

Monitoring Bitcoin mining pool transaction selection

Can we detect transaction censorship by mining pools?



0xB10C

Bitcoin Developer

supported by a brink.dev grant

MIT Bitcoin Expo 2022

March 30, 2021 5:43pm EDT

Marathon to Produce Bitcoin that is Fully AML and OFAC Compliant by Exclusively Processing Transactions that Meet U.S. Regulatory Standards

[..] To set up its pool, Marathon has exclusively licensed technology from DMG Blockchain that allows the Company to filter transactions. [..]

Marathon Digital Holdings press release from March 30th, 2021

<https://ir.marathondh.com/news-events/press-releases/detail/1233/correction-marathon-digital-holdings-to-launch-the-first>

Censorship Resistance of Bitcoin

No one should be able to

- prevent others from interacting with the Bitcoin network
- indefinitely* block a valid transaction from being confirmed

Censorship Resistance of Bitcoin

No one should be able to

- prevent others from interacting with the Bitcoin network
- indefinitely* block a valid transaction from being confirmed

* mining pools can freely choose not to confirm a transaction

* transactions paying a competitive fee should confirm eventually

Censorship Resistance of Bitcoin

No one should be able to

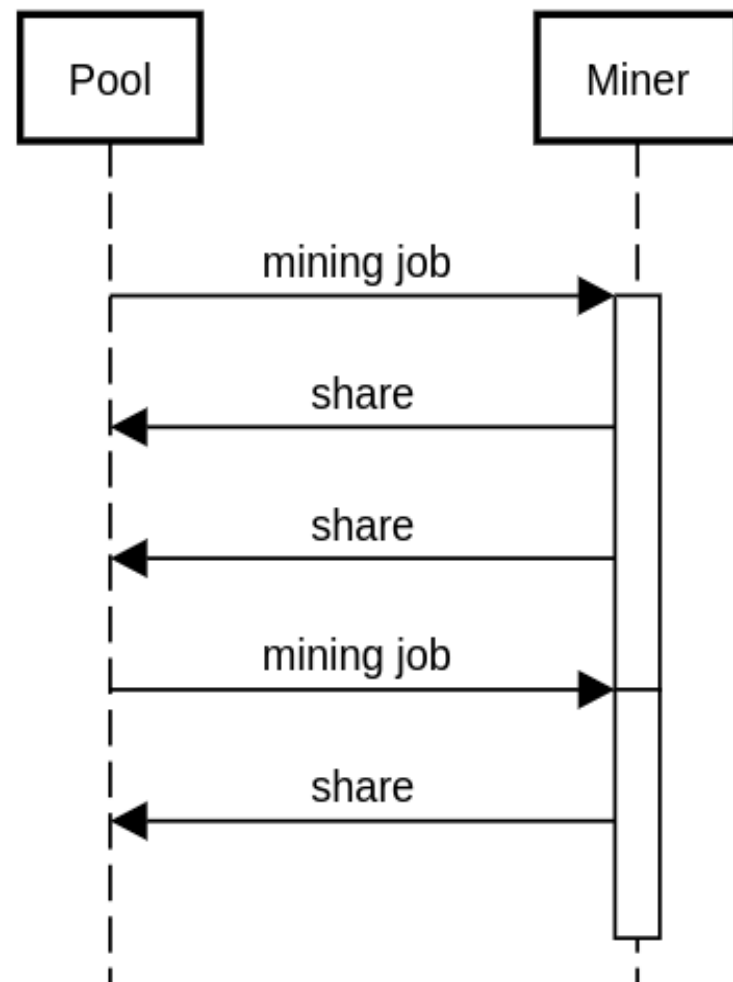
- prevent others from interacting with the Bitcoin network
- indefinitely* block a valid transaction from being confirmed

* mining pools can freely choose not to confirm a transaction

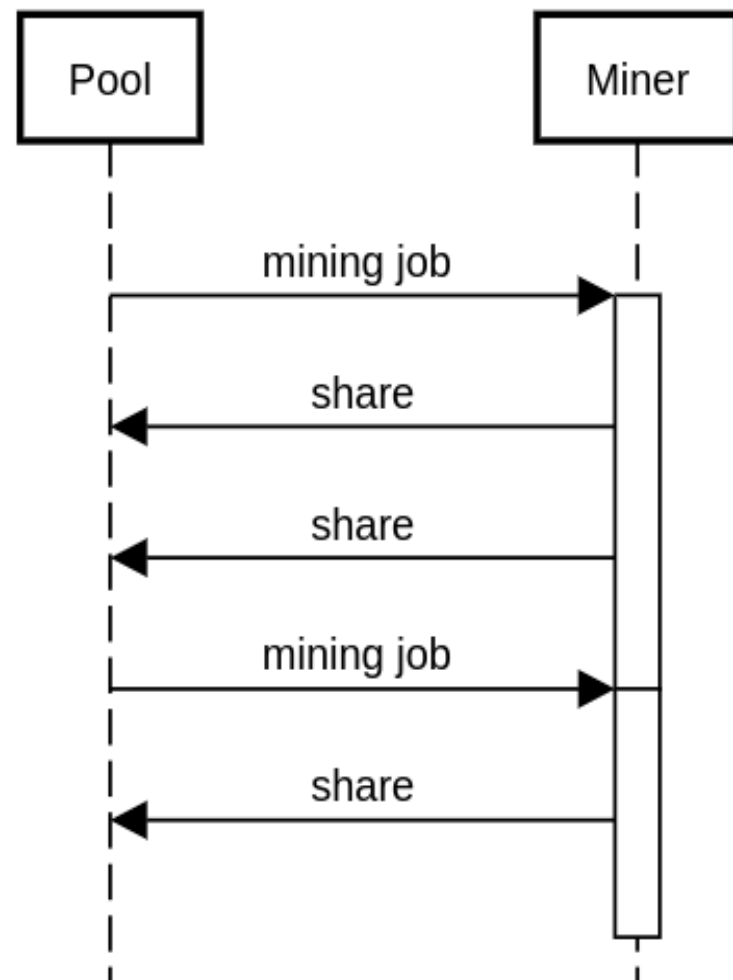
* transactions paying a competitive fee should confirm eventually

Can we detect transaction censorship by mining pools?

