



ZeroNet

Decentralized web platform using Bitcoin cryptography and BitTorrent network.

ABOUT ZERONET

Why?

We believe in open, free, and uncensored network and communication.

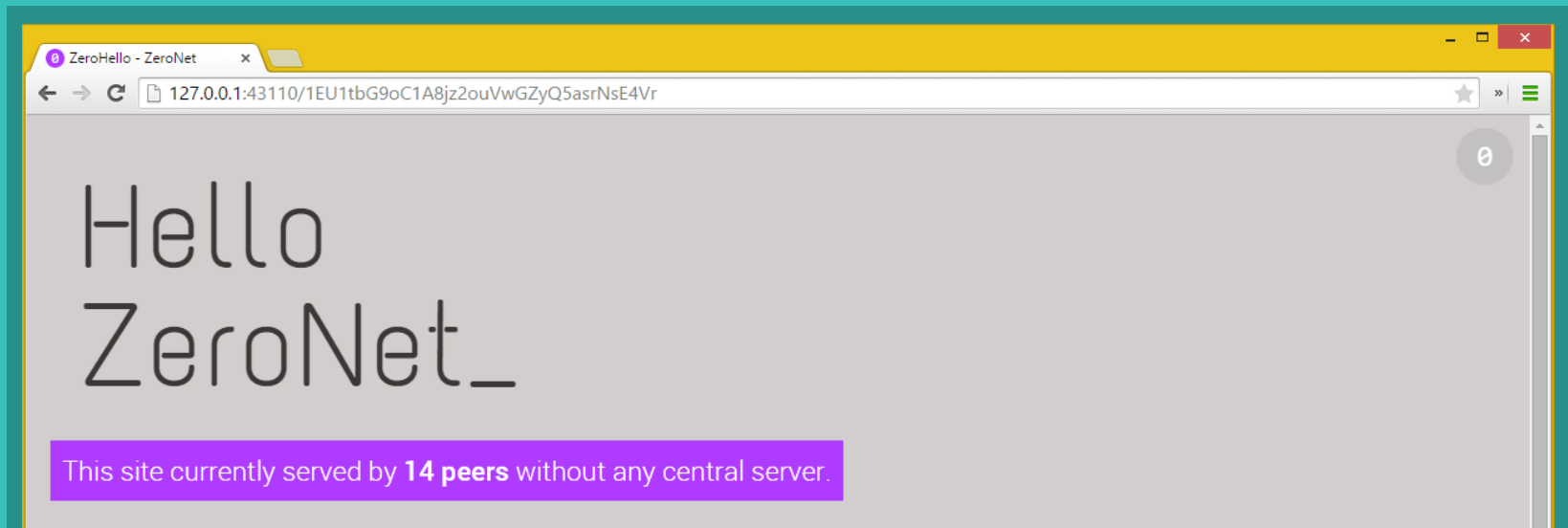
- **No hosting costs**
Sites are served by visitors.
- **Impossible to shut down**
It's nowhere because it's everywhere.
- **No single point of failure**
Site remains online so long as at least 1 peer serving it.
- **Fast and works offline**
You can access the site even if your internet is unavailable.

Current features

- **Real-time updated sites**
- Namecoin .bit domain support
- **Multi-user sites**
- Password less, Bitcoin's BIP32-based authorization
- Built-in SQL server with P2P data synchronization
- Tor network support
- Works in any browser/OS



HOW DOES IT WORK?



THE BASICS OF ASYMMETRIC CRYPTOGRAPHY

When you create a new site you get two keys:



Private key

5JNiiGspzqt8sC8FM54FMr53U9XvLVh8Waz6YYDK69G6hso9xu

- **Only you have it**
- Allows you to **sign** new content for your site.
- **No central registry**
It never leaves your computer.
- Impossible to modify your site without it.



