ZeroNet

Decentralized web platform using Bitcoin cryptography and BitTorrent network.

ABOUT ZERONET

Why?

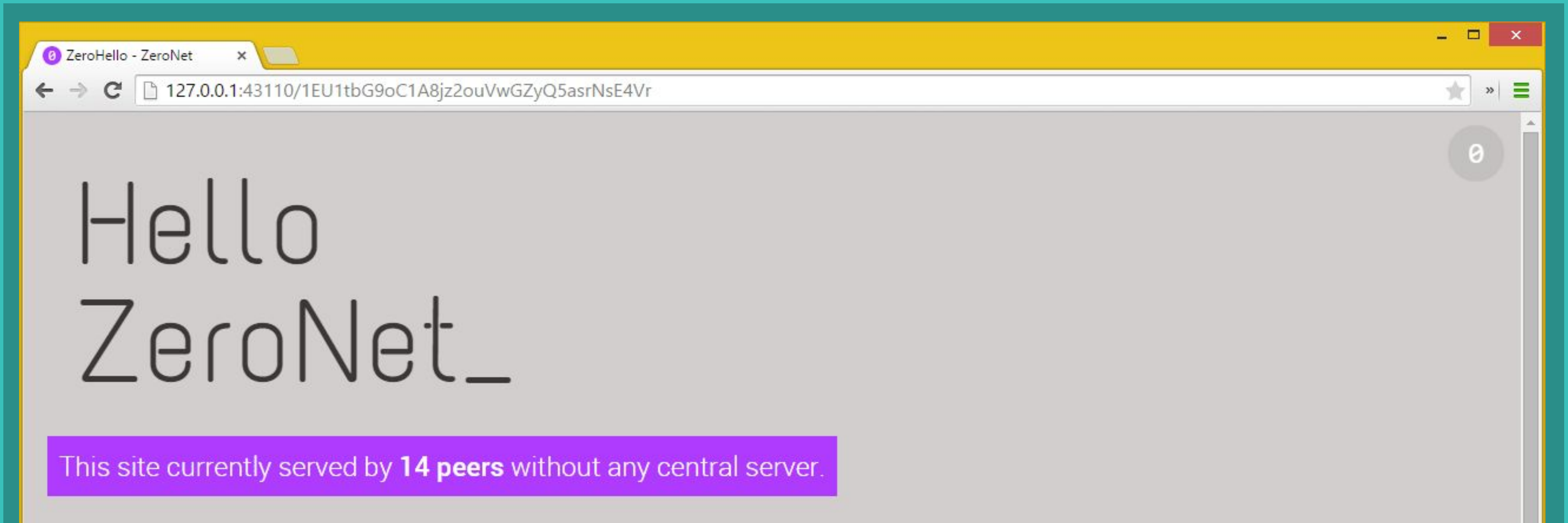
We believe in open, free, and uncensored network and communication.

- **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
- Open proxies: Try it without any download anything.

HOW DOES IT WORK?



127.0.0.1:43110/1EU1tbG9oC1A8jz2ouVwGZyQ5asrNsE4Vr

Hello
ZeroNet_

This site currently served by **14 peers** without any central server.

THE BASICS OF ASYMMETRIC CRYPTOGRAPHY

When you create a new site you get two keys:

Private key

5JNiiGspzqt8sC8FM54FMr53U9XvLVh8Waz6YYDK69gG6hso9xu

- **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

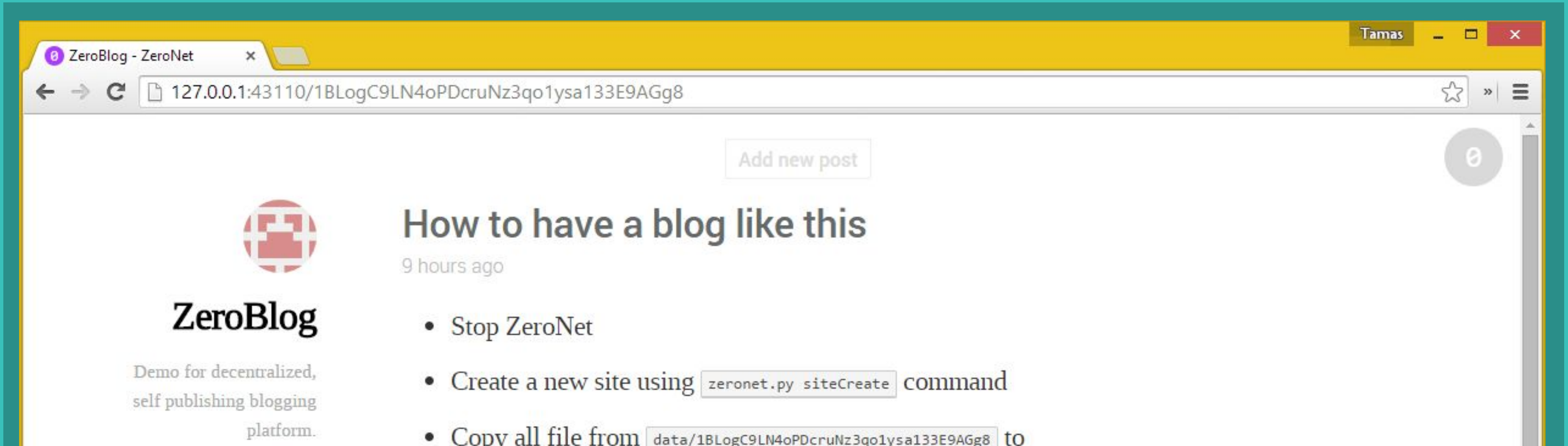
16YsjZK9nweXyy3vNQQPKT8tfjCNjEX9JM

- **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?



ZeroBlog

Demo for decentralized, self publishing blogging platform.

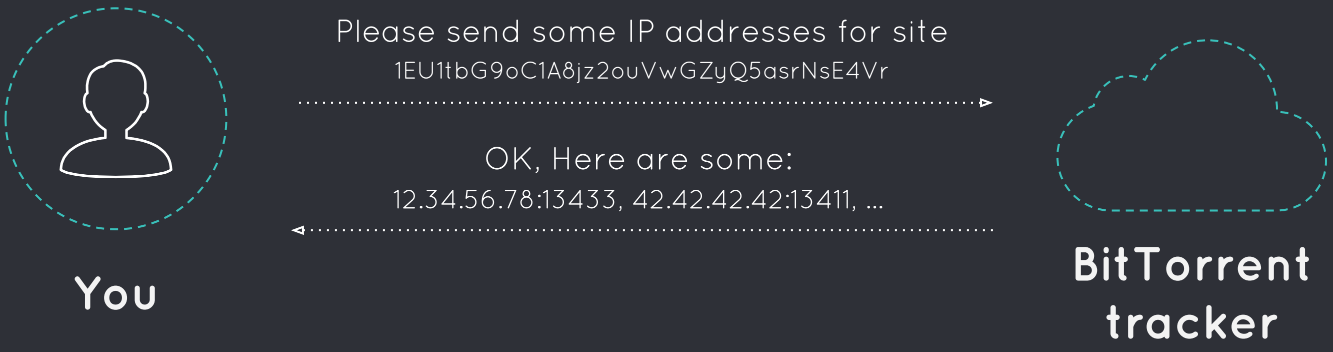
How to have a blog like this

9 hours ago

- Stop ZeroNet
- Create a new site using `zeronet.py siteCreate` command
- Copy all file from `data/1BLogC9LN4oPDcruNz3qo1ysa133E9AGg8` to

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

1 Gathering visitors IP addresses:



Please send some IP addresses for site
1EU1tbG9oC1A8jz2ouVwGZyQ5asrNsE4Vr

OK, Here are some:
12.34.56.78:13433, 42.42.42.42:13411, ...

