



Sound Money Properties  
Series

#9: Transparent, Open Source &  
Auditable

with @SimplestBTCBook and @DJSATOSHI18

- Ⓝ PORTABLE, DURABLE, DIVISIBLE, FUNGIBLE
- Ⓝ TRULY SCARCE
- Ⓝ DISTRIBUTED & DECENTRALIZED
- Ⓝ CENSORSHIP RESISTANT & UNCONFISCATABLE
- Ⓝ IMMUTABLE & INCORRUPTIBLE
- Ⓝ EASILY VERIFIABLE & CAN'T BE COUNTERFEITED
- Ⓝ PERMISSIONLESS, FRICTIONLESS & PEER-TO-PEER
- Ⓝ NEUTRAL & VOLUNTARY
- Ⓝ TRANSPARENT, OPEN-SOURCE & AUDITABLE
- Ⓝ BORDERLESS
- Ⓝ PROVIDES SETTLEMENT FINALITY
- Ⓝ PSEUDONYMOUS & TRUSTLESS
- Ⓝ SECURE & SCALABLE
- Ⓝ DISINFLATIONARY/DEFLATIONARY

# TRANSPARENT

Definition of transparent:

: free from pretense or deceit

: easily detected or seen through

: readily understood

: characterized by visibility or accessibility of information, especially concerning business practices

- [merriamwebster.com](https://www.merriam-webster.com)

# TRANSPARENT

- Bitcoin is often perceived as an anonymous payment network.
- But in reality, Bitcoin is probably the most transparent payment network in the world.
- At the same time, Bitcoin can provide acceptable levels of privacy when used correctly.
- Always remember that it is your responsibility to adopt good practices in order to protect your privacy.

~ [bitcoin.org](https://bitcoin.org)

For greater privacy, it's best to use bitcoin addresses only once.

~ Satoshi Nakamoto, Nov.25, 2009

## Transparency of bitcoin:

Bitcoin is a fair and transparent system because its rules are set and consistently enforced, allowing for a level playing field for all participants.

~ Bitcoin Exemplifies Fair And Transparent Rules  
By Tim Niemeyer  
Dec 12, 2022

# OPEN SOURCE

Definition of open source:

: having the source code freely available for possible modification and redistribution

- [merriamwebster.com](https://www.merriam-webster.com/dictionary/open%20source)

Open source is source code that is made freely available for possible modification and redistribution. Products include permission to use the source code,<sup>[1]</sup> design documents,<sup>[2]</sup> or content of the product. The open-source model is a decentralized software development model that encourages open collaboration.<sup>[3][4]</sup>

- Wikipedia

# BITCOIN IS OPEN SOURCE

- ⓑ Bitcoin is open-source; its design is public, nobody owns or controls Bitcoin and everyone can take part.
- ⓑ Bitcoin is free software and any developer can contribute to the project. Everything you need is in the [GitHub repository](#). Please make sure to read and follow the development process described in the README, as well as to provide good quality code and respect all guidelines.
- ⓑ Development discussion takes place on GitHub and the [bitcoin-dev](#) mailing list. Less formal development discussion happens on [irc.libera.chat #bitcoin-core-dev](#) ([web interface](#), [logs](#)).

~ bitcoincore.org



# Open-Source Software

Open-source refers to software that is publicly accessible and can be downloaded, redistributed and/or modified. It's *open* in the sense that its source code is a collaborative effort and can be freely inspected. Satoshi Nakamoto chose to release Bitcoin under a permissive software license.

