

# Bitcoin Core v0.17

john newbery --- 20th August 2018

[github.com/jnewbery](https://github.com/jnewbery)

[twitter.com/jfnewbery](https://twitter.com/jfnewbery)

# \$ apropos

- Bitcoin Core release schedule
- Facts and figures
- Interesting PRs

# Release Schedule



# Bitcoin Core


- ‘Reference implementation’ of Bitcoin
- Continuation of Satoshi’s Bitcoin software first released on January 9th 2009
- Repository hosted at [github.com/bitcoin/bitcoin](https://github.com/bitcoin/bitcoin)
- Project page at [bitcoincore.org](https://bitcoincore.org)
- Bitcoin Core ≠ Bitcoin

# Life Cycle

- Major releases every 6-7 months
- Minor releases when necessary
- Last major release: v0.16 --- 26th Feb 2018
- <https://bitcoincore.org/en/lifecycle/>

# Version 0.17

<https://github.com/bitcoin/bitcoin/issues/12624>



laanwj commented on Mar 6 • edited • Member + 😊 ...

Here is a proposed release schedule for 0.17.0, the next major release of Bitcoin Core. Like for previous major releases I've aimed for a release 6 months after the last (#11449).

**2018-07-02**

- Open Transifex translations for 0.17
- Soft translation string freeze (no large or unnecessary string changes until release)
- Finalize and close translations for 0.15

**2018-07-23**

- Feature freeze (bug fixes only until release)
- Translation string freeze (no more source language changes until release)

**2018-08-13**

- Split off `0.17` branch from `master`
- Start RC cycle, tag and release `0.17.0rc1`
- Start merging for 0.18 on master branch

**2018-09-08**

- Release 0.17.0 final (aim)

If any specific dates or timeframes are a problem for you, let me know.

👍 1 🎉 18

[Release Scedule](#)

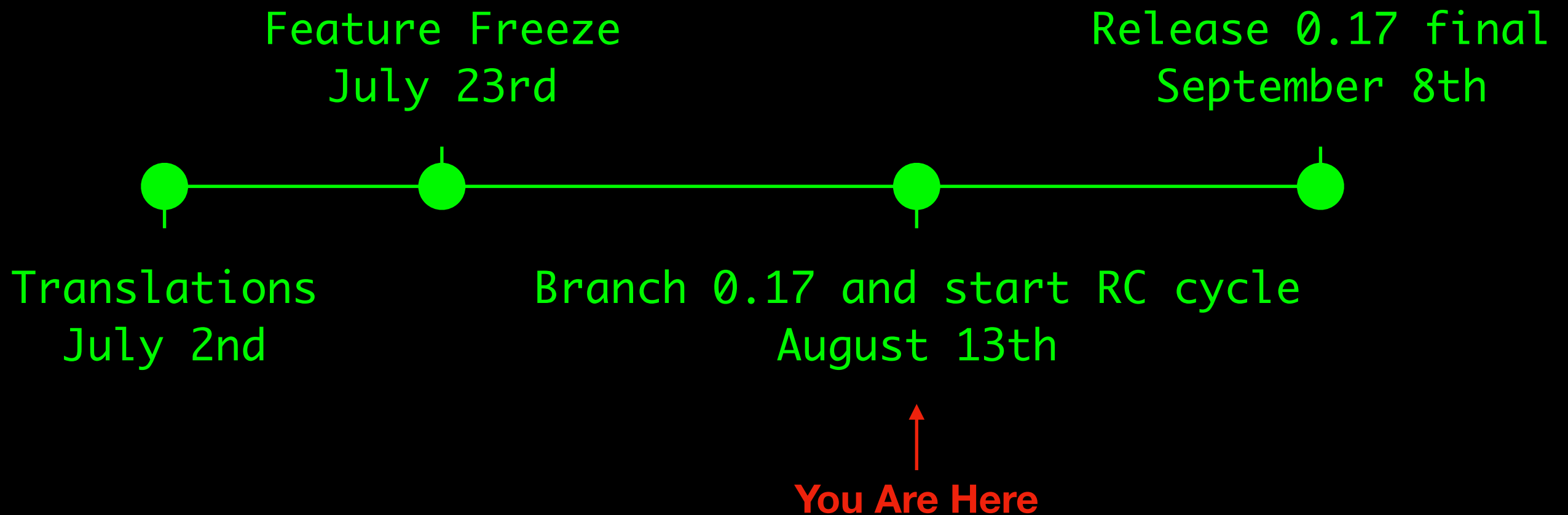


[Facts & Figures](#)



[Interesting PRs](#)

# \$ ca1



# Facts and Figures

Release Scedule



Facts & Figures



Interesting PRs



WARNING!

