

شبکه Tor چیست و چگونه کار می کند

به همراه راهنمای تصویری اتصال کیف پول الکتراام از طریق این شبکه

## فهرست مطالب

- شبکه تور چیست و چه کاربردی دارد
- تاریخچه مختصر پیدایش شبکه و مرورگر تور
- شبکه تور چگونه کار می کند
- نصب مرورگر تور و اتصال به شبکه
- اتصال در شرایطی که ارتباط با شبکه تور سانسور شده است
- اثر استفاده از مرورگر تور بر موقعیت مکانی اعلام شده به شبکه اینترنت
- سرویس های لایه ای چیستند و چگونه می توان با مرورگر تور به آن ها دسترسی پیدا کرد
- کاربرد شبکه تور و سرویس های لایه ای در کیف پول های بیت کوین
- مواردی که باید حین استفاده از مرورگر تور در نظر گرفته شوند
- آیا استفاده از مرورگر تور تضمین کننده حریم خصوصی کاربران است
- آیا خلاف کاران از مرورگر تور و سرویس های onion استفاده می کنند
- راهنمای تصویری اتصال کیف پول الکترا به سرورهای عمومی الکترا از طریق سرویس های لایه ای شبکه تور

## شبکه تور چیست و چه کاربردی دارد

تور<sup>۱</sup> ابزاری است برای کسانی که می‌خواهند در فضای اینترنت ناشناس باشند یا به سایت‌هایی که سانسور شده‌اند یا سایت‌های پنهان<sup>۲</sup> در لایه‌های این شبکه دسترسی پیدا کنند. در این خودآموز همچنین یک جنبه کاربردی شبکه تور را معرفی می‌کنیم و آن سرویس‌های onion است که برای کاربران کیف پول‌های بیت‌کوین کاربردی هستند و در ادامه به آن‌ها خواهیم پرداخت.

### تاریخچه مختصر پیدایش شبکه و مرورگر تور

مفهوم مسیریابی لایه‌ای<sup>۳</sup> که بعداً بیشتر درباره دلیل نام‌گذاری آن صحبت خواهیم کرد، اولین بار در سال ۱۹۹۵ و به دلیل نبود امنیت در ارتباطات اینترنتی و امکان ردگیری و نظارت افراد، توسط بخش تحقیقات و توسعه نیروی دریایی آمریکا<sup>۴</sup> تأمین سرمایه شد. هدف از ایجاد این پروژه این بود که حریم خصوصی کاربران اینترنت به روش مسیریابی لایه‌ای و ارسال ترافیک از چند سرور و رمزنگاری اطلاعات در هر مرحله و در بالاترین سطح فراهم شود.

در اوایل دهه ۲۰۰۰ میلادی دو نفر از فارغ‌التحصیلان دانشگاه صنعتی ماساچوست<sup>۵</sup> روی یک پیاده‌سازی متفاوت از نسخه موجود شروع به کار کردند و برای تمایز نام آن را تور گذاشتند. این شبکه در ماه اکتبر سال ۲۰۰۲ شروع به کار کرد و کُد آن هم به صورت اپن-سورس منتشر شد و تا آخر سال ۲۰۰۳ یک دوجین نود به صورت داوطلبانه در آن مشارکت داشتند.

---

1 Tor  
2 Onion services  
3 The Onion Routing  
4 Naval Research Lab  
5 MIT

در سال ۲۰۰۴ بنیاد مرزهای الکترونیکی<sup>۶</sup> با درک مزایای این پروژه و اثرات مثبت آن بر حریم خصوصی افراد اقدام به تأمین مالی این پروژه کرد. تا اینکه در نهایت در سال ۲۰۰۶ پروژه تور<sup>۷</sup> به صورت یک نهاد غیرانتفاعی و برای توسعه و نگهداری از آن تاسیس شد.

تور بین فعالان و کاربران علاقه‌مند به حفظ حریم خصوصی و آشنا با ابزارهای فنی محبوب شد و مورد استفاده قرار گرفت ولی استفاده از آن برای افرادی که با ابزارهای فنی آشنا نبودند همچنان دشوار بود. بنابراین از سال ۲۰۰۵ توسعه ابزارهایی که استفاده از تور را برای عموم مردم امکان‌پذیر کند شروع شد و مرورگر تور<sup>۸</sup> یکی از این ابزارها بود.

---

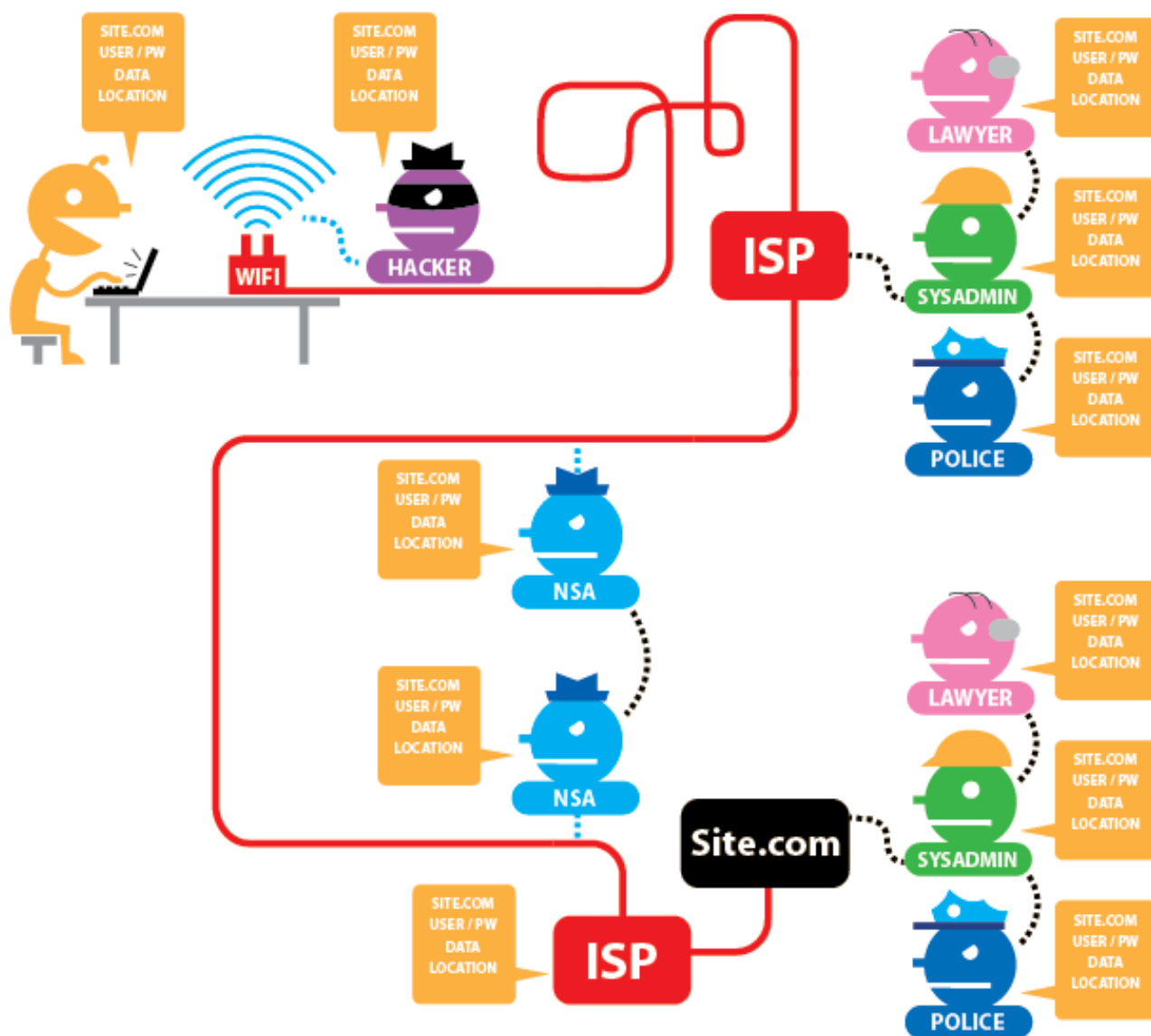
6 Electronic Frontier Foundation

7 Tor Project, Inc

8 Tor Browser

## شبکه تور چگونه کار می کند

برای درک طرز کار شبکه تور باید نحوه گردش اطلاعات در شبکه TCP/IP را مرور کنیم. برای این کار ابتدا فرض می کنیم یک سایت http بدون گواهی SSL را روی یک مرورگر معمولی مثل فایرفاکس باز کنیم.



