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 2.1.1.
Fonts used include **Linux Libertine**.
This book was rendered on 2022-01-03T12:36:20+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. See 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 CRYPTOMATOR

2.2.1 Background

CRYPTOMATOR is a cross-platform file storage privacy application. It permits storing files on a third-party file storage services (e.g. DROPBOX) in encrypted form and accessible to the user as a virtual mountable drive. In other words, CRYPTOMATOR acts as an encryption layer between a user and a file storage service. Compiled binary releases are available for WINDOWS, MACOS, LINUX, ANDROID, and IOS[2.2.1].

As of 2021-12-22, the latest version of CRYPTOMATOR is version *1.6.5 (Hotfix)* available on GITHUB.[2.2.2] Judging from commit signatures of the GITHUB repository[2.2.3], the main developers appear to be SEBASTIAN STENZEL (0x667B866EA8240A09) ARMIN SCHRENK (0x748E55D51F5B3FBC), and TOBIAS HAGEMANN (0x69CEFAD519598989).

2.2.2 History

2015-01-01. First snapshot of https://cryptomator.org captured on the INTERNET ARCHIVE.[2.2.4] Signature of latest version of CRYPTOMATOR (*1.4.11*) uses PGP key 0x509C9D6334C80F11.[2.2.5]

2018-06-17. Binary signing PGP key 0x509C9D6334C80F11 published as GITHUB gist.[2.2.6] Key used to sign CRYPTOMATOR versions prior to *1.5.8*.

2020-09-01. Binary signing PGP key 0x615D449FE6E6A235 published as GITHUB gist.[2.2.7] Key used to sign CRYPTOMATOR version *1.5.8* onward (as of 2021-12-22).

2020-09-02. Old binary signing PGP key 0x615D449FE6E6A235 signed by new PGP key 0x509C9D6334C80F11.[2.2.8] Notice of revocation of old key and signing of new key by old key posted in GITHUB issue thread.[2.2.9]

2.2.3 Public Key Details

2.2.3.1 Binary signing key (–v1.5.7)

PGP key used to sign compiled binary releases of CRYPTOMATOR prior to version *1.5.8*.

```
pub   rsa4096/0x509C9D6334C80F11 2016-06-24 [SC] [expires: 2021-12-31]
      Key fingerprint = 5054 3A3D A4B1 DB81 DA3E  79CB 509C 9D63 34C8 0F11
uid                   [ unknown] Cryptobot (Release Manager) <releases@cryptomator.org>
```

2.2.1. See https://cryptomator.org/downloads/ .

2.2.2. See https://github.com/cryptomator/cryptomator/releases/tag/1.6.5 .

2.2.3. See https://github.com/cryptomator/cryptomator .

2.2.4. See https://web.archive.org/web/20150101033915/http://cryptomator.org/ .

2.2.5. Signature file at: https://web.archive.org/web/20210502041159/https://dl.bintray.com/cryptomator/cryptomator/1.4.11/cryptomator-1.4.11-x86_64.AppImage.asc . Signed file at: https://web.archive.org/web/20210502115653/https://dl.bintray.com/cryptomator/cryptomator/1.4.11/cryptomator-1.4.11-x86_64.AppImage .

2.2.6. See https://gist.github.com/cryptobot/8ccf8fd686d0c2d8381b69126bb3f2f8/9fdeef62bddf9edf7b73f61f42423f1f123d3218 .

2.2.7. See https://gist.github.com/cryptobot/211111cf092037490275f39d408f461a/1a8e133a1d7e6ae4eb2bcc0830e4567393e5162a .

2.2.8. See https://gist.github.com/cryptobot/211111cf092037490275f39d408f461a/d416c6f0d35506116436cbe2f872baa217f3f72a . Verify with `$ gpg --import` and `$ gpg --list-signatures` to show the signature (**highlighted**):

```
pub   rsa4096/0x615D449FE6E6A235 2020-08-18 [SC] [expires: 2031-01-01]
      Key fingerprint = 5811 7AFA 1F85 B3EE C154  677D 615D 449F E6E6 A235
uid                   [ unknown] Cryptobot <releases@cryptomator.org>
sig 3        0x615D449FE6E6A235 2020-08-18  Cryptobot <releases@cryptomator.org>
sig          0x667B866EA8240A09 2020-08-18  [User ID not found]
sig          0x509C9D6334C80F11 2020-09-02  Cryptobot (Release Manager) <releases@cryptomator.org>
```

2.2.9. See https://github.com/cryptomator/cryptomator.github.io/issues/25#issuecomment-685308263 .

2.2.3.2 Binary signing key (v1.5.8–)

PGP key used to sign compiled binary releases of CRYPTOMATOR after version *1.5.8* (as of 2021-12-22).

```
pub   rsa4096/0x615D449FE6E6A235 2020-08-18 [SC] [expires: 2031-01-01]
      Key fingerprint = 5811 7AFA 1F85 B3EE C154  677D 615D 449F E6E6 A235
uid                   [ unknown] Cryptobot <releases@cryptomator.org>
```

2.3 DEBIAN

2.3.1 Background

DEBIAN is a free operating system from which many GNU/LINUX systems are derived. Such derived systems include UBUNTU, TAILS, KALI LINUX, and others.