Public key

16YsjZK9nweXyy3vNQPKT8tfjCNjEX9JM

- **This is your site address**
- Using this anyone can **verify** if the file is created by the site owner.
- Every downloaded file is verified, makes it **safe** from malicious code inserts or any modifications.

● MORE INFO ABOUT CRYPTOGRAPHY OF ZERONET

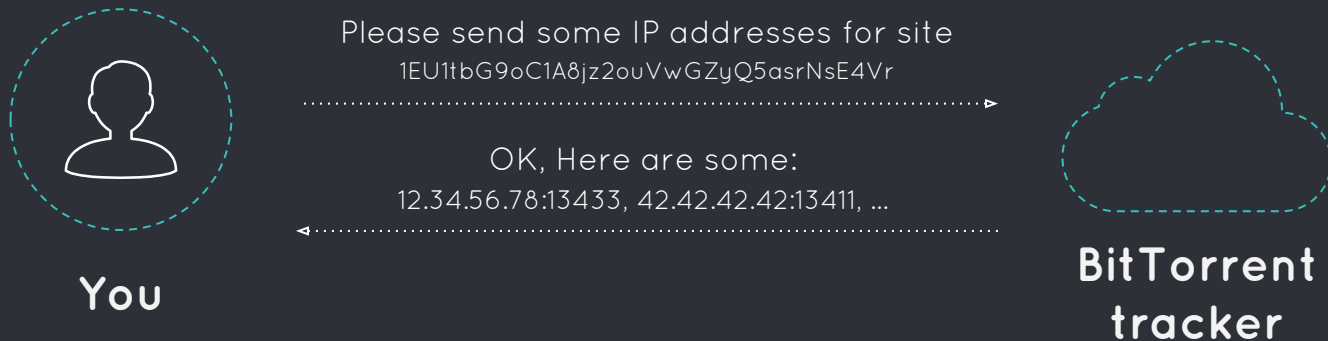
- ZeroNet uses the same elliptic curve based encryption as in your Bitcoin wallet.
- You can accept payments directly to your site address.
- Using the current fastest supercomputer, it would take around 1 billion years to "hack" a private key.

WHAT HAPPENS WHEN YOU VISIT A ZERONET SITE?



WHAT HAPPENS WHEN YOU VISIT A ZERONET SITE? (1/2)

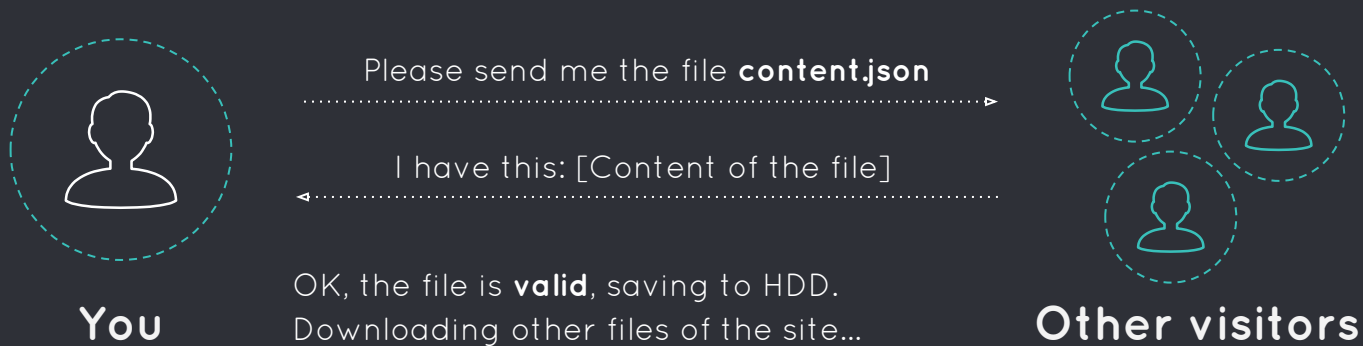
1 Gathering visitors IP addresses:



- Asks visitors IP addresses from the BitTorrent trackers.
- Also registers you as a visitor.
- Tracker-less peer exchange also supported.

