Universitat Autònoma
de Barcelona

SeNDA
Security of Networks and
Distributed Applications

Analysis of the Bitcoin UTXO set

Sergi Delgado Segura,
Cristina Pérez Solà,
Guillermo Navarro Arribas,
Jordi Herrera Joancomartí

@sr_gi

Motivation

- ❖We could not find a tool to access and analyze the UTXO set.
- ❖How Bitcoin unspent outputs are organized?
- ❖How many outputs of each type can be found in the set?
- ❖How many unspent outputs are actually worth spending?
- ❖How many outputs not worth spending is every full node storing?
- ❖Curiosity!

Unspent TX Output

A UTXO is a transaction output that has not been spent yet. When we talk about bitcoins we are actually referring to UTXOs.

The UTXO set

The UTXO set is where all UTXOs are stored. We can see it as wallet that includes all unspent bitcoins. No matter their type, “owner” nor value.

Properties of the UTXO set

- It is part of every full node.
- The Bitcoin value of a UTXO does not affect its size (bigger value != bigger size).
- The larger the output script of a UTXO, the larger space it occupies in the set.

STATUS

STadistical Analysis Tools for UTXO Set

Suite of tools to analyze the UTXO Set (Bitcoin Core version)

Open source code available on Github https://git.io/vAzHL

Data overview

Analysis data

Snapshot date	22/02/18
Block heigh	510535
Core version	0.15.1
UTXO set size	3.4 GB
#UTXOs	55.47 M

Output distribution

P2PKH	P2SH	P2PK	Others
81,2 %	18 %	0,1 %	0,7 %

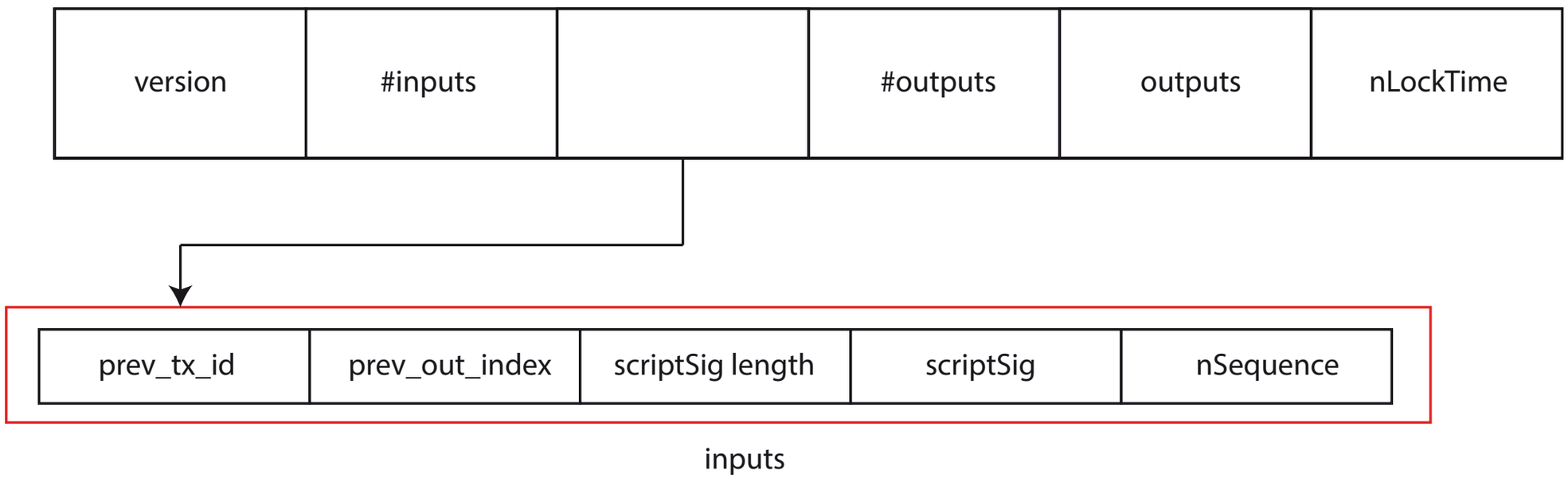
Dust and non-profitable outputs analysis

Definitions

dust utxo: transaction fees≥ 1/3 utxo value
non-profitable utxo: transaction fees > utxo value

