ZeroNet

使用 Bitcoin 加密和 BitTorrent 网络的去中心化网络架构

关于 ZERONET

为什么？

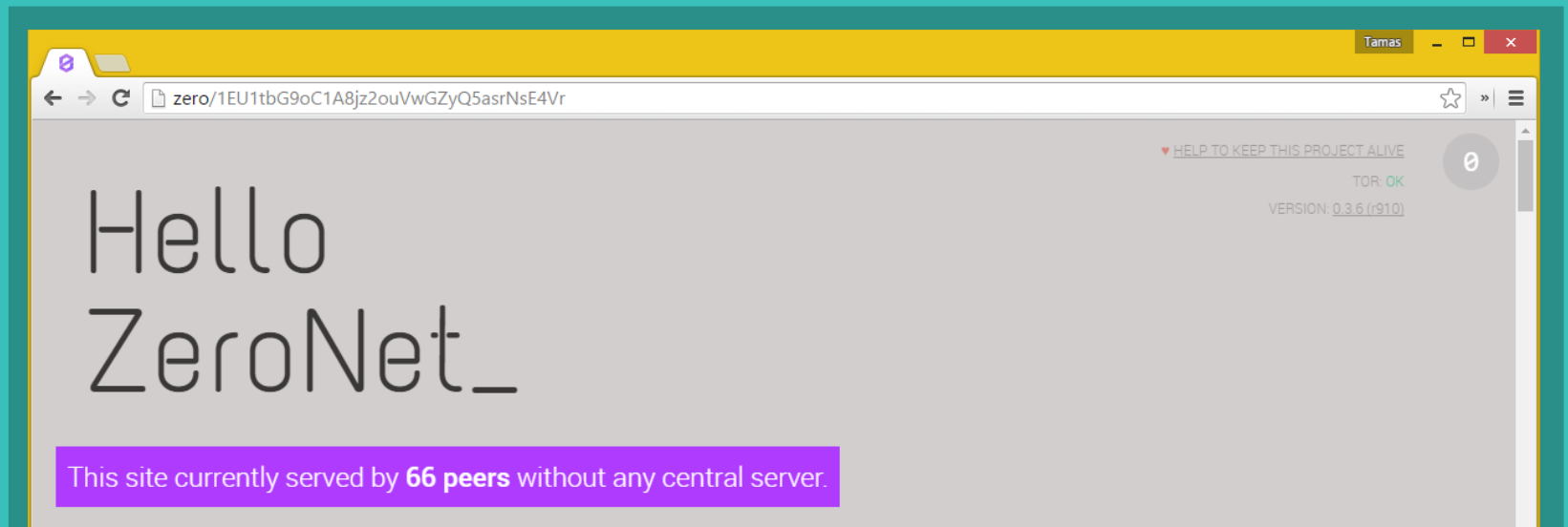
我们相信开放，自由，去中心化的网络与通讯

- **无需托管费用**
  你的站点由访客保存
- **无法被关闭**
  因为节点无处不在
- **避免单点故障**
  只要有任何在线的节点站点就可以访问
- **快捷并可离线运行**
  即使离线，你也可以使用保存过的站点

现有功能

- **站点可实时更新**
- 支持 Namecoin 的 .bit 域名
- **支持多用户站点**
- 无需密码，基于 Bitcoin 的 BIP32 认证
- 内建 SQL 服务器和点对点数据同步
- 支持 Tor 网络
- 可以在任何浏览器 / 系统中使用
- 开放式代理：你不需要下载任何东西就可以体验它

这是怎么做到的？


Tamas
zero/1EU1tbG9oC1A8jz2ouVwGZyQ5asrNsE4Vr
♥ HELP TO KEEP THIS PROJECT ALIVE
TOR: OK
VERSION: 0.3.6 (r910)
0
Hello
ZeroNet_
This site currently served by 66 peers without any central server.

