Being a Bitcoin developer

My experience being one for 6 years now

WHERE'S WALDO?®

The Animated Series

"Nobody ever asks 'How's Waldo?'"

How is Calvin doing

As a Bitcoin developer for 6 years

2013

BUSINESS INSIDER

TECH

How To 'Mine' Bitcoins And Make Real Money

By Dylan Love

Mar 8, 2013, 11:00 AM GMT+9


CLASSIFIED
GeForce
GTX 460
GeForce
GTX 460

New account confirmation

Inbox ×

mining.bitcoin.cz <no-reply@bitcoin.cz> Jan 22, 2014, 8:07 PM

to me

Hello [redacted]

thank you for signing up for an bitcoin.cz account!

To activate your account, click to this activation link

Best regards,
slush
The Pool Operator

Payout Settings

Request Payout

Frequency	Destinati	Actions
Threshold (0.5 BTC)	Wallet	Edit rule

[Mine-Litecoin] 2nd WARNING: Account marked for termination

Inbox ×

Mine-Litecoin <do-not-reply@mine-litecoin.com>

Tue, Apr 1, 2014, 9:04 AM

to me

Images are not displayed. Display images below - Always display images from do-not-reply@mine-litecoin.com

Your account has expired. Failure to login to the account will terminate the account and delete all user information from our systems.

If you would like to keep your account please login below:

https://mine-litecoin.com/index.php?page=login

[DogeCoin Pool - Nut2Pools] Pool Closure

Inbox ×

DogeCoin Pool - Nut2Pools <do-not-reply@nut2pools.com>

Fri, Jun 5, 2015, 7:29 PM

to me

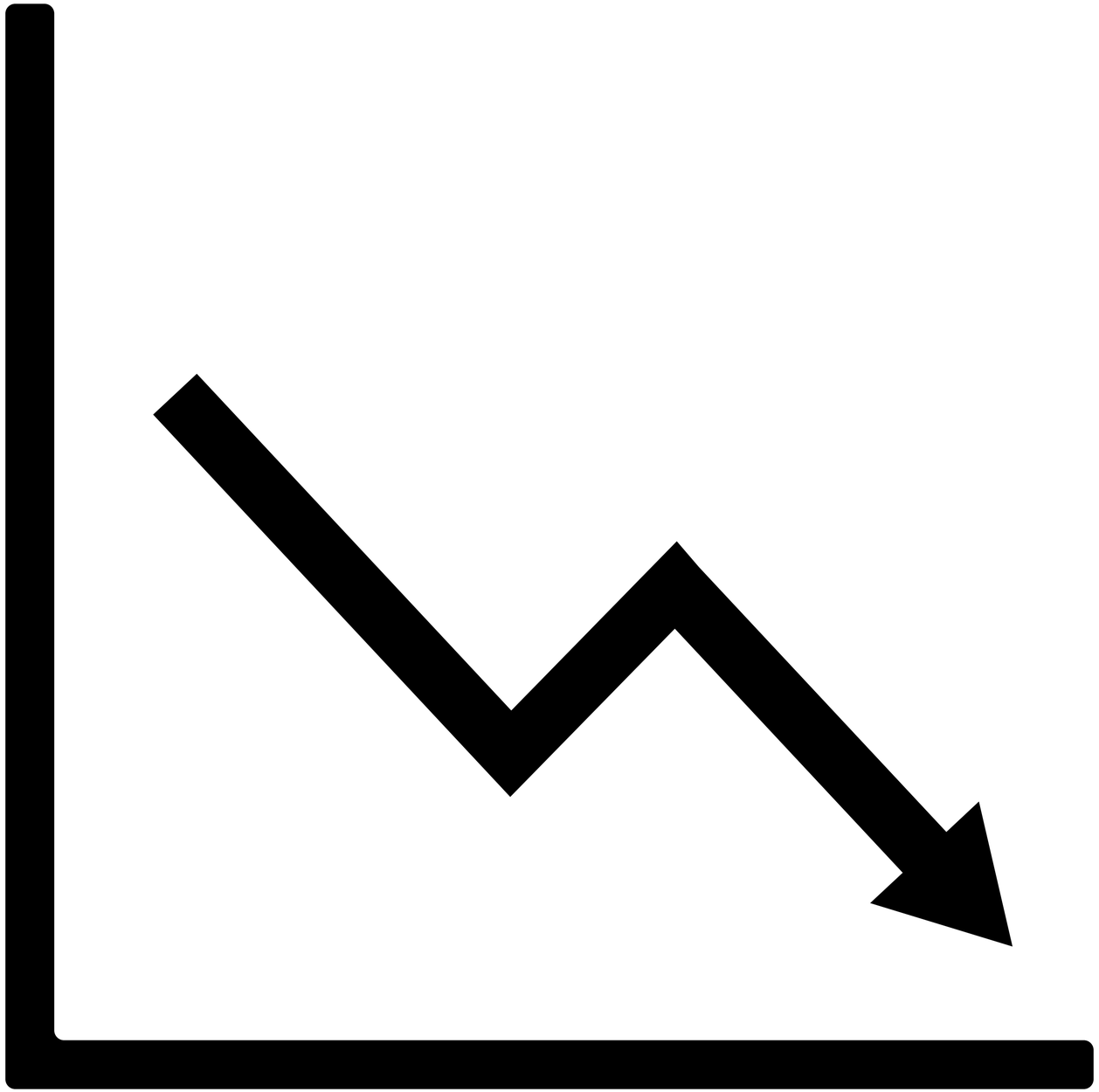
Dear scyshc,

Hi All, It's with a heavy heart that we are announcing the need to close the doge.nut2pols.com pool. It will be closing on the 10th June as the operating costs and time required are simply unbearable.
The pool will close completely and the sites and wallets wiped from the servers on the 11th June 2015.
Please ensure you cashout any balances by this time as any funds left in the pools wallets will be treated as a donation to the pool in a bid to recoup at least some of the costs.
We'd like to thank all the miners that have mined with us over the last couple of years and wish them luck with finding a new mining home.
All the best
Nut

ROBERT MCMILLAN
BUSINESS MAR 3, 2014 6:30 AM

The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster

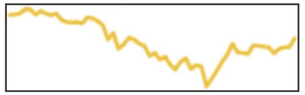
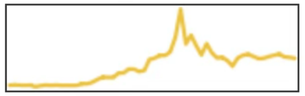
Tokyo-based bitcoin exchange Mt. Gox filed for bankruptcy last week, saying hackers had stolen the equivalent of $460 million from its online coffers. The news rocked the bitcoin world, and it could even bring down the much-hyped digital currency.

