

Bitcoin Core 0.16.3

<https://github.com/bitcoin/bitcoin/releases/tag/v0.16.3>

<https://nvd.nist.gov/vuln/detail/CVE-2018-17144>

Bitcoin Core 0.17rc4

<https://github.com/bitcoin/bitcoin/releases/tag/v0.17.0rc4>

Bitcoin Core PRs

<https://github.com/bitcoin/bitcoin/pull/14053>

<https://github.com/bitcoin/bitcoin/pull/14060>

<https://github.com/bitcoin/bitcoin/pull/14079>

<https://github.com/bitcoin/bitcoin/pull/14075>

<https://github.com/bitcoin/bitcoin/pull/14220>

<https://github.com/bitcoin/bitcoin/pull/12676>

(merged)<https://github.com/bitcoin/bitcoin/pull/12254>

<https://github.com/bitcoin/bitcoin/pull/13152>

<https://github.com/bitcoin/bitcoin/pull/12490>

<https://github.com/bitcoin/bitcoin/commit/b2f49bd7325989267017260a9e7c843588a8c237>
(/merged)

Optech

<https://bitcoinops.org/en/newsletters/2018/08/21/>

<https://bitcoinops.org/en/newsletters/2018/08/28/>

<https://bitcoinops.org/en/newsletters/2018/09/04/>

<https://bitcoinops.org/en/newsletters/2018/09/11/>

<https://bitcoinops.org/en/newsletters/2018/09/18/>

BIP 151 Overhall

<https://github.com/bitcoin/bitcoin/pull/14032>

<https://github.com/bitcoin/bitcoin/pull/14047>

<https://github.com/bitcoin/bitcoin/pull/14049>

<https://github.com/bitcoin/bitcoin/pull/14050>

BIP: Generic Signed Message Format by kallewoof

<https://github.com/bitcoin/bips/pull/725>

[bitcoin-dev] SIGHASH2 for version 1 witness programme

<https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-August/016345.html>

[bitcoin-dev] bustapay BIP :: a practical sender/receiver coinjoin protocol

<https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-September/016384.html>

Stats

<https://dashboard.bitcoinops.org/d/TDhboADmk/bitcoin-optech-dashboards?orgId=1>

<https://asicboost.dance>

<https://btc.com/00000000000000000021868c2cefc52a480d173c849412fe81c4e5ab806f94ab>

Lightning Network

c-lightning 0.6.1

<https://github.com/ElementsProject/lightning/releases/tag/v0.6.1>

first version of lib-autopilot.py

<https://github.com/ElementsProject/lightning/pull/1888>

Spark: A new GUI for c-lightning

<https://medium.com/@notgrubles/spark-a-new-gui-for-c-lightning-2cf2f024500c>

Lightning Desktop 0.2.2-alpha Release

<https://blog.lightning.engineering/announcement/2018/09/10/lightning-app.html>

LND 0.5 Release

<https://blog.lightning.engineering/announcement/2018/09/14/lnd-v0.5.html>

LND PRs

<https://github.com/lightningnetwork/lnd/pull/1937>

<https://github.com/lightningnetwork/lnd/pull/1941>

(merged)<https://github.com/lightningnetwork/lnd/pull/1818>

<https://github.com/lightningnetwork/lnd/pull/1824>

<https://github.com/lightningnetwork/lnd/pull/1516>

<https://github.com/lightningnetwork/lnd/pull/1843>

<https://github.com/lightningnetwork/lnd/pull/1809> (/merged)

LND performance improvements

<https://twitter.com/alexbosworth/status/1040460464826642435>

Zap Desktop 0.2.1

<https://medium.com/@JimmyMow/zap-desktop-0-2-1-cant-stop-won-t-stop-61acb2e4ee15>

Schnorr and Taproot in Lightning

<https://jonasnick.github.io/blog/2018/09/04/schnorr-and-taproot-in-lightning/>

Atomic on-chain ETH to off-chain BTC swap

<https://medium.com/@jason.hcwong/atomic-on-chain-eth-to-off-chain-btc-swap-3c959ab22e52>

MimbleWimble

Enable non-interactive transactions in Grin

[https://www.reddit.com/r/grincoin/comments/9deh40/is_there_any_idea_to_enable_noninteracti
ve/e5j12rn](https://www.reddit.com/r/grincoin/comments/9deh40/is_there_any_idea_to_enable_noninteracti/e5j12rn)

BIP32 Wallet Compliance - Aggsig Updates - Bulletproof Update

<https://github.com/mimblewimble/grin/pull/1501>

Research

Routing Cryptocurrency with the Spider Network

<http://arxiv.org/abs/1809.05088v2>

Airdrops and Privacy: A Case Study in Cross-Blockchain Analysis

<http://arxiv.org/abs/1809.05360v1>

The Unreasonable Effectiveness of Address Clustering

<https://arxiv.org/abs/1605.06369v3>

Superspace: Scaling Bitcoin Beyond SegWit

[http://diyhl.us/~bryan/papers2/bitcoin/Superspace:%20Scaling%20bitcoin%20beyond%20segw
it%20-%202018.pdf](http://diyhl.us/~bryan/papers2/bitcoin/Superspace:%20Scaling%20bitcoin%20beyond%20segwit%20-%202018.pdf)

On the Provable Security of Two-Round Multi-Signatures

<https://eprint.iacr.org/2018/417.pdf>

Mainstay: enabling trustless immutability in federated sidechains

[https://www.commerceblock.com/wp-content/uploads/2018/03/commerceblock-mainstay-whitep
aper.pdf](https://www.commerceblock.com/wp-content/uploads/2018/03/commerceblock-mainstay-whitepaper.pdf)

Misc.

Linux 4.19-rc4 released, an apology, and a maintainership note

<https://lkml.org/lkml/2018/9/16/167>

Bitmain and Its Patent Dispute with Whatsminer

[https://medium.com/@cryptovenus/bitmain-and-its-patent-dispute-with-pangolin-miner-6a51b32f
55a1](https://medium.com/@cryptovenus/bitmain-and-its-patent-dispute-with-pangolin-miner-6a51b32f55a1)

Photos: Inside one of the world's largest bitcoin mines

<https://qz.com/1055126/photos-china-has-one-of-worlds-largest-bitcoin-mines/>

InfoSec

Hacking the Bitfi.

<https://www.pentestpartners.com/security-blog/hacking-the-bitfi-part-1/>

Exploit Affecting Tor Browser Burned In A Tweet

<https://www.bleepingcomputer.com/news/security/exploit-affecting-tor-browser-burned-in-a-tweet/>

SonarSnoop: Active Acoustic Side-Channel Attacks

<https://arxiv.org/pdf/1808.10250v1.pdf>

Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels

<https://www.cs.tau.ac.il/~tromer/synesthesia/synesthesia.pdf>

One&Done: A Single-Decryption EM-Based Attack on OpenSSL's Constant-Time Blinded RSA

<https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-alam.pdf>

The Chilling Reality of Cold Boot Attacks

<https://blog.f-secure.com/cold-boot-attacks/>