Pooled Bitcoin Mining: Stratum V1

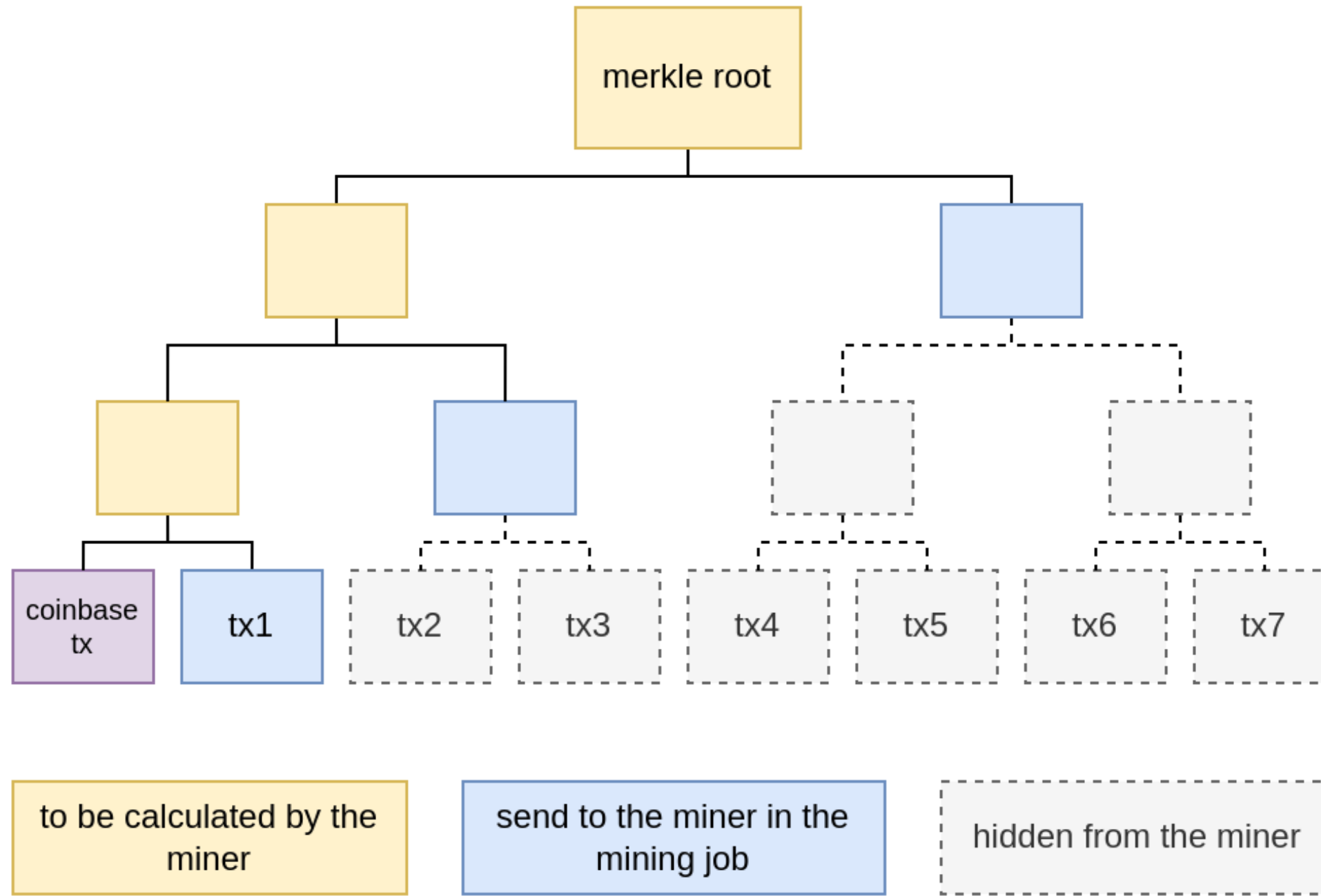


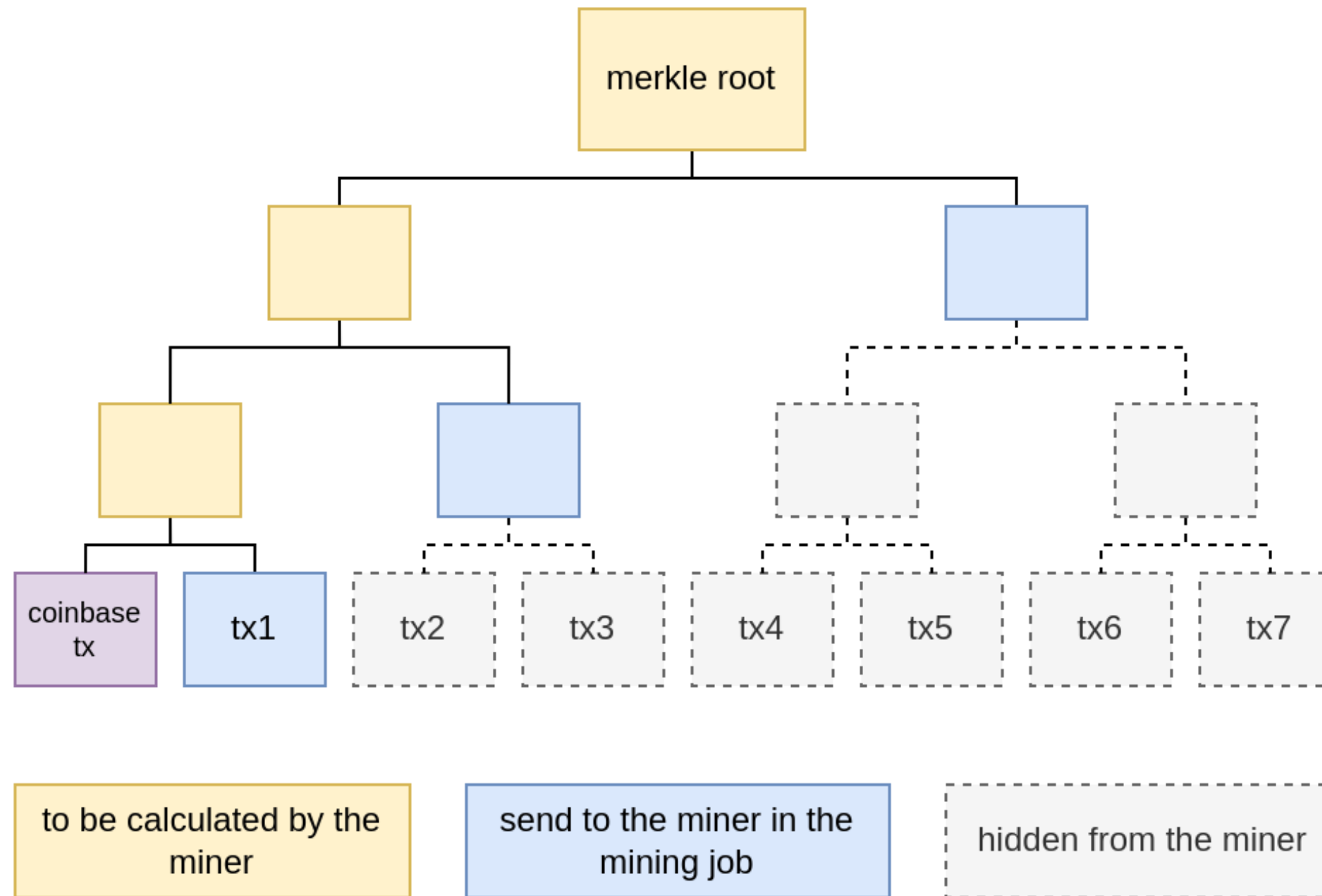
Pooled Bitcoin Mining: Stratum V1



mining jobs contain the information needed to construct a block header

- metadata: job id, clean jobs flag
- block version, bits, time
- previous block hash
- coinbase transaction in two parts
- branches of the transaction merkle tree





Miners don't know which transactions they are mining

May 05, 2021 4:00pm EDT

Company Successfully Directs all of its Hashrate to the Marathon OFAC Pool, the First North American-Based Bitcoin Mining Pool, Fully Compliant with U.S. Regulations

LAS VEGAS, May 05, 2021 (GLOBE NEWSWIRE) -- **Marathon Digital Holdings, Inc.** (**NASDAQ:MARA**) ("**Marathon**" or "**Company**"), one of the largest enterprise Bitcoin self-mining companies in North America, has successfully directed all of its hashrate to the Marathon OFAC Pool, Marathon's recently launched mining.pool [..]

