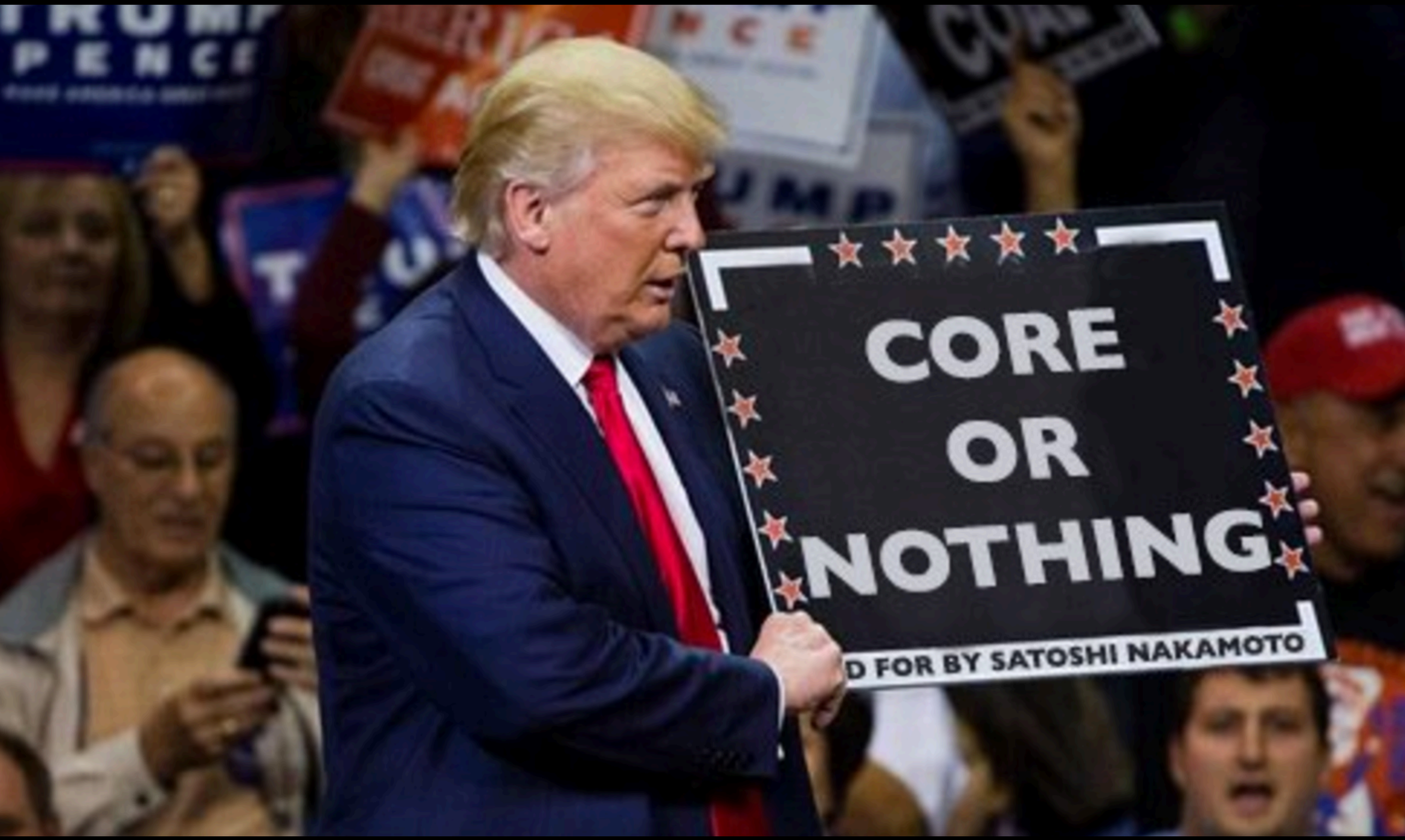

CORE
OR
NOTHING
D FOR BY SATOSHI NAKAMOTO

BitcoinCore

What is Bitcoin-**Core**?