关于非对称加密你需要知道的

在你创建站点时，你会得到两个密钥：

私钥

5JNiiGspzqt8sC8FM54FMr53U9XvLVh8Waz6YYDK69gG6hso9xu

- **只有你知道**
- 允许你对你的站点的新内容进行签名
- **无需中心注册**
  这永远不会离开你的电脑
- 你必须有它才能更改你的站点

公钥

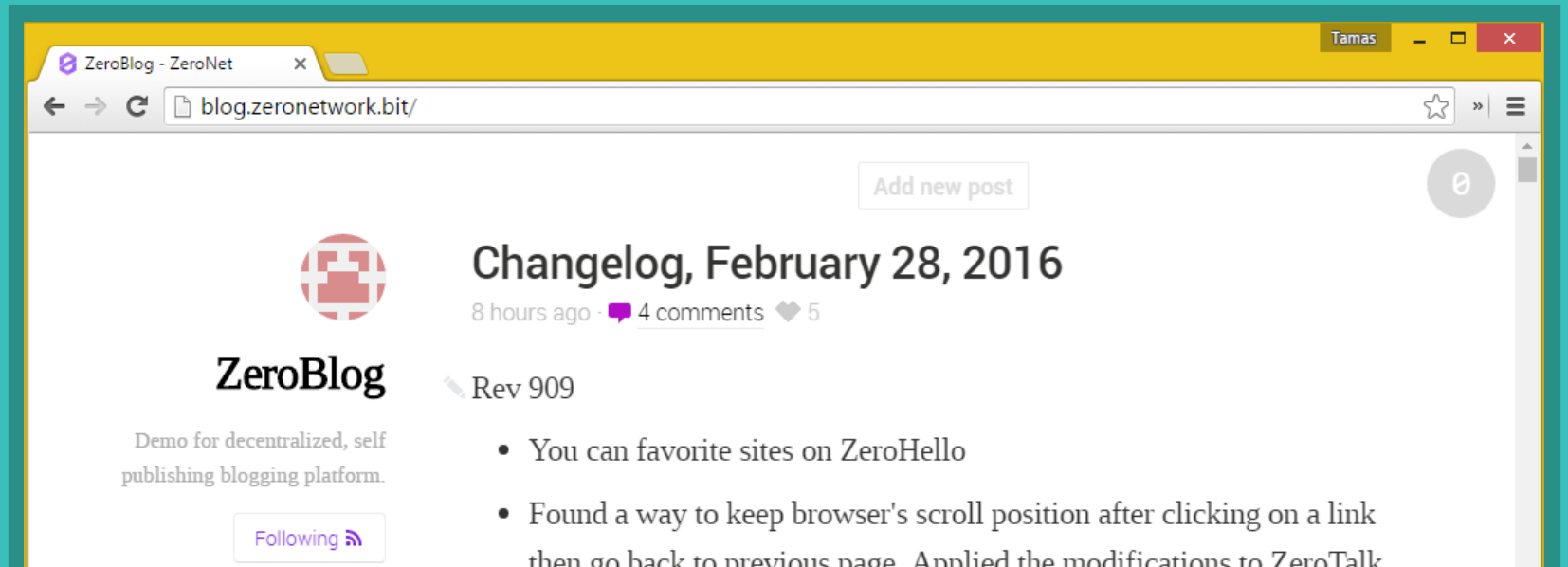
16YsjZK9nweXyy3vNQQPKT8tfjCNjEX9JM

- **这会被用作你的站点地址**
- 用于验证文件是否是由站长创建的
- 每一个下载的文件都会被验证来确保不会被插入恶意代码或被未经授权的更改

有关于 ZERONET 加密的更多信息

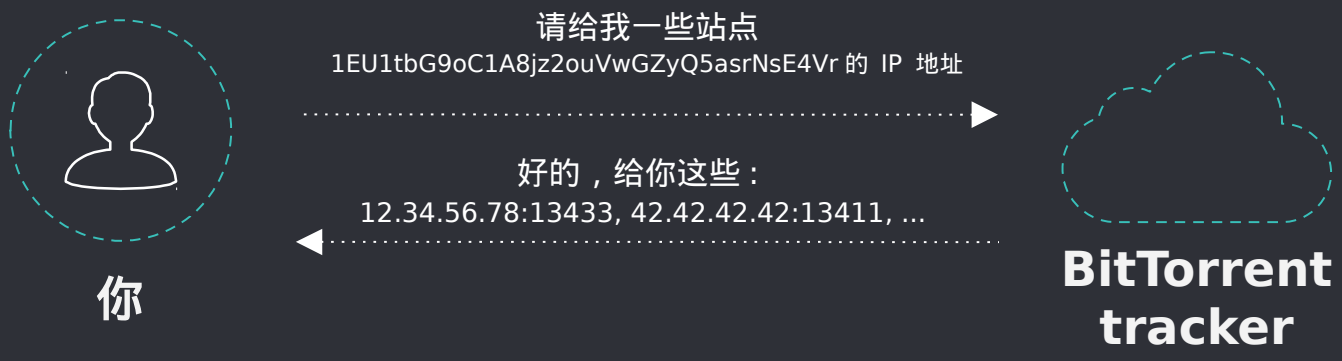
- ZeroNet 使用与你的 Bitcoin 钱包相同的基于椭圆曲线的加密
- 你可以直接使用你的站点地址来接受付款
- 即使使用现在最快的超级计算机也需要 10 亿年才能破解一个私钥