Fees are payed in a per byte fashion

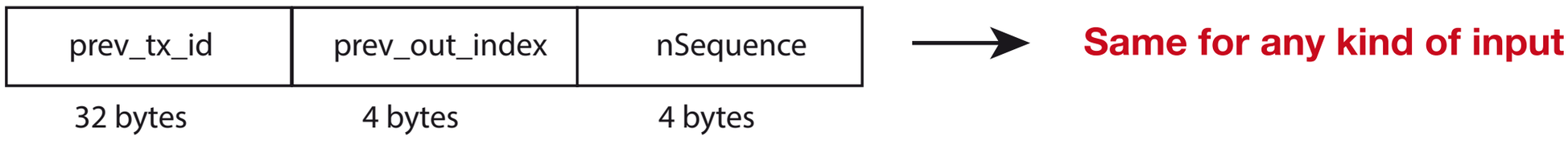
Minimum size approximation



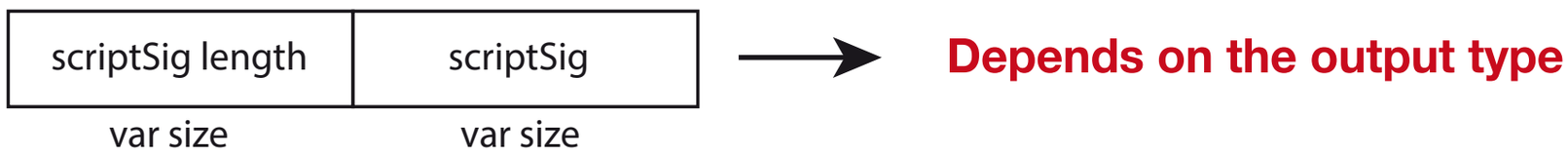
Set a lower bound!

Minimum size approximation

Fixed size



Variable size



P2PKH size approximation

Variable size

PUSH sig (1 byte) + sig (71 bytes) + PUSH pk (1 byte) + pk (33-65 bytes) → **106 / 138 bytes**

↓ Lower bound

↓ Compressed / uncompressed

Total size

fixed size (40 bytes) + scripSig length (1 byte) + variable size (106 / 138 bytes) → **147 / 179 bytes**