Marathon Digital Holdings press release from May 5th, 2021

<https://ir.marathondh.com/news-events/press-releases/detail/1239/marathon-digital-holdings-becomes-the-first-north-american>

Block < 682170 >

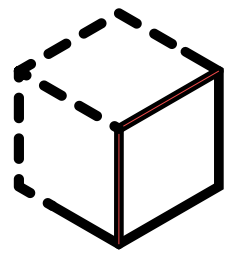
Hash	000000...fef8777 	Total fees	0.05 BTC \$2,056
Timestamp	2021-05-06 06:50 (1 year ago)	Subsidy + fees:	6.30 BTC \$254,272
Size	2.32 MB	Miner	MARA Pool
Weight	3.99 MWU		

9f6f1a8e55623aa320f430f9e3c6dc762c147035e713b96d72c20a58cf45fbbf

2021-05-06 06:50

→ Coinbase (Newly Generated Coins)	3LC8dDKyBsrWPfzhXyt7aAyjXxGYkfDdHu	6.30095356 BTC →
<div>h 8\ MARA Pool - OFAC Compliant Block \A[p.</div>	OP_RETURN !+%x1Xcنg\$	0.00000000 BTC →
		6.30095356 BTC

https://mempool.space/block/000000000000000000000003f8cb66fe1ecfb38754abc9c4d4a62b71de45fef8777