在你浏览一个 ZeroNet 站点时，都发生了什么？



在你浏览一个 ZeroNet 站点时，都发生了什么？(1/2)

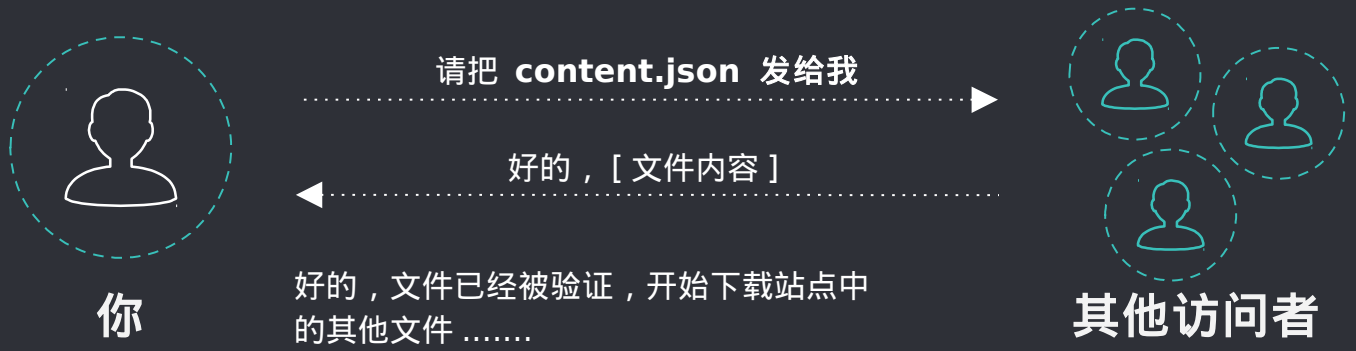
1 请求访问者的 IP 地址：



- 向 BitTorrent trackers 请求 IP 地址
- 把你也注册为一个访问者
- 也支持无需 Tracker 的节点间传输

在你浏览一个 ZeroNet 站点时，都发生了什么？(2/2)

2 下载站点中的文件



1. 下载名为 **content.json** 的文件，其中包含了**其他所有文件的文件名，校验和以及站长的签名**
2. 使用站点地址和站长的签名来**验证**所下载的 content.json
3. 下载其他文件（html, css, js,...）并使用 content.json 中的 SHA512 校验和进行验证