P2SH size approximation

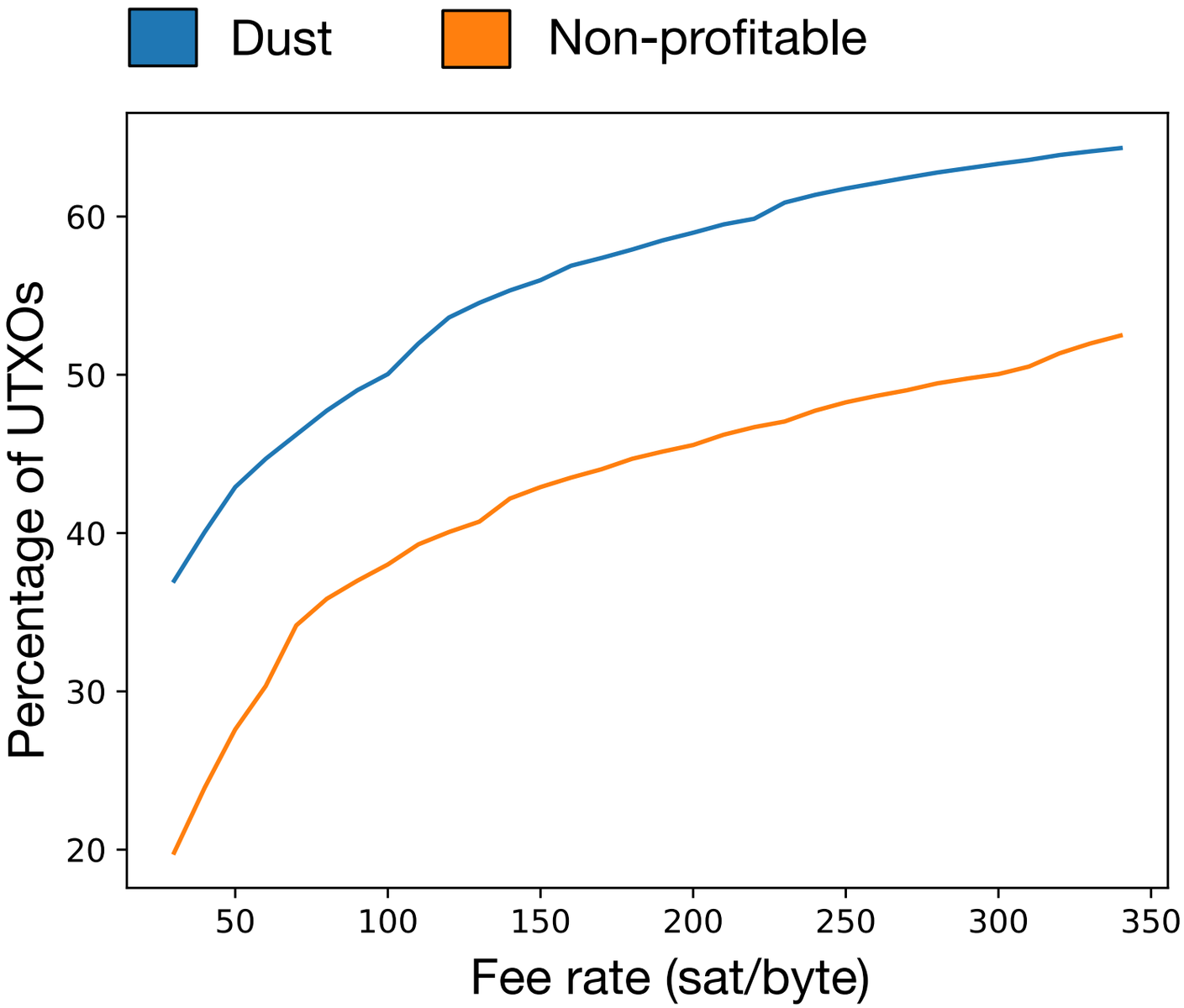
Variable size

Total size

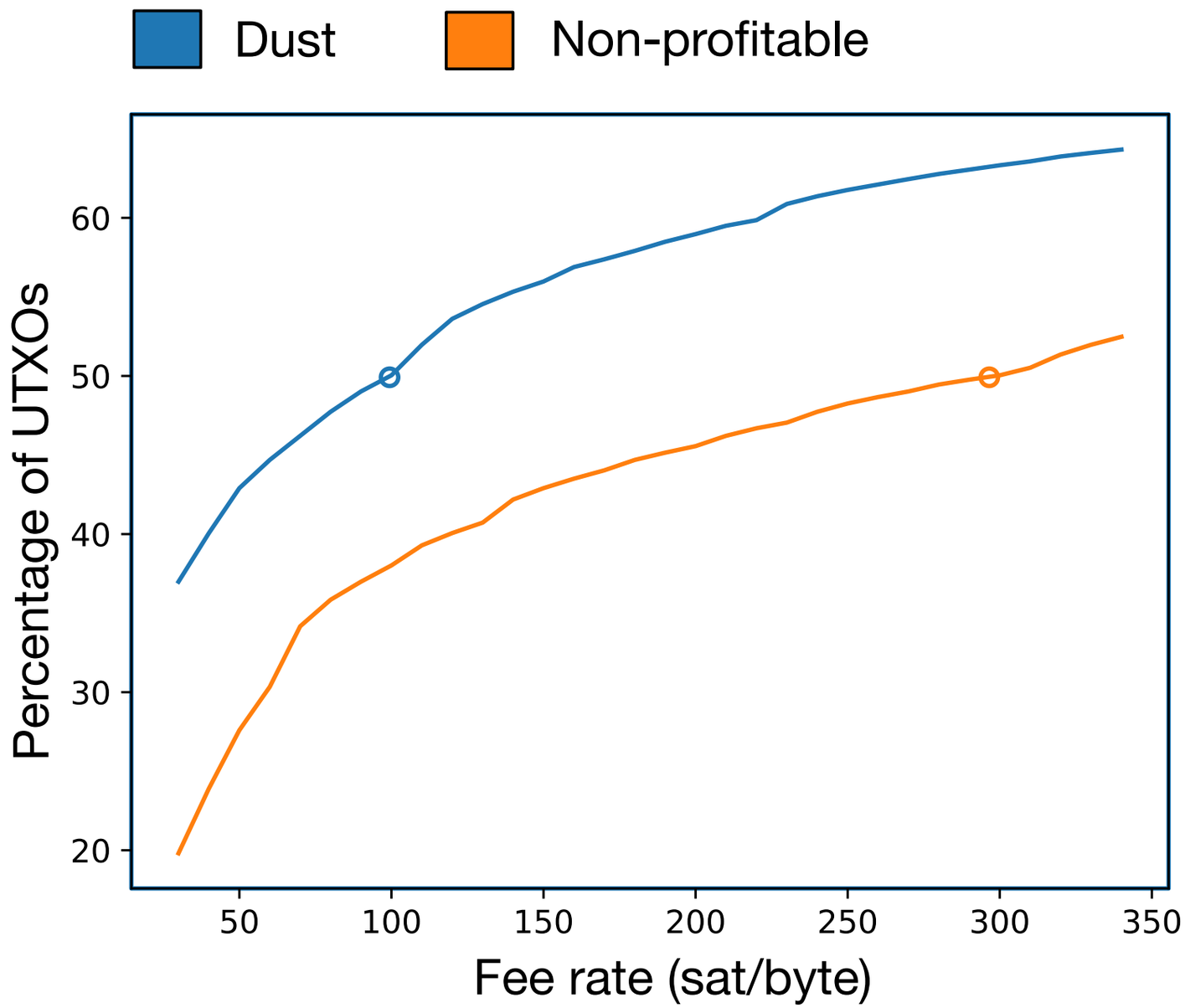
fixed size (40 bytes)

