WHY BITCOIN NEEDS A SCALING SOLUTION

June 30th, 2017

by Nikita Zhavoronkov <nikzh@nikzh.com>

EXPLAIN LIKE I'M FIVE

- There's a bus coming to a bus stop every 10 minutes
- Each bus is capable to carry 10 passengers
- There are 11 people at the bus stop and new people are constantly arriving

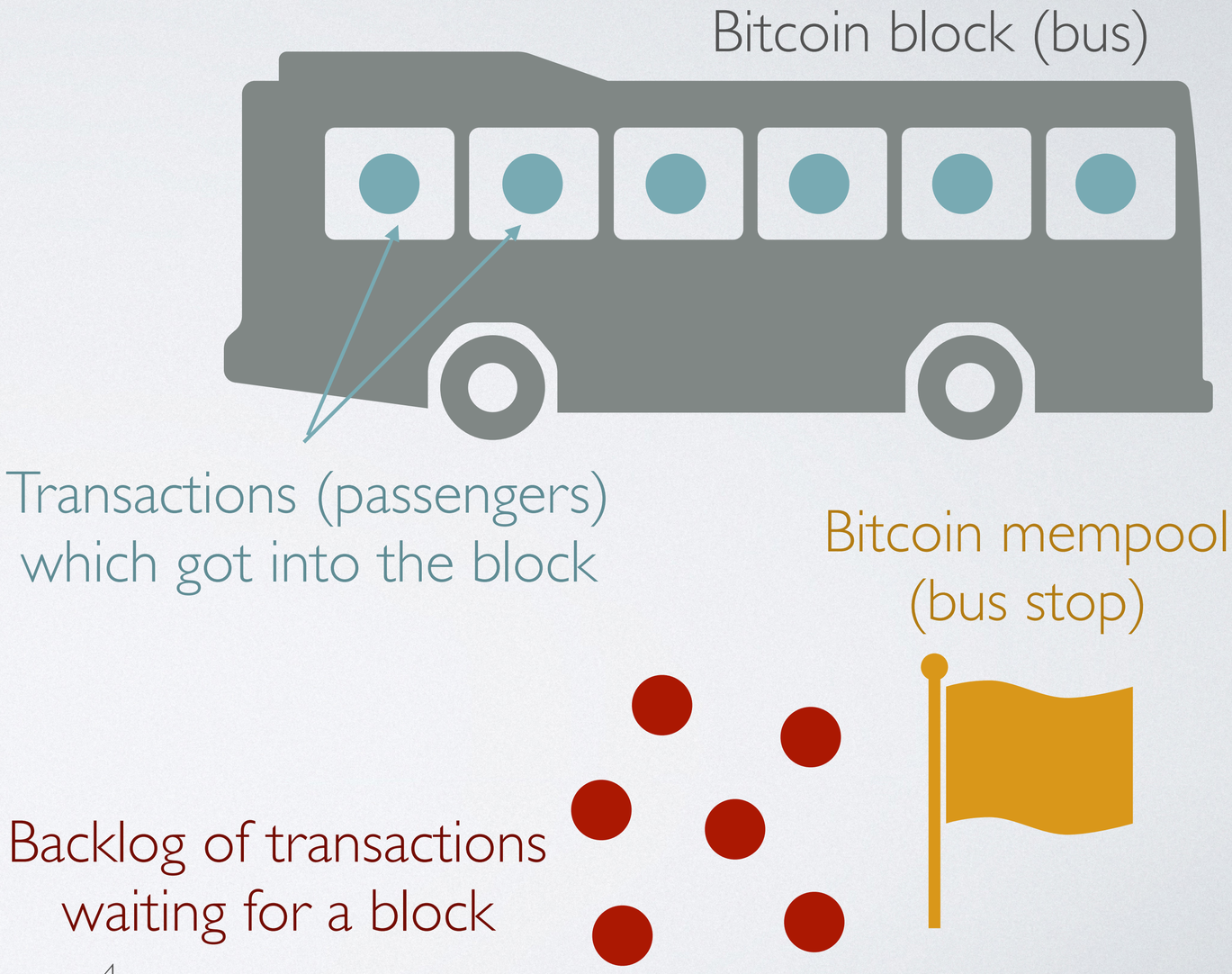
Image: https://www.collegetimes.com/life/people-love-hate-bus-78960

EXPLAIN LIKE I'M FIVE

- So the demand is 11 people / 10 minutes
- And the supply is just 10 people / 10 minutes
- In order to get into a bus people will have to start to outbid each other until someone gives up

B IS FOR BITCOIN, NOT BUS!

