

Parallel Blockchain validation with Utreexo Compact State Nodes

33조

Utreexo Accumulators?

- Project started by Tadge Dryja, a MIT research scientist and the Lightning Network co-author
- Allows the representation of a set to be very small (< 1KB)
- Can prove the inclusion of a member in the set



tadge dryja | research scientist

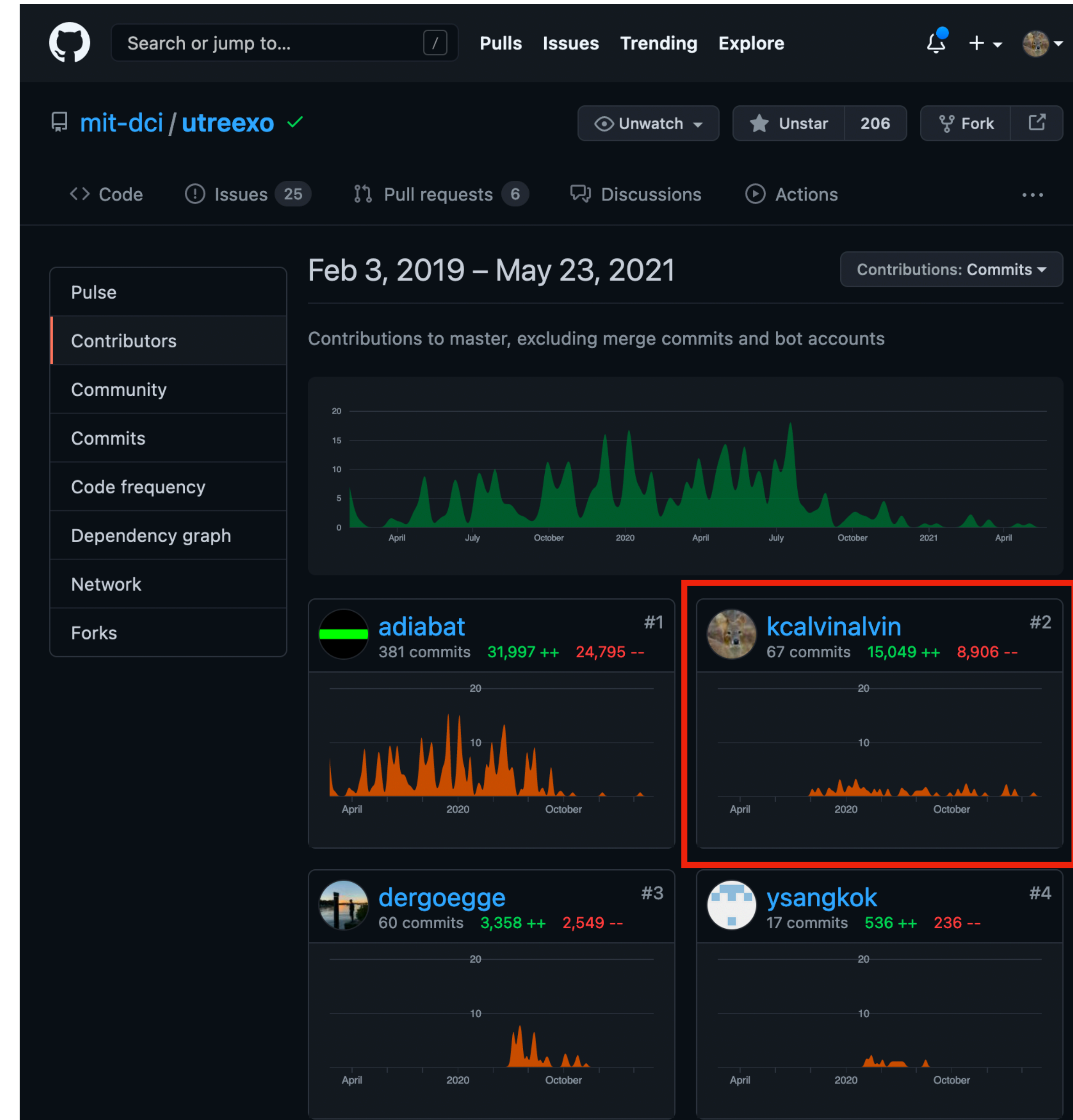


A creator of the Lightning Network, one of the most promising Bitcoin scaling solutions, Tadge Dryja leads DCI research focused on the scaling and interoperability of cryptocurrencies and smart contracts. Follow @tdryja on Twitter.

