



ZeroNet

Un web décentralisée
construit sur la cryptographie
Bitcoin et le réseau BitTorrent.

Pourquoi ?

Les réseaux et communications devraient être non censurées, ouvertes et gratuites.

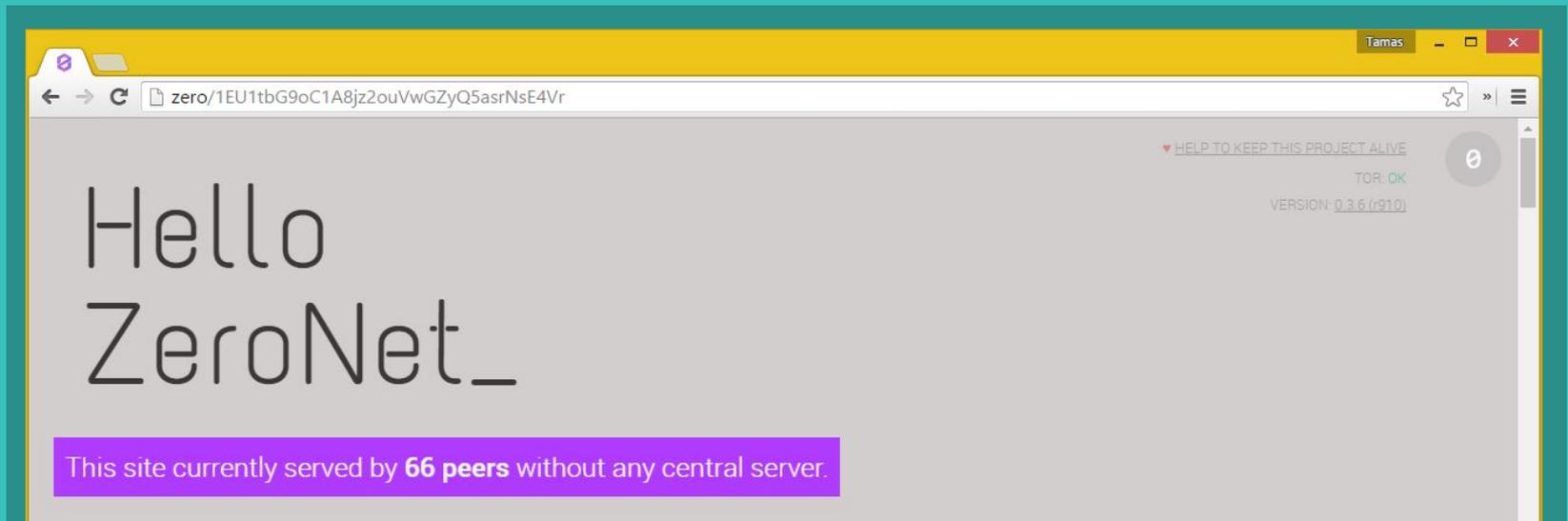
- **Pas de frais d'hébergement**
Les sites sont servis par les visiteurs.
- **Impossible à arrêter**
Les sites ne sont nulle part parce qu'ils sont partout.
- **Pas de single point of failure**
Les sites restent en ligne à partir du moment où au moins 1 pair le sert.
- **Hors-ligne.**
Vous pouvez accéder aux sites même si votre connexion internet n'est pas disponible.

Functionalités actuelles

- **Site web mis à jour en temps réel.**
- Support des domaines en .bit grâce à Namecoin.
- **Sites multi-utilisateurs**
- Pas besoin de mots de passe (authentication via BIP32).
- Base de données SQL embarquée, avec des données qui synchronisent en P2P.
- Support du réseau Tor.
- Fonctionne sous tous les OS / navigateurs
- Proxies: Essayez sans installer quoi que ce soit.



Comment ça marche ?



LES BASES DE LA CRYPTOGRAPHIE ASYMÉTRIQUE

Lors de la création d'un site, deux clés sont créées



Clé privée

5JNiiGspzqt8sC8FM54FMr53U9XvLVh8Waz6YYDK69gG6hso9xu

- **Vous en êtes le seul possesseur**
- Vous permet de **signer** les nouveaux contenus de votre site.
- **Pas de registre central**
Cette clé reste sur votre ordinateur
- Impossible de modifier votre site sans.