- Bitcoin blocks arrive each 10 minutes in average
- Bitcoin blocks are limited to 1 megabyte
- The demand for on-chain space is much higher!



BITCOIN BLOCKCHAIN'S CAPACITY

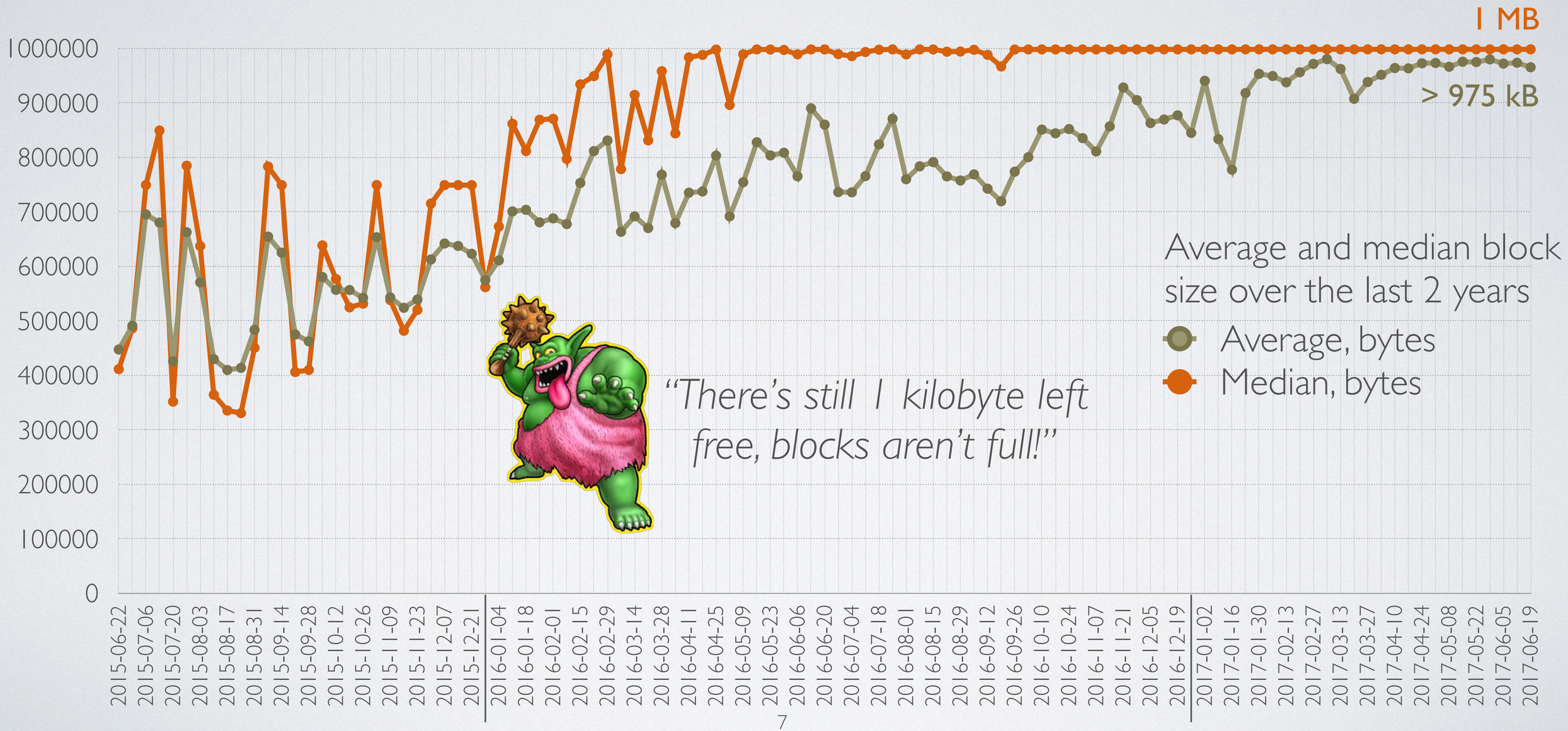
- Average transaction size is ~500 bytes
- 1.000.000 bytes / 500 bytes = 2.000 transactions per block
- 2.000 transactions / 10 minutes = **3.33 transactions per second**