DON'T COUNT COMMITS



```
$ git log 0.16..0.17
```

- 195 days
- 1225 non-merge commits (6.3/day)
- 748 PRs merged (3.8/day)
- 135 unique commit authors (67 new authors)
- 958 files changed, +45370/-65542 (568/day)

```
$ curl https://api.github.com
```

- 9553 PR and review comments (49/day)
- 182 unique commenters

Commenter	comments
MarcoFalke	1188
laanwj	985
promag	966
jnewbery	744
practicalswift	561
sipa	499
Empact	371
jonasschnelli	294
fanquake	284
ryanofsky	263

# Historical context

	v0.15	v0.16	v0.17
Days	181	166	195
Commits	1275 (7.0)	933 (5.6)	1225 (6.3)
PRs	626 (3.5)	498 (3.0)	748 (3.8)
LOC	+51219/-21104 (399)	+72926/-28638 (611)	+45370/-65542 (568)
New authors	56 (0.31)	60 (0.36)	67 (0.34)
Comments	6963 (38)	6368 (38)	9553 (49)

BCFI

0.14

0.07

0.13

Release Scedule



Facts & Figures



Interesting PRs

# Interesting PRs



# Wallet Changes

9662 - "disableprivatekeys" to create watchonly wallets

10637 - Branch and Bound Coin Selection

10740 - `loadwallet` RPC - load wallet at runtime

12196 - Add scantxoutset RPC method

12610 - Multiwallet for the GUI

12714 - Introduce interface for signing providers

12953 - Deprecate accounts

13557 - BIP 174 PSBT Serializations and RPCs

13666 - Always create signatures with Low R values

# Other Changes

- 13120 - (policy) Treat segwit as always active
- 13191 - (consensus) Specialized double-SHA256 with 64 byte inputs
- 10244 - (GUI) separate gui from wallet and node
- 13033 - (Node) Build txindex in parallel with validation

# watchonly wallets

**This mode creates pure watch-only mode, ideal for a use-case where one uses Bitcoin-Core in conjunction with a hardware-wallet or other solutions for cold-storage.**

**We have support for custom change addresses in fundrawtransaction, so pure watch-only wallets including coin-selection are possible and make sense for some use cases.**

**This new mode disables all forms of private key generation and ensure that no mix between hot and cold keys are possible.**



# Branch and Bound Coin Selection

The algorithm was designed to purposefully find exact matches, to be less computationally expensive than Bitcoin Core's previous coin selection policy, and to be easy to implement.

The study of the subset sum problem was an inspiration as it describes a similar combinatorial problem. The main ideas were:

- 1. *Effective value of UTXOs.*** The previous implementation attempted to pack a knapsack whose size changed while it was being packed. Effective values allow reframing of the problem such that the target remains fixed.
- 2. *Efficient search for exact matches.*** Instead of restarting the search multiple times and repeatedly exploring the same combinations, the combination space of the effective values can be searched exhaustively once with less effort.

# Dynamic Wallet Load/Create/Unload

**Bitcoin Core allows multiple wallets to be run on the same node. Previously all wallets would need to be loaded or created at start time.**

**This series of PRs allows wallets to be loaded, created and unloaded during runtime.**

# scantxoutset RPC Method

**Takes output descriptors and looks up scripts in the UTXO set matching those descriptors.**

**Returns an array similar to `listunspent`, which is compatible with `createrawtransaction` and `signrawtransaction`.**

**This makes it possible to prepare sweeps and have them signed in a secure (cold) space.**

# An aside on output descriptors

- Human-readable descriptors of sets of scriptPubKeys, together with information about how to spend them ("solving"), and optionally also private keys.
- Public keys, xpubs, and their secret key versions don't carry any information about the type of scripts to be used.
- Historically, this was addressed by implying certain types of scripts with keys (P2PKH and P2PK, and later P2WPKH and P2SH-P2WPKH). That was ambiguous, inflexible and scaled badly.
- Output descriptors is a language that is sufficiently flexible to serve as the primary source of information about what outputs are treated as belonging to a certain wallet.
- <https://gist.github.com/sipa/e3d23d498c430bb601c5bca83523fa82>