WHAT HAPPENS WHEN YOU VISIT A ZERONET SITE? (2/2)

2 Downloading site's files



1. Downloads a file named **content.json**, which holds all other file-names, **hashes** and the site owner's cryptographic signature.
2. **Verifies** the downloaded **content.json** file using the site's **address** and the site owner's **signature** from the file.
3. **Downloads other files** (html, css, js,...) and verifies them using the SHA512 hash from the **content.json** file.

EXAMPLE OF GENERATED CONTENT.JSON FILE

```
{
  "address": "1Name2NXVi1RDPDgf5617UoW7xA6YrhM9F",
  "title": "ZeroName",
  "description": "Namecoin address registry",

  "files": {
    "css/all.css": {
      "sha512": "f00818c5b52013a467dc1883214b57cf6ac3dbe6da2df3f0af3cb232cd74877b",
      "size": 69952
    },
    "data/names.json": {
      "sha512": "341e4b1eb28a9aebef1ff86c981288b7531ec957552cf9a675c631d1797a48df",
      "size": 1002
    },
    "index.html": {
      "sha512": "b3fd5f2e61666874b06cc08150144015c0e88c45d3e7847ff8d4c641e789807d",
      "size": 2160
    },
    "js/all.js": {
      "sha512": "4426ca2dfacd524fb995c9f7522ca4e6f70c3e524b4bd8ca67f6416f93fca111",
      "size": 90523
    }
  },

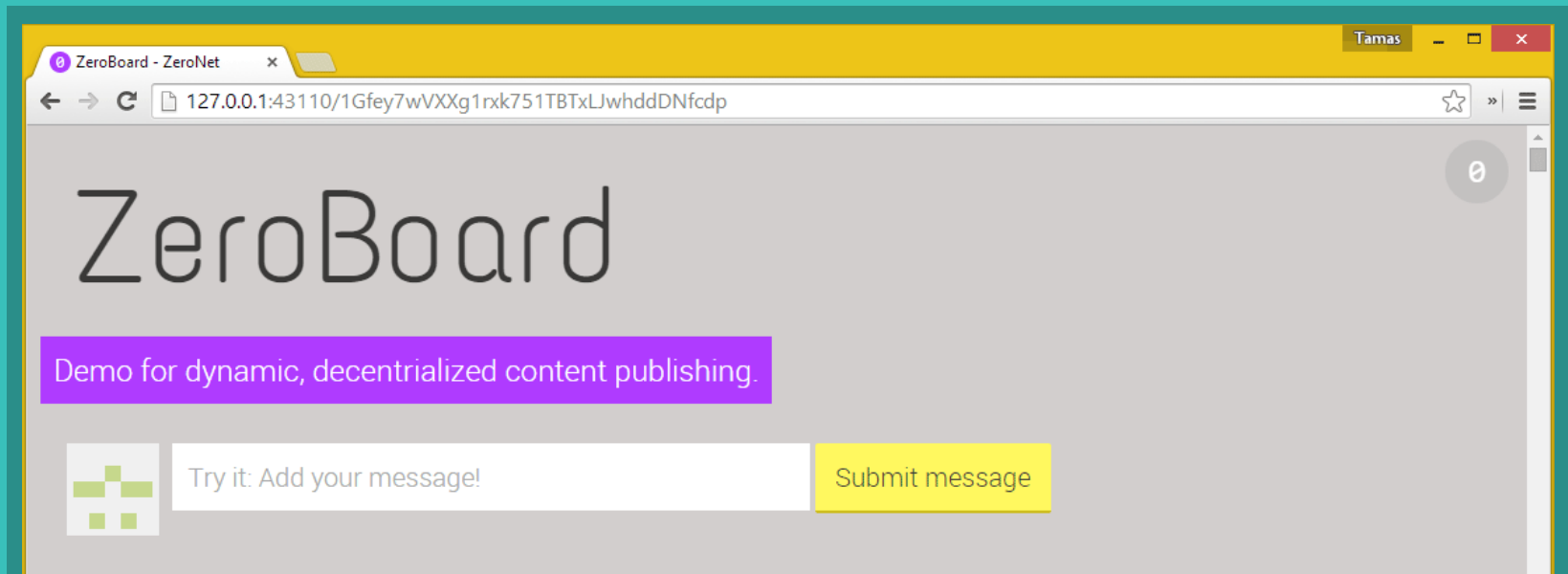
  "signers_sign": "H0KZByY9p02Iqh5UE+Nb7N5qb2cTvhULB3euvszufDnGIVeF4mswur3PyXxGXM+tJ8kZ0FzspFRI10g0yCE0tCM=",
  "signs": {
    "1Name2NXVi1RDPDgf5617UoW7xA6YrhM9F": "G6X42ZmEBf66jjy1Snx45Uee9J+Q07dLt1CLYULI17L78AFaUDVHYohEYUGxAFqKx75UpwGsPGSY1S71r/Fe3EU="
  },
  "signs_required": 1,

  "ignore": "(js|css)/(?!all.(js|css))",
  "modified": 1429483269.681872,
  "zeronet_version": "0.2.9"
}
```

