ZeroNet

Plataforma web descentralizada
Usando la criptografía Bitcoin
Y la red BitTorrent.

ACERCA DE ZERONET

¿Por que?

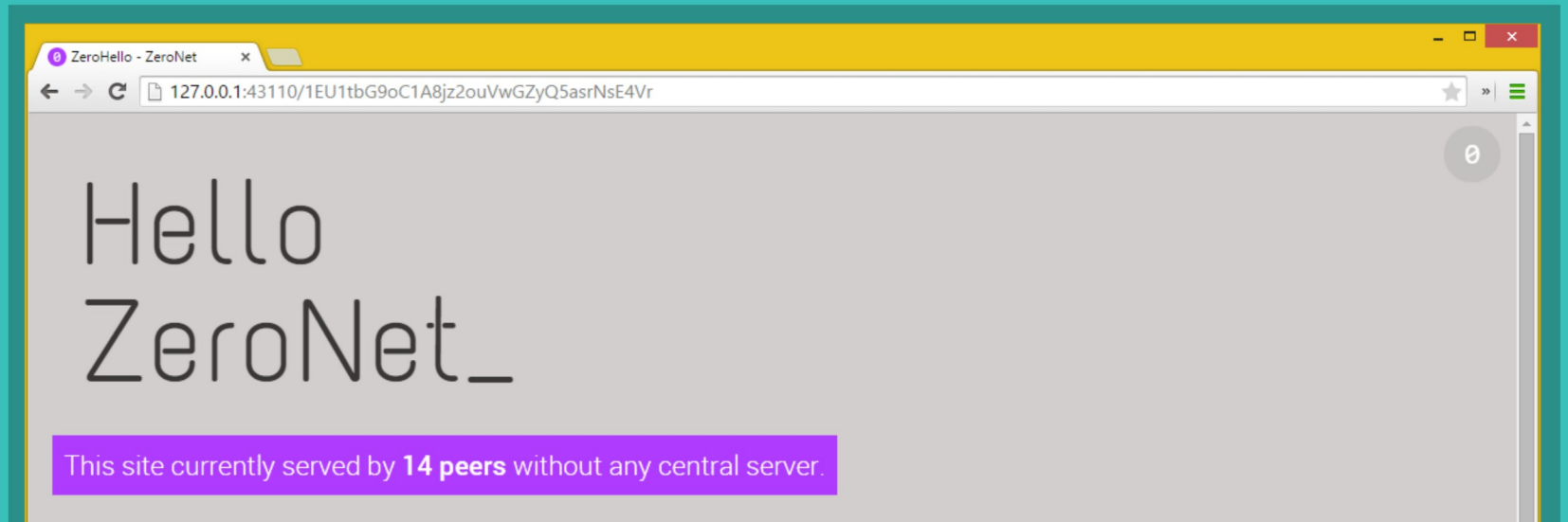
Creemos en redes de comunicación, abiertas, libres y sin censura.

- **Sin costes de alojamiento**
  Los sitios son servidos por los visitantes.
- **Imposible de cerrar**
  No está en ningún lugar porque está en todas partes.
- **Ningún punto de falla**
  El sitio se mantiene en linea mientras al menos un par siembre este.
- **Rápido y funciona fuera de linea**
  Puedes acceder al sitio incluso si tu Internet no esta disponible.

Características Actuales

- **Sitios** actualizados en **tiempo real.**
- Soporte de **dominios .bit** Namecoin.
- Sitios **multi-usuarios.**
- **Sin contraseña**, autorización basada en el sistema **BIP32.**
- **Servidor SQL** integrado con sincronización de datos **P2P.**
- Soporte de red **Tor.**
- Funciona en cualquier **explorador** o **sistema operativo.**

¿COMO FUNCIONA?



FUNDAMENTOS DE LA CRIPTOGRAFÍA ASIMÉTRICA

Cuando creas un nuevo sitio obtienes dos claves:

Llave Privada

5JNiiGspzqt8sC8FM54FMr53U9XvLVh8Waz6YYDK69gG6hso9xu

- Solo tu la tienes
- Te permite **firmar** nuevo contenido para tu sitio.
- Ningún registro central nunca sale de su computadora.
- Imposible modificar su sitio sin ella.