dci.mit.edu/thaddeus-dryja-tadge

About me

- Have been contributing to the Utreexo project since 2019. Wrote roughly half of the accumulator library
- Leading the implementation of the Utreexo Accumulators into a Bitcoin node (github.com/mit-dci/utcd)
- Leading a Rust port of the Utreexo Accumulators (github.com/mit-dci/rustreexo)



About me

- Funded by Bitmex since 2020 (a Bitcoin futures exchange)

blog.bitmex.com/calvin-kim/

digital
currency
initiative

mit
media
lab

search

aboutresearcheducationeventsgithub

Calvin Kim is awarded for his role as an Utreexo Collaborator: "BitMex awards its last developer grant to a Bitcoin scalability solution from MIT"

by [MICHAEL KAPILKOV](#) on AUG 24, 2020

BitMex's 100x Group has [awarded](#) its last Bitcoin development grant of the year. The company has awarded a grant valued at \$40,000 to Calvin Kim for his Bitcoin scalability solution, Utreexo – a project originally created by Tadge Dryja from the MIT Digital Currency Initiative.

Bitcoin's protocol checks every proposed transaction to make sure that the sender has enough coins to complete the request. All unspent Bitcoin ([BTC](#)) is saved in what is known as UTXO, or Unspent Transaction Outputs. While the entire Bitcoin blockchain is currently around 300 GB, the UTXO is only 4 GB. MIT researchers have claimed that as the network grows, this may one day present a bottleneck of its own.

dci.mit.edu/research/2020/9/2/calvin-kim-is-awarded-for-his-role-as-an-utreeexo-collaborator-announced-in-cointelegraphs-bitmex-awards-its-last-developer-grant-to-a-bitcoin-scalability-solution-from-mit

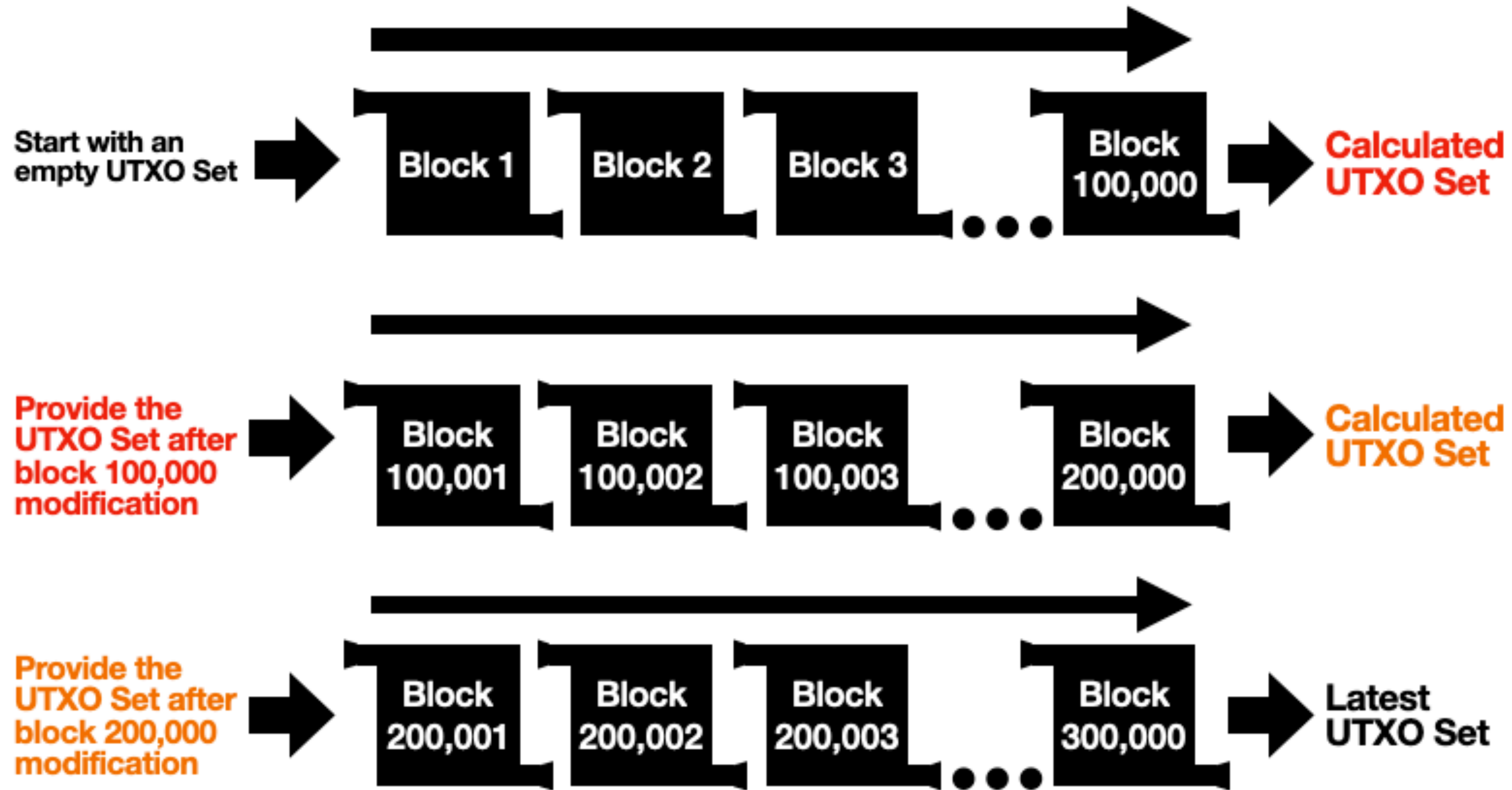
Scope of the project for Capstone Design