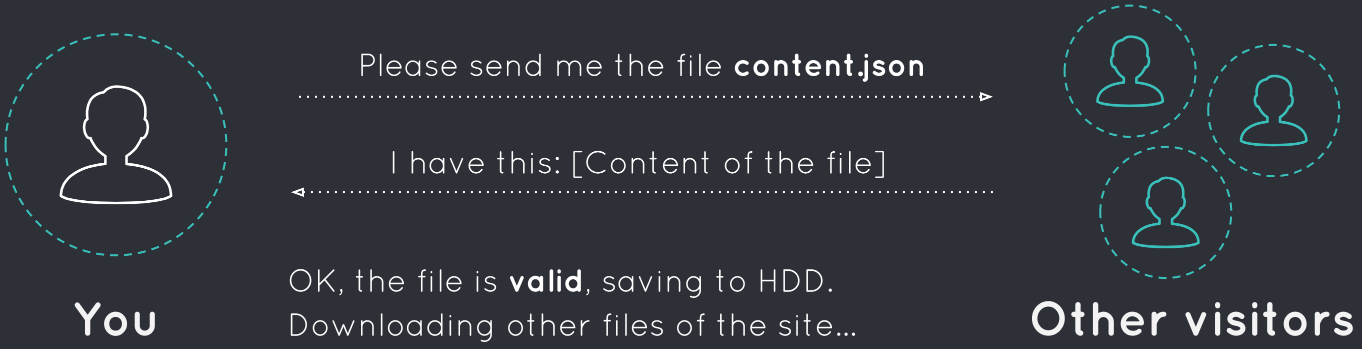
You

BitTorrent tracker

- 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



Please send me the file **content.json**

I have this: [Content of the file]

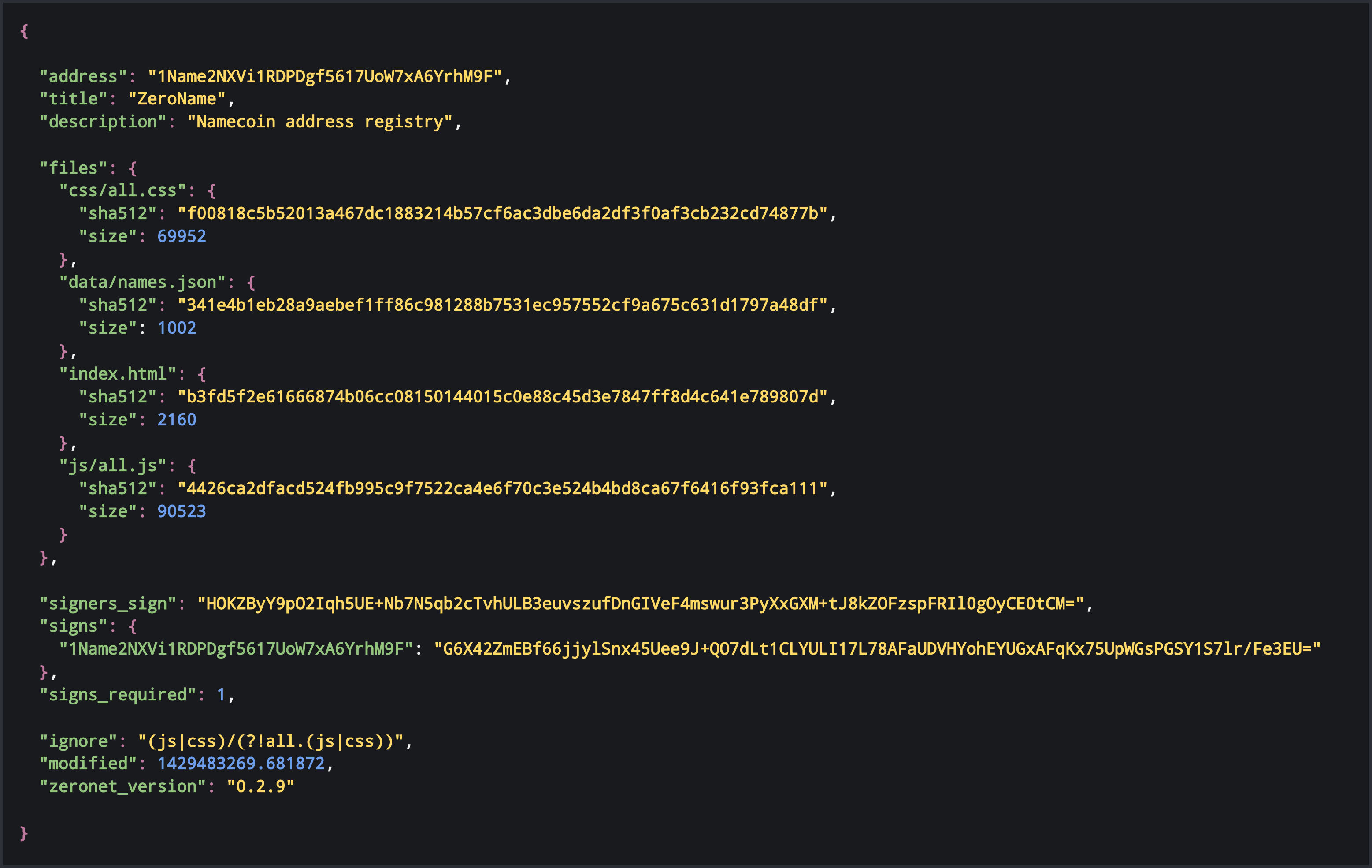
OK, the file is **valid**, saving to HDD.
Downloading other files of the site...

