Scaling Bitcoin Operations

John Newbery - Bitcoin Optech

Feb 15, 2019

Scaling Bitcoin Operations

- What is Scaling?
- Why Bitcoin Optech?
- Scaling today
- What’s coming?
- What about fees?

What is scaling?

use the chain for
what the chain is
good for

verify, don’t compute

Verify, don't compute

- Only reveal spending conditions at time of spend
  => P2SH or P2WSH
- Batch multiple payments into one on-chain commitment
  => layer 2 (eg lightning)
- Only reveal the branch of the contract that was executed
  => MAST, Taproot
- In the common case where everyone agrees, only broadcast a single (threshold) signature
  => Taproot, Graftroot
- Combine multiple signatures into a single signature
  => threshold signatures, MuSig
- Embed additional conditions/commitments invisibly into digital signatures
  => adaptor signatures and scriptless scripts

the invisible hand

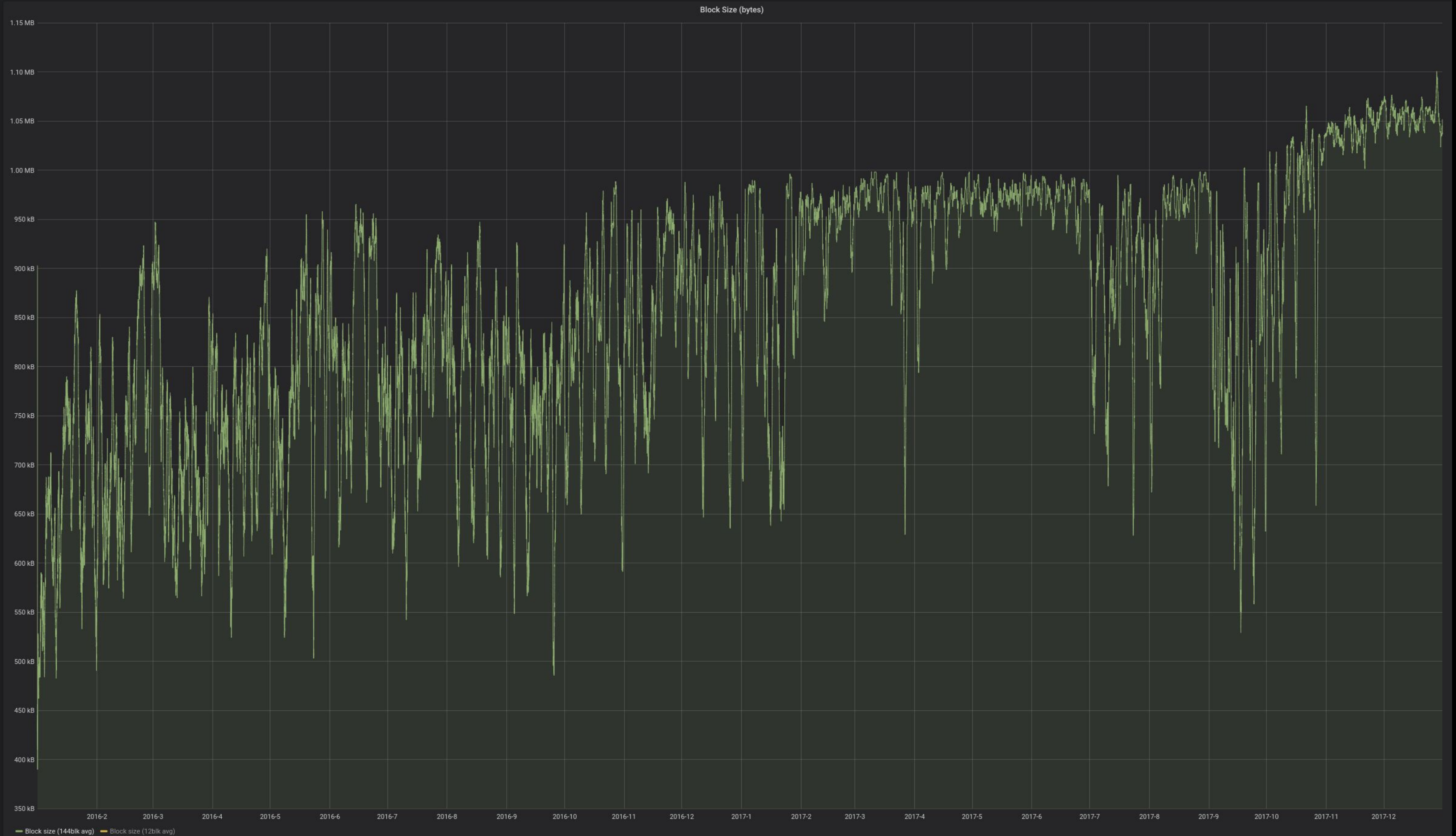
the invisible hand

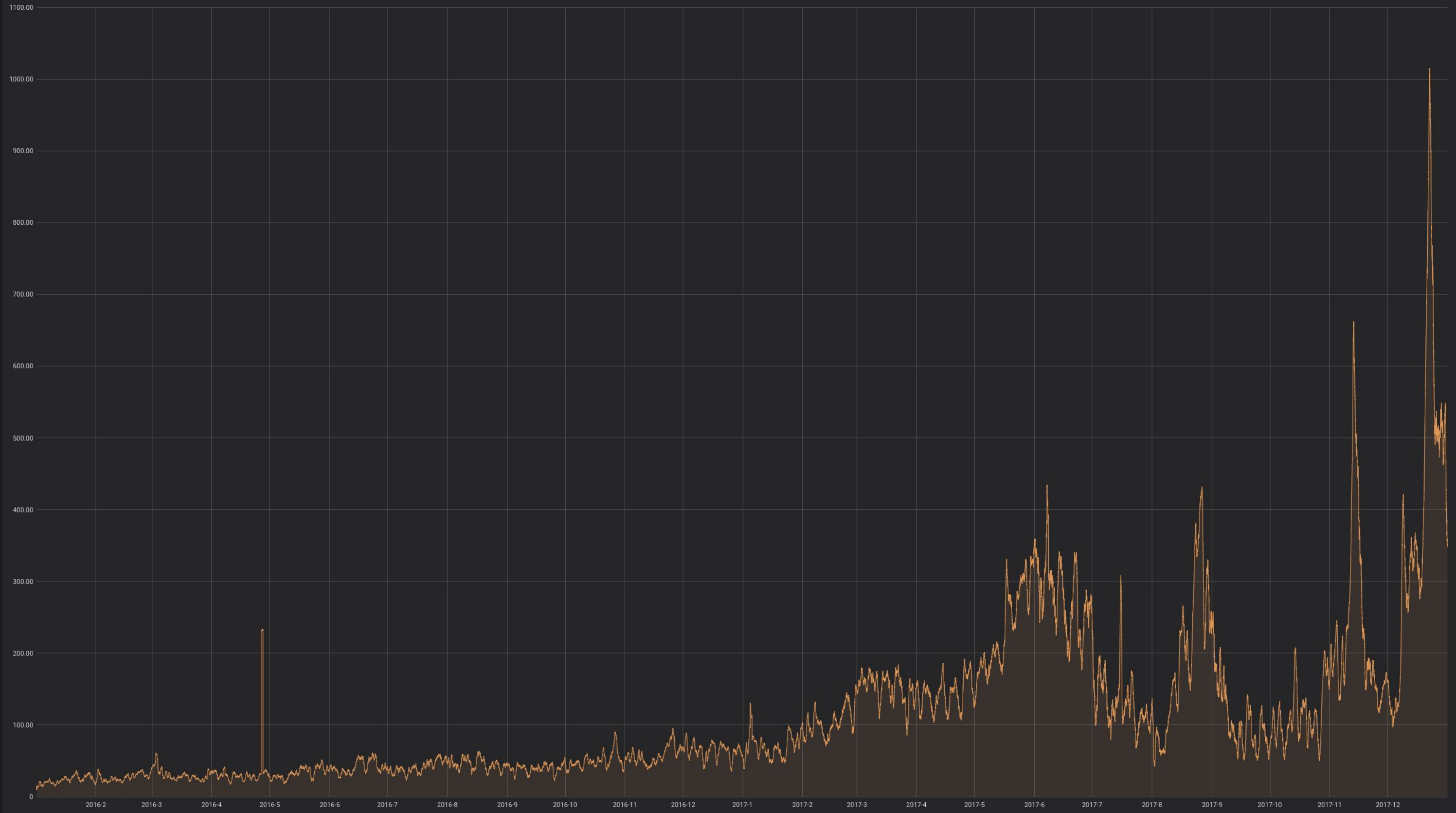
- Bitcoin incentivizes users to act efficiently
- Block space is a scarce resource
- The fee market helps allocate that resource to those who value it most
- The fee market can only work when blocks are full

Why no supersize blocks?

- Destroys decentralization
- Can never be large enough
- Destroys the fee market - removes incentive to implement optimizations
- Who decides?

Why Bitcoin Optech?