Results

Number of outputs



Number of outputs

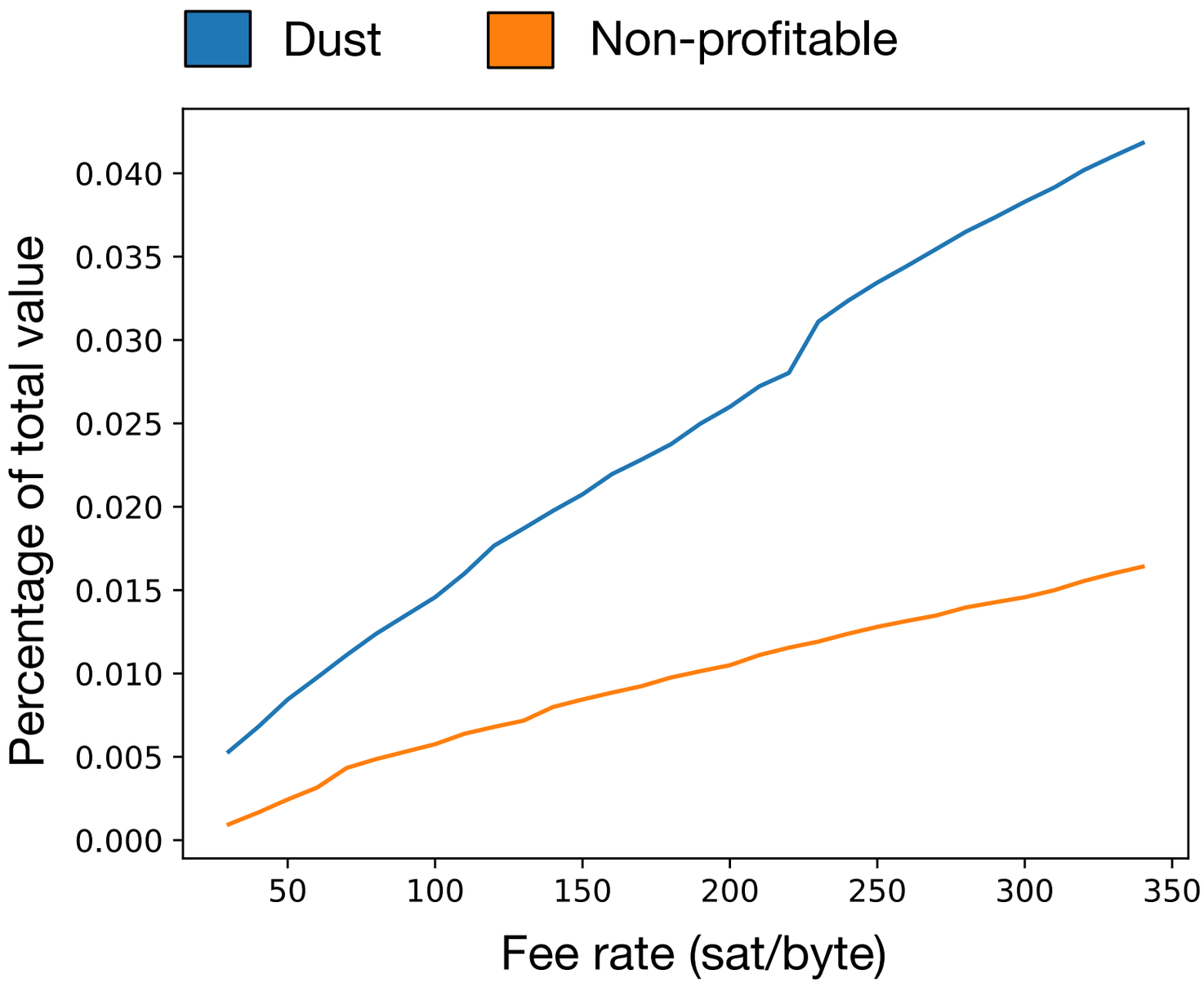


50% outs are dust
