Selfish & opaque transaction ordering in the Bitcoin blockchain: the case for chain neutrality

Exclusive mining, accelerated transactions, and Omni transactions

Johnnatan Messias
http://johnnatan.me

This is a complementary analysis of our ACM IMC'21 paper.
Selfish & Opaque Transaction Ordering in the Bitcoin Blockchain: The Case for Chain Neutrality
Johnnatan Messias, Mohamed Alzayat, Balakrishnan Chandrasekaran, Krishna P. Gummadi, Patrick Loiseau, and Alan Mislove.
In Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC 2021). Virtual Event. November, 2021.

Exclusive Mining

- It refers to users who have private communication with a particular MPO to avoid announcing their transactions to the entire network. Only the MPO and the user/issuer are aware of this transaction until the MPO includes it in a block.

- They pointed out that there could be **3 reasons** why this might happen:

  - Reducing transaction cost volatility ("confirmation as a service").

  - Hiding unconfirmed transactions from the network to prevent front-running.

  - Camouflaging wealth transfers as transaction costs to evade taxes or launder money.

- References

  - Paper/report: Exclusive Mining of Blockchain Transactions

  - Coin Telegraph

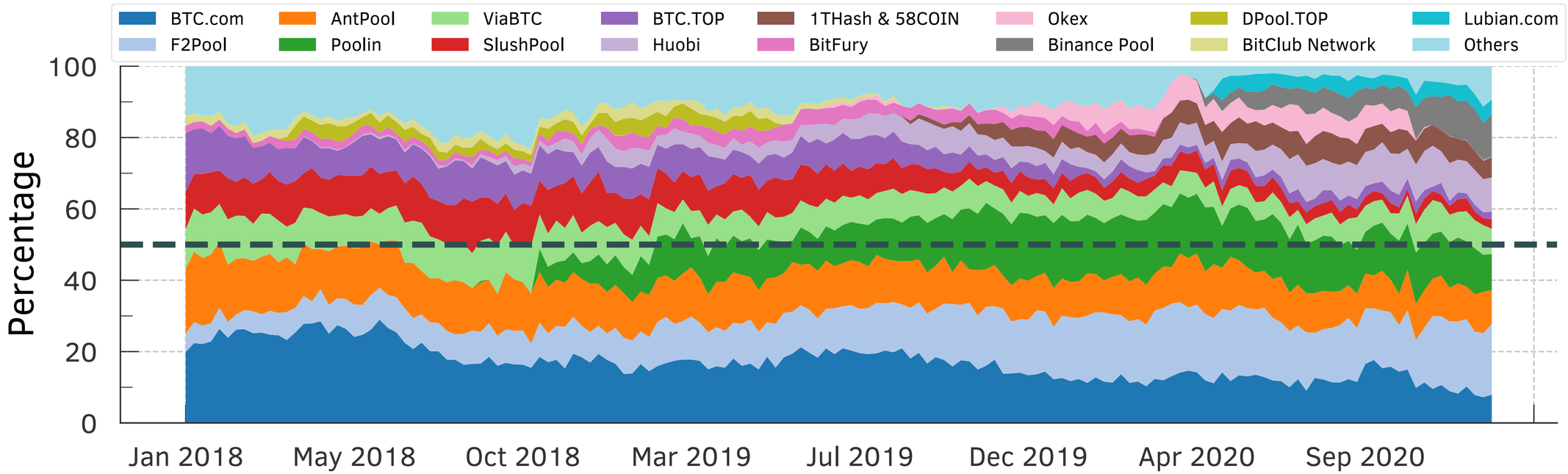
Johnnatan Messias

Exclusive Mining

- There is a Front-running as a Service (FRaaS) available for Ethereum
  - Essentially, there is a private blockchain network called "Taichi Network" (TN) that works together with SparkPool (the major Ethereum MPO) that allow users to send their transactions privately to SparkPool. One of the main incentives is that using the TN would be possible to avoid front-running (see here).
  - Perhaps this may be the first (not sure if the only) transaction acceleration (or FRaaS) available in Ethereum! Of course, good (by avoiding front-running) and bad (by decreasing user transparency) things can happen by allowing users to send their transactions privately.
  - Note: now, we also have Flashbots and Eden.

MPOs hashrate

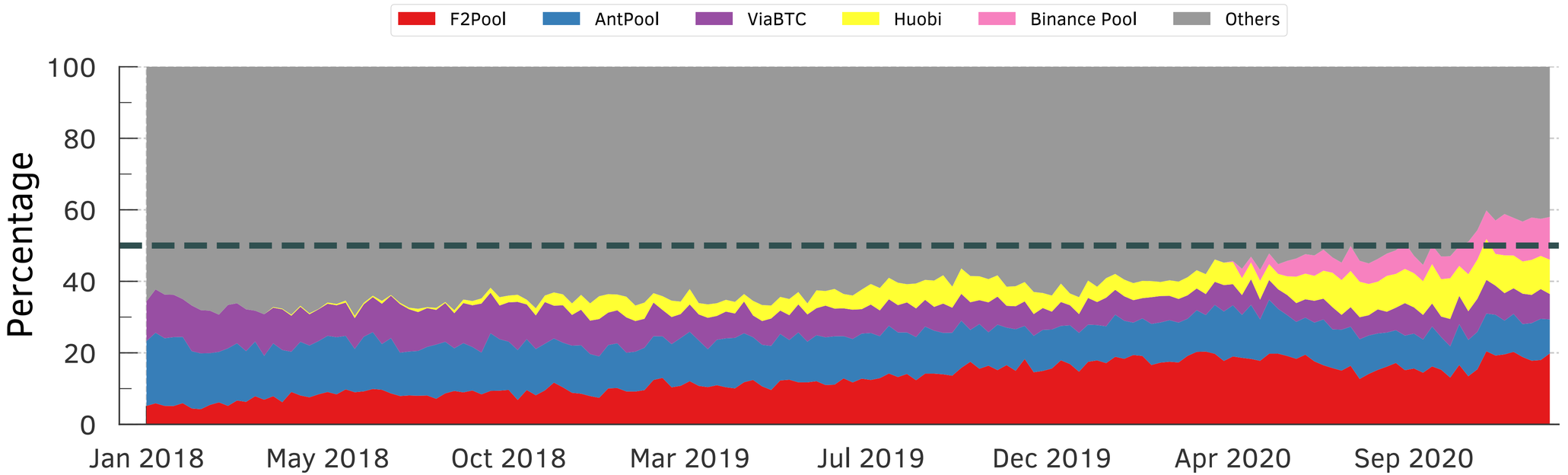
- The plot shows the percentage of the MPOs **hash-rate** over the period of 3 years.



Johnnatan Messias

MPOs hashrate

- Active vs. Others
  - MPOs in the active experiment (excluding BTC.com) increased their hash rate in 2020 in such way that together they accounted for more than 55% of the overall hash rate.
  - Active: MPOs that included transactions accelerated by ourselves.
  - The plot shows the percentage of the MPOs **hash-rate** over the period of 3 years.

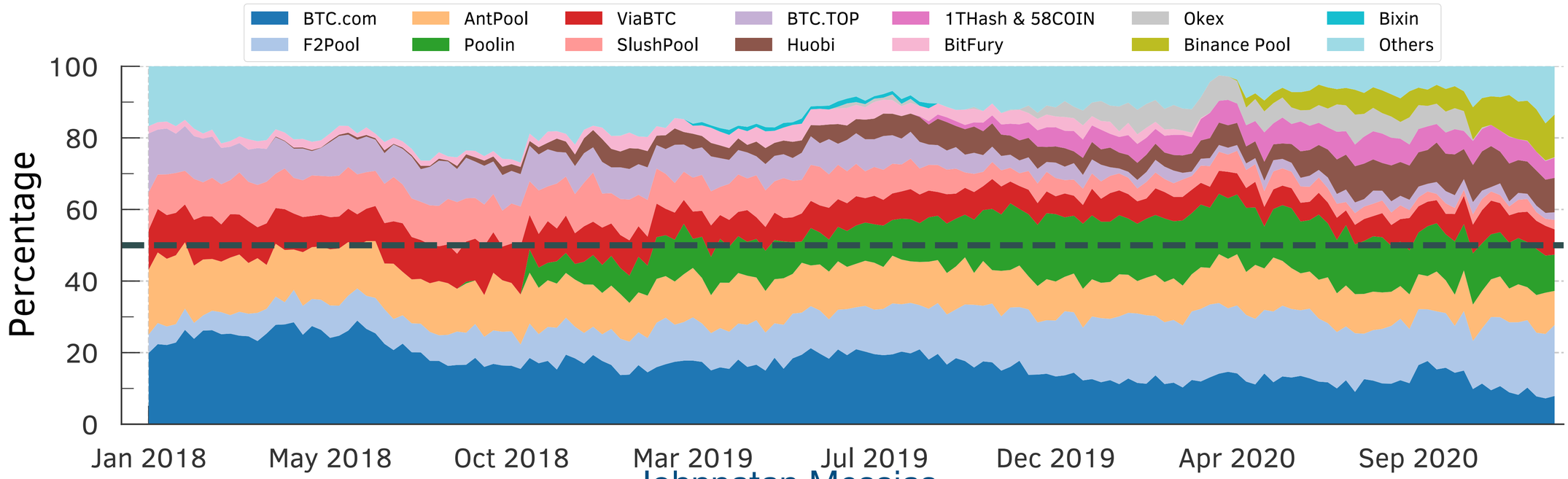


Johnnatan Messias

The accelerated transactions are available here

MPOs hashrate

- Passive + Active vs. Others
  - Passive: MPOs that included transactions inferred to be accelerated using BTC.com API.
  - The plot shows the percentage of the MPOs **hash-rate** over the period of 3 years.