- Build a Bitcoin node that verifies blocks in parallel using the Utreexo Accumulators

Initial block download (IBD)

- Synchronization of the blockchain
- Download&verify block 0 to tip

General Idea



General Idea

if **Provided UTXO
Set after block
100,000
modification** == **Calculated
UTXO Set** and

**Provided UTXO
Set after block
200,000
modification** == **Calculated
UTXO Set** :

**Latest
UTXO Set = valid**

General Idea

Input:

Start UTXO Set
End UTXO Set
Block Data
Rules



Block validation function

Output:
Valid or Invalid

Why is Utreexo needed?

Utreexo is tiny

Utreexo is tiny

Input:

Start UTXO Set
End UTXO Set
Block Data
Rules

Block validation function

Output:
Valid or Invalid

**Utreexo eliminates disk
access**

Dis~~X~~i/o

->

SHA256

Benchmarks

Benchmarks

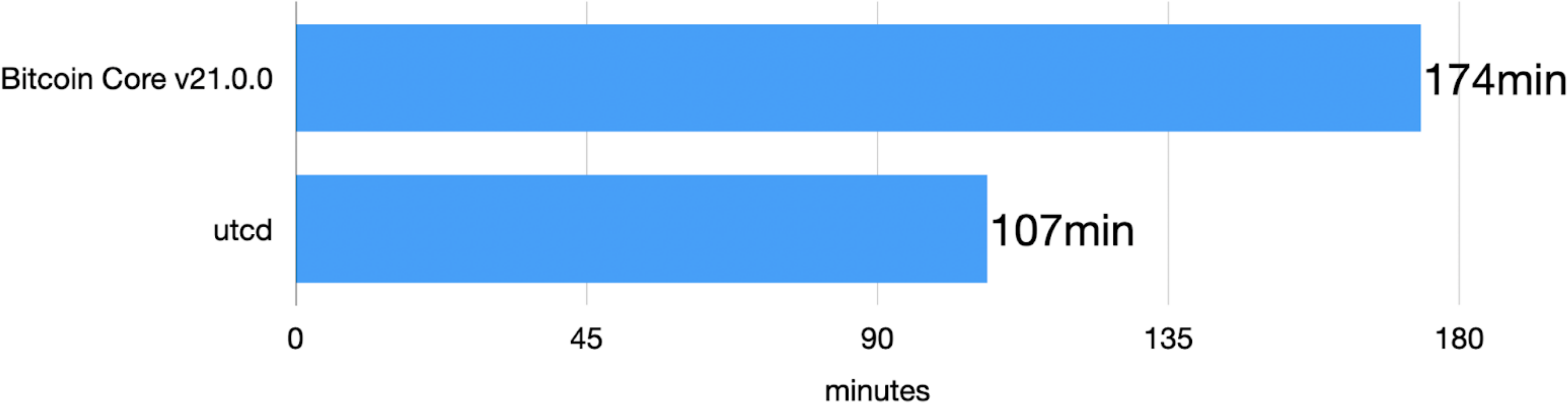
- Tests based on Bitcoin Core v21.0.0 and utcd
- utcd tests are reproducible by following instructions at github.com/mit-dci/utcd