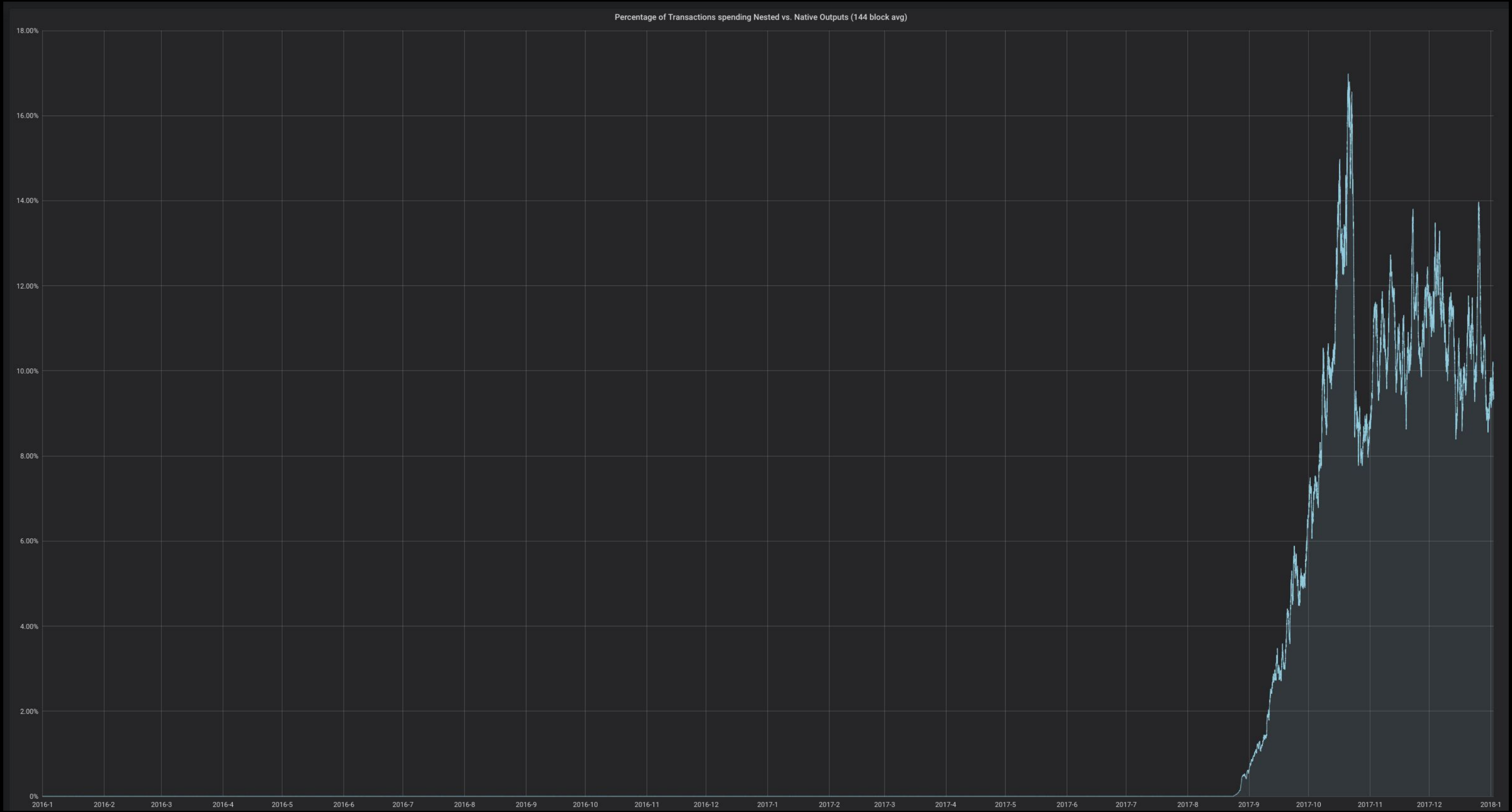

Block Size (bytes)
1.15 MB
1.10 MB
1.05 MB
1.00 MB
950 kB
900 kB
850 kB
800 kB
750 kB
700 kB
650 kB
600 kB
550 kB
500 kB
450 kB
400 kB
350 kB
2016-2
2016-3
2016-4
2016-5
2016-6
2016-7
2016-8
2016-9
2016-10
2016-11
2016-12
2017-1
2017-2
2017-3
2017-4
2017-5
2017-6
2017-7
2017-8
2017-9
2017-10
2017-11
2017-12
Block size (144blk avg)
Block size (12blk avg)



Total Fee (in BTC)

2017

- Intense fee pressure at end of year
- Low segwit usage
- Many exchanges not batching
- Lots of low hanging fruit


Percentage of Transactions spending Nested vs. Native Outputs (144 block avg)
18.00%
16.00%
14.00%
12.00%
10.00%
8.00%
6.00%
4.00%
2.00%
0%
2016-1
2016-2
2016-3
2016-4
2016-5
2016-6
2016-7
2016-8
2016-9
2016-10
2016-11
2016-12
2017-1
2017-2
2017-3
2017-4
2017-5
2017-6
2017-7
2017-8
2017-9
2017-10
2017-11
2017-12
2018-1

What we're doing

- Engage companies
- Hold workshops
- Weekly newsletter
- Scaling book
- Exec briefing
- Dashboard
- Future scaling opportunities

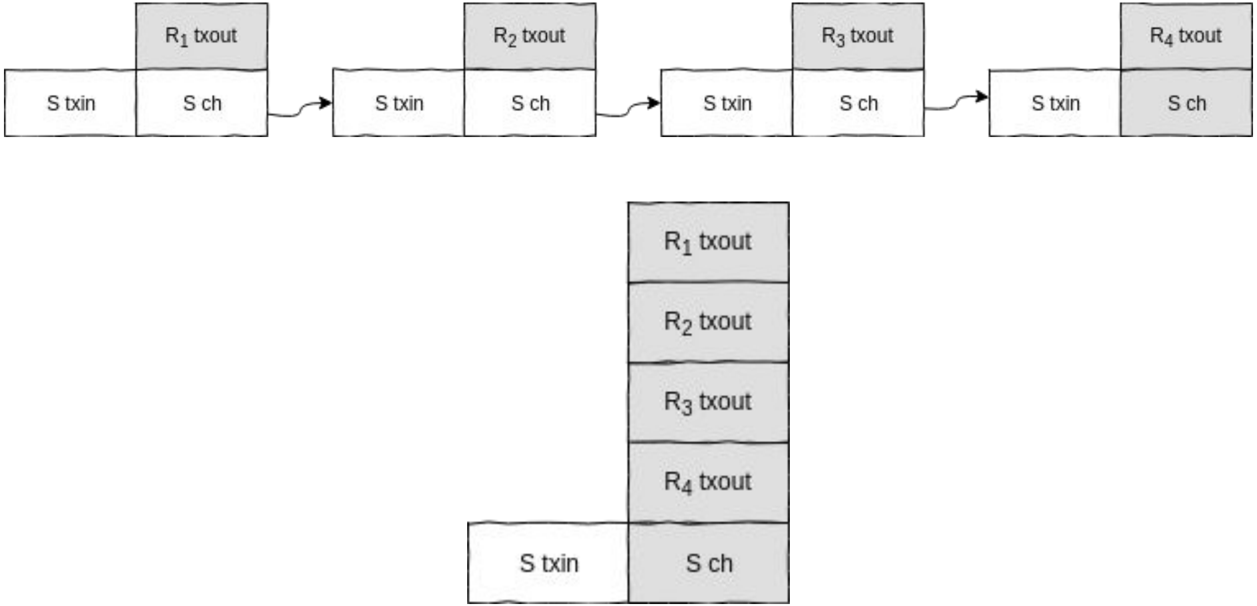
How can we scale today?

