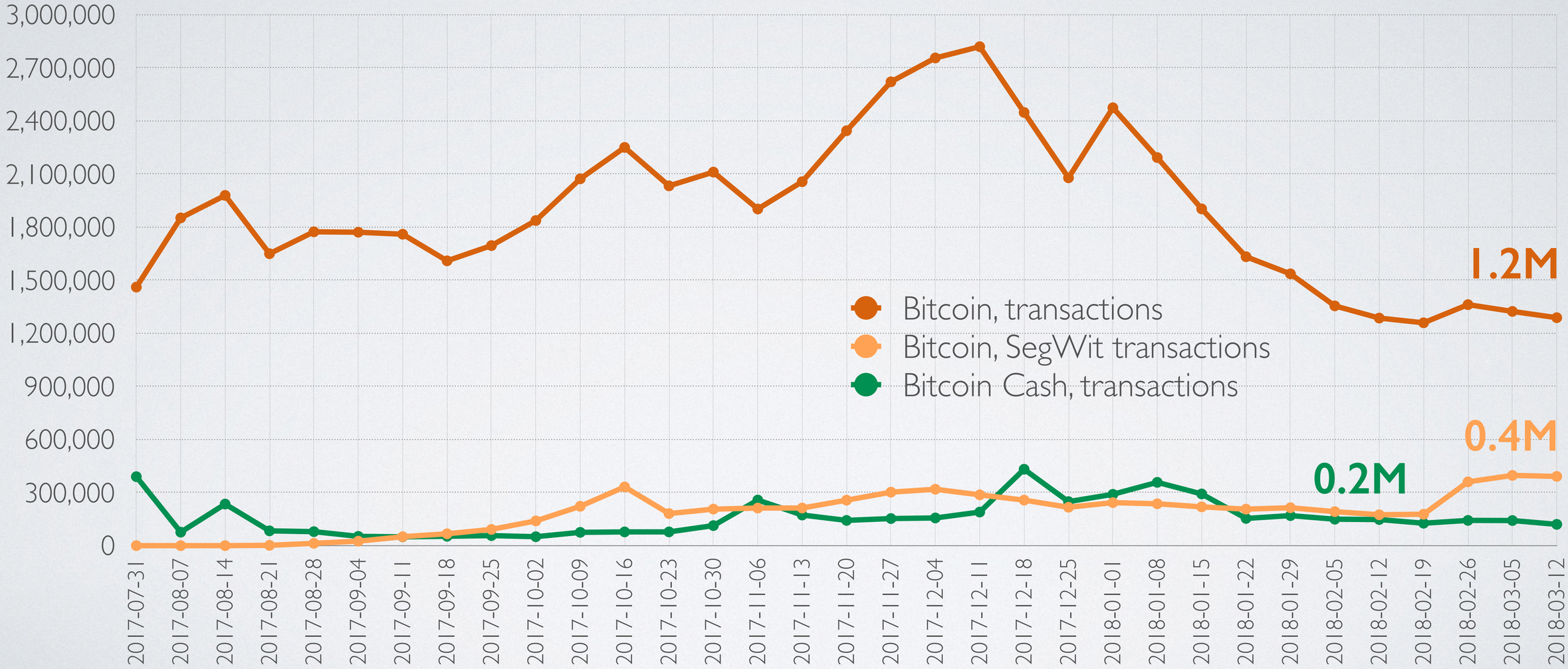
2017-08 **2018-03**

% OF BITCOIN MINERS NEEDED TO 51%-ATTACK BITCOIN CASH

- 4 Bitcoin mining pools have at least 11% of the entire hashrate each: BTC.com (25%), AntPool (16%), SlushPool (12%), ViaBTC (11%)