# Multiwallet for the GUI

**Allows users to access multiple wallets through the GUI.**

**Multiwallet was introduced in V0.16, but was a RPC-only feature. This allows GUI users to use the multiwallet feature.**

# Introduce interface for signing providers

**Currently, the Bitcoin Core wallet contains keys, and we determine whether outputs are ours using ad-hoc logic that mostly answers the question "Could we sign this?"**

**We'd like to move away from loose pieces of information that define what we consider ours when the puzzle pieces fit, and instead structure everything in records. Each record would correspond to an exact scriptPubKey.**

**This PR (and others in v0.17) start the work of seperating the keystore from the signing logic.**

# Remove accounts API

**Deprecates the 'accounts' API, and introduces a 'labels' API.**

**Accounts were added as a bolt-on feature and suffered from many problems (didn't scale well, could show negative balances, etc).**

**Accounting should be done outside the Bitcoin Core wallet.**

**This series of PRs retains the ability to label addresses (using the label API), but removes the account balances feature.**

**Accounts will be fully removed in v0.18.**

# Implement Partially Signed Bitcoin Transactions (PSBT)

**Implements the BIP 174 specification.**

**BIP 174 specifies a binary transaction format which contains the information necessary for a signer to produce signatures for the transaction and holds the signatures for an input while the input does not have a complete set of signatures.**

**Introduces new PSBT RPCs `createpsbt`, `decodepsbt`, `finalizepsbt`, etc.**



# Always create signatures with Low R values

A DER-encoded ECDSA signature can be *up to* 73 bytes, depending on the 'R' and 'S' values in the signature.

Standardness rules dictate that 'S' must be low (32 bytes).

This PR ensures that 'R' is also low (32 or fewer bytes).

This ensures all signatures produced by the wallet will be 71 bytes or smaller.

# Specialized double-SHA256 with 64 byte inputs with SSE4.1 and AVX2

**introduces a framework for specialized double-SHA256 with 64 byte inputs.**

**Benchmarks for computing the Merkle root of 9001 leaves (supported lengths / special instructions / parallelism):**

- **7.2 ms with varsize/naive/1way (before, non-SSE4 hardware)**
- **5.8 ms with size64/naive/1way (after, non-SSE4 capable systems)**
- **4.8 ms with varsize/SSE4/1way (before, SSE4 hardware)**
- **2.9 ms with size64/SSE4/4way (after, SSE4 hardware)**
- **1.1 ms with size64/AVX2/8way (after, AVX2 hardware)**

# Separate gui from wallet and node

**Refactoring PR that does not change behaviour. Creates abstract Node and Wallet interfaces and updates GUI code to call the new interfaces.**

**This provides a single place to define the interface between GUI and daemon code, allows better testing, and will allow process separation in a future PR.**