Benchmarks

CPU	Ryzen 3600
Memory	Samsung 32GB DDR4 2666MHz
Storage	1TB HP SSD EX950 M.2 NVMe
Bitcoin Core version	v21.0.0
Linux Kernel Version	5.7.19
bitcoin.conf settings	-dbcache=24000-maxmempool=1000

Benchmarks

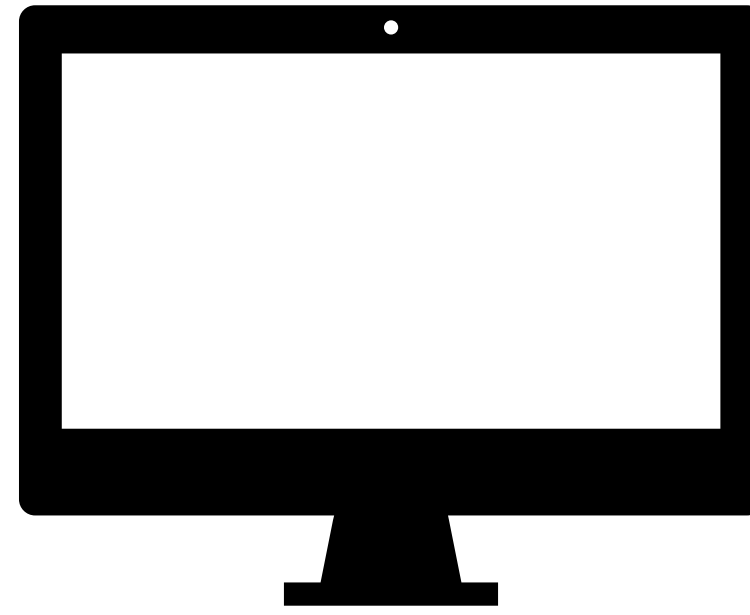
Initial Block Download Speeds - local nodes
(default mode, no signature checks until block 654,683)



