



SeedSigner Workshop

with [orange.surf](https://www.orange-surf.nl)

SeedSigner - An Introduction

What is **SeedSigner**?

1. A Device
2. A Project
3. A Founder

What is SeedSigner | **The Device**



What is SeedSigner | **The Device**

Seedsigner is a bitcoin signing device which is

- DIY
- Airgapped
- Stateless
- FOSS

What is SeedSigner | The Device | **DIY**

- Built by anyone
- Using off the shelf components
- Reduce Opportunity for a Supply Chain Attack
- Reduce risk of \$5 wrench due to leaked shipping address

What is SeedSigner | The Device | **Airgapped**

- Minimise attack surface (no connected device)

What is SeedSigner | The Device | **Stateless**

- No persistent digital copy of your private key
- Device is wiped on power off
- Seed loaded into device each time

What is SeedSigner | The Device | **FOSS**

- Free as in Freedom
- MIT License

What is SeedSigner | **The Device**

- Computer Raspberry Pi (Zero 1.3 best)
- Screen Waveshare 1.3" 240x240 pxl LCD
- Camera OV5647 with ribbon cable for Pi
- Case Many designs available
- SeedQR Paper / Metal (vulcan21.com)

What is SeedSigner | The Device | **Capability**

- Generate a seed
 - 99 dice rolls
 - Seed words
 - Take photo
- Sign a PSBT (partially signed bitcoin transaction)

What is SeedSigner | The Device | **Use Case**

1. Great as an extra key in a multisig
2. Lack of abstraction forces learning

What is SeedSigner | The Device | **Take Care**

1. Requires private key on each use
2. Vulnerable to an evil maid attack
3. Even with SeedSigner OS a Pi is a full computer with a large attack surface

What is SeedSigner | The Project

The screenshot shows the GitHub repository page for SeedSigner. At the top, the repository name 'SeedSigner / seedsigner' is displayed. Below this, navigation tabs for 'Code', 'Issues (80)', 'Pull requests (18)', 'Actions', 'Projects', 'Security', and 'Insights' are visible. The repository is public, with 36 watchers, 117 forks, and 477 stars. A 'dev' branch is selected, showing 17 branches and 19 tags. A recent merge pull request #351 is highlighted. A file tree on the left lists various files and folders, including 'docs', 'enclosures', 'src', 'tests', 'tools', and configuration files like '.coveragerc', '.gitignore', 'LICENSE.md', 'README.md', 'pytest.ini', 'requirements.txt', 'seedsigner_pubkey.gpg', and 'setup.py'. The 'About' section describes the project as a Raspberry Pi Zero signing device for Bitcoin. The 'Releases' section shows the latest release, 'The "Two More Weeks"™ Rel...', published on Feb 21. The 'Packages' section indicates no packages are published. The 'Contributors' section shows 23 contributors.

SeedSigner / seedsigner

Search Type to search

<> Code Issues 80 Pull requests 18 Actions Projects Security Insights

seedsigner Public

Watch 36 Fork 117 Star 477

dev 17 branches 19 tags

Go to file Add file Code

newtonick Merge pull request #351 from newtonick/fix_p2tr_change_bug 9c36f5c last week 972 commits

docs	Update manual_installation.md	last month
enclosures	Update open_pill_notes.md	2 months ago
src	Merge pull request #351 from newtonick/fix_p2tr_change_bug	last week
tests	Merge pull request #351 from newtonick/fix_p2tr_change_bug	last week
tools	Generalizing reusable components	2 years ago
.coveragerc	minimize default coverage report	4 months ago
.gitignore	adds test coverage	4 months ago
LICENSE.md	Create LICENSE.md	2 years ago
README.md	Merge pull request #346 from Marc-Gee/post-060	4 months ago
pytest.ini	Adds initial test suite setup	2 years ago
requirements.txt	bip85 child seeds via embit.bip85.derive_mnemonic()	6 months ago
seedsigner_pubkey.gpg	Add GPG public key	2 years ago
setup.py	bump version to 0.6.0	5 months ago

README.md

Build an offline, airgapped Bitcoin signing device

About

Use an air-gapped Raspberry Pi Zero to sign for Bitcoin transactions! (and do other cool stuff)

