Unraveling Bitcoin [Core]

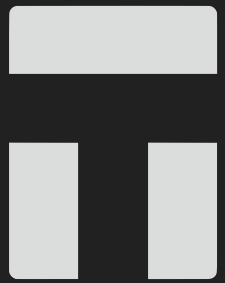
Andrew Pantyukhin

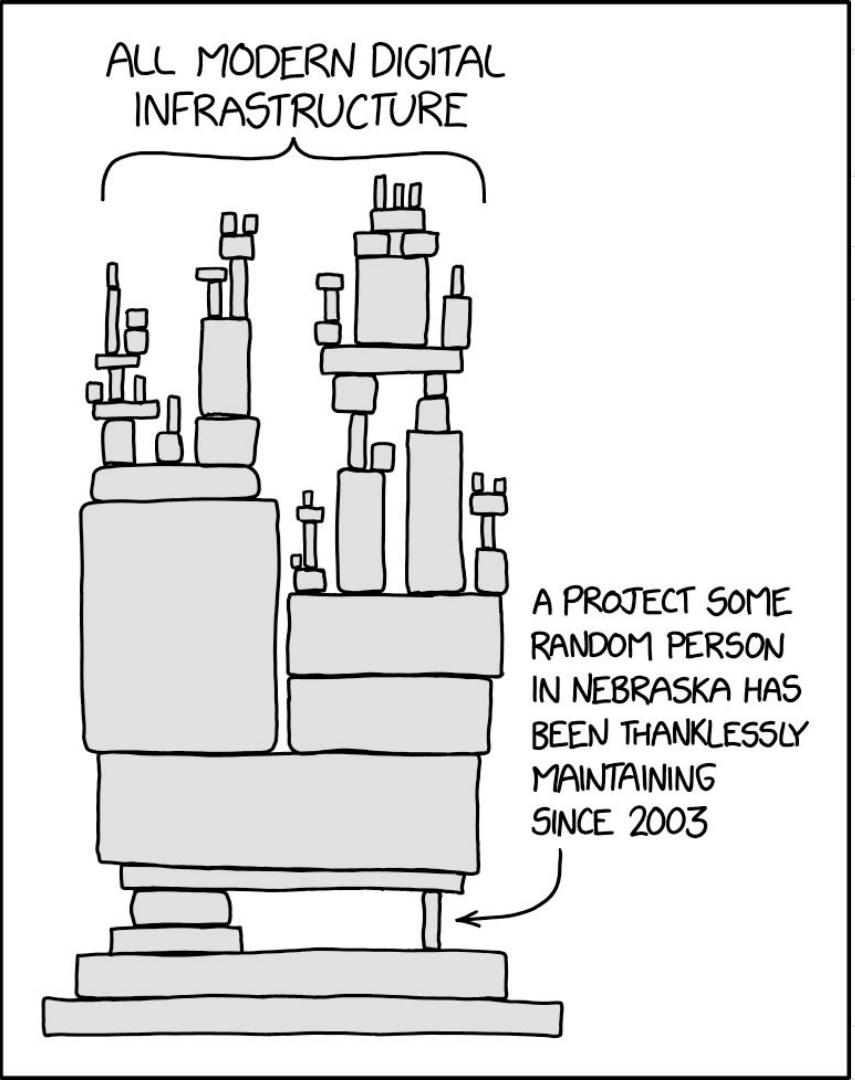
Aspects of Bitcoin

Divine Gift	Engineering Breakthrough	Proof of Concept
Saylor, Jack	Sjors, Lopp	Balaji, Vitalik

whoami(1)





btc-hn-1

RUN | SAVE QUERY | SHARE | SCHEDULE | MORE | Query compl

```
timestamp asc LIMIT 1000;
2  SELECT count(*)as btcposts,datetime_trunc(timestamp,year)as year FROM `bigquery-public-data.
   hacker_news.full` where contains_substr((title,text),'bitcoin') group by datetime_trunc(timestamp,
   year);
```

Press Option+F1 for Accessibility Options

Query results

SAVE RESULTS | EXPLORE DATA

B INFORMATION | RESULTS | CHART PREVIEW | JSON | EXECUTION DETAILS | EXECUTION

btcposts by year

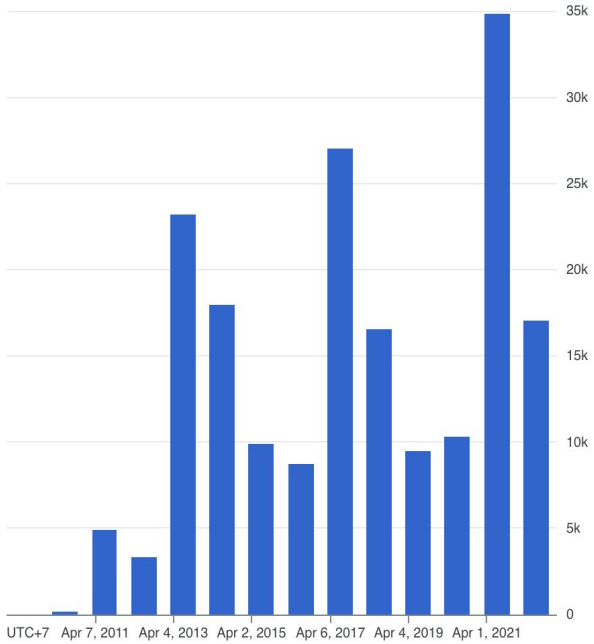


Chart configuration

Chart type
Bar

Dimension (x-axis)
year

Measures (y-axis)
btcposts

Select up to 5 measures

PERSONAL HISTORY | PROJECT HISTORY | REFRESH

Bitcoin's Future Depends on a Handful of Mysterious Coders

Developers with power to change the cryptocurrency's software hold an unorthodox role, are elusive—and have been known to head off disaster for the coin

[bitcoin-dev] Full Disclosure: CVE-2023-40231 / CVE-2023-40232 / CVE-2023-40233 / CVE-2023-40234 "All your mempool are belong to us"

Antoine Riard antoine.riard at gmail.com
Sat Oct 21 20:05:35 UTC 2023

- Previous message: [bitcoin-dev] Full Disclosure: CVE-2023-40231 / CVE-2023-40232 / CVE-2023-40233 / CVE-2023-40234 "All your mempool are belong to us"
- Next message: [bitcoin-dev] OP_Expire and Coinbase-Like Behavior: Making HTLCs Safer by Letting Transactions Expire Safely
- **Messages sorted by:** [date] [thread] [subject] [author]

Hi,

As I've been shown offline Twitter posts misrepresenting my previous mail,
I think it's good to correct them. The security flaws are not "intentional
backdoor" or whatever misrepresentation that would question the competence
and know-how of the Bitcoin and Lightning development community.

The replacement cycling issue discovered has been known by a small circle
of Bitcoin developers since December 2022. As it appears to some experts
and it has been commented publicly, changes at the bitcoin base-layer might
be the most substantial fixes. Those changes take time and here this is
akin to how the linux kernel, bsds and OS vendors are working [0].

All I can say is that we had recently had internal discussion on how to
improve coordinated security fixes and patching processes for the coming

Content

not a code dive

how do similar projects work

how Bitcoin [Core] differs

Core in Oct ‘23

25600 commits, up 2200 YoY

13500 merges, up 1100 YoY

300 open PRs, 19500 closed

330 open issues, 7300 closed

1200 authors, 120 in last year

25 maintainers, 7 in last year, **5 now**

CodeScene

BACK TO PROJECTS

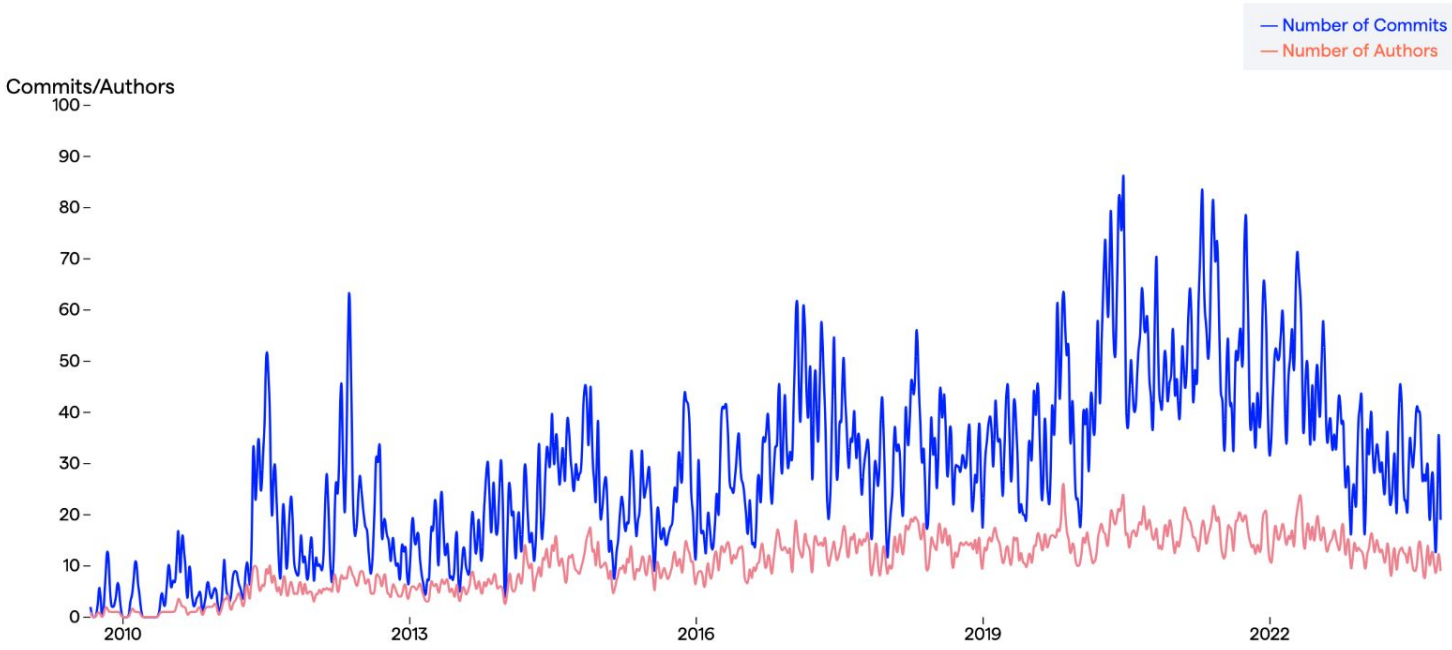
BITCOIN

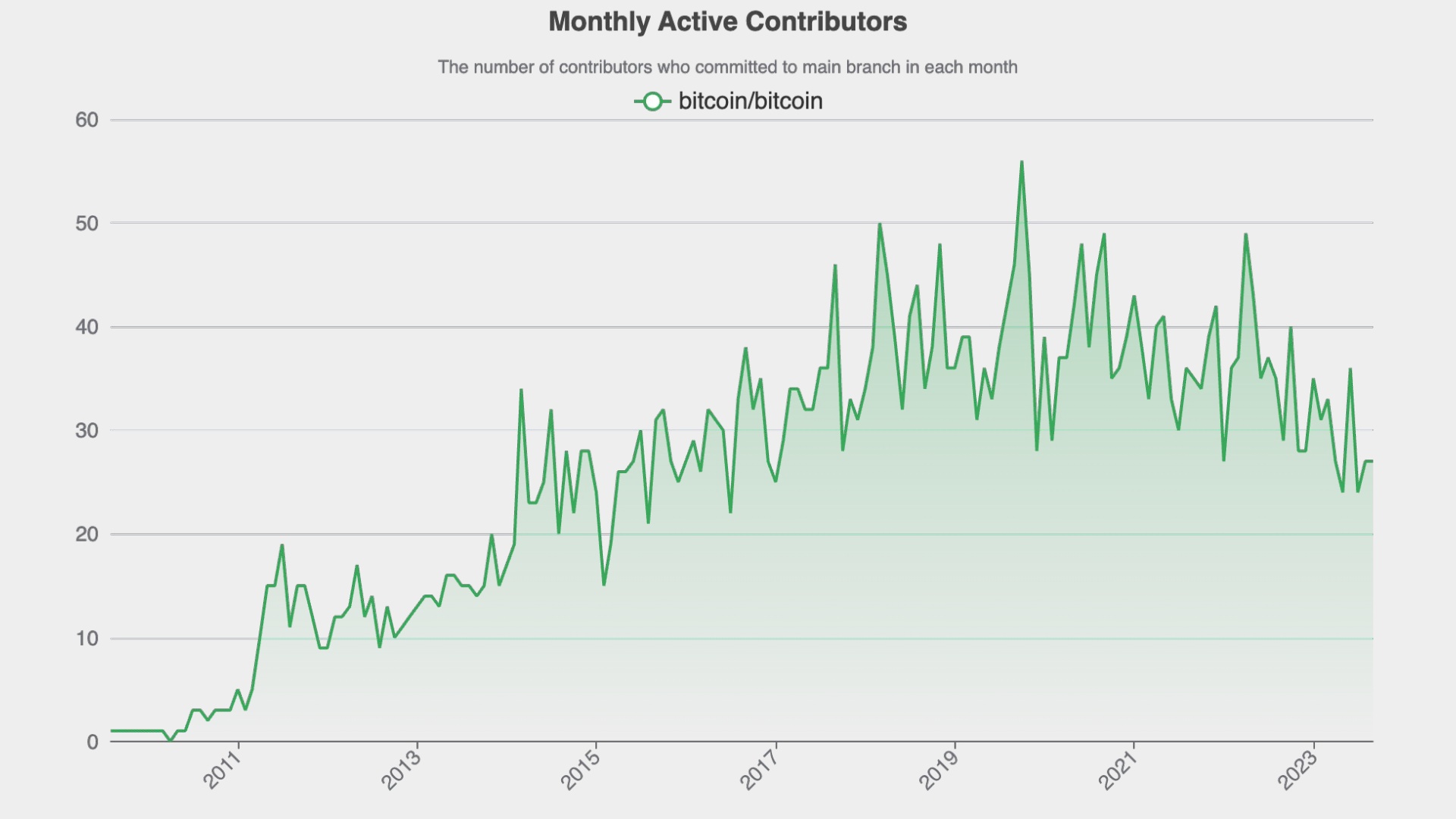
- Dashboard
- Scope
  - Analysis data
  - System trends
- Goals
- Code
- Architecture
- Team Dynamics
- System
- Delivery Performance
- Simulations