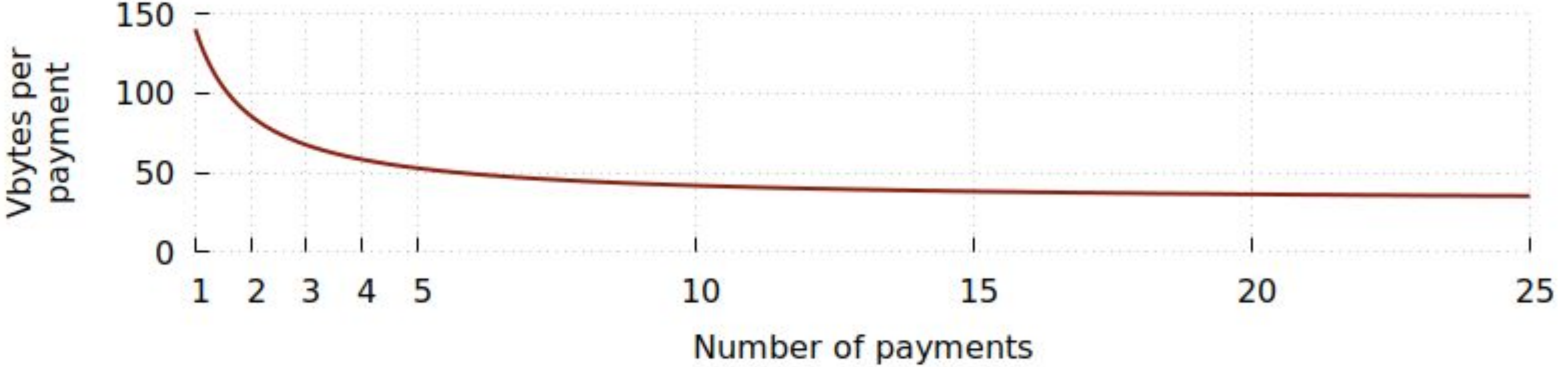
Scaling today

- Payment batching
- Segwit
- Patient spending
- Others

https://en.bitcoin.it/wiki/Techniques_to_reduce_transaction_fees

Payment Batching




150
100
50
0
Vbytes per payment
1
2
3
4
5
10
15
20
25
Number of payments

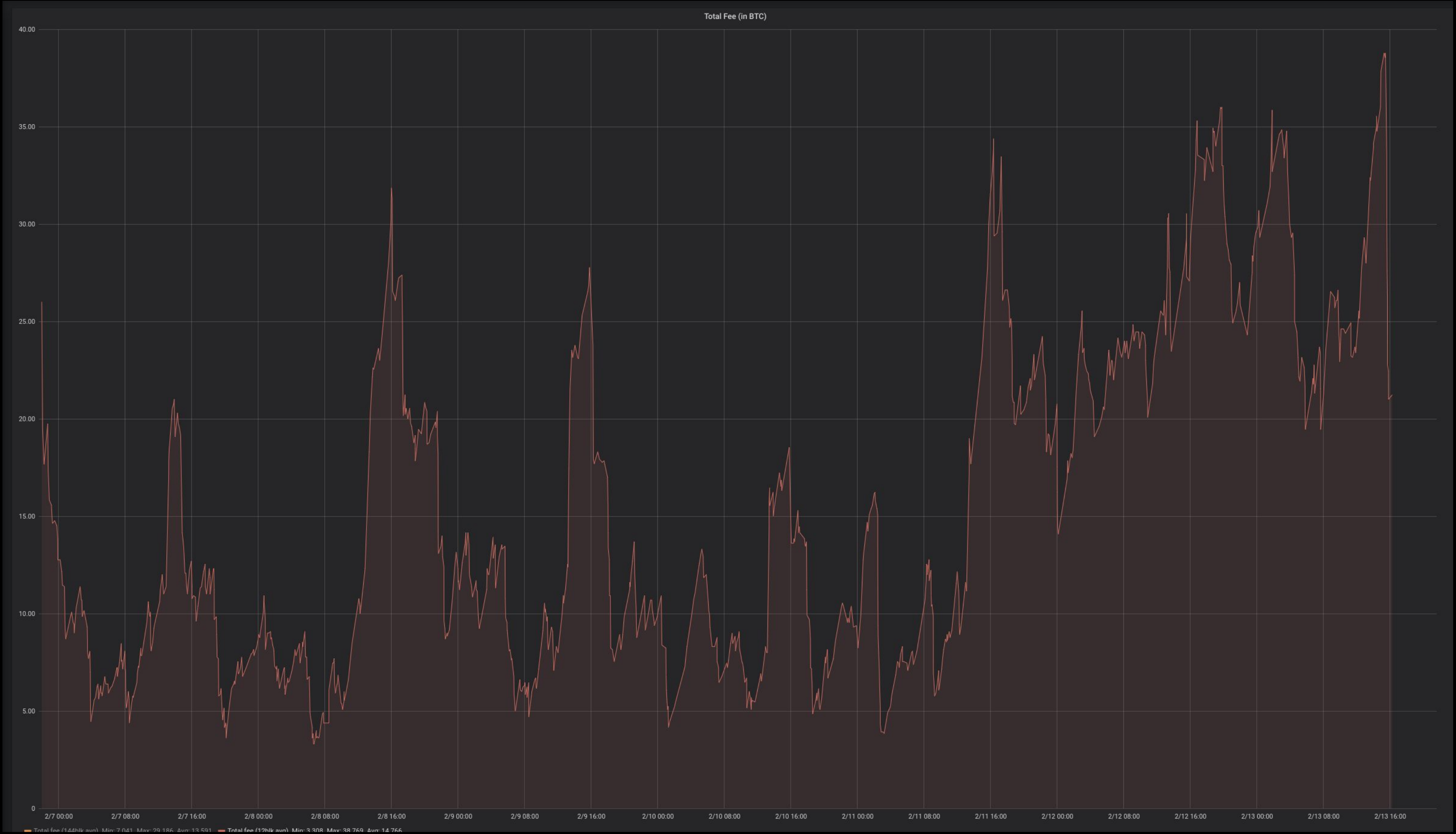
Segwit

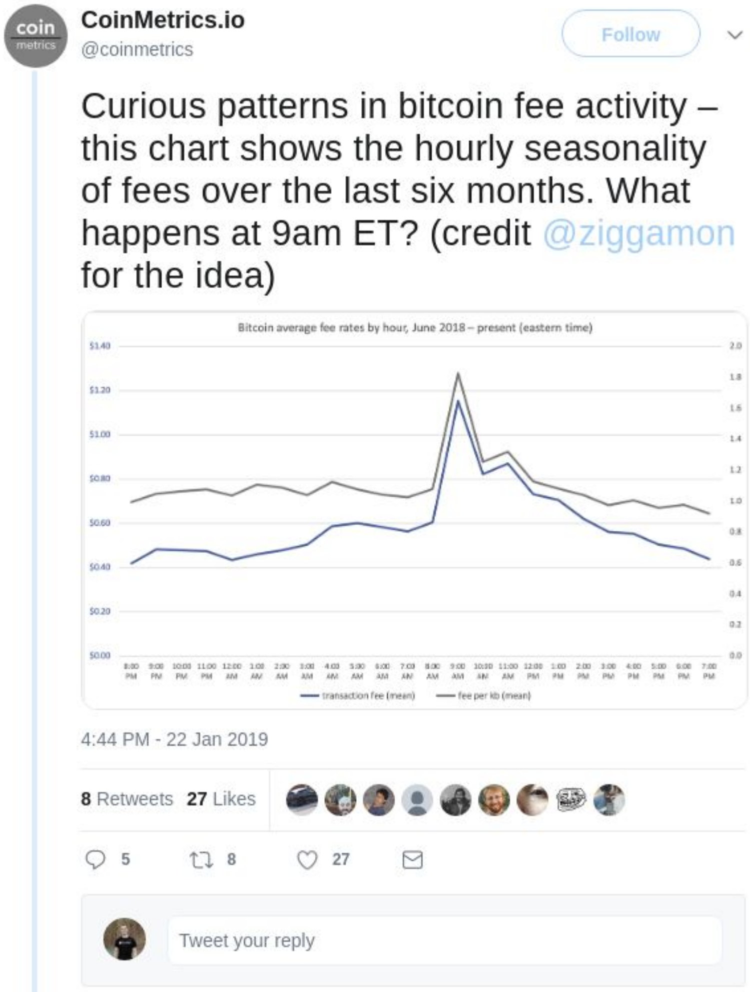
- Rebalances fee *weight* to add onchain capacity
- Incentivizes consuming UTXOs over creating UTXOs
- Can be *native* segwit or *P2SH-wrapped* segwit