IN COMPARISON

	Current average	Maximum
Bitcoin	3.33 tps	3.33 tps
PayPal	200 tps	500 tps
VISA	1,700 tps	56,000 tps

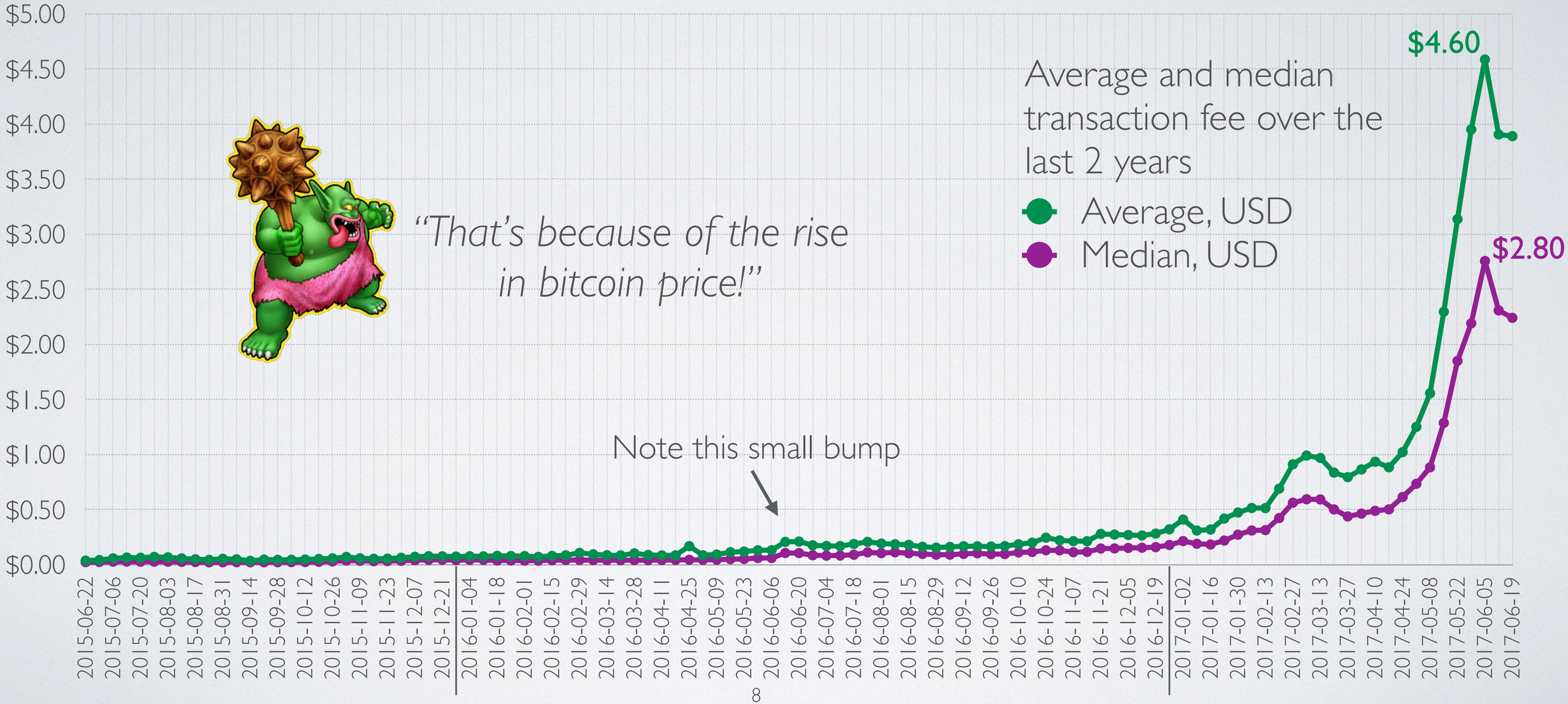
Black Fridays and Cyber Mondays require increased throughput