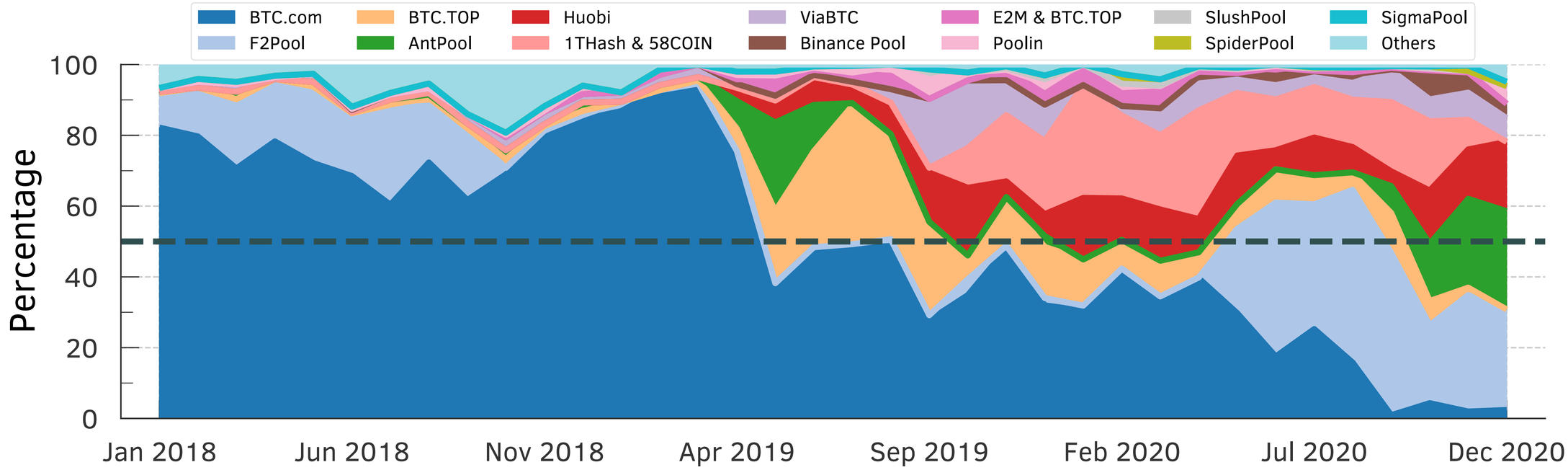


Johnnatan Messias

The accelerated transactions are available here

Front-Running as a Service (FRaaS)

- Monthly moving average
  - The plot shows the percentage of **accelerated** transaction inclusion by each MPO over the period of 3 years.



Johnnatan Messias

The accelerated transactions are available here

OP_RETURN opcode

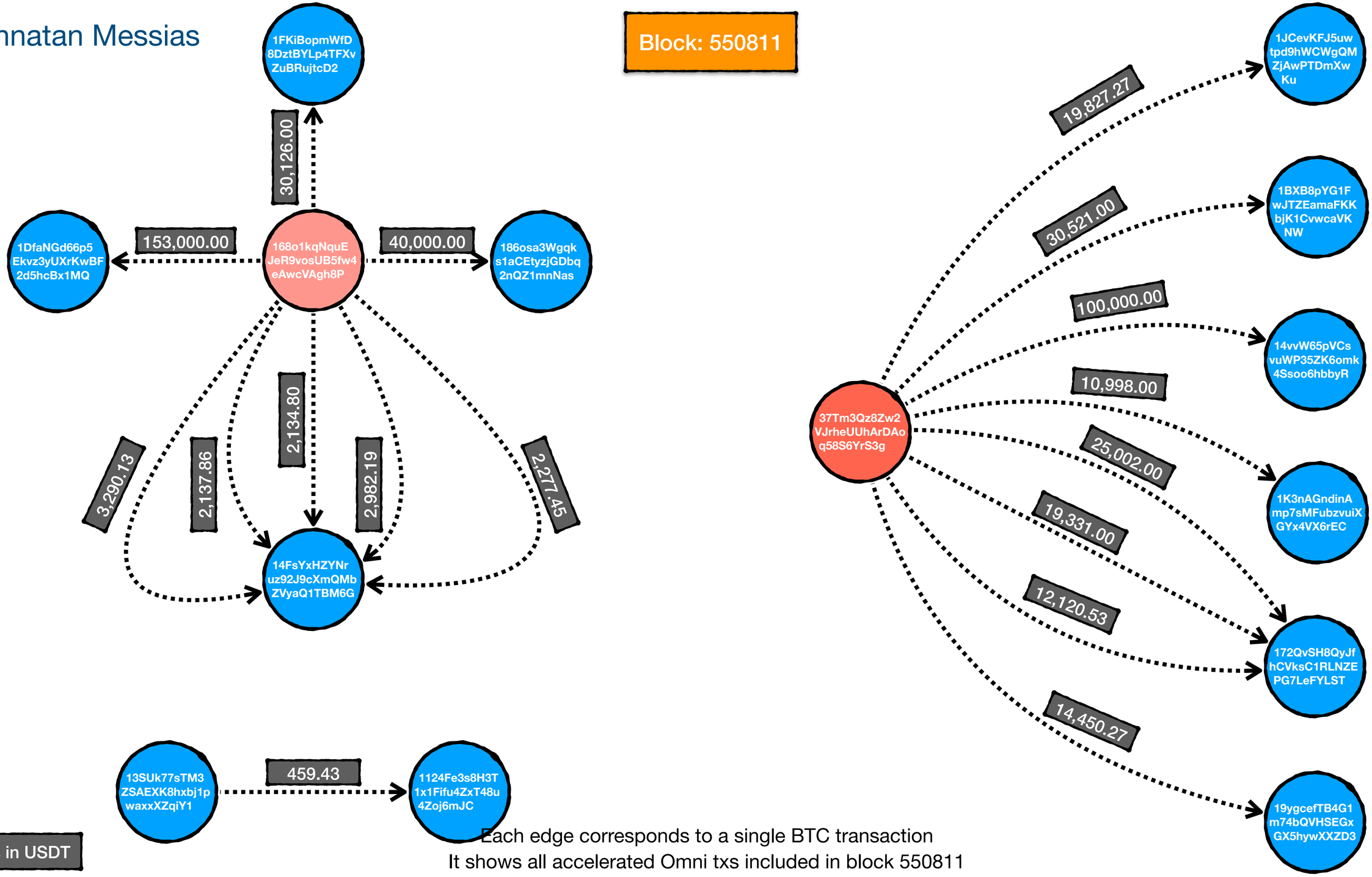
- From 313,737,341 of all includes txs, 42,994,249 (13.70%) contain OP_RETURN opcode.
- From 161,954 blocks, 161,536 (99.74%) of their coinbase txs contain OP_RETURN opcode.
- From 313,575,387 of all issued txs, 42,832,713 (13.66%) contains OP_RETURN opcode.
  - 17,993,300 txs belong to Omni Layer Protocol (an average of ~111 txs per block) which represents 5.74% of all issued txs and 42% of all OP_RETURN opcode transactions. From all Omni txs, 97.27% belongs to Tether USDT token
  - From our set of ~14k **accelerated** transactions, we have that 1805 OP_RETURN txs were **accelerated**. From this set, 1740 accelerated txs belong to Omni Layer Protocol. 1739 txs belong to Tether token (USDT) and 1 to Omni token.

Omni txs accelerated

- When we take a deeper look at those **accelerated** Omni transactions, we see that on average 83,291.33 USDT was transferred.
  - mean: 83,291.33
  - std: 383,060.22
  - min: 0.18
  - 1%: 0.22
  - 5%: 200.00
  - 10%: 654.52
  - 20%: 1,999.20
  - 25%: 3,006.29
  - 50%: 15,274.34
  - 75%: 68,692.14
  - 80%: 88,046.97
  - 90%: 190,503.94
  - 95%: 300,000.00
  - 99%: 996,187.60
  - max: 13,000,000.00