Llave Publica

16YsjZK9nweXyy3vNQQPKT8tfjCNjEX9JM

- Esta es la dirección de tu sitio.
- Usando esto cualquiera puede verificar si el archivo es creado por el dueño del sitio.
- Cada archivo descargado es **verificado,** esto lo hace seguro en contra de cualquier código malicioso que intente insertar cualquier modificación.

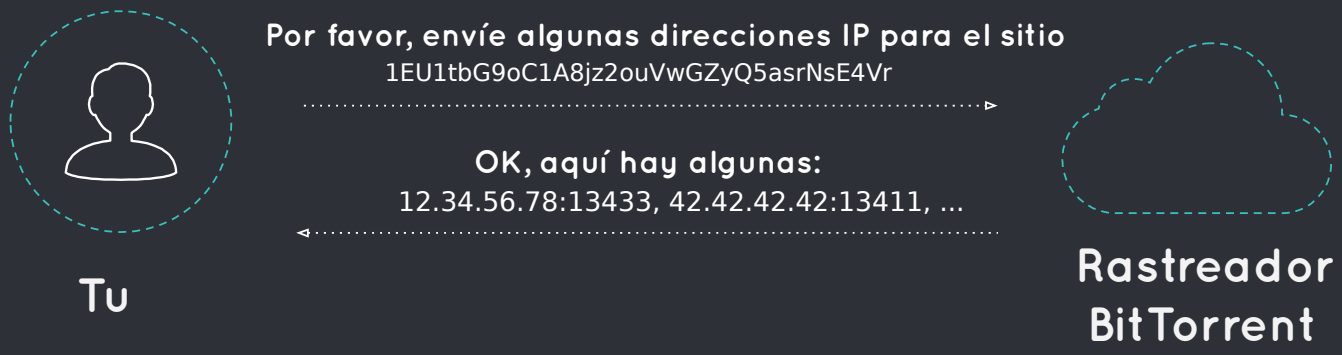
MAS INFORMACIÓN ACERCA DE LA CRIPTOGRAFÍA ZERONET

- ZeroNet utiliza la misma **codificación** basada en la **curva elíptica** de las billeteras Bitcoin.
- Puedes aceptar **pagos** directamente a la **dirección** de tu sitio.
- Utilizando el ordenador más rápido actual, se necesitaría alrededor de **mil millones** de **años** para "hackear" una clave privada.

¿QUE PASA CUANDO VISITAS UN SITIO ZERONET?

¿QUE PASA CUANDO VISITAS UN SITIO ZERONET? (1/2)

1 Recopilación de direcciones IP de los visitantes:



- Pregunta a los **visitantes** las direcciones **IP** de los **rastreadores** de BitTorrent.
- También te **registra** como un visitante.
- El **intercambio** de pares **sin rastreador** también es soportado.

¿QUE PASA CUANDO VISITAS UN SITIO ZERONET? (2/2)

2 Descarga de archivos del sitio

1. Descarga un archivo denominado **content.json**, que contiene todos los demás nombres de archivo **hashes** y la firma criptográfica del propietario del sitio.
2. **Verifica** el archivo descargado content.json utilizando la **dirección** del sitio y la **firma** del propietario del sitio del archivo.
3. **Descarga otros archivos** (html, css, js, ...) y los verifica utilizando el hash SHA512 del archivo content.json.