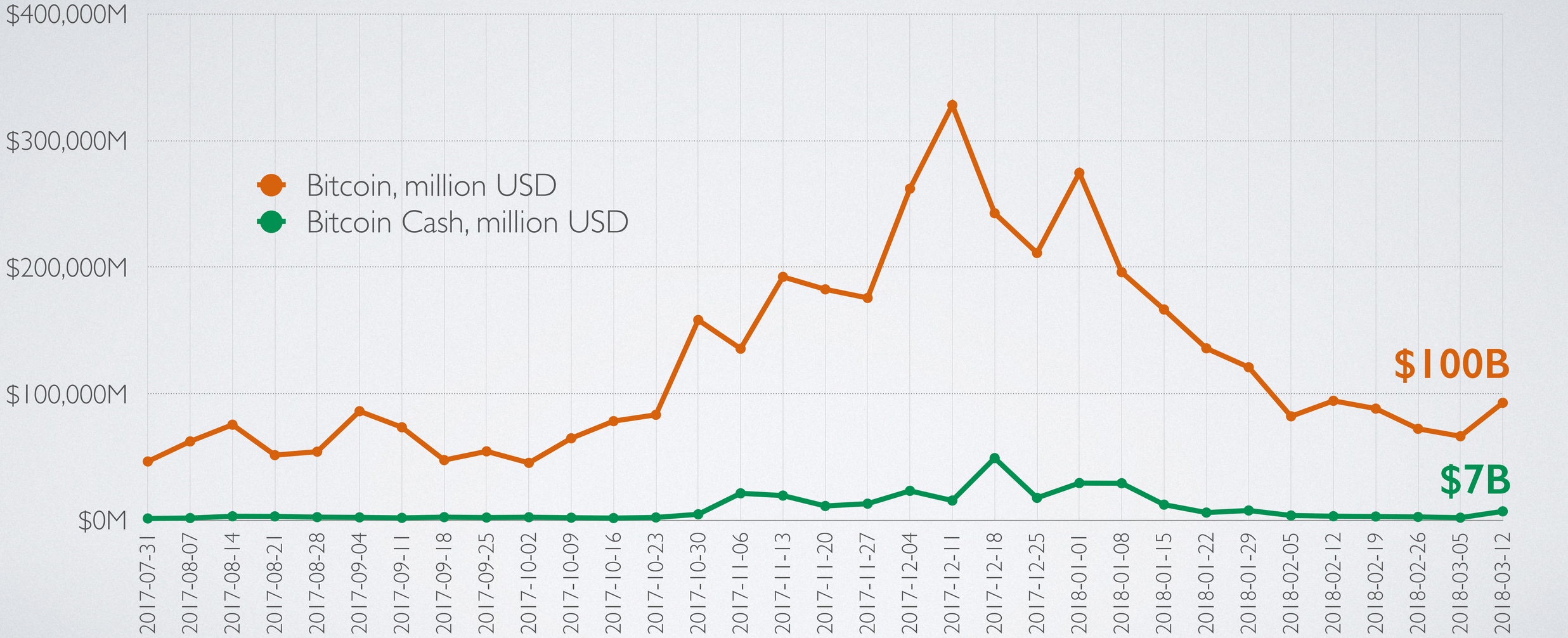


NUMBER OF TRANSACTIONS



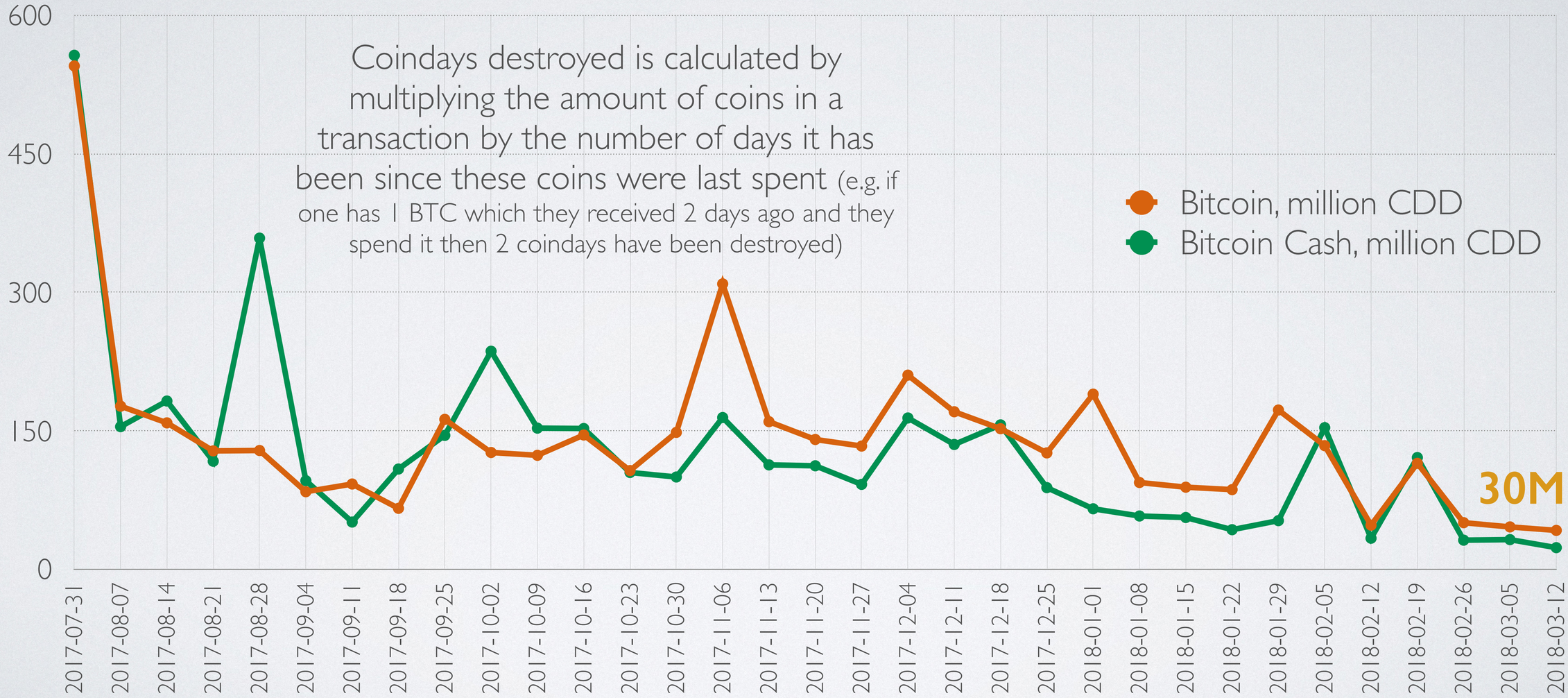
2017-08 **2018-03**

MONEY TURNOVER



2017-08 **2018-03**

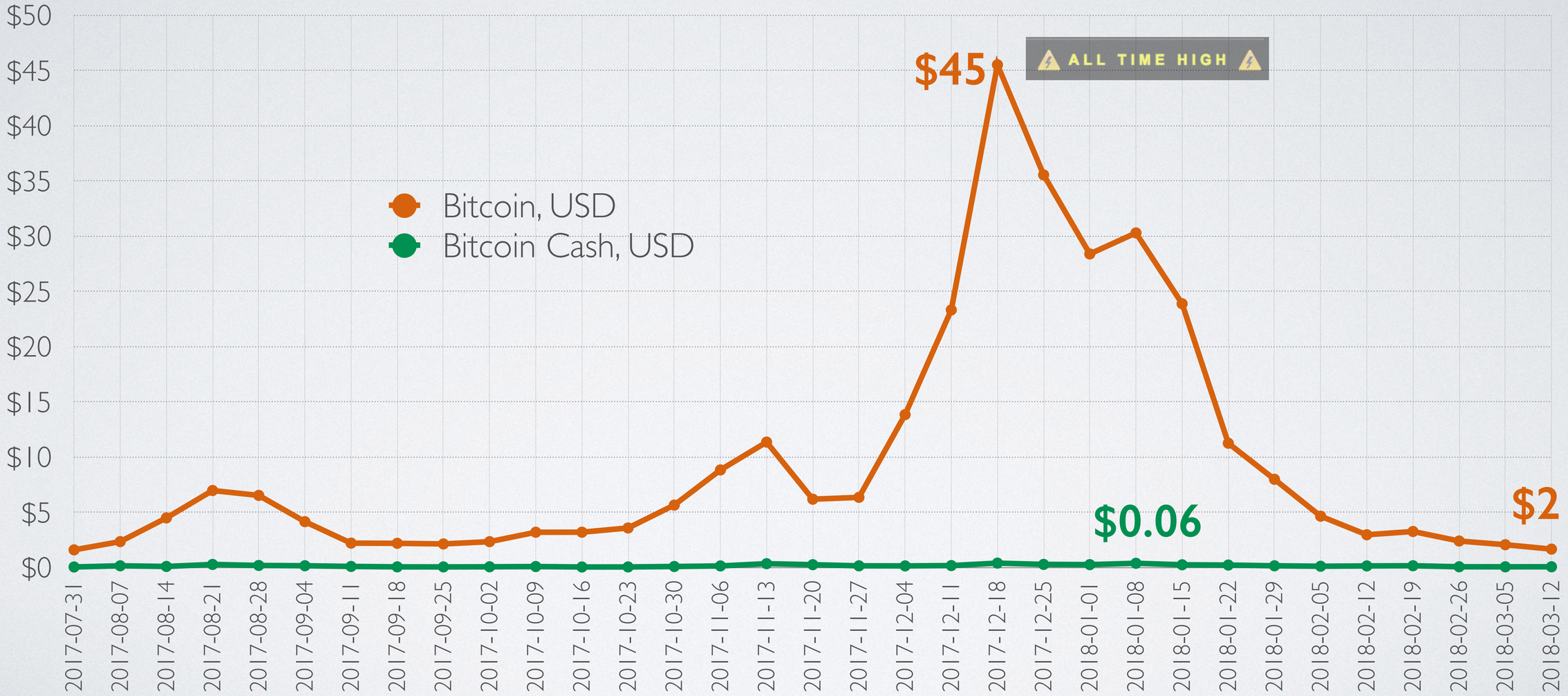