- ✓ Implementation of the „**consensus rules**“ (Validation)
- ✓ Historical block database (~complete blockchain)
- ✓ P2P network client/daemon
- ✓ Wallet
- ✓ RPC / ZMQ / REST API

Satoshi Nakamoto / 2009

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort

30th August 2009

First open source commit

File	Date	Author	Commit
trunk	2009-08-30	sirius-m	[r1] First commit

```
BitCoin v0.1.5 ALPHA

Copyright (c) 2009 Satoshi Nakamoto
Distributed under the MIT/X11 software license, see the accompanying
file license.txt or http://www.opensource.org/licenses/mit-license.php.
This product includes software developed by the OpenSSL Project for use in
the OpenSSL Toolkit (http://www.openssl.org/).  This product includes
cryptographic software written by Eric Young (eay@cryptsoft.com).
```

Today

~50 (real) code contributors
~10 devs do >80%

The Bitcoin blockchain is probably the **most inefficient database**

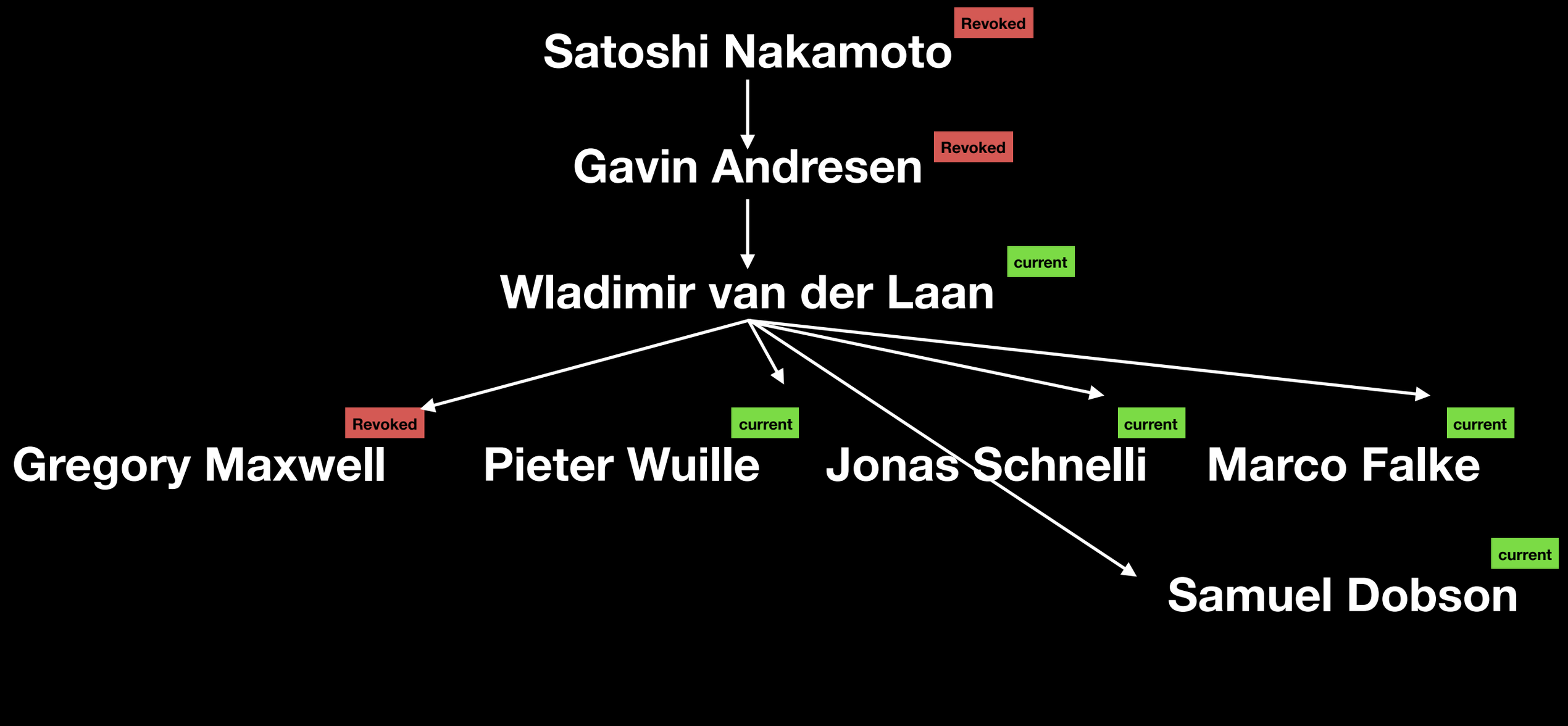
>**1$** for **80bytes**

Write operation takes **~10** mins

Bitcoin is the **22th** most **forked** and the **81th** most **starred** **GitHub** repository.

