

# Hunting Moby Dick

An analysis of past spam attacks

Collaboration between @khannib and @LaurentMT

# About us

Antoine Le Calvez (@khannib)

p2sh.info

Various technical charts about Bitcoin (P2SH adoption, fee estimations, etc..)

LaurentMT (@LaurentMT)

OXT.me

A tool designed for Exploratory Blockchain Analysis of the bitcoin ledger.

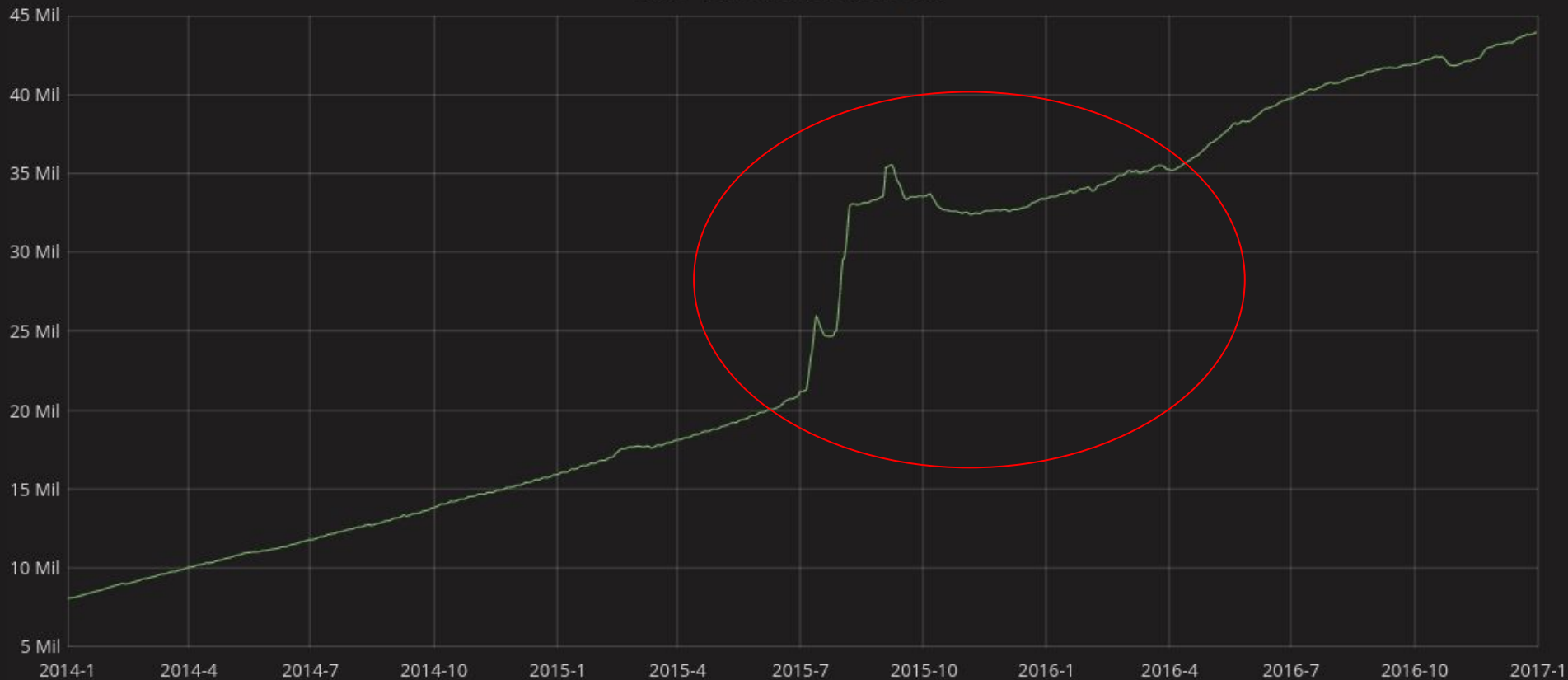
# A note about spam

- Contentious issue with a lot of FUD

“On a blockchain, any sufficiently inefficient process is indistinguishable from spam.”