Clé publique

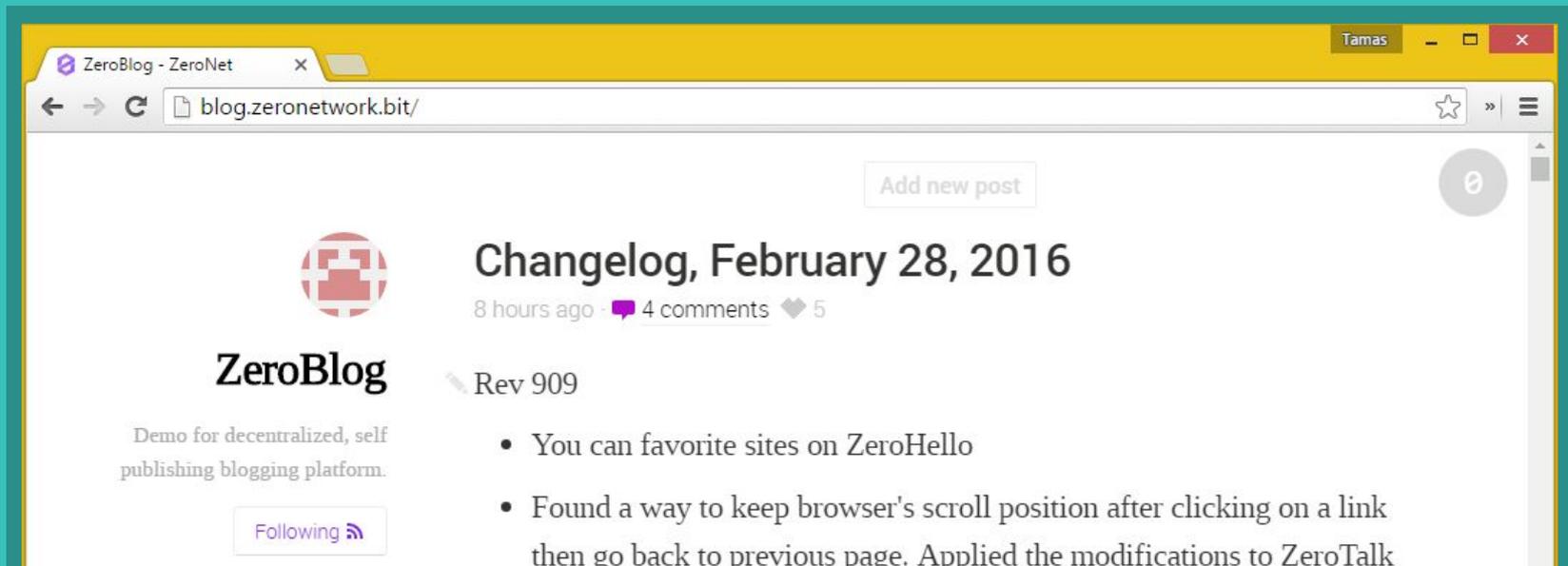
16YsjZK9nweXyy3vNQQPKT8tfjCNjEX9JM

- **Il s'agit de l'adresse de votre site.**
- En l'utilisant, tout le monde peut **valider** que les fichiers services ont été créés par le propriétaire du site.
- Chaque fichier téléchargé est vérifié, ce qui permet de se **protéger** des attaques de noeuds malicieux.

● PLUS D'INFORMATIONS SUR LA CRYPTOGRAPHIE DE ZERONET

- ZeroNet utilise la même cryptographie elliptique qui est utilisée dans vos portefeuilles Bitcoin.
- Vous pouvez accepter des paiements directement en utilisant l'adresse de votre site.
- En utilisant l'ordinateur le plus rapide actuellement, cela prendrait autour d'un millier d'années pour "hacker" une clé privée.

QUE SE PASSE T-IL LORS D'UNE VISITE D'UN SITE ZERONET ?



The screenshot shows a web browser window with the address bar displaying 'blog.zeronetwork.bit/'. The page content includes a header with 'Add new post' and a profile section for 'ZeroBlog' with a red and white grid logo. Below the profile, there is a post titled 'Changelog, February 28, 2016' with a timestamp of '8 hours ago', '4 comments', and '5' likes. The post content starts with 'Rev 909' and lists two bullet points: 'You can favorite sites on ZeroHello' and 'Found a way to keep browser's scroll position after clicking on a link then go back to previous page. Applied the modifications to ZeroTalk'.