Readme MIT license Activity 477 stars 36 watching 117 forks Report repository

Releases 19

The "Two More Weeks"™ Rel... Latest on Feb 21

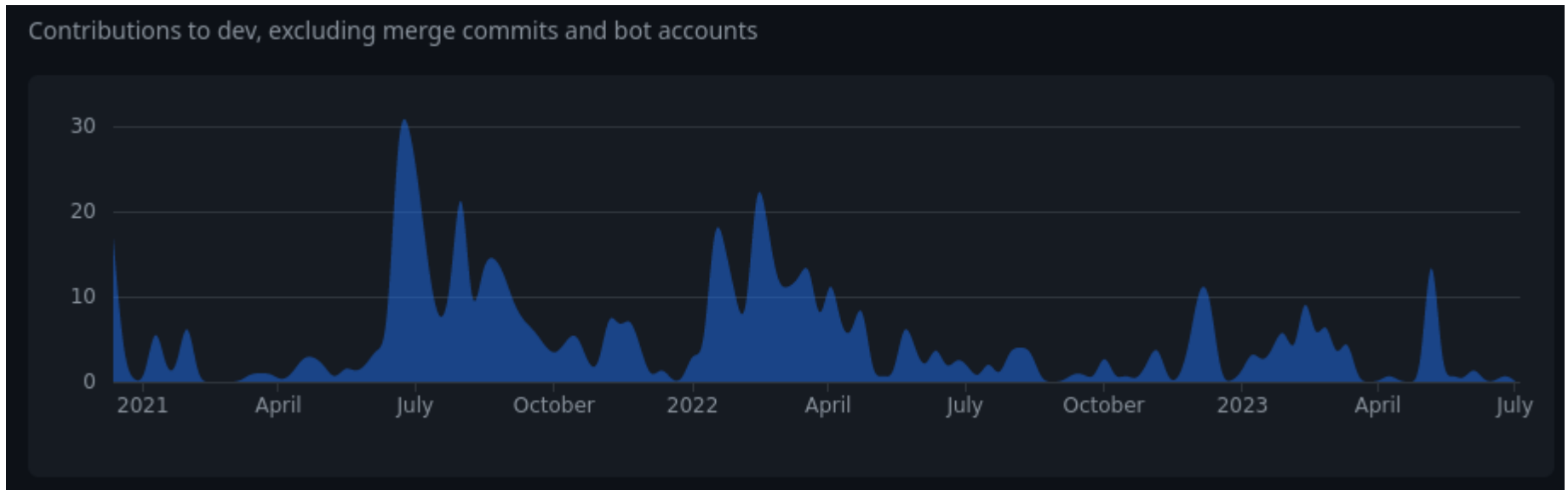
+ 18 releases

Packages

No packages published

Contributors 23

What is SeedSigner | **The Project**



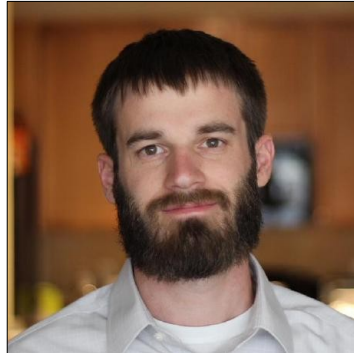
What is SeedSigner | The Project | **The Team**

*Project Founder /
Lead*



Seed
Signer

Lead Maintainer



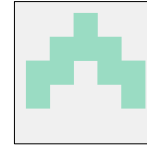
Nick
Klockenga

Lead Developer



Keith
Mukai

+ 16 More...



Marc-Gee



Desobediente
Tecnológico



Bitcoin
Precept



jase100k

How to start

How to start

- Build/Download the latest .img release
- Flash to a microSD card
- Assemble the device
- Use

Build/Download the latest .img release

github.com/SeedSigner/seedsigner/releases/

The screenshot shows the GitHub repository page for SeedSigner/seedsigner. The top navigation bar includes the repository name and a search bar. Below the navigation bar, there are tabs for Code, Issues (80), Pull requests (18), Actions, Projects, Security, and Insights. The main content area is divided into two tabs: Releases (selected) and Tags. A search bar for releases is also present. The latest release is titled "The 'Two More Weeks™' Release" and is marked as "Latest". The release date is Feb 21. The release description states: "This release has been a long time in the making... But it's been worth the wait." The "New Features:" section lists several updates:

- SeedSigner OS (custom Linux operating system)
 - Remove microSD after start-up
 - Networking/BT/swap/usb removed from kernel
 - Deployment image is ~100x smaller
 - Build from scratch with minimal commands
- Single/multisig receive/change address explorer
- BIP-85 deterministic seed derivation
- Support for p2tr (taproot) signing
- Compact SeedQR now enabled by default

Verify the release

```
gpg --fetch-keys https://keybase.io/seedsigner/pgp_keys.asc
```

```
gpg --verify seedsigner.0.6.*.sha256.sig
```

...

```
Looking for "Good signature" from ... C7EF709007260119
```

...

```
shasum -a 256 --ignore-missing --check seedsigner.0.6.*.sha256
```

...

```
Looking for "....img:ok"
```

...

Flash to a microSD card

etcher.balena.io



[More Products](#) ▾ [Resources](#) ▾ [Customers & Partners](#) ▾ [Pricing](#) [Contact](#)

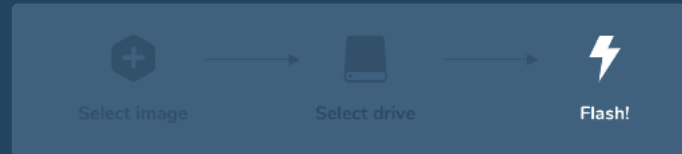
[Login](#)

[Sign Up](#)

ETCHER

Flash. Flawless.

Flash OS images to SD cards & USB drives, safely and easily.