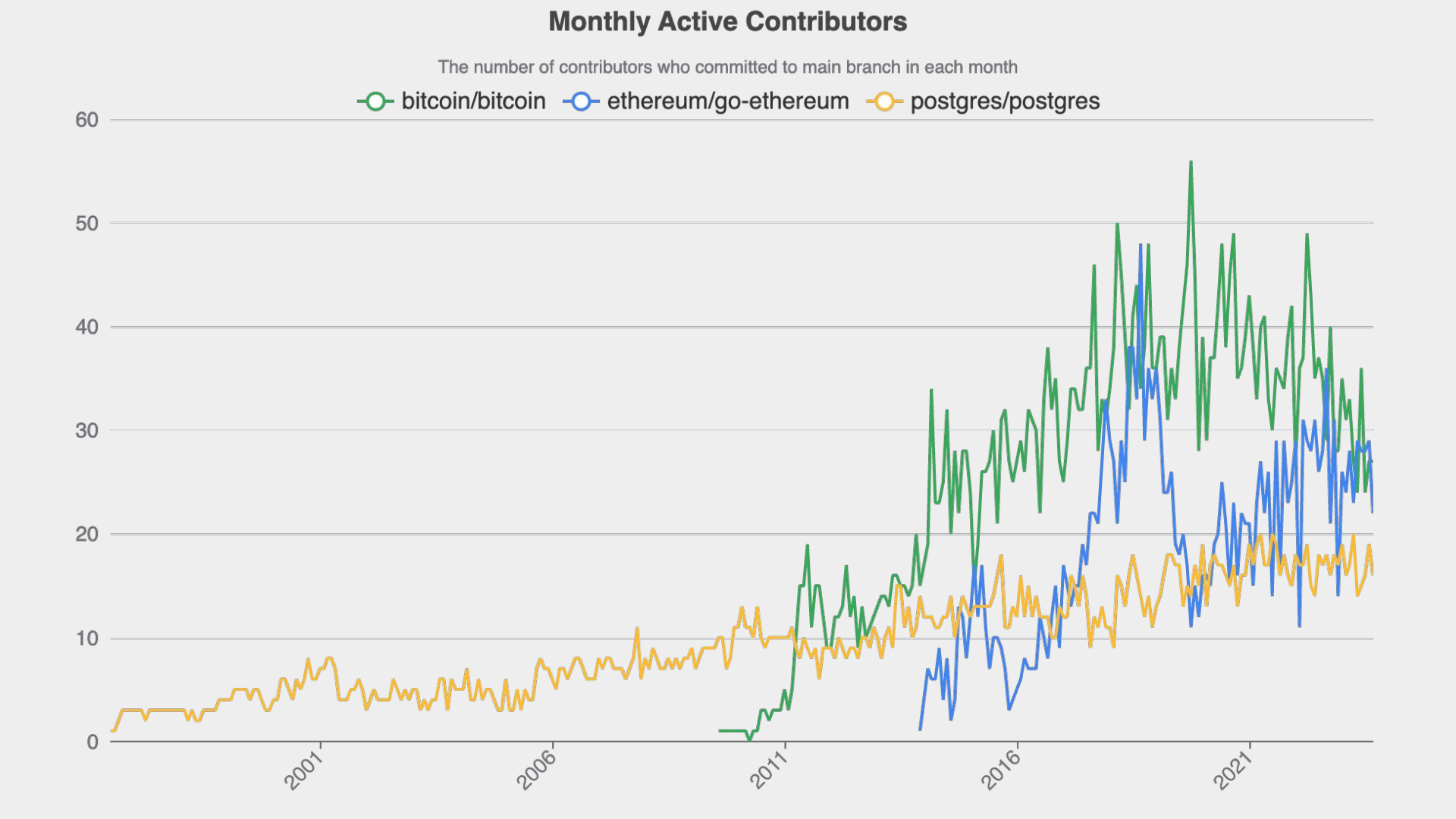
System Trends

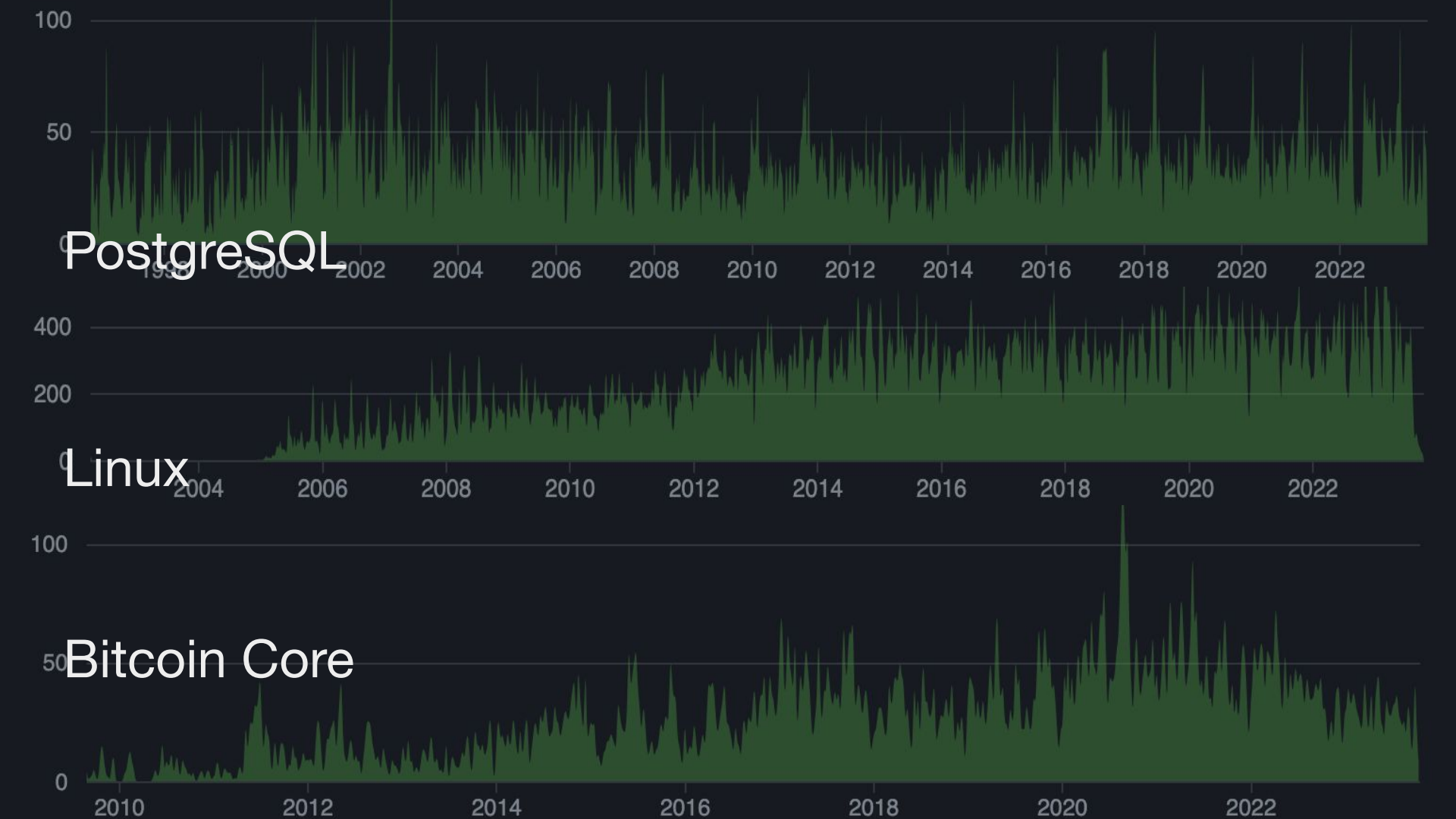
By Date | By Task | System Complexity | Component Trends | Code Age Trends | Change Frequency Distribution

Commit Activity Trend




Monthly Active Contributors
The number of contributors who committed to main branch in each month
bitcoin/bitcoin
60
50
40
30
20
10
0
2011
2013
2015
2017
2019
2021
2023


Monthly Active Contributors
The number of contributors who committed to main branch in each month
bitcoin/bitcoin
ethereum/go-ethereum
postgres/postgres
60
50
40
30
20
10
0
2001
2006
2011
2016
2021


100
50
0
1998
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
2022
PostgreSQL
400
200
0
2004
2006
2008
2010
2012
2014
2016
2018
2020
2022
Linux
100
50
0
2010
2012
2014
2016
2018
2020
2022
Bitcoin Core

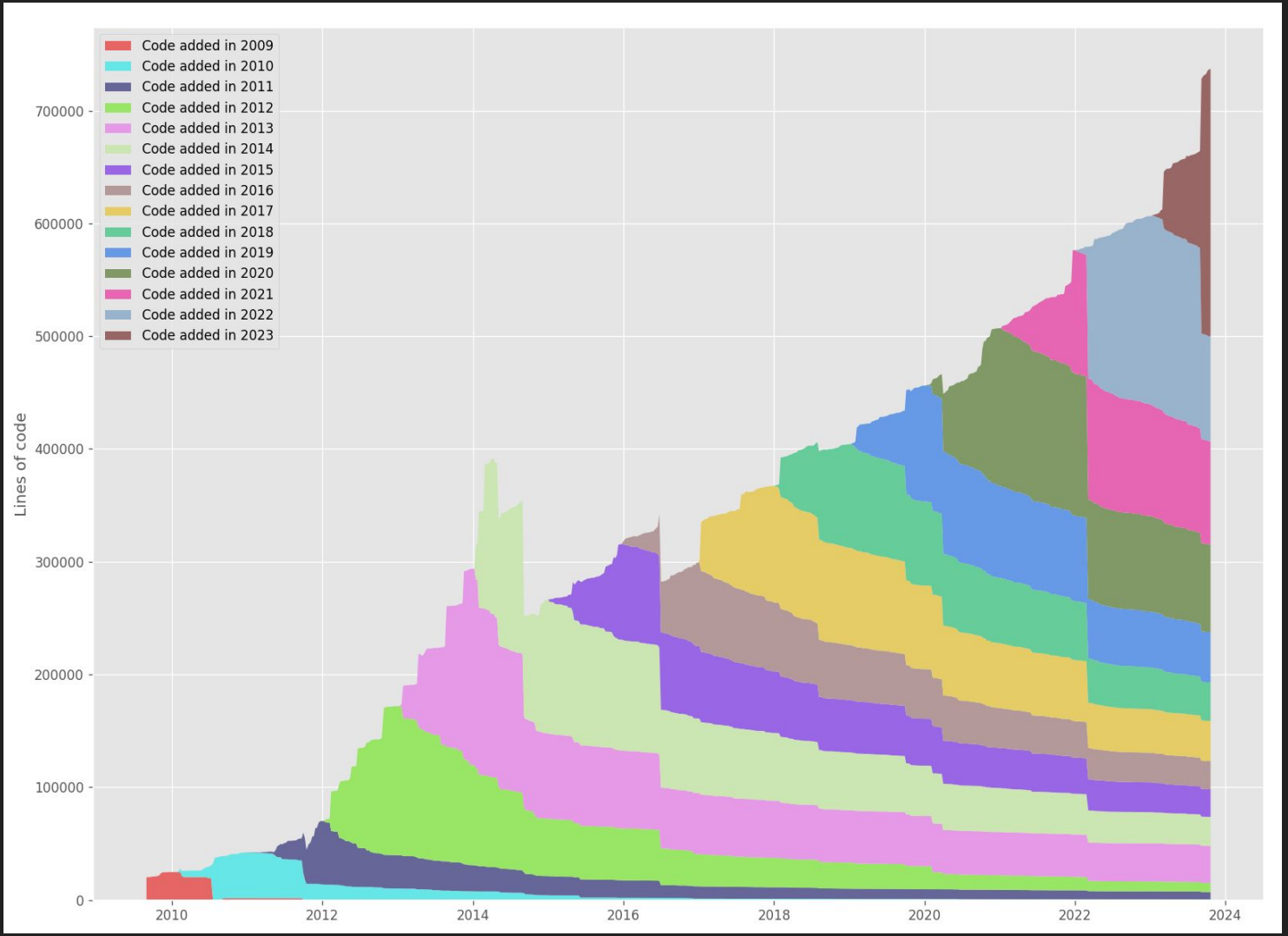
```
    2447 text files.
    2292 unique files.
     273 files ignored.

github.com/AlDanial/cloc v 1.98  T=2.50 s (917.8 files/s, 321670.4 lines/s)
```

Language	files	blank	comment	code
Qt Linguist	118	284	0	311983
C++	713	24966	22372	158045
Python	315	11546	11675	49216
C/C++ Header	532	11583	21145	48678
C	22	1200	1292	36155
Markdown	197	7165	40	28716
JSON	92	338	0	14000
Qt	19	2	0	8276
XML	22	31	0	6423
m4	18	939	191	5202
Bourne Shell	53	422	881	4733
make	59	558	288	3449
YAML	16	89	85	1252
CMake	14	172	138	1183
Text	5	14	0	1113
Bourne Again Shell	11	295	478	1070
diff	35	203	672	887
Assembly	1	84	105	726
SVG	20	8	15	697
Scheme	1	29	34	555
HTML	2	39	0	460
Fish Shell	6	50	48	209
Windows Resource File	6	19	0	184
Visual Studio Solution	1	0	1	161
Objective-C++	3	32	20	134
Dockerfile	3	14	17	52
Gradle	1	10	0	42
INI	1	5	0	21
Java	1	5	0	18
CSV	1	0	0	16
Qt Project	2	6	1	15
Properties	1	0	0	4
DOS Batch	1	0	0	1
SUM:	2292	60108	59498	683676

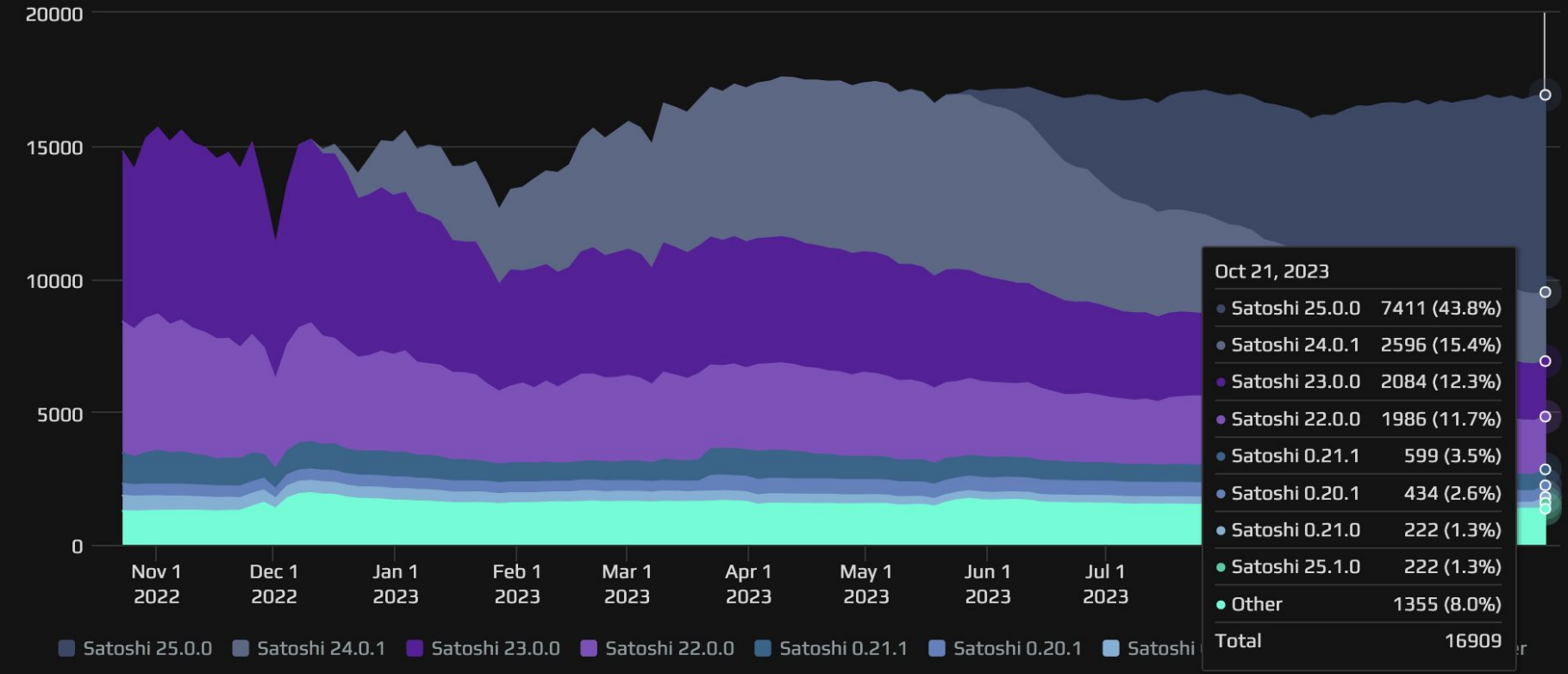
```
    2447 text files.
    2292 unique files.
     273 files ignored.

github.com/AlDanial/cloc v 1.98  T=2.50 s (917.8 files/s, 321670.4 lines/s)
-------------------------------------------------------------------------------
Language                     files          blank        comment           code
-------------------------------------------------------------------------------
Qt Linguist                    118            284              0         311983
C++                            713          24966          22372         158045
Python                         315          11546          11675          49216
C/C++ Header                   532          11583          21145          48678
C                               22           1200           1292          36155
Markdown                       197           7165             40          28716
JSON                            92            338              0          14000
Qt                              19              2              0           8276
XML                             22             31              0           6423
m4                              18            939            191           5202
```


Code added in 2009
Code added in 2010
Code added in 2011
Code added in 2012
Code added in 2013
Code added in 2014
Code added in 2015
Code added in 2016
Code added in 2017
Code added in 2018
Code added in 2019
Code added in 2020
Code added in 2021
Code added in 2022
Code added in 2023
Lines of code
0
100000
200000
300000
400000
500000
600000
700000
2010
2012
2014
2016
2018
2020
2022
2024

USER AGENTS

Chart shows the distribution of reachable Bitcoin nodes across leading user agents. Series can be enabled or disabled from the legend to view the chart for specific user agents.