Tether (USDT) is a stable-coin: 1 USDT == 1 USD

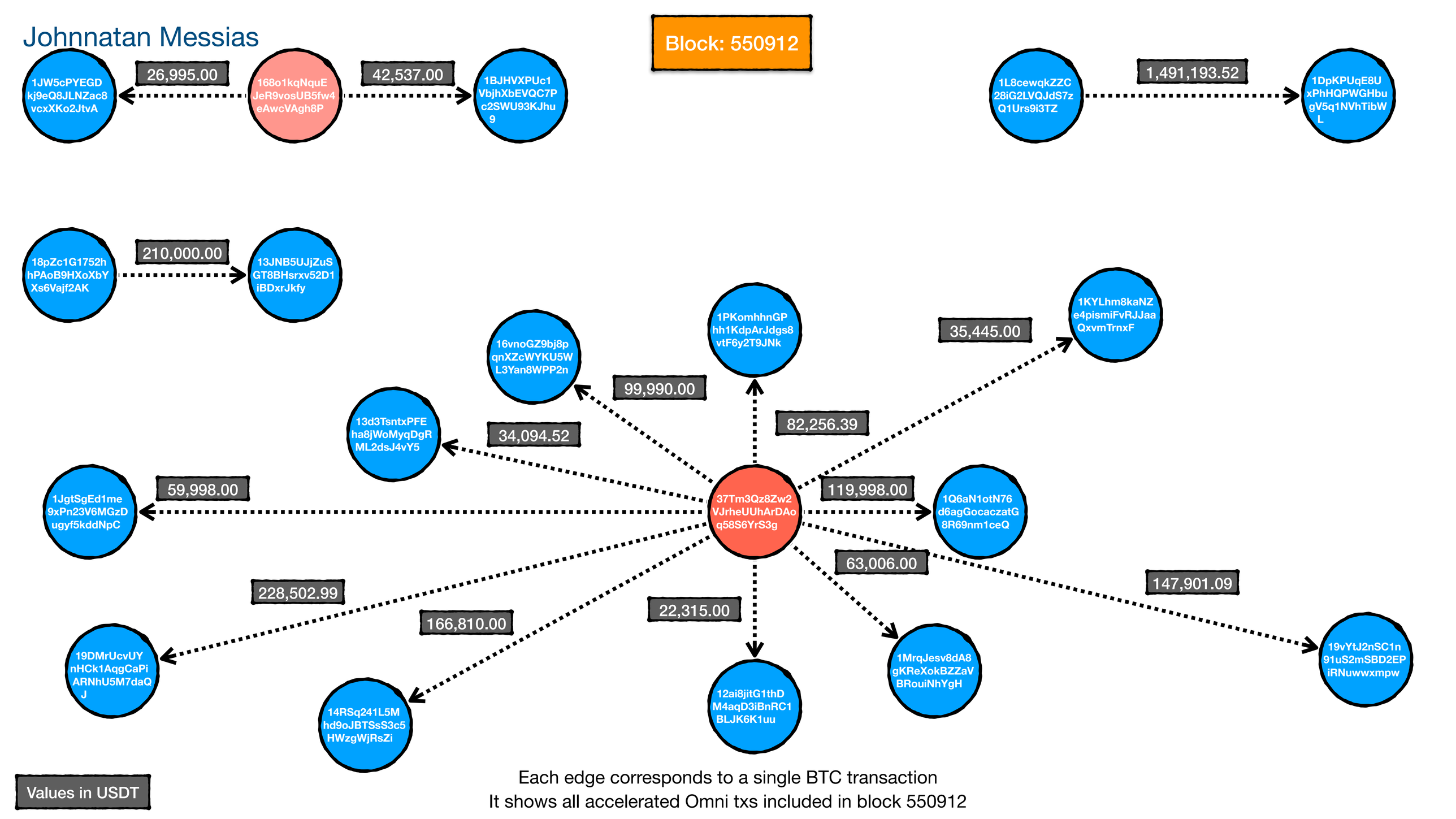
Johnnatan Messias



Each edge corresponds to a single BTC transaction
It shows all accelerated Omni txs included in block 550811

Johnnatan Messias

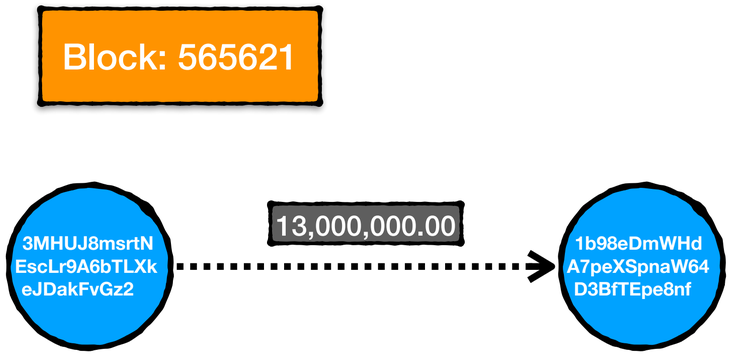
Block: 550912

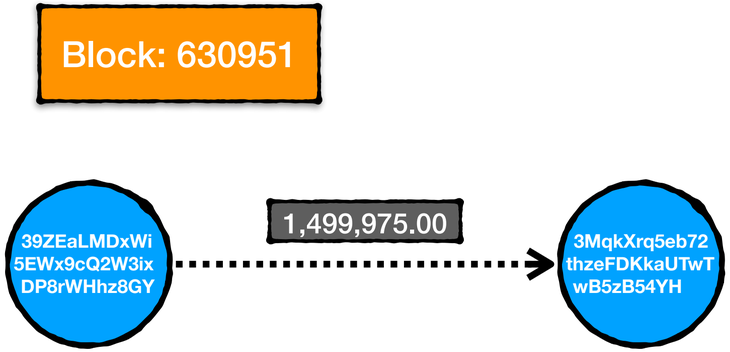


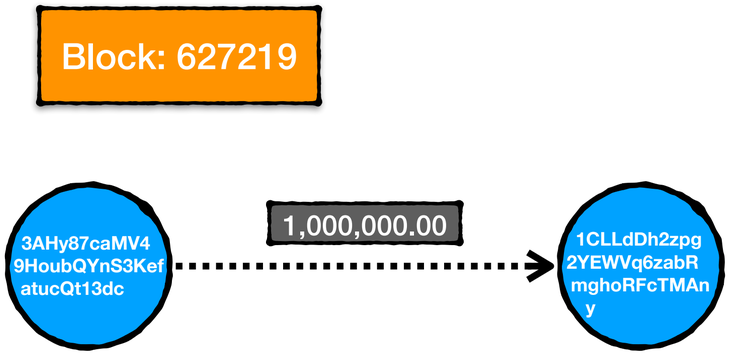
Values in USDT

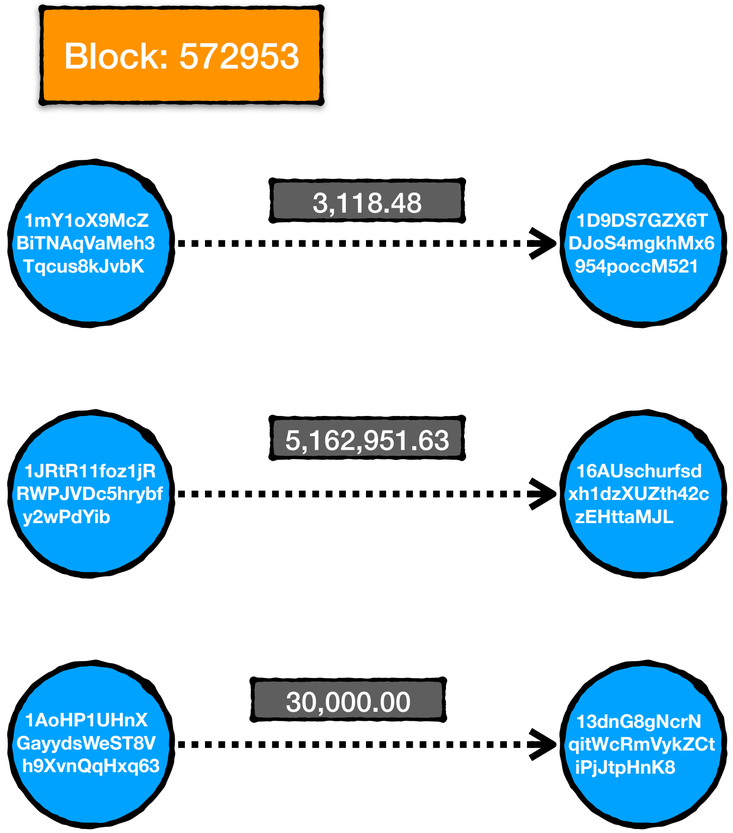
Each edge corresponds to a single BTC transaction
It shows all accelerated Omni txs included in block 550912

Johnnatan Messias









Values in USDT

Each edge corresponds to a single BTC transaction
It shows all accelerated Omni txs included in blocks 565621, 572953, 627219, and 630951

Selfish & opaque transaction ordering in the Bitcoin blockchain: the case for chain neutrality

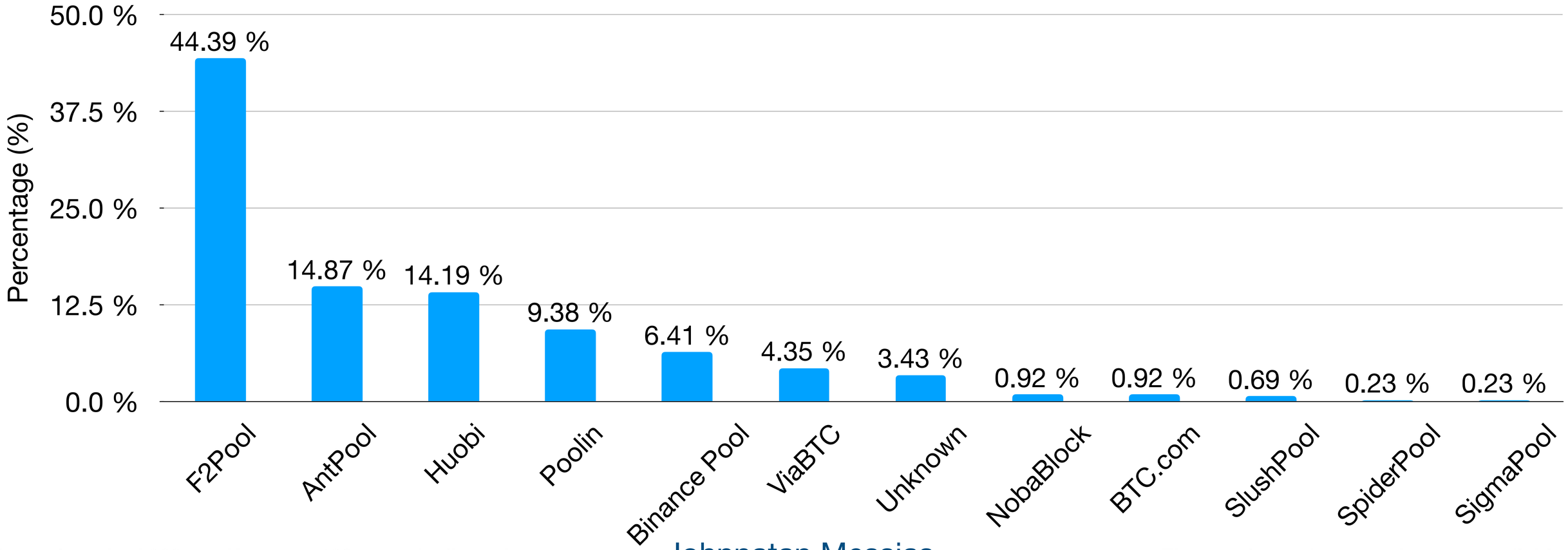
F2Pool accelerated transactions

Johnnatan Messias
http://johnnatan.me

This is a complementary analysis of our ACM IMC'21 paper.
Selfish & Opaque Transaction Ordering in the Bitcoin Blockchain: The Case for Chain Neutrality
Johnnatan Messias, Mohamed Alzayat, Balakrishnan Chandrasekaran, Krishna P. Gummadi, Patrick Loiseau, and Alan Mislove.
In Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC 2021). Virtual Event. November, 2021.