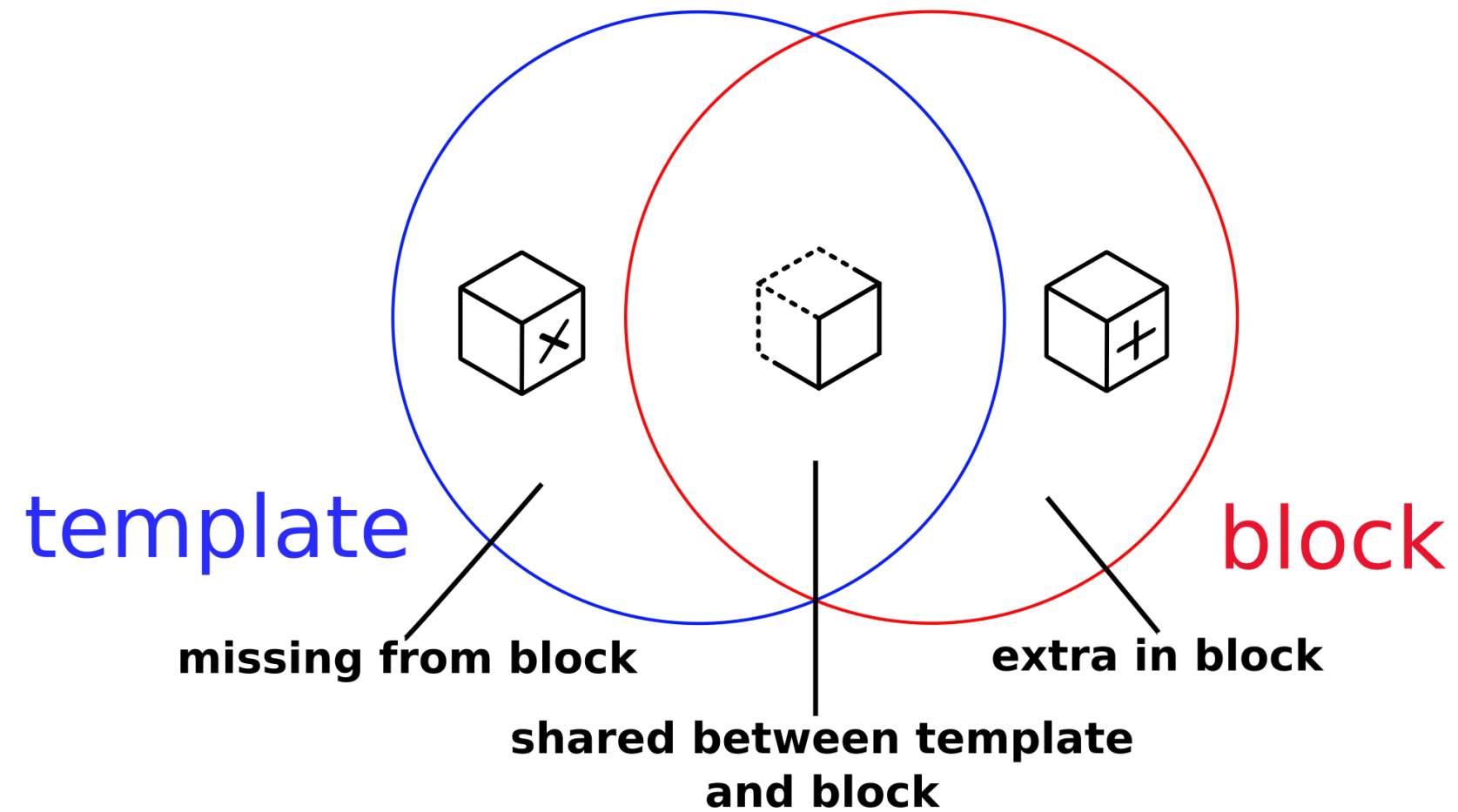


miningpool-observer

Transparency for Mining Pool Transaction Selection

source on github.com/0xB10C/miningpool-observer
live on miningpool.observer


Comparing templates and blocks





First MARA Pool block on miningpool-observer


Template & Block 00000000000000000000000003f8cb66fe1ecfb38754abc9c4d4a62b71de45fef8777


mined by	MARA Pool	height	682170
coinbase reward	6.30095356 BTC	last package feerate	3.02 sat/vByte
weight	3993.01kWU	full	99.83%
seen time	2021-05-06 04:50:25 UTC	parent block	goto parent block

 Template	
transactions	171
packages	170
fees	0.0539021 BTC
creation time	2021-05-06 04:50:13 UTC

 Block	
transactions	178 (+7)
packages	177 (+7)
fees	0.05095356 BTC (-2.94854 mBTC)
miner-set time	2021-05-06 04:50:11 UTC

 5 missing transactions

 166 shared transactions

 12 extra transactions

3 mBTC ≈ 120 USD @ \$40k USD/BTC

<https://miningpool.observer/template-and-block/00000000000000000000000003f8cb66fe1ecfb38754abc9c4d4a62b71de45fef8777>



Missing Transactions (5)

Transactions only included in the Template

Young

RBF signaling

OP_RETURN

▶ 1da708266cf8e21adbf77a96593c4764a250d185b4e60...

fee	49000 sat	feerate	141.22 sat/vByte
vsize	347 vByte	output sum	0.78636814 BTC
inputs	▶ 1	outputs	▶ 4
mempool age	12s		
transaction position in template (8 of 171)			
<div></div>			

Young

▶ 7a77e111b02a49b21eb01da459aaf90ab740c9349fc65...

fee	20050 sat	feerate	106.65 sat/vByte
vsize	188 vByte	output sum	0.00188496 BTC
inputs	▶ 1	outputs	▶ 1
mempool age	12s		
transaction position in template (18 of 171)			
<div></div>			

Young

Large

SegWit spending

▶ a6cd71e80f608b39f40a9743faf2e3cbad3b2582468c8...

fee	231552 sat	feerate	86.63 sat/vByte
vsize	2673 vByte	output sum	8.10502242 BTC



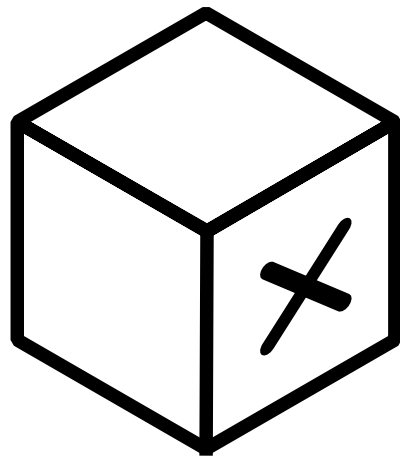
Extra Transactions (12)