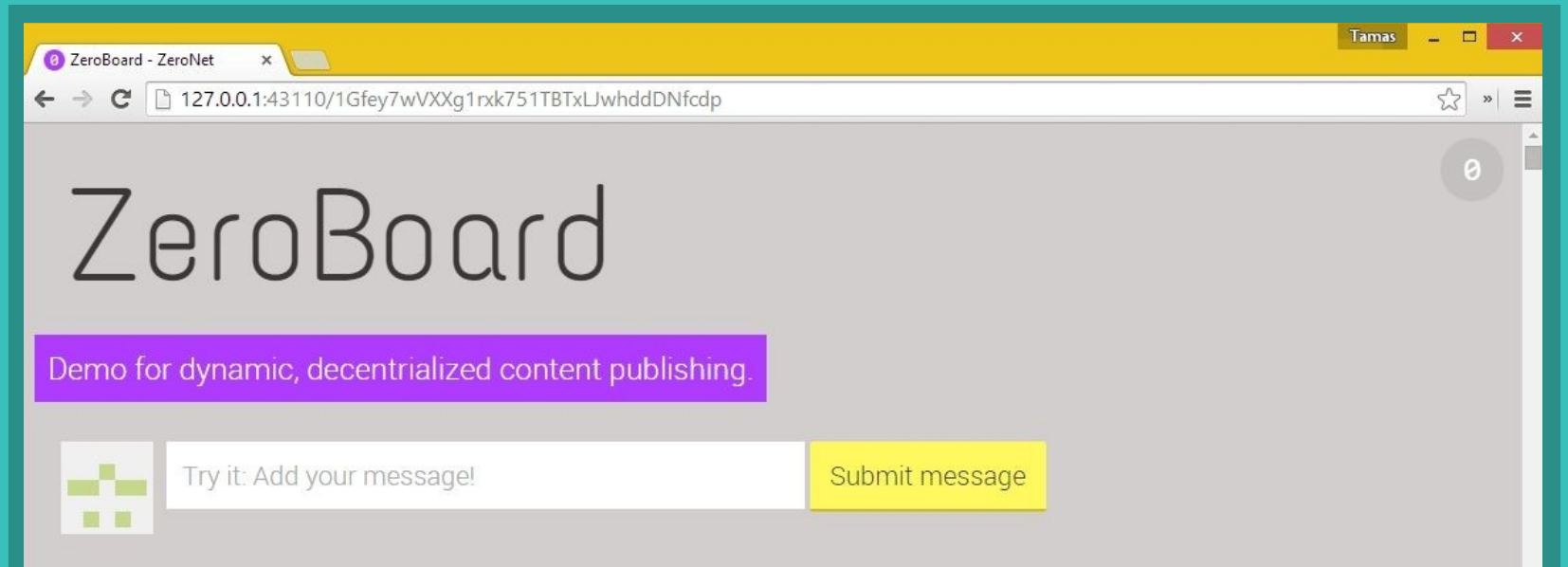
所生成的 CONTENT.JSON 的示例


```
{

  "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"

}
```

关于浏览站点 ……

- 在你浏览站点时你便开始储存它们
- 下载时划分优先级以获得最快的浏览体验
- 你可以使用 Tor 网络来隐藏自己的 IP 地址
- 支持可选文件，它们将只会在你的浏览器发出请求时被下载

站点是如何更新的？


ZeroBoard - ZeroNet
Tamas
127.0.0.1:43110/1Gfey7wVXXg1rxk751TBTxLJwhddDNfcdp
0
ZeroBoard
Demo for dynamic, decentrialized content publishing.
Try it: Add your message!
Submit message

ZERONET 站点的更新

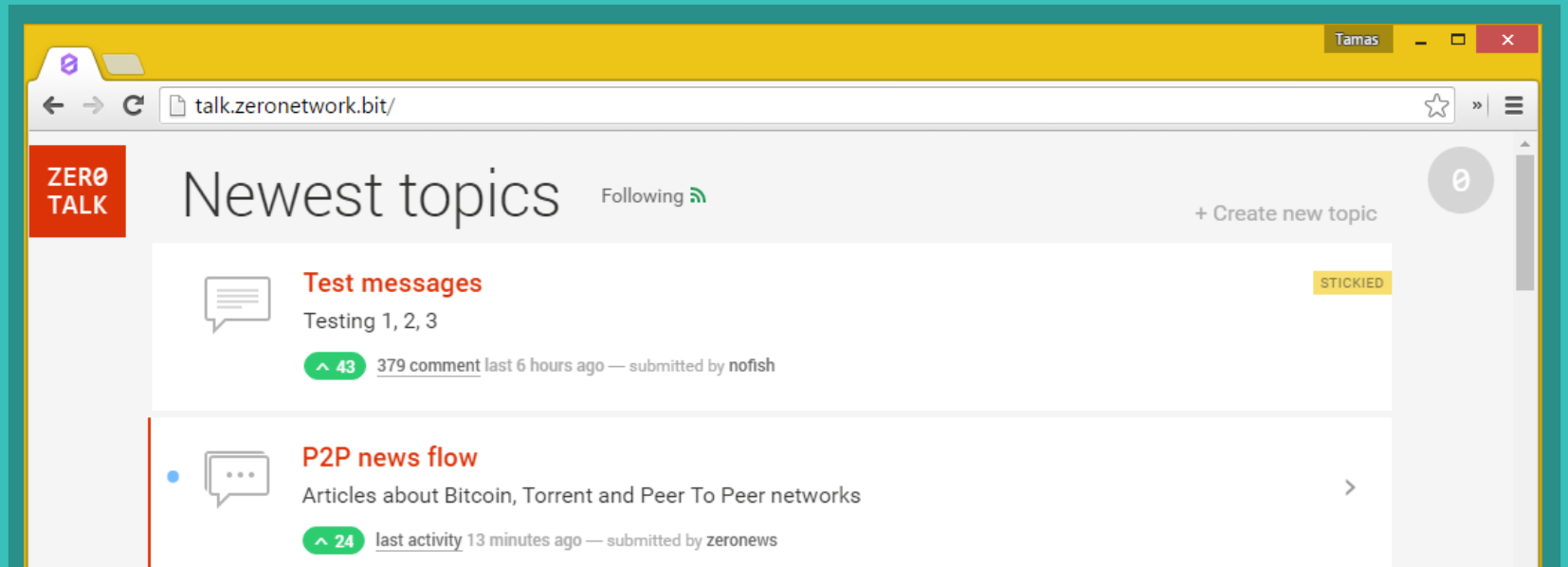
站长为新的 content.json 文件签名，然后 .....