IS THIS CAPACITY LIMIT HIT?

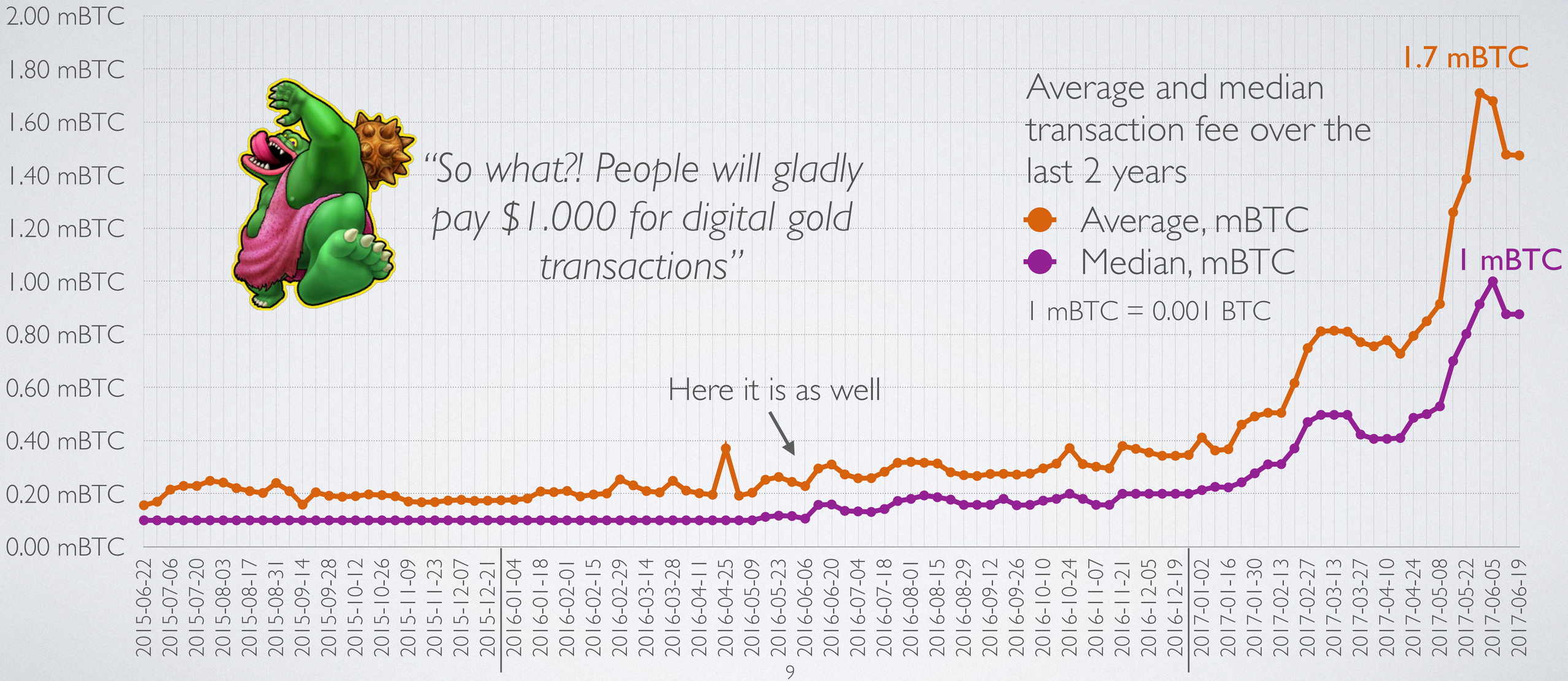


"There's still 1 kilobyte left free, blocks aren't full!"