ZeroBlog - ZeroNet x

blog.zeronetwork.bit/

Add new post

 **ZeroBlog**

Demo for decentralized, self publishing blogging platform.

Following 

Changelog, February 28, 2016

8 hours ago · 4 comments · 5

Rev 909

- You can favorite sites on ZeroHello
- Found a way to keep browser's scroll position after clicking on a link then go back to previous page. Applied the modifications to ZeroTalk

QUE SE PASSE T-IL LORS D'UNE VISITE ? (1/2)

1 Récupération de l'adresse IP des visiteurs:



Vous

Envoyez moi l'adresse IP pour le site
1EU1tbG9oC1A8jz2ouVwGZyQ5asrNsE4Vr

OK, en voila quelques unes:
12.34.56.78:13433, 42.42.42.42:13411, ...



**Tracker
BitTorrent**

- Demande l'adresse des visiteurs au tracker BitTorrent.
- Vous enregistre comme visiteur.
- L'échange pair à pair sans tracker est aussi supporté.

QUE SE PASSE T-IL LORS D'UNE VISITE ? (2/2)

2 Téléchargement des fichiers du site



Vous

Envoyez moi le fichier **content.json**

J'ai ça: [Contenu du fichier]

OK, le fichier est valide, sauvegarde
le sur le disque.
Téléchargement des autres fichiers
du site...



**Les autres
visiteurs**

1. Télécharge un fichier nommé **content.json**, qui contient l'ensemble des autres noms de fichiers, leurs **hashs** et la signature du propriétaire du site.
2. **Vérifie** le fichier content.json en utilisant l'adresse du site et la signature du propriétaire du site.
3. **Télécharge les autres fichiers** (html, css, js,...) et les vérifie en utilisant le SHA512 du fichier content.json.

EXEMPLE DE FICHER CONTENT.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
    }
  },

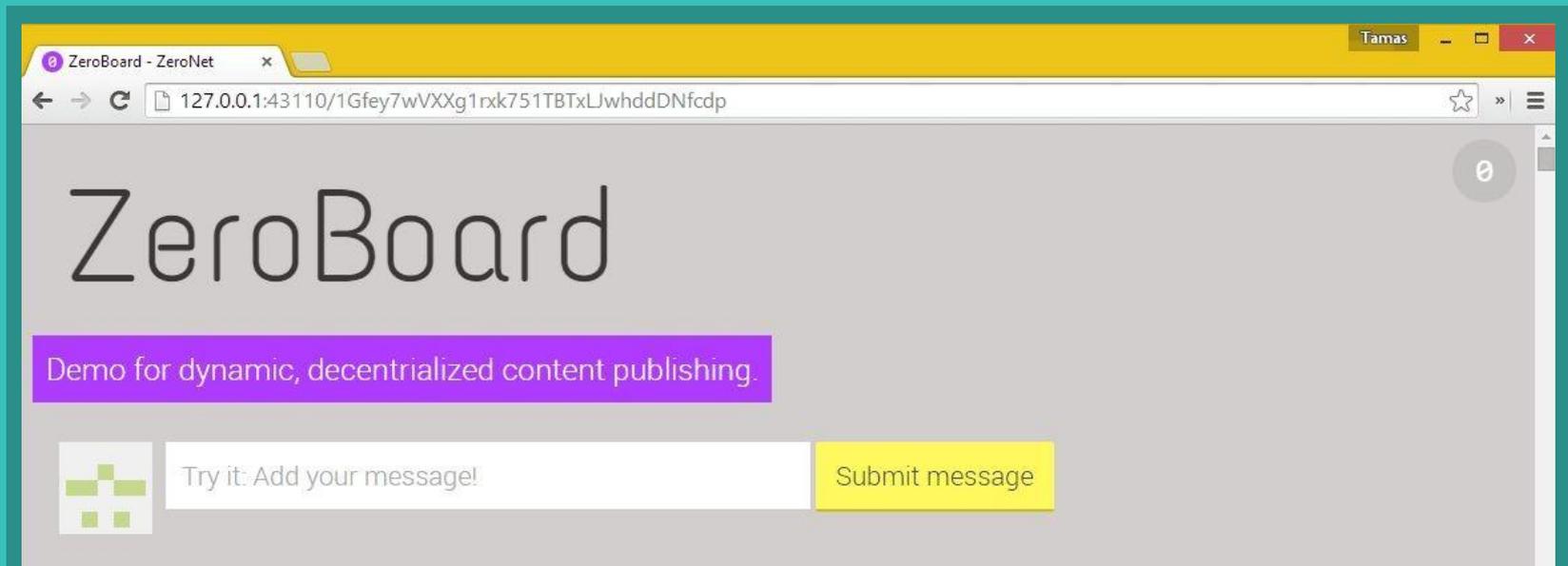
  "signers_sign": "H0KZByY9p02Iqh5UE+Nb7N5qb2cTvhlULB3euvszufDnGIVeF4mswur3PyXxGXM+tJ8kZ0FzspFRI10g0yCE0tCM=",
  "signs": {
    "1Name2NXVi1RDPDgf5617UoW7xA6YrhM9F": "G6X42ZmEBf66jjy1Snx45Uee9J+Q07dLt1CLYULI17L78AFaUDVHYohEYUGxAFqKx75UpwGsPGSY1S71r/Fe3EU="
  },
  "signs_required": 1,

