
Charles Jacobsen
H. O. Petersen
Frank Hill
The W. H. Nicol Co.
Ralph W. Lee
A. Gude & Co.
Selzer Heating Co.
John H. Nolan
Martin Bros.
Estate
Harvey
W. J. Watson
Cassidy's
Hugh A. Harvey

sigops

moar like sigoops

> @niftynei

- Blockstreamer
- Core Lightning contributor
- Founder of Base58
- Bitcoin++ instigator in chief

- AIESECer
- Graduate* of Recurse Center NYC

*technically never graduated

sigops

sigops

‘Signature operations’

<pubkey> OP_CHECKSIG

OP_CHECKSIG

OP_CHECKSIG
OP_CHECKSIGVERIFY

OP_CHECKSIG
OP_CHECKSIGVERIFY
OP_CHECKMULTISIG

OP_CHECKSIG
OP_CHECKSIGVERIFY
OP_CHECKMULTISIG
OP_CHECKMULTISIGVERIFY

<pubkey> OP_CHECKSIG

<pubkey> OP_CHECKMULTISIG

Each `OP_CHECKSIG` and `OP_CHECKSIGVERIFY` is counted as 1 sigop.

<pubkey> OP_CHECKSIG

<pubkey> OP_CHECKMULTISIG

If `OP_CHECKMULTISIG` or `OP_CHECKMULTISIGVERIFY` are in a redeemScript (i.e. it's P2SH), then the number of sigops is the number of public keys in the multisig redeemScript. If there is more than 16 public keys, then it is always accounted as 20.

<pubkey> OP_CHECKMULTISIG

SegWit

For non-segwit inputs, these numbers are multiplied by 4, so 4 sigops for `OP_CHECKSIG` and `OP_CHECKSIGVERIFY`, and 80 sigops for `OP_CHECKMULTISIG` and `OP_CHECKMULTISIGVERIFY`.

80,000 sigops

OP_IF

<>

OP_ELSE

<>

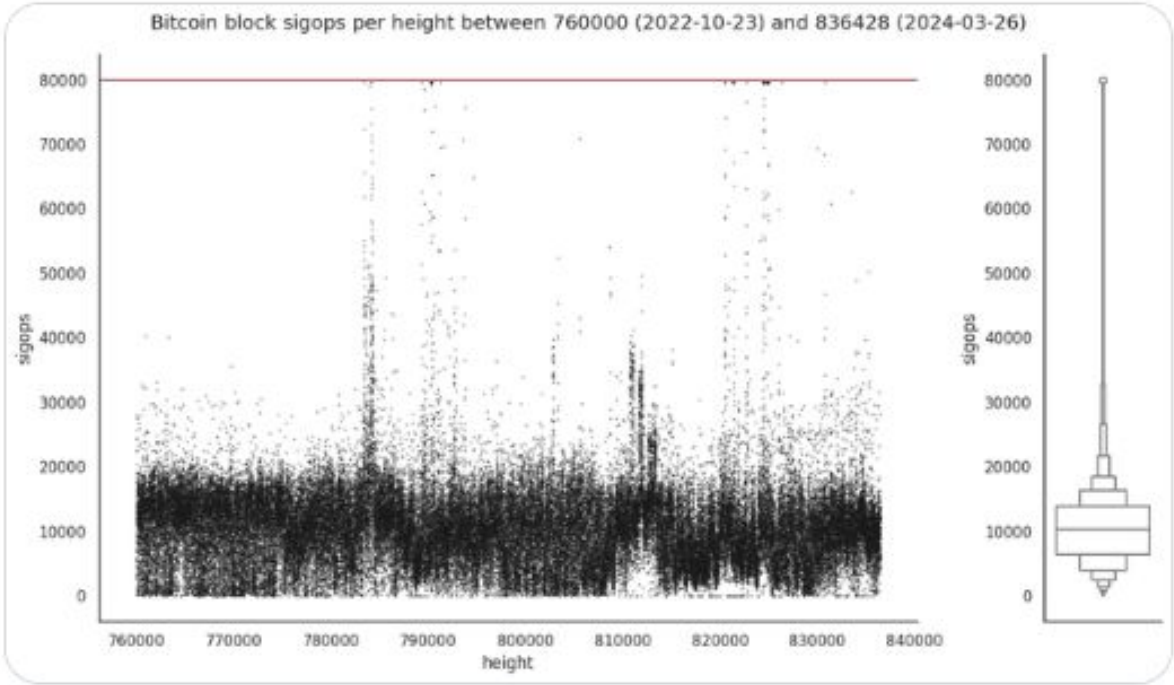
OP_ENDIF

OP_CHECKSIGADD??

- In P2TR taproot scripts:
  - Sigops are not counted.

0xB10C @0xB10C · Apr 2

sigops per block between 760000 and 836428



Invalid F2Pool blocks 783426 and 784121 (April 2023)

The April F2Pool's joke that wasn't a joke

Tuesday, April 2, 2024

My notes on the two `bad-blk-sigops: too many sigops` invalid blocks, 783426 and 784121, mined by F2Pool in April 2023.