- Spam is
  - Unsolicited
  - High volume

UTXO count from 2014 to 2017



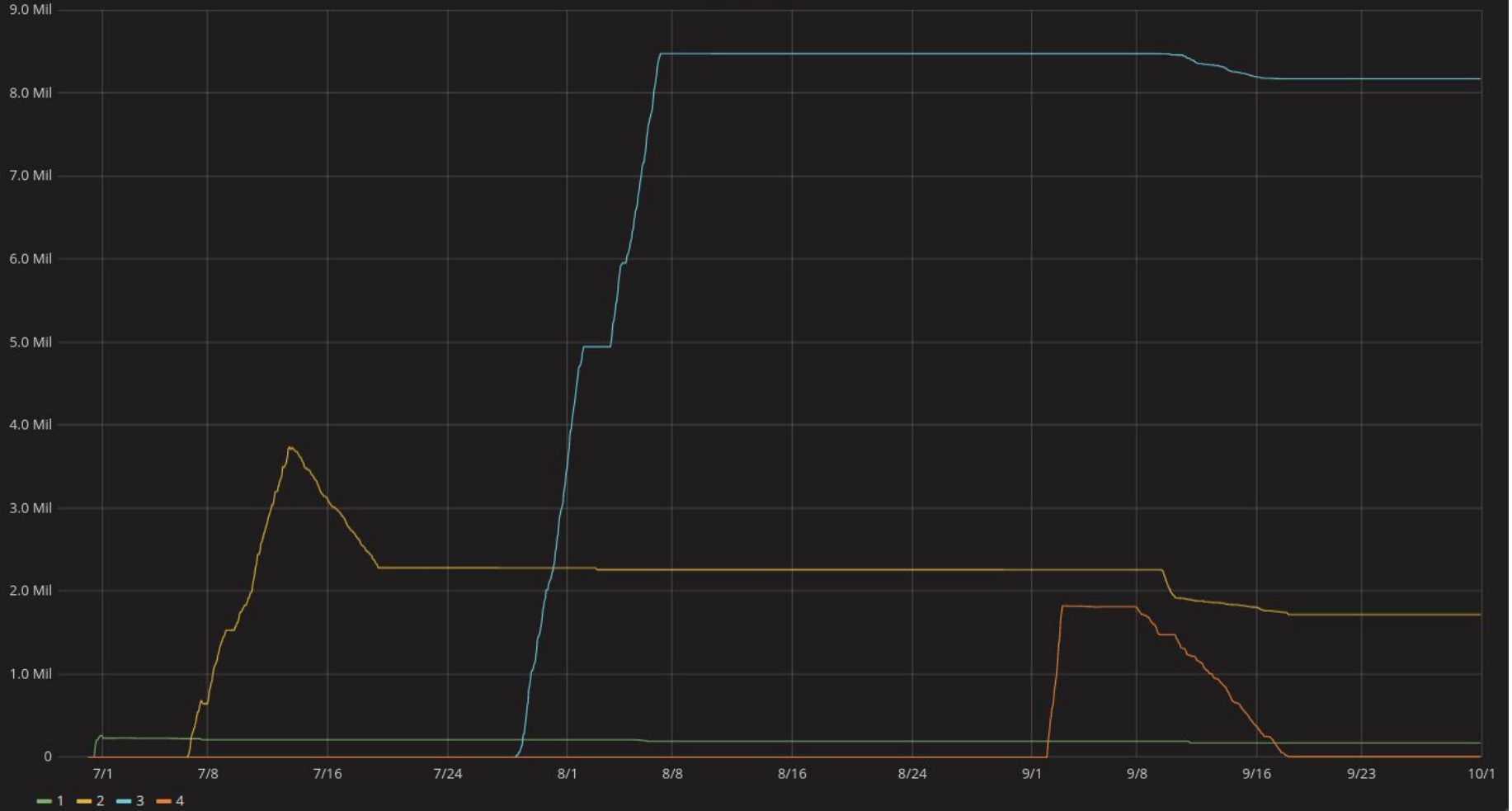
UTXO count where value between 1k and 10k satoshis



# Semi-manual analysis

- wave 1: between 16/06/2015 and 01/07/2015
  - Claimed by Coinwallet.eu
  - 10,000 satoshis outputs
- wave 2: between 06/07/2015 and 17/07/2015
  - Made miners produce 1M blocks, including a monster, 1MB, 2 txs block.
  - 1,000 satoshis outputs
- wave 3: between 25/07/2015 and 09/08/2015
  - The most mysterious one
  - 1,000 satoshis outputs
- wave 4: between 01/09/2015 and 07/09/2015
  - Claimed by Coinwallet.eu
  - 1,000 satoshis outputs