Transactions only included in the Block

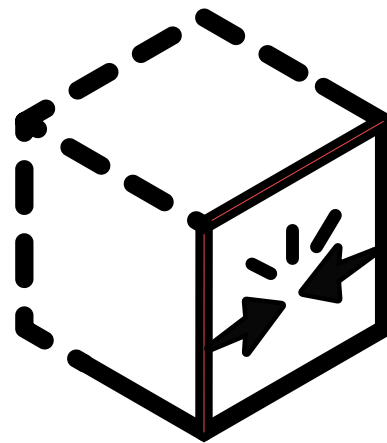
Coinbase RBF signaling OP_RETURN			
▶ 9f6f1a8e55623aa320f430f9e3c6dc762c147035e713b...			
fee	0 sat	feerate	0 sat/vByte
vsize	200 vByte	output sum	6.30095356 BTC
inputs	▶ 1	outputs	▶ 2
transaction position in block (1 of 178)			
<div></div>			
SegWit spending Multisig spending RBF signaling Height-Locked			
▶ 8f4a22ff816ba593a38168e7e0f5b8578a52dc788ac06...			
fee	1017 sat	feerate	3.02 sat/vByte
vsize	337 vByte	output sum	0.01118431 BTC
inputs	▶ 2	outputs	▶ 2
transaction position in block (168 of 178)			
<div></div>			
RBF signaling Height-Locked			
▶ d410c73b7ea0264a1f89c2104a79a53b85ed1b51a29de...			
fee	1020 sat	feerate	3.02 sat/vByte
vsize	338 vByte	output sum	0.0000708 BTC
inputs	▶ 2	outputs	▶ 1
transaction position in block (169 of 178)			
<div></div>			

<https://miningpool.observer/template-and-block/000000000000000000000003f8cb66fe1ecfb38754abc9c4d4a62b71de45fef8777>

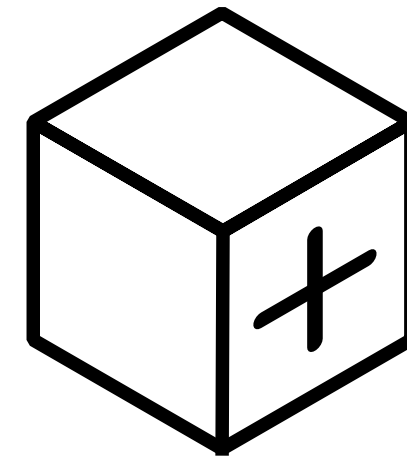
Mining Pool Transaction Selection Observations



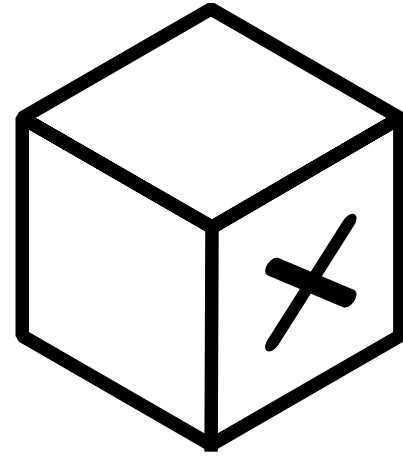
transactions missing
from multiple blocks



conflicts between
blocks and
templates

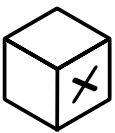


extra transactions
included by pools



Why are transactions sometimes missing from blocks?

- transaction not propagated well enough yet
- other transactions were prioritized
- conflicts with other transactions
- transaction was filtered



Missing P2TR spends

miningpool.observer/missing/3d1e1215d126d9674ca3351092709ea63663eeea56c175cc7123b64a68a27a41

Missing Transaction 3d1e1215d126d9674ca3351092709ea63663eeea56c175cc7123b64a68a27a41

SegWit spending

Taproot spending

RBF signaling

Height-Locked

fee	720 sat	feerate	5.08 sat/vByte
vsize	142 vByte	output sum	0.01612249 BTC
inputs	▼ 1 <ul style="list-style-type: none">1x P2TR key-path	outputs	▼ 2 <ul style="list-style-type: none">1x P2WPKH v01x P2TR

The transaction was present in **6 block templates** but wasn't included in blocks by **F2Pool**, and **AntPool**.
| **Note:** This **does not mean** these pools filter this transaction out. [FAQ: Why can a transaction be missing from a block?](#)

Block 000000000000000000000354957a6251370023d08d86384da2e0c86de5c9683833			
pool	F2Pool	time	2021-11-14 19:27:47 UTC
height	709715	mempool age	46m 55s
last block package feerate	1.12 sat/vByte	transaction position in template (1496 of 2862) <div><div></div></div>	

Block 0000000000000000000005983e344e69b92cf76186fe43a2e806ed7b6a4cd01ad5			
pool	AntPool	time	2021-11-14 19:12:08 UTC
height	709714	mempool age	30m 49s
last block package feerate	1.09 sat/vByte	transaction position in template (568 of 1010) <div><div></div></div>	

Block 0000000000000000000000ef34d6a810cf28a4f9dd1922b26a0afb6376b6bacce7			
pool	F2Pool	time	2021-11-14 19:07:11 UTC

Missing Counterparty transactions

Multitple missing Counterparty transactions from **F2Pool**'s and **ViaBTC**'s blocks

Missing Transaction `a2d84646f7600ba72f058472192fee4a55b12d4683845bcc4b731895d920ee7c`

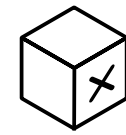
OP_RETURN

fee	1385 sat	feerate	5.04 sat/vByte
vsize	275 vByte	output sum	0.04377586 BTC
inputs	▶ 1	outputs	▼ 2
			<ul style="list-style-type: none">• 1x OP_RETURN• 1x P2PKH

Missing Transaction `cf01557d4e6b0eec45d07d871e37253285e33672a3a9c0708a593c096ea98e16`

fee	1000 sat	feerate	1.94 sat/vByte
vsize	516 vByte	output sum	0.04394571 BTC
inputs	▶ 1	outputs	▼ 3
			<ul style="list-style-type: none">• 2x P2MS• 1x P2PKH

miningpool.observer/missing/e08c3d808317731ef6040799646de2f567590ff890c8fe920a12e36502d8ceb0
miningpool.observer/missing/229028368caadfbab2654f888e919062f117e24da5b3a1974ea9796162191a56
miningpool.observer/missing/cf01557d4e6b0eec45d07d871e37253285e33672a3a9c0708a593c096ea98e16



Missing Counterparty transactions

Multiple missing Counterparty transactions from **F2Pool**'s and **ViaBTC**'s blocks

Missing T...