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

● PLUS D'INFORMATION SUR LES VISITES DE SITES

- Vous commencez à servir les sites dès que vous y accédez
- Les téléchargements sont priorisés pour une expérience web plus fluide
- Vous pouvez utiliser le réseau Tor pour cacher votre réelle adresse IP.
- Il est aussi possible d'avoir des fichiers optionnels, téléchargés uniquement si votre navigateur en fait la requete.

ET POUR LA MISE A JOUR ?



MISE A JOUR DES SITES ZERONET

Le propriétaire du site signe le nouveau fichier **content.json**, puis...

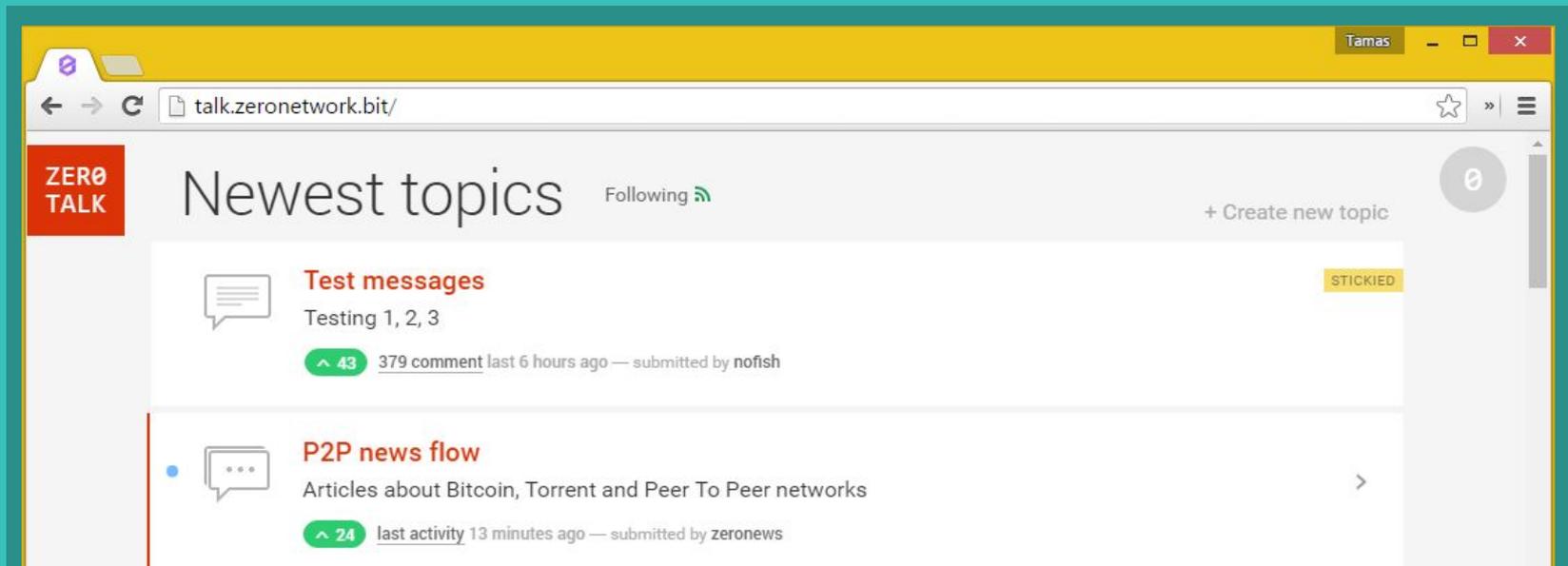


1. Le **propriétaire envoie** le nouveau content.json à un petit nombre de visiteurs.
2. Le **visiteur vérifie** si c'est plus récent que sa version courante.
3. Le visiteur télécharge les **fichiers modifiés**.
4. Puis envoi les mises à jour **aux autres visiteurs**.