برای مشاهده این صفحه در سایت بنیاد مرزهای الکترونیکی به آدرس زیر بروید:

<https://www.eff.org/pages/tor-and-https>

## کاربر

- می‌خواهد به سایت `site.com` برود
- برای وارد شدن به این سایت نام کاربری و پسورد خود را وارد می‌کند
- اطلاعاتی بین این کاربر و سایت در قالب فرم‌های وب رد و بدل می‌شود
- موقعیت مکانی تقریبی این کاربر با توجه به IP او مشخص است

## هکر یا کسی که به شبکه داخلی کاربر دسترسی دارد

- به همه اطلاعاتی که کاربر در شبکه ارسال یا دریافت می‌کند دسترسی دارد

## وکلای پلیس، و مسئول شبکه تأمین کننده اینترنت، که به ISP کاربر دسترسی دارند

- به همه اطلاعاتی که کاربر در شبکه ارسال یا دریافت می‌کند دسترسی دارند

## نهادهای نظارتی ملی و بین‌المللی که به لینک شبکه داخلی یا بین‌المللی دسترسی دارند

- به همه اطلاعاتی که کاربر در شبکه ارسال یا دریافت می‌کند دسترسی دارند

## افرادى که به شبکه ISP تأمین کننده اینترنت میزبان سایت دسترسی دارند

- به همه اطلاعاتی که کاربر در شبکه ارسال یا دریافت می‌کند دسترسی دارند

## وکلای پلیس، و مسئول شبکه تأمین کننده اینترنت، که به سرور میزبان سایت

## `site.com` دسترسی دارند

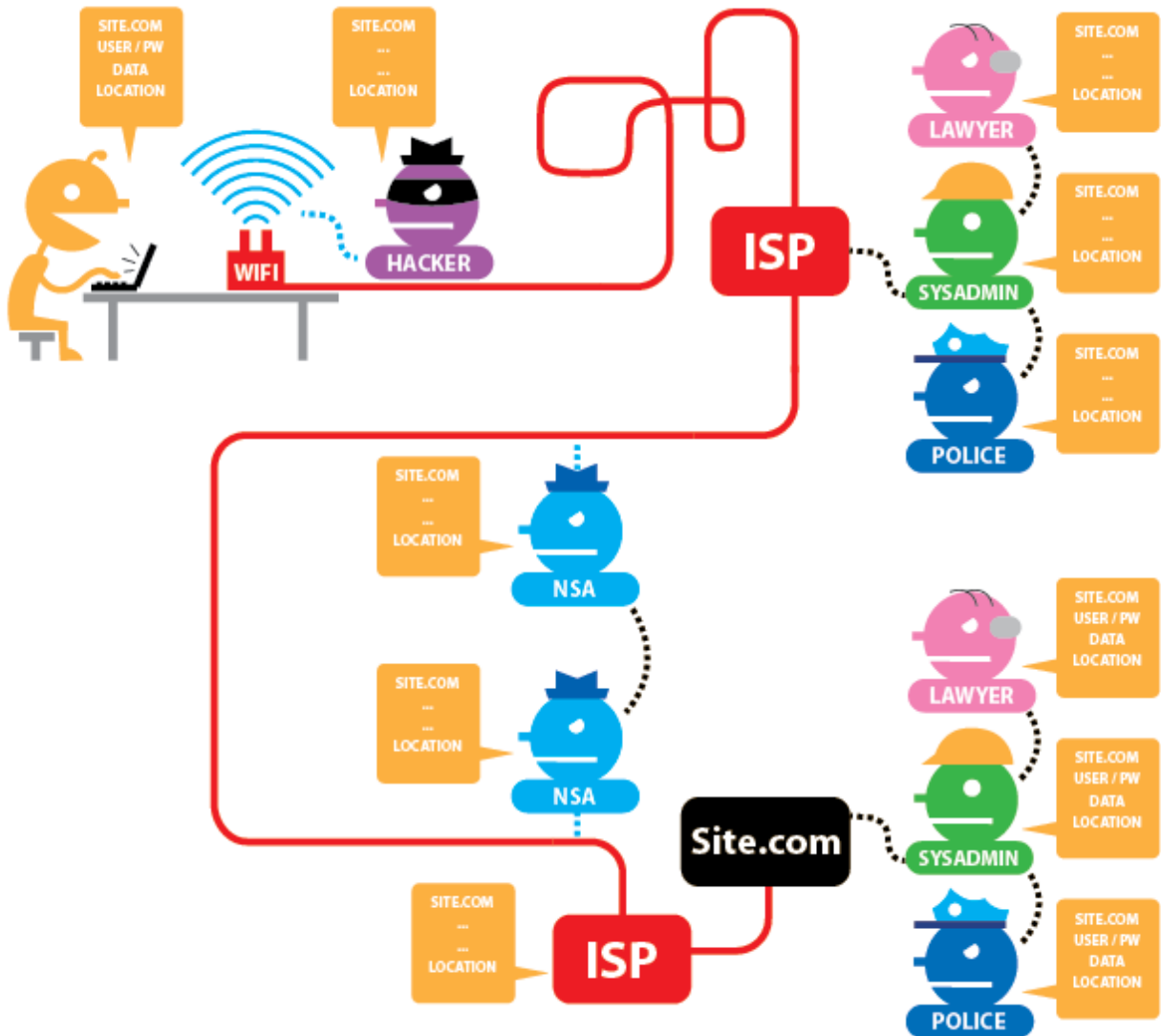
- به همه اطلاعات کاربر دسترسی دارند

همانطور که مشاهده می کنید در صورت بازدید از یک سایت http با یک مرورگر معمولی، هر کس در صورت دسترسی به کانال ارتباطی، به محتوا و اطلاعاتی که منتقل می شود دسترسی خواهد داشت.



پیغام مرورگر فایرفاکس مبنی بر اینکه ارتباط شما رمزگذاری نشده است (ssl نیست) و هر کس به شبکه ارتباطی شما دسترسی پیدا کند می تواند محتوای ارسال و دریافت شده را بخواند.

حال اگر ارتباط با این سایت از طریق SSL باشد، وضعیت به چه صورت خواهد شد؟





## کاربر

- می‌خواهد به سایت `site.com` برود
- برای وارد شدن به این سایت نام کاربری و پسورد خود را وارد می‌کند
- اطلاعاتی بین این کاربر و سایت در قالب فرم‌های وب رد و بدل می‌شود
- موقعیت مکانی تقریبی این کاربر با توجه به IP او مشخص است

## هکر یا کسی که به شبکه داخلی کاربر دسترسی دارد

- مقصد سایت مورد نظر کاربر را می‌داند
- با توجه به معلوم بودن IP کاربر، از موقعیت تقریبی او اطلاع دارد

## وُکلا، پلیس، و مسئول شبکه تأمین کننده اینترنت، که به ISP کاربر دسترسی دارند

- مقصد سایت مورد نظر کاربر را می‌دانند
- با توجه به معلوم بودن IP کاربر، از موقعیت تقریبی او اطلاع دارند

## نهادهای نظارتی ملی و بین‌المللی که به لینک شبکه داخلی یا بین‌المللی دسترسی دارند

- مقصد سایت مورد نظر کاربر را می‌دانند
- با توجه به معلوم بودن IP کاربر، از موقعیت تقریبی او اطلاع دارند

## افرادى که به شبکه ISP تأمین کننده اینترنت میزبان سایت دسترسی دارند

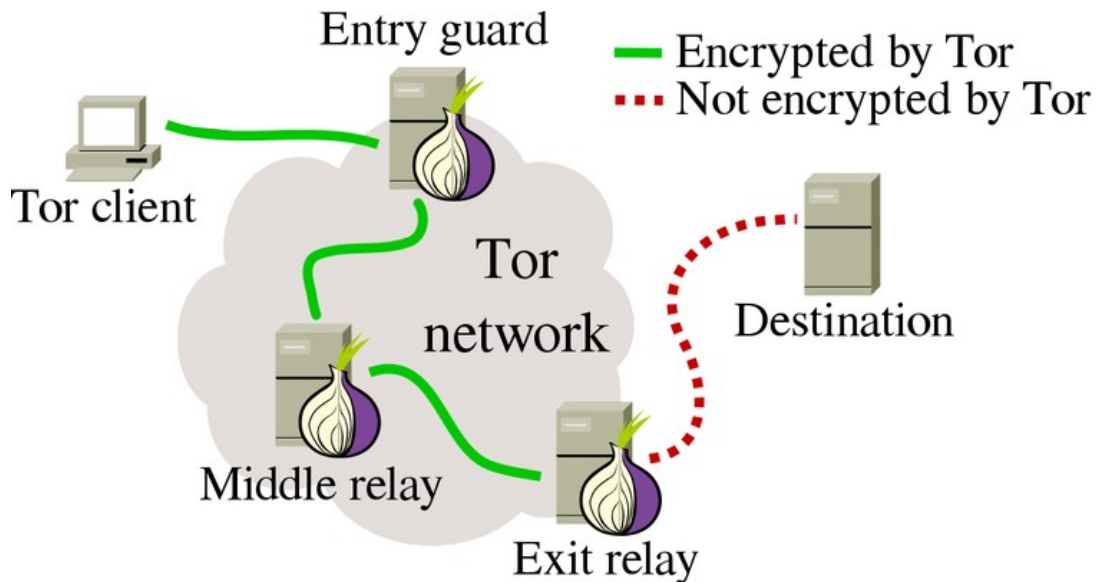
- مقصد سایت مورد نظر کاربر را می‌دانند
- با توجه به معلوم بودن IP کاربر، از موقعیت تقریبی او اطلاع دارند

وُکلا، پلیس، و مسئول شبکه تأمین کننده اینترنت، که به سرور میزبان سایت  
**site.com** دسترسی دارند

• به همه اطلاعات کاربر دسترسی دارند

همانطور که مشاهده می کنید در حالت **https** اطلاعات منتقل شده بین کاربر و سایت  
رمزنگاری می شود ولی همچنان موقعیت مکانی او برای همه افرادی که به کانال ارتباطی  
دسترسی دارند معلوم است.