HOW MUCH PEOPLE ARE WILLING TO PAY?



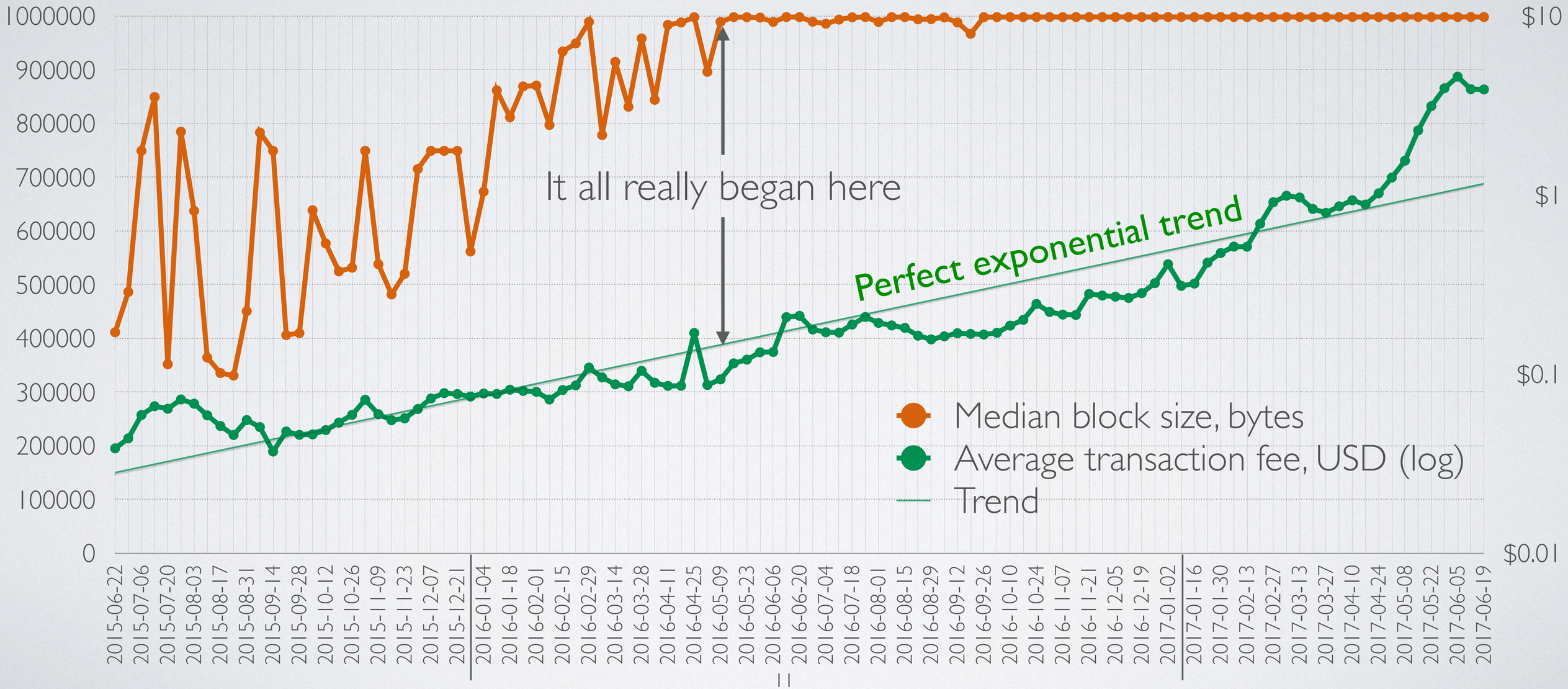
HOW MUCH PEOPLE ARE WILLING TO PAY?



HOW ABOUT A FORECAST?