*"Open source is very much a meritocracy. You've got the hive mind building solutions. You get all that scrutiny and that comes back to security. Bitcoin Core is probably one of the most heavily scrutinized code bases in the world."*

**-@BTCSchellingPt**



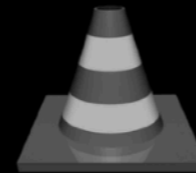
Database



Programming



Operating Systems



Media



Publishing



Browser



Money

From: Few Understand This by @anilsaidso

# Bitcoin on Github.com

Product Solutions Open Source Pricing Search Sign in Sign up

bitcoin/bitcoin Public Notifications Fork

<> Code Issues 340 Pull requests 284 Projects 5 Security Insights

master 5 branches 291 tags Go to file Code

fanquake Merge #27790: walletdb: Add PrefixCursor ... 7f20197 2 days ago 37,710 commits

.github	github: Switch to yaml issue templates	4 months ago
.tx	qt: Bump Transifex slug for 25.x	4 months ago
build-aux/m4	build: Bump minimum supported GCC to g++-9	3 weeks ago
build_msvc	Merge #27696: build: Do not define ENABLE_ZMQ when ZMQ is not ...	2 weeks ago
ci	Merge #27737: ci: compile Clang and compiler-rt in msan jobs	3 days ago
contrib	Merge #27507: lint: stop ignoring LIEF imports	last week
depends	depends: remove redundant stdlib option	2 weeks ago
doc	Merge #27225: doc: document json rpc endpoints	2 days ago
share	Modernize rpcauth.py and its tests	4 months ago
src	Merge #27790: walletdb: Add PrefixCursor	2 days ago
test	Merge #27603: test: added coverage to mining_basic.py	3 days ago
.cirrus.yml	ci: return to using Ubuntu 22.04 in MSAN jobs	last week
.editorconfig	ci: Drop AppVeyor CI integration	2 years ago
.gitattributes	Separate protocol versioning from clientversion	9 years ago
.gitignore	refactor: cleanups post unsubtree'ing univalued	last year
.python-version	Bump python minimum version to 3.8	2 months ago

About  
Bitcoin Core integration/staging tree  
[bitcoincore.org/en/download](https://bitcoincore.org/en/download)  
c-plus-plus cryptography bitcoin p2p cryptocurrency

Readme MIT license Security policy 69.8k stars 3.9k watching 34.3k forks Report repository

Releases 43  
Bitcoin Core 25.0 Latest last week  
+ 42 releases

Contributors 911

# The MIT License - [opensource.org](https://opensource.org/licenses/MIT)

---

*Begin license text.*

---

Copyright <YEAR> <COPYRIGHT HOLDER>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

---

*End license text.*

---

# Code Review

- ⓑ Bitcoin Core is security software that helps protect assets worth billions of dollars, so **every code change needs to be reviewed by experienced developers.**
- ⓑ It can take a long time for other developers to review your pull requests.
- ⓑ Remember that **all reviewers are taking time away from their own projects to review your pull requests**, so be patient and respectful of their time.
- ⓑ **Please also consider helping to review other people's pull requests.**
- ⓑ You don't need to be an expert in Bitcoin, the Bitcoin Core codebase, or C++ (although all these things help).
- ⓑ There are almost always open pull requests that any programmer can review.

# Bitcoin Core PR Review Club

## bitcoincore.reviews

- 🔗 Anyone can contribute to bitcoin by joining the Bitcoin Core PR Review Club.
- 🔗 This is a weekly review club for Bitcoin Core PRs (Pull Requests)
- 🔗 It is held at 17:00 UTC on Wednesdays in the #bitcoin-core-pr-reviews IRC channel on <http://libera.chat>
- 🔗 The meetings are scheduled by Gloria Zhao @glozow & @Stphnvlstk and are hosted by various core devs.



# AUDITABLE

Adj. of Audit

Definition of Audit:

: a formal examination of an organization's or individual's accounts or financial situation

: the final report of an audit

: a methodical examination and review

- [merriamwebster.com](https://www.merriam-webster.com)

# AUDITABLE

- ⓑ So, **why Bitcoin?** Why is this relatively-straightforward technology (ingenious and elegant, complex and nuanced, but straightforward nonetheless) the answer to the impending doom we all face if we are unable to prime and restart our national and international trust engine?
- ⓑ It's simple. **Because Bitcoin is the truth.** On a most basic level, the Bitcoin protocol - and the tens of thousands of nodes that run the software - verifies each and every transaction that takes place on chain.
- ⓑ No one is in control. No one's word needs to be taken as fact. **The truth is manifest and auditable on the blockchain itself.** Countless, entirely-objective nodes make falsification of the record an impossibility. **Bitcoin is thus an inviolable, immutable, incontrovertible truth.**

~ From: The Death Of Trust: As Institutions Erode, Bitcoin Is Our Only Hope  
By Dan Weintraub



(Not) Trusting the Fed's financial statements  
are true and accurate



Trusting the open-source code,  
verifiable by anyone!