OP_RETURN

fee

vsize

inputs

Missing

fee

vsize

inputs

DANK REACTOR

INFINITE CLEAN DANK MEME ENERGIES

INPUT = MEMES
OUTPUT = DANKNESS

WHAT COULD POSSIBLY GO WRONG?

Rare Pepe Thug Life

♥:Yolo 🦊:Over 9000

Special:
Rekt

*Only playable for one turn

13zbxgCFH6jQgMDKcUimpnTXsEG8SmBtym

FOLDERPEPE

🦊 = 100 ♥♥♥ = ∞

folderpepe knows what to do...

MINE MEDICINE NOT HASHES

miningpool.observer/missing/cf01557d4e6b0eec45d07d871e37253285e33672a3a9c0708a593c096ea98e16

Missing transaction due to conflict (UTXO spend twice)

Missing Transaction 931bf263e5afd023924a1a183cbb960d472097bde1ccaebc3f9b44c99e204317

Conflicting

fee	9534 sat	feerate	42.76 sat/vByte
vsize	223 vByte	output sum	0.00010466 BTC
inputs	▶ 1	outputs	▶ 1

The transaction was present in **11 block templates** but wasn't included in blocks by **Poolin**, **Binance Pool**, **Foundry USA**, **AntPool**, **SlushPool**, **Luxor**, **SBI Crypto**, and **ViaBTC**.
| **Note:** This **does not mean** these pools filter this transaction out. [FAQ: Why can a transaction be missing from a block?](#)

Block 00000000000000000000000028319cfe61275dd9b12be5d6613f778f3c575f134eda7

pool	Poolin	time	2022-03-02 04:17:28 UTC
height	725535	mempool age	Unknown
last block package feerate	24.57 sat/vByte	transaction position in template (37 of 1508) <div></div>	

Block 0000000000000000000000007d48dce90d2a7d15972a11e0491feb9db6f9bb254a770

pool	Binance Pool	time	2022-03-02 04:14:06 UTC
height	725534	mempool age	2h 26m 20s
last block package feerate	26 sat/vByte	transaction position in template (151 of 1441) <div></div>	

Block 000000000000000000000000725134a6c985a3fafd28b853bc1915f4dcd72e9f323a1

pool	Foundry USA	time	2022-03-02 03:57:39 UTC
------	--------------------	------	-------------------------

Missing transaction due to conflict (UTXO spend twice)

Conflicts between Template and Block

Template Transactions				Block Transactions			
Conflicting				Conflicting			
▶ 931bf263e5afd023924a1a183cbb960d472097bde1cca...				▶ 6df702632790e87f120abed14217e65d3439021d203e0...			
fee	9534 sat	feerate	42.76 sat/vByte	fee	17847 sat	feerate	80.76 sat/vByte
vsize	223 vByte	output sum	0.00010466 BTC	vsize	221 vByte	output sum	0.00002153 BTC
inputs	▶ 1	outputs	▼ 1	inputs	▶ 1	outputs	▼ 1
			• 1x P2PKH				• 1x P2WPKH v0

Conflicting on these previous transaction outputs:

Output #0 of f94ef04427c2716d080532f54dddc167214bdf3e0e686aa14d98f79434946a10

► [open in explorer](#)

<https://miningpool.observer/conflicting/0000000000000000000028319cfe61275dd9b12be5d6613f778f3c575f134eda7>

Missing transaction due to conflict (UTXO spend twice)

Conflict on UTXO belonging to this address

1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T

Missing transaction due to conflict (UTXO spend twice)

Conflict on UTXO belonging to this address

1JwSSubhmg6iPtRjtyqhUYYH7bZg3Lfy1T


brain wallet (private key) for this address

"correct horse battery staple"

Low feerate version of conflict is mined (UTXO spend twice)

Block mined by **Foundry USA**


Conflicts between Template and Block

 Template Transactions

Conflicting

► 3c72abe860b34393066b7d943920022342764375cae98...

fee	42500 sat	feerate	192.31 sat/vByte
vsize	221 vByte	output sum	0.000575 BTC
inputs	► 1	outputs	▼ 1
			• 1x P2WPKH v0

 Block Transactions

Conflicting

► c2d6a35b30c571bdbbc8914ebf26ba548d679928353e1...

fee	4428 sat	feerate	19.77 sat/vByte
vsize	224 vByte	output sum	0.00095572 BTC
inputs	► 1	outputs	▼ 1
			• 1x P2PKH

Conflicting on these previous transaction outputs:

Output #0 of 9fd14daf1d6daa60aab078d7aeceb052245458a4e36fb3c6484d028c169a457c

► open in explorer

<https://miningpool.observer/conflicting/0000000000000000000000004ff584d9c2862fbc13cca3900dddcfe7395822477cb84>