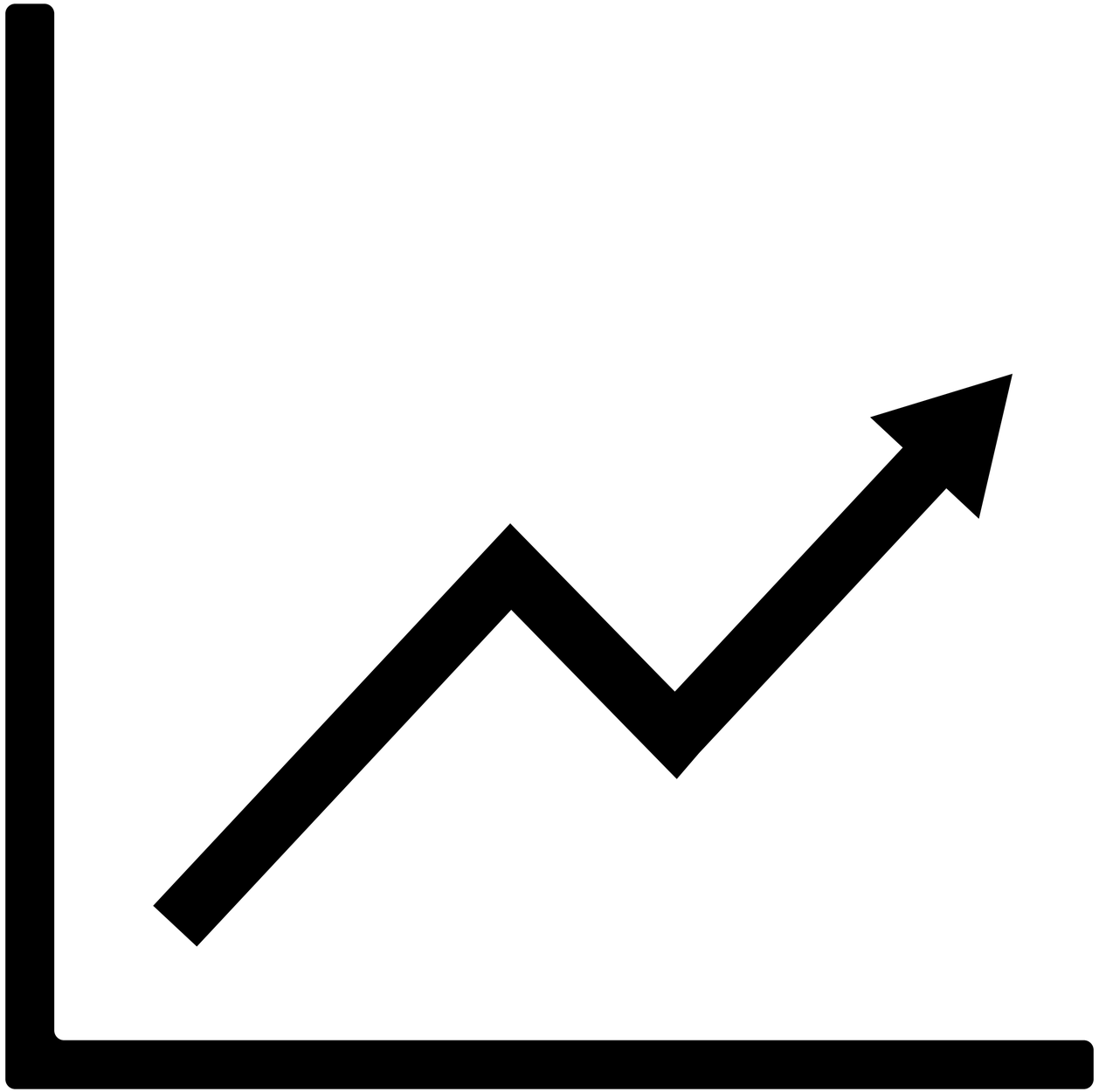


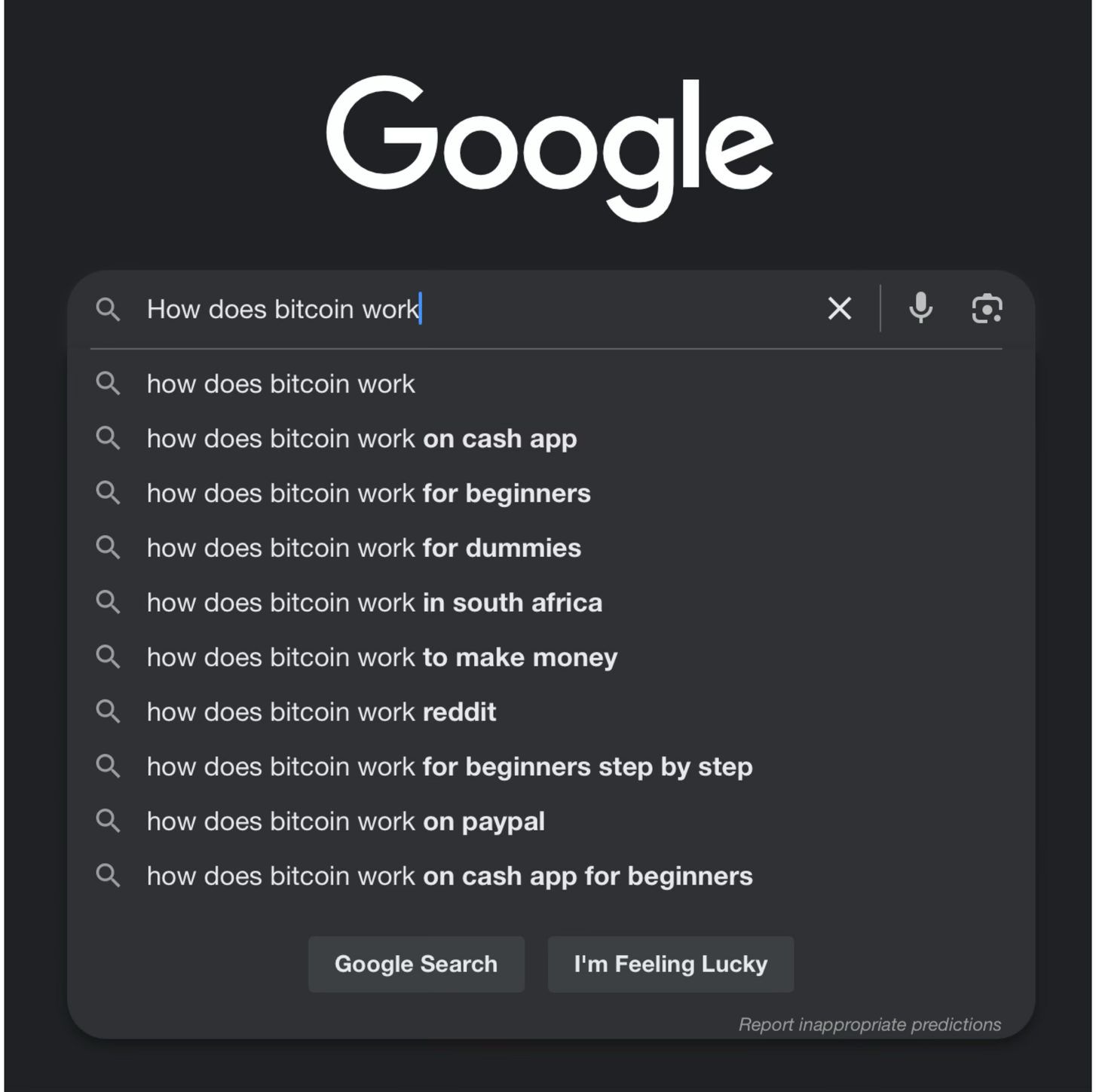
Cryptocurrency Market Capitalizations

Market Cap | Trade Volume | Trending | Tools | Search Currencies

All | Coins | Tokens | USD | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$113,575,018,572	$6809.10	$3,310,790,000	16,679,887 BTC	2.14%	
2	Ethereum	$31,975,515,073	$334.01	$1,078,720,000	95,731,349 ETH	4.83%	
3	Bitcoin Cash	$21,246,782,899	$1264.49	$1,658,610,000	16,802,650 BCH	-1.01%	
4	Ripple	$8,067,313,434	$0.208874	$115,692,000	38,622,870,411 XRP *	0.77%	
5	Litecoin	$3,390,666,002	$62.99	$176,306,000	53,831,032 LTC	2.68%	
6	Dash	$3,279,607,441	$426.53	$124,119,000	7,688,989 DASH	1.71%	
7	NEO	$1,920,360,000	$29.54	$40,999,800	65,000,000 NEO *	3.41%	
8	Monero	$1,890,285,675	$123.12	$55,932,100	15,353,197 XMR	0.65%	




Google
How does bitcoin work
how does bitcoin work
how does bitcoin work on cash app
how does bitcoin work for beginners
how does bitcoin work for dummies
how does bitcoin work in south africa
how does bitcoin work to make money
how does bitcoin work reddit
how does bitcoin work for beginners step by step
how does bitcoin work on paypal
how does bitcoin work on cash app for beginners
Google Search
I'm Feeling Lucky
Report inappropriate predictions