● PLUS D'INFOS SUR LA MISE A JOUR DES SITES ZERONET

- Le navigateur est notifié directement à propos du changement de fichier grâce à une connection WebSocket.
Ce qui permet des mises à jour en temps réel.
- Il est possible d'avoir des sites avec plusieurs signatures.
- Pour un accès plus rapide et facile, les fichiers json peuvent être directement liés à une base de données SQL locale.

SITES MULTI-UTILISATEURS



SITES ZERONET MULTI-UTILISATEURS

Demande d'une permission au propriétaire

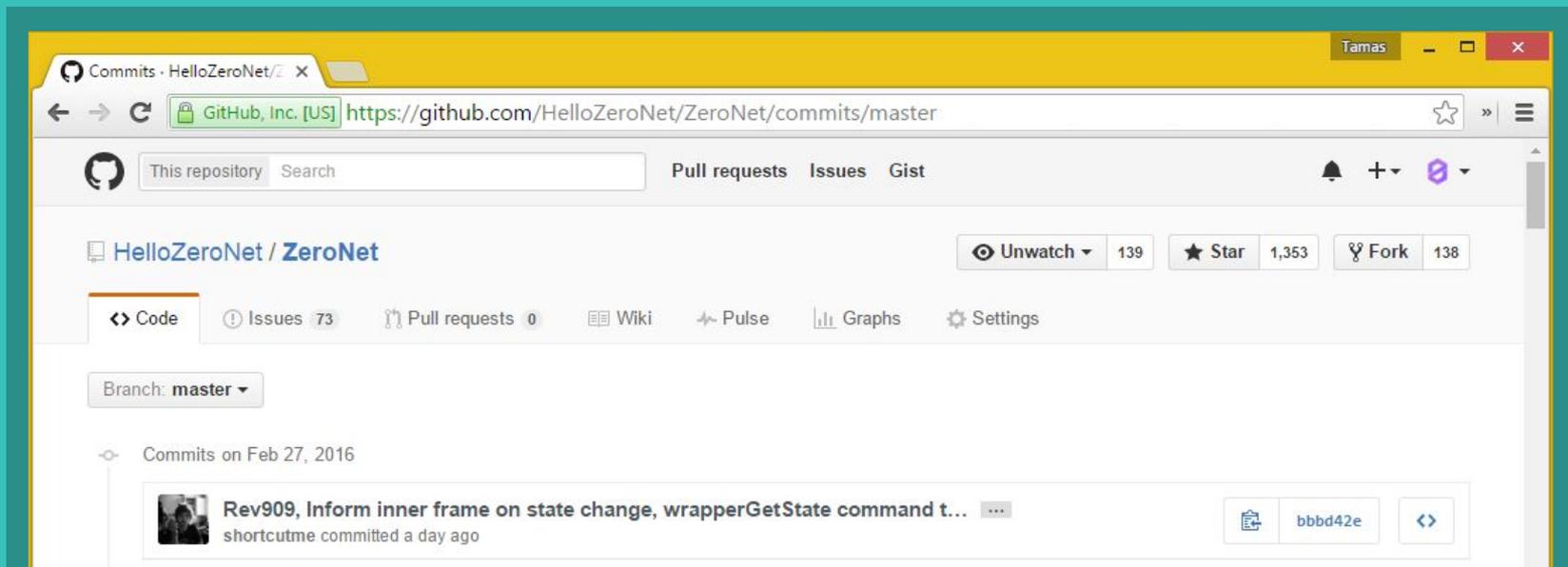


1. Envoie de votre **identitié** au propriétaire.
2. Le propriétaire créé un nouveau fichier et **renseigne** votre identité comme un signeur **valide**.
3. Le propriétaire **publie** le nouveau fichier et les changements de permissions aux **visiteurs** du site.

