Notable Public Keys

STEVEN BALTAKATEI SANDOVAL

Email: baltakatei@gmail.com

Web: https://reboil.com

Front Matter

The book is available as source code in a `git` repository available at:

https://reboil.com/gitweb/BK-2021-09.git

This book was typeset using **TEXMACS** version 2.1.
Fonts used include **Linux Libertine**.
This book was rendered on 2021-07-21T10:42:09+0000.

Table of contents

Chapter 1
Trust through Stories

This book contains stories about where certain public keys came from and a little about the people who use them.

Some people use public key cryptography to digitally sign their works. They do this so others can prove where copies of such works came from. Usually, digital tools automatically verify these digital signatures so people don't have to manually. However, in order to verify such tools, at some point a person must verify at least one digital signature for themselves.

Chapter 2
List of Public Keys

Each section in this chapter contains a story about a person or organization that uses a public-private key pair. Each story consists of some brief background information, a history of notable events, and public key information. Key fingerprints are included. Links to public keys are made available where possible.

2.1 BITCOIN CORE

2.1.1 Background

BITCOIN CORE is the "reference implementation" of the BITCOIN protocol. It is maintained by a group of people who have become known as the BITCOIN CORE developers.

Early in the blockchain's history, the software that verified transactions against balances of previous transactions was a WINDOWS executable known as BITCOIN. The initial release of this software was by an entity that called themselves SATOSHI NAKAMOTO. Satoshi later gave up the code maintainer role of the project. The person who subsequently gained control was a person named Gavin Andresen. The software was rebranded from BITCOIN to BITCOIN CORE at version *0.9.0*.[2.1.1] A developer named WLADIMIR J. VAN DER LAAN became owner of the signing keys of the reference implementation starting at version *0.9.3*. VAN DER LAAN originally used a personal key (`0x74810B012346C9A6`) to sign binaries but later created a dedicated key (`0x90C8019E36C2E964`) to sign binaries.

There exist various dubious theories regarding PGP key use by SATOSHI NAKAMOTO.[2.1.2] The most likely candidate (`0x18C09E865EC948A1`) is one signed by BITCOIN CORE developers Peter Todd (`0x7FAB114267E4FA04`) and WLADIMIR J. VAN DER LAAN (`0x74810B012346C9A6`).

2.1.2 History

2011-08-24. Creation date of VAN DER LAAN's personal signing key `0x74810B012346C9A6`.

2011-12-15. Creation date of Andresen's dedicated code signing key `0x29D9EE6B1FC730C1`.

2013-03-23. Earliest snapshot of the `https://bitcoin.org` website on the INTERNET ARCHIVE.[2.1.3] It is a redirect to `https://bitcoin.org/en` .

2013-04-11. Earliest snapshot of the `https://bitcoincore.org` website on the INTERNET ARCHIVE.[2.1.4]

2013-07-27. Earliest snapshot of main GITHUB repository at `https://github.com/bitcoin/bitcoin` on the INTERNET ARCHIVE.[2.1.5]

2014-03-19. The reference client rebranded from BITCOIN to BITCOIN CORE.

2014-04-08. Gavin Andresen steps down as lead developer. Hands over role to WLADIMIR J. VAN DER LAAN.[2.1.6] Andresen maintains commit privileges to the GITHUB repository.

2015-06-24. Creation date of VAN DER LAAN's dedicated code signing key `0x90C8019E36C2E964`.

2016-05-02. Gavin Andresen's commit privileges were revoked by other BITCOIN CORE developers after Andresen published a blog post claiming Craig Wright was Satoshi Nakamoto.[2.1.7]

2.1.3 Public Key Details

2.1.3.1 Binary Signing Key (v0.11.0–)

This key[2.1.8], owned by WLADIMIR J. VAN DER LAAN, has been used to sign BITCOIN CORE releases since version `0.11.0`.