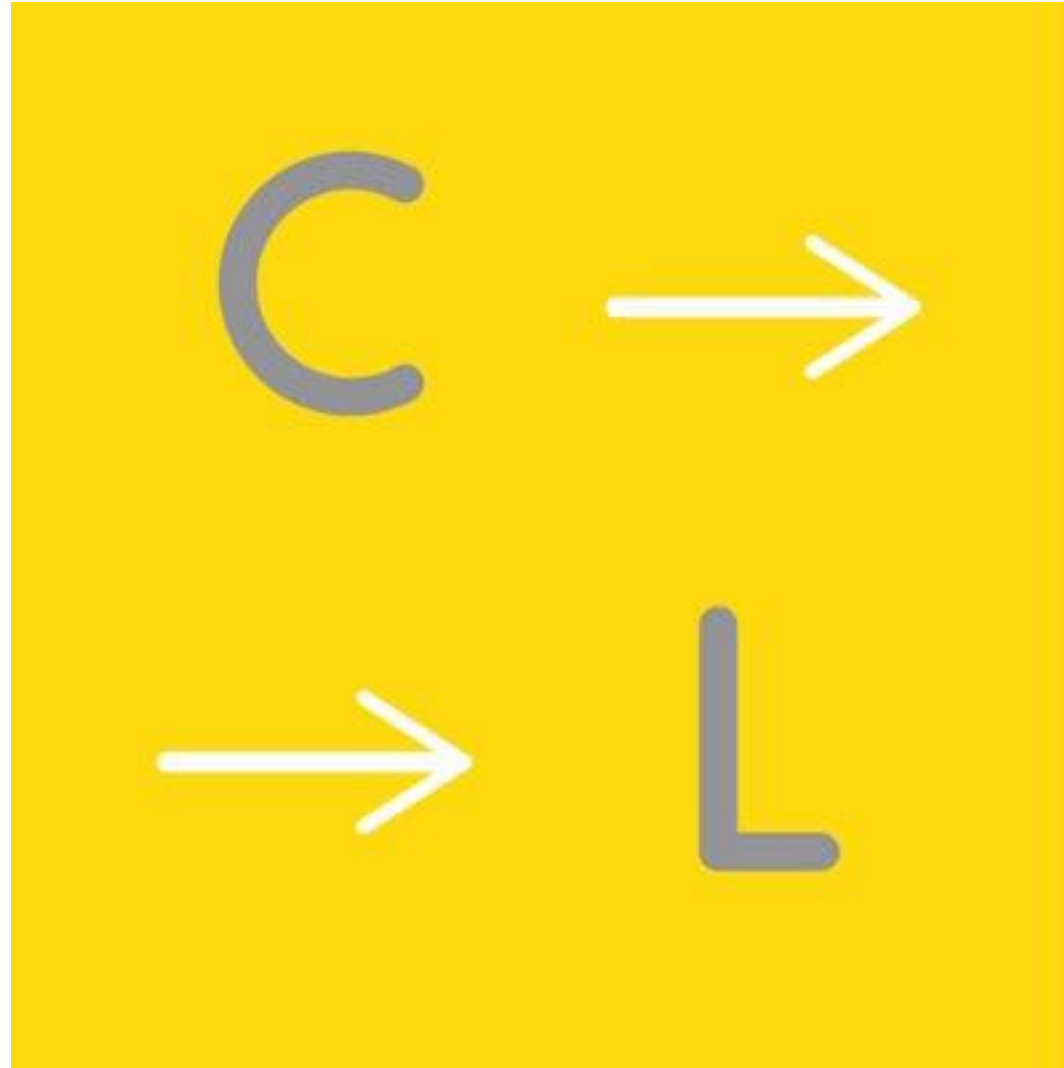
# Build txindex in parallel with validation

**Refactors the tx index code to be in its own class and get built concurrently with validation code.**

**The main benefit is decoupling and moving the txindex into a separate DB.**

**Lays the groundwork for other indexers that might be desired (such as compact filters).**

Q & A



**Chaincode Labs exists to support and develop Bitcoin and other peer-to-peer decentralized systems.**

<https://chaincode.com>

[twitter.com/ChaincodeLabs](https://twitter.com/ChaincodeLabs)

Chaincode Residency

[ABOUT](#) [SESSIONS](#) [MENTORS](#) [APPLY](#) [MEETUPS](#)

Chaincode Residency

**JANUARY 29TH - FEBRUARY 23RD 2018**



# Bitcoin Optech





# What we're doing

- Engaging companies
- Workshops
- Newsletter
- Cookbook
- Engineer forum
- Website
- Dashboard



# Engaging Companies

- Taken meetings with ~25 Bitcoin companies
- Exploring common pain points, blockchain usage
- Companies from across the industry:
  - Exchanges
  - Custodians
  - Wallets
- Technical deep dives



# Workshops

- San Francisco - July 17th
- Covers RBF/CPFP, coin selection, engaging with open source community
- 7 companies attending
- More workshops to follow!