F2Pool transaction accelerator

- From the 727 unique transactions accelerated by F2Pool pushtx service, 437 (60.11%) were mined by the following MPOs (the remaining hasn't gotten included yet).



In total, we had 920 txs. However, 193 were duplicated

Johnnatan Messias

The accelerated transactions are available here

F2Pool transaction accelerator

- 437 transactions were accelerated by F2Pool pushtx service. Below, we have the distribution of transactions positions.

  - mean: 289.37
  - std: 540.73
  - min: 1
  - 1%: 1
  - 5%: 1
  - 10%: 1
  - 20%: 1
  - 25%: 2
  - 50%: 14
  - 75%: 409
  - 80%: 586.80
  - 90%: 962.60
  - 95%: 1542.60
  - 99%: 2439.72
  - max: 3100

Johnnatan Messias

The accelerated transactions are available here

Selfish & opaque transaction ordering in the Bitcoin blockchain: the case for chain neutrality

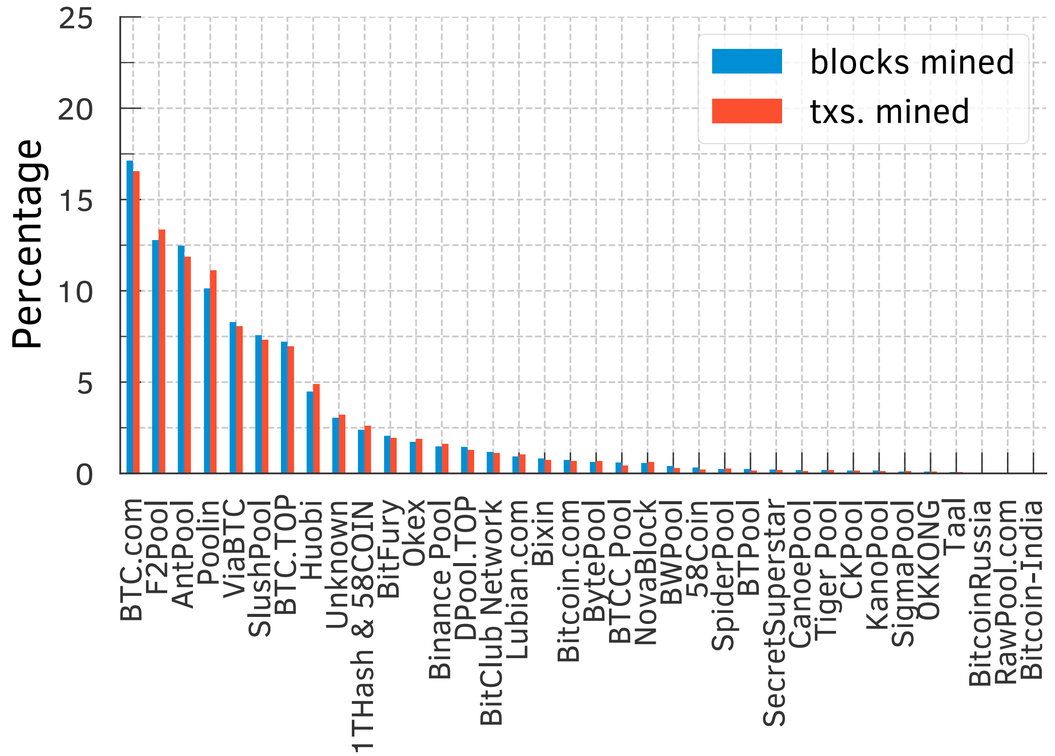
Transaction characterization in our 3-year data set

Johnnatan Messias
http://johnnatan.me

This is a complementary analysis of our ACM IMC'21 paper.
Selfish & Opaque Transaction Ordering in the Bitcoin Blockchain: The Case for Chain Neutrality
Johnnatan Messias, Mohamed Alzayat, Balakrishnan Chandrasekaran, Krishna P. Gummadi, Patrick Loiseau, and Alan Mislove.
In Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC 2021). Virtual Event. November, 2021.

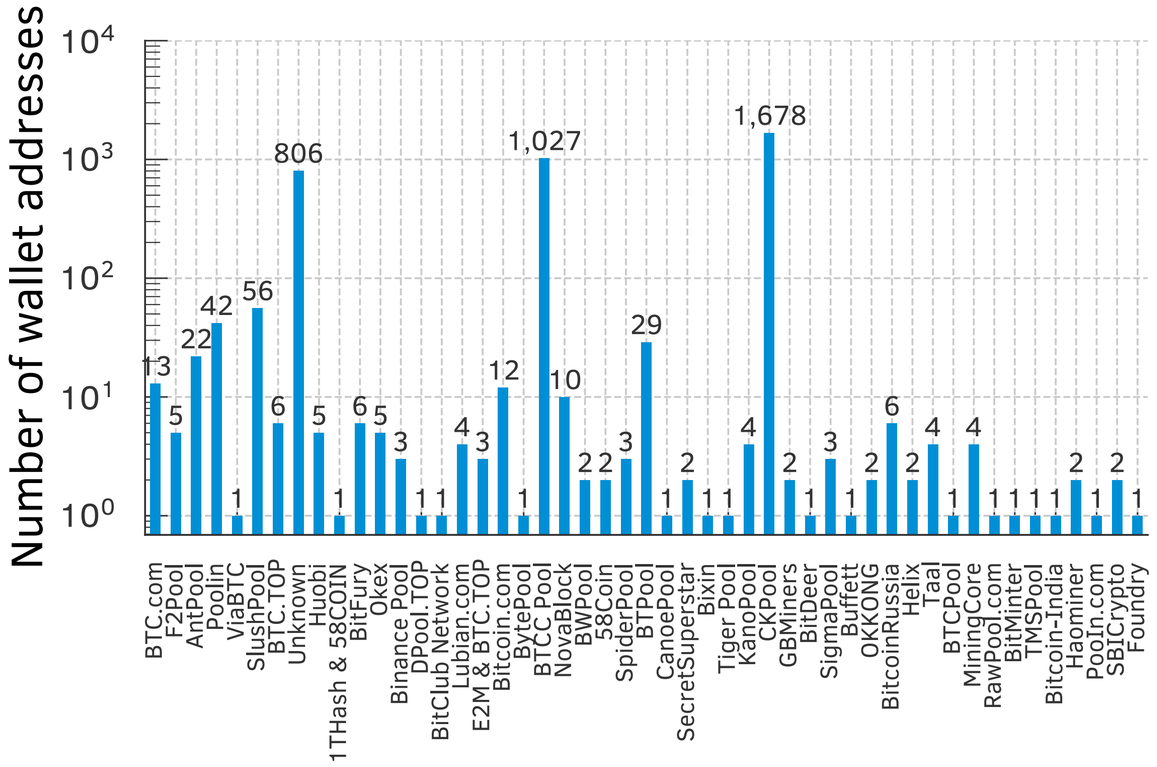
MPOs hash-rate

- The plot shows the percentage of transactions and blocks mined per each MPO over the 3-year period.