COINDAYS DESTROYED



2017-08

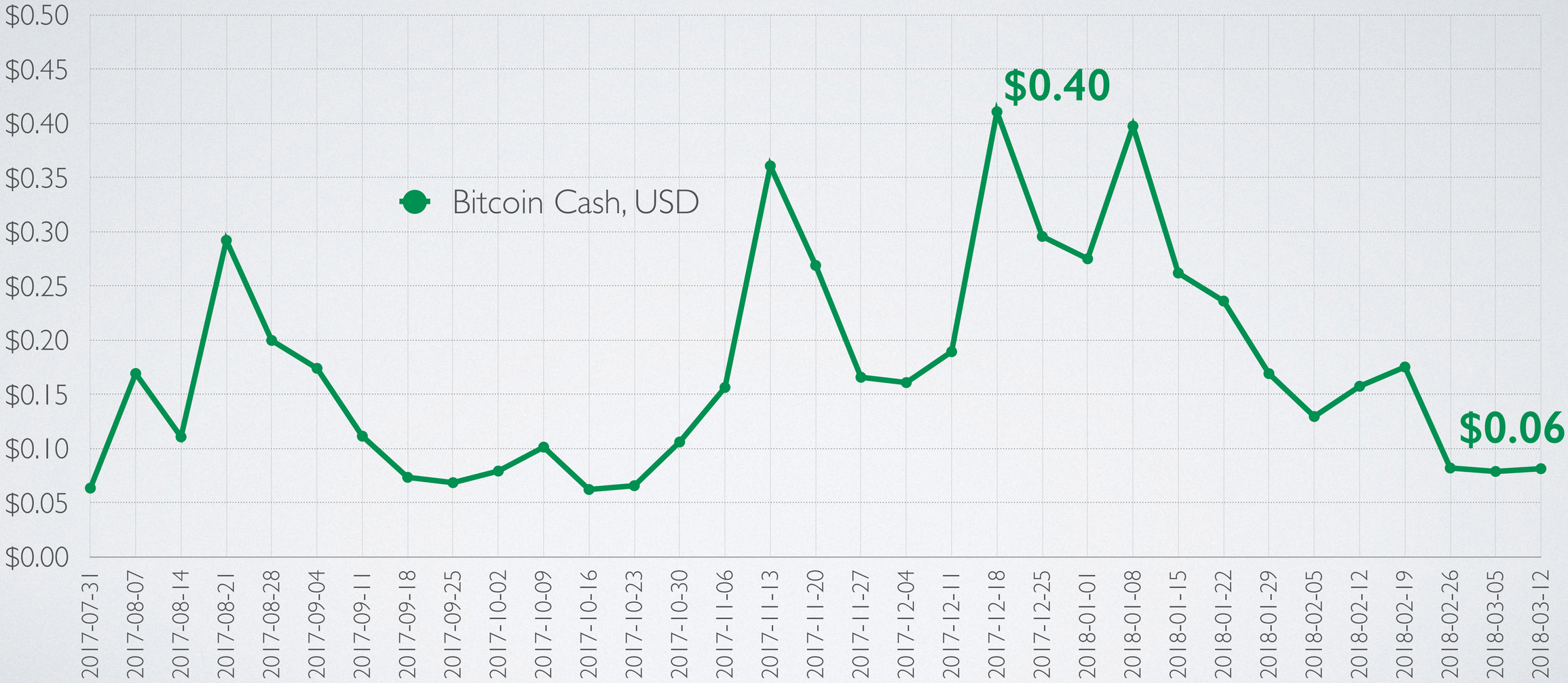
2018-03

AVERAGE FEES



2017-08 **2018-03**

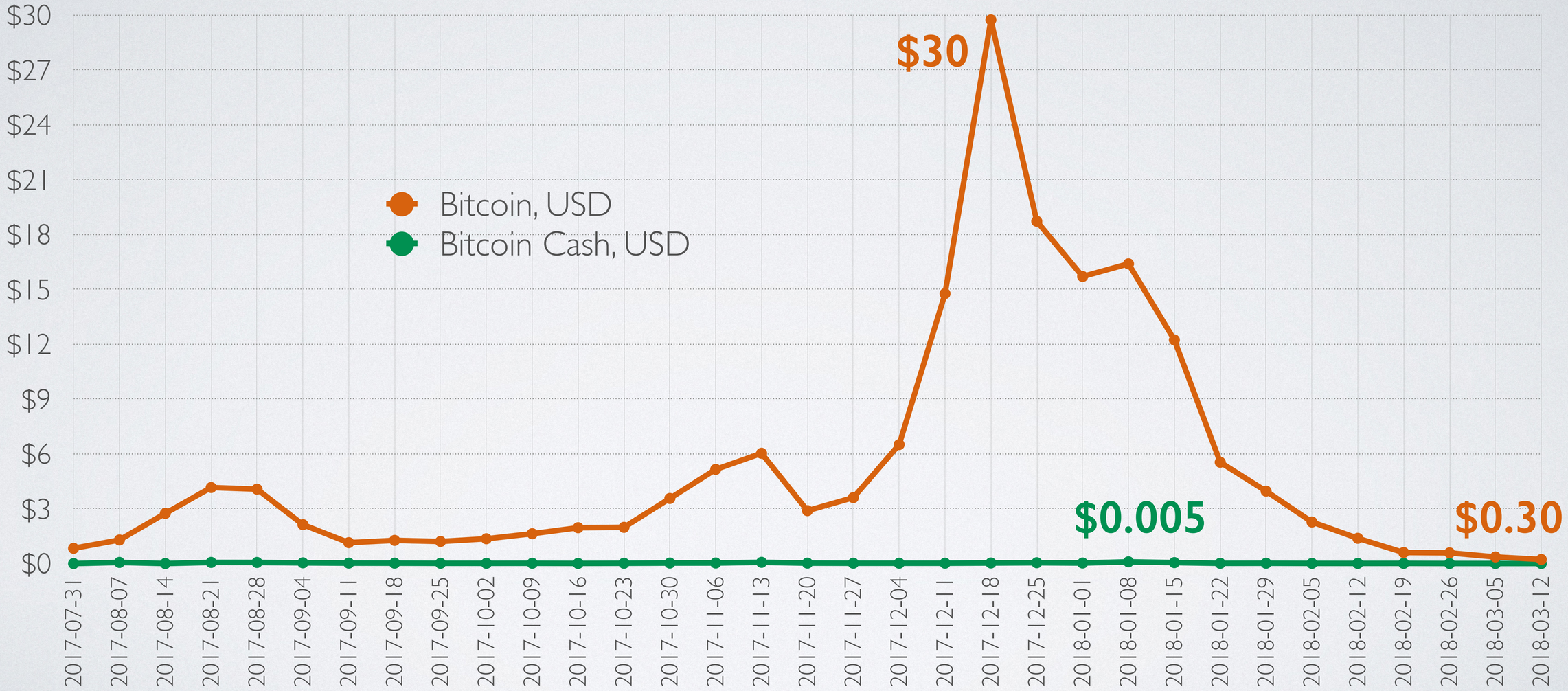
AVERAGE FEES



2017-08