DEBIAN is maintained by an association of developers who use GNUPG keys to sign announcements of software they contribute in order to protect against forgeries. A `git` repository containing GNUPG keyrings of DEBIAN keys is available at `https://salsa.debian.org/debian-keyring/keyring` or by installation of the `debian-keyring` package[2.3.1] within a DEBIAN system.

The DEBIAN PROJECT was founded in 1993 by IAN ASHLEY MURDOCK. Various individuals have led the project since.[2.3.2] As of 2021-09-25, the latest release of the oeprating system is called "DEBIAN 11 (BULLSEYE)".

2.3.2 History

1993-08-16. The DEBIAN PROJECT officially founded by IAN ASHLEY MURDOCK.

1999-01-30. Creation date of the Debian CD signing key `7C3B 7970 88C7 C1F7`.

2000-09-16. Creation date of SANTIAGO GARCIA MANTINAN's key `72FD C205 F6A3 2A8E`.

2004-06-20. Creation date of DANIEL BAUMANN's key `F82E 5CC0 4B2B 2B9E`.

2009-10-03. Creation date of the Debian CD signing key `9880 21A9 64E6 EA7D`.

2011-01-05. Creation date of the Debian CD signing key `DA87 E80D 6294 BE9B`.

2014-04-15. Creation date of the Debian Testing CDs Automatic Signing Key `4246 8F40 09EA 8AC3`.

2.3.3 Public Key Details

2.3.3.1 Installation Image Signature Keys

The DEBIAN website makes available images of the operating system that can be installed onto and executed from removable media such as Compact Discs (CD), Digital Versatile Disc (DVD), and Universal Serial Bus (USB) storage devices. A set of GNUPG public key fingerprints have been listed on the `debian.org` website at `https://debian.org/CD/verify` . Table 2.3.1 summarizes the creation dates, long IDs, and availabilities of these keys. Full fingerprints and other information may be found in section 2.3.3.2.

2.3.1. See `https://tracker.debian.org/pkg/debian-keyring`

2.3.2. For a list of DEBIAN Project Leaders, see `https://www.debian.org/doc/manuals/project-history/leaders` .

Date	Long ID	Description	Available	Link
1999-01-30	7C3B 7970 88C7 C1F7	Debian CD signing key	2011–2015 [2.3.3]	[2.3.4]
2000-09-16	72FD C205 F6A3 2A8E	Santiago Garcia Mantinan	2011–2015 [2.3.3]	[2.3.5]
2004-06-20	F82E 5CC0 4B2B 2B9E	Daniel Baumann	2011–2015 [2.3.3]	
2009-05-21	39BE 2D72 5CEE 3195	Daniel Baumann	2011–2015 [2.3.3]	
2009-10-03	9880 21A9 64E6 EA7D	Debian CD signing key	2011–2021 [2.3.3]	
2011-01-05	DA87 E80D 6294 BE9B	Debian CD signing key	2011–2021 [2.3.3]	[2.3.4]
2011-03-09	6F95 B499 6CA7 B5A6	Debian Live Signing Key	2012–2015 [2.3.6]	
2013-05-06	510A D6B9 AD11 CF6A	Debian Live Signing Key	2013–2015 [2.3.7]	
2014-01-03	1239 00F2 A9B2 6DF5	Live Systems Project	2014–2015 [2.3.8]	
2014-04-15	4246 8F40 09EA 8AC3	Debian Testing CDs Automatic Signing Key	2014–2021 [2.3.9]	

Table 2.3.1. A list of keys used to sign DEBIAN installation images. Keys identified from INTERNET ARCHIVE snapshots of https://debian.org/CD/verify .