FINTECH

Bigger than bitcoin? Enterprise Ethereum Alliance grows in size

PUBLISHED WED, MAY 24 2017•1:31 AM EDT | UPDATED THU, MAY 25 2017•12:05 PM EDT

Neil Ainger, special to CNBC.com

https://www.cnbc.com/2017/05/23/bigger-than-bitcoin-enterprise-ethereum-alliance-grows-in-size.html

Seoul Bitcoin Meetup

Bitcoin Primer Webinar Part 03

February 3, 2020
23:00 - 00:30 UTC

REGISTER NOW

MARIO GIBNEY
Customer Support Lead

Blockstream

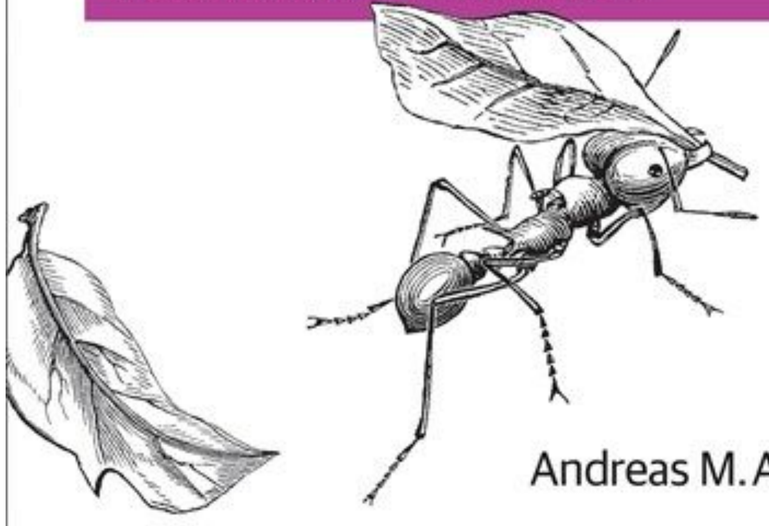
Sanket Kanjalkar

O'REILLY®

2nd Edition

Mastering Bitcoin

PROGRAMMING THE OPEN BLOCKCHAIN



Andreas M. Antonopoulos

DECENTRALIZED

TRUSTLESS

REPLACE THE GOVERNMENT

TRUST A RANDOM WALLET COMPANY

"Run a node"

Some Bitcoiners

TAKES DAYS TO START UP

FIDDLE AROUND WITH CONNECTING YOUR WALLET FOR DAYS

RESTART IT AND TAKE HOURS TO SYNC

Bitcoin is trustless

How I'm using Bitcoin is not trustless

Thaddeus Dryja the 3rd

Tadge Dryja

Research Scientist
MIT Media Lab

BUIDL 2019

www.buidl.asia

Utreexo: A dynamic hash-based accumulator optimized for the Bitcoin UTXO set

Thaddeus Dryja
tdryja@media.mit.edu

MIT Digital Currency Initiative

Abstract

In the Bitcoin consensus network, all nodes come to agreement on the set of Unspent Transaction Outputs (The "UTXO" set). The size of this shared state is a scalability constraint for the network, as the size of the set expands as more users join the system, increasing resource requirements of all nodes. Decoupling the network's state size from the storage requirements of individual machines would reduce hardware requirements of validating nodes. We introduce a hash based accumulator to locally represent the UTXO set, which is logarithmic in the size of the full set. Nodes attach and propagate inclusion proofs to the inputs of transactions, which along with the accumulator state, give all the information needed to validate a transaction. While the size of the inclusion proofs results in an increase in network traffic, these proofs can be discarded after verification, and aggregation methods can reduce their size to a manageable level of overhead. In our simulations of downloading Bitcoin's blockchain up to early 2019 with 500MB of RAM allocated for caching, the proofs only add approximately 25% to the amount otherwise downloaded.