Type	**Legacy vbytes**	**P2SH-wrapped segwit vbytes**	**Savings**	**Native segwit vbytes**	**Savings**
Single signature	226	167	26%	141	37%
2-of-2	335	197	41%	169	50%
2-of-3	365	206	44%	178	51%
3-of-4	469	233	50%	205	56%

Patient spending

- Use high fees when confirmation time is urgent, low fee otherwise
- Make on-chain payments when others aren’t
- Spread out payments
- Set expectations!


Total Fee (in BTC)
40.00
35.00
30.00
25.00
20.00
15.00
10.00
5.00
0
2/7 00:00
2/7 08:00
2/7 16:00
2/8 00:00
2/8 08:00
2/8 16:00
2/9 00:00
2/9 08:00
2/9 16:00
2/10 00:00
2/10 08:00
2/10 16:00
2/11 00:00
2/11 08:00
2/11 16:00
2/12 00:00
2/12 08:00
2/12 16:00
2/13 00:00
2/13 08:00
2/13 16:00
Total fee (144blk avg) Min: 7.041 Max: 29.186 Avg: 13.591
Total fee (12blk avg) Min: 3.308 Max: 38.769 Avg: 14.766



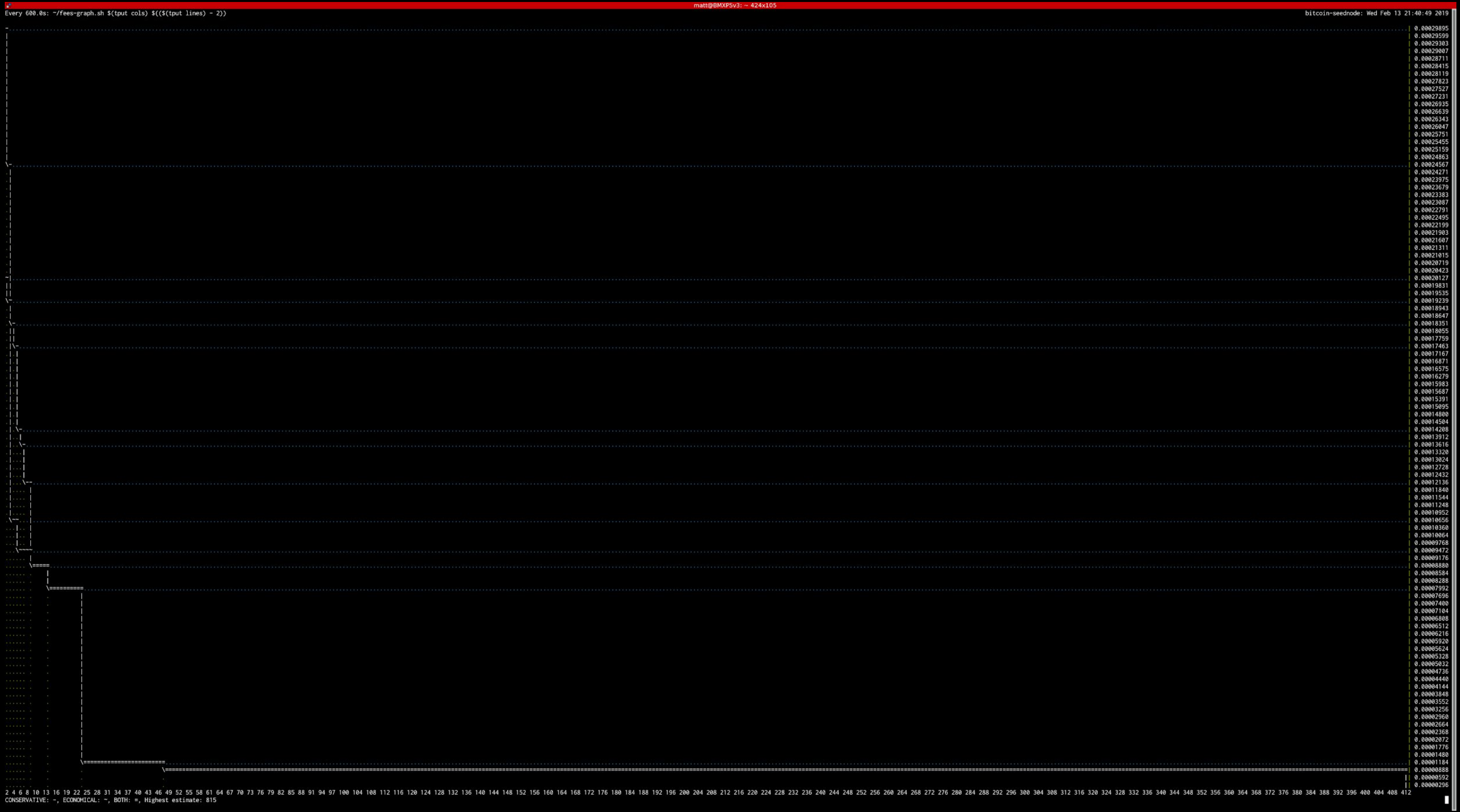
CoinMetrics.io
@coinmetrics

Curious patterns in bitcoin fee activity – this chart shows the hourly seasonality of fees over the last six months. What happens at 9am ET? (credit @ziggamon for the idea)