# Auditing Supply

*"The Fed's financial statements are also a matter of public record, and are audited annually by independent, outside auditors.."*

*"I am well aware of this because I chair the committees that have oversight responsibility for the audits."*

**-Jerome Powell** (Chair of the Federal Reserve)



**"IN GOD WE TRUST"**

***bitcoin-cli gettxoutsetinfo***

**"height": 679,066**

**"total\_amount": 18,681,463**



**"DON'T TRUST, VERIFY"**



# WHY ARE TRANSPARENCY AND AUDITABILITY IMPORTANT PROPERTIES OF SOUND MONEY?

- 🔴 In order for money to be (and to remain) truly sound, it must be open, transparent and auditable so that anyone, anywhere, anytime can look at it and:
  - ★ Know precisely what the current supply is.
  - ★ Can independently verify their own balance.
  - ★ Can verify the status of any transactions they make.
  - ★ Can easily determine if any bad actors are attempting to manipulate it.
  - ★ And, once all the bitcoin are mined in 2140, can continue to verify the total supply remains constant forever onward.
- 🔴 **Note:** These attributes do NOT mean that bitcoin can not or should not be private. Satoshi specifically made addresses pseudonymous. It is up to us to continue developing ways to use bitcoin privately, in the same way we can currently use cash privately.

# WHY IS HAVING OPEN SOURCE SOFTWARE AN IMPORTANT PROPERTY OF SOUND MONEY?

- ⓑ Sound money must be based on open source software so that anyone, anywhere can view, verify and contribute to the source code.
- ⓑ This is **critical** because it keeps the money out of the hands of any one entity, government, institution etc.
- ⓑ **No one entity can ever control**, manipulate, debase or inflate bitcoin.
- ⓑ The current centralized Fiat monetary systems worldwide, are opaque, difficult to learn about, and **impossible to audit and verify**.
- ⓑ No one can tell you exactly how many US dollars exist.
- ⓑ Central banks and governments are fighting against the use of Bitcoin because **it threatens their power to create currency out of thin air**.

# ON THE OTHER HAND..

- 🔸 **Anyone** with a computer and internet connection may download, install, and run the free open source software that is Bitcoin (<http://BitcoinCore.org>)
- 🔸 **This gives everyone access** to run their own node, their own copy of the Bitcoin time chain (aka blockchain/public ledger) so that you don't have to trust someone else's node.
- 🔸 **This allows one to check the following:**
  - ★ Total current supply
  - ★ Current difficulty
  - ★ When the next difficulty adjustment will take place
  - ★ When the next halving is due
  - ★ Current block number
  - ★ Current fee range
  - ★ All the transactions in any block ever validated

- 🔸 There are currently more than 17,000 publicly accessible Bitcoin nodes and many thousands more private nodes.
- 🔸 (This is what we mean when we say Bitcoin is decentralized, because it would require all of these nodes to be destroyed or to collude to lie about a transaction, or to push through a change to the software.)
- 🔸 Everyone running their own node gets to choose whether to update to a new version, and all updates must be backwards compatible so that people who don't want to update can continue to use and run an older version of the software.
- 🔸 If you don't run your own node, check out [timechainstats.com](https://timechainstats.com) by Ant @2140data to view any stats you are curious about.

By being open-source and transparent,

bitcoin is fully auditable

by anyone anywhere.

Bitcoin is the separation of money and state.



Thanks for listening!

Feedback always welcome!

Next week we will discuss how bitcoin is

Borderless