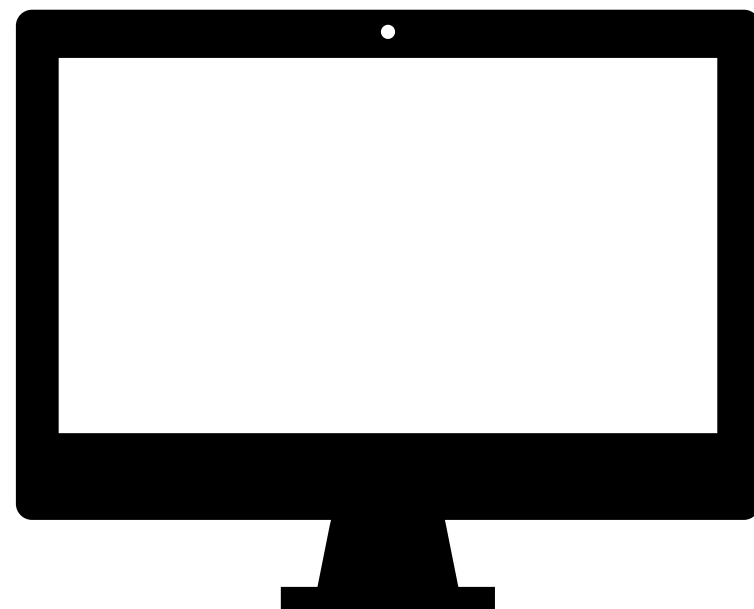
Multi-machine Benchmarks

Multi-machine Benchmarks

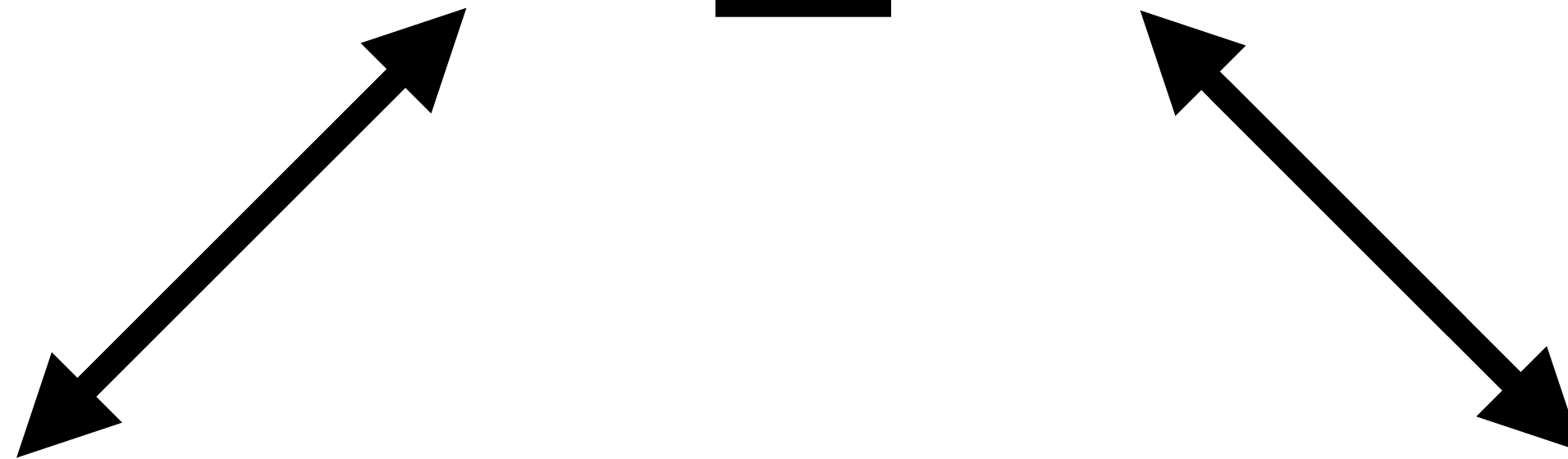
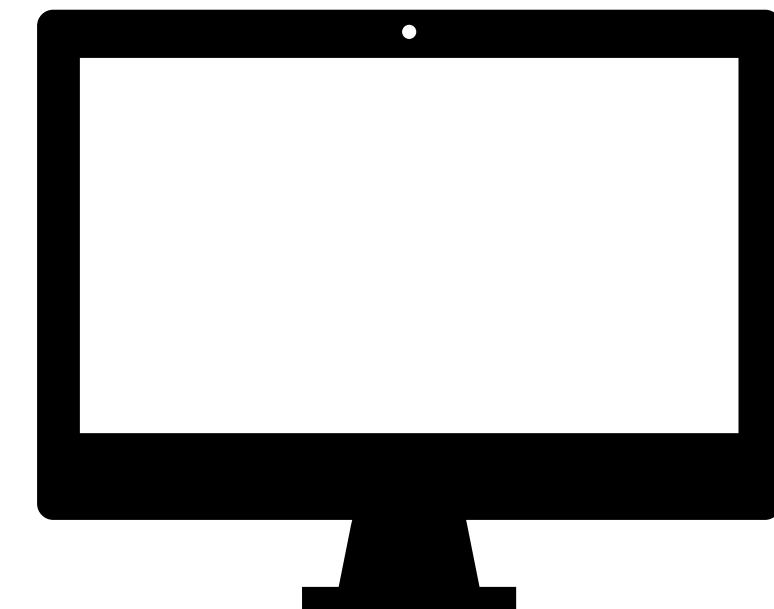
Coordinator