- Have you noticed that small bump? Why did it happen?
- Let's superimpose the block size and the fee charts and put the fees on a log scale

EXPONENTIAL GROWTH OF FEES

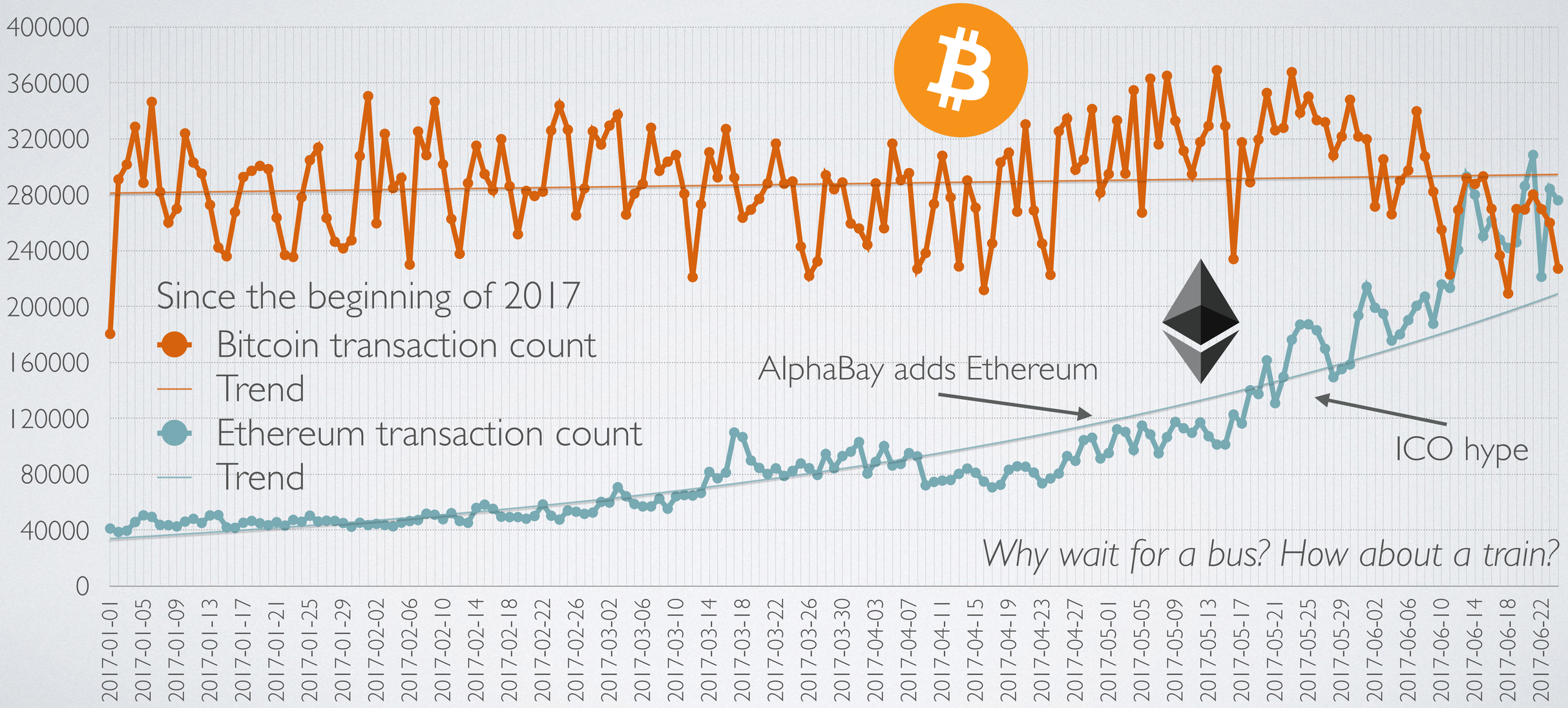


THE FORECAST IS OVERCAST

- 2015 average fee: $0.02
- 2016 average fee: $0.20
- 2017 average fee: $2.00
- Guess what happens next?