You

Other visitors

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

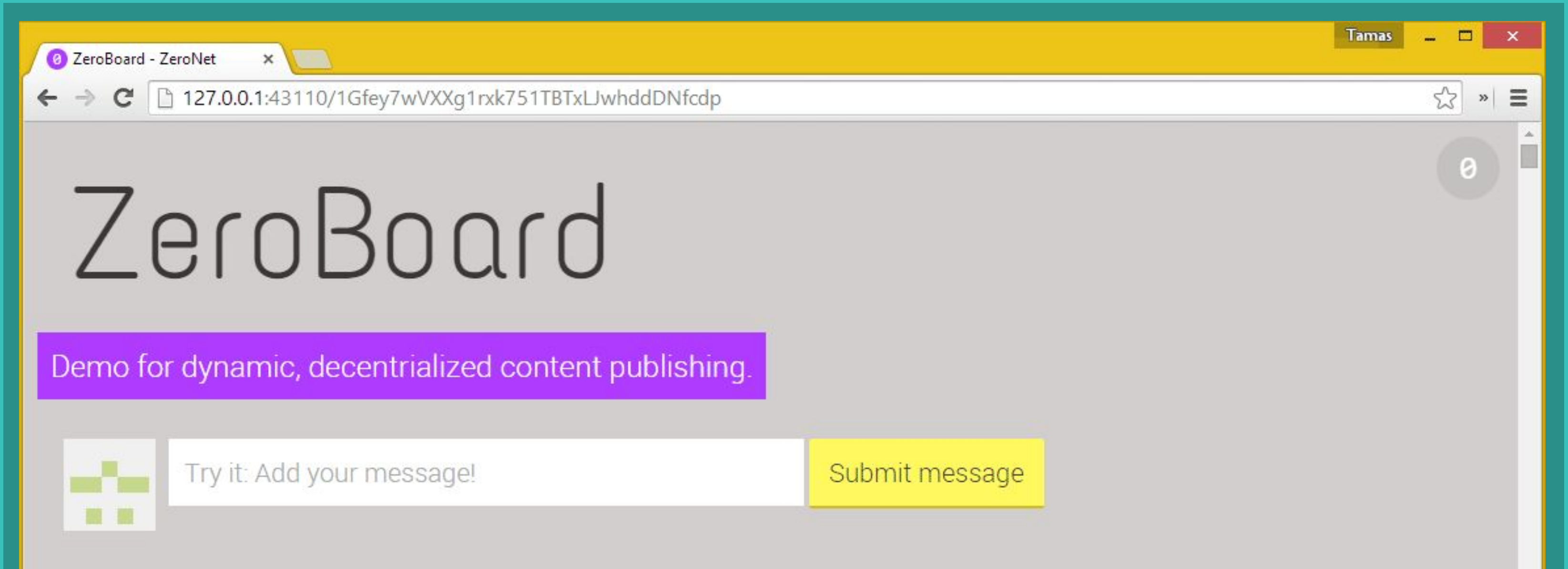


```json
{

  "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": "HOKZByY9pO2Iqh5UE+Nb7N5qb2cTvhULB3euvszufDnGIVeF4mswur3PyXxGXM+tJ8kZOFzspFRIl0gOyCE0tCM=",
  "signs": {
    "1Name2NXVi1RDPDgf5617UoW7xA6YrhM9F": "G6X42ZmEBf66jjylSnx45Uee9J+QO7dLt1CLYULI17L78AFaUDVHYohEYUGxAFqKx75UpWGsPGSY1S7lr/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.
- Optional files also supported which are only downloaded if your browser requests them.

WHAT ABOUT SITE UPDATES?



ZeroBoard

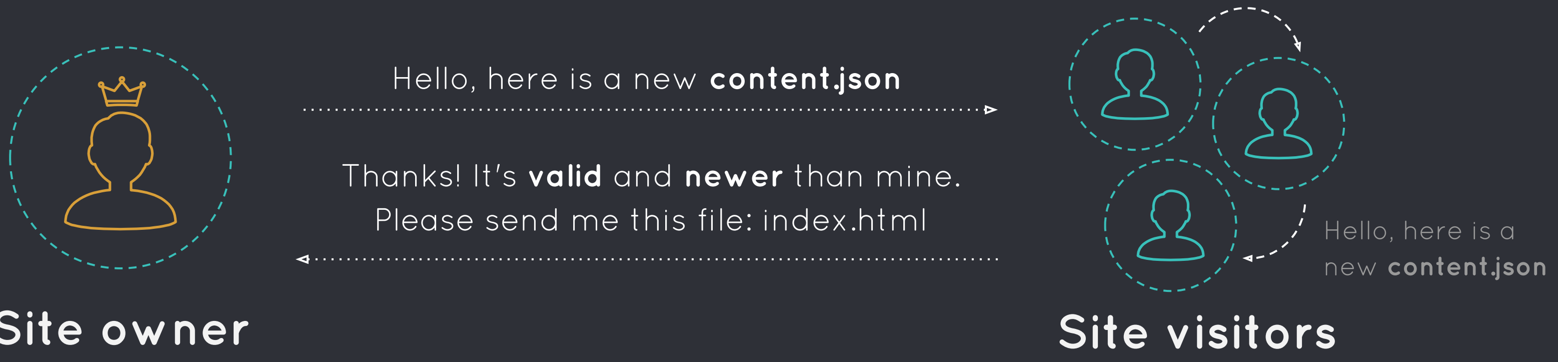
Demo for dynamic, decentrialized content publishing.

Try it: Add your message!

Submit message