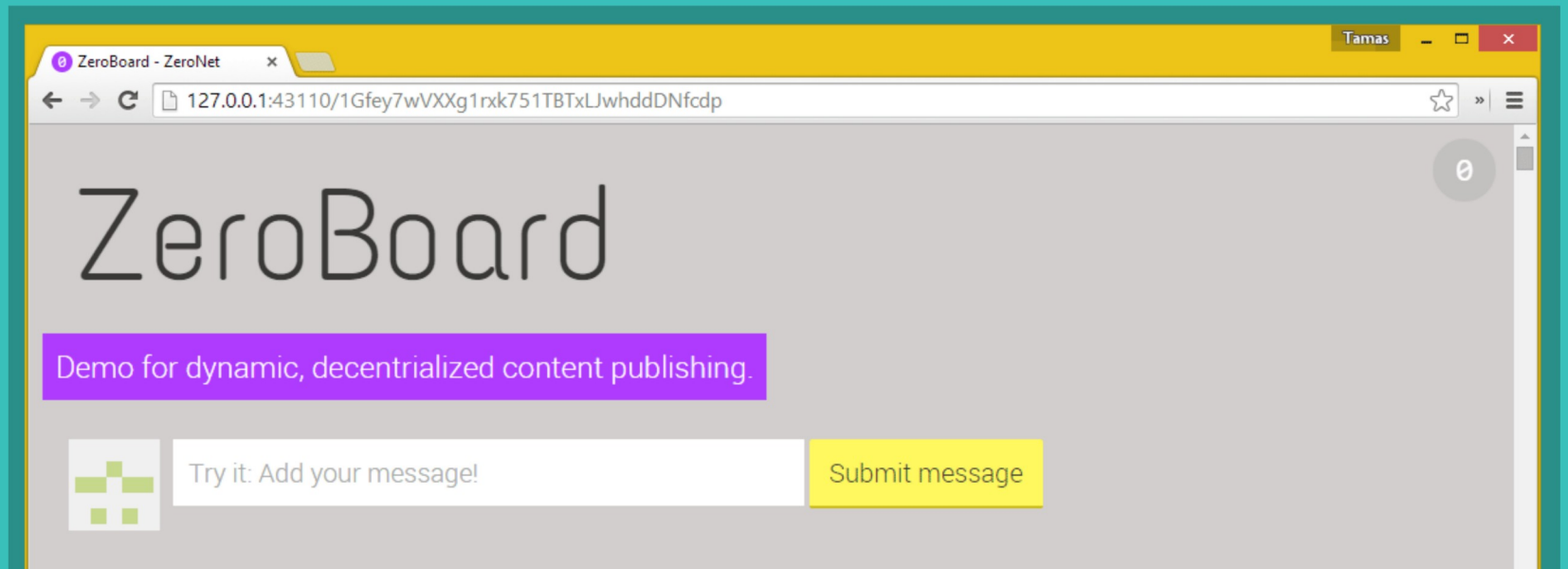
EJEMPLO DEL ARCHIVO CONTENT.JSON GENERADO


```
{

 "address": "1Name2NXVi1RDPDgf5617UoW7xA6YrhM9F",
 "title": "NombreZero",
 "description": "Dirección de registro Namecoin",

 "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+Nb7N5qb2cTvhULB3euvszufDnGlVeF4mswur3PyXxGXM+tJ8kZOFzspFRll0gOyCE0tCM=",
 "signs": {
  "1Name2NXVi1RDPDgf5617UoW7xA6YrhM9F": "G6X42ZmEBf66jjylSnx45Uee9J+QO7dLt1CLYULI17L78AFaUDVHYohEYUGxAFqKx75UpWGsPGSY1S7lr/Fe3EU="
 },
 "signs_required": 1,

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

}
```

MAS INFORMACIÓN SOBRE VISITAS DEL SITIO

- Usted comienza a **sembrar** los sitios tan pronto como usted los visita.
- Las **descargas** son priorizadas para una experiencia web más **rápida.**
- Puede utilizar la red **Tor** para ocultar su dirección **IP** real.

¿QUÉ HAY ACERCA DE LAS ACTUALIZACIONES DEL SITIO?