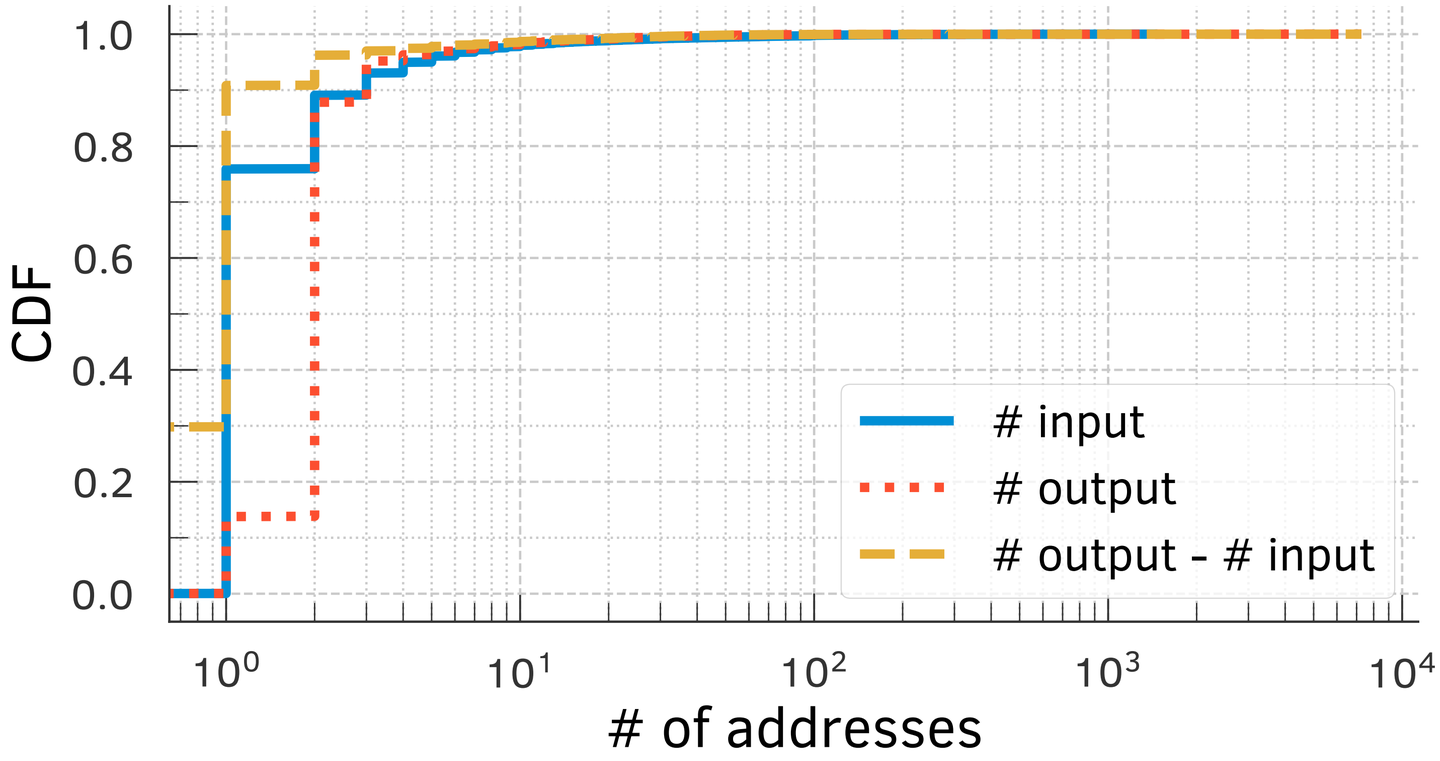
MPOs wallets

- The plot shows the number of wallet address used for each MPO to collect their block reward over the 3-year period.



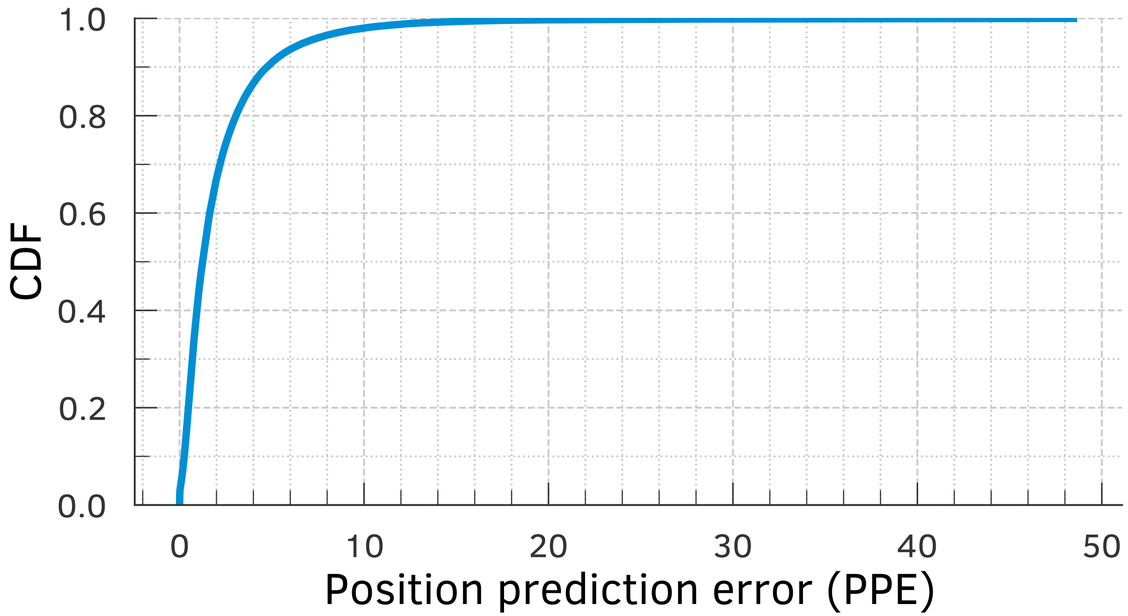
Transactions input and output

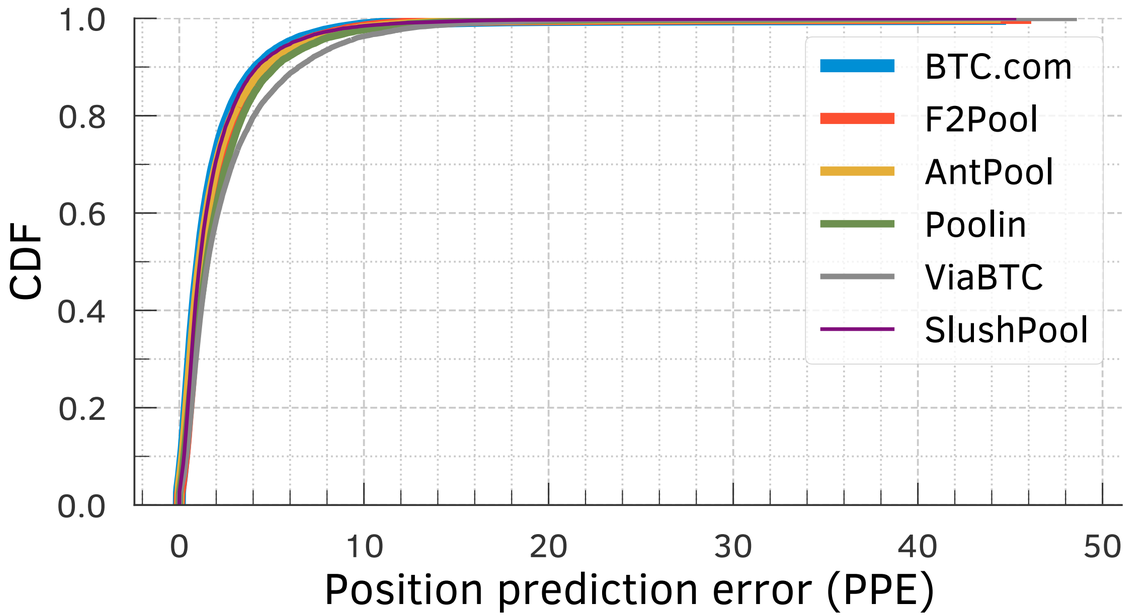
- The plot shows the cumulative distribution function (CDF) of the number of inputs and outputs for each transaction in our data set over the 3-year period.



PPE

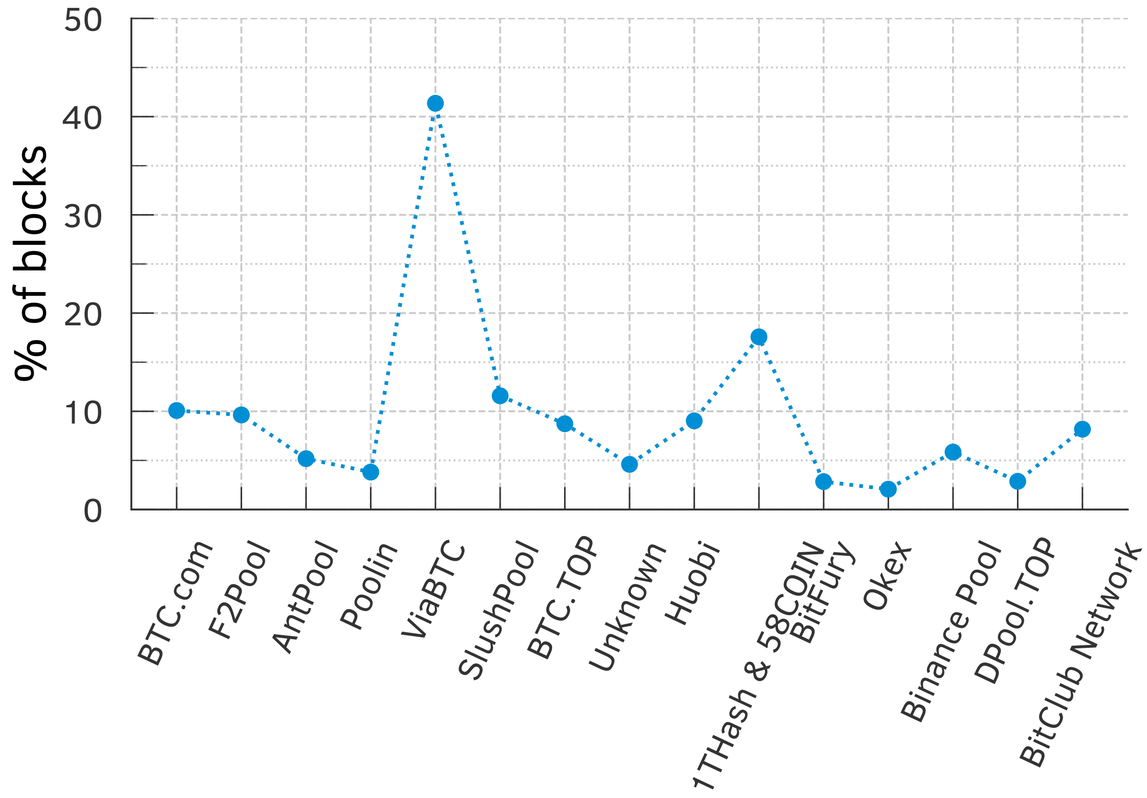
- Mean PPE for each block over the 3-year period.