ZERONET SITE UPDATES

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

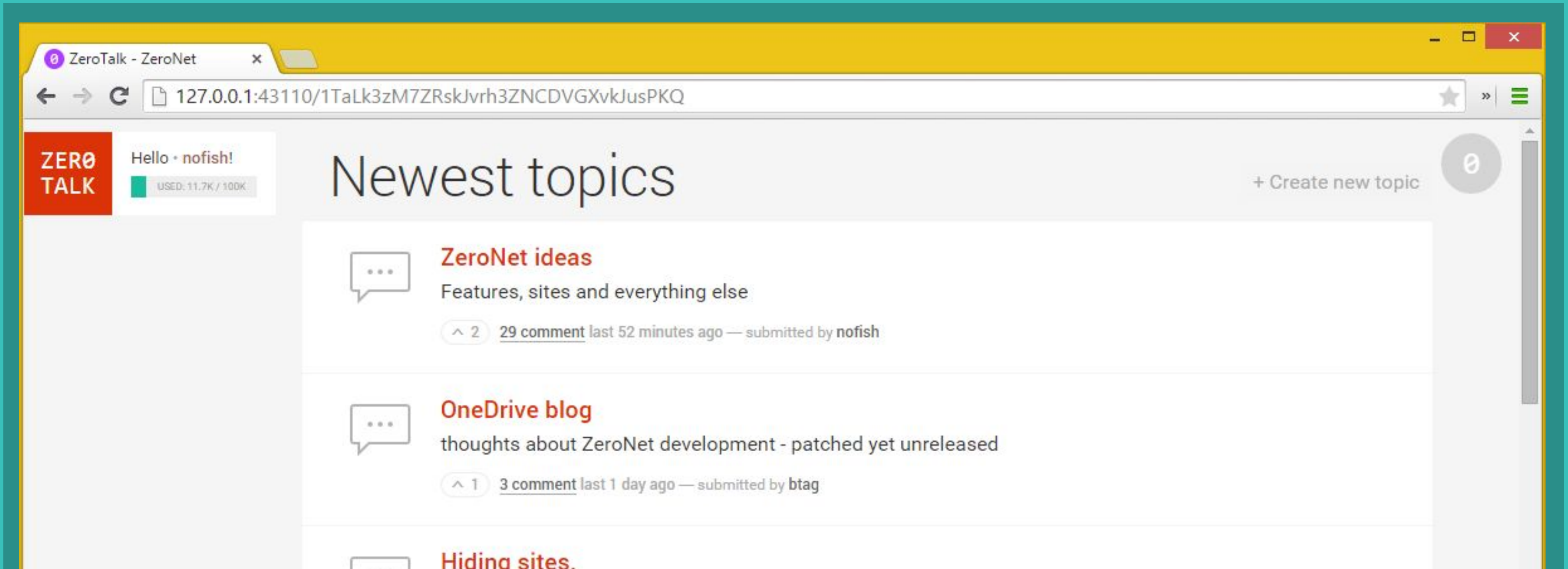

Hello, here is a new **content.json**
Thanks! It's **valid** and **newer** than mine.
Please send me this file: index.html
Hello, here is a new **content.json**
Site owner
Site visitors

1. The **site owner sends** the new content.json to a few number of visitors.
2. The **visitor checks** if it's 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



Newest topics

ZeroNet ideas

Features, sites and everything else

^ 2 29 comment last 52 minutes ago — submitted by nofish

OneDrive blog

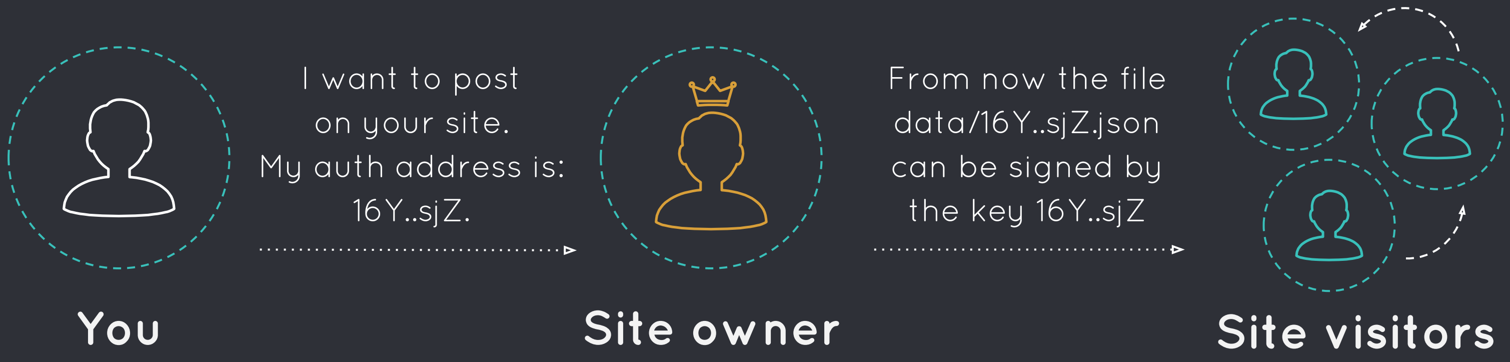
thoughts about ZeroNet development - patched yet unreleased

^ 1 3 comment last 1 day ago — submitted by btag