ACTUALIZACIONES DE SITIOS ZERONET

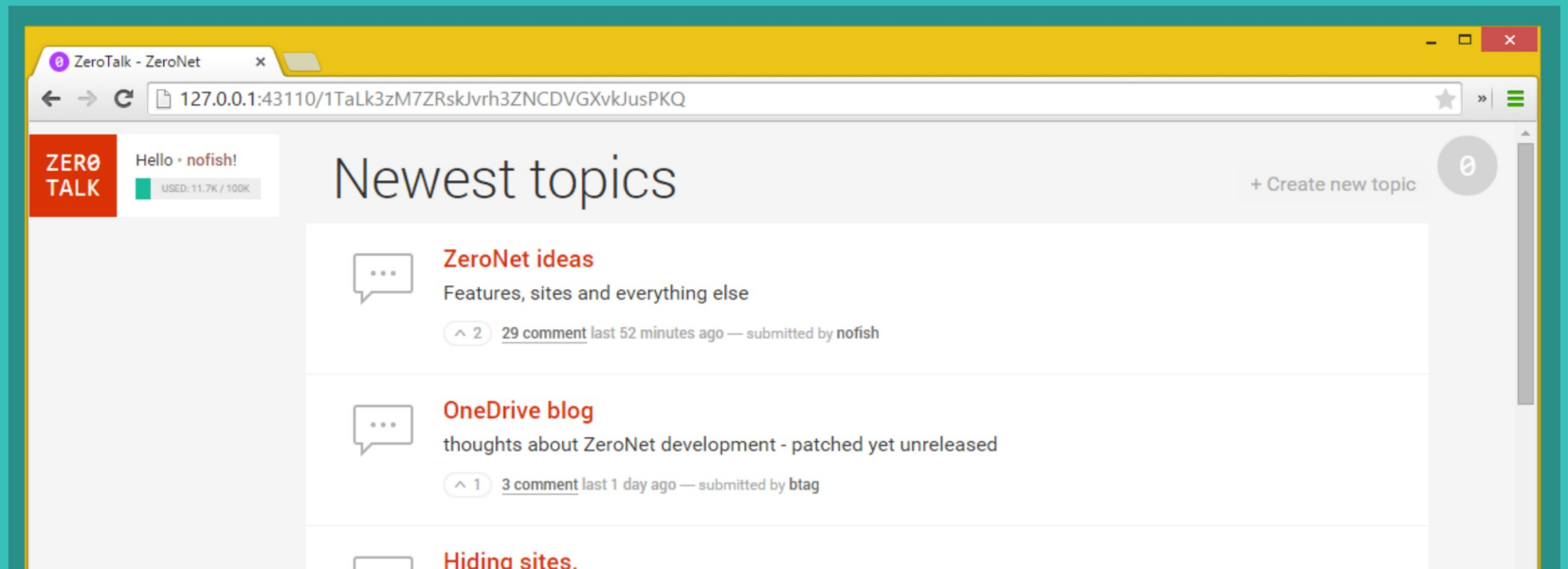
El dueño del sitio firma el content.json, entonces..

1. El **propietario del sitio envía** el nuevo content.json a un n mero reducido de visitantes.
2. El **visitante verifica** si es más reciente que su archivo actual.
3. El visitante descarga los **archivos modificados.**
4. Luego el/ella envía la **actualización** a otros visitantes

MAS INFORMACIÓN ACERCA DE LAS ACTUALIZACIONES DE LAS PAGINAS ZERONET

- El navegador es **notificado** inmediatamente sobre los cambios de archivo usando la API de **WebSocket**. Esto permite que los sitios sean actualizados en **tiempo real.**
- También son posibles sitios **multi-firmas.**
- Para un acceso más **rápido** y sencillo a los datos, los archivos json se pueden asignar **automáticamente** a una base de datos **SQL** incorporada.