1. 站长把新的 content.json 发送给其他几个浏览者
2. 浏览者检查文件，如果比自己这里的新 .....
3. 浏览者下载修改过的文件

关于 ZeroNet 站点更新的更多信息 ……

- 浏览器将会通过 WebSocket API 实时通知文件的更新情况，这将允许你构建实时更新的站点
- 也可能构建多签名站点
- 为了更快和更简单的数据访问， .json 文件将会被自动映射到一个内建的 SQL 数据库

关于多用户站点


Tamas
talk.zeronetwork.bit/
ZER0 TALK
Newest topics
Following
+ Create new topic
Test messages
Testing 1, 2, 3
STICKIED
43
379 comment last 6 hours ago — submitted by nofish
P2P news flow
Articles about Bitcoin, Torrent and Peer To Peer networks
24
last activity 13 minutes ago — submitted by zeronews

关于 ZERONET 中的多用户站点

向站长请求权限：

1. 把你的授权地址发送给站长
2. 站长创建一个新文件并将你的授权地址设置为有效的
3. 站长向网站的访问者发布新文件和更改的权限

关于 ZeroNet 中多用户站点的更多信息 ……

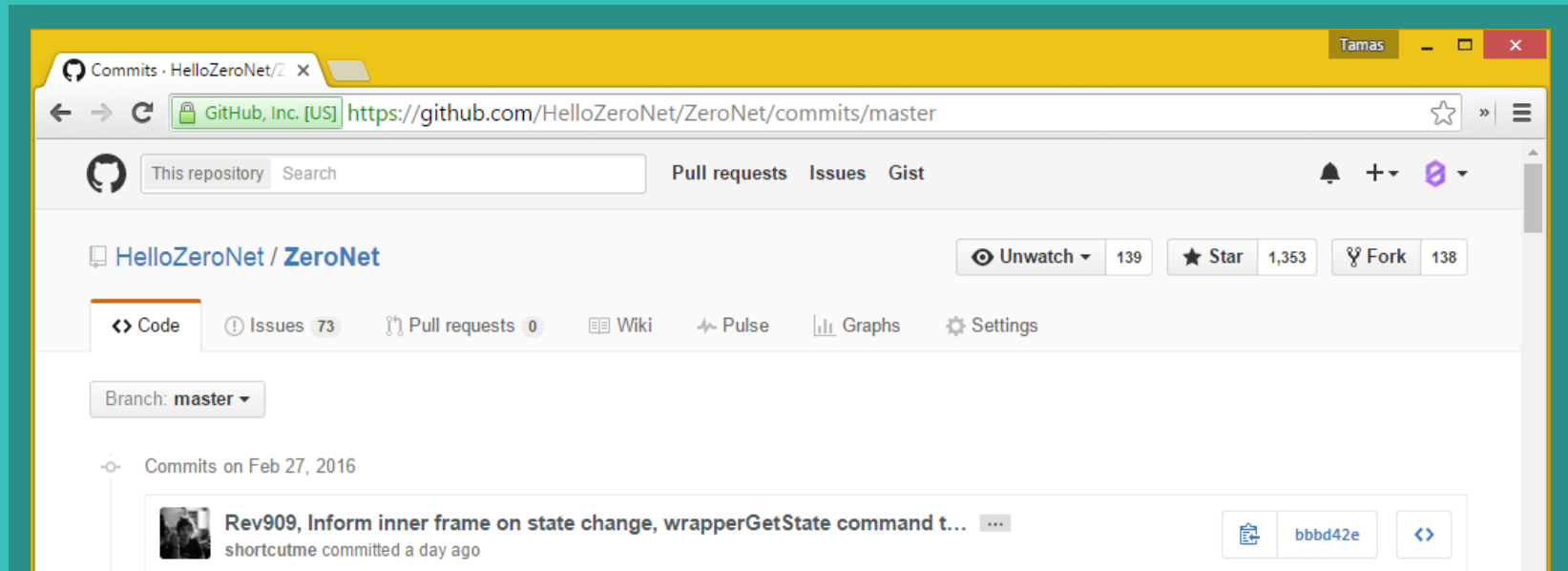
1. 你如果你信任其他站点的用户，可以通过使用授权提供功能来跳过注册流程