No, it's not $20 in 2018, it's called "there's a competition in the cryptocurrency market". Also Snape kills Dumbledore.

BITCOIN VS. ETHEREUM DAILY TX COUNT



BITCOIN VS. ETHEREUM MARKET CAP

LET'S GET BACK TO THE TOPIC

Why Bitcoin needs a scaling solution?

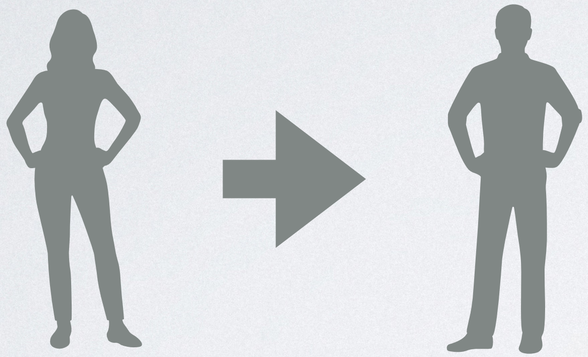
- Most importantly — in order to survive competition
- But wait a second! The question we're asking is wrong. Bitcoin doesn't need ***a*** scaling solution, it needs multiple scaling solutions!

WHAT MULTIPLE SCALING SOLUTIONS?

- An on-chain scaling solution (i.e. increasing the block size limit)
- An off-chain scaling solution (i.e. second layer solutions)
- Neither alone is sufficient for the Future of Bitcoin to be bright

WHAT MULTIPLE SCALING SOLUTIONS?

On-chain



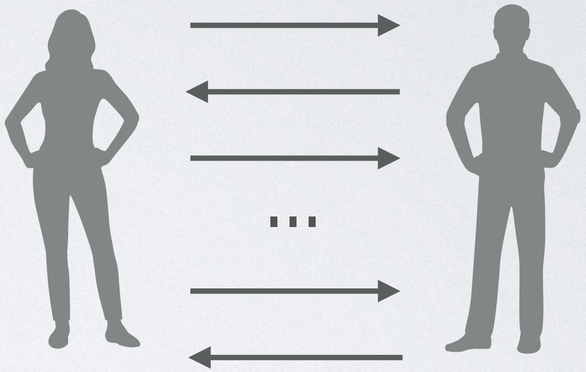
Alice pays Bob 1,000 bitcoins

or

Alice tranfers some property to Bob

The result: 1 on-chain transaction

Off-chain



Alice opens a channel with Bob for micropayments (e.g. she pays 0.000001 bitcoin for every minute Bob consults her via Skype)

The result: 2 on-chain transactions (opening and closing a channel) + ∞ number of off-chain transactions

WHY ฿ NEEDS AN ON-CHAIN SOLUTION?

- Off-chain solutions (like Lightning networks) mostly scale many transactions of one user, they don't scale users themselves
- Users have to open and close channels for off-chain transactions on-chain. The less on-chain space there is, the less channels they will have, thus the more centralized such system will be

WHY ฿ NEEDS AN ON-CHAIN SOLUTION?