مرورگر تور برای حل این مشکل و تأمین حریم خصوصی کاربران و برای تغییر آی پی و در پی آن تغییر موقعیت مکانی آن‌ها، از روش مسیریابی لایه‌ای استفاده می‌کند و ترافیک کاربر را با رد کردن از میان ۳ گره در شبکه تور به مقصد می‌رساند.

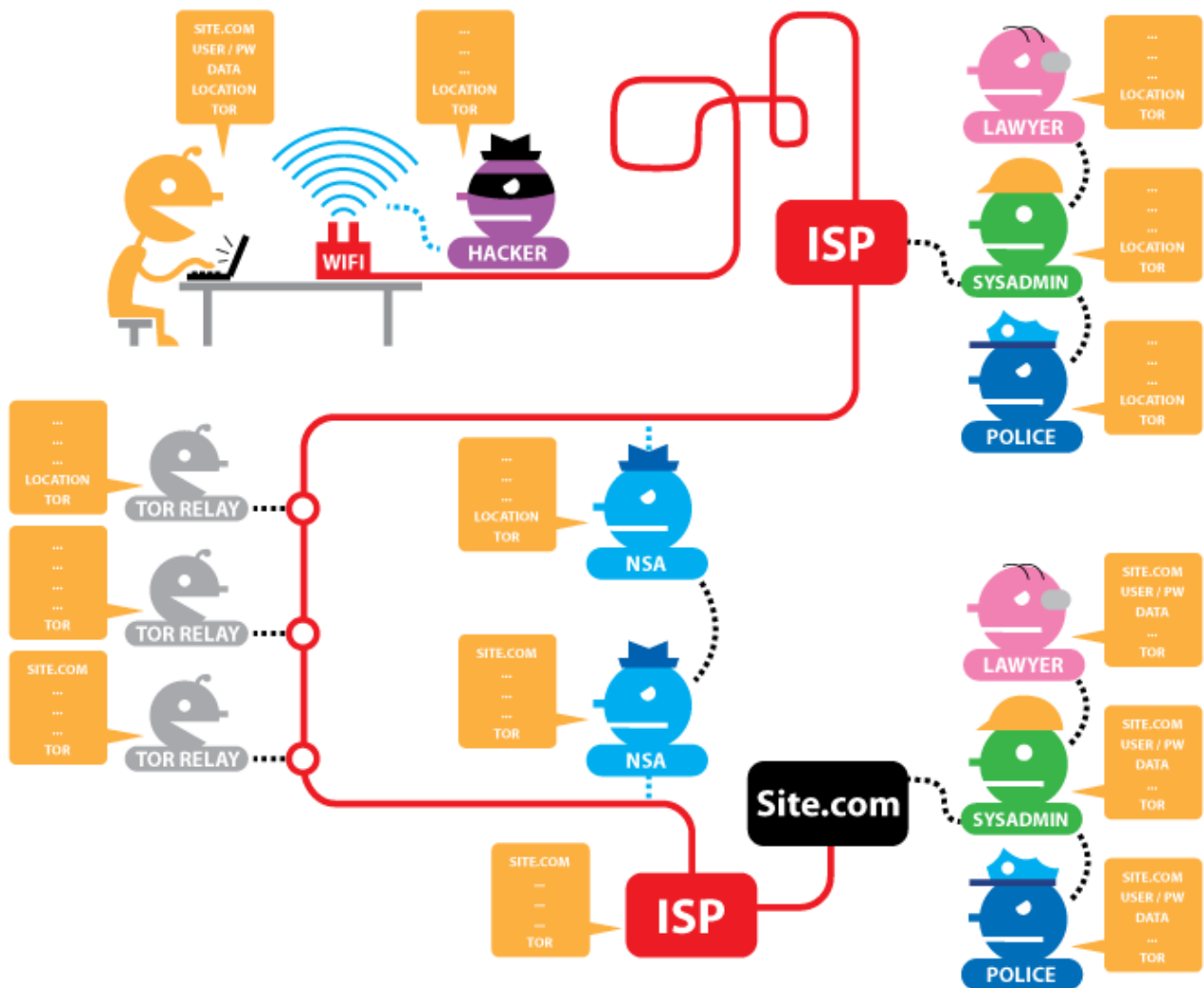


مرورگر تور در اولین اجرا تلاش می‌کند به شبکه تور<sup>۹</sup> وصل شود و اطلاعات شبکه را دانلود کند. در صورت اتصال موفق به شبکه، اگر آدرس یک سایت را در مرورگر تور بنویسید، برای ارسال درخواست به مقصد<sup>۱۰</sup> اول از یک نود ورودی<sup>۱۱</sup> استفاده می‌کند. بعد این ترافیک از طریق یک نود میانی<sup>۱۲</sup> و در نهایت از طریق نود خروجی<sup>۱۳</sup> به مقصد می‌رسد و نتیجه درخواست از همان مسیر به کاربر ارسال می‌شود.

به لینک بین نودها توجه کنید. ارتباطات سبز از طریق مرورگر تور رمزگذاری<sup>۱۴</sup> شده است ولی ارتباط بین نود خروجی به مقصد از طریق مرورگر تور رمزگذاری نشده است.

9 Tor Network  
 10 Destination  
 11 Entry Guard  
 12 Middle Relay  
 13 Exit Relay  
 14 Encrypted by Tor

حال اگر با مرورگر تور یک سایت **https** را باز کنیم. اطلاعات کاربر به چه شکل بر روی شبکه منتقل می‌شود؟



## کاربر

- با استفاده از مرورگر تور به سایت `site.com` می‌رود
- برای وارد شدن به این سایت نام کاربری و پسورد خود را وارد می‌کند
- بعد از وارد شدن به سایت اطلاعاتی بین این کاربر و سایت رد و بدل می‌شود
- موقعیت مکانی تقریبی این کاربر با توجه به IP او مشخص است

## هکر یا کسی که به شبکه داخلی کاربر دسترسی دارد

- برای او معلوم است که کاربر از مرورگر تور استفاده می‌کند
- با توجه به معلوم بودن IP کاربر، از موقعیت تقریبی او اطلاع دارند

## وکلا، پلیس، و مسئول شبکه تأمین کننده اینترنت، که به ISP کاربر دسترسی دارند

- برای آن‌ها معلوم است که کاربر از مرورگر تور استفاده می‌کند
- با توجه به معلوم بودن IP کاربر، از موقعیت تقریبی او اطلاع دارند

## نهادهای نظارتی ملی و بین‌المللی که به لینک شبکه داخلی یا بین‌المللی دسترسی دارند

- برای آن‌ها معلوم است که کاربر از مرورگر تور استفاده می‌کند
- با توجه به معلوم بودن IP کاربر، از موقعیت تقریبی او اطلاع دارند

## اولین نود تور که به Tor Guard معروف است

- برای او معلوم است که کاربر از مرورگر تور استفاده می‌کند
- با توجه به معلوم بودن IP کاربر، از موقعیت تقریبی او اطلاع دارند

نود میانی تور که به **Middle Relay** معروف است

- این نود فقط اطلاعات رمزنگاری شده را در شبکه جابجا می کند و به هیچ اطلاعاتی دسترسی ندارد

نود آخر که به **Exit Relay** معروف است

- این نود با توجه به اینکه نود آخر در مسیر ترافیک تور است از آدرس سایت مقصد اطلاع دارد و ترافیک را تحویل آن می دهد

نهادهای نظارتی ملی و بین المللی که به لینک شبکه داخلی یا بین المللی دسترسی دارند

- برای آن ها معلوم است که کاربر از مرورگر تور استفاده می کند
- مقصد سایت مورد نظر کاربر را می دانند

افرادی که به شبکه **ISP** تأمین کننده اینترنت میزبان سایت دسترسی دارند

- برای آن ها معلوم است که کاربر از مرورگر تور استفاده می کند
- مقصد سایت مورد نظر کاربر را می دانند