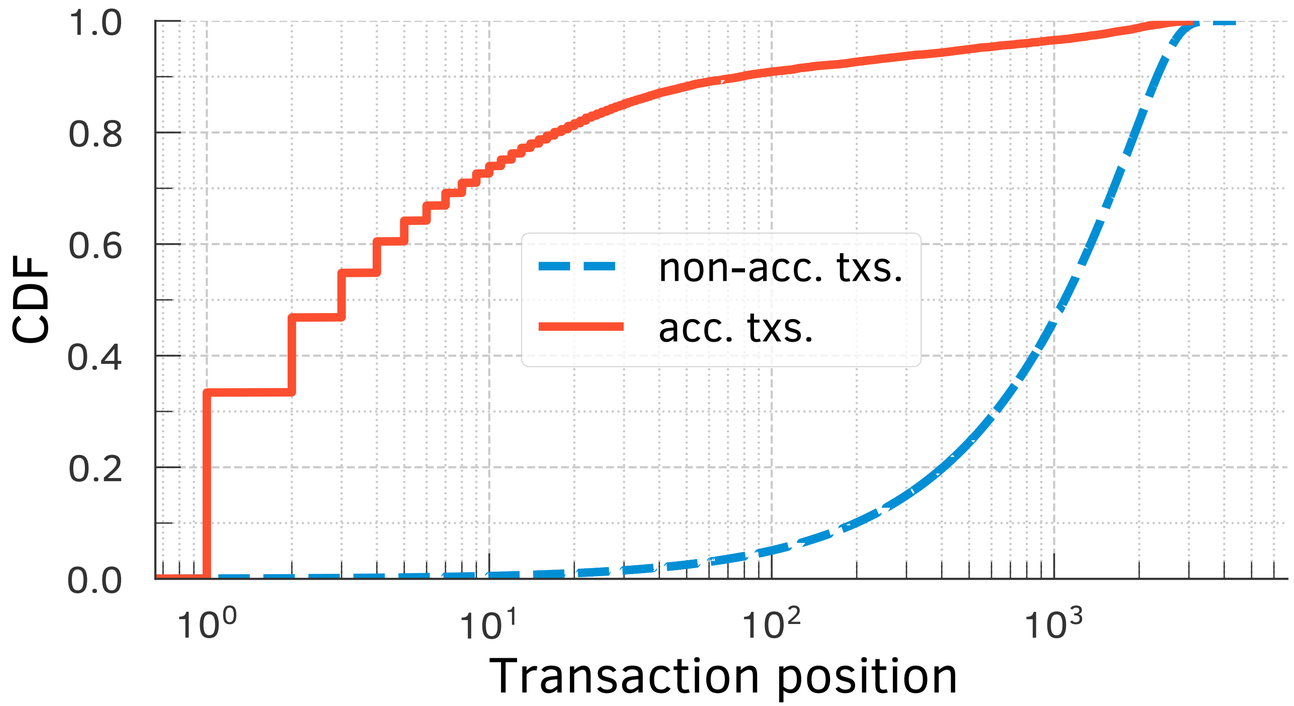
SPPE

- Blocks with SPPE >= 99% are quite common among the top 15 MPOs.



Front-Running as a Service (FRaaS)

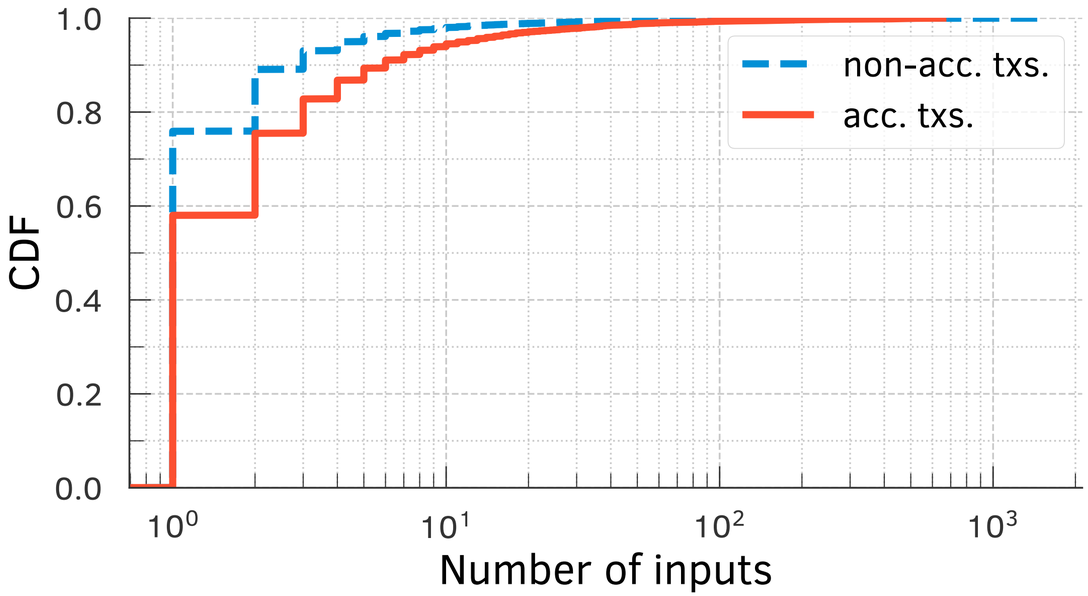
- Accelerated transactions are included earlier in the block than non-accelerated txs.

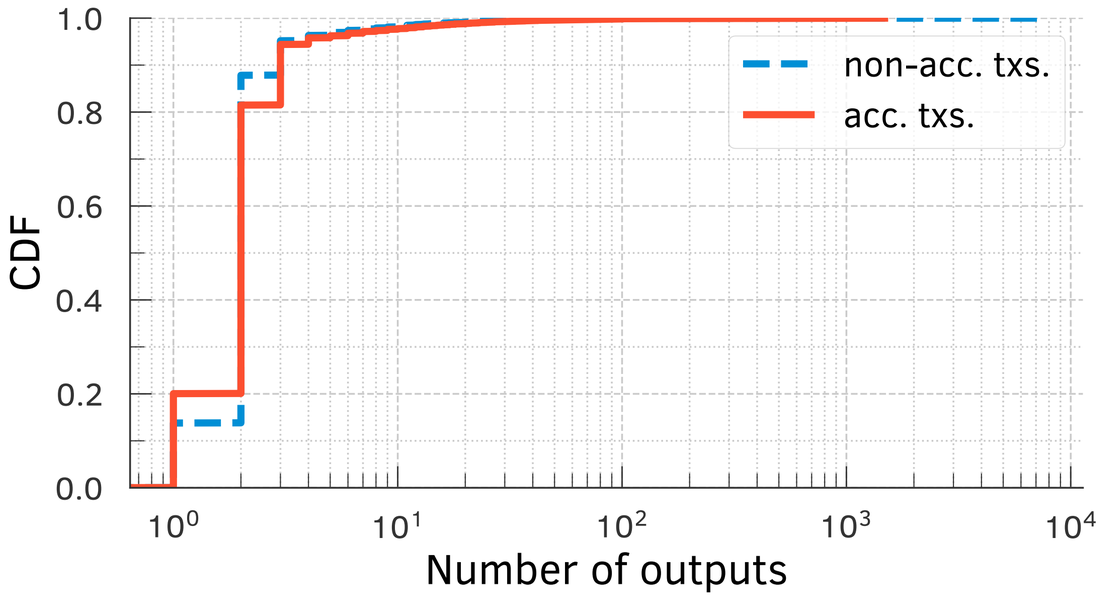


The accelerated transactions are available here

Front-Running as a Service (FRaaS)

- Accelerated transactions have more inputs.