MORE INFO ABOUT SITE VISITS

- You start serving sites as soon as you visit them.
- The downloads are prioritized for the fastest web experience.
- You can use the Tor network to hide your real IP address.

WHAT ABOUT SITE UPDATES?



ZERONET SITE UPDATES

The site owner signs the new content.json, then..



Site owner

Hello, here is a new **content.json**

Thanks! It's **valid** and **newer** than mine.
Please send me this file: index.html



Site visitors

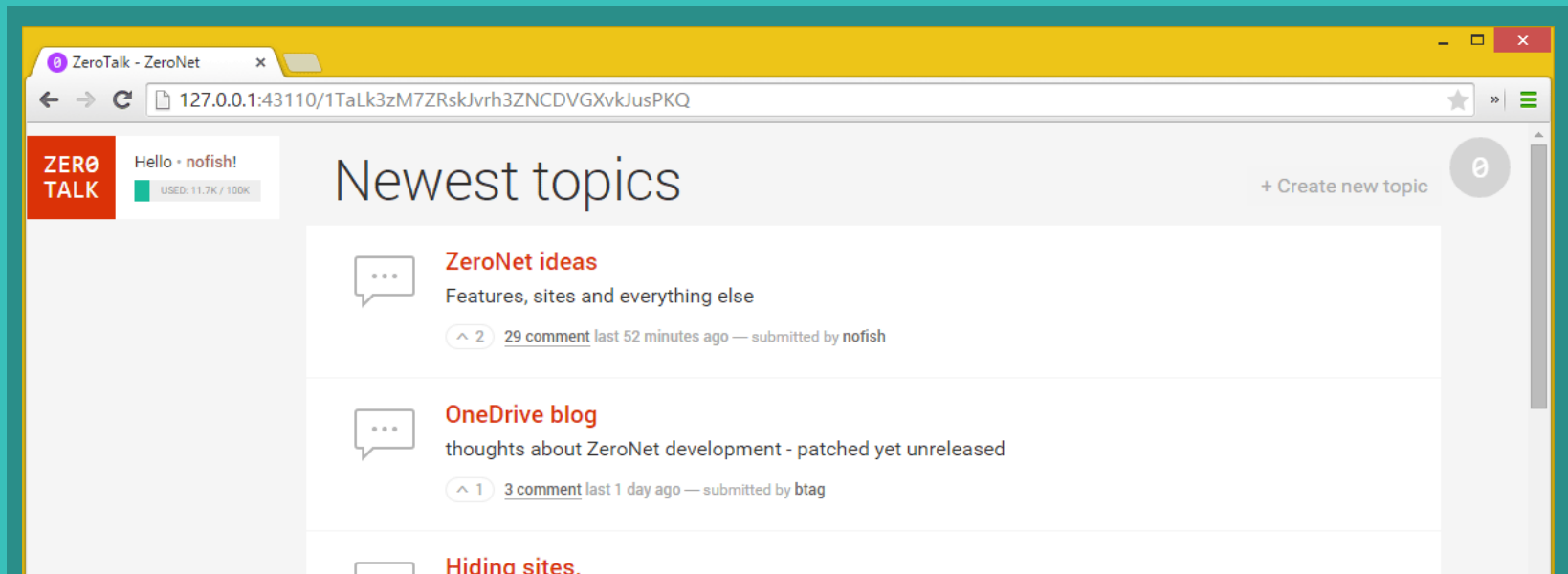
Hello, here is a
new **content.json**

1. The **site owner sends** the new content.json to a few number of visitors.
2. The **visitor checks** if its newer than his/her current file.
3. The visitor downloads the **changed files**.
4. Then he/she sends the update **to other visitors**.

MORE INFO ABOUT ZERONET SITE UPDATES

- The browser is notified immediately about the file changes using the WebSocket API. This allows real-time updated sites.
- Multi-signature sites are also possible.
- For faster and easier data access the json files can be automatically mapped to a built-in SQL database.

MULTI-USER SITES



MULTI-USER ZERONET SITES

Requesting permission from site owner:

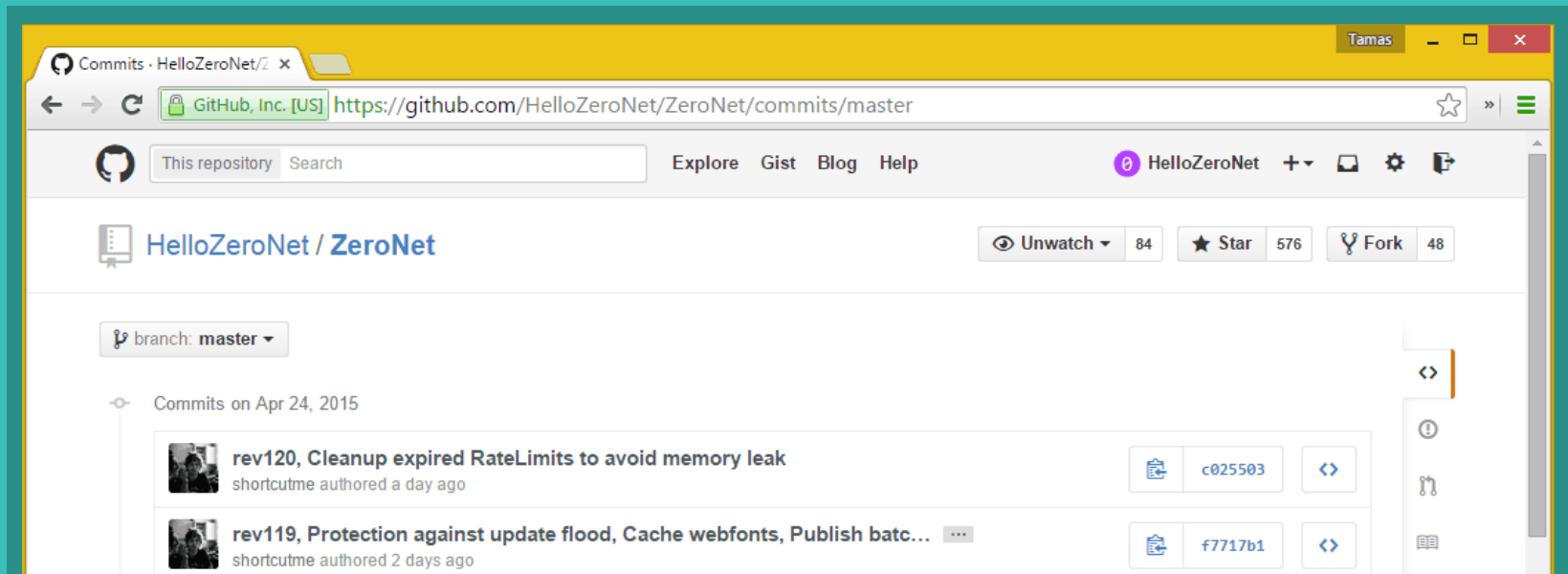


1. Sending your **auth address** to site owner.
2. The site owner **creates** a new file and set your auth address as the valid signer.
3. The site owner **publishes** the new file and the changed permissions to **visitors** of the site.

MORE INFO ABOUT MULTI-USER ZERONET SITES

- After the visitor got the permission granted he/she able to push the modifications directly to other peers without contacting the site owner again.
- The site owner is able to remove misbehaving users.
- The user files size can be limited to help avoid spamming.
- Unique auth address / private key generated for every site. (BIP32 based)

CURRENT STATUS AND PLANS

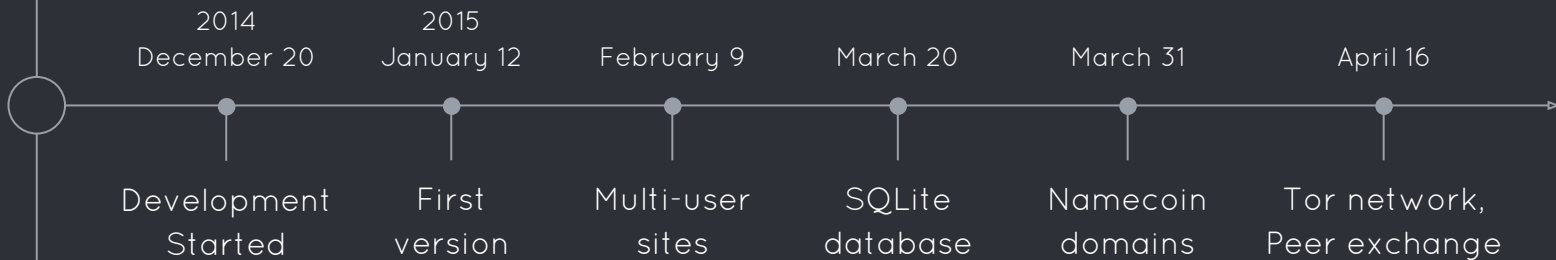


The screenshot shows a web browser window displaying the GitHub repository page for HelloZeroNet/ZeroNet. The browser's address bar shows the URL <https://github.com/HelloZeroNet/ZeroNet/commits/master>. The repository name is "HelloZeroNet / ZeroNet". The page shows the commit history for the master branch, with the following commits listed:

- rev120, Cleanup expired RateLimits to avoid memory leak** by shortcutme, authored a day ago. Commit hash: c025503.
- rev119, Protection against update flood, Cache webfonts, Publish batc...** by shortcutme, authored 2 days ago. Commit hash: f7717b1.

The page also displays repository statistics: 84 Unwatch, 576 Star, and 48 Fork. The current branch is set to master.

CURRENT STATUS



FUTURE PLANS

- Focus on content: Email-like messaging, Github alternative, News site, Marketplace, etc...
- Torrent-like, file splitting and optional files support
- Password or public key based private sites
- ~~Easier multi-user sites: Trusted authorization partners~~
- I2P and better Tor support (hidden services)

ZERONET IS...

- An alternative web distribution platform.
- Focused on speed, usability and user experience.
- Not trying to compete with 10+ year old projects. (Freenet, I2P)
- Not more anonymous than BitTorrent. (you can use Tor to hide your IP)
- Not a replacement for the current client <> server based model.

Thanks!

YOU CAN START USING ZERONET TODAY

<https://github.com/HelloZeroNet/ZeroNet>

@HelloZeroNet

/r/ZeroNet

#ZeroNet @ freenode