و کلا، پلیس، و مسئول شبکه تأمین کننده اینترنت، که به سرور میزبان سایت

**site.com** دسترسی دارند

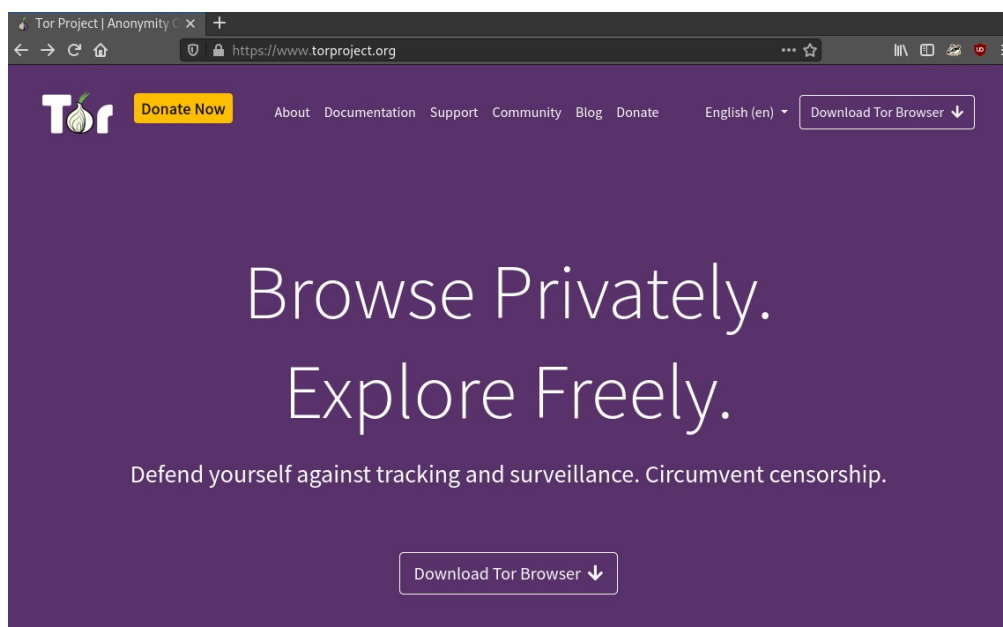
- به همه اطلاعات کاربر به جز موقعیت مکانی او دسترسی دارند

همان‌طور که مشاهده می‌کنید با استفاده از مرورگر تور و به محض عبور از اولین نود تور، موقعیت مکانی از دسترس افرادی که به شبکه دسترسی دارند خارج می‌شود. در واقع IP کاربر با آخرین نود تور جایگزین می‌شود.