(As of March 6th 2019)

Source-Code administrator history



Jonas Schnelli
@_jonasschnelli_

Bitcoin Core Git/GitHub Stats 2018:
* Total Pull Request Created: 1'451 (~3.98 per day)
* Merged Pull Requests: 1'305 (3.58 per day)
* GitHub Comments/Reviews: 26'185 (71.7 per day)
* Commits: 2'023 (5.5 per day)
* Git Contributors: 194
* GitHub Contributors: 1'131

7:34 AM - 3 Jan 2019

Bitcoin-**Core** is the continuation of the „BitCoin“ project started by Satoshi Nakamoto in 2009.

Bitcoin was rebranded as „Bitcoin **Core**“ Dec. 16th 2013
(deployed with version 0.9.0)

~98% of the active nodes are (based on) Bitcoin **Core.**

[1] estimation, node count is impossible in theory
[2] estimation is based on the coin.dance node counter

Who is behind Bitcoin **Core**?

- ✓ Open source volunteers distributed all over the world (~**50** total, ~**10** [very]active)
- ✓ No legal organisation
- ✓ No marketing or PR operations

Who can change the code of Bitcoin **Core**?

- ✓ Everyone can propose a change
- ✓ Everyone can comment on a proposed change
- ✓ Every proposal is public
- ✓ Scientific level discussions (no leadership judging)
- ✓ Reasonable changes will be **merged**

Which proposals are getting „**merged**“?

- ✓ Everyone can review, accept or decline a proposal
- ✓ If one declines a proposal, it needs reasonable arguments
- ✓ A reasonable amount of „accepts“ leads to a **merge**

Who can **merge**?

- ✓ Currently **5** maintainers

  Wladimir van der Laan (**lead**)

  Pieter Wuille / Jonas Schnelli / Marco Falke / Samuel Dobson
- ✓ Current maintainers can revoke or add new maintainers

Ultimative, „Users“ decide what is **Bitcoin**

By running a full node and validate / define the consensus rules

Users = Individuals, Miners, Businesses

Everyone can continue its own code-fork of „Bitcoin **Core**“

How about changing the „**consensus rules**“?

- ✓ Should use the BIP process
- ✓ Softfork

  (graceful upgrade)
- ✓ Hardforks

  (everyone needs to upgrade at a single point in time)

Softfork activation

- ✓ Was (and probably will be) triggered by **miners** **signaling** „readiness“
- ✓ Other methods have been proposed (UASF)
- ✓ No sudden decrease of network security

Bitcoin **Core** Project Decentralization

- ✓ Git (code is forked hundred times across the world)
- ✓ Multiple developers/maintainers across the world
- ✓ Complete redundant public record of discussions
- ✓ GPG signed git history

Binary distribution

- ✓ Deterministic build system for static binaries
- ✓ GPG signatures from various developers / maintainers
- ✓ GPG signatures from Bitcoin Core (lead maintainer)
- ✓ Association for centralized OS code signing