2.3.3. See https://web.archive.org/web/20110413065857/http://www.debian.org/CD/verify .

2.3.6. See https://web.archive.org/web/20120815030316/http://www.debian.org:80/CD/verify .

2.3.7. See https://web.archive.org/web/20130813130619/http://www.debian.org/CD/verify .

2.3.8. See https://web.archive.org/web/20140410065231/http://www.debian.org/CD/verify .

2.3.9. See https://web.archive.org/web/20140528012106/https://www.debian.org/CD/verify .

2.3.4. Public key available at https://web.archive.org/web/20210928205206/https://www.einval.com/~steve/pgp/ .

2.3.5. Public key available at https://web.archive.org/web/20210928220426/https://reboil.com/res/2021/txt/20210928_72FDC205F6A32A8E..debian_manty.asc .

2.3.3.2 Verbose key details

Key 1999-01-30 (7C3B 7970 88C7 C1F7)

A 1024-bit DSA key that is the earliest dated key for signing Debian CDs mentioned at https://debian.org/CD/verify according to the INTERNET ARCHIVE [2.3.10]. Mention of this key was removed from that page by the end of 2015. A copy of this key can be found at the personal website of STEVE MCINTYRE, a debian developer.[2.3.11]

```
pub   1024D/88C7C1F7 1999-01-30
      Key fingerprint = AC65 6D79 E362 32CF 77BB  B0E8 7C3B 7970 88C7 C1F7
uid                  Steve McIntyre <93sam@debian.org>
uid                  Debian CD signing key <debian-cd@lists.debian.org>
```

Key 2000-09-16 (72FD C205 F6A3 2A8E)

A 1024-bit DSA key listed as being a signing key for Debian CD images as of 2011 at https://debian.org/CD/verify according to the INTERNET ARCHIVE. Mention of this key was removed from that page by the end of 2015. A copy of this key was archived from the pgp.mit.edu keyserver.[2.3.12] This 1024-bit DSA key was deprecated in favor of a 4096-bit RSA key with fingerprint B868 8CA3 D876 D5A3 in a signed blog post at blog.manty.net .[2.3.13]

```
pub   1024D/F6A32A8E 2000-09-16
      Key fingerprint = 3F0A 12FC 0B55 A917 D791  82D3 72FD C205 F6A3 2A8E
uid                  Santiago Garcia Mantinan (manty) <manty@debian.org>
sub   1024g/8D0EB704 2000-09-16
```

2.3.10. See https://web.archive.org/web/20110413065857/http://www.debian.org/CD/verify.

2.3.11. Key 7C3B 7970 88C7 C1F7 is available at https://web.archive.org/web/20210928205229/https://www.einval.com/~steve/pgp/7C3B797088C7C1F7.asc .

2.3.12. Key 72FD C205 F6A3 2A8E is available at https://web.archive.org/web/20210928220426/https://reboil.com/res/2021/txt/20210928_72FDC205F6A32A8E..debian_manty.asc .

2.3.13. Key transition statement available at https://web.archive.org/web/20150614033612/http://blog.manty.net/2014/12/transitioning-from-0xf6a32a8e-to.html . To verify, use gpg --import command on text copied from between the <listing> tags. A copy of this text is also archived at https://web.archive.org/web/20210928222521/https://reboil.com/res/2021/txt/20210928..72FDC205F6A32A8E_to_B8688CA3D876D5A3_pgp_transition_statement.txt .

Key 2004-06-20 (F82E 5CC0 4B2B 2B9E)

A key listed as being a signing key for Debian CD images as of 2011 at https://debian.org/CD/verify according to the INTERNET ARCHIVE. Mention of this key was removed from that page by the end of 2015.

```
pub   1024D/4B2B2B9E 2004-06-20
      Key fingerprint = 709F 54E4 ECF3 1956 2332  6AE3 F82E 5CC0 4B2B 2B9E
uid                  Daniel Baumann <daniel@debian.org>
sub   1024g/19ED1B2F 2004-06-20
```

Key 2009-05-21 (39BE 2D72 5CEE 3195)

A key listed as being a signing key for Debian CD images as of 2011 at https://debian.org/CD/verify according to the INTERNET ARCHIVE.

```
pub   4096R/5CEE3195 2009-05-21
      Key fingerprint = D2FB 633A DDC2 0485 CBCE  6D12 39BE 2D72 5CEE 3195
uid                  Daniel Baumann <daniel@debian.org>
sub   4096R/E7D77F65 2009-05-21
```

Key 2009-10-03 (9880 21A9 64E6 EA7D)

A key listed as being a signing key for Debian CD images as of 2011 at https://debian.org/CD/verify according to the INTERNET ARCHIVE.

```
pub   4096R/64E6EA7D 2009-10-03
      Key fingerprint = 1046 0DAD 7616 5AD8 1FBC  0CE9 9880 21A9 64E6 EA7D
uid                  Debian CD signing key <debian-cd@lists.debian.org>
```