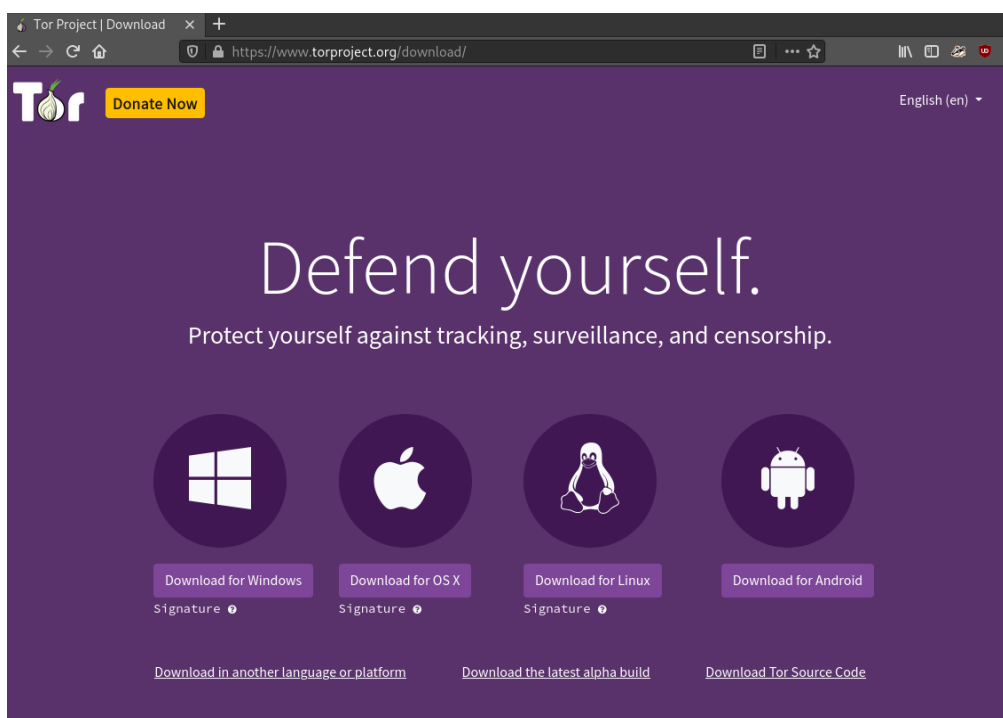
## نصب مرورگر تور و اتصال به شبکه

برای نصب مرورگر تور به سایت رسمی آن بروید

<https://www.torproject.org>

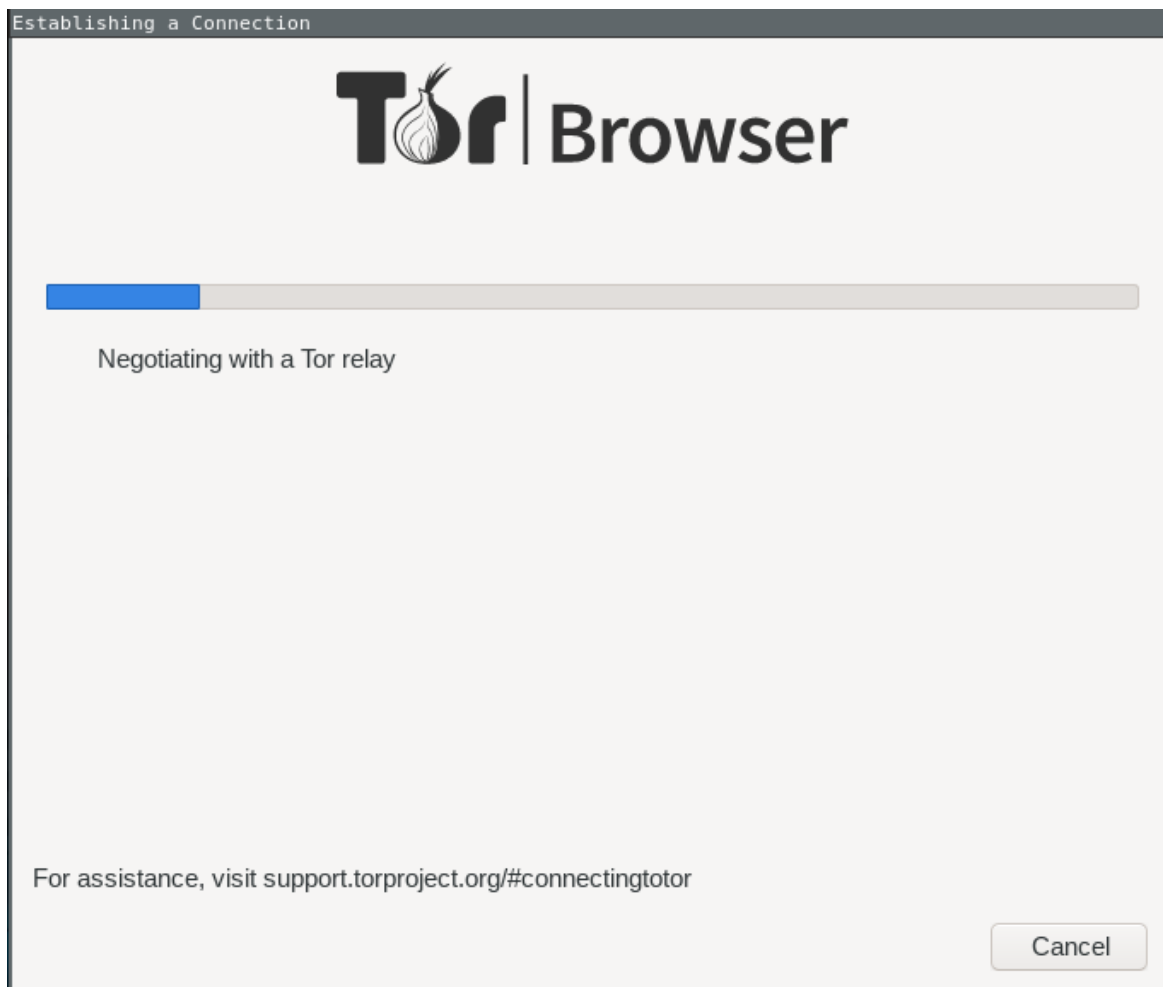


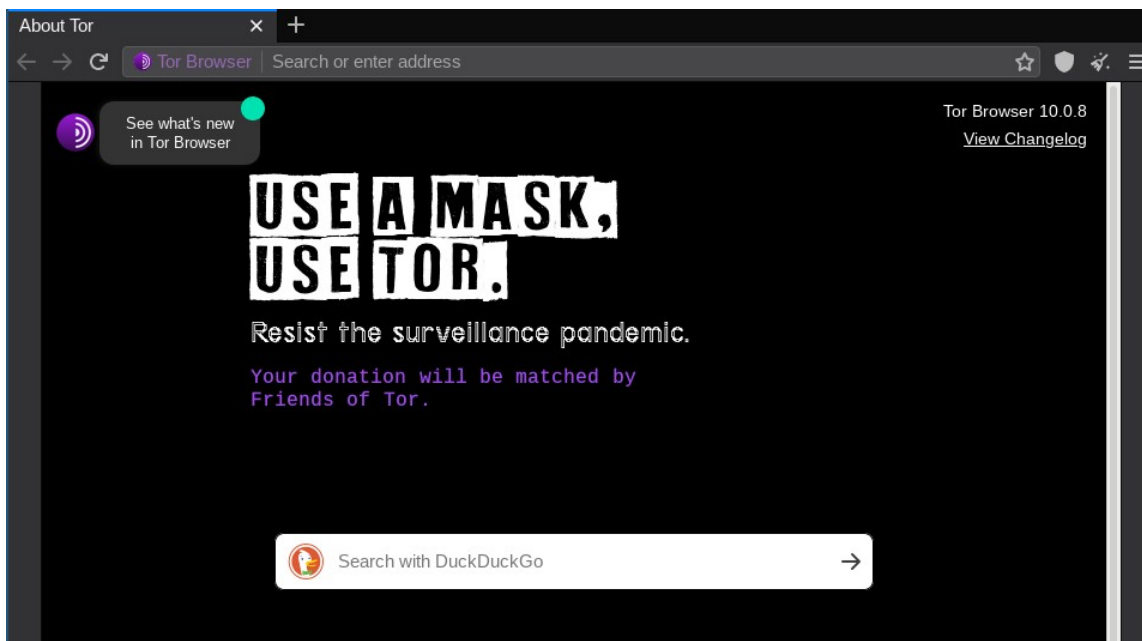
و فایل نصب آن را بر اساس سیستم عامل خود دانلود کنید





بعد از نصب مرورگر تور و اجرای آن، مرورگر شما تلاش می کند با اتصال به شبکه لیستی از نودهای شبکه را دانود کند و اگر این عملیات موفقیت آمیز باشد، مرورگر تور در قالب یک مرورگر فایرفاکس اجرا خواهد شد.

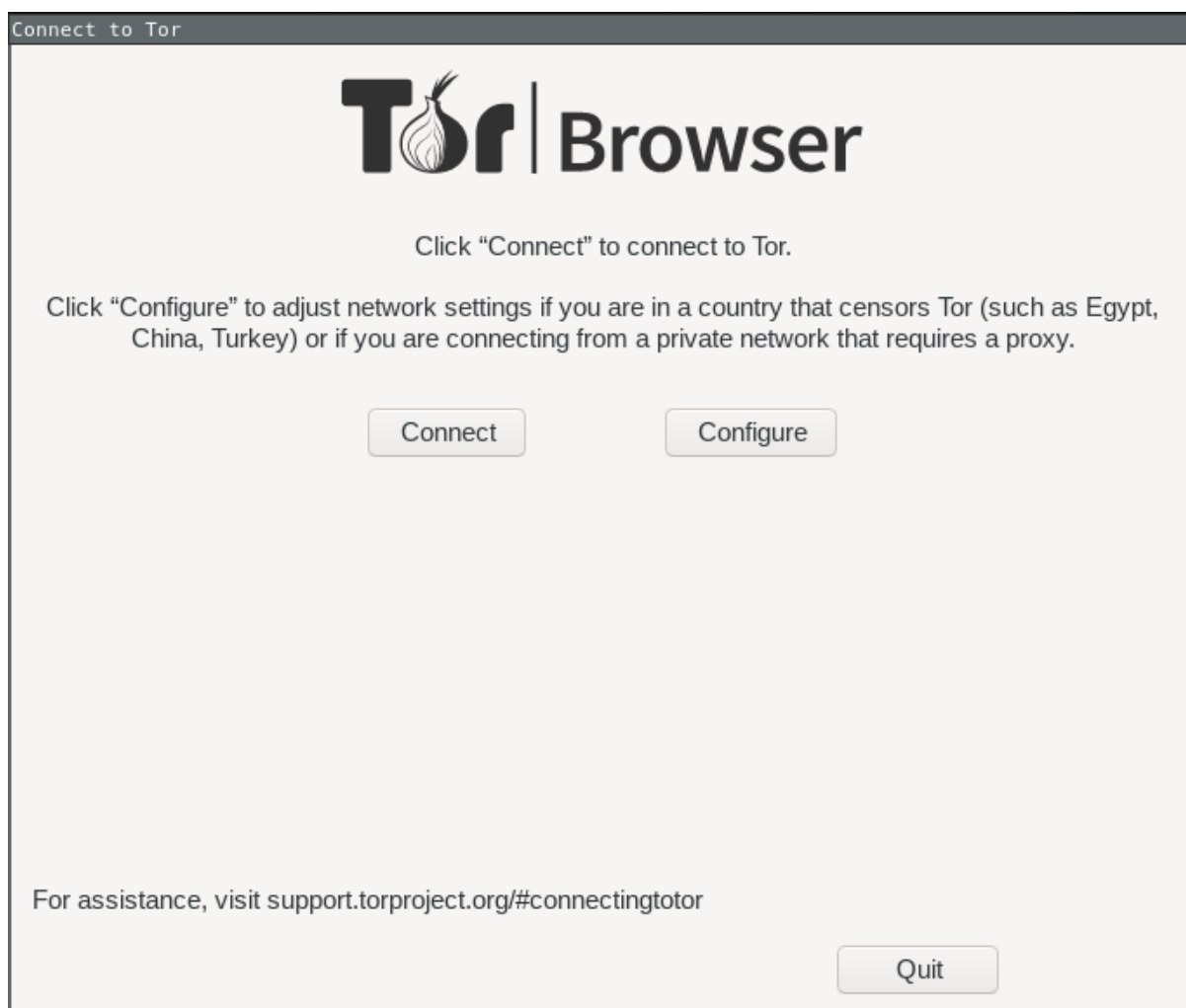




اگر مرورگر تور در مرحله اتصال به شبکه قفل شد و اتصال به شبکه موفقیت آمیز نبود به احتمال خیلی زیاد شرکتی که ارتباط اینترنتی شما را فراهم می کند، ارتباط با شبکه تور را سانسور می کند. برای رفع این مشکل می توانید از Tor Bridges استفاده کنید. این نودها در واقع Relay های معمولی شبکه تور هستند که به صورت عمومی اعلام نشده اند و امکان سانسور آنها برای شرکت های اینترنتی دشوارتر است.

اتصال در شرایطی که ارتباط با شبکه تور سانسور شده است

در صفحه‌ای که مرورگر تور تلاش می‌کند به شبکه وصل شود دکمه Cancel را بزنید تا به این پنجره منتقل شوید.



گزینه سانسور بودن شبکه تور را انتخاب کنید

Tor Network Settings

Tor is censored in my country

Select a built-in bridge [?](#) obfs4 ▼

Request a bridge from torproject.org

Provide a bridge I know

I use a proxy to connect to the Internet [?](#)

For assistance, visit [support.torproject.org/#connectingtotor](https://support.torproject.org/#connectingtotor)

Quit Back Connect

پروتکل obfs4 را انتخاب کنید و دکمه Connect را بزنید.

اگر اتصال همچنان موفقیت آمیز نبود دوباره به صفحه قبل بازگردید. اگر VPN دارید آن را روشن کنید و گزینه دوم را انتخاب کنید، دکمه Request a Bridge را بزنید و مراحل را پیش بروید.

Tor Network Settings

Tor is censored in my country

Select a built-in bridge ?

Request a bridge from torproject.org

Request a Bridge...

Provide a bridge I know

I use a proxy to connect to the Internet ?