On April 1st, 2023, F2Pool mined an invalid block at height 783426. Bitcoin Core nodes rejected the block with the reason `bad-blk-sigops` and the note `too many sigops` . On April 6th, 2023, F2Pool mined another `bad-blk-sigops` block at height 784121. Mining an invalid block with a valid proof-of-work is an expensive

Why sigops?

CVE-2010-5138

Date: 2010-07-29
Summary: Unlimited SigOp DoS
Fix Deployment: 100%

Affected		Fix
bitcoind wxBitcoin	* - 0.3.?	0.3.?

On July 29 2010, it was discovered that block 71036 contained several transactions with a ton of OP_CHECKSIG commands. There should only ever be one such command. This caused every node to do extra unnecessary work, and it could have been used as a denial-of-service attack. A new version of Bitcoin was quickly released. The new version did not cause a fork on the main network, though it did cause one on the test network (where someone had played around with the attack more).

References

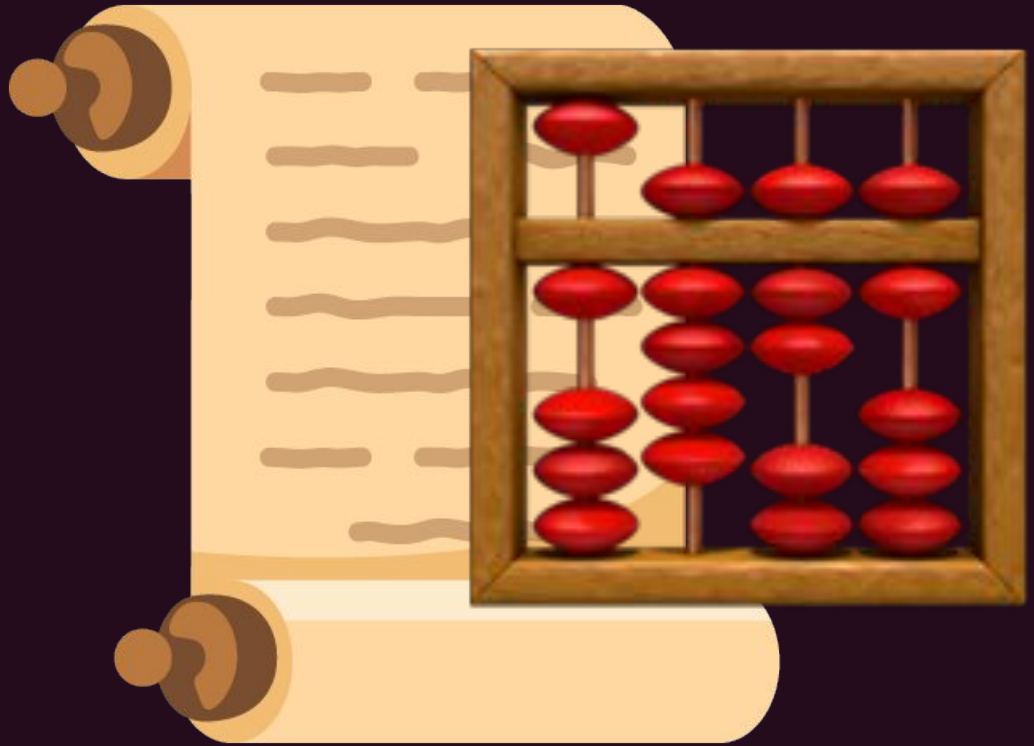
- US-CERT/NIST

Execution costs??

201 non-push op limit

201 non-push op limit

Counts pubkeys in multisigs!



The Great Script Restoration Project

You're probably aware that v0.3.1 of Bitcoin disabled numerous Script opcodes, most famously OP_CAT. Bringing them back unlock great deal of power, and there are a few additional opcodes that complement them w in a modern Bitcoin system (such as key

Courses Testimonials FAQ

Let us take you from zero to timechain hero

Base58⛓️🔓 is a bitcoin protocol school. Our online and in-person courses are the perfect starting place for technical beginners looking to scratch the surface to even the most experienced devs looking to challenge themselves with a dive deep into the bitcoin protocol itself. Wherever you are on your journey into the technical side of bitcoin, we're here to level you up.

Explore Courses

What our students say →

Bitcoin Triva w/ Austin BitDevs + Base58⛓️🔓

MAY
2

Thursday, May 2
7:00 PM - 8:30 PM

Bitcoin Commons ↗
Austin, Texas

Registration

Welcome! To join the event, please register below.

niftynei hello@base58.school

One-Click Register

You have manage access for this event. Manage ↗

Hosted By

niftynei

10 Going

Ishan Anand, nickcalabs and 8 others

About Event

Austin BitDevs is teaming up with Base58⛓️🔓 to bring you a night of bitcoin trivia!

Find your deep-pocket bitcoin dev nerd friends and bring them along for 3 rounds of bar-style team trivia.

Prizes TBD :)