for 100+ sat/byte

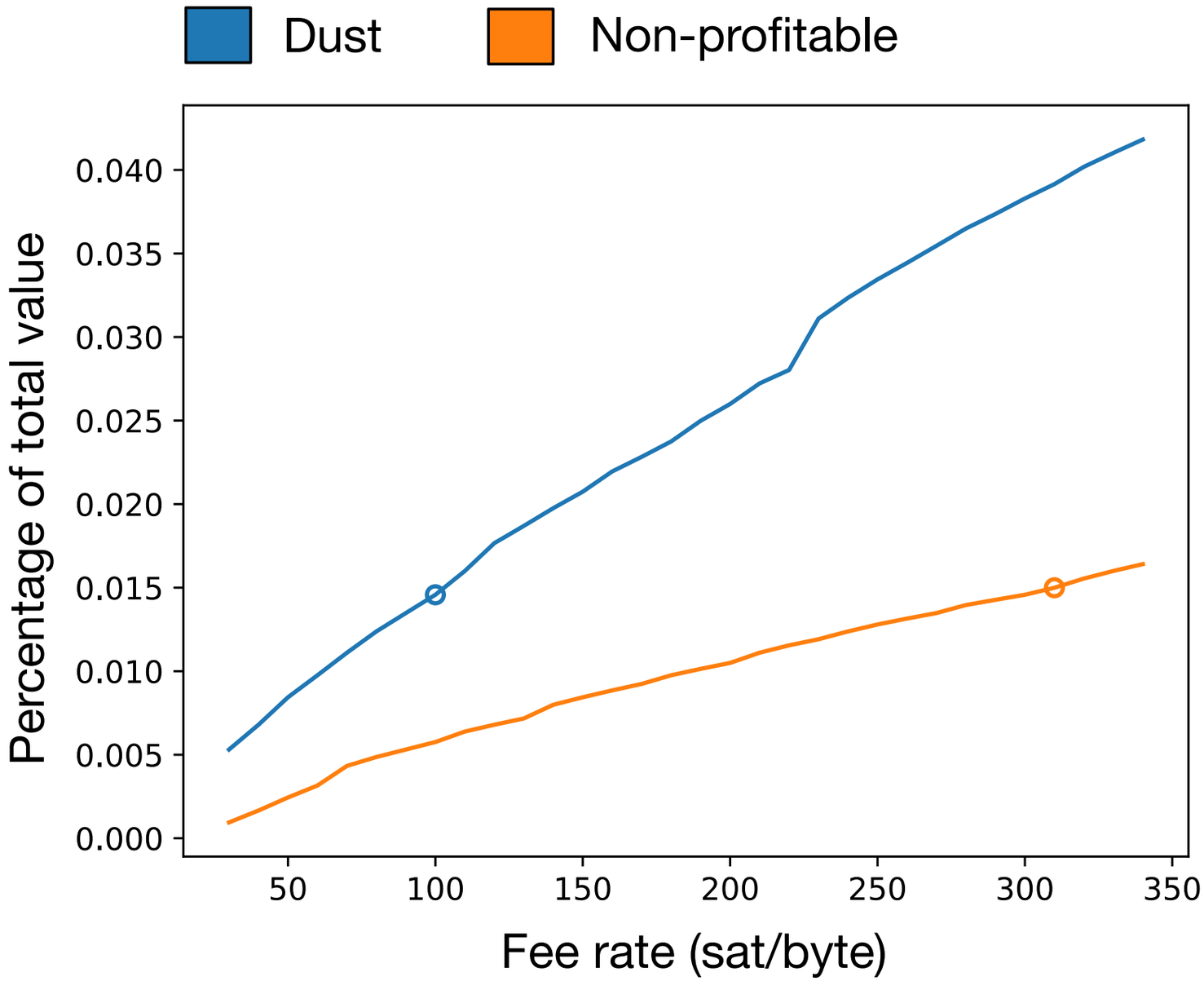
50% outs are
non-profitable
for 310+ sat/byte