## Workshops

### Workshop #1 - SF Edition

Tuesday, July 17  
Square - San Francisco, CA  
1-2 engineers from SF Bay Area Bitcoin companies

#### Agenda:

12:30-1:00 Introductions  
1:00-2:00 Topic #1: Coin selection  
2:00-2:15 Break  
2:15-3:15 Topic #2: Fee estimation, RBF, CPFP  
3:15-3:30 Break  
3:45-4:45 Topic #3: Optech community and communication  
4:45-5:00 Wrap up

5:30-7:30 Dinner at TBD nearby restaurant

#### Format:

- Each topic will be a roundtable discussion in which every participant has an equal opportunity to engage.
- There will be a moderator and rotetaker. The moderator will be responsible for a brief introduction of a topic and keeping discussion on track and on time.
- We want participants to be comfortable to speak freely, so it is intended that notes and action items taken will be distributed to participants but not beyond. Participants are free to share discussion details internally at their companies and publicly, but should refrain from attributing any particular statement to a given individual (Chatham House Rules).

#### Possible Topic Discussion Points

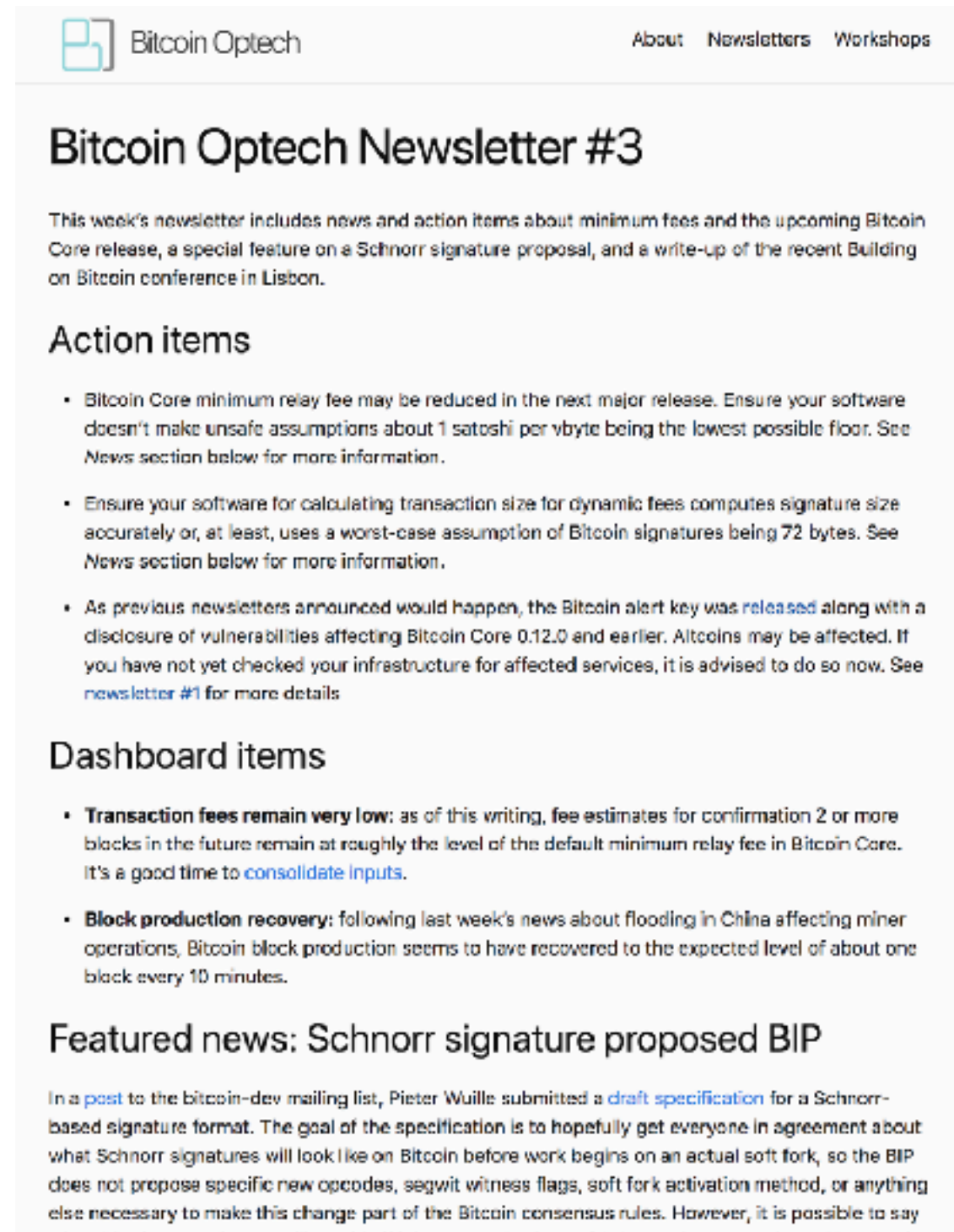
Topic #1: Coin selection

- What do you do today?
- What constraints do you face?
- How do you prioritize potentially competing factors: blockchain efficiency, transaction throughput, privacy, minimizing fees?