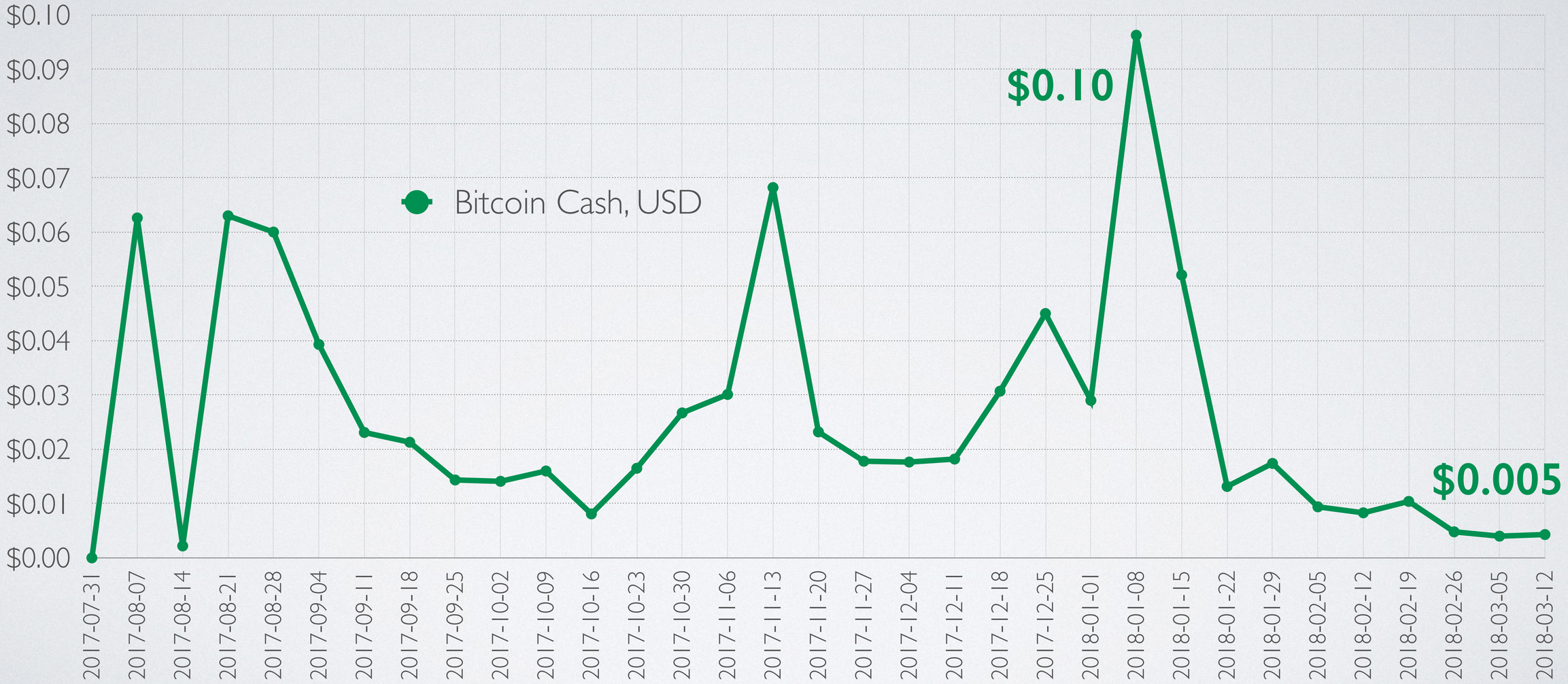
2018-03

MEDIAN FEES



2017-08 **2018-03**

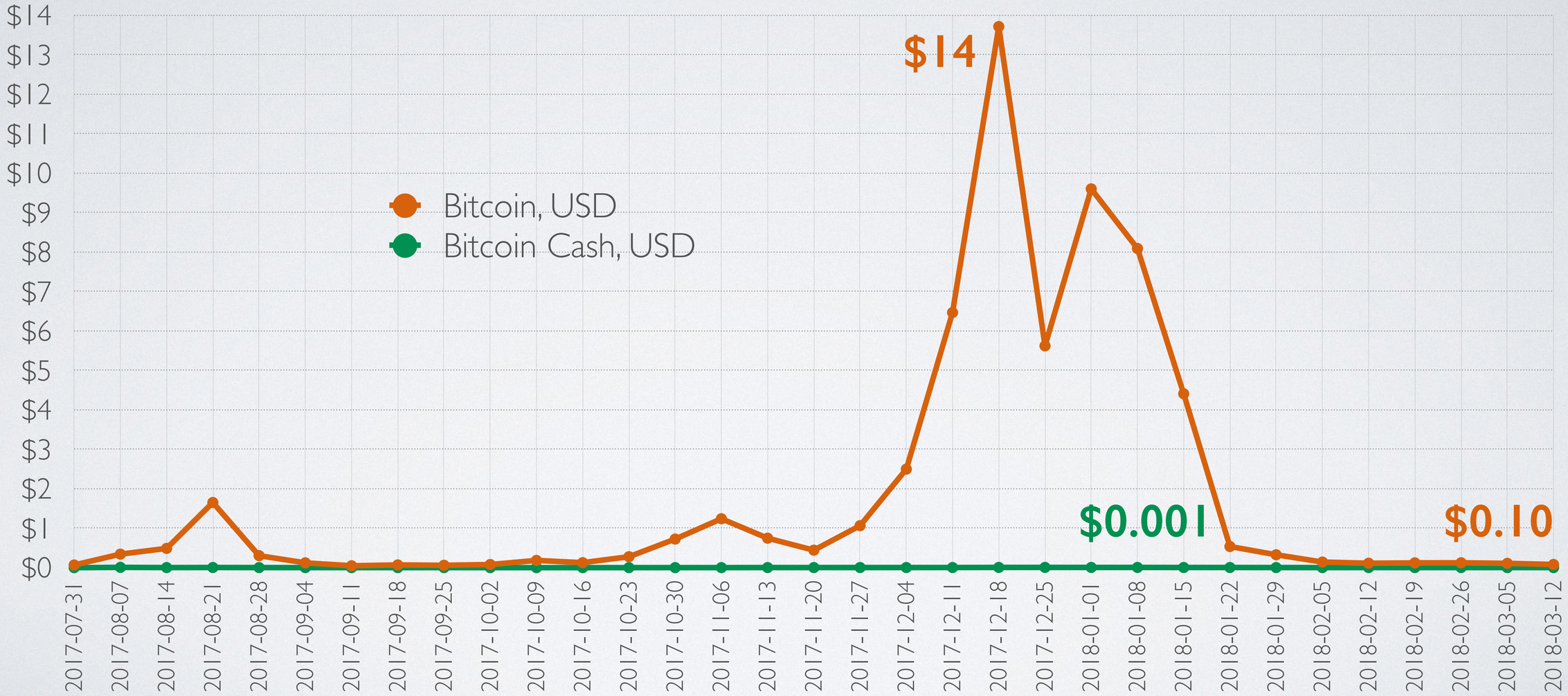
MEDIAN FEES



2017-08

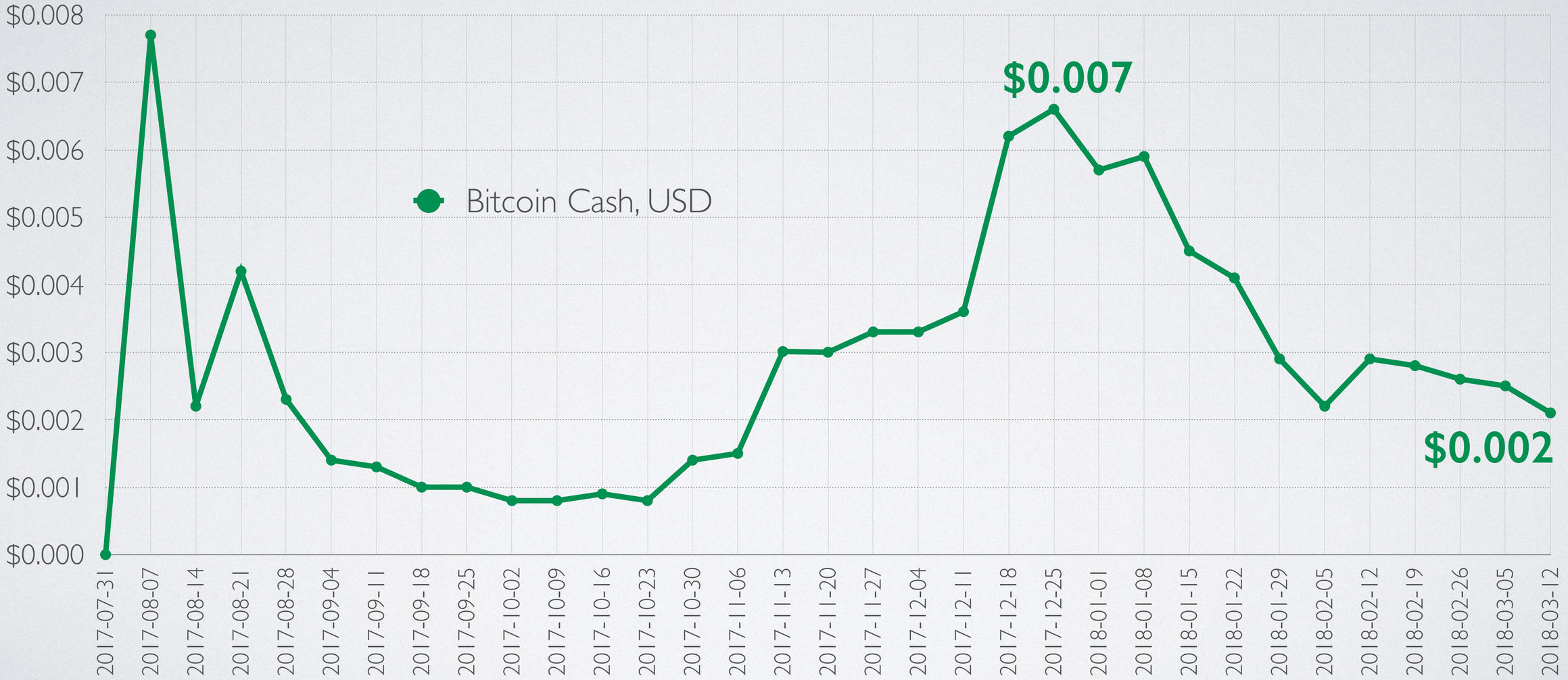
2018-03