1.7GB per full node

Outputs value



Outputs value

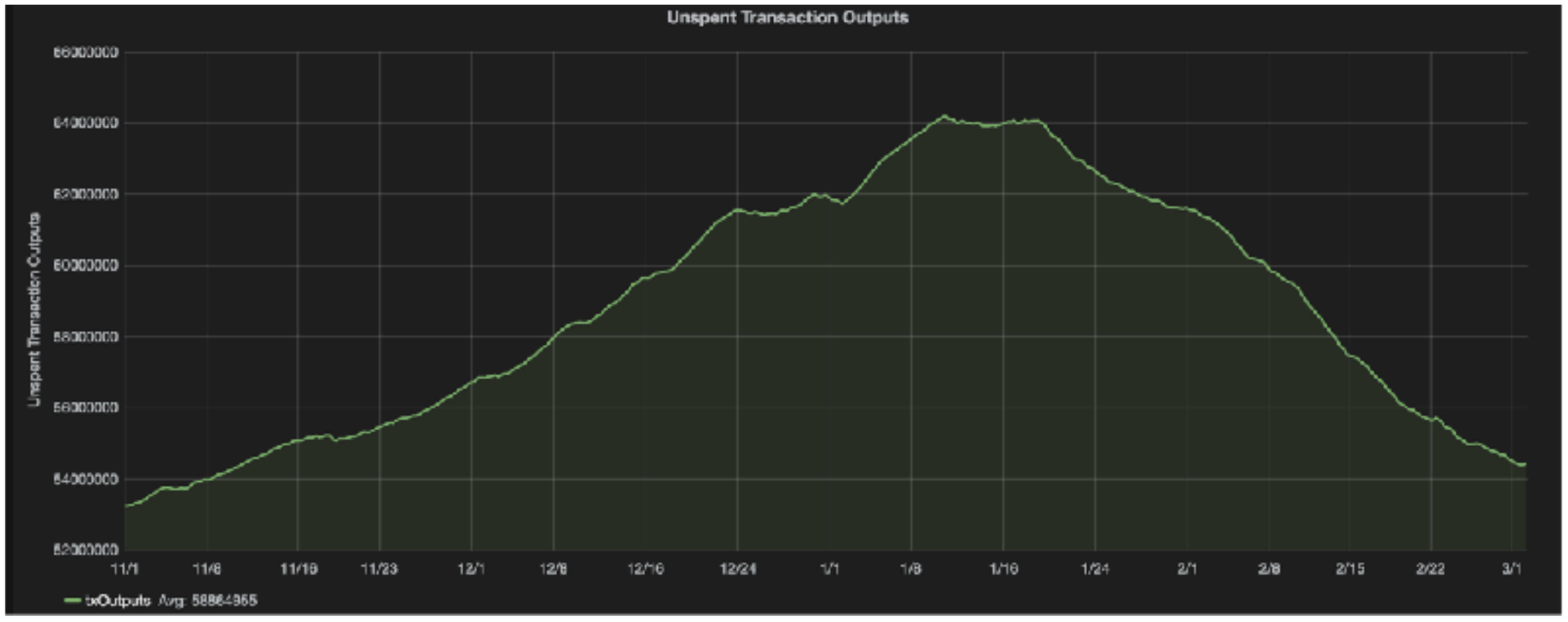


Around 0.015%* of total available bitcoins in both cases.