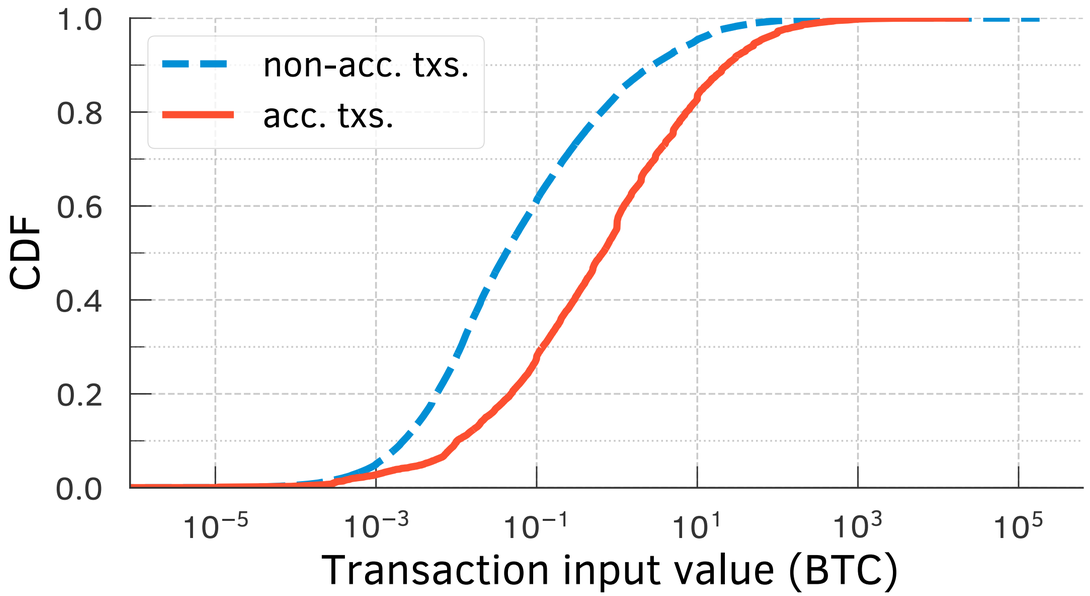


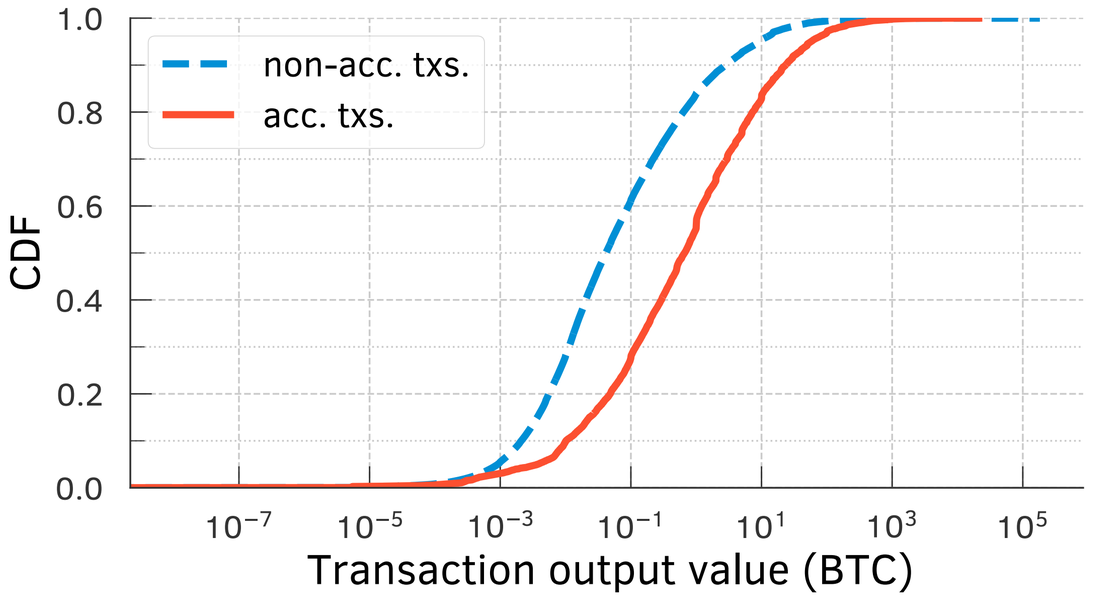


The accelerated transactions are available here

Front-Running as a Service (FRaaS)

- Accelerated transactions use higher input and output values than non-accelerated transactions. Perhaps users have incentives on accelerating high valued transactions.



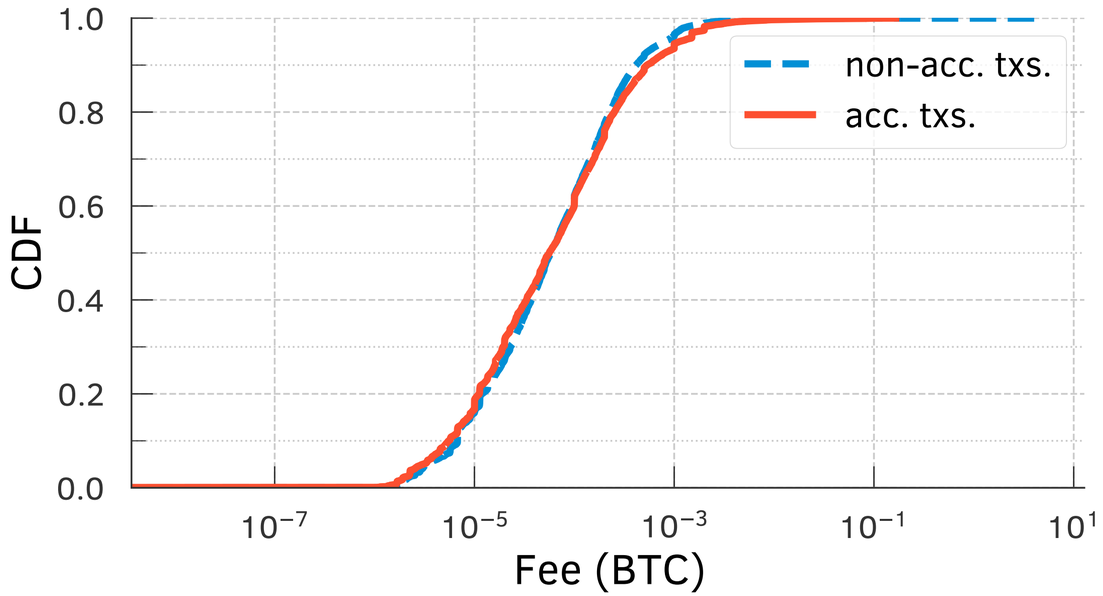


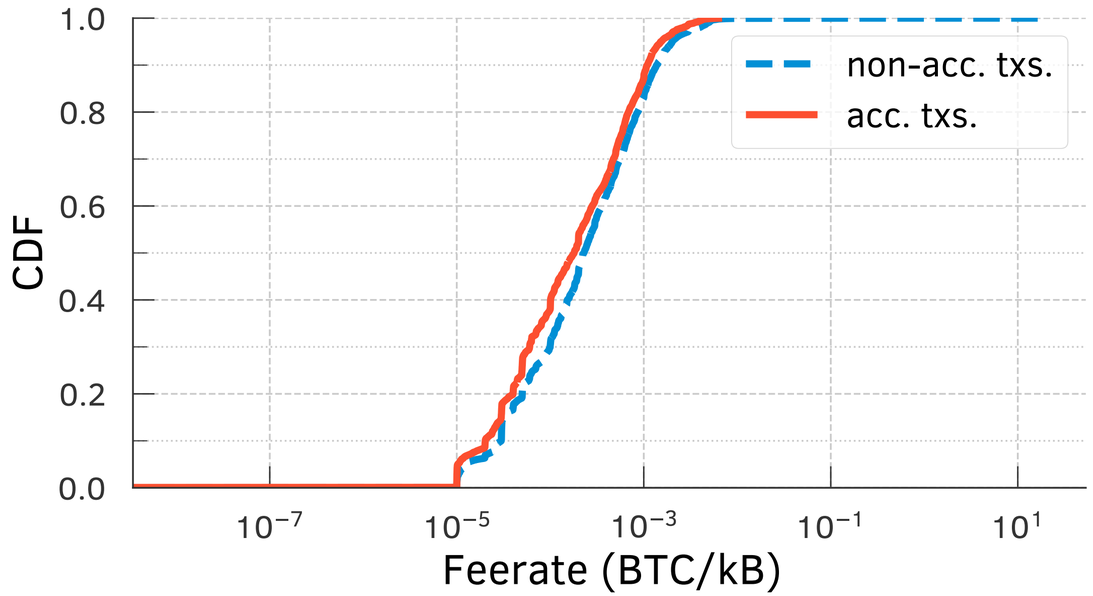
Johnnatan Messias

The accelerated transactions are available here

Front-Running as a Service (FRaaS)

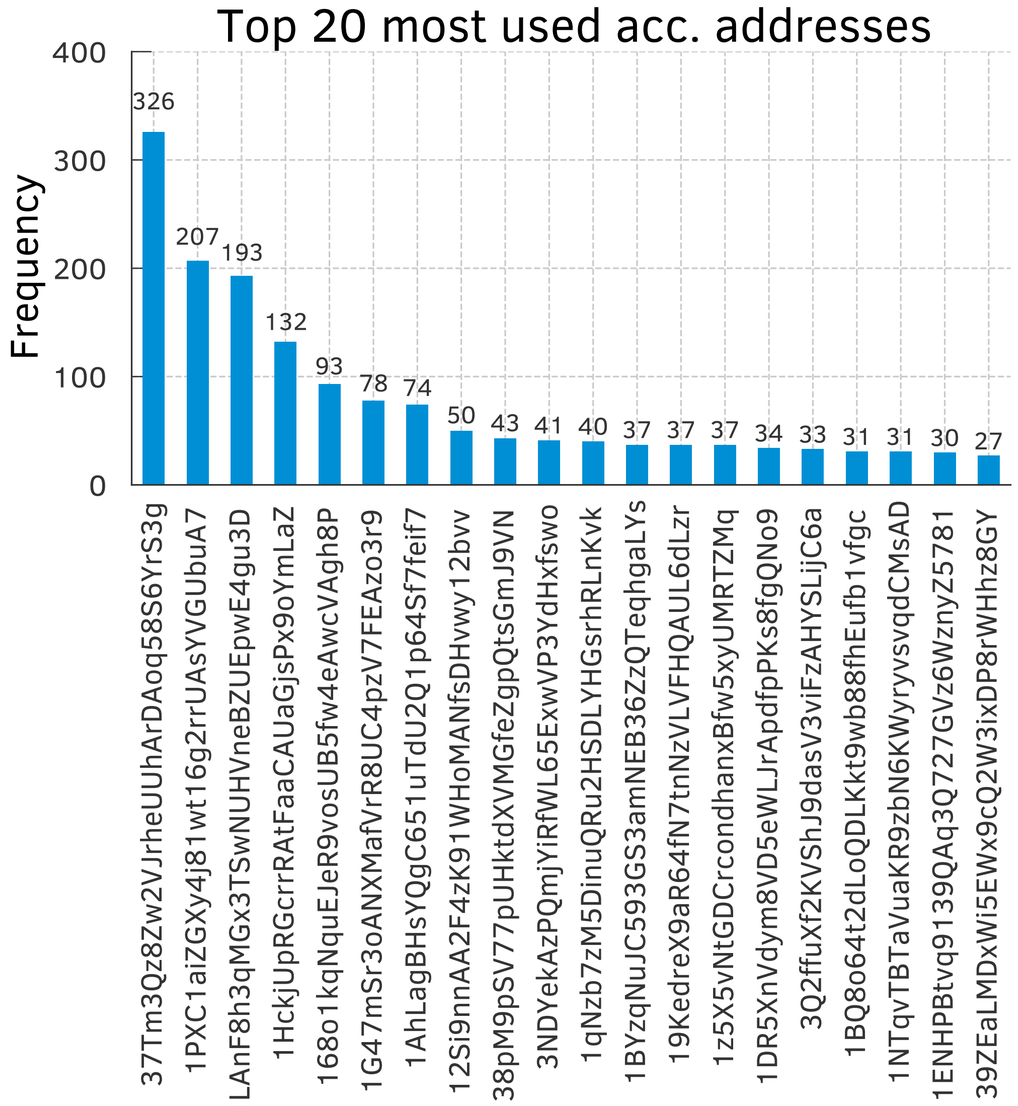
- Non-accelerated transactions offer slightly higher feerate than accelerated transactions