10TH PERCENTILE FEES



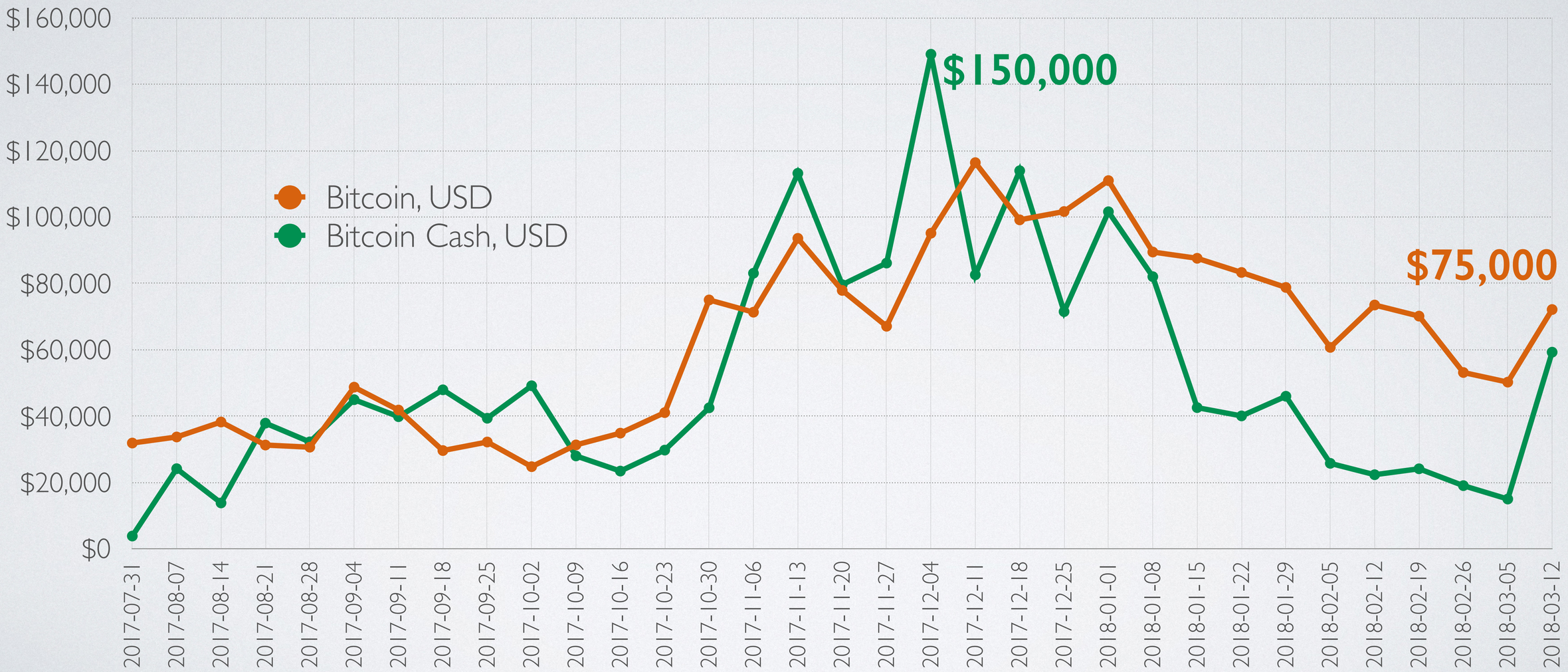
2017-08 **2018-03**

10TH PERCENTILE FEES



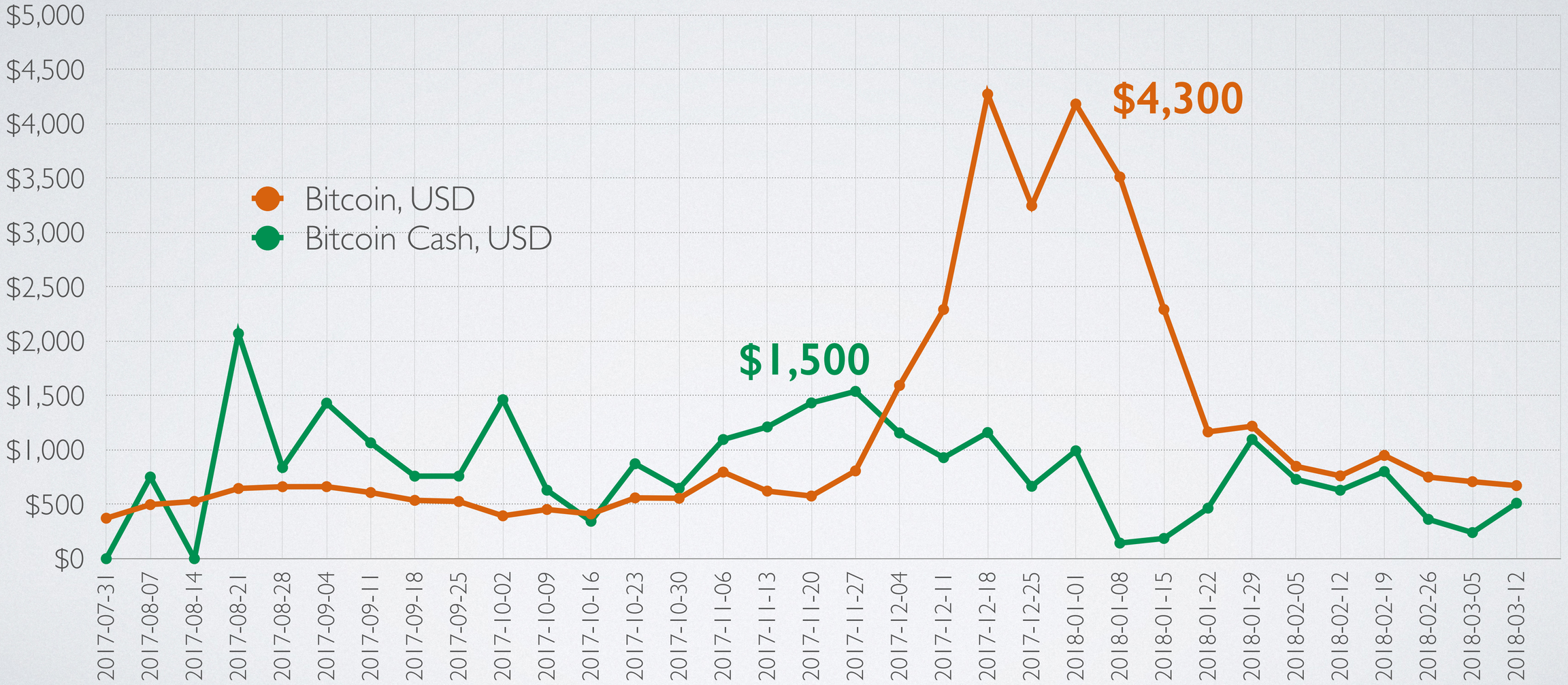
2017-08 **2018-03**

AVERAGE TRANSACTION AMOUNT