2.1.1. See `https://bitcoin.org/en/release/v0.9.0#rebranding-to-bitcoin-core` .

2.1.2. See `https://www.vice.com/en/article/jpgq3y/satoshis-pgp-keys-are-probably-backdated-and-point-to-a-hoax` .

2.1.3. See `https://web.archive.org/web/20130323195546/http://bitcoin.org/en` .

2.1.4. See `https://web.archive.org/web/20130411033932/http://bitcoincore.org/` .

2.1.5. See `https://web.archive.org/web/20130727135658/https://github.com/bitcoin/bitcoin` .

2.1.6. See `https://www.coindesk.com/gavin-andresen-steps-bitcoins-lead-developer` .

2.1.7. `https://twitter.com/peterktodd/status/727078284345917441` , `https://laanwj.github.io/2016/05/06/hostility-scams-and-moving-forward.html` , `https://www.bbc.com/news/technology-36202904` , and `https://www.theguardian.com/technology/2016/may/06/bitcoin-project-blocks-out-gavin-andresen-over-satoshi-nakamoto-claims` .

2.1.8. See `https://reboil.com/res/2021/txt/20210719_90C8019E36C2E964..bitcoin_vanderlaan.asc`

```
pub   rsa4096/0x90C8019E36C2E964 2015-06-24 [SC] [expires: 2022-02-10]
      Key fingerprint = 01EA 5486 DE18 A882 D4C2  6845 90C8 019E 36C2 E964
uid                   [ unknown] Wladimir J. van der Laan (Bitcoin Core ...) <laanwj@gmail.com>
```

2.1.3.2 Binary Signing Key (v0.9.3–v0.10.2)

WLADIMIR VAN DER LAAN used his personal key[2.1.9] to sign BITCOIN versions v0.9.3–v0.10.2.

```
pub   rsa2048/0x74810B012346C9A6 2011-08-24 [SC] [expires: 2022-02-10]
      Key fingerprint = 71A3 B167 3540 5025 D447  E8F2 7481 0B01 2346 C9A6
uid                   [ unknown] Wladimir J. van der Laan <laanwj@visucore.com>
uid                   [ unknown] Wladimir J. van der Laan <laanwj@gmail.com>
uid                   [ unknown] Wladimir J. van der Laan <laanwj@protonmail.com>
sub   rsa2048/0x69B4C4CDC628F8F9 2017-05-17 [A] [expires: 2022-02-10]
sub   rsa2048/0xF69705ED890DE427 2011-08-24 [E]
sub   rsa2048/0x1E4AED62986CD25D 2017-05-17 [S] [expires: 2022-02-10]
```

2.1.3.3 Binary Signing Key (v0.8.6–v0.9.2.1)

Gavin Andresen used this dedicated code-signing key[2.1.10] to sign BITCOIN versions v0.8.6–v0.9.2.1. As of 2021-07-19, these versions and their signatures are available at https://bitcoincore.org/bin/insecure/ .

```
pub   rsa4096/0x29D9EE6B1FC730C1 2011-12-15 [SC]
      Key fingerprint = 2664 6D99 CBAE C9B8 1982  EF60 29D9 EE6B 1FC7 30C1
uid                   [ unknown] Gavin Andresen (CODE SIGNING KEY) <gavinandresen@gmail.com>
sub   rsa4096/0x1B7BFB457BF6E212 2013-11-01 [S]
sub   rsa4096/0x36E924A98E30B3ED 2011-12-15 [E]
```