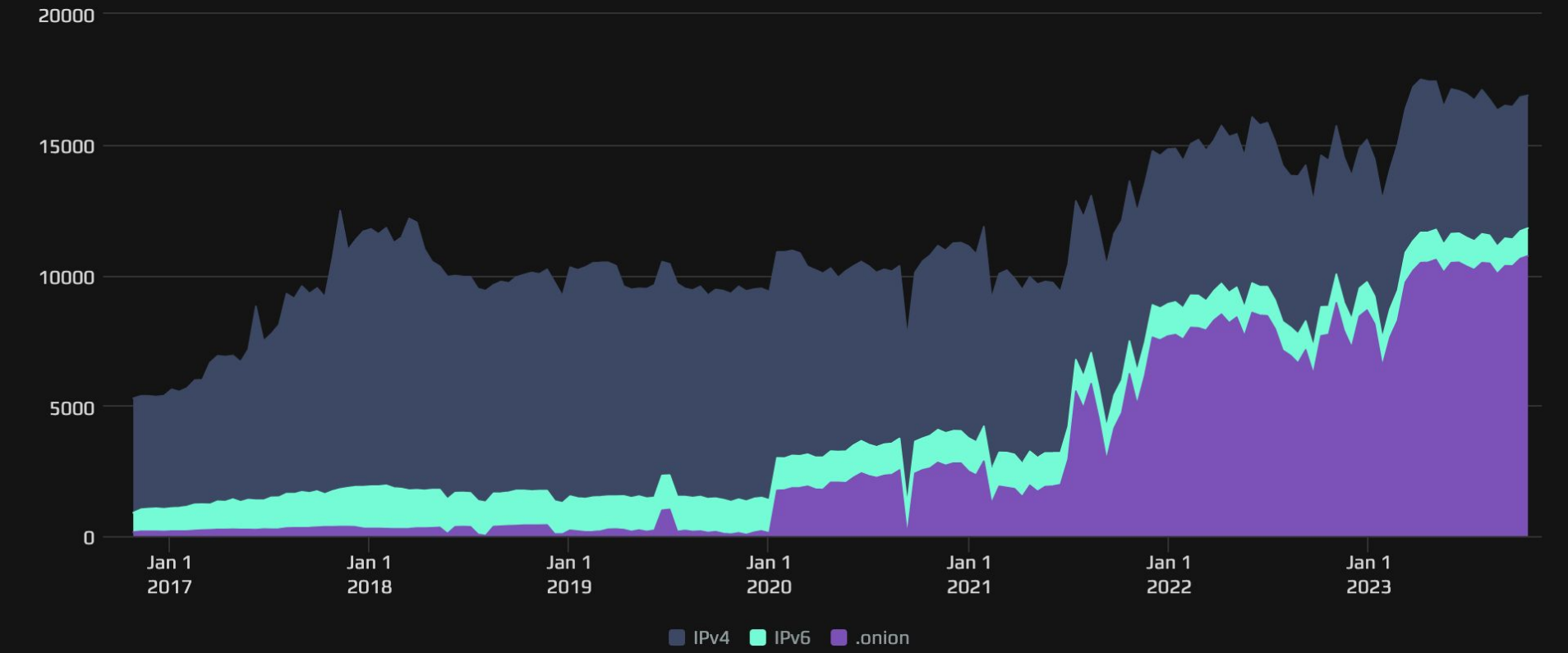


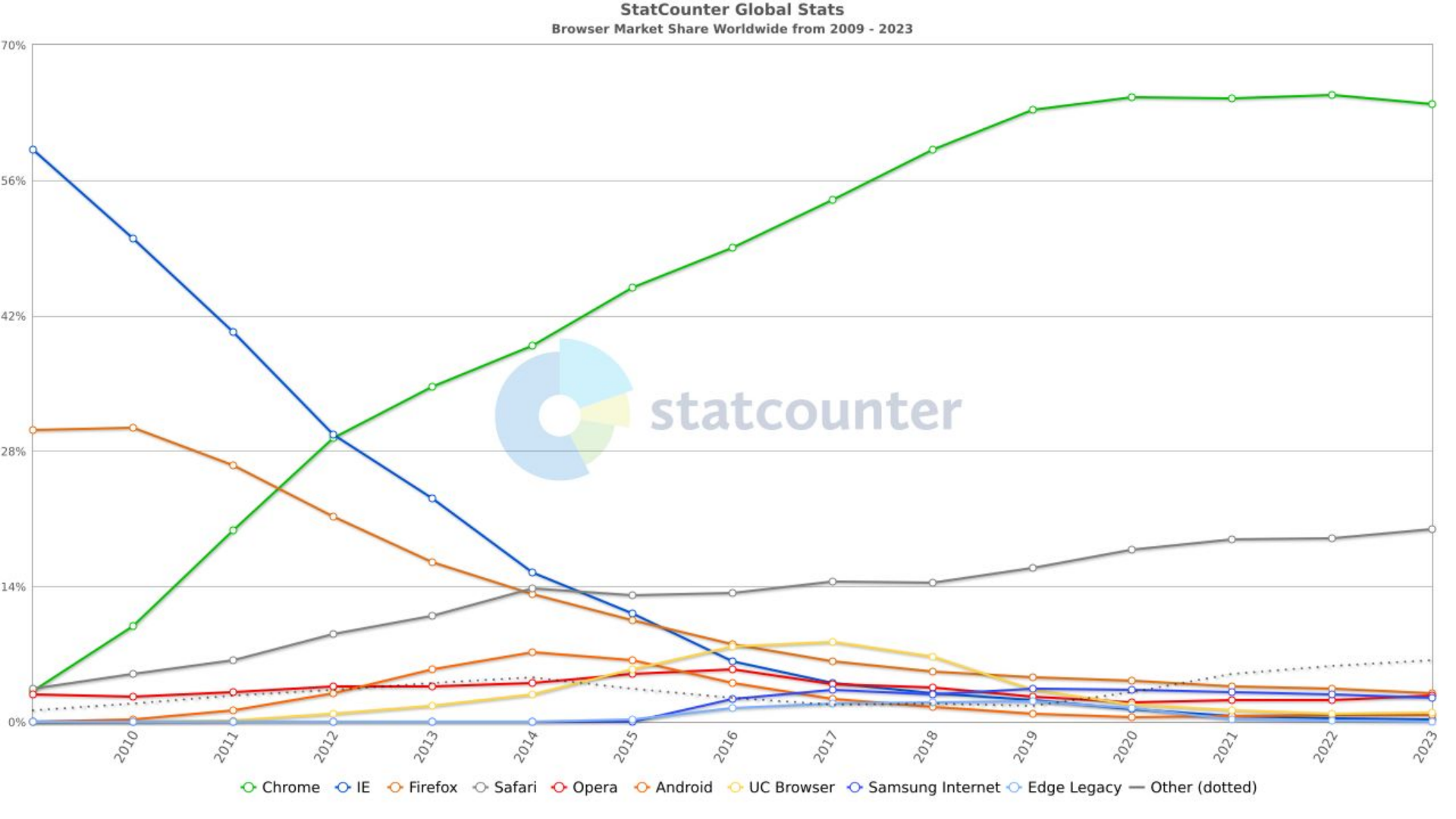
NODES

Chart shows the number of reachable Bitcoin nodes during the last 7 years. Series can be enabled or disabled from the legend to view the chart for specific networks.

24h | 90d | 1y | 7y

Lo 5277 Hi 17494 Avg 11331 Last 16878 nodes




StatCounter Global Stats
Browser Market Share Worldwide from 2009 - 2023
70%
56%
42%
28%
14%
0%
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
statcounter
Chrome
IE
Firefox
Safari
Opera
Android
UC Browser
Samsung Internet
Edge Legacy
Other (dotted)

Hugo Nguyen
@hugohanoi

I'm a Bitcoin Core maximalist, because I don't trust any persons or groups to be able to replicate Core software 100% correctly. It doesn't matter how good you are as a dev.

Maybe in 20 years AI will be advanced enough to change this. But until then, Core all the way.

> 
> **Hugo Nguyen** @hugohanoi · Nov 2, 2022
> Replying to @hugohanoi
> Another reason to stick to Bitcoin Core for consensus: consensus is so hard (and 10x more critical for a monetary base protocol), even Core must honor its past selves!
>
> twitter.com/hugohanoi/stat...

12:37 PM · Nov 2, 2022

Hugo Nguyen
@hugohanoi

That’s because unlike most other software and protocols we know, in Bitcoin the implementation _is_ the spec.

Not just any spec, but the soul of a live, 14-year running network that millions of people depend on. So we have to make do of what we have. Improvise.

11:54 PM · Nov 1, 2022

1 4 1

The total word count of the W3C specification catalogue is 114 million words at the time of writing. If you added the combined word counts of the C11, C++17, UEFI, USB 3.2, and POSIX specifications, all 8,754 published RFCs, and the combined word counts of everything on Wikipedia's list of longest novels, you would be 12 million words short of the W3C specifications.[2]

I conclude that **it is impossible to build a new web browser**. The complexity of the web is *obscene*. The creation of a new web browser would be comparable in effort to the Apollo program or the Manhattan project.

It is impossible to:

- Implement the web correctly
- Implement the web securely
- Implement the web **at all**

if Bitcoin grows to be *defined* by a million words, we won't own Bitcoin anymore

New Ideas in Tech

Proof of Concept

Protocol

Reference Implementation

Production Implementations (alpha, beta, 1.0, …)

various competing vendors, mostly interoperable

New Ideas in Tech

TCP/IP DNS WWW SMTP

H264 GPT/LLM BitTorrent

JS OpenGL SQL

Bitcoin 2007–2010

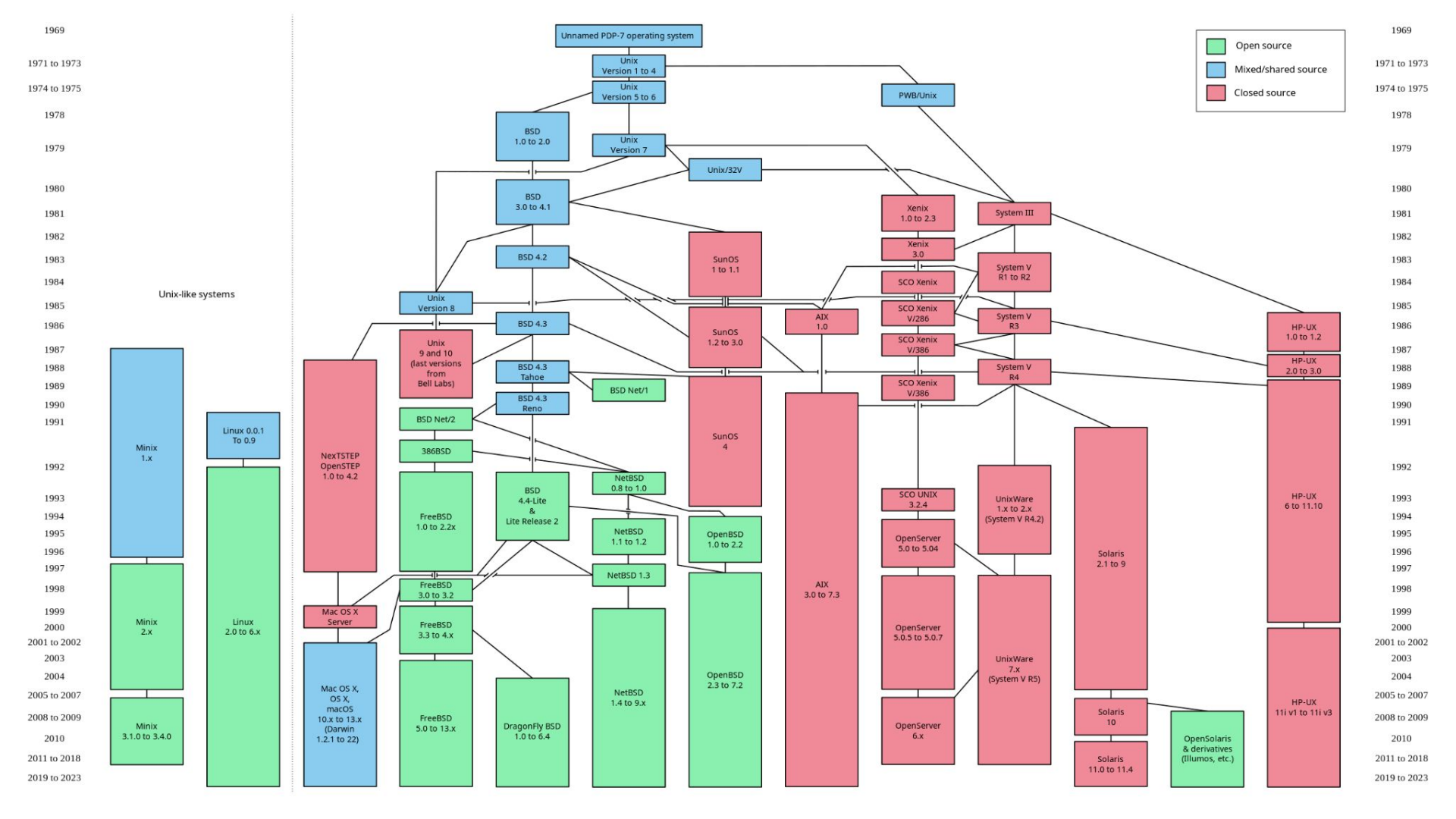
Whitepaper + 0.1.0~0.3.19 = refined PoC,

implied future ref and spec that never came

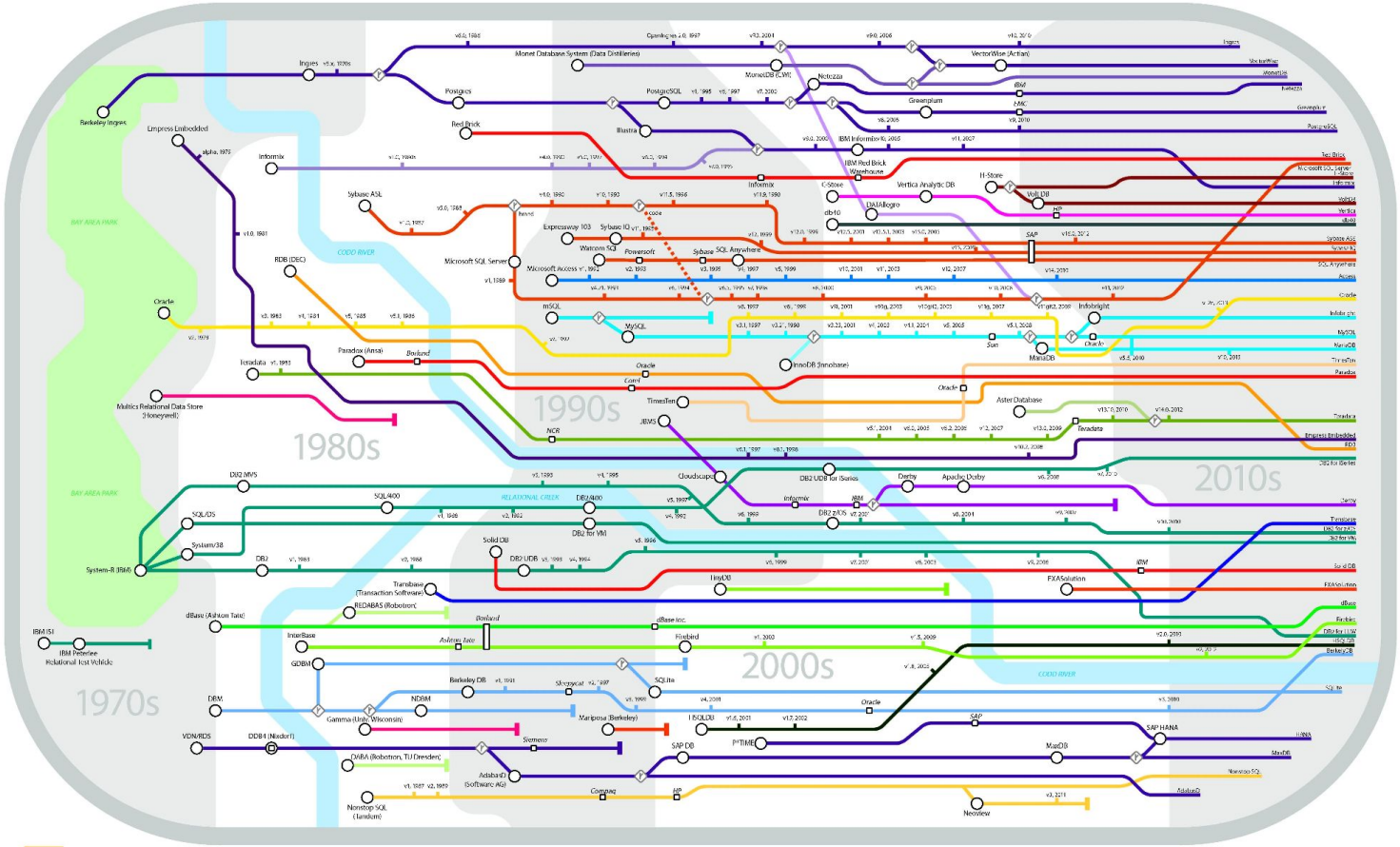
Bitcoin [Core] 2011–now

Ongoing attempts to document and reimplement

Open-Source Forks
!= Bitcoin Forks


1969
1971 to 1973
1974 to 1975
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001 to 2002
2003
2004
2005 to 2007
2008 to 2009
2010
2011 to 2018
2019 to 2023
Open source
Mixed/shared source
Closed source
Unix-like systems
Minix 1.x
Minix 2.x
Minix 3.1.0 to 3.4.0
Linux 0.0.1 To 0.9
Linux 2.0 to 6.x
Unnamed PDP-7 operating system
Unix Version 1 to 4
Unix Version 5 to 6
Unix Version 7
PWB/Unix
BSD 1.0 to 2.0
Unix/32V
BSD 3.0 to 4.1
BSD 4.2
Xenix 1.0 to 2.3
Xenix 3.0
SCO Xenix
SCO Xenix V/286
SCO Xenix V/386
System III
System V R1 to R2
System V R3
System V R4
SunOS 1 to 1.1
SunOS 1.2 to 3.0
SunOS 4
AIX 1.0
AIX 3.0 to 7.3
Unix Version 8
Unix 9 and 10 (last versions from Bell Labs)
BSD 4.3
BSD 4.3 Tahoe
BSD 4.3 Reno
BSD Net/1
BSD Net/2
386BSD
FreeBSD 1.0 to 2.2x
FreeBSD 3.0 to 3.2
FreeBSD 3.3 to 4.x
FreeBSD 5.0 to 13.x
BSD 4.4-Lite & Lite Release 2
DragonFly BSD 1.0 to 6.4
NetBSD 0.8 to 1.0
NetBSD 1.1 to 1.2
NetBSD 1.3
NetBSD 1.4 to 9.x
OpenBSD 1.0 to 2.2
OpenBSD 2.3 to 7.2
NeXTSTEP OpenSTEP 1.0 to 4.2
Mac OS X Server
Mac OS X, OS X, macOS 10.x to 13.x (Darwin 1.2.1 to 22)
SCO UNIX 3.2.4
OpenServer 5.0 to 5.04
OpenServer 5.0.5 to 5.0.7
OpenServer 6.x
UnixWare 1.x to 2.x (System V R4.2)
UnixWare 7.x (System V R5)
Solaris 2.1 to 9
Solaris 10
Solaris 11.0 to 11.4
OpenSolaris & derivatives (Illumos, etc.)
HP-UX 1.0 to 1.2
HP-UX 2.0 to 3.0
HP-UX 6 to 11.10
HP-UX 11i v1 to 11i v3