For assistance, visit [support.torproject.org/#connectingtotor](https://support.torproject.org/#connectingtotor)

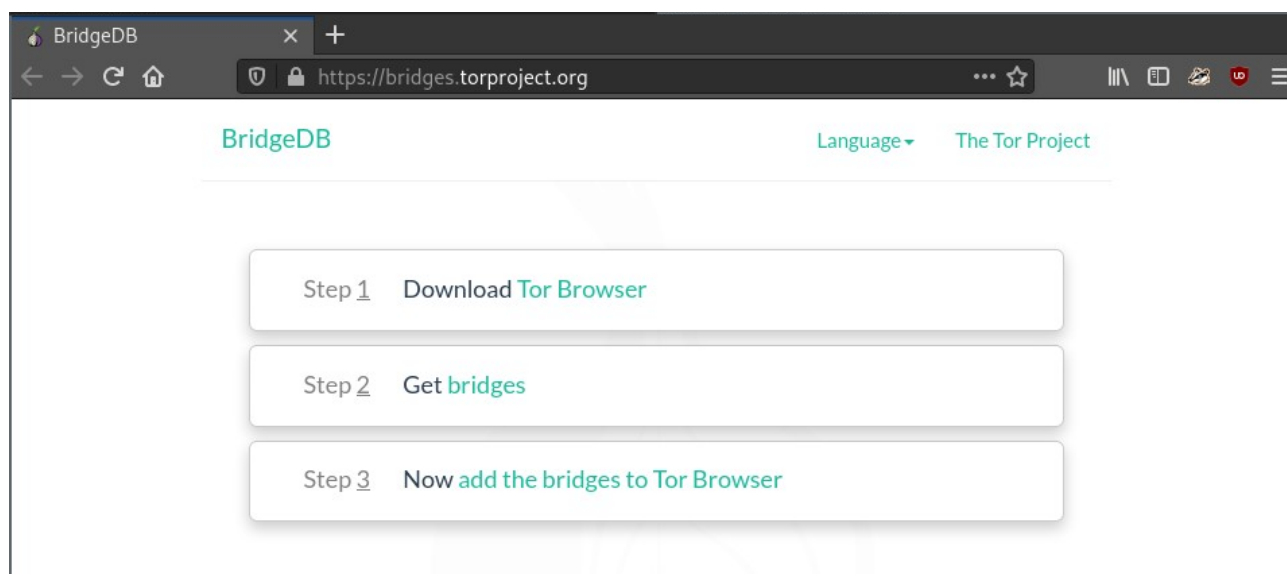
Quit Back Connect

اگر اتصال موفقیت آمیز بود، مرورگر تور را ببندید. بعد VPN را خاموش کنید و دوباره مرورگر تور را باز کنید و اتصال را تست کنید.

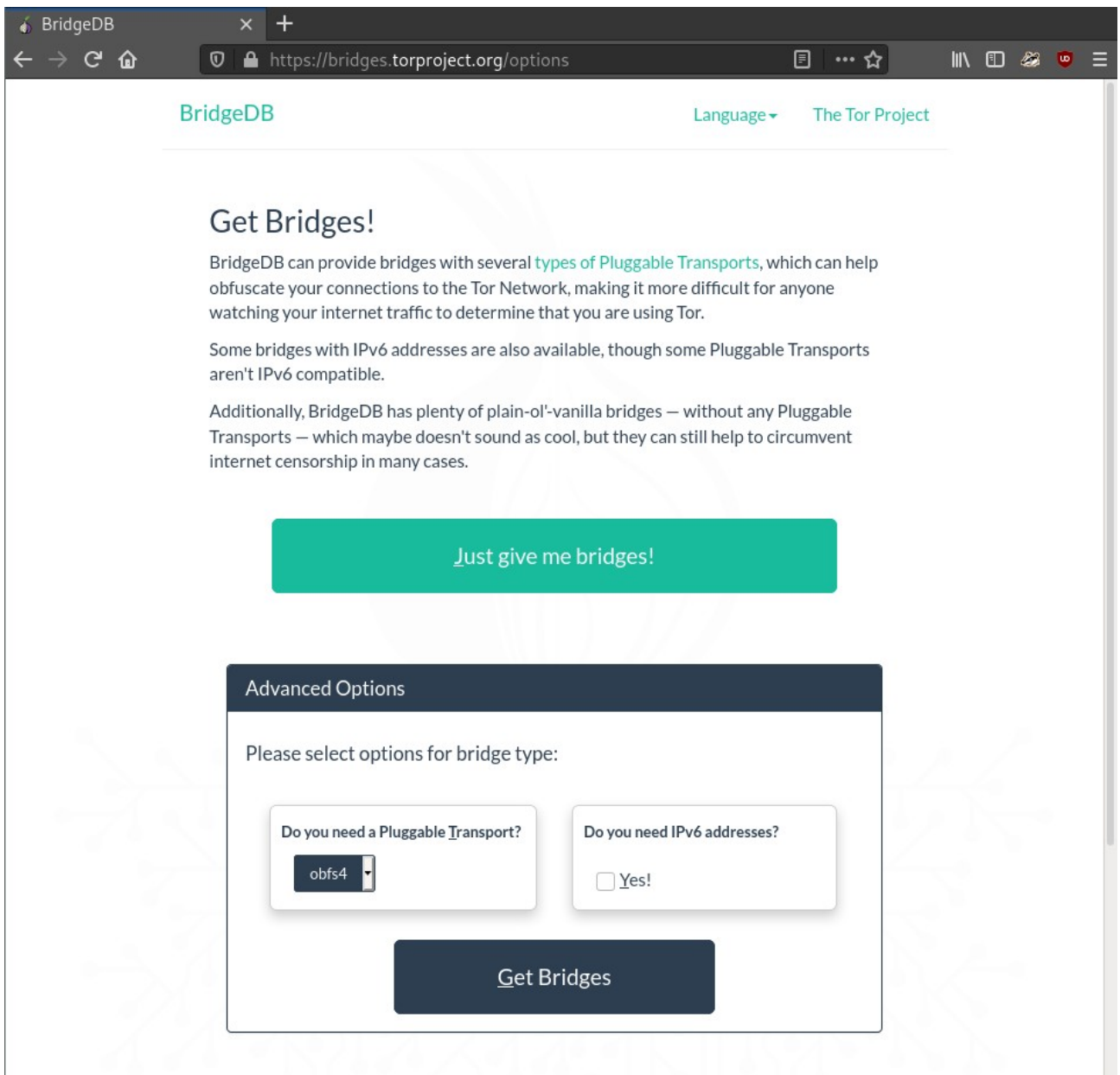
اگر همچنان اتصال به شبکه موفقیت آمیز نبود دوباره به صفحه اول برگردید. VPN را روشن کنید و با یک مرورگر به آدرس زیر بروید

<https://bridges.torproject.org>

مراحل را به شکلی که در ادامه نشان داده شده است جلو بروید و آدرس‌هایی که به شما داده می‌شود را کپی و دوباره در صفحه اتصال مرورگر تور وارد کنید.



## در قسمت Advanced Options روی دکمه Get Bridges کلیک کنید



The screenshot shows a web browser window with the URL `https://bridges.torproject.org/options`. The page title is "BridgeDB" and it includes a "Language" dropdown and "The Tor Project" link. The main heading is "Get Bridges!". Below this, there is explanatory text about Pluggable Transports and IPv6 compatibility. A large green button labeled "Just give me bridges!" is present. Below that, a dark blue "Advanced Options" panel is shown, containing the text "Please select options for bridge type:". This panel has two input fields: "Do you need a Pluggable Transport?" with a dropdown menu set to "obfs4", and "Do you need IPv6 addresses?" with an unchecked checkbox labeled "Yes!". At the bottom of the panel is a dark blue button labeled "Get Bridges".

BridgeDB

Language The Tor Project

### Get Bridges!

BridgeDB can provide bridges with several [types of Pluggable Transports](#), which can help obfuscate your connections to the Tor Network, making it more difficult for anyone watching your internet traffic to determine that you are using Tor.

Some bridges with IPv6 addresses are also available, though some Pluggable Transports aren't IPv6 compatible.

Additionally, BridgeDB has plenty of plain-ol'-vanilla bridges — without any Pluggable Transports — which maybe doesn't sound as cool, but they can still help to circumvent internet censorship in many cases.

[Just give me bridges!](#)

**Advanced Options**

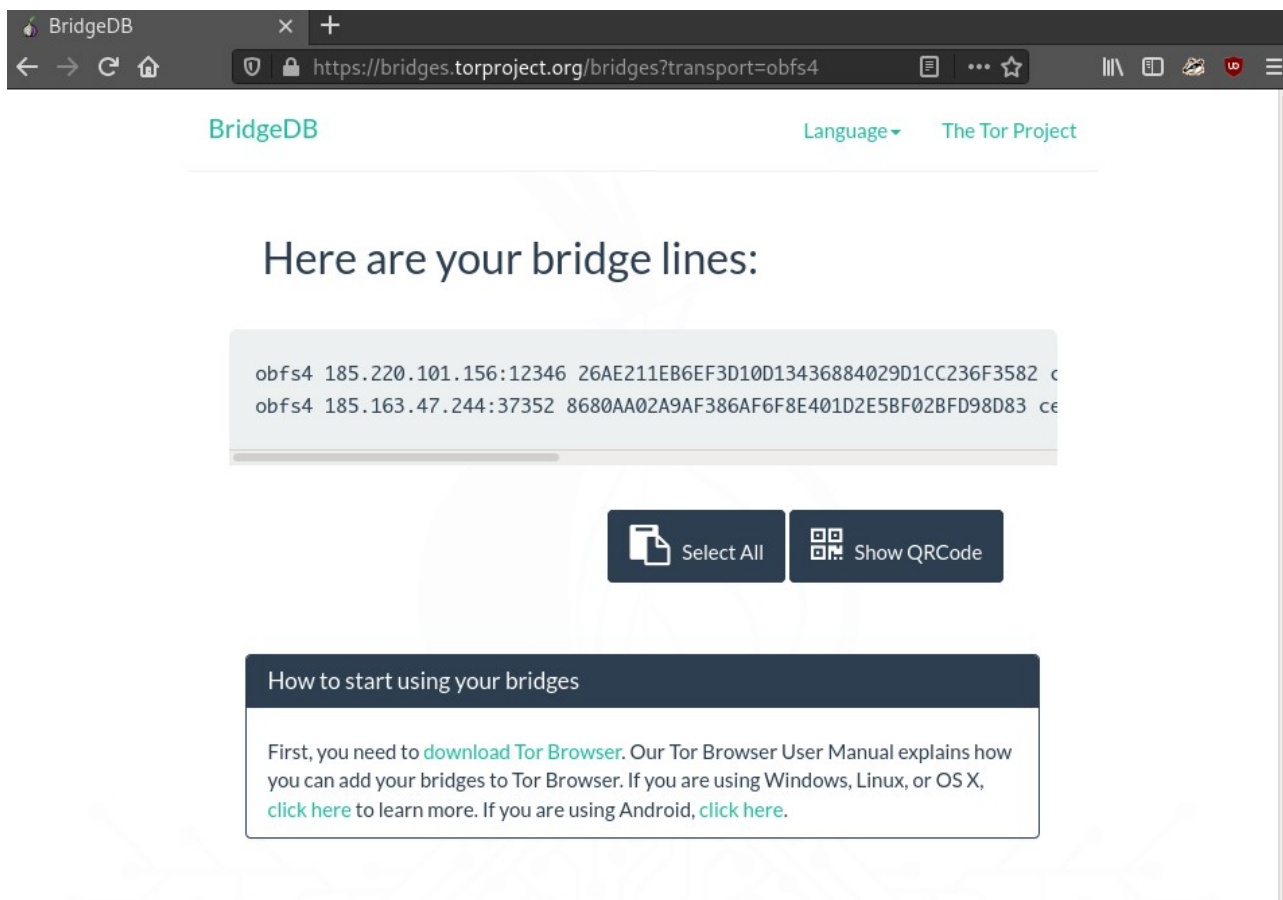
Please select options for bridge type:

Do you need a Pluggable Transport?  
obfs4

Do you need IPv6 addresses?  
 Yes!

[Get Bridges](#)

کپچا را حل کنید تا به لیست آدرسهای Bridge برسید.



The screenshot shows the BridgeDB website interface. At the top, there is a navigation bar with "BridgeDB" on the left, "Language" with a dropdown arrow in the center, and "The Tor Project" on the right. Below the navigation bar, the main heading reads "Here are your bridge lines:". Underneath this heading, there is a light gray box containing two lines of bridge identifiers: "obfs4 185.220.101.156:12346 26AE211EB6EF3D10D13436884029D1CC236F3582 c" and "obfs4 185.163.47.244:37352 8680AA02A9AF386AF6F8E401D2E5BF02BFD98D83 ce". Below the bridge lines, there are two dark blue buttons: "Select All" with a document icon and "Show QRCode" with a QR code icon. At the bottom of the screenshot, there is a dark blue box with the title "How to start using your bridges" and a paragraph of text: "First, you need to [download Tor Browser](#). Our Tor Browser User Manual explains how you can add your bridges to Tor Browser. If you are using Windows, Linux, or OS X, [click here](#) to learn more. If you are using Android, [click here](#)."

لیست آدرسها را کپی کنید



و در قسمت گزینه سوم وارد کنید

Tor Network Settings

Tor is censored in my country

Select a built-in bridge ?

Request a bridge from torproject.org

Provide a bridge I know

Enter bridge information from a trusted source.

```
obfs4 185.220.101.156:12346 26AE211EB6EF3D10D13436884029D1CC236F3582 cē  
obfs4 185.163.47.244:37352 8680AA02A9AF386AF6F8E401D2E5BF02BFD98D83 cē
```

I use a proxy to connect to the Internet ?

For assistance, visit [support.torproject.org/#connectingtotor](https://support.torproject.org/#connectingtotor)

اتصال به VPN را خاموش کنید و دوباره دکمه Connect را بزنید.

اگر دسترسی به VPN ندارید می‌توانید با ارسال یک ایمیل به آدرس

[bridges@torproject.org](mailto:bridges@torproject.org)

و خالی گذاشتن قسمت موضوع ایمیل و نوشتن عبارت زیر در متن ایمیل

get transport obfs4

آدرس‌های bridge را دریافت کنید.

## What are bridges?

**Bridges** are Tor relays that help you circumvent censorship.

## I need an alternative way of getting bridges!

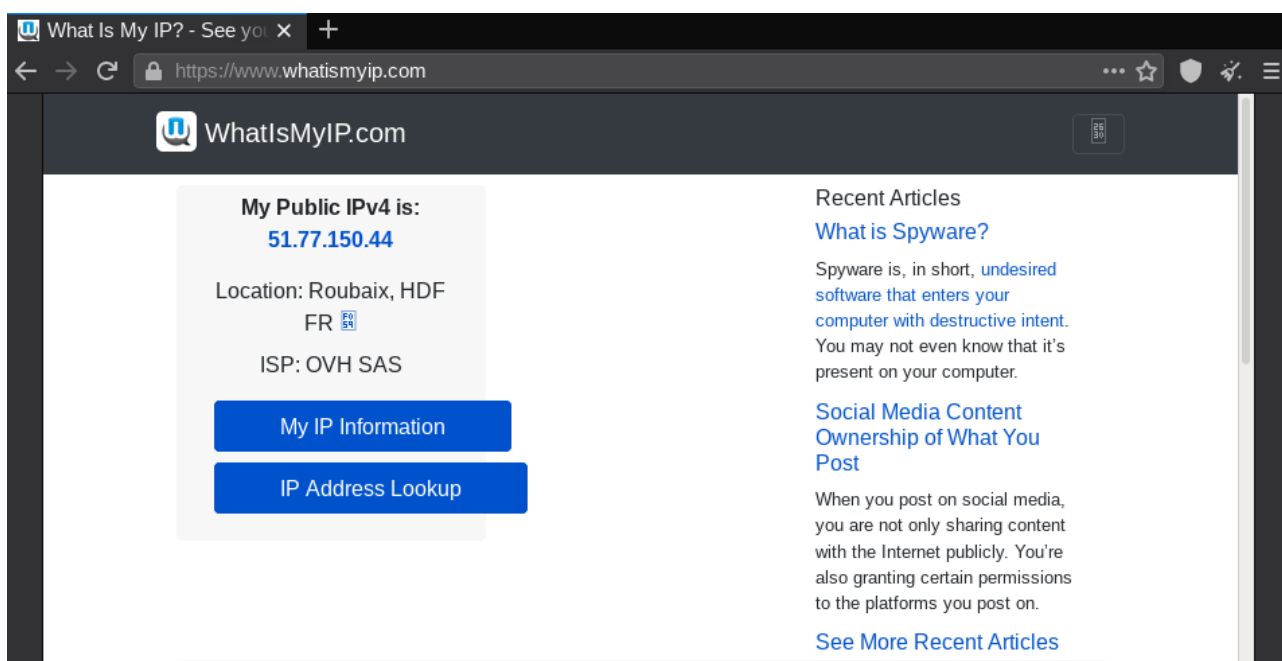
Another way to get bridges is to send an email to [bridges@torproject.org](mailto:bridges@torproject.org). Leave the email subject empty and write "get transport obfs4" in the email's message body. Please note that you must send the email using an address from one of the following email providers: [Riseup](#) or [Gmail](#).

اثر استفاده از مرورگر تور بر موقعیت مکانی اعلام شده به شبکه اینترنت

بعد از اتصال می‌توانید مرورگر تور و نحوه کار آن را با مشاهده IP خود در اینترنت تست کنید.

برای این کار با مرورگر تور و همزمان با مرورگر فایرفاکس یا کروم خود به سایت [whatismyip.com](https://www.whatismyip.com) بروید و IP های اعلام شده را با هم مقایسه کنید.

سؤال برای خوانندگان: IP که مرورگر تور به شما نشان می‌دهد در واقع متعلق به کدام نود در شبکه تور است؟



The screenshot shows a web browser window with the URL <https://www.whatismyip.com>. The page displays the following information:

- My Public IPv4 is:** 51.77.150.44
- Location:** Roubaix, HDF FR
- ISP:** OVH SAS

There are two blue buttons: "My IP Information" and "IP Address Lookup".

**Recent Articles**

- What is Spyware?**  
Spyware is, in short, **undesired software that enters your computer with destructive intent.** You may not even know that it's present on your computer.
- Social Media Content Ownership of What You Post**  
When you post on social media, you are not only sharing content with the Internet publicly. You're also granting certain permissions to the platforms you post on.