# Newsletters

- Action items
- News
- Network stats
- Feedback please!



The screenshot shows the Bitcoin Optech Newsletter #3 page. At the top left is the Bitcoin Optech logo and name. At the top right are links for 'About', 'Newsletters', and 'Workshops'. The main heading is 'Bitcoin Optech Newsletter #3'. Below it is a paragraph summarizing the newsletter's content: 'This week's newsletter includes news and action items about minimum fees and the upcoming Bitcoin Core release, a special feature on a Schnorr signature proposal, and a write-up of the recent Building on Bitcoin conference in Lisbon.' The page is divided into three sections: 'Action items', 'Dashboard items', and 'Featured news: Schnorr signature proposed BIP'. Each section contains a list of bullet points with links to related articles.

Bitcoin Optech [About](#) [Newsletters](#) [Workshops](#)

## Bitcoin Optech Newsletter #3

This week's newsletter includes news and action items about minimum fees and the upcoming Bitcoin Core release, a special feature on a Schnorr signature proposal, and a write-up of the recent Building on Bitcoin conference in Lisbon.

### Action items

- Bitcoin Core minimum relay fee may be reduced in the next major release. Ensure your software doesn't make unsafe assumptions about 1 satoshi per vbyte being the lowest possible floor. See [News](#) section below for more information.
- Ensure your software for calculating transaction size for dynamic fees computes signature size accurately or, at least, uses a worst-case assumption of Bitcoin signatures being 72 bytes. See [News](#) section below for more information.
- As previous newsletters announced would happen, the Bitcoin alert key was [released](#) along with a disclosure of vulnerabilities affecting Bitcoin Core 0.12.0 and earlier. Altcoins may be affected. If you have not yet checked your infrastructure for affected services, it is advised to do so now. See [newsletter #1](#) for more details

### Dashboard items

- **Transaction fees remain very low:** as of this writing, fee estimates for confirmation 2 or more blocks in the future remain at roughly the level of the default minimum relay fee in Bitcoin Core. It's a good time to [consolidate inputs](#).
- **Block production recovery:** following last week's news about flooding in China affecting miner operations, Bitcoin block production seems to have recovered to the expected level of about one block every 10 minutes.

### Featured news: Schnorr signature proposed BIP

In a [post](#) to the bitcoin-dev mailing list, Pieter Wuille submitted a [draft specification](#) for a Schnorr-based signature format. The goal of the specification is to hopefully get everyone in agreement about what Schnorr signatures will look like on Bitcoin before work begins on an actual soft fork, so the BIP does not propose specific new opcodes, segwit witness flags, soft fork activation method, or anything else necessary to make this change part of the Bitcoin consensus rules. However, it is possible to say