Genealogy of Relational Database Management Systems



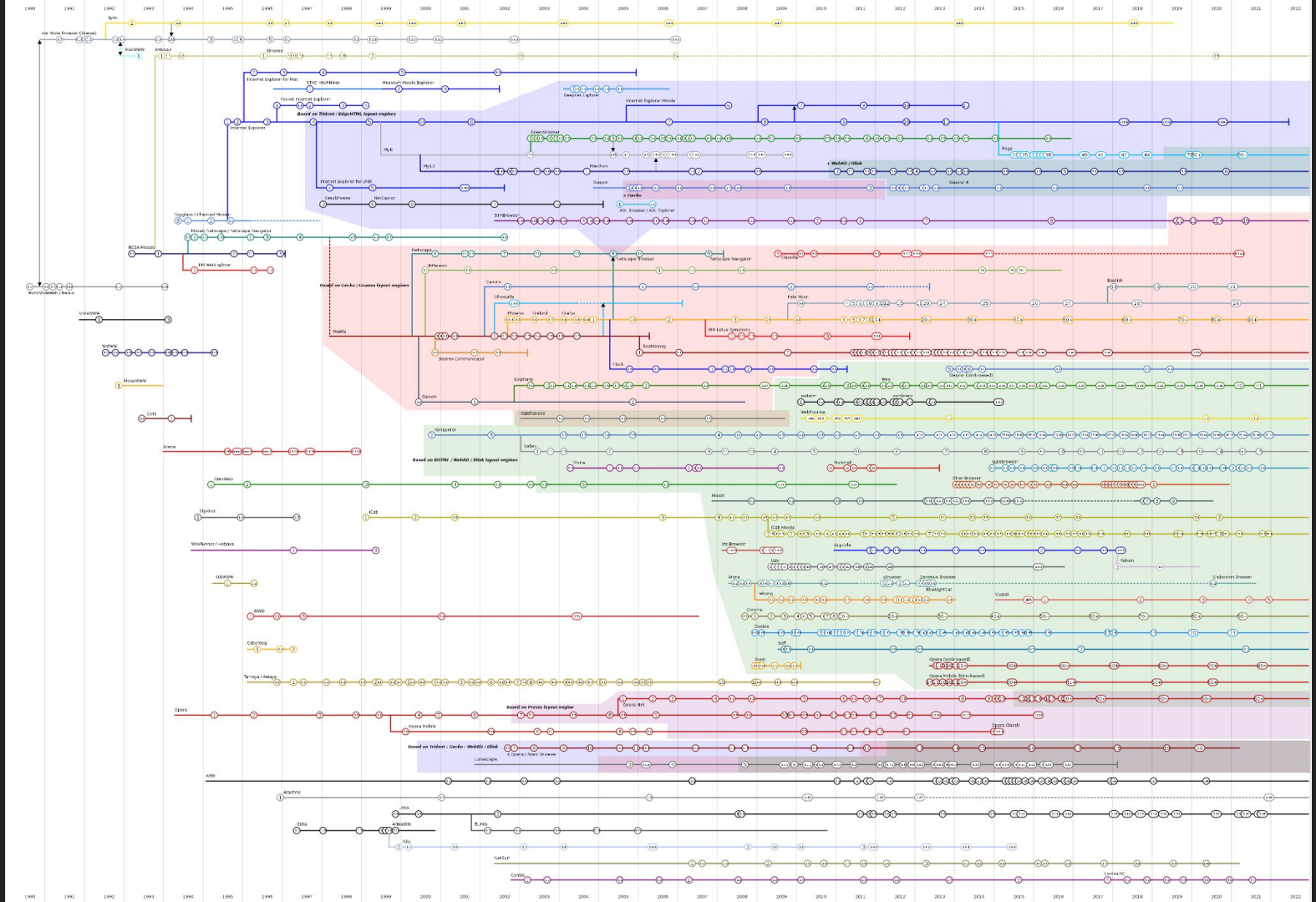
HPI Hasso Plattner Institut
IT Systems Engineering | Universität Potsdam

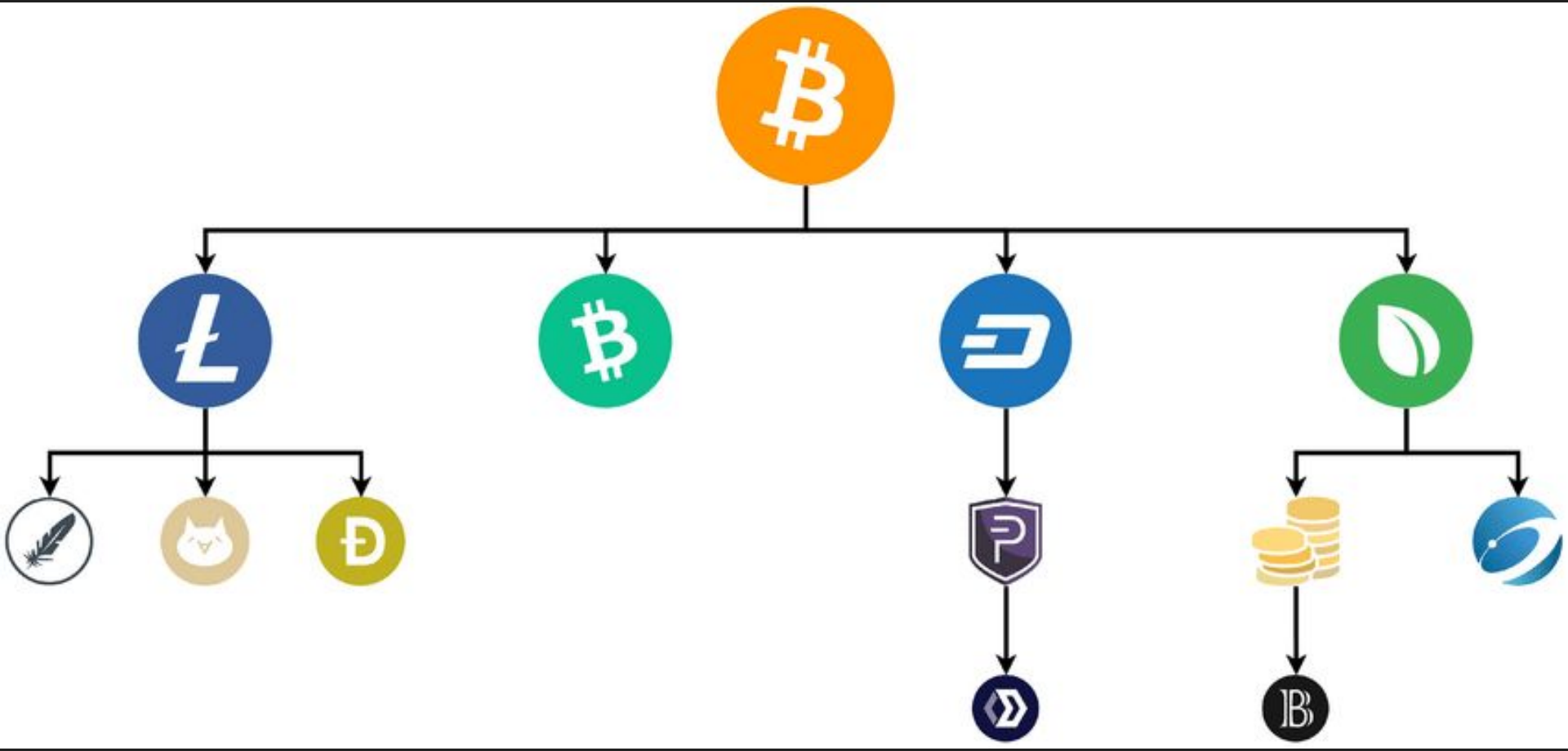
Key to lines and symbols

Publishing Date | Acquisition | Versions | Discontinued | Branch (Intellectual and/or code) | Crossing lines have no special semantics

Felix Naumann, Jana Bauckmann, Claudia Exeler, Jan-Peer Rudolph, Fabian Tschirschnitz
Contact - Hasso Plattner Institut, Potsdam, Felix.Naumann@hpi.uni-potsdam.de
Design - Alexander Sandt Grafik-Design, Hamburg

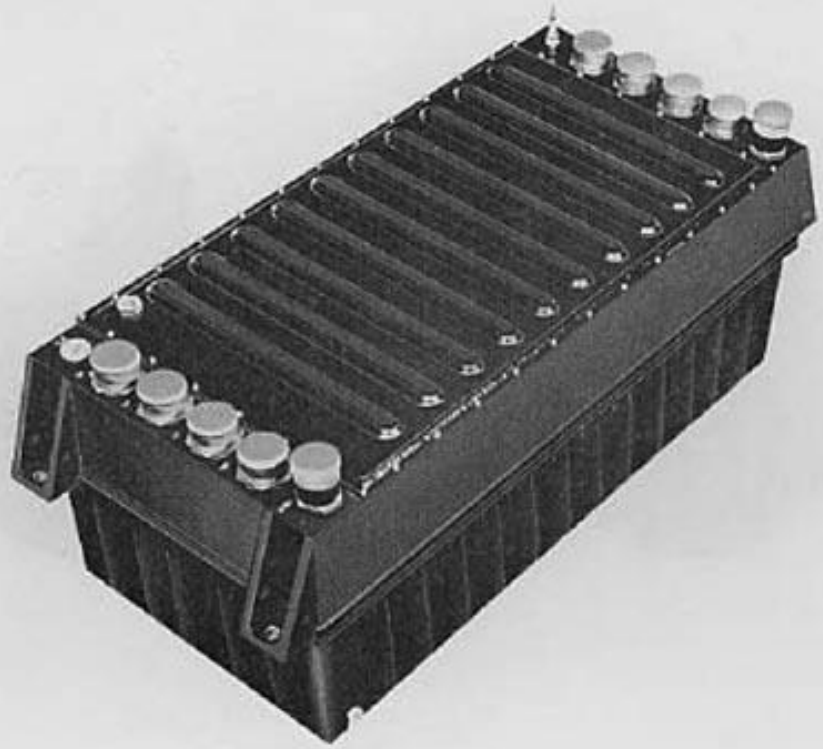
Version 4.0 - August 2013
http://www.hpi.uni-potsdam.de/naumann/projekte/rdbms_genealogy.html


Based on Trident / EdgeHTML layout engines
Based on Gecko / Gnumma layout engines
Based on KHTML / WebKit / Blink layout engines
Based on Presto layout engine
Based on Trident + Gecko + WebKit / Blink

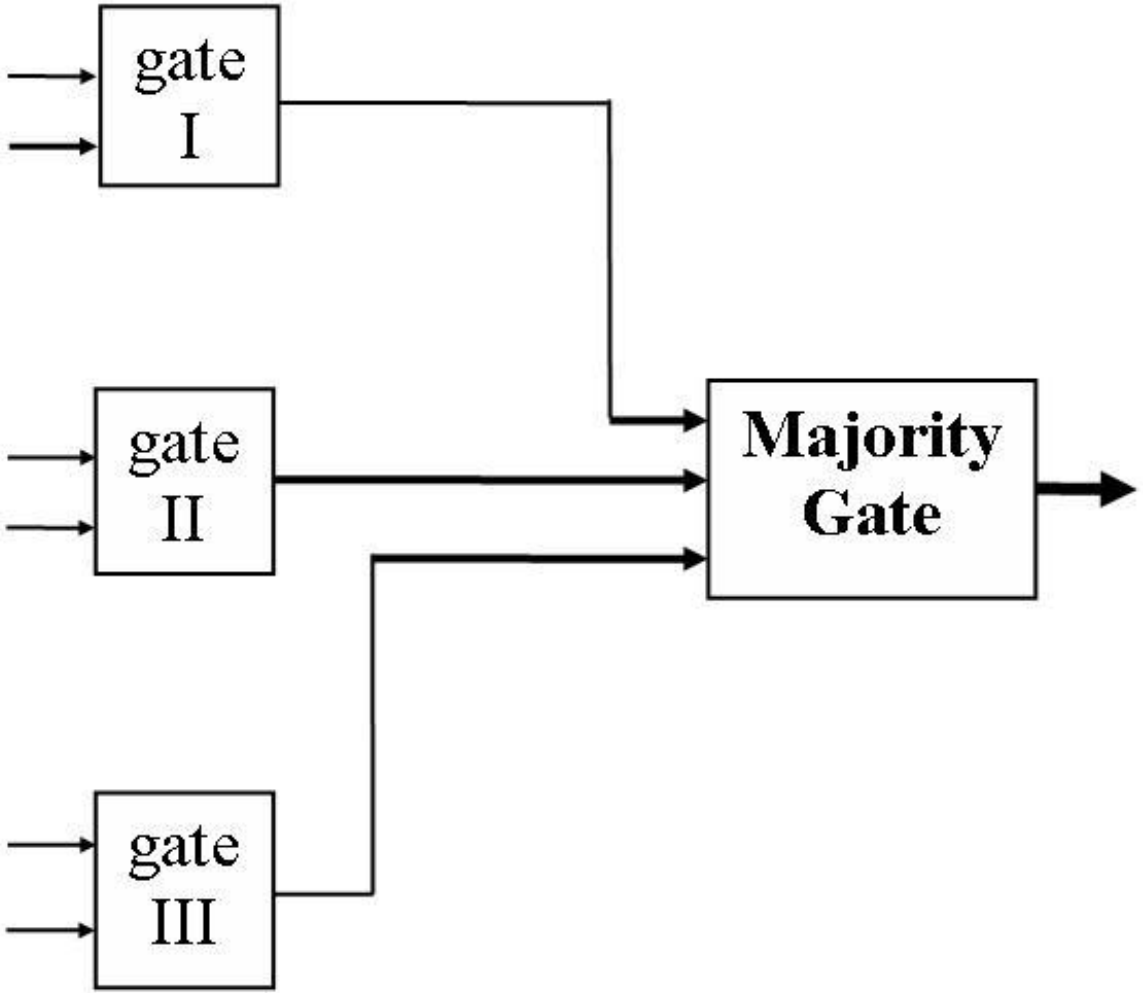


Software Reliability

IU



IBM N37


gate
I
gate
II
gate
III
Majority
Gate

An Attack Surface Metric Suitable for Heterogeneous Redundant System with the Voting Mechanism

Liqun Wang, Zheng Zhang, Weichao Li, Zhenwu Liu and Hao Liu

State key Laboratory of Mathematical Engineering and Advanced Computing, MEAC, Zhengzhou, Henan, 450001, China

*Corresponding author's e-mail: standoutking@126.com

Abstract. With the development of cyberspace security "asymmetry in attack and defense", heterogeneous redundancy design is gradually being widely used. Heterogeneous redundancy design can enhance the robustness and security of the system through the differentiation of heterogeneous components. But the complex structural design of the system makes it difficult to apply the existing attack surface metric to measure the security of heterogeneous redundant system. In this paper, based on the attack surface metric proposed by Manadhata, we provide a new attack surface metric suitable for heterogeneous redundant system with voting mechanism. In this new metric, we define a new notion named attack surface arbitration, and also propose a new method for quantifying result of arbitration. The experiment result shows that the new attack surface metric can properly describe the attack surface of a heterogeneous redundant system with voting mechanism, which changes with the adjustment of voting algorithm.