4:44 PM - 22 Jan 2019

8 Retweets **27** Likes

5 8 27



```
matt@BMXPSv3: ~ 424x105
Every 600.0s: ~/fees-graph.sh $(tput cols) $(($(tput lines) - 2))                bitcoin-seednode: Wed Feb 13 21:40:49 2019
```

```
| 0.00029895
| 0.00029599
| 0.00029303
| 0.00029007
| 0.00028711
| 0.00028415
| 0.00028119
| 0.00027823
| 0.00027527
| 0.00027231
| 0.00026935
| 0.00026639
| 0.00026343
| 0.00026047
| 0.00025751
| 0.00025455
| 0.00025159
| 0.00024863
| 0.00024567
| 0.00024271
| 0.00023975
| 0.00023679
| 0.00023383
| 0.00023087
| 0.00022791
| 0.00022495
| 0.00022199
| 0.00021903
| 0.00021607
| 0.00021311
| 0.00021015
| 0.00020719
| 0.00020423
| 0.00020127
| 0.00019831
| 0.00019535
| 0.00019239
| 0.00018943
| 0.00018647
| 0.00018351
| 0.00018055
| 0.00017759
| 0.00017463
| 0.00017167
| 0.00016871
| 0.00016575
| 0.00016279
| 0.00015983
| 0.00015687
| 0.00015391
| 0.00015095
| 0.00014800
| 0.00014504
| 0.00014208
| 0.00013912
| 0.00013616
| 0.00013320
| 0.00013024
| 0.00012728
| 0.00012432
| 0.00012136
| 0.00011840
| 0.00011544
| 0.00011248
| 0.00010952
| 0.00010656
| 0.00010360
| 0.00010064
| 0.00009768
| 0.00009472
| 0.00009176
| 0.00008880
| 0.00008584
| 0.00008288
| 0.00007992
| 0.00007696
| 0.00007400
| 0.00007104
| 0.00006808
| 0.00006512
| 0.00006216
| 0.00005920
| 0.00005624
| 0.00005328
| 0.00005032
| 0.00004736
| 0.00004440
| 0.00004144
| 0.00003848
| 0.00003552
| 0.00003256
| 0.00002960
| 0.00002664
| 0.00002368
| 0.00002072
| 0.00001776
| 0.00001480
| 0.00001184
| 0.00000888
| 0.00000592
| 0.00000296
2 4 6 8 10 13 16 19 22 25 28 31 34 37 40 43 46 49 52 55 58 61 64 67 70 73 76 79 82 85 88 91 94 97 100 104 108 112 116 120 124 128 132 136 140 144 148 152 156 160 164 168 172 176 180 184 188 192 196 200 204 208 212 216 220 224 228 232 236 240 244 248 252 256 260 264 268 272 276 280 284 288 292 296 300 304 308 312 316 320 324 328 332 336 340 344 348 352 356 360 364 368 372 376 380 384 388 392 396 400 404 408 412
CONSERVATIVE: -, ECONOMICAL: ~, BOTH: =, Highest estimate: 815
```

Other fee saving techniques

- Coin selection
- Fee estimation
- UTXO consolidation / adaptive coin selection
- Fee-bumping (RBF and CPFP)

https://en.bitcoin.it/wiki/Techniques_to_reduce_transaction_fees

What’s coming?

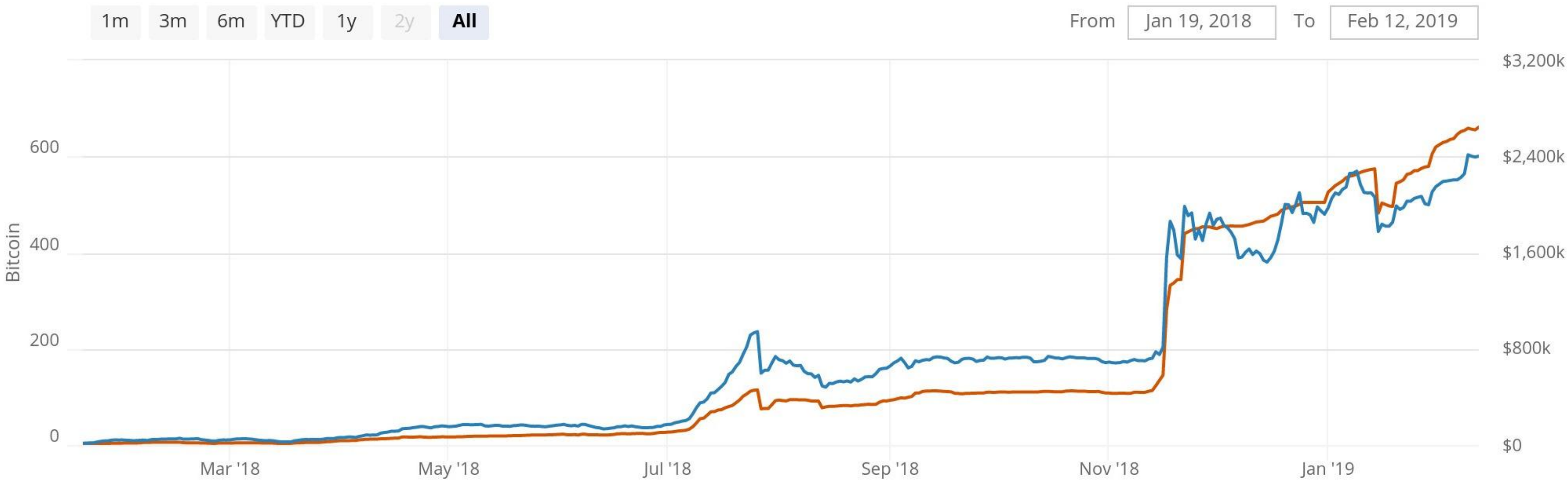
What’s coming

- Lightning
- Schnorr
- Threshold Signatures / MuSig
- Taproot

Lightning

Lightning

- ‘Layer 2’ payment network
- Many payments can be made between participants with minimal activity on the blockchain
- Over $2.5M capacity and increasing