UTXO per wave



# Overall Statistics

2.78 GB of block space (2.2% of current block chain)

268 BTC in fees (9.6 sat/B average)

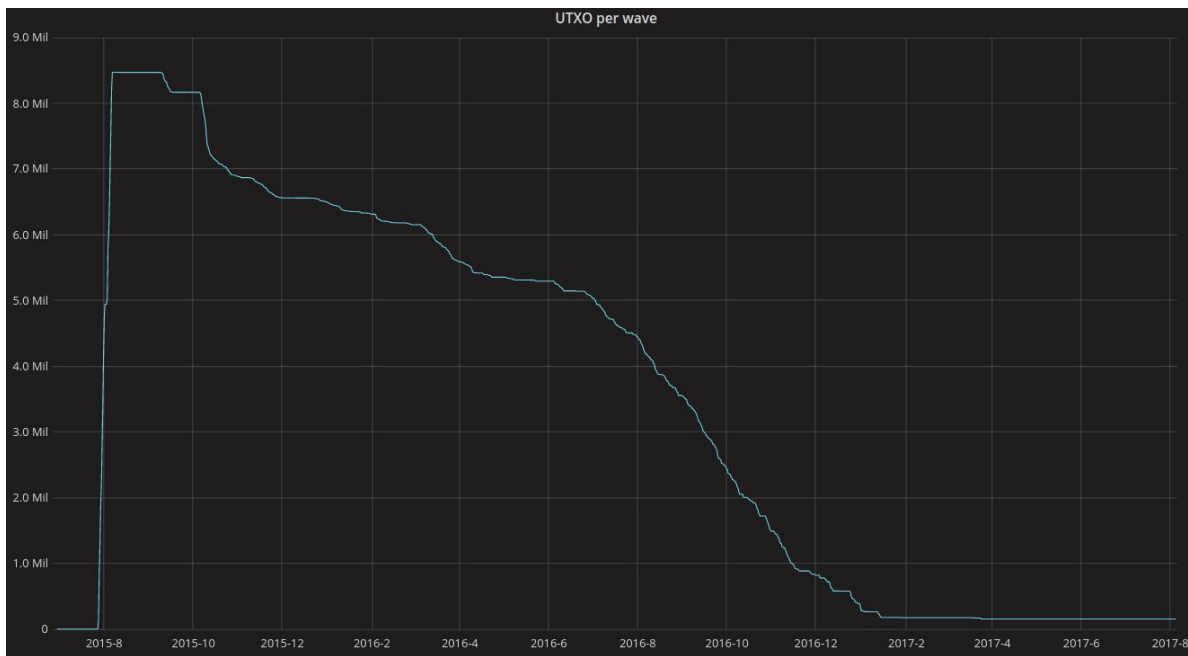
1.34M transactions (0.05% of total)

2M still unspent outputs (3.7% of current UTXO)



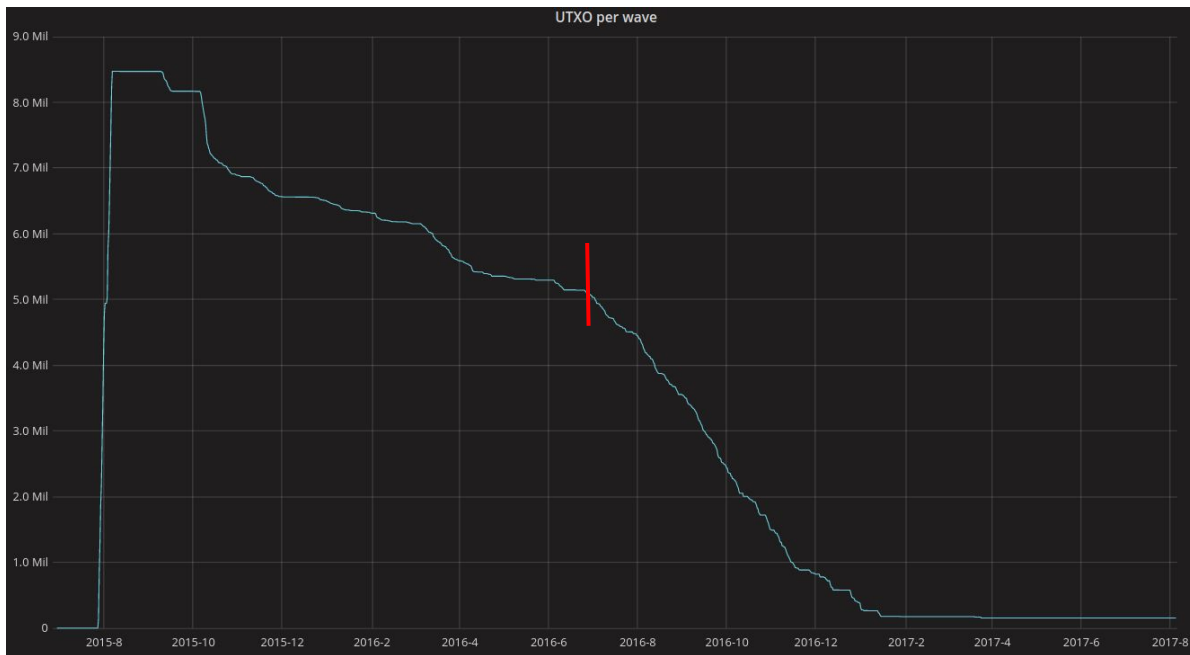
# A two step dance

- Creation of outputs: days, visible, one party
- Consumption of outputs: months, unnoticed, several parties



# A strange timing

*“Don’t pay attention to those spam broadcasts, as all miners have been ignoring them since October by using the minrelaytxfee command line/bitcoin.conf option.”—jtoomim, May 2016*



# What can we do?

Fees are a barrier to entry

Targets could use SegWit (cheaper claiming of outputs)

Raising dust limit

Better monitoring

Spam resistant coin selection algorithms

Thanks for your time, questions?