Replace-by-Fee causing conflict

Conflicts between Template and Block

Template Transactions				Block Transactions			
<div> <div>Conflicting</div> <div>RBF signaling</div> <div>OP_RETURN</div> </div>				<div> <div>Conflicting</div> <div>RBF signaling</div> <div>OP_RETURN</div> </div>			
▶ b892112bcef7215ab4317f93089d7147e929fbadbeddd...				▶ a092b06a5bd3fc9bc77c094b94c0557ce132fb4085d69...			
fee	8395 sat	feerate	24.13 sat/vByte	fee	9093 sat	feerate	26.13 sat/vByte
vsize	348 vByte	output sum	1.83401116 BTC	vsize	348 vByte	output sum	1.83400418 BTC
inputs	▶ 1	outputs		inputs	▶ 1	outputs	
		▼ 4				▼ 4	
		• 2x P2SH				• 1x OP_RETURN	
		• 1x P2PKH				(Stacks v2 blockcommit)	
		• 1x OP_RETURN				• 2x P2SH	
		(Stacks v2 blockcommit)				• 1x P2PKH	

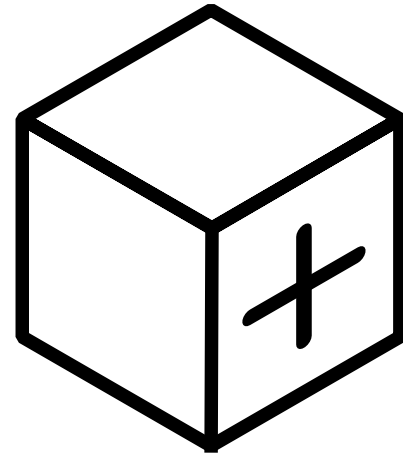
Conflicting on these previous transaction outputs:

Output #3 of 3e46b343e4175806854f5652328d8365e49bf04ba84e35942950345d39c3bd4c

► [open in explorer](#)

2 sat/vbyte are added to stacks.co blockcommit-transactions every minute via a fee-bump

<https://miningpool.observer/conflicting/000000000000000000001a22d4174f7fd50a67fbc263548de51f87d87a92a1732>



Why do pools sometimes include extra transactions in blocks?

- privately transmitted to the miner
- prioritized via out-of-band fee payment
- transaction did not propagated yet

not-broadcast transactions (zero-fee)

Block 715489 by **F2Pool** includes two zero-fee transactions.

A pool UTXO consolidation and a pool payout transaction.

LargeZero-FeeHigh-ValueConsolidation

▶ 81f37d24c47042bf24f7bf27b975f7251f4c9ea761ea7...

fee	0 sat	feerate	0 sat/vByte
vsize	3121 vByte	output sum	199.47550792 BTC
inputs	▼ 17	outputs	▼ 2
	• 17x P2PKH		• 2x P2PKH

transaction position in block (2 of 1000)

LargeZero-FeeHigh-Value

▶ 9cedc04e12e9863fcebcbfd3c494875c858bae57236f0d...

fee	0 sat	feerate	0 sat/vByte
vsize	122413 vByte	output sum	129.39483984 BTC
inputs	▼ 1	outputs	▼ 3748
	• 1x P2PKH		• 1x P2TR
			• 1491x P2PKH
			• 1015x P2WPKH v0
			• 1213x P2SH
			• 28x P2WSH v0

transaction position in block (3 of 1000)


<https://miningpool.observer/template-and-block/0000000000000000000002f62770dae04d5e0f911ca2bf3319cedbec0cd6fcaa46>


Out-of-band fees (ViaBTC)


Template & Block 000000000000000000000000734cc3c9b1f642388d099ec63d6abbaba616fe5800260


mined by	ViaBTC	height	732870
coinbase reward	6.37277976 BTC	last package feerate	10.65 sat/vByte
weight	3992.999kWU	full	99.82%
seen time	2022-04-21 14:13:14 UTC	parent block	goto parent block

 Template	
transactions	3057
packages	2439
fees	0.15802344 BTC
creation time	2022-04-21 14:12:32 UTC

 Block	
transactions	1455 (-1602)
packages	1202 (-1237)
fees	0.12277976 BTC (-35.24368 mBTC)
miner-set time	2022-04-21 14:12:24 UTC

 1661 missing transactions

 1396 shared transactions

 59 extra transactions

<https://miningpool.observer/template-and-block/000000000000000000000000734cc3c9b1f642388d099ec63d6abbaba616fe5800260>

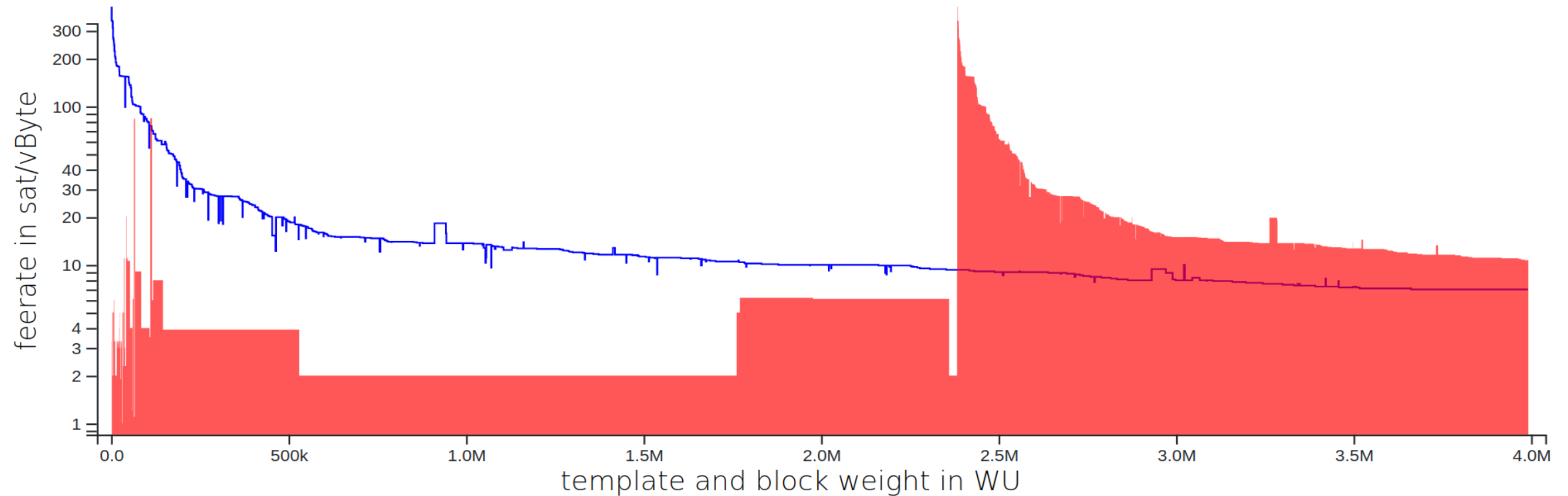
Out-of-band fees (ViaBTC)