Hiding sites.

MULTI-USER ZERONET SITES

Requesting permission from site owner:



I want to post
on your site.
My auth address is:
16Y..sjZ.

From now the file
data/16Y..sjZ.json
can be signed by
the key 16Y..sjZ

You

Site owner

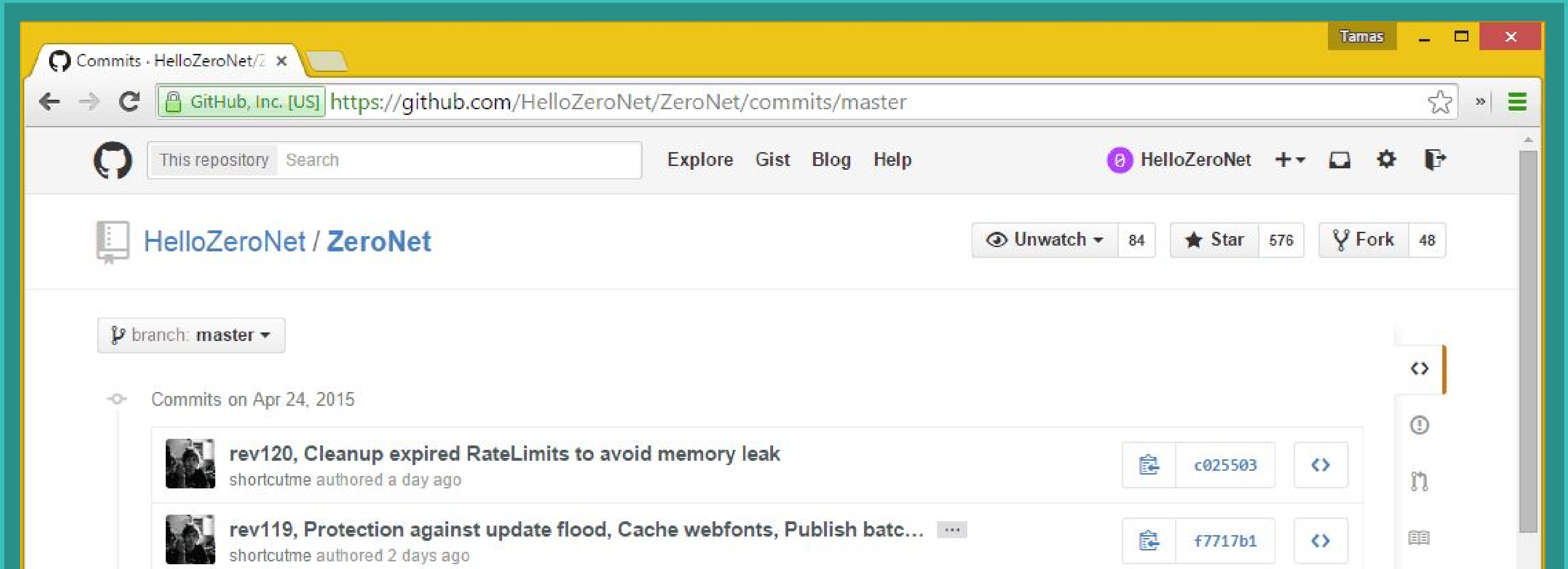
Site visitors

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

- You can skip the registration process by trusting other site's users using the authorization provider feature.
- The site owner is able to remove misbehaving users.
- The user files size can be limited to help avoid spamming.
- An unique, BIP32 based, valid Bitcoin address generated for every user of the site.

CURRENT STATUS AND PLANS

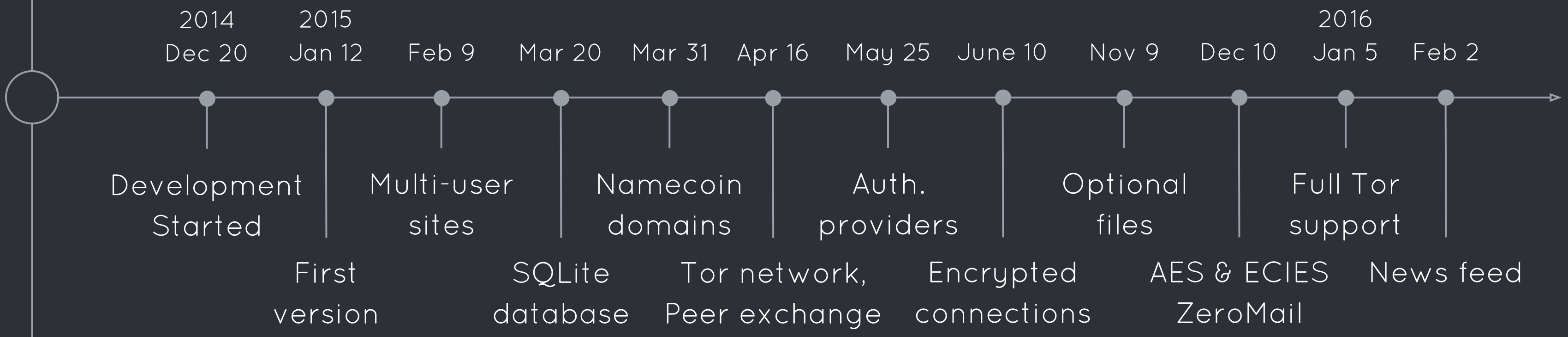