2.1.3.4 Satoshi Nakamoto

The `dsa1024` algorithm this key[2.1.11] uses is considered weak by the the NIST standard SP800-57 Part 1 Revision 5: *Recommendation for Key management*.[2.1.12] The key offers only 80 bits of security against the possibility of impersonation via a brute force attack. Nevertheless, this key has a signature of BITCOIN CORE developer Peter Todd (`0x7FAB114267E4FA04`) dated 2013-10-12. Todd also committed the full fingerprint in a BITCOIN FOUNDATION document on 2013-04-26[2.1.13]. This key also has a signature of BITCOIN CORE maintainer VLADIMIR J. VAN DER LAAN's personal key (`0x74810B012346C9A6`) dated 2013-05-10.

```
pub   dsa1024/0x18C09E865EC948A1 2008-10-30 [SC]
      Key fingerprint = DE4E FCA3 E1AB 9E41 CE96  CECB 18C0 9E86 5EC9 48A1
uid                   [ unknown] Satoshi Nakamoto <satoshin@gmx.com>
sig 3        0x18C09E865EC948A1 2008-10-30  Satoshi Nakamoto <satoshin@gmx.com>
sig          0x74810B012346C9A6 2013-05-10  Wladimir J. van der Laan <laanwj@visucore.com>
sig 1        0x7FAB114267E4FA04 2013-10-12  Peter Todd <pete@petertodd.org>
sub   elg2048/0xCF1857E6D6AAA69F 2008-10-30 [E]
sig          0x18C09E865EC948A1 2008-10-30  Satoshi Nakamoto <satoshin@gmx.com>
```

2.1.9. See https://reboil.com/res/2021/txt/20210719_74810B012346C9A6..bitcoin_vanderlaan.asc

2.1.10. See https://reboil.com/res/2021/txt/20210719_29D9EE6B1FC730C1..bitcoin_andresen.asc

2.1.11. See https://reboil.com/res/2021/txt/20210719_18C09E865EC948A1..bitcoin_nakamoto.asc

2.1.12. See https://doi.org/10.6028/NIST.SP.800-57pt1r5 , table 2, page 54. `dsa1024` keys have only offer 80 bits of security against brute force attacks.

2.1.13. See https://github.com/pmlaw/The-Bitcoin-Foundation-Legal-Repo/commit/fb70771a9927e04ebe5ae33c46ba6589a9703e40 .

2.2 GITHUB

2.2.1 Background

GITHUB is a commercial GIT repository hosting service company founded in 2008. It was purchased by MICROSOFT in 2016.[1]

2.2.2 History

2008. GITHUB founded in San Francisco.[1]

2008-03-10. GITHUB parent company LOGICAL AWESOME, LLC registered in San Francisco by Chris Wanstrath.[2.2.1]

2008-05-14. First snapshot of the `https://github.com` website on the INTERNET ARCHIVE.[2.2.2]

2017-08-16. Creation date of the `0x4AEE18F83AFDEB23` public key according to itself.

2017-11-14. Date of INTERNET ARCHIVE snapshot containing an early link to `https://github.com/web-flow.gpg` from a page on the `help.github.com` domain.[2.2.3] Also the date of a post by GITHUB user `jonathancross`[2.2.4] observing that the `0x4AEE18F83AFDEB23` key appears to be a new feature[2.2.5]:

> Yeah, just experimented and saw the same thing. Strange new "feature" of GitHub it seems.

2018-06-04. First snapshot of the `0x4AEE18F83AFDEB23` public key `https://github.com/web-flow.gpg` on the INTERNET ARCHIVE.[2.2.6]

2021-05-25. Public key `0x4AEE18F83AFDEB23` fingerprint explicitly published at GITHUB documentation website.[2.2.7]

2.2.3 Public Key Details

As of 2021-07-19, when a user logs into `github.com` and creates a GIT commit through a web browser, GITHUB will automatically sign the commit against a GPG key[2.2.8] with the fingerprint:

```
pub   rsa2048/0x4AEE18F83AFDEB23 2017-08-16 [SC]
      Key fingerprint = 5DE3 E050 9C47 EA3C F04A  42D3 4AEE 18F8 3AFD EB23
uid                   [ unknown] GitHub (web-flow commit signing) <noreply@github.com>
```

This key is available for download at GITHUB's documentation website at `https://github.com/web-flow.gpg` .[2.2.9] This particular link as well as the full key fingerprint was added to the GITHUB documentation repository in a commit dated 2021-05-25[2.2.10].

2.2.1. See `https://businesssearch.sos.ca.gov/Document/RetrievePDF?Id=200807010145-721605` and `https://businesssearch.sos.ca.gov/Document/RetrievePDF?Id=200807010145-2544282` from `https://opencorporates.com/companies/us_ca/200807010145` .