[Download Etcher](#)

Start Playing (On Testnet)

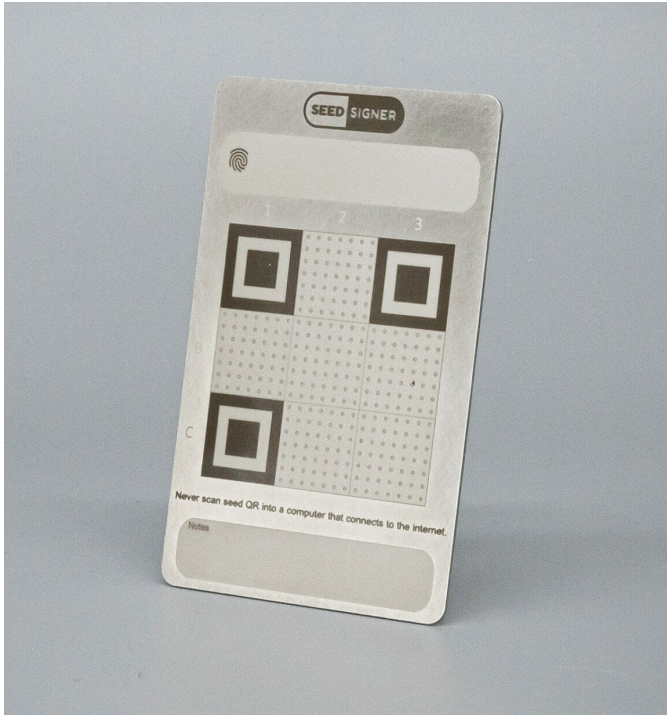


bluwallet.io

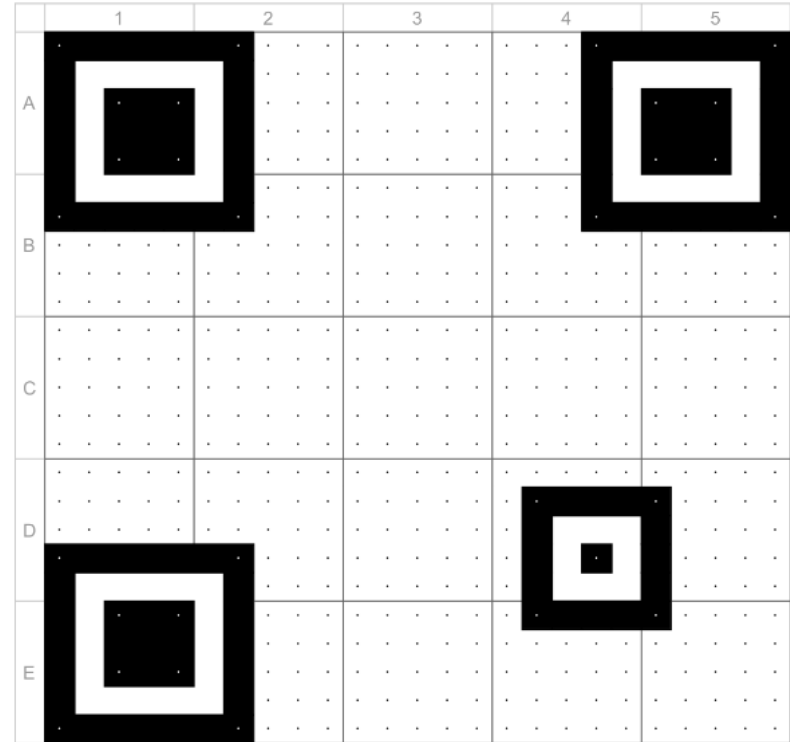


sparrowwallet.com

Seed QR




vulcan21.com/
In person purchase recommended



Seedsigner github

Get Help



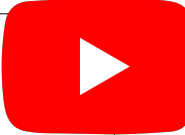
SEED SIGNER

SeedSigner Community

1 739 members, 186 online

Group Invite Link: https://t.me/joinchat/GHNuc_nhNQjLPWsS

JOIN GROUP



SEED SIGNER

Seed Signer


@seedsigner5695 645 subscribers 9 videos

More about this channel >

HOME VIDEOS PLAYLISTS COMMUNITY CHANNELS


Uploads ▶ Play all

- Open Pill Mini (w/ Faceplate) Assembly**
732 views · 4 months ago
- Create and Spend from a Single-Sig Bitcoin Wallet wit...**
4.3K views · 1 year ago
- Generate Seed Checksum Word & SeedQR Manual...**
4.7K views · 1 year ago



SeedSigner

12.7K Tweets



SEED SIGNER

Following

SeedSigner

@SeedSigner Follows you

Privately build a secure bitcoin signing device for less than most HWWs (all software/designs are FOSS). GPG: 4673 9B74 B56A D88F 14B0 882E C7EF 7090 0726 0119

seedsigner.com Joined November 2020

2,651 Following 21.6K Followers

Followed by Dax, sx6 bitcoin backup plates, and 287 others you follow



<https://tips.orange.surf>