"Utreexo makes nodes easier to run"

Tadge

Combined blockparser, txottl, and ibdsim. Added flags for them #13

Edit Code

Merged **adiabat** merged 1 commit into `mit-dci:master` from `kcalvinalvin:combined-cmd-added-flag` on Oct 23, 2019

Conversation 5 Commits 1 Checks 0 Files changed 9 +112 −82


ONE YEAR
LATER...

MEDIA 09-02-2020

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.

READ THE FULL ARTICLE HERE

https://www.dci.mit.edu/dci-news/calvin-kim-is-awarded-for-his-role-as-an-utreexo-collaborator-bitmex-awards-its-last-developer-grant-to-a-bitcoin-scalability-solution-from-mit

"I think we can do parallel block validation with utreexo"

Me

"Yes."

Tadge

"It'd be so much faster than the normal way"

Me

"Yes."

Tadge


ONE YEAR
LATER...

Out of Order Block Validation with Utreexo Accumulators

BitMEX Research 20 May 2021

Abstract: In this piece, BitMEX grantee Calvin Kim explains why the order in which blocks are validated does not matter under Utreexo. This is because the disk space savings make UTXO snapshots practical, which in turn allows for the parallelisation of the validation of the Bitcoin Blockchain. Calvin goes on to explain that one can check if an incoming transaction is valid by verifying the accumulator proof, getting rid of the need to access the UTXO set. This allows Utreexo nodes to eliminate disk access requirements, in exchange for more hashing, which can be an excellent trade-off. Calvin then discusses how Utreexo can change how we think about block validation.