From Jan 19, 2018 To Feb 12, 2019

Schnorr signatures

Schnorr signatures

- Slightly smaller encoding than DER encoding (64 bytes -vs- 72 bytes)
- Uses same elliptical curve and compatible with existing private keys
- Has same assumption as ECDSA of hard discrete log problem
- Unlike ECDSA, has a security proof
- Schnorr signatures are *linear* in the components of the signature (s,R) and can be added:

  $s_1G = R_1 + eP_1$

  $s_2G = R_2 + eP_2$

  $(s_1 + s_2)G = (R_1 + R_2) + e(P_1 + P_2)$

Schnorr signature linearity

- n-of-n multisig can be replaced by a single public key / signature
- Enables many other innovations:
  - Scriptless Scripts
  - Taproot
  - Musig
  - Graftroot
- (With more consensus changes):
  - Enables signature aggregation
  - Enables batch validation

threshold signatures and MuSig

Threshold Signatures and MuSig

- MuSig is a multi-signature scheme that aggregates keys
- Any n-of-n or k-of-n multisignature at the cost of 1 signature
- n-of-n does not require interactivity during key setup (assuming all parties know pubkeys)
- k-of-n is an interactive protocol requiring 3 rounds when signing
- Lots of active research!

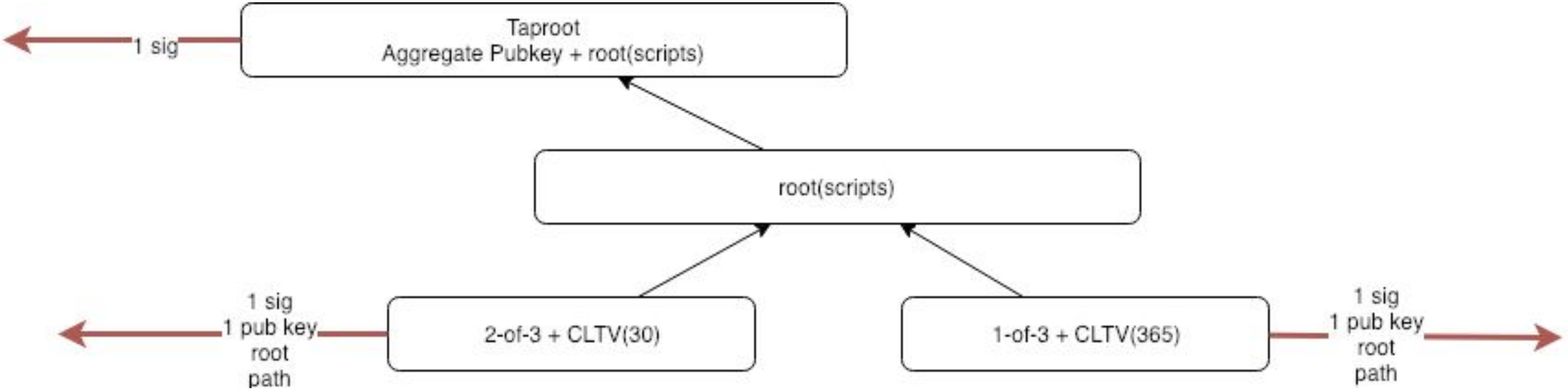
Taproot

MAST and Taproot

- Bitcoin script encumbers transaction outputs with spending conditions
- P2SH encumbers a transaction output with a commitment to spending conditions
- MAST encumbers a transaction output with a commitment to one of several spending conditions
- Taproot places the MAST commitment into a (tweaked) pubkey
    - In the common case, everyone signs and there's only one (tweaked) signature
    - In non-cooperative case, provide:
        - Tweak
        - Untweaked pubkey
        - Merkle proof to branch
        - Spending conditions

Taproot example

- Steve, Mike and I hold private keys.
- We create an output that can be spent by:
  - All three of us signing (common case)
  - Two of us signing if one month has passed
  - One of us signing if a year has passed



1 sig

Taproot
Aggregate Pubkey + root(scripts)

root(scripts)

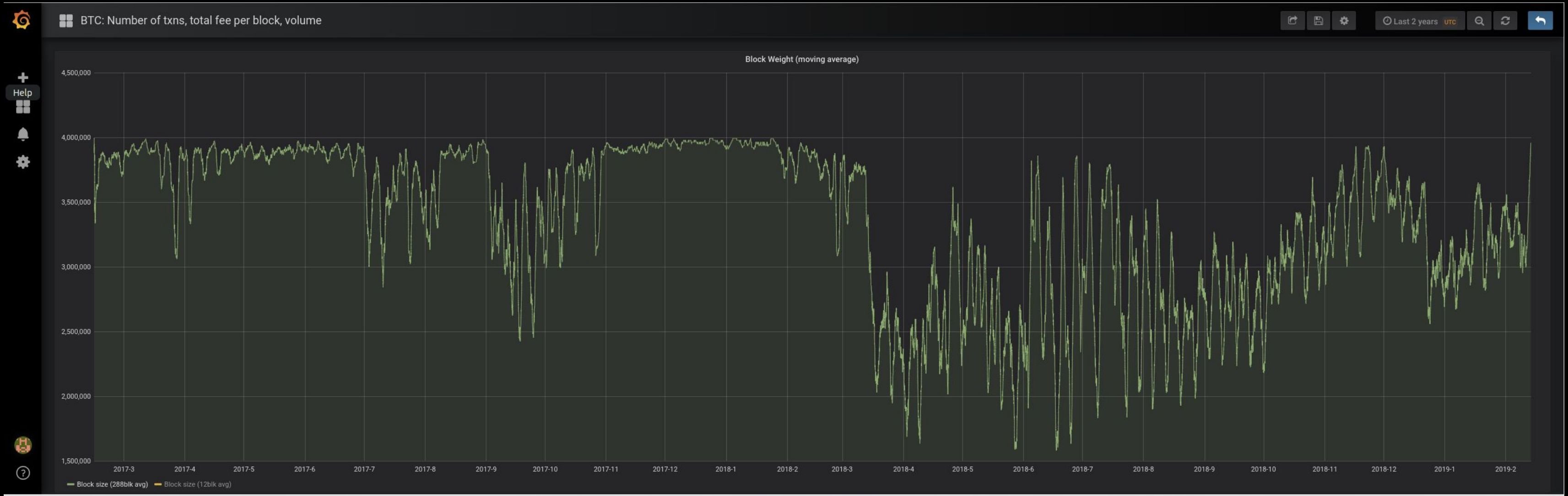
1 sig
1 pub key
root
path

2-of-3 + CLTV(30)