提訴
CODE:263
FILE:MAGI.SYS
EXTENTION:2004
EX_MODE:OFF
PRIORITY:AAA
決議
審議中
CASPER・3
MAGI
MELCHIOR・1

Computer Science > Logic in Computer Science

[Submitted on 5 Jul 2023]

Towards a Formal Verification of the Lightning Network with TLA+

Matthias Grundmann, Hannes Hartenstein

Payment channel networks are an approach to improve the scalability of blockchain-based cryptocurrencies. Because payment channel networks are used for transfer of financial value, their security in the presence of adversarial participants should be verified formally. We formalize the protocol of the Lightning Network, a payment channel network built for Bitcoin, and show that the protocol fulfills the expected security properties. As the state space of a specification consisting of multiple participants is too large for model checking, we formalize intermediate specifications and use a chain of refinements to validate the security properties where each refinement is justified either by model checking or by a pen-and-paper proof.

Subjects: **Logic in Computer Science (cs** ter
Computing (cs.DC)

Cite as: arXiv:2307.02342 [cs.LO]

(or arXiv:2307.02342v1 [cs.LO]

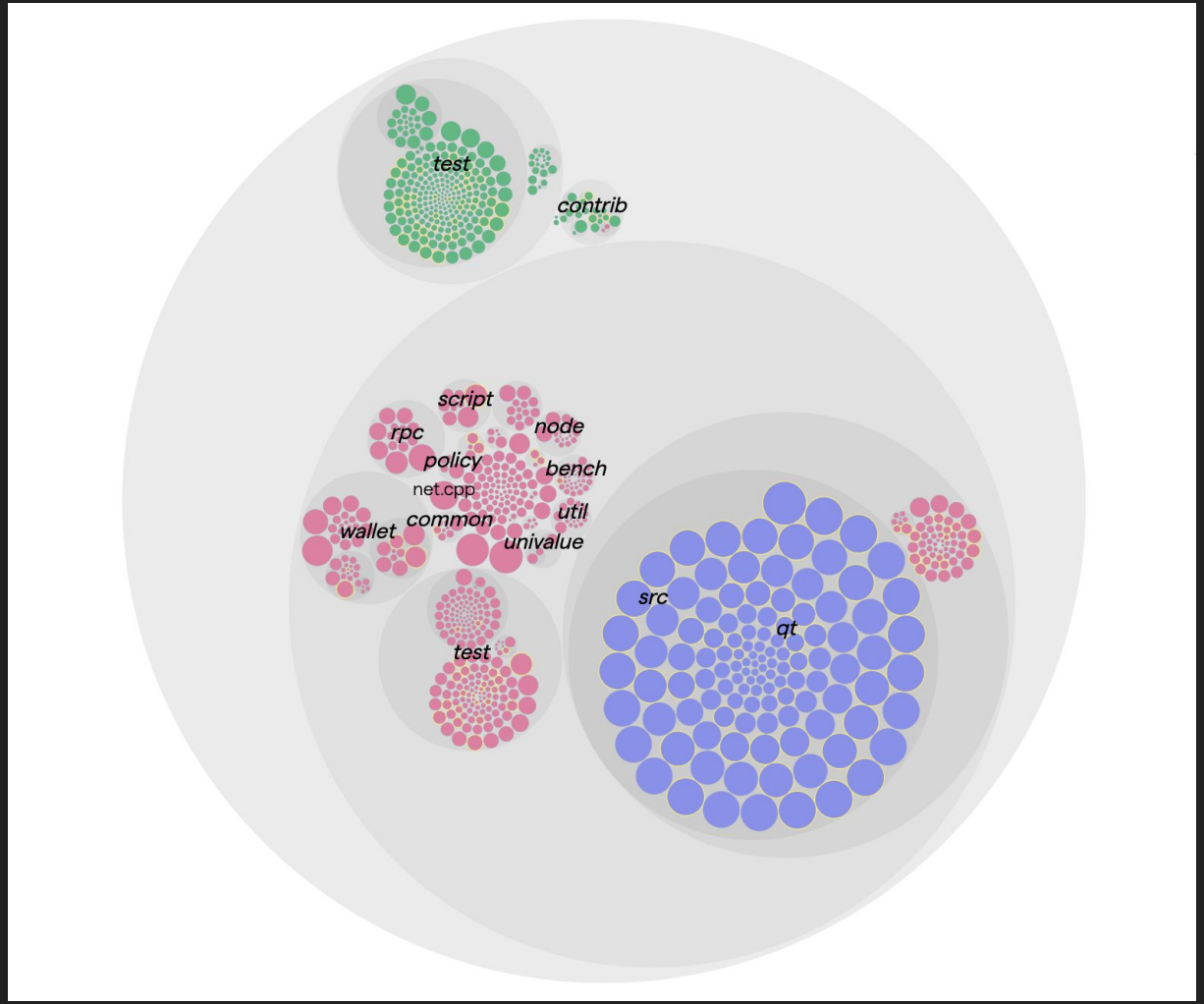
https://doi.org/10.48550/arXi

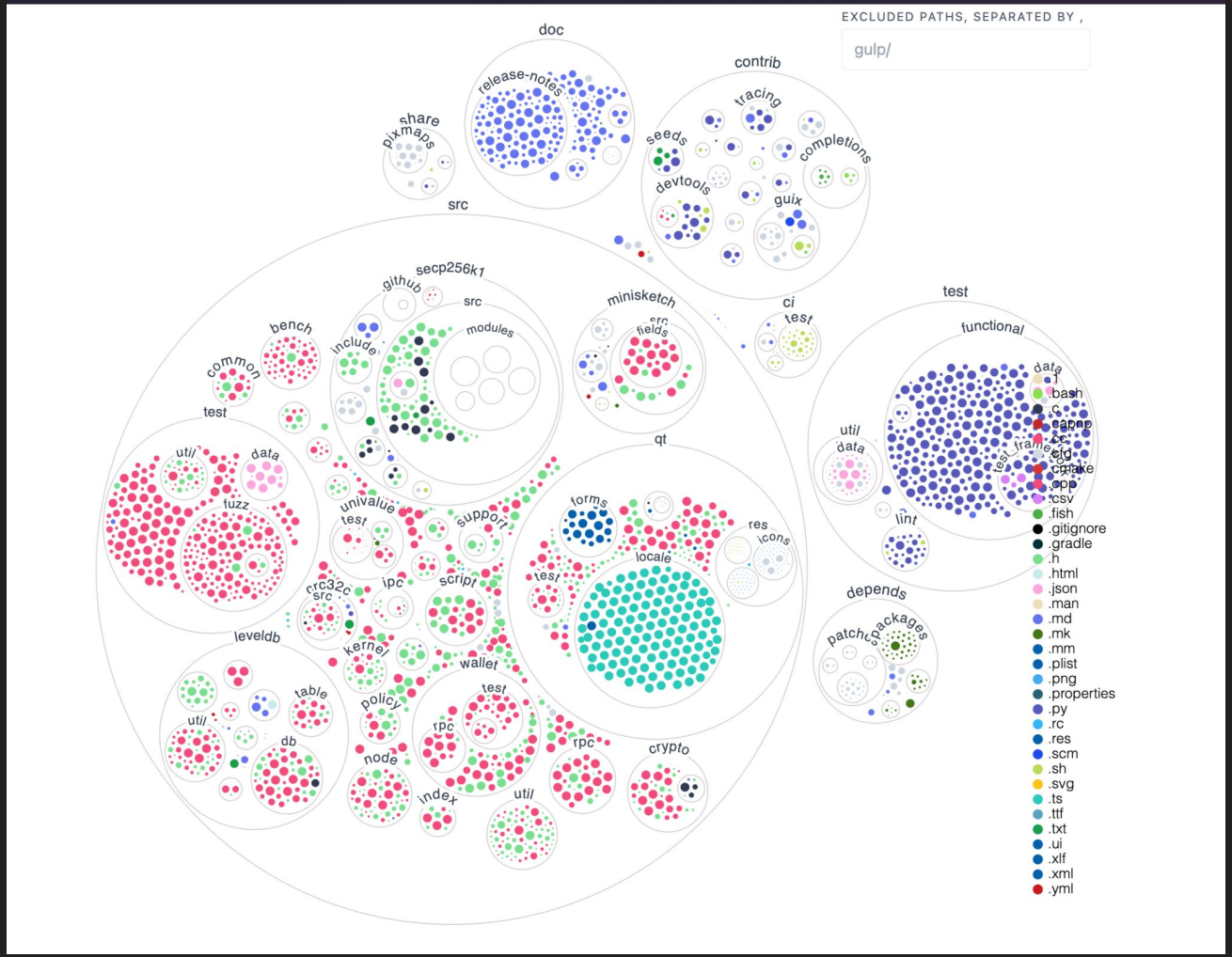
Submission history

From: Matthias Grundmann [view email]

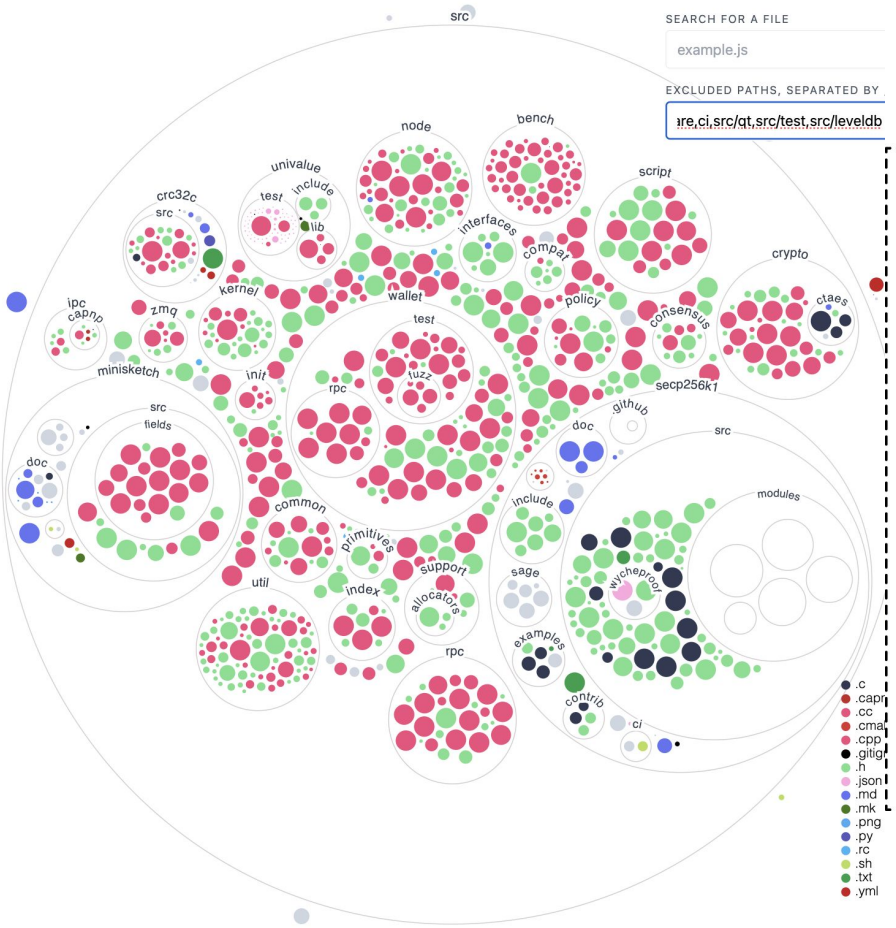
[v1] Wed, 5 Jul 2023 14:56:03 UTC (237 KB)

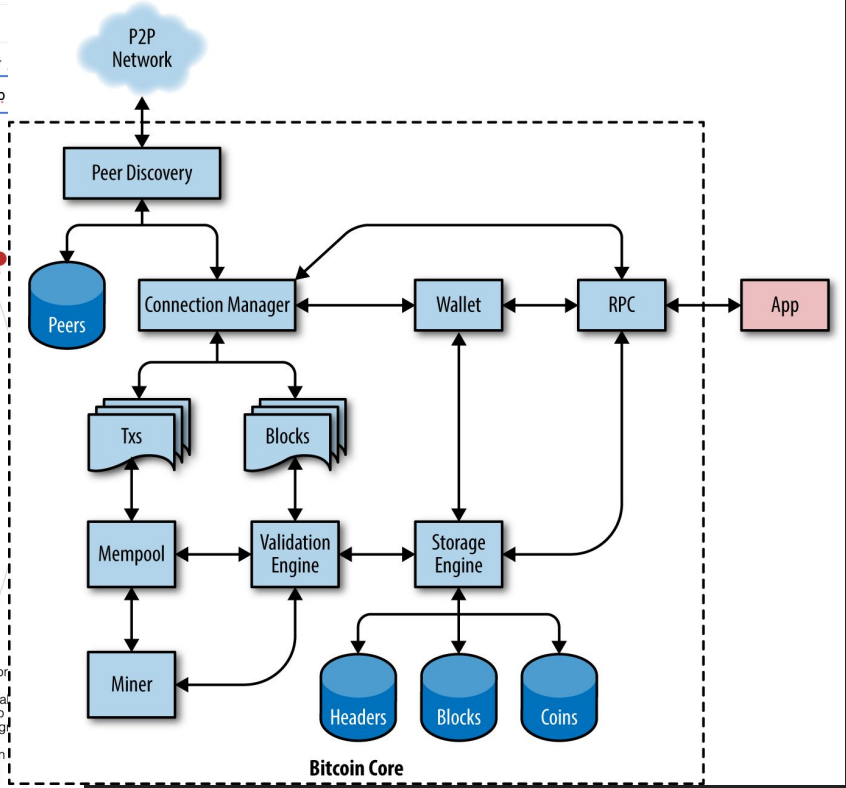
Core Code

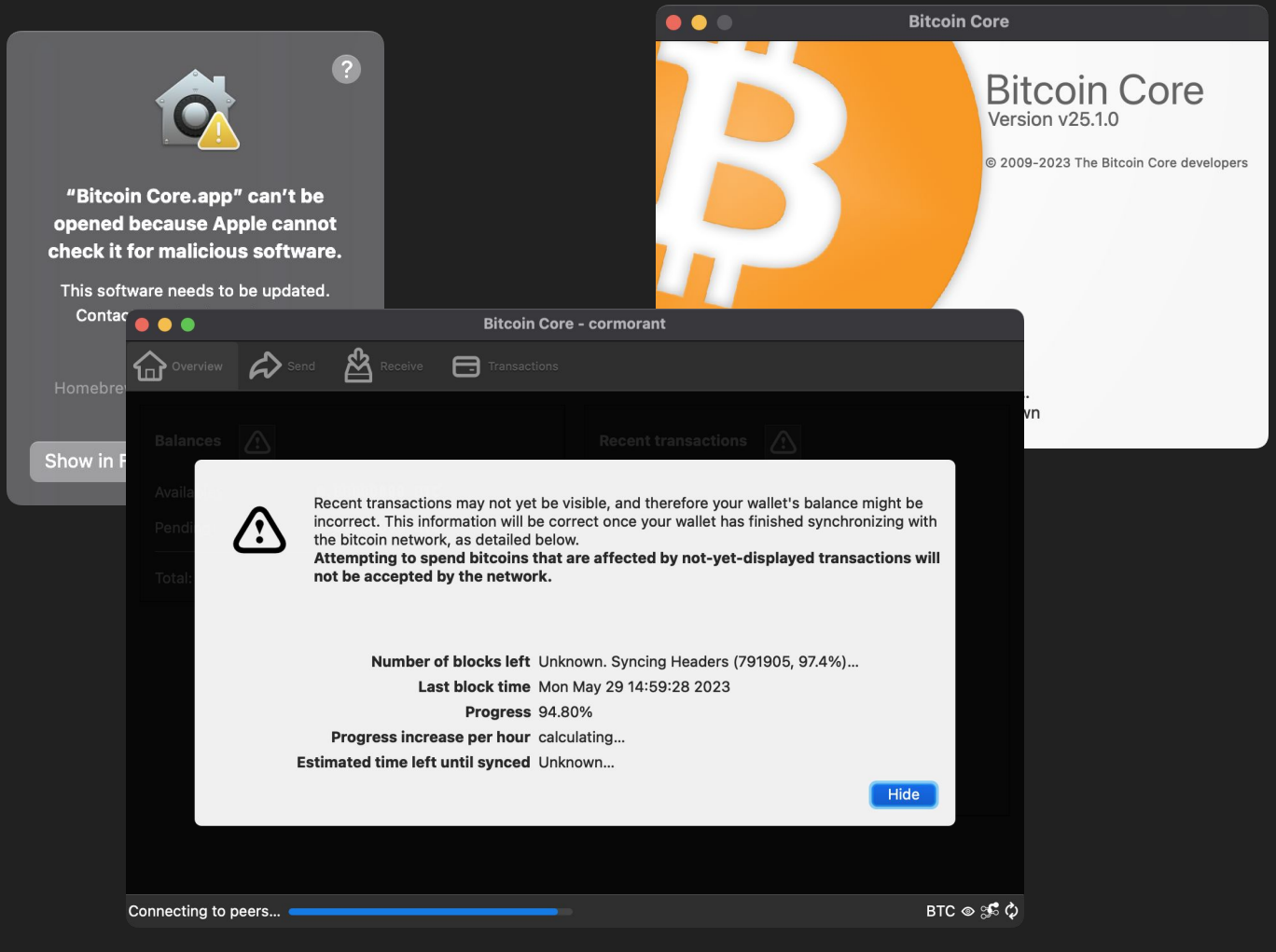

test
contrib
script
rpc
node
policy
bench
net.cpp
util
common
wallet
univalue
test
src
qt