2. 站点的所有者可以移除恶意用户

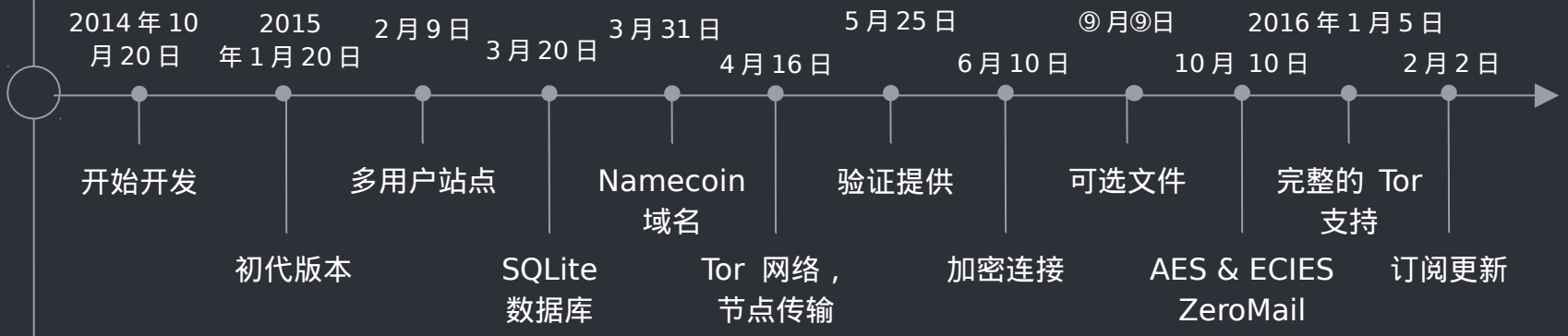
3. 可以限制用户的文件限额来阻止垃圾内容

4. 一个独特的，基于 BIP32 的算法将会为站点中的每一个用户生成有效的 Bitcoin 地址

现在的状态以及之后的计划



现在的状态



未来的计划

1. 关注内容：社交网络， Github 的替代品，新闻网站，在线市场等 ...
2. 类似于 BitTorrent 的文件拆分
3. 基于密码或者公钥的私有站点
4. 支持 I2P 网络

ZERONET 是 ...

- 成为一个可以替代 web 的分发平台
- 关注速度，可用性和用户体验

- 不试图于 10 年以上的项目竞争（Freenet, I2P）
- 匿名性不比 BitTorrent 好
  （你可以使用 Tor 来隐藏你的 IP）
- 不是现有的 C/S 架构的替代品

其他 ZERONET 的好处

1. 站点 100% 透明：任何人都可以查看站点中的任何部分
2. 一键克隆：为任何站点创建你自己的版本
3. 没有后端代码：直接从 JavaScript 执行 SQL 命令，无网络延迟。
4. 即时 CDN ：你的内容分布在世界各地
5. 可以在非互联网网络中工作（蓝牙，WiFi 直连，无线电通信，Meshnets 等）
6. 零歧视：相同，零成本的基础设施给每个人相同的机会
7. 零信任：站点无法在没有私钥的情况下被修改

感谢！

你可以今天就开始使用 ZeroNet ！

https://zeronet.io

@HelloZeroNet

/r/ZeroNet

#ZeroNet @ freenode