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

Faster Blockchain Validation with Utreexo Accumulators

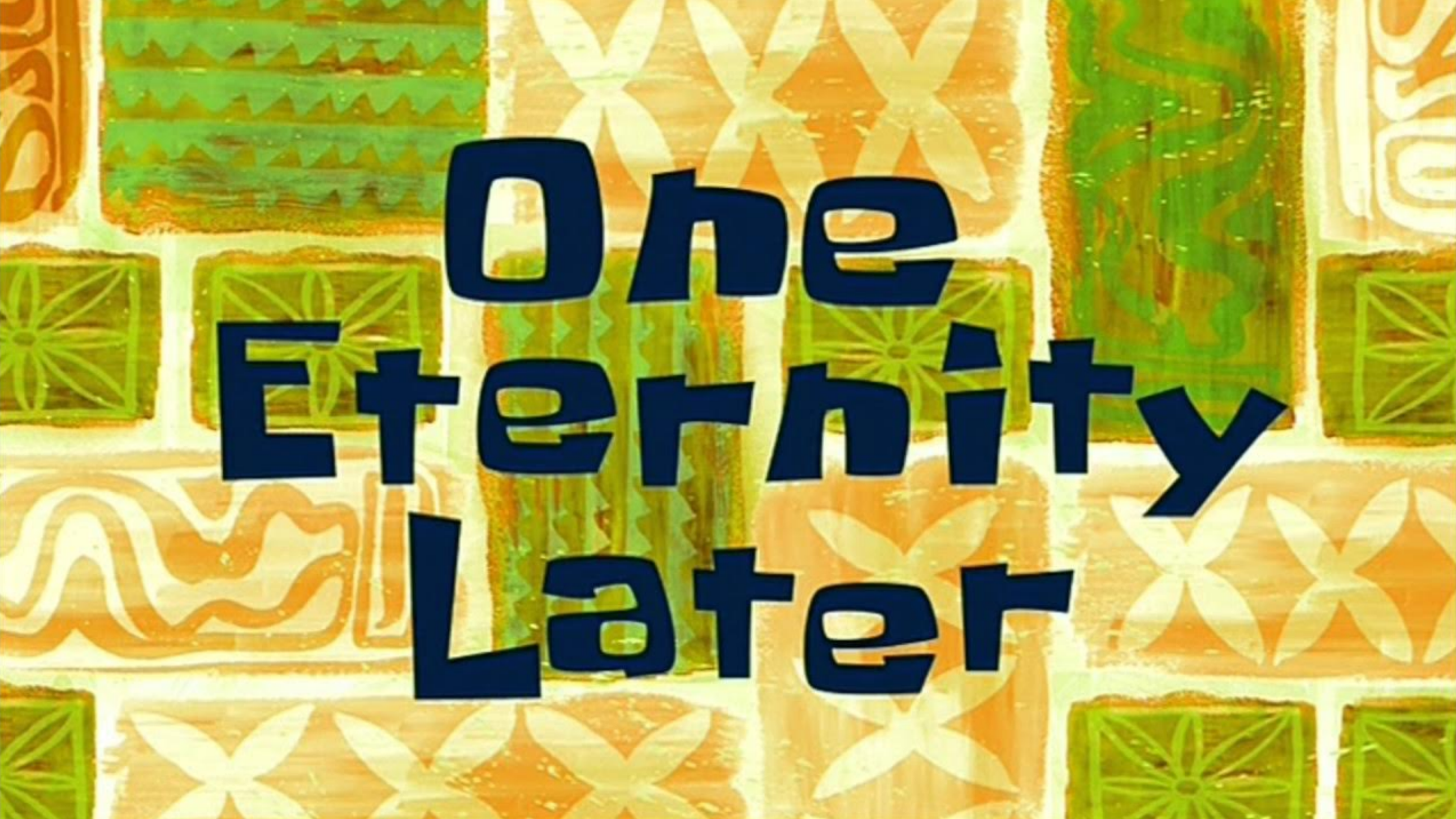
BitMEX Research 19 May 2021

Abstract: In this piece, 100x Group grantee Calvin Kim announces the success in speeding up Bitcoin's Initial Block Download (IBD) using the Utreexo client. While the speed improvement can vary depending on one's local hardware and bottlenecks, the initial download and verification can be up to 62% faster compared to Bitcoin Core. Since many optimisations are yet to be implemented, the speedup is expected to increase. Calvin goes on to talk about how the IBD can be split up into multiple tasks, and therefore conducted by multiple computers. Eventually the plan is to implement Utreexo in C++ and get it merged into Bitcoin Core. While this may be a long way off, the C++ implementation has already been started.

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

"We should try to not do research now and ship something"

Me


One
Eternity
Later

ADDRESS	USER AGENT	HEIGHT	LOCATION	NETWORK
[redacted] Since 1 week, 2 days ago	/btcwire:0.5.0/utreexod:0.4.1/ (70013) NODE_NETWORK, NODE_BLOOM, NODE_WITNESS, NODE_NETWORK_LIMITED (16778253)	899731	Cheonan, Korea (the Republic of) Asia/Seoul	SK Broadband Co Ltd (AS9318)

Abstract

This document defines the process for representing, updating and verifying proofs for the Utreexo accumulator.

License

Motivation

The Bitcoin UTXO set continues to grow, currently over 10GB. While much less than the size of the blockchain, UTXO set growth is only bounded by the 1MB un-discounted block size limit. This is problematic as every fully validating node needs to store the entire UTXO set.
The Utreexo accumulator removes this requirement, allowing fully validating nodes to store a small cryptographic accumulator of the UTXO set instead of the entire set.
The accumulator requires storage of O(log_2(N)) where N is the number of UTXOs.

This BIP document describes the design of the accumulator structure used in Utreeexo, which uses the accumulator to commit UTXO data into leaves of the accumulator. The reset of this document

https://github.com/utreexo/biptreexo/blob/main/utreexo-accumulator-bip.md

"How do I become a Bitcoin developer"

Some people

"idk"

Me

"Can we use Utreexo to do balance validation on hardware wallets"

What I hope some people would ask

"yes"

Me

I liked Bitcoin

Bitcoin didn't really work the way I thought it would

I decided to change it

I did it long enough that people started giving me money

Getting paid to do on things I would do for free