EXCLUDED PATHS, SEPARATED BY ,
gulp/
doc
release-notes
contrib
tracing
seeds
completions
devtools
guix
share
pixmaps
src
secp256k1
github
src
modules
include
bench
common
test
util
data
fuzz
minisketch
src
fields
ci
test
qt
forms
locale
test
res
icons
univalue
test
support
script
ipc
crc32c
src
kernel
wallet
leveldb
table
util
db
policy
node
index
rpc
test
rpc
crypto
util
test
functional
data
util
data
test
framework
lint
depends
patches
packages
.bash
.c
.cpp
.cc
.cmake
.csv
.fish
.gitignore
.gradle
.h
.html
.json
.man
.md
.mk
.mm
.plist
.png
.properties
.py
.rc
.res
.scm
.sh
.svg
.ts
.ttf
.txt
.ui
.xlf
.xml
.yml

bitcoin/bitcoin






"Bitcoin Core.app" can't be opened because Apple cannot check it for malicious software.
This software needs to be updated.
Contac
Homebre
Show in F
Bitcoin Core
Bitcoin Core
Version v25.1.0
© 2009-2023 The Bitcoin Core developers
Bitcoin Core - cormorant
Overview
Send
Receive
Transactions
Balances
Recent transactions
Recent transactions may not yet be visible, and therefore your wallet's balance might be incorrect. This information will be correct once your wallet has finished synchronizing with the bitcoin network, as detailed below.
Attempting to spend bitcoins that are affected by not-yet-displayed transactions will not be accepted by the network.
Number of blocks left Unknown. Syncing Headers (791905, 97.4%)...
Last block time Mon May 29 14:59:28 2023
Progress 94.80%
Progress increase per hour calculating...
Estimated time left until synced Unknown...
Hide
Connecting to peers...
BTC

Core Dev Comms

IRC: quiet, weekly meetings (50MB)

Mailing List: low volume (30MB)

Github: comments, PRs, issues (**2.5GB**)

Core on Github

Centralized, proprietary, closed-source, vulnerable

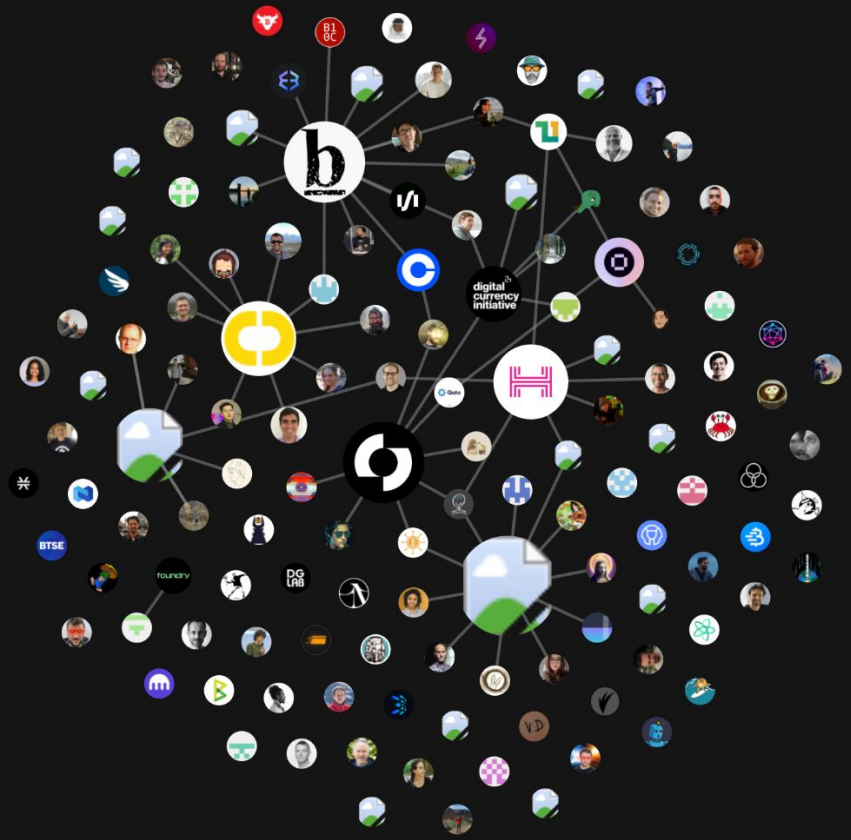
Active developers somewhat aware of the problem

Efforts to archive comms and set up a Gitlab mirror

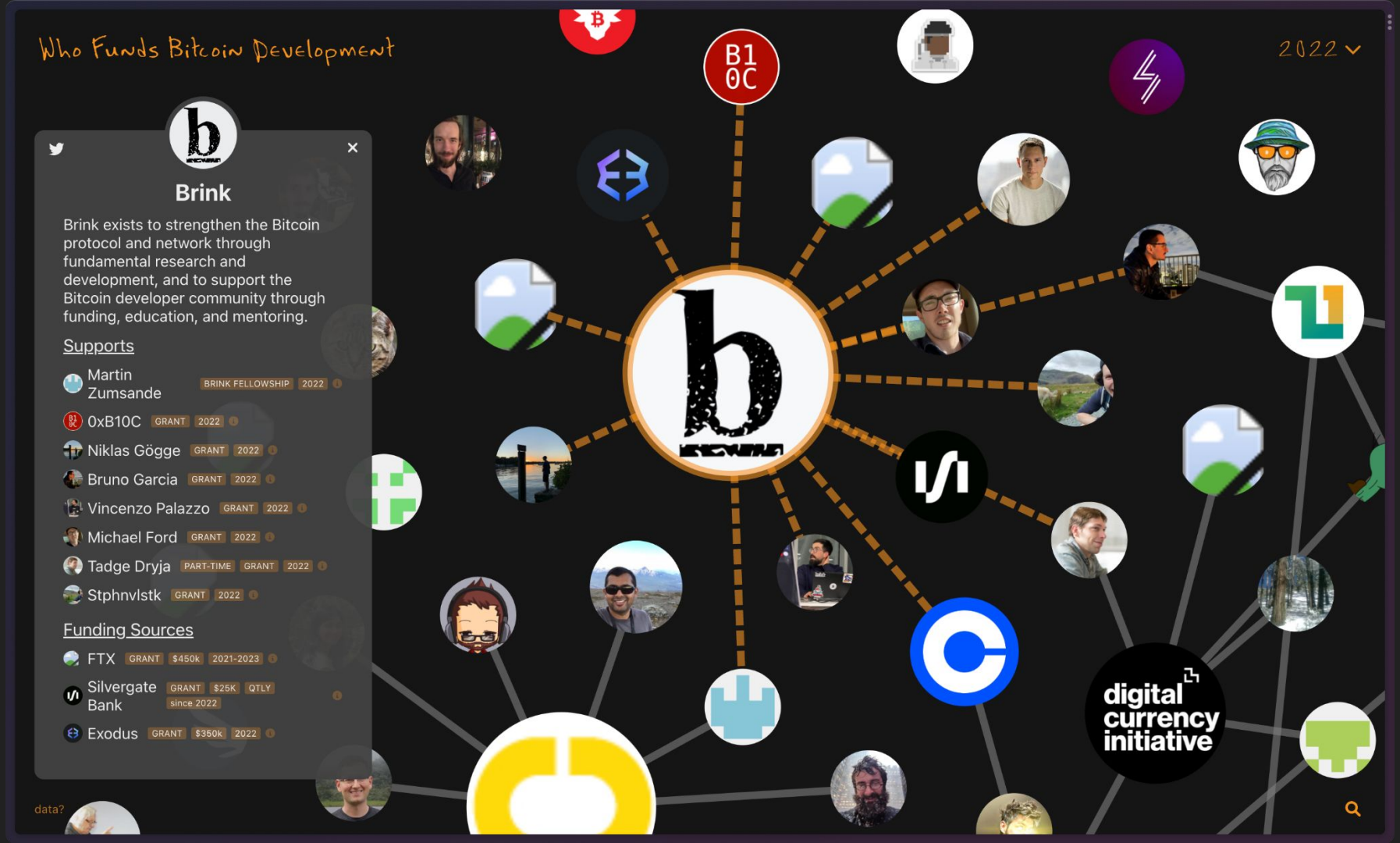
Developer Funding

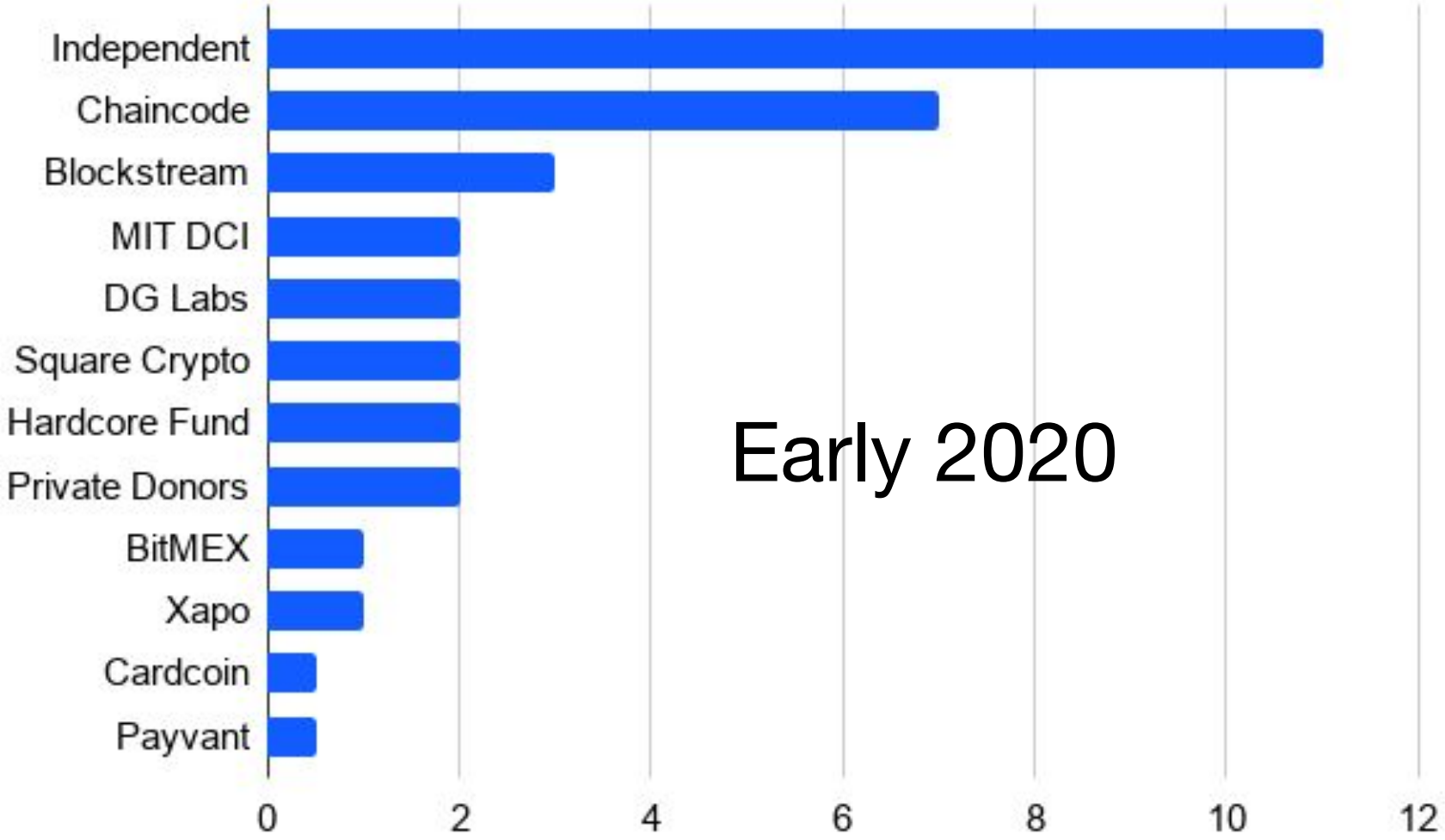
Who Funds Bitcoin Development

2022



data?


Who Funds Bitcoin Development
2022
Brink
Brink exists to strengthen the Bitcoin protocol and network through fundamental research and development, and to support the Bitcoin developer community through funding, education, and mentoring.
Supports
Martin Zumsande BRINK FELLOWSHIP 2022
0xB10C GRANT 2022
Niklas Gögge GRANT 2022
Bruno Garcia GRANT 2022
Vincenzo Palazzo GRANT 2022
Michael Ford GRANT 2022
Tadge Dryja PART-TIME GRANT 2022
Stphnvlstk GRANT 2022
Funding Sources
FTX GRANT $450k 2021-2023
Silvergate Bank GRANT $25K QTLY since 2022
Exodus GRANT $350k 2022
digital currency initiative
data?


Independent
Chaincode
Blockstream
MIT DCI
DG Labs
Square Crypto
Hardcore Fund
Private Donors
BitMEX
Xapo
Cardcoin
Payvant
0
2
4
6
8
10
12
Early 2020

WORDS

WORDS is a bastion of Bitcoin knowledge. Read **WORDS**.

Subscribe
Twitter
Telegram
GitHub
Support **WORDS**
Email

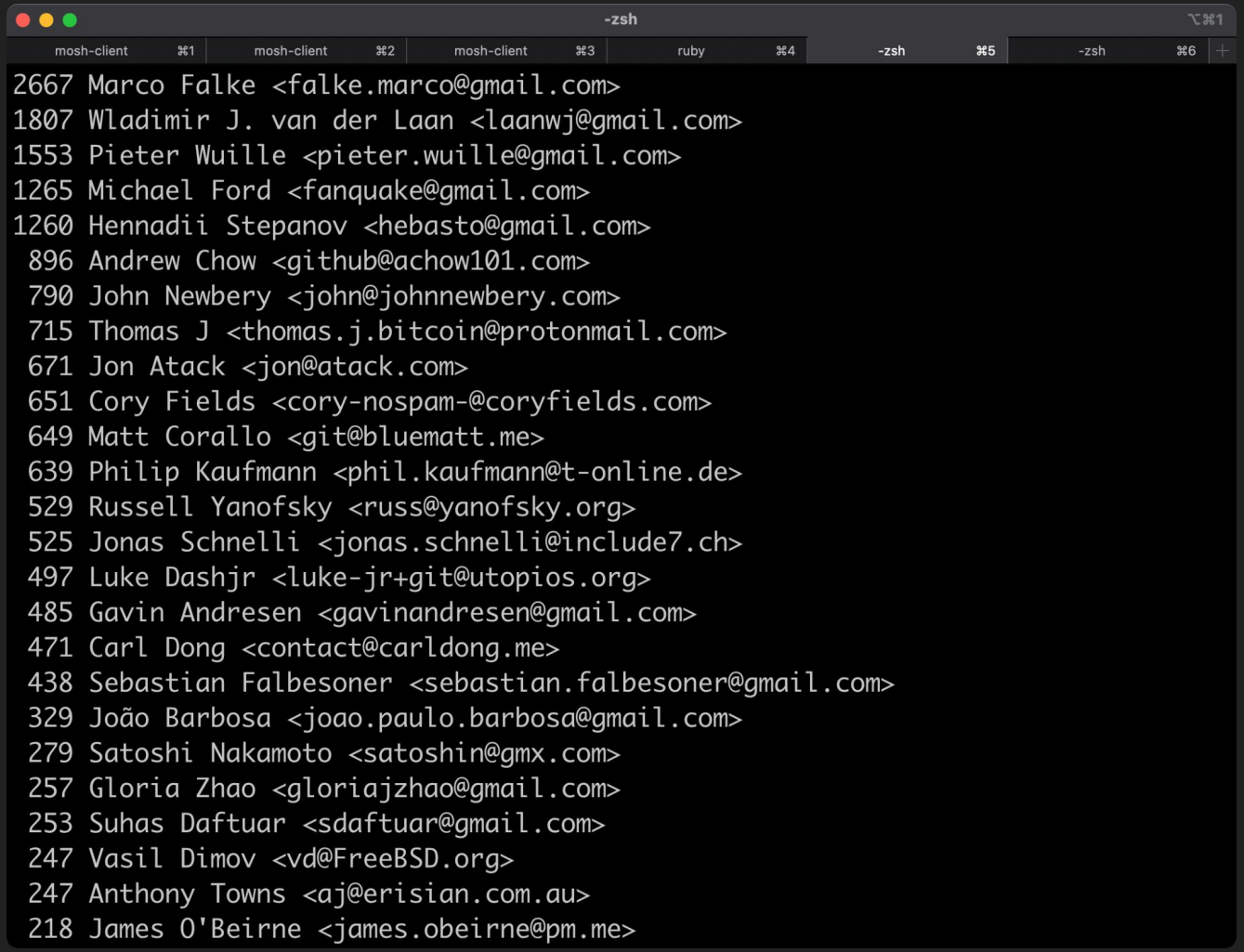
Bitcoin Grants

This page is an attempt to track all the Bitcoin grants. This is a work in progress. Please send me details if I am missing a grant.