● PLUS D'INFOS SUR LES SITES MULTI-UTILISATEURS

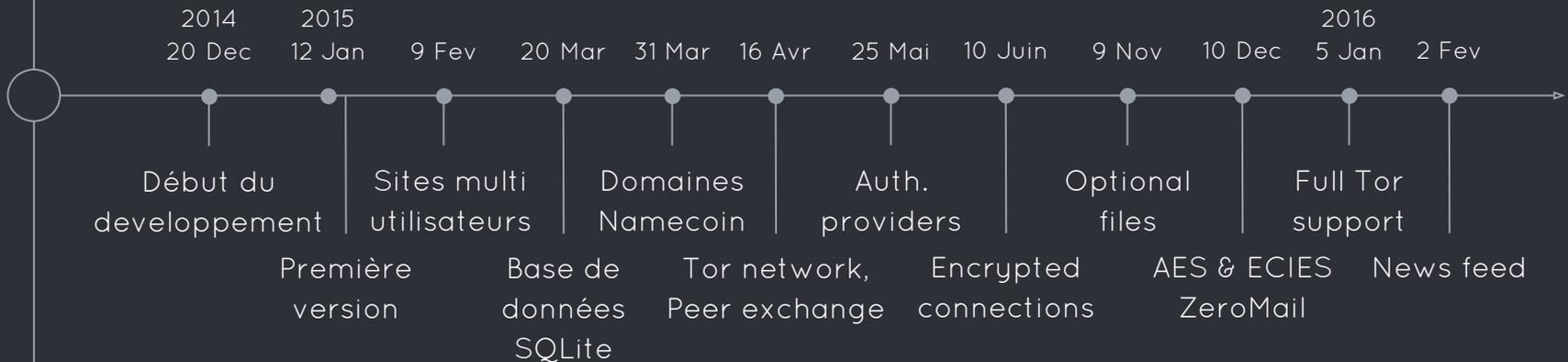
- Vous pouvez éviter l'étape d'enregistrement en faisant confiance aux autres utilisateurs du site, en utilisant la fonction de *provideur* d'identité.
- Le propriétaire est capable de supprimer les utilisateurs malicieux.
- La taille des fichiers utilisateurs peut être limitée pour éviter le spam.
- Une adresse unique (basée sur BIP32), qui est aussi une adresse Bitcoin valide est générée pour chaque utilisateur du site

ÉTAT ACTUEL ET PLANS FUTURS



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 features navigation links for "Code", "Issues 73", "Pull requests 0", "Wiki", "Pulse", "Graphs", and "Settings". The current branch is "master". A commit from February 27, 2016, is visible, titled "Rev909, Inform inner frame on state change, wrapperGetState command t..." by user "shortcutme". The commit hash is "bbbd42e". The repository has 139 watchers, 1,353 stars, and 138 forks.

ÉTAT ACTUEL



PLANS FUTURS

- Se concentrer sur le contenu: Réseaux sociaux, Alternative à Github, Site de news, Marketplace, etc.
- Séparation des gros fichiers, comme Torrent
- Faire des sites basés sur des clés publiques ou des mots de passe.
- Support du réseau I2P

ZERONET EST...

- Une manière de distribuer le Web de manière alternative.
- Concentré sur la rapidité, l'usabilité et l'expérience utilisateur.
- N'essaye pas d'être en compétition avec des projets vieux de plus de 10 ans (Freenet, I2P)
- Pas plus anonyme que le réseau BitTorrent (vous pouvez utiliser Tor pour cacher votre IP)
- Pas un remplacement au modèle actuel client <> serveur.

● BENEFICES DE ZERONET

1. Sites 100% ouverts: N'importe qui peut auditer le site et son fonctionnement.
2. Il est très facile de cloner des sites: Créez votre propre version de n'importe quel site.
3. Pas de backend: Exécutez directement vos commandes SQL depuis JavaScript, sans aucune latence réseau.
4. CDN: Votre contenu est distribué dans le monde entier.
5. Pas de discrimination: L'infrastructure ne coûte rien, pour tout le monde !
6. Confiance: il est impossible de modifier votre site sans la clé privée associée.

Merci!

**VOUS POUVEZ UTILISER
ZERONET DES MAINTENANT !**

<https://zeronet.io>

@HelloZeroNet

/r/ZeroNet

#ZeroNet @ freenode