Commits on Apr 24, 2015

rev120, Cleanup expired RateLimits to avoid memory leak
shortcutme authored a day ago
c025503

rev119, Protection against update flood, Cache webfonts, Publish batc… …
shortcutme authored 2 days ago
f7717b1

CURRENT STATUS



2014 Dec 20 Development Started

2015 Jan 12 First version

Feb 9 Multi-user sites

Mar 20 SQLite database

Mar 31 Namecoin domains

Apr 16 Tor network, Peer exchange

May 25 Auth. providers

June 10 Encrypted connections

Nov 9 Optional files

Dec 10 AES & ECIES ZeroMail

2016 Jan 5 Full Tor support

Feb 2 News feed

FUTURE PLANS

- Focus on content: Social network, Github alternative, News site, Marketplace, etc...
- Torrent-like file splitting
- Password or public key based private sites
- I2P networks support

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.

OTHER BENEFITS OF ZERONET

1. 100% transparent sites: Anyone able to audit the full working mechanism.
2. 1 click site cloning: Create your own copy of any site.
3. No backend code: Query and execute SQL commands directly from javascript with zero network latency.
4. Instant CDN: Your content is distributed around the world.
5. Zero discrimination: Same, zero cost infrastructure and opportunity for anyone around the world.
6. Zero trust: Impossible to modify your site without the private key.

Thanks!

YOU CAN START USING ZERONET TODAY

http://zeronet.io

@HelloZeroNet

/r/ZeroNet

#ZeroNet @ freenode

Presentation template by SlidesCarnival