Grants

Need to add Square Crypto grants from Jan-Mar 2021.

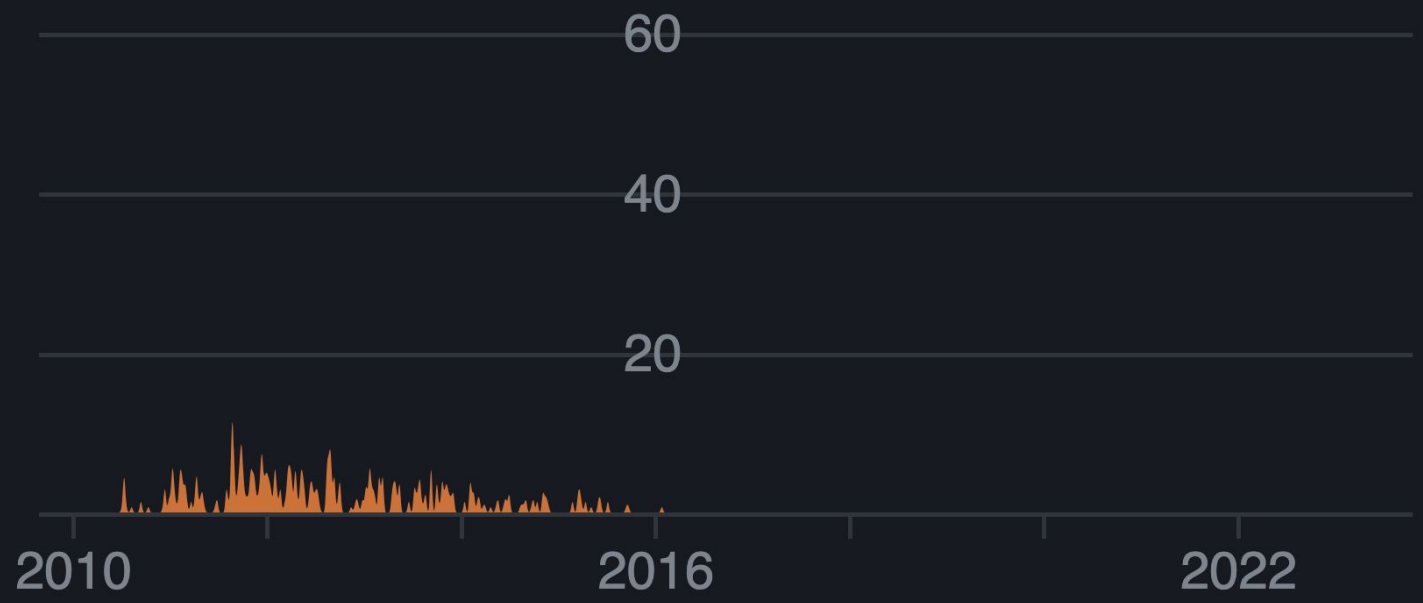
Grant Date	Grantor	Grantee	Project Information	GitHub/Source Code	Contribution	Amount
2021/03	OKCoin	Antoine Riard	Why we may fail lightning	ariard	Bitcoin and Lightning development	-
2021/03	HRF	Jesse Posner	Discreet Log Contracts	-	DLC's and adapter signatures	$25,000
2021/03	HRF	Muun Wallet	Muun Wallet	Bitcoin & Lightning wallet	making self-custody easier	$25,000
2021/03	HRF	Janine	This Month in Bitcoin Privacy	Enegnei	Bitcoin privacy newsletter	$10,000


-zsh
⌥⌘1
mosh-client ⌘1
mosh-client ⌘2
mosh-client ⌘3
ruby ⌘4
-zsh ⌘5
-zsh ⌘6
2667 Marco Falke <falke.marco@gmail.com>
1807 Wladimir J. van der Laan <laanwj@gmail.com>
1553 Pieter Wuille <pieter.wuille@gmail.com>
1265 Michael Ford <fanquake@gmail.com>
1260 Hennadii Stepanov <hebasto@gmail.com>
896 Andrew Chow <github@achow101.com>
790 John Newbery <john@johnnewbery.com>
715 Thomas J <thomas.j.bitcoin@protonmail.com>
671 Jon Atack <jon@atack.com>
651 Cory Fields <cory-nospam-@coryfields.com>
649 Matt Corallo <git@bluematt.me>
639 Philip Kaufmann <phil.kaufmann@t-online.de>
529 Russell Yanofsky <russ@yanofsky.org>
525 Jonas Schnelli <jonas.schnelli@include7.ch>
497 Luke Dashjr <luke-jr+git@utopios.org>
485 Gavin Andresen <gavinandresen@gmail.com>
471 Carl Dong <contact@carldong.me>
438 Sebastian Falbesoner <sebastian.falbesoner@gmail.com>
329 João Barbosa <joao.paulo.barbosa@gmail.com>
279 Satoshi Nakamoto <satoshin@gmx.com>
257 Gloria Zhao <gloriajzhao@gmail.com>
253 Suhas Daftuar <sdaftuar@gmail.com>
247 Vasil Dimov <vd@FreeBSD.org>
247 Anthony Towns <aj@erisian.com.au>
218 James O'Beirne <james.obeirne@pm.me>

gavinandresen

#15

488 commits 64,236 ++ 76,334 --



Dev Leadership

Satoshi (till 2011)

Gavin (till 2014)

LaanWJ (till 2023)

None (since February)

Maintainers (Oct ‘23)

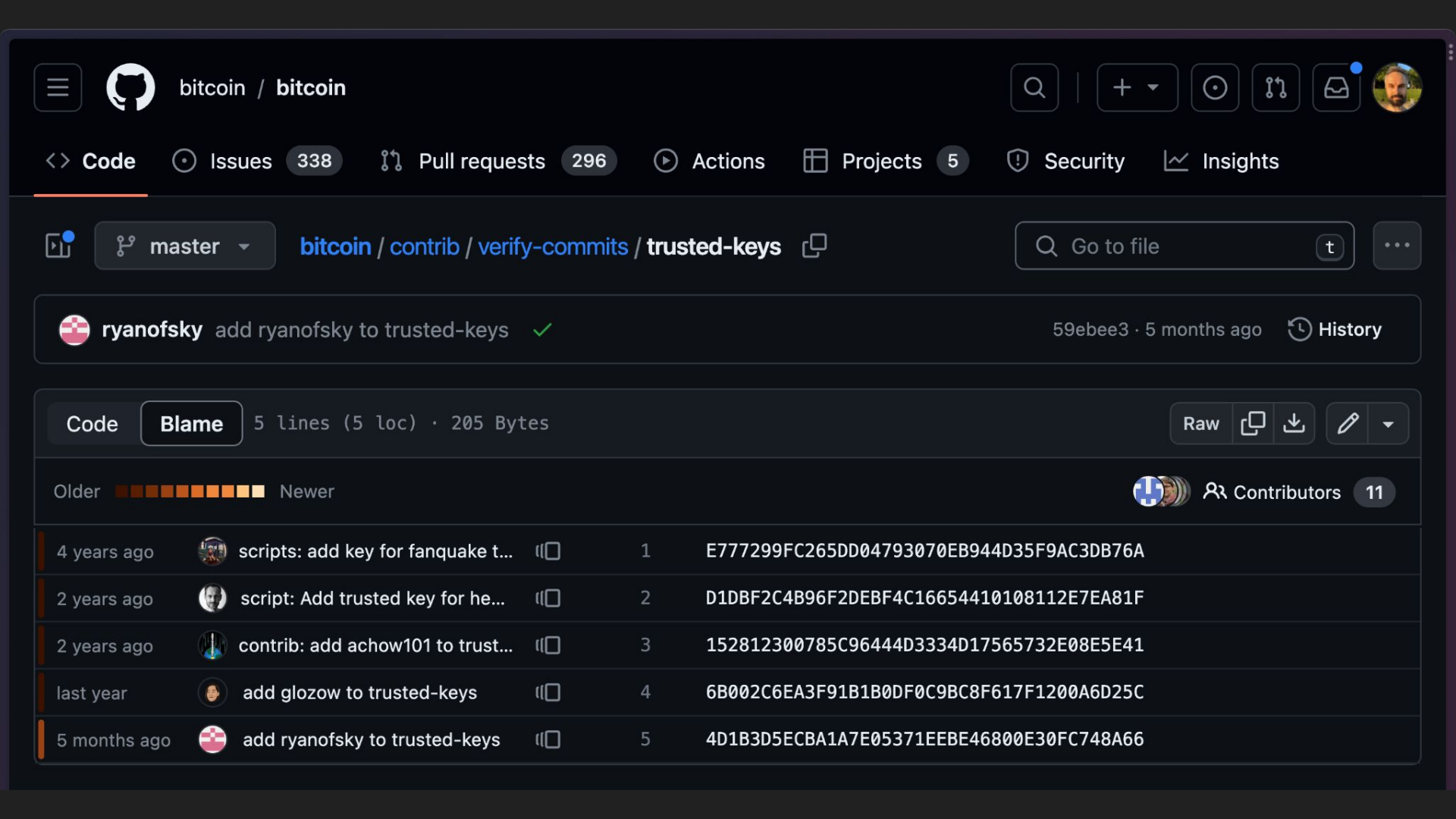
Michael Ford (since 2019)

Hennadii Stepanov (since 2021)

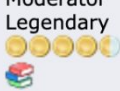
Andrew Chow (since 2021)

Gloria Zhao (since 2022)

Russell Yanofsky (since 2023)


bitcoin / bitcoin
Code
Issues 338
Pull requests 296
Actions
Projects 5
Security
Insights
master
bitcoin / contrib / verify-commits / trusted-keys
Go to file t
ryanofsky add ryanofsky to trusted-keys
59ebee3 · 5 months ago
History
Code
Blame
5 lines (5 loc) · 205 Bytes
Raw
Older
Newer
Contributors 11
4 years ago scripts: add key for fanquake t... 1 E777299FC265DD04793070EB944D35F9AC3DB76A
2 years ago script: Add trusted key for he... 2 D1DBF2C4B96F2DEBF4C16654410108112E7EA81F
2 years ago contrib: add achow101 to trust... 3 152812300785C96444D3334D17565732E08E5E41
last year add glozow to trusted-keys 4 6B002C6EA3F91B1B0DF0C9BC8F617F1200A6D25C
5 months ago add ryanofsky to trusted-keys 5 4D1B3D5ECBA1A7E05371EEBE46800E30FC748A66

achow101 (OP)
Moderator
Legendary



Activity: 3206
Merit: 6002

Just writing some code

List of people who have had commit access to Bitcoin Core

February 01, 2017, 10:19:06 PM #1

Merited by DdmrDdmr (3), Husna QA (1), nullius (1)

I am creating this thread in response to the discussion occurring at https://bitcointalk.org/index.php?topic=1773558.msg17697805#msg17697805. This list will contain the names (or pseudonyms) of everyone who I can find evidence for ever having commit access to Bitcoin Core, the dates during which they had commit access, sources for all of this information, and reasoning for the access. Those who currently have commit access are in **bold**.

- Satoshi Nakamoto (satoshi, s_nakamoto): 2009-01-03 - 2011-09-13[1] Creator, first Lead Maintainer
- Martti Malmi (Sirius, sirius_m): 2009-08-30 - 2011-09-13[1][2] Creator of first SVN repo
- Laszlo (laszloh) 2010-08-04 - 2011-09-131[1] Original OSX Builds and support
- Gavin Andresen (gavinandresen): 2010-10-11 - 2016-05-02[3] Frequent contributor; later Lead Maintainer
- Chris Moore (dooglus): 2011-01-21 - 2011-03-31 Frequent contributor for some time; Still occasionally contributes
- Pieter Wuille (sipa): 2011-05-01 - 2022-07-07 Frequent contributor
- Jeff Garzik (jgarzik): 2011-05-06 - July/Aug 2016 [4] Frequent Contributor
- **Wladimir J. van der Laan (laanwj, wumpus): 2011-06-05 - present[5] Frequent contributor; later Lead Maintainer**
- Nils Schneider (tcatm): 2011-09-19 - 5/31/12 Frequent contributor for some time
- Greg Maxwell (gmaxwell): 2012-02-11 - 2015-12-17 Frequent contributor; Gave up commit access due to toxicity and drama from the community
- Jonas Schnelli (jonasschnelli): 2015-11-13 - 2021-10-21[6] Frequent contributor; given access after becoming GUI Maintainer; Stepped down for personal reasons
- **Marco Falke (marcofalke): 2016-04-13 - present[7] Frequent Contributor; given access after becoming QA/Testing Maintainer**
- Samuel Dobson (MeshCollider): 2018-12-06 - 2021-09-12[8] Frequent Contributor; given access after volunteering to be the wallet maintainer; Stepped down to focus on his PhD
- **Michael Ford (fanquake): 2019-06-08 - present[9] Frequent Contributor; given access after being nominated by several other frequent contributors and maintainers to become a maintainer.**
- **Hennadii Stepanov (hebasto): 2021-04-19 - present Frequent Contributor; given access after volunteering to help maintain the GUI**
- **Andrew Chow (achow101): 2021-12-20 - present[10] Frequent Contributor; given access after volunteering to be the wallet maintainer.**
- **Gloria Zhao (glozow): 2022-07-07 - presentt[11] Frequent contributor, given access after being nominated by several frequent contributors and maintainers to become a maintainer.**

Neutral Citation Number: [2023] EWCA Civ 83

Case No: CA-2022-001050
CA-2022-001062
CA-2022-002184

IN THE COURT OF APPEAL (CIVIL DIVISION)
ON APPEAL FROM HIGH COURT OF JUSTICE
BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
BUSINESS LIST (ChD)
Mrs Justice Falk [2022] EWHC 667 (Ch)
BL-2021-000313

Royal Courts of Justice
Strand, London, WC2A 2LL

Date: 03/02/2023

Before :

LORD JUSTICE LEWISON
LORD JUSTICE POPPLEWELL
and
LORD JUSTICE BIRSS

Between :

Tulip Trading Limited (a Seychelles company)	**Appellant/ Claimant**
- and -	
(2) Wladimir Jasper van der Laan **(3) Jonas Schnelli** **(4) Pieter Wuille** **(5) Marco Patrick Falke** **(6) Samuel Dobson** **(7) Michael Rohan Ford** **(8) Cory Fields** **(9) George Michael Dombrowski** **(10) Matthew Gregory Corallo** **(11) Peter Todd** **(12) Gregory Fulton Maxwell** **(14) Roger Ver** **(15) Amaury Séchet** **(16) Jason Bradley Cox**	**Respondents / Defendants**
(1) Bitcoin Association for BSV **(a Swiss verein)** **(13) Eric Lombrozo**	