Feerate Distribution in Template and Block

This graph shows the feerates of transaction packages in the template and the block. The package [weight](#) in *Weight Units* (WU) is used for the x-Axis. A full template or block can have a maximum weight of 4,000,000 WU (4 MWU).

Hide Template

Hide Block



<https://miningpool.observer/template-and-block/000000000000000000000734cc3c9b1f642388d099ec63d6abbaba616fe5800260>

May 31, 2021 12:00pm EDT

Marathon's Mining Pool, MaraPool, To Cease Filtering Transactions

LAS VEGAS, May 31, 2021 (GLOBE NEWSWIRE) -- **Marathon Digital Holdings, Inc. (NASDAQ:MARA)** ("**Marathon**" or "**Company**"), one of the largest enterprise Bitcoin self-mining companies in North America, announced that the Company's Bitcoin mining pool, MaraPool, has adopted and implemented Bitcoin Core version 0.21.1.

[..]

Marathon will adopt the update without modification. As a result, Marathon's mining pool, MaraPool, will no longer filter transactions. Once the update is complete, the pool will begin validating transactions in a manner consistent with all other miners who use the standard node.

Marathon Digital Holdings press release from May 31th, 2021

<https://ir.marathondh.com/news-events/press-releases/detail/1244/marathon-signals-for-taproot>

Can we detect censorship by mining pools?

Can we detect censorship by mining pools?

When done at scale, yes.

Can we detect censorship by mining pools?

When done at scale, yes.

Do we have evidence for censorship by mining pools?

Can we detect censorship by mining pools?

When done at scale, yes.

Do we have evidence for censorship by mining pools?

No, not to the best of our knowledge.

Can we detect censorship by mining pools?

When done at scale, yes.

Do we have evidence for censorship by mining pools?

No, not to the best of our knowledge.

How to avoid transaction censorship moving forward?

Can we detect censorship by mining pools?

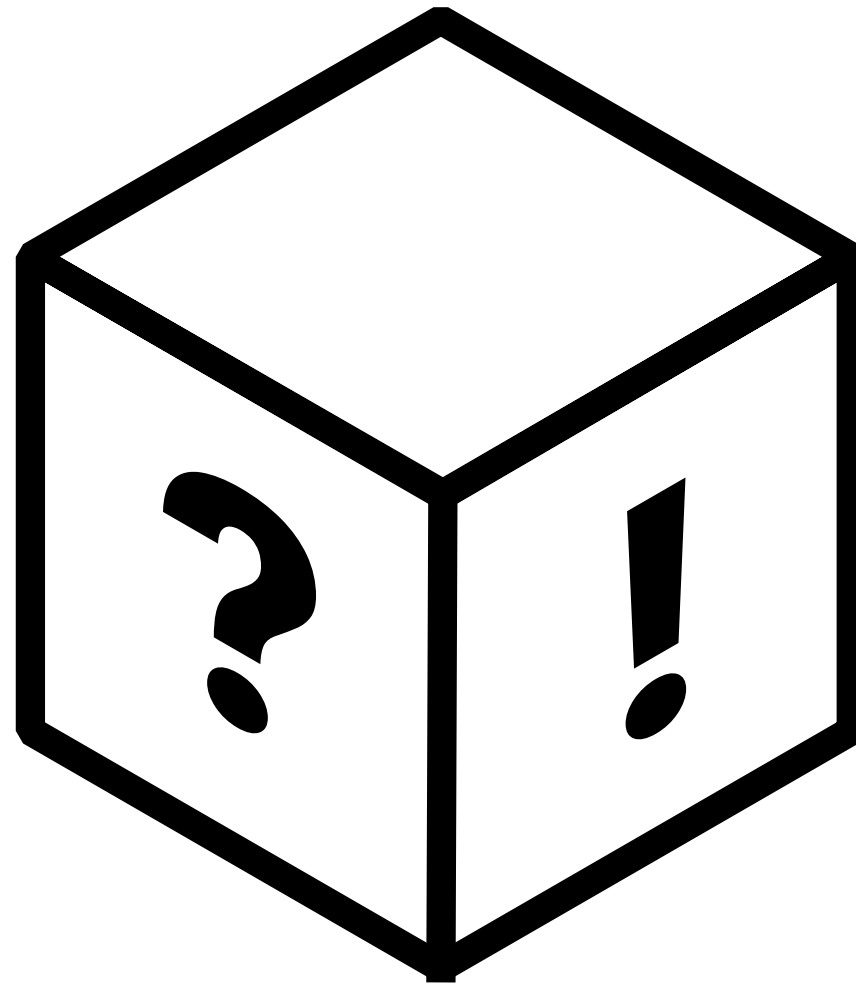
When done at scale, yes.

Do we have evidence for censorship by mining pools?

No, not to the best of our knowledge.

How to avoid transaction censorship moving forward?

Adopt Stratum V2 and its Job Negotiation Protocol as industry standard.



github.com/0xB10C/miningpool-observer

[miningpool.observer](#)

[b10c.me/talks](#)

[@0xB10C](#)