[See More Recent Articles](#)

## سرویس‌های لایه‌ای<sup>۱۵</sup> چیستند و چگونه می‌توان با مرورگر تور به آن‌ها دسترسی پیدا کرد

ویژگی این سرویس‌ها این است که فقط از درون شبکه تور قابل دسترسی هستند. یعنی فقط با مرورگر تور می‌توان به آن‌ها وصل شد. اگر شما یک سرویس لایه‌ای بر روی شبکه تور ایجاد کنید، برای کاربران‌تان امنیت **https** و مزیت‌های مرورگر تور را فراهم خواهید کرد. یکی دیگر از ویژگی‌های بسیار کاربردی این سرویس‌ها این است که شما برای ایجاد یک وب‌سایت نیازی به تهیه یک آی‌پی ایستا<sup>۱۶</sup> نخواهید داشت، چون در داخل شبکه تور از آی‌پی استفاده نمی‌شود. آدرس این وب‌سایت‌ها یا به‌طور کلی سرویس‌ها با عبارت **onion** پایان می‌یابد و برای دسترسی به آن‌ها باید آدرس آن‌ها در مرورگر تور وارد شود. این سایت‌ها در سایت‌های جستجوی اینترنتی مثل گوگل لیست نشده‌اند و دسترسی به آن‌ها فقط از طریق آدرس آن‌ها امکان‌پذیر است.

### کاربرد شبکه تور و سرویس‌های لایه‌ای در کیف پول‌های بیت‌کوین

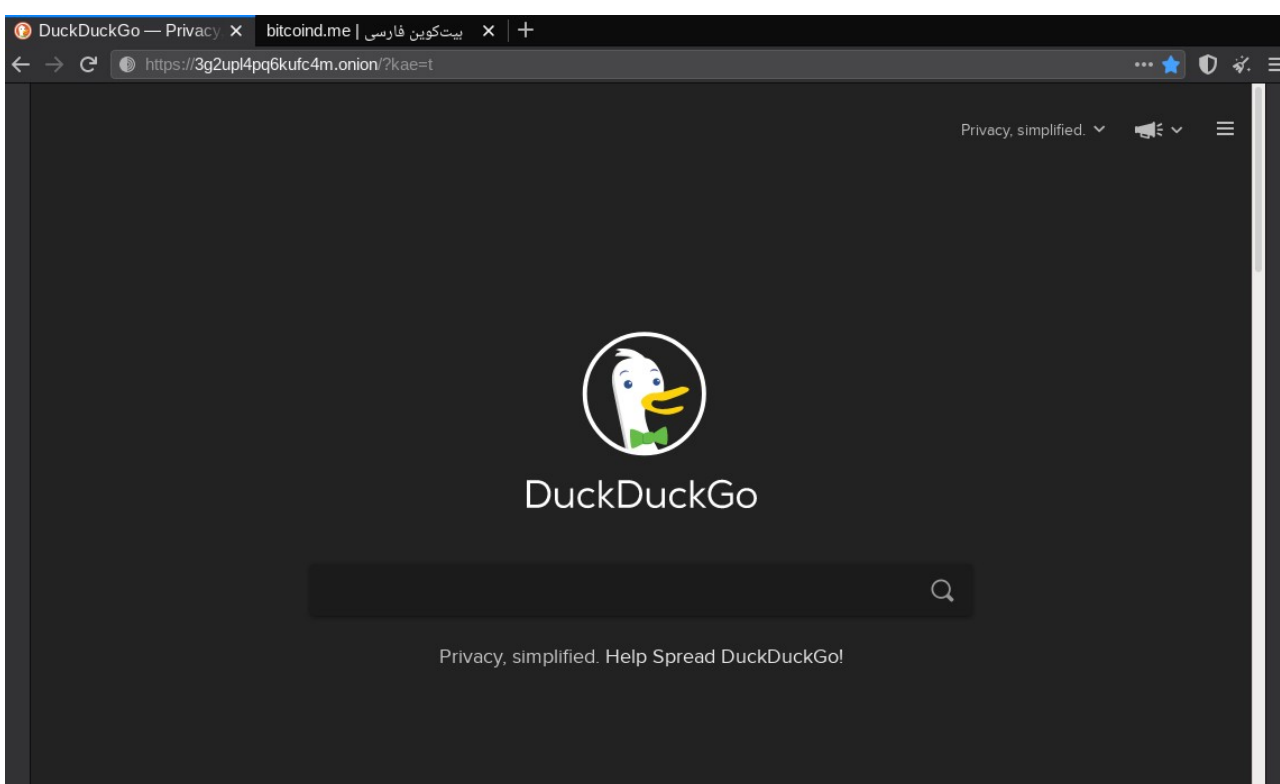
همان‌طور که گفتیم برای ایجاد و اتصال به یک سرویس لایه‌ای در شبکه تور نیازی به یک IP استاتیک نیست. بنابراین اگر شما در منزل یک فول‌نود بیت‌کوین راه‌اندازی کرده باشید می‌توانید کیف پول خود را به راحتی و از طریق شبکه تور در هر کجای دنیا که باشید به فول‌نود خود در منزل وصل کنید.

---

15 Onion Services

16 Static IP

آدرس‌های سرویس‌های **.onion** در دونسخه ارائه می‌شوند. آدرس‌های نسخه ۲ کوتاه‌تر از نسخه ۳ هستند. برای نمونه



[3g2upl4pq6kufc4m.onion](https://3g2upl4pq6kufc4m.onion)

آدرس سایت جستجوی duckduckgo (نسخه ۲)



[bitcoin6djvpbydmvqhdbdb2oai cnp6pbu2kwpcfwpcy2h4v urvjad.onion](https://bitcoin6djvpbydmvqhdbdb2oai cnp6pbu2kwpcfwpcy2h4v urvjad.onion)

آدرس سایت منابع فارسی بیت کوین (نسخه ۳)

## مواردی که باید حین استفاده از مرورگر تور در نظر گرفته شوند

- هرگز با مرورگر تور به سایت‌هایی که در آن‌ها حساب کاربری دارید وارد نشوید. این سایت‌ها برای امنیت حساب شما IP شما را رصد می‌کنند و با توجه به اینکه لیست همه نودهای خروجی برای آن‌ها معلوم است، نسبت به استفاده از مرورگر تور حساسیت دارند. برای مثال اگر با مرورگر تور وارد حساب توئیتر یا جیمیل خود شوید، این سایت‌ها برای محافظت از حساب کاربری شما ممکن است حساب شما را تعلیق کنند.
- مراقب Javascript باشید. این زبان برنامه‌نویسی بر روی مرورگر اجرا می‌شود و امکان لو دادن IP شما را به شبکه بالا می‌برد. حتماً به تنظیمات Security Level مرورگر تور خود توجه کنید.
- مراقب باشید که اغلب دوربین‌های گوشی‌های موبایل اطلاعاتی را به‌عنوان فراداده<sup>۱۷</sup> در فایل عکس ذخیره می‌کنند. یکی از این اطلاعات مربوط به موقعیت مکانی است که عکس در آنجا گرفته شده است. حتماً قبل از ارسال عکس به سایت یا یک فرد دیگر، اطمینان حاصل کنید همه این فراداده‌ها حذف شده باشند.
- سایت‌ها و سرویس‌های لایه‌ای تور در موتورهای جستجو لیست نمی‌شوند و نمی‌توان آن‌ها را سانسور کرد.

## آیا استفاده از مرورگر تور تضمین کننده حریم خصوصی کاربران است

این مسأله همواره در میان طرفداران مباحث حریم خصوصی مورد بحث بوده است. بعضی از افراد معتقدند نهادهای نظارتی دولت‌های قدرتمند دنیا به‌ویژه ایالات متحده توانایی رمزگشایی شبکه تور را در اختیار دارند. حال سؤال این است که آیا این نهادها در مواقع خاصی امکان رمزگشایی دارند یا این امکان در هر زمانی که اراده کنند در اختیار آنها است. از طرف دیگر شبکه تور بارها در مواقع حساس توسط سوت‌زن‌ها<sup>۱۸</sup> و با موفقیت به کار گرفته شده است. برای نمونه ادوارد اسنودن<sup>۱۹</sup> از شبکه تور برای ارسال مدارک به خبرنگاران استفاده کرد و به عقیده طرفداران امنیت شبکه تور، این یعنی امکان کرک این شبکه وجود ندارد.

## آیا خلاف کاران از مرورگر تور و سرویس‌های onion استفاده می‌کنند؟

بله. خلاف کاران معمولاً در استفاده از تکنولوژی‌های جدید از مردم عادی جلوتر هستند. از طریق مرورگر تور می‌توان به بازارهای سیاهی که توسط خلاف کاران ایجاد شده است دسترسی پیدا کرد. در واقع اولین بازار غیرقانونی اینترنتی که از بیت کوین به‌عنوان انتقال ارزش استفاده می‌کرد با نام سیلک‌رود<sup>۲۰</sup> بر روی شبکه تور راه‌اندازی شده بود. گردانندگان این بازارهای غیرقانونی معمولاً بعد از گذشت چند سال از فعالیت‌شان توسط پلیس‌های بین‌المللی شناسایی و دستگیر می‌شوند. اگر به شنیدن داستان‌های پلیسی با تم علوم کامپیوتر و رمزنگاری علاقه‌مندید حتماً شنیدن پادکست داستان‌های دارک‌نت<sup>۲۱</sup> برای شما سرگرم‌کننده و آموزنده خواهد بود.