- and -

(2) Wladimir Jasper van der Laan

(3) Jonas Schnelli

(4) Pieter Wuille

(5) Marco Patrick Falke

(6) Samuel Dobson

(7) Michael Rohan Ford

(8) Cory Fields

(9) George Michael Dombrowski

(10) Matthew Gregory Corallo

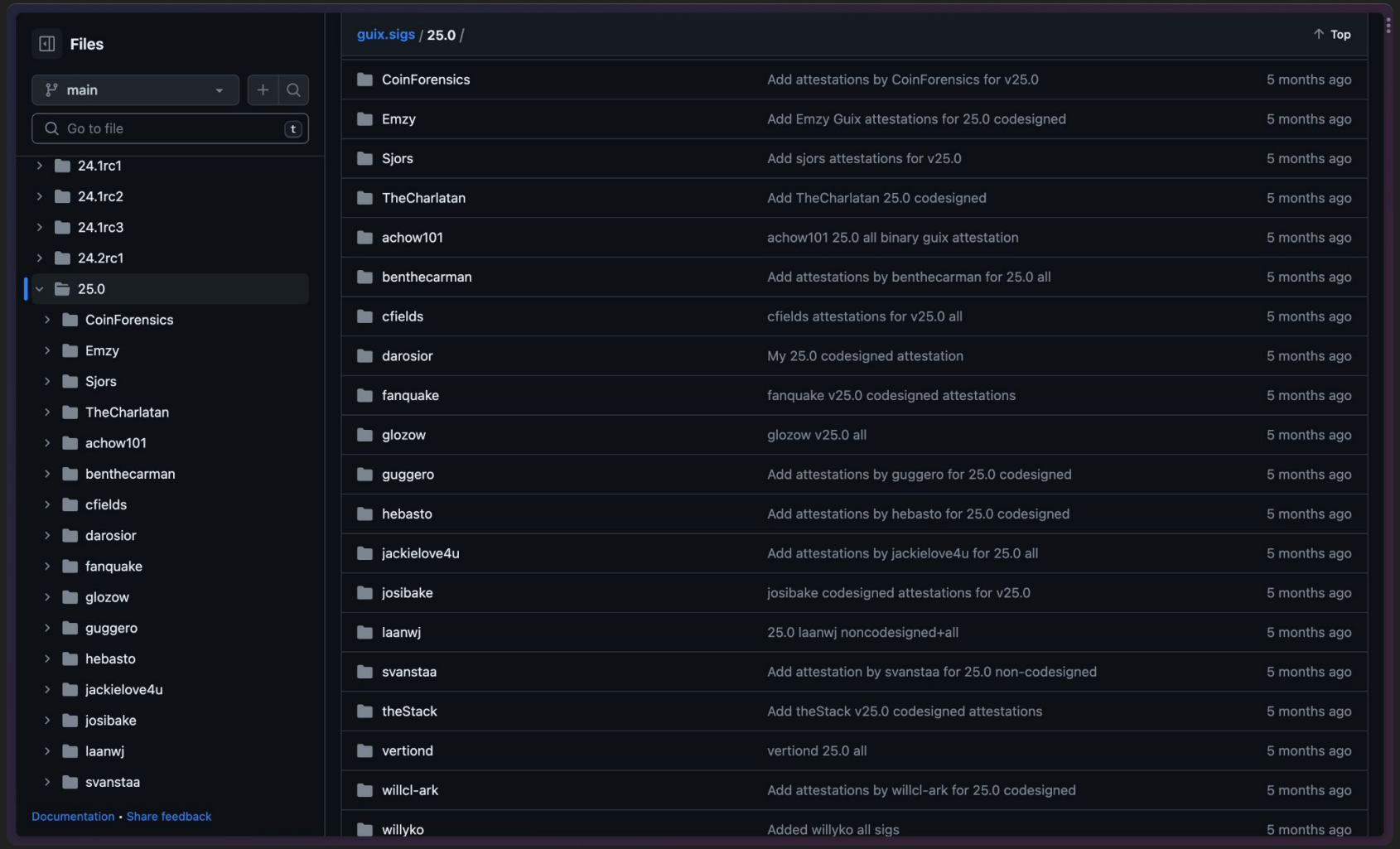
(11) Peter Todd

(12) Gregory Fulton Maxwell

(14) Roger Ver

(15) Amaury Séchet

(16) Jason Bradley Cox


Files
main
Go to file
t
24.1rc1
24.1rc2
24.1rc3
24.2rc1
25.0
CoinForensics
Emzy
Sjors
TheCharlatan
achow101
benthecarman
cfields
darosior
fanquake
glozow
guggero
hebasto
jackielove4u
josibake
laanwj
svanstaa
Documentation • Share feedback
guix.sigs / 25.0 /
Top
CoinForensics Add attestations by CoinForensics for v25.0 5 months ago
Emzy Add Emzy Guix attestations for 25.0 codesigned 5 months ago
Sjors Add sjors attestations for v25.0 5 months ago
TheCharlatan Add TheCharlatan 25.0 codesigned 5 months ago
achow101 achow101 25.0 all binary guix attestation 5 months ago
benthecarman Add attestations by benthecarman for 25.0 all 5 months ago
cfields cfields attestations for v25.0 all 5 months ago
darosior My 25.0 codesigned attestation 5 months ago
fanquake fanquake v25.0 codesigned attestations 5 months ago
glozow glozow v25.0 all 5 months ago
guggero Add attestations by guggero for 25.0 codesigned 5 months ago
hebasto Add attestations by hebasto for 25.0 codesigned 5 months ago
jackielove4u Add attestations by jackielove4u for 25.0 all 5 months ago
josibake josibake codesigned attestations for v25.0 5 months ago
laanwj 25.0 laanwj noncodesigned+all 5 months ago
svanstaa Add attestation by svanstaa for 25.0 non-codesigned 5 months ago
theStack Add theStack v25.0 codesigned attestations 5 months ago
vertiond vertiond 25.0 all 5 months ago
willcl-ark Add attestations by willcl-ark for 25.0 codesigned 5 months ago
willyko Added willyko all sigs 5 months ago

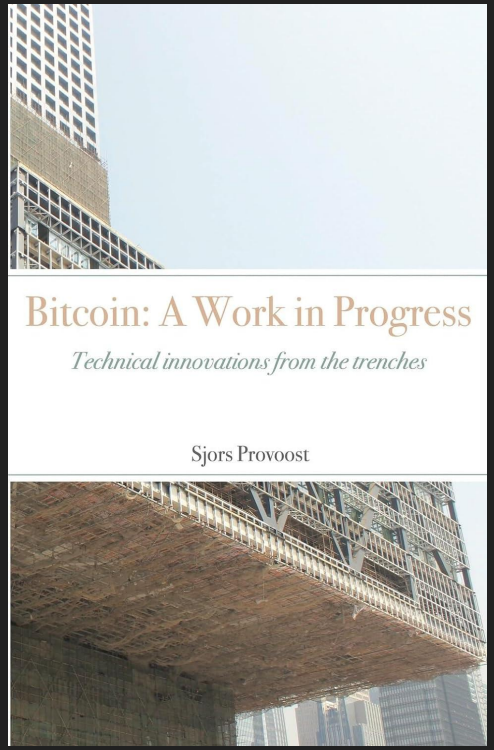
Website

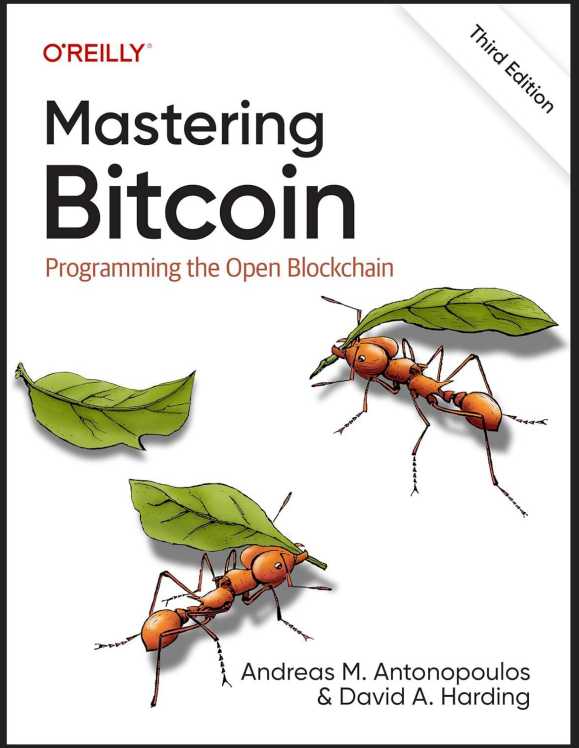
bitcoincore.org — healthy, basic

bitcoin.org — original, stalled (Cøbra)

bitcoin.com — compromised

Voices of Reason





NOV 4, 2022 • 16 MIN READ • **HISTORY**

The Death of Decentralized Email

A historical review of the multi-decade centralization and capture of the email protocol.

The widening gyre

Recent events have made me reflect on a few things in my life I was already thinking about for a while. Also, responses on social media have made me realize that people have *strange* expectations from me, and what my role in the Bitcoin Core project is.

growth

Bitcoin has grown a lot since I started contributing to it in 2011. Some arrangements that were acceptable for a small scale FOSS project are no longer so for one runing a 600 billion dollar system. Market cap is famously deceptive, but my point is not about specific numbers here.

One thing is clear: this is a serious project now, and we need to start taking decentralization seriously.

Takeaways

Bitcoin [Core] is still *really* a work in progress

Concept proven, need spec + ref + prod

Feature creep vs refinement

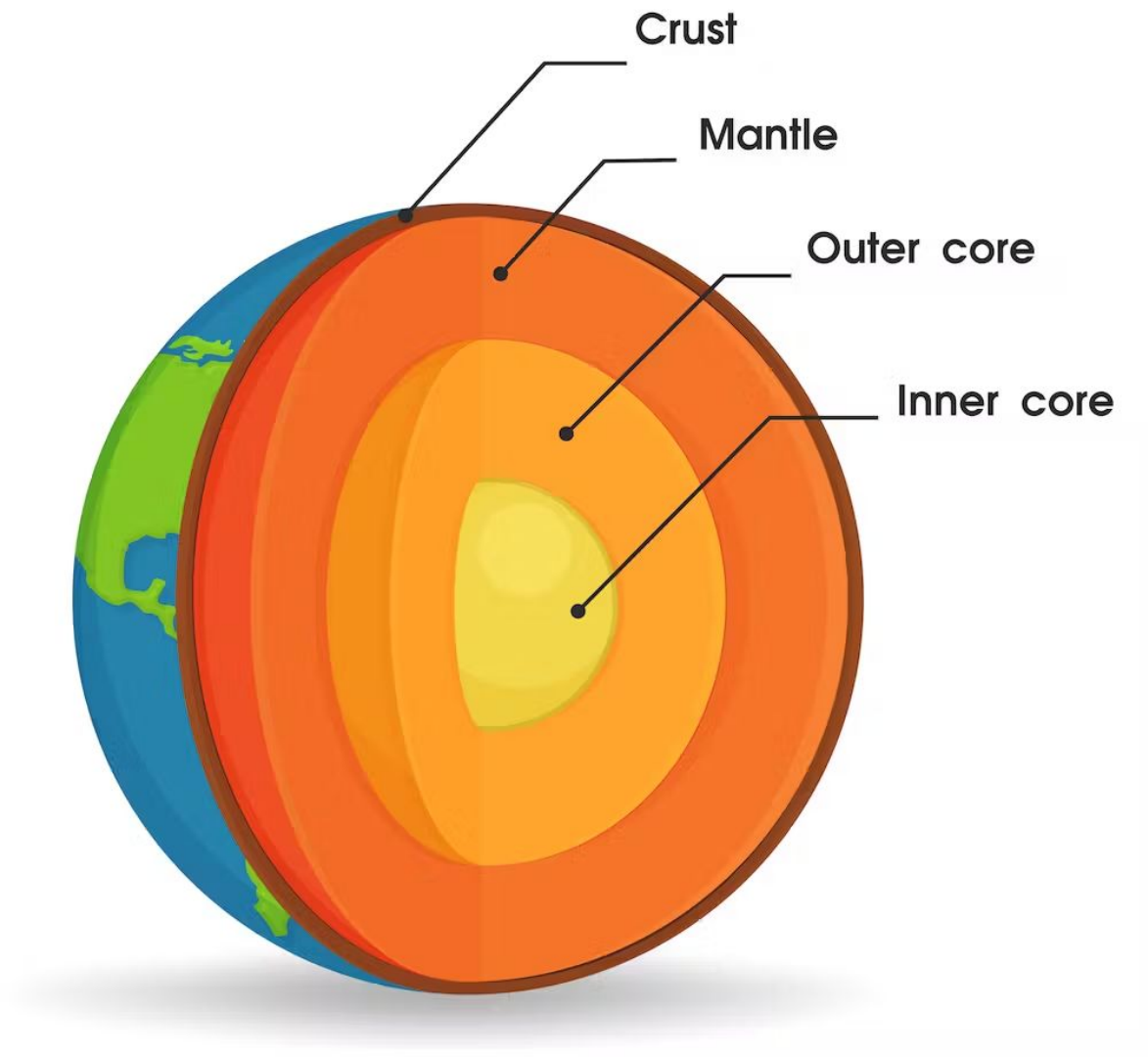
Definitions from Oxford Languages · Learn more

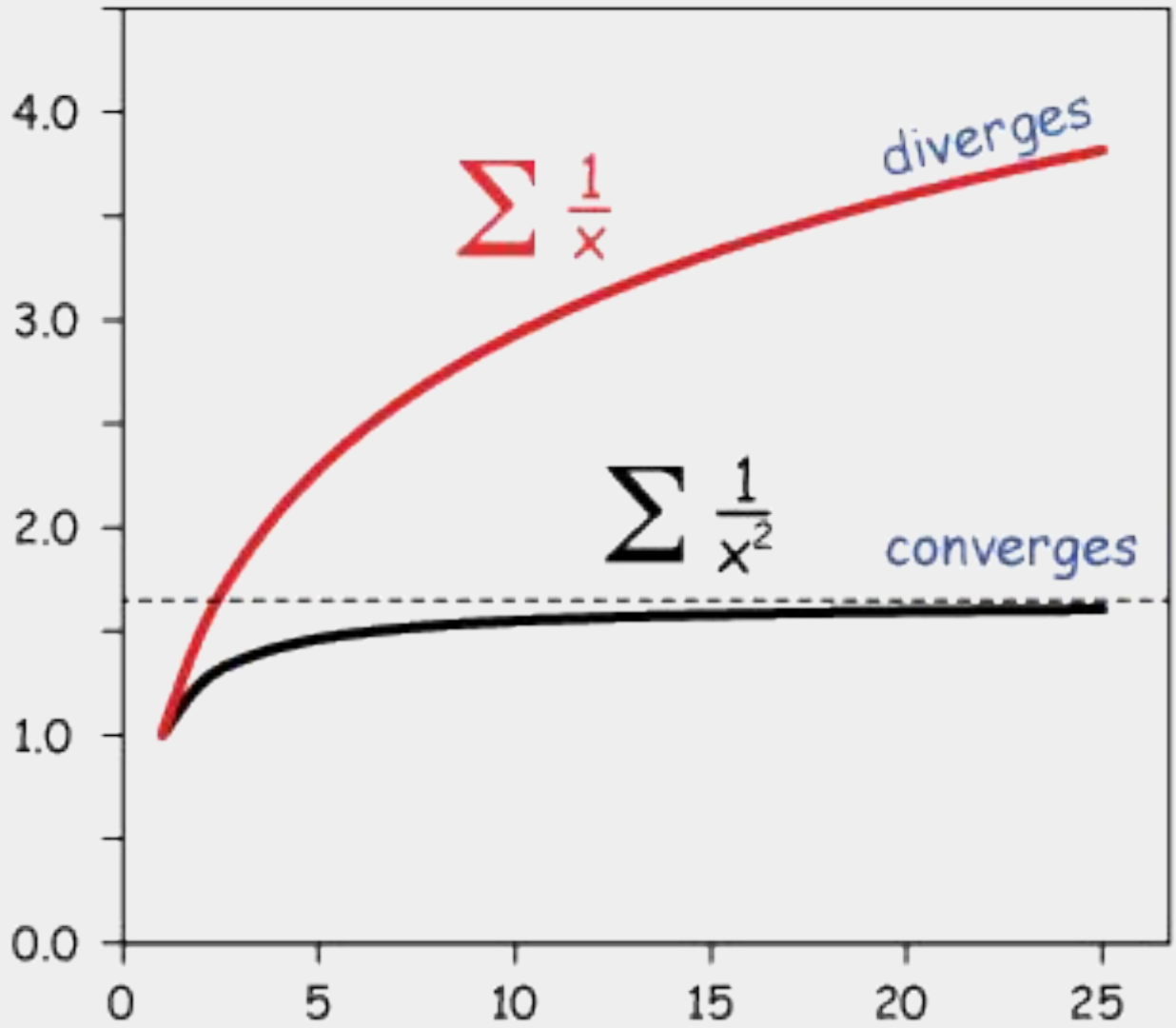
core

/kɔː/

Origin

Middle English: of unknown origin.


Crust
Mantle
Outer core
Inner core


4.0
3.0
2.0
1.0
0.0
0
5
10
15
20
25
$\sum \frac{1}{x}$
diverges
$\sum \frac{1}{x^2}$
converges