Key 2011-01-05 (DA87 E80D 6294 BE9B)

A key listed as being a signing key for Debian CD images as of 2011 at https://debian.org/CD/verify according to the INTERNET ARCHIVE.

```
pub   4096R/6294BE9B 2011-01-05
      Key fingerprint = DF9B 9C49 EAA9 2984 3258  9D76 DA87 E80D 6294 BE9B
uid                  Debian CD signing key <debian-cd@lists.debian.org>
sub   4096R/11CD9819 2011-01-05
```

Key 2011-03-09 (6F95 B499 6CA7 B5A6)

This key was mentioned at https://debian.org/CD/verify at the end of 2012, according to the INTERNET ARCHIVE.

```
pub   4096R/6CA7B5A6 2011-03-09
      Key fingerprint = 696F 95F0 88E4 D359 947F  7AEB 6F95 B499 6CA7 B5A6
uid                  Debian Live Signing Key <debian-live@lists.debian.org>
sub   4096R/6E7B0CD3 2011-03-09
```

Key 2013-05-06 (510A D6B9 AD11 CF6A)

This key was mentioned at https://debian.org/CD/verify at the end of 2013, according to the INTERNET ARCHIVE.

```
pub   4096R/AD11CF6A 2013-05-06
      Key fingerprint = 1E4F 435C 4E9A 42B3 D9DF  BE3A 510A D6B9 AD11 CF6A
uid                  Debian Live Signing Key (2013) <debian-live@lists.debian.org>
sub   4096R/B72E3E00 2013-05-06
```

Key 2014-01-03 (1239 00F2 A9B2 6DF5)

This key was mentioned at https://debian.org/CD/verify at the end of 2014, according to the INTERNET ARCHIVE.

```
pub   4096R/A9B26DF5 2014-01-03
      Key fingerprint = 8A36 A2E8 91A5 C2A9 0DEB  7A8B 1239 00F2 A9B2 6DF5
uid                  Live Systems Project <debian-live@lists.debian.org>
sub   4096R/D0125917 2014-01-03
```

Key 2014-04-15 (4246 8F40 09EA 8AC3)

This key was mentioned at https://debian.org/CD/verify at the end of 2014, according to the INTERNET ARCHIVE.

```
pub   4096R/09EA8AC3 2014-04-15
      Key fingerprint = F41D 3034 2F35 4669 5F65  C669 4246 8F40 09EA 8AC3
uid                  Debian Testing CDs Automatic Signing Key <debian-cd@lists.debian.org>
sub   4096R/6BD05CFB 2014-04-15
```

2.4 GITHUB

2.4.1 Background

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

2.4.2 History

2008. GITHUB founded in San Francisco.[1]

2008-03-10. GITHUB parent company LOGICAL AWESOME, LLC registered in San Francisco by Chris Wanstrath.[2.4.1]

2008-05-14. First snapshot of the `https://github.com` website on the INTERNET ARCHIVE.[2.4.2]

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.[2.4.3] Also the date of a post by GITHUB user `jonathancross`[2.4.4] observing that the `0x4AEE18F83AFDEB23` key appears to be a new feature[2.4.5]:

> 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.[2.4.6]

2021-05-25. Public key `0x4AEE18F83AFDEB23` fingerprint explicitly published at GITHUB documentation website.[2.4.7]

2.4.3 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[2.4.8] 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` .[2.4.9] This particular link as well as the full key fingerprint was added to the GITHUB documentation repository in a commit dated 2021-05-25[2.4.10].

2.4.1. 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` .

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

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

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

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

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

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

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

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

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

2.5 RASPIBLITZ

2.5.1 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.[2.5.1] As of 2021-07-18, the principal maintainer appears to be CHRISTIAN "ROOTZOL" ROTZOLL[2.5.2].

2.5.2 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.[2.5.3] 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.[2.5.4]

2021-02-07. Andreas Antonopoulos posted a YouTube video identifying RASPIBLITZ as a popular Bitcoin full node software package.[2.5.5]

2021-05-18. ROOTZOL added their public key fingerprint `0x1C73060C7C176461` to the README of the RASPIBLITZ GITHUB repository.