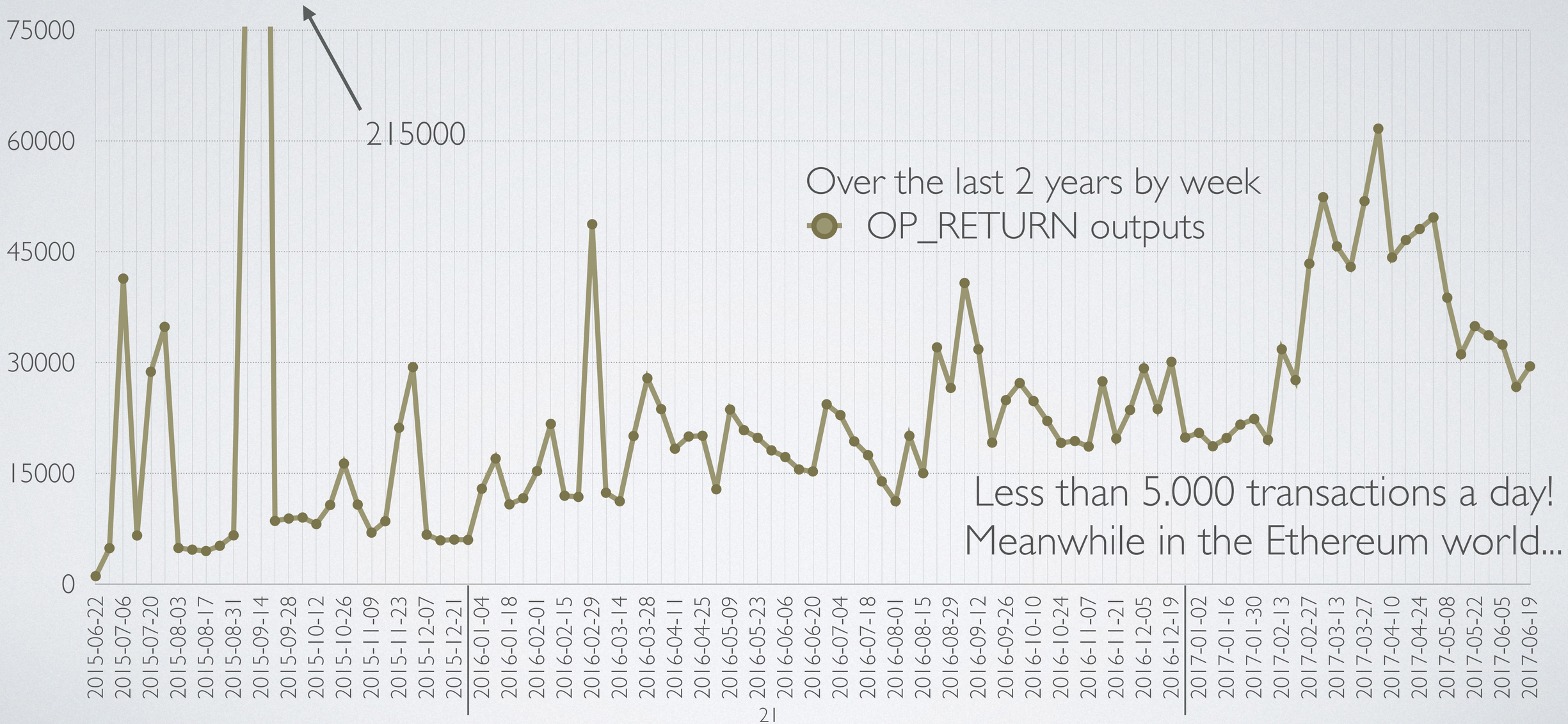
- The Bitcoin blockchain has non-monetary use cases! We can't scale notarisation of documents via an off-chain solution.
- Tokens on the Bitcoin blockchain (Open Assets, Omni Layer, etc.) use special *OP_RETURN*-outputs in order to work. They are currently not supported by any off-chain solution.

WHY ฿ NEEDS AN ON-CHAIN SOLUTION?

Two more issues many people forget about:

- Bitcoin mixers heavily rely on on-chain transactions
- Spam attacks are tons cheaper if the blocks are filled and there's already a huge backlog

NUMBER OF OP_RETURN OUTPUTS



WHY ฿ NEEDS AN OFF-CHAIN SOLUTION?

- The easiest solution to the bus problem would be to enlarge the bus (to increase the blocks) each time the fees go very high

- But obviously, such strategy won't last long — we can't sustain 1 exabyte blocks

Image: https://commons.wikimedia.org/wiki/File:Knight_Bus_3.jpg

TO SUMMARIZE

- ✗ No solution at all: Ethereum and other cryptos will overtake Bitcoin this year
- ✗ An on-chain solution only: no one will be able to run a node
- ✗ An off-chain solution only: leads to a centralized settlement system
- ✓ Both solutions: Bitcoin will be able to adopt the entire 7.5 billion world pop.

Thanks for your attention!

CONTACTS

- 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!