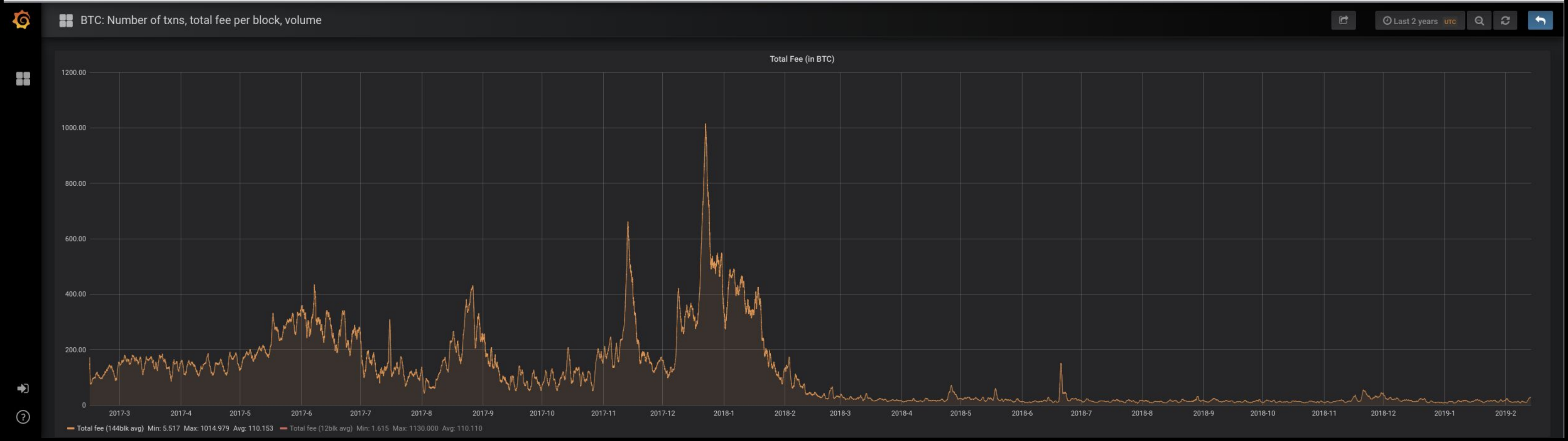
1-of-3 + CLTV(365)

1 sig
1 pub key
root
path

What about fees?

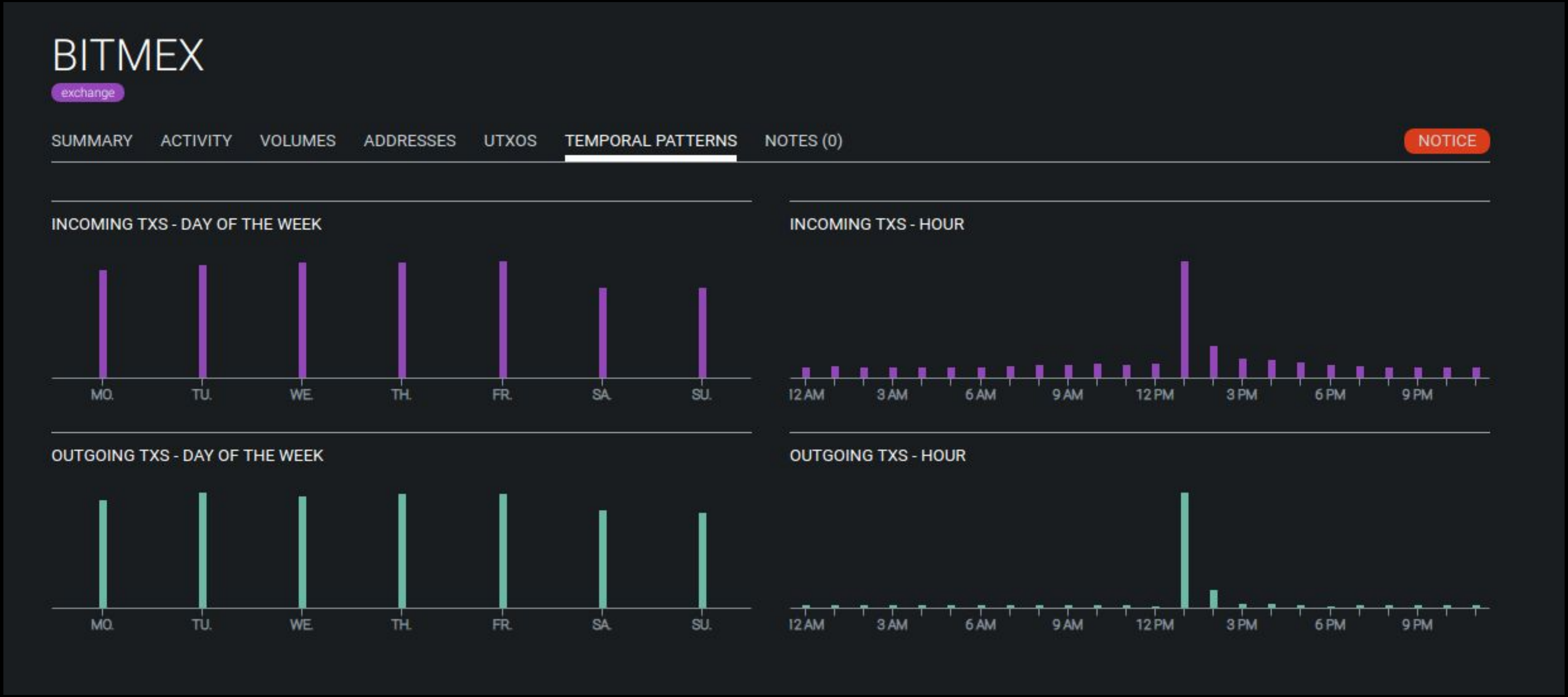


BTC: Number of txns, total fee per block, volume



BTC: Number of txns, total fee per block, volume

https://www.oxt.me/entity/bitmex



Questions?