2.5.3 Public Key Details

2.5.3.1 CHRISTIAN "ROOTZOL" ROTZOLL

ROOTZOL's PGP key[2.5.6] may be downloaded from their Keybase page.[2.5.7]. 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]
```

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

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

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

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

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

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

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

2.6 SATOSHI LABS

2.6.1 Background

SATOSHI LABS is a company that produces cryptocurrency hardware wallets called TREZOR.[2.6.1] These devices enable a user to privately manage their private keys necessary to create transactions. Publishing transactions and viewing current balances typically requires software running on a computer connected to the internet. SATOSHI LABS uses an OpenPGP key to sign these software packages published on their website https://trezor.io .

SATOSHI LABS was founded in 2013 by MAREK "SLUSH" PALATINUS, PAVOL "STICK" RUSNÁK, and ALENA VRANOVA.[2.6.2] It is based in Prague, Czech Republic.

As of 2022-01-03, the primary TREZOR program requiring verification is TREZOR SUITE.

2.6.2 History

2012-03-07. Creation date of PAVOL RUSNÁK's personal PGP key (91F3 B339 B9A0 2A3D).

2014-07-18. First snapshot of https://mytrezor.com appears on the INTERNET ARCHIVE.[2.6.3]

2017-01-11. mytrezor.com , buytrezor.com , and other domains migrated to https://trezor.io .[2.6.4]

2017-01-28. The first snapshot of https://trezor.io appears on the INTERNET ARCHIVE.[2.6.5]

2020-10-20. Creation date of the 2020 signing key (26A3 A566 62F0 E7E2).

2021-01-04. Creation date of the 2021 signing key (E21B 6950 A2EC B65C).

2021-07-14. TREZOR SUITE launched[2.6.6] in order to replace an older web wallet implementation.[2.6.7]

2.6.3 Public Key Details

2.6.3.1 PAVOL RUSNÁK

A key[2.6.8] used by a developer named PAVOL "STICK" RUSNÁK.[2.6.9] This key has been used to sign TREZOR software in the past[2.6.10] such as TREZOR BRIDGE[2.6.11] and other various GITHUB commits.

```
pub   rsa4096/0x91F3B339B9A02A3D 2012-03-07 [SC] [expires: 2022-01-16]
      Key fingerprint = 86E6 792F C27B FD47 8860  C110 91F3 B339 B9A0 2A3D
uid                   [ unknown] Pavol Rusnák <pavol@rusnak.io>
uid                   [ unknown] Pavol Rusnák <stick@gk2.sk>
uid                   [ unknown] Pavol Rusnák <prusnak@opensuse.org>
uid                   [ unknown] Pavol Rusnák <stick@satoshilabs.com>
uid                   [ unknown] [jpeg image of size 2449]
sub   rsa4096/0x22AF226D38DC1F4D 2012-03-07 [E] [expires: 2023-01-08]
      Key fingerprint = E177 6F65 0601 E596 9E7F  9E25 22AF 226D 38DC 1F4D
```

2.6.3.2 2020 Signing Key

A key[2.6.12] used to sign the software required by a PC to communicate with the TREZOR product line. Expired as of 2021-01-01.

2.6.1. Company website: https://satoshilabs.com/ .

2.6.2. See https://web.archive.org/web/20140627154535/http://satoshilabs.com/team/ .

2.6.3. See https://web.archive.org/web/20140718104157/https://mytrezor.com/ .

2.6.4. See https://web.archive.org/web/20201111170337/https://blog.trezor.io/new-trezor-io-55cf687c88d5?gi=3481ee5b4637 .

2.6.5. See https://web.archive.org/web/20170128023418/https://trezor.io/ .

2.6.6. See https://blog.trezor.io/trezor-suite-launches-8958c1d37d33 .

2.6.7. See https://github.com/trezor-graveyard .

2.6.8. Download key at https://rusnak.io/public/pgp.txt .

2.6.9. Twitter: https://twitter.com/pavolrusnak .

2.6.10. See https://github.com/trezor/trezord-go/issues/211 .

2.6.11. See https://github.com/trezor/webwallet-data/tree/master/bridge .

2.6.12. Download key at https://trezor.io/security/satoshilabs-2020-signing-key.asc .

```
pub   rsa4096/0x26A3A56662F0E7E2 2020-10-20 [SC] [expired: 2021-01-01]
      Key fingerprint = 5406 7D8B BF00 5541 81B5  AB8F 26A3 A566 62F0 E7E2
uid                   [ expired] SatoshiLabs 2020 Signing Key
```

2.6.3.3 2021 Signing Key

A key[2.6.13] used to sign the software required by a PC to communicate with the Trezor product line.

```
pub   rsa4096/0xE21B6950A2ECB65C 2021-01-04 [SC]
      Key fingerprint = EB48 3B26 B078 A4AA 1B6F  425E E21B 6950 A2EC B65C
uid                   [ unknown] SatoshiLabs 2021 Signing Key
```

2.6.13. Download key at https://trezor.io/security/satoshilabs-2021-signing-key.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