*2500 bitcoins

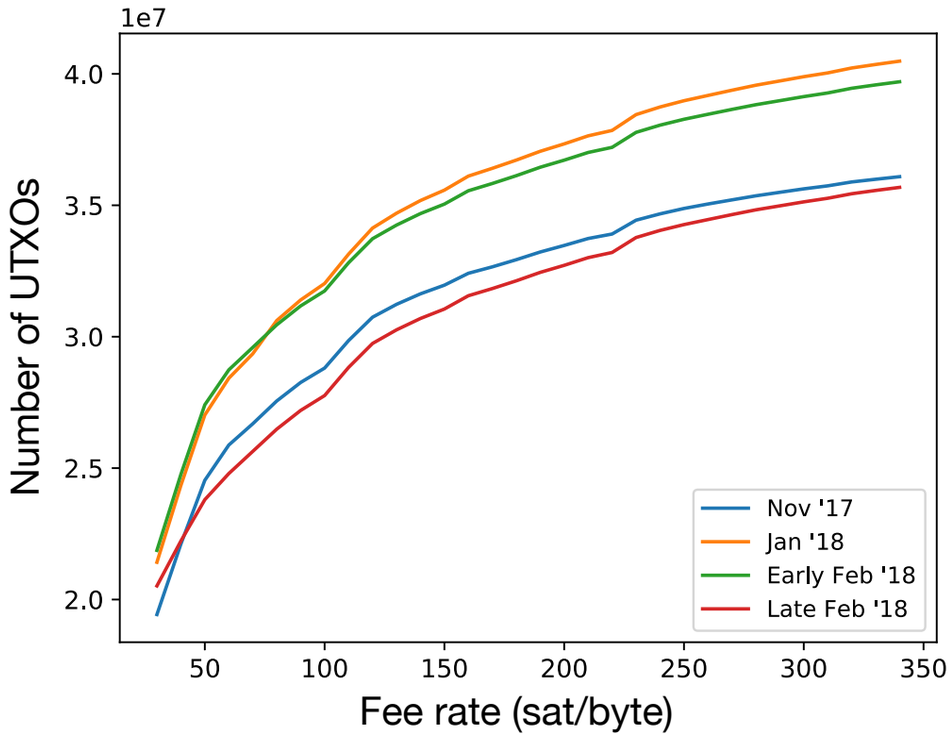
UTXO consolidation

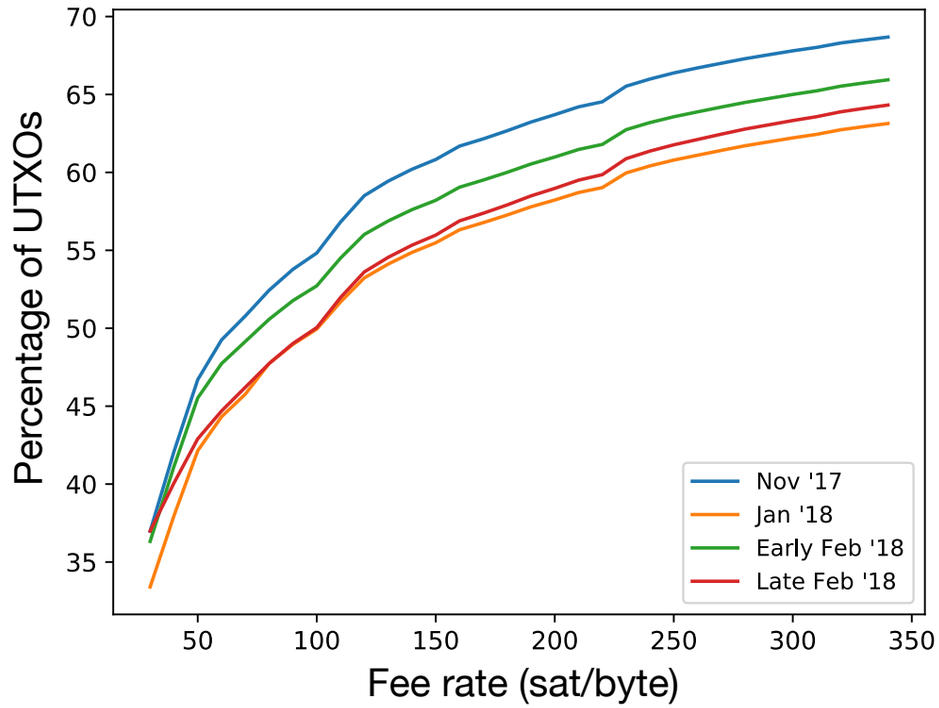
UTXO consolidation



source: statoshi.info

Dust consolidation





Conclusions

- A huge part of the UTXO set is covered with dust
- Take advantage of low fees to perform consolidation
- Consensus rule to ease dust consolidation (lower fees to encourage it)?

Thank you!

Questions?