2.2.2. See `https://web.archive.org/web/20080514210148/http://github.com/` .

2.2.3. See `https://web.archive.org/web/20171114055613/https://help.github.com/articles/about-gpg/` .

2.2.4. Key fingerprint `0xC0C076132FFA7695`. Key at `https://github.com/jonathancross.gpg` .

2.2.5. `https://github.com/keepassxreboot/keepassxc/issues/1183#issuecomment-344386172` .

2.2.6. `https://web.archive.org/web/20180604123146/https://github.com/web-flow.gpg` .

2.2.7. See See `https://github.com/github/docs/commit/c4e1cb7a97704f0d90c0d6ed7e52d72b1e4946c1` .

2.2.8. See `https://reboil.com/res/2021/txt/20210719_4AEE18F83AFDEB23..github.asc` or `https://github.com/web-flow.gpg` .

2.2.9. See `https://docs.github.com/en/github/authenticating-to-github/managing-commit-signature-verification/about-commit-signature-verification` .

2.2.10. See `https://github.com/github/docs/commit/c4e1cb7a97704f0d90c0d6ed7e52d72b1e4946c1` .

2.3 RaspiBlitz

2.3.1 Background

RaspiBlitz is a software package designed to facilitate operation of a Lightning Network and Bitcoin node. The software is version controlled using git, with the main git repository available at GitHub.[2.3.1] As of 2021-07-18, the principal maintainer appears to be Christian "rootzol" Rotzoll[2.3.2].

2.3.2 History

2019-09-03. The creation date of rootzol's 0x1C73060C7C176461 public key.

2019-09-05. rootzol added their public key fingerprint 0x1C73060C7C176461 to the FAQ of the RaspiBlitz GitHub repository.[2.3.3] They linked their keybase.io page as a source of the public key.

2020-10-31. The first snapshot of the raspiblitz.org website appeared on the Internet Archive.[2.3.4]

2021-02-07. Andreas Antonopoulos posted a YouTube video identifying RaspiBlitz as a popular Bitcoin full node software package.[2.3.5]

2021-05-18. rootzol added their public key fingerprint 0x1C73060C7C176461 to the README of the RaspiBlitz GitHub repository.

2.3.3 Public Key Details

2.3.3.1 Christian "rootzol" Rotzoll

rootzol's PGP key[2.3.6] may be downloaded from their Keybase page.[2.3.7]. Their fingerprint information is as follows:

```
pub   rsa4096/0x1C73060C7C176461 2019-09-03 [C]
      Key fingerprint = 92A7 46AE 33A3 C186 D014  BF5C 1C73 060C 7C17 6461
uid                  [ unknown] Christian Rotzoll <christian@rotzoll.de>
sub   rsa4096/0xAA9DD1B5CC5647DA 2019-09-03 [S] [expires: 2021-10-21]
sub   rsa4096/0xD40D94E6C7C9B4D9 2019-09-03 [E] [expires: 2021-10-21]
sub   rsa4096/0x1C29DC2F8D764F9A 2019-09-03 [A] [expires: 2021-10-21]
```

2.3.1. See https://github.com/rootzoll/raspiblitz .

2.3.2. Their public key 0x1C73060C7C176461 is available at: https://keybase.io/rootzoll .

2.3.3. See https://github.com/rootzoll/raspiblitz/commit/75ebdd8d571cccc427b5d023a25c6e2e9e8a2da2 .

2.3.4. See https://web.archive.org/web/20201031223643/https://raspiblitz.org/ .

2.3.5. See https://www.youtube.com/watch?v=AXUfwvhr3lg&t=26m27s .

2.3.6. See https://reboil.com/res/2021/txt/20210719_0x1C73060C7C176461..raspiblitz_rootzol.asc

2.3.7. See https://keybase.io/rootzoll/pgp_keys.asc .

Appendix A
How Public Key Cryptography Works

This appendix describes in more detail how public key cryptography works.

Appendix B
How to use GNUPG

This appendix describes in more detail how to use GNUPG.

Bibliography

[1] Steve Lohr . Microsoft Buys GitHub for $7.5 Billion, Moving to Grow in Coding's New Era. *New York Times*, 2018.

Index