Companies actively putting resources at Bitcoin Core

Blockstream

C → H → A → I → N → C → O → D → E →

BLOCKCHAIN

BITMAIN

digital currency initiative

Digital Garage

Alternatives

btcd

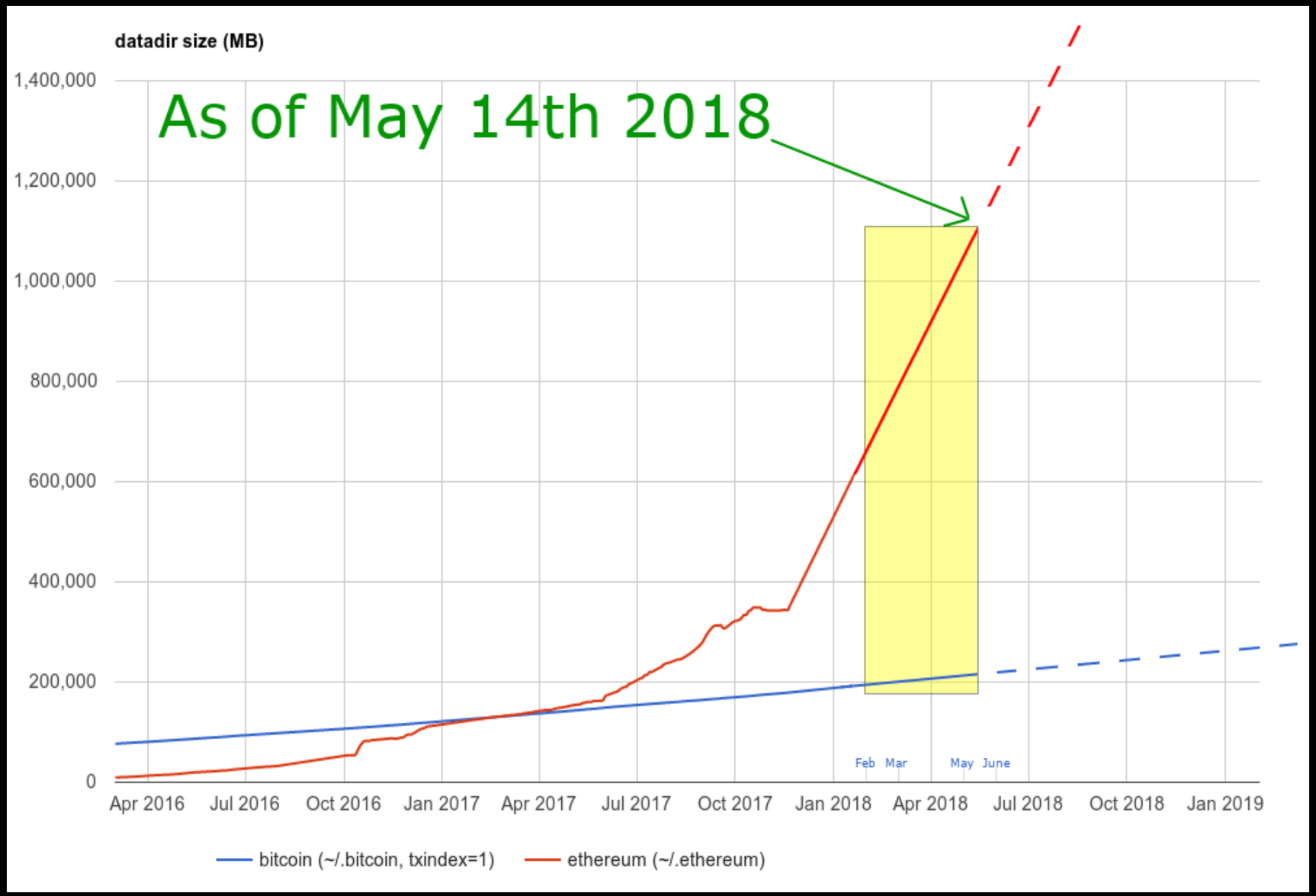
build passing | license ISC | godoc reference

bitcoinunlimited

The Ivory Tower?

Decentralization and **censorship resistance**

are two – if not the most – important properties of Bitcoin.


datadir size (MB)
As of May 14th 2018
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
Apr 2016
Jul 2016
Oct 2016
Jan 2017
Apr 2017
Jul 2017
Oct 2017
Jan 2018
Apr 2018
Jul 2018
Oct 2018
Jan 2019
Feb
Mar
May
June
bitcoin (~/.bitcoin, txindex=1)
ethereum (~/.ethereum)

March 2019

DataDir = ~225GB

220GB Blocks/Undos

UTXOs = 51’250’205

3.02 GB diskspace

Advanced Topics

- ✓ Pruning / Autopruning
- ✓ NODE_NETWORK_LIMITED
- ✓ Regtest
- ✓ User Interfaces
  - ✓ P2P
  - ✓ ZMQ
  - ✓ REST
  - ✓ RPC
- ✓ Gitian

Thanks, Q&A?

dev@jonasschnelli.ch

PGP: CA1A2908DCE2F13074C62CDE1EB776BB03C7922D

jonasschnelli

github.com/jonasschnelli