SITIOS MULTI-USUARIOS



SITIOS ZERONET MULTI-USUARIOS

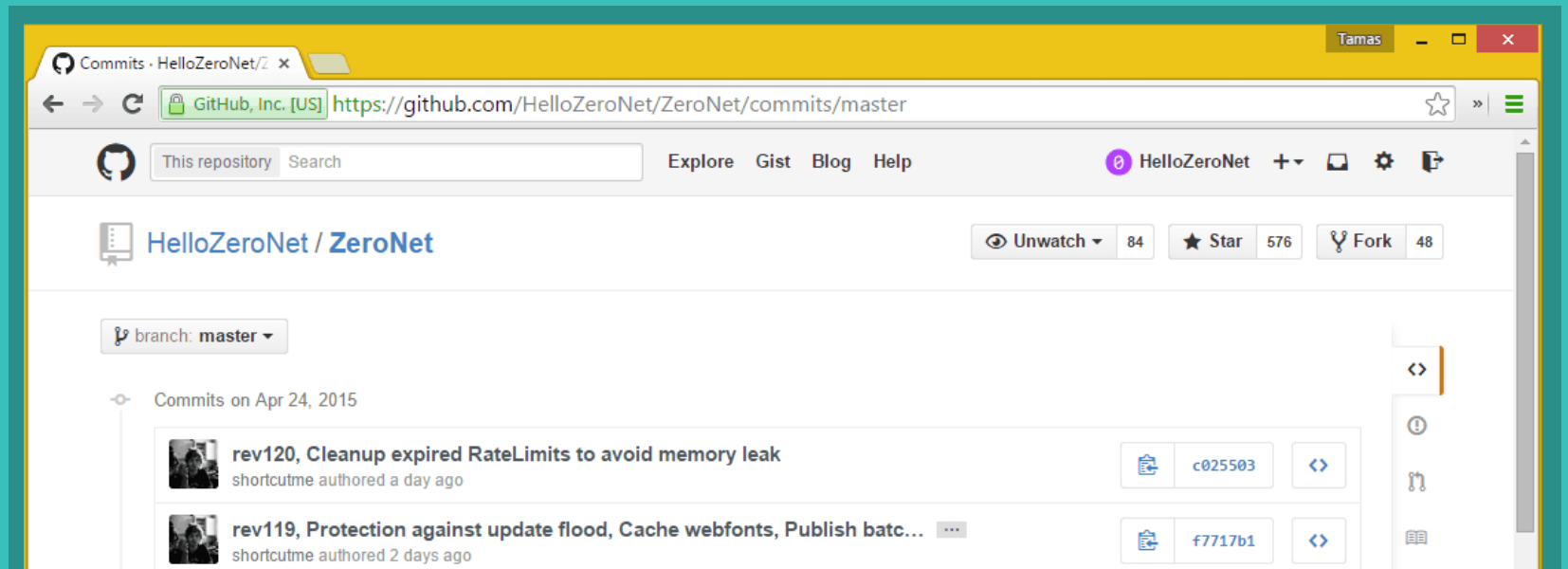
Solicitar permiso del propietario del sitio:

1. Se envía tu **dirección de autenticación** al propietario del sitio.
2. El propietario del sitio **crea** un nuevo archivo y establece la dirección de autenticación como un firmante válido.
3. El propietario del sitio **publica** el nuevo archivo y los permisos modificados para los **visitantes** del sitio.

MAS INFORMACIÓN ACERCA DE LAS PAGINAS ZERONET MULTI-USUARIOS

- Después de que el visitante obtenga el permiso concedido, él/ella es capaz de **empujar** las **modificaciones** directamente a otros compañeros **sin** ponerse en contacto con el **propietario** del sitio de nuevo.
- El propietario del sitio puede **eliminar** a los **usuarios** que **no** sigan las **normas.**
- El **tamaño** de los archivos de usuario puede **limitarse** para evitar **spam.**
- Dirección de autenticación / clave privada **única** generada para **cada** sitio. (Basado en **BIP32)**

ESTADO ACTUAL Y PLANES



ESTADO ACTUAL

PLANES FUTUROS

- **Enfoque en el contenido:** ~~mensajes de correo electrónico,~~ alternativa a Github, sitio de noticias, Mercado, etc...
- **División de archivos** como los Torrents y archivos opcionales.
- **Sitios privados** basados en clave o clave p blica
- ~~**Multi-usuario más fáciles:** socios de autorización de confianza~~
- **I2P** y mejor soporte **Tor (servicios ocultos)**

ZERONET ES...

- Una plataforma de distribución **web alternativa.**
- Enfocado en la **velocidad, usabilidad** y la **experiencia** del usuario.
- **No** tratando de **competir** con **proyectos** de más de 10 años de edad. (Freenet, I2P).
- **No** más **anónimo** que **BitTorrent** (Puede usar **Tor** para ocultar su **IP).**
- **No** es un **reemplazo** para el **modelo** actual basado en **cliente <> servidor.**

¡Gracias!

PUEDES EMPEZAR A USAR ZERONET HOY

https://github.com/HelloZeroNet/ZeroNet

@HelloZeroNet

/r/ZeroNet

#ZeroNet @ freenode