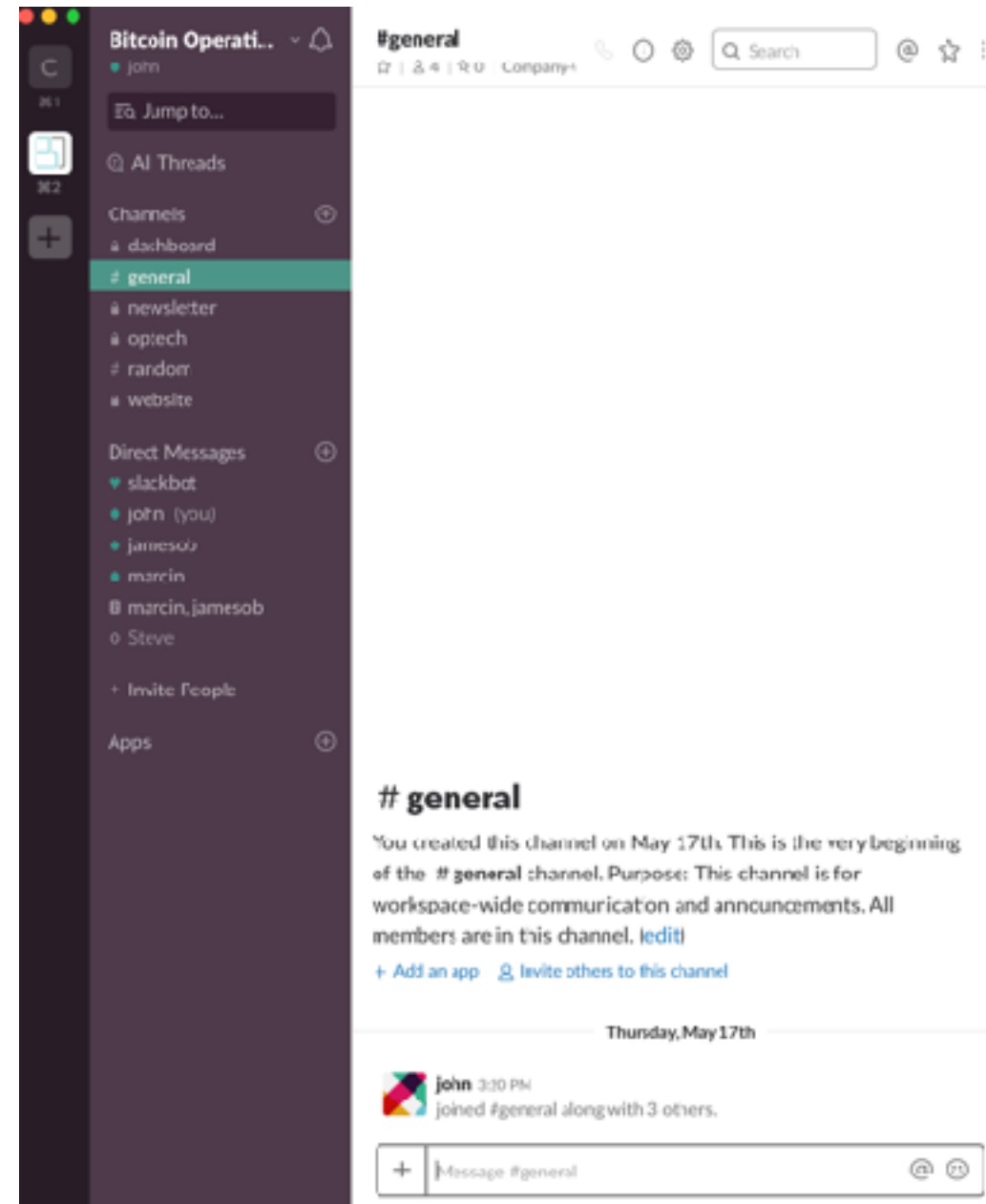
# Cookbook

- First chapter is on RBF/CPFP.
- Looking for contributors and reviewers.
- We need feedback and suggestions for future chapters.



# Engineer forum

- Open for members and open-source developers



# Website

<https://bitcoinops.org>

- Information and engagement
- Blog
- Dashboard
- Newsletters



The screenshot shows the Bitcoin Optech website homepage. At the top left is the Bitcoin Optech logo, a stylized 'B' made of two overlapping shapes. To its right are navigation links: 'About', 'Newsletters', and 'Workshops'. The main content area features a large, light blue version of the logo above the text 'Bitcoin Optech'. Below this is a paragraph of text: 'The Bitcoin Operations Technology Group (Optech) works to bring the best open source technologies and techniques to Bitcoin-using businesses in order to lower costs and improve customer experiences.' This is followed by another paragraph: 'An initial focus for the group is working with its member organizations to reduce transaction sizes and minimize the effect of subsequent transaction fee increases.' The next paragraph states: 'Long-term goals include providing documentation and training materials, a weekly newsletter, original research, and facilitating improved relations between businesses and the open source community.' The following paragraph reads: 'Optech does not exist to make a profit, and all materials and documentation produced are placed in the public domain. We are supported by our generous founding sponsors and contributions from member companies.' Below this is a section titled 'Founding Sponsors' with the text: 'Our founding sponsors have generously provided funds and resources to cover our start-up and ongoing costs.' At the bottom of the page, there are two small portrait photos of men, likely the founding sponsors mentioned in the text.



Bitcoin Optech

<https://bitcoinops.org>

@bitcoinoptech

# Dashboard