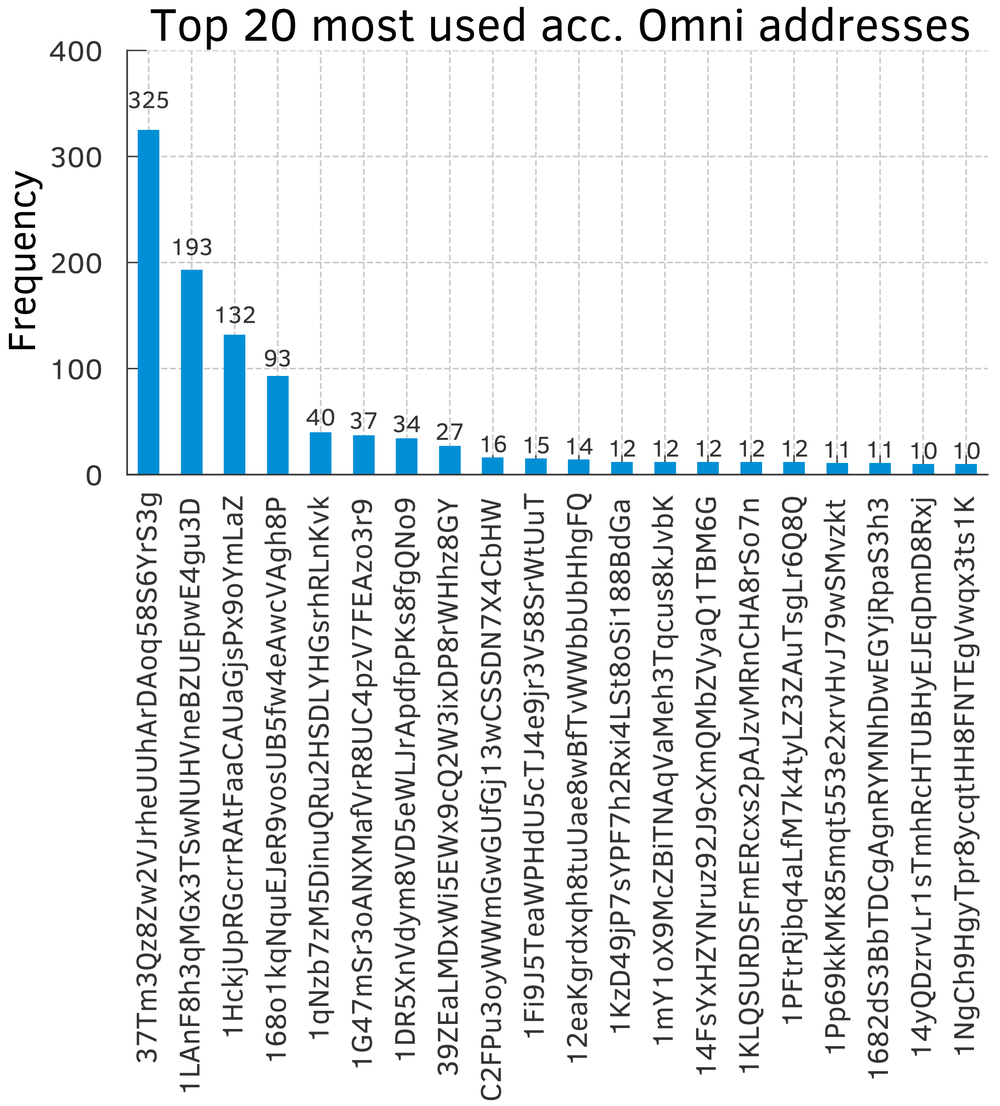




The accelerated transactions are available here

Acc. Transactions addresses





Johnnatan Messias

Selfish & opaque transaction ordering in the Bitcoin blockchain: the case for chain neutrality

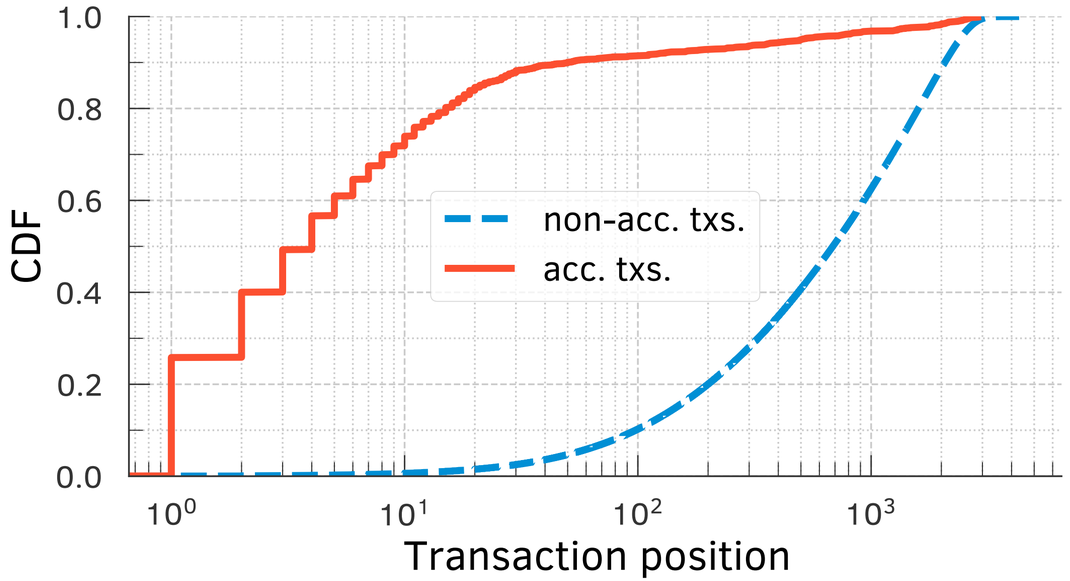
Omni

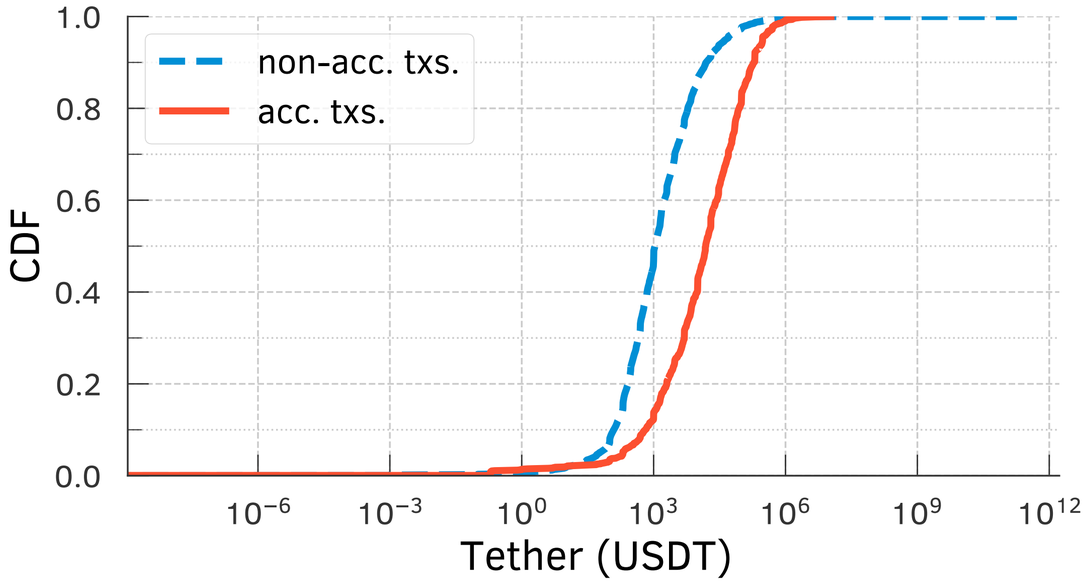
Johnnatan Messias
http://johnnatan.me

This is a complementary analysis of our ACM IMC'21 paper.
Selfish & Opaque Transaction Ordering in the Bitcoin Blockchain: The Case for Chain Neutrality
Johnnatan Messias, Mohamed Alzayat, Balakrishnan Chandrasekaran, Krishna P. Gummadi, Patrick Loiseau, and Alan Mislove.
In Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC 2021). Virtual Event. November, 2021.

Omni transactions

- Also here, accelerated transactions are included on top of the block.
- Accelerated transactions make higher transfers
  - Tx. accelerated median value: 15,274.34 USDT vs Tx. non-Accelerated median value: 1057.30 USDT





Johnnatan Messias

Tether correspond to 97.27% of all Omni transactions