2017-08 **2018-03**

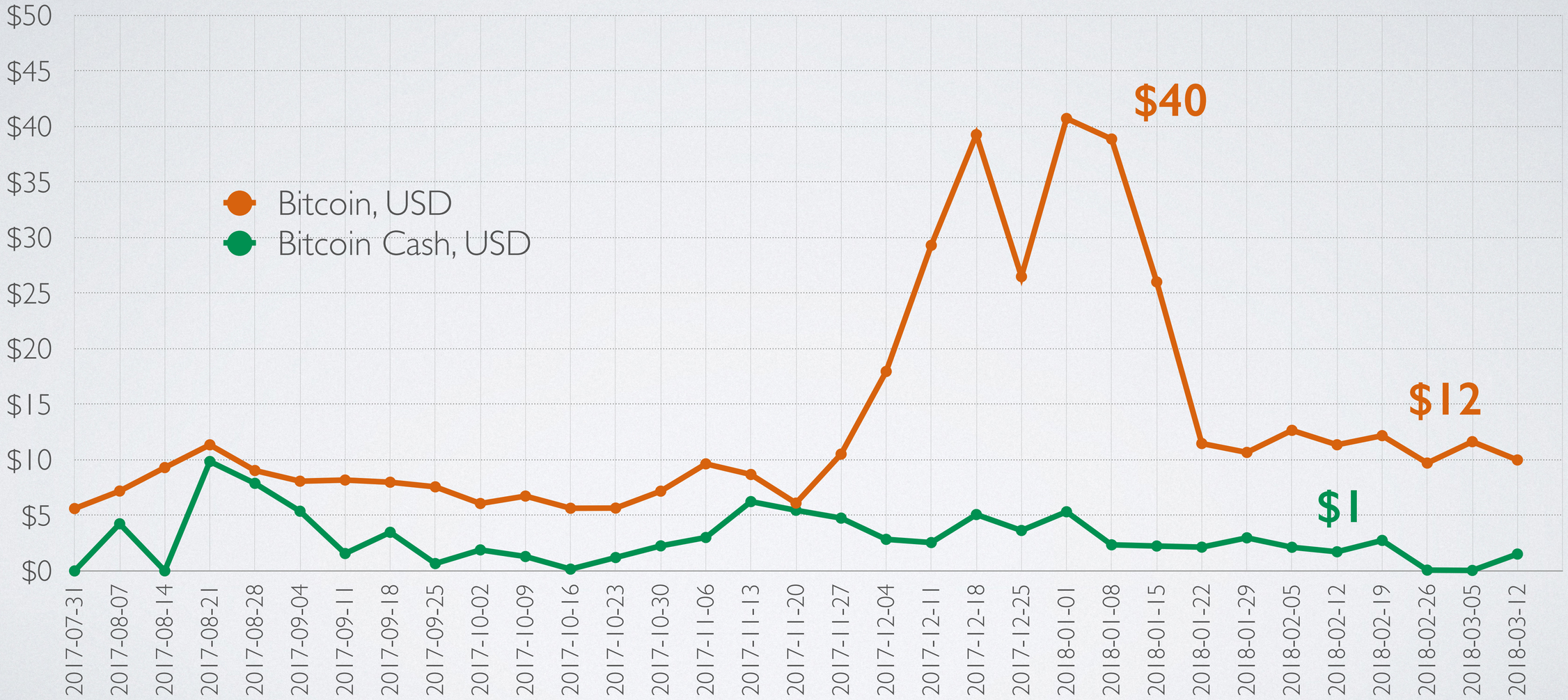
MEDIAN TRANSACTION AMOUNT



2017-08

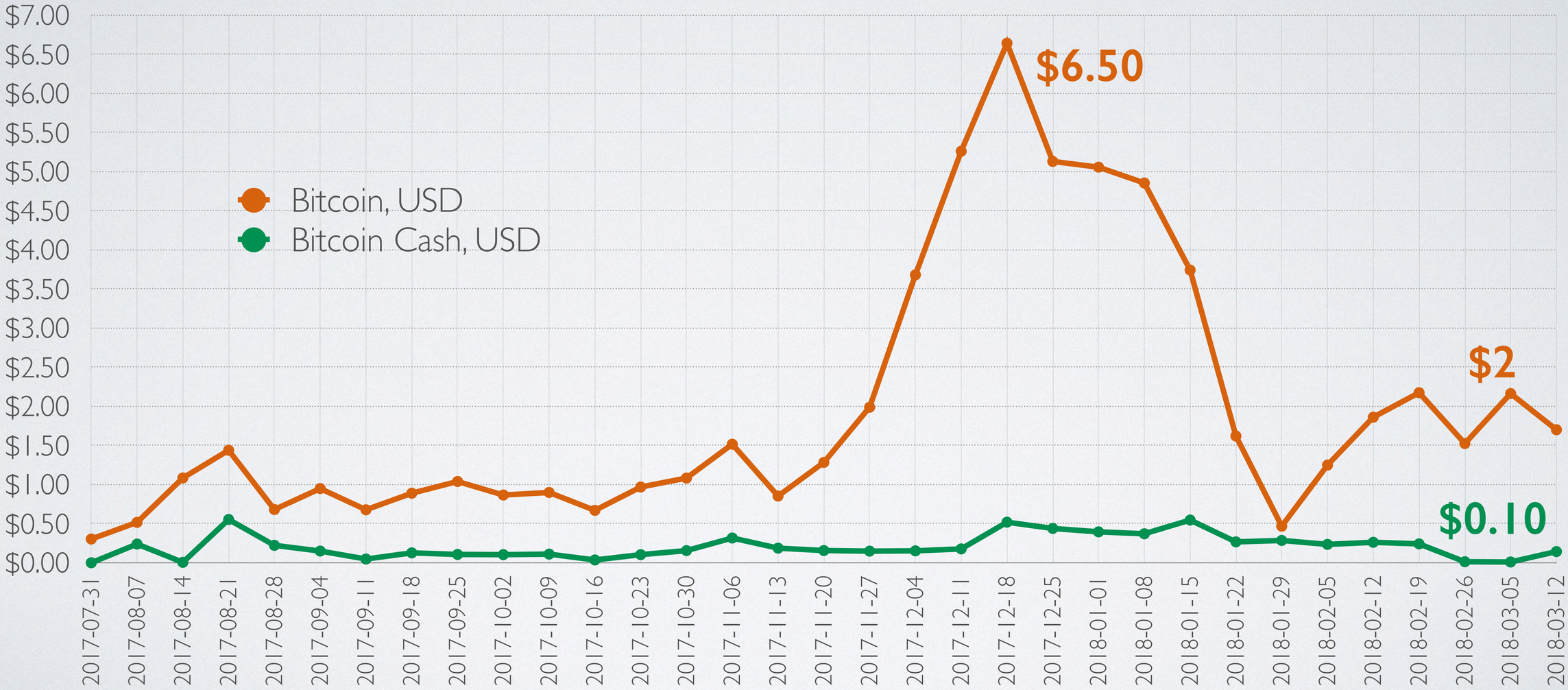
2018-03

10TH PERCENTILE TRANSACTION AMOUNT



2017-08 **2018-03**

1ST PERCENTILE TRANSACTION AMOUNT



2017-08 **2018-03**

THANKS FOR YOUR ATTENTION

- Nikita Zhavoronkov:
  - nikzh@nikzh.com
  - twitter.com/nikzh
- BLOCKCHAIR
  - https://blockchair.com/
  - twitter.com/blockchair

Special thanks to my friends Yedige Davletgaliyev <yedige@blockchair.com>
and Alexandra Ivanisenko <alexandra@blockchair.com> who helped me with this presentation!