worker



worker



Multi-machine Benchmarks

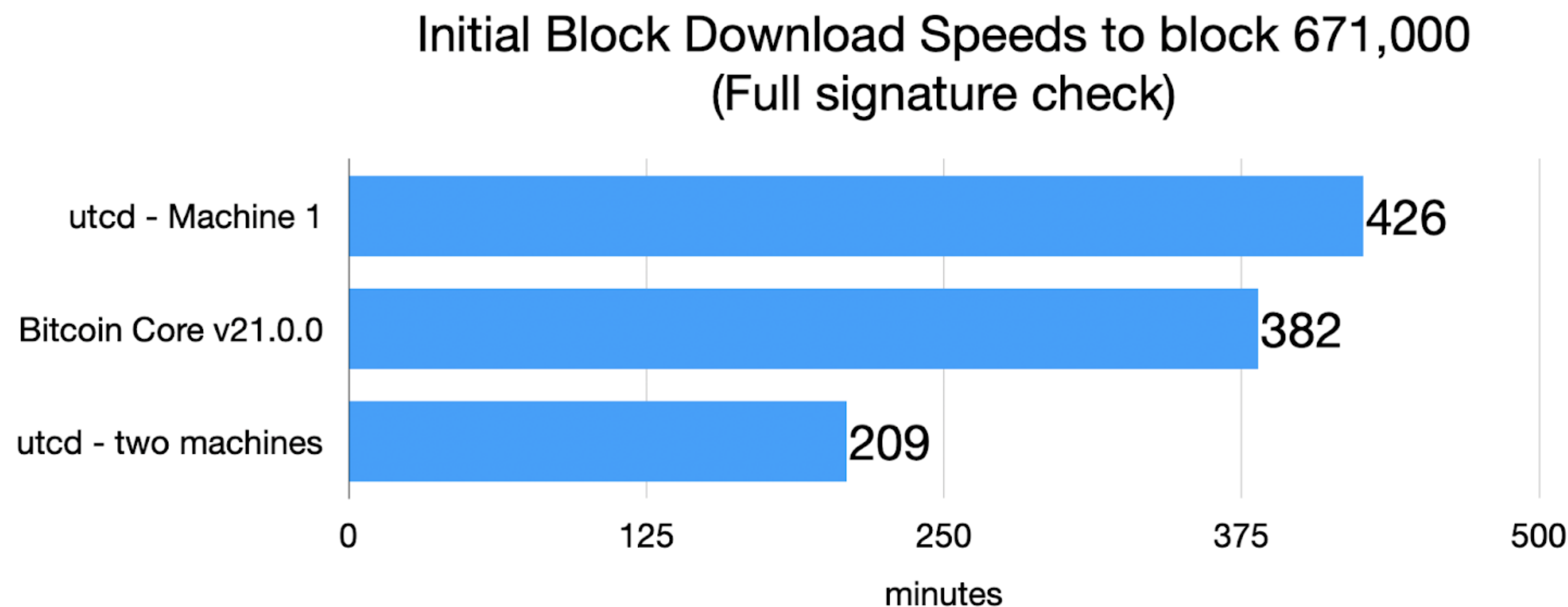
Machine 1

CPU	Ryzen 3600
Memory	Samsung 32GB DDR4 2666MHz
Storage	1TB HP SSD EX950 M.2 NVMe

Machine 2

Macbook Pro M1 – 8GB Unified Memory (MacBookPro17,1)
--

Multi-machine Benchmarks



Multi-machine Benchmarks

- Results also on Bitmex Research

<https://blog.bitmex.com/faster-blockchain-validation-with-utreexo-accumulators/>

- Along with a more detailed explanation of how it works


<https://blog.bitmex.com/out-of-order-block-validation-with-utreexo-accumulators/>

In the press


In the press

- Results on the parallel blockchain validation on [nasdaq.com](https://www.nasdaq.com/articles/utreexo-can-speed-bitcoin-initial-block-download-by-62-2021-05-19)

<https://www.nasdaq.com/articles/utreexo-can-speed-bitcoin-initial-block-download-by-62-2021-05-19>



[MARKET ACTIVITY](#)[NEWS + INSIGHTS](#)[SOLUTIONS](#)[ABOUT](#)

 Latest News

Stitch Fix Earnings: Will the Stock Unravel Again Post-Earnings Release?
32 MINS AGO

AgTech: Cultivating Sustainable Solutions to Food Inflation
1 HOUR AGO

BITCOIN

Utreexo Can Speed Bitcoin Initial Block Download By 62%

CONTRIBUTOR

Namcios — [Bitcoin Magazine](#)

PUBLISHED

MAY 19, 2021 2:28PM EDT



BitMEX Research grantee Calvin Kim has demonstrated how the Utreexo client can speed up the Bitcoin Initial Block Download by 62%.



BitMEX Research grantee Calvin Kim has [announced](#) that the Utreexo project can successfully finish Bitcoin's Initial Block Download (IBD) 62% faster than Bitcoin Core. Kim also noted that the speedup is expected to increase even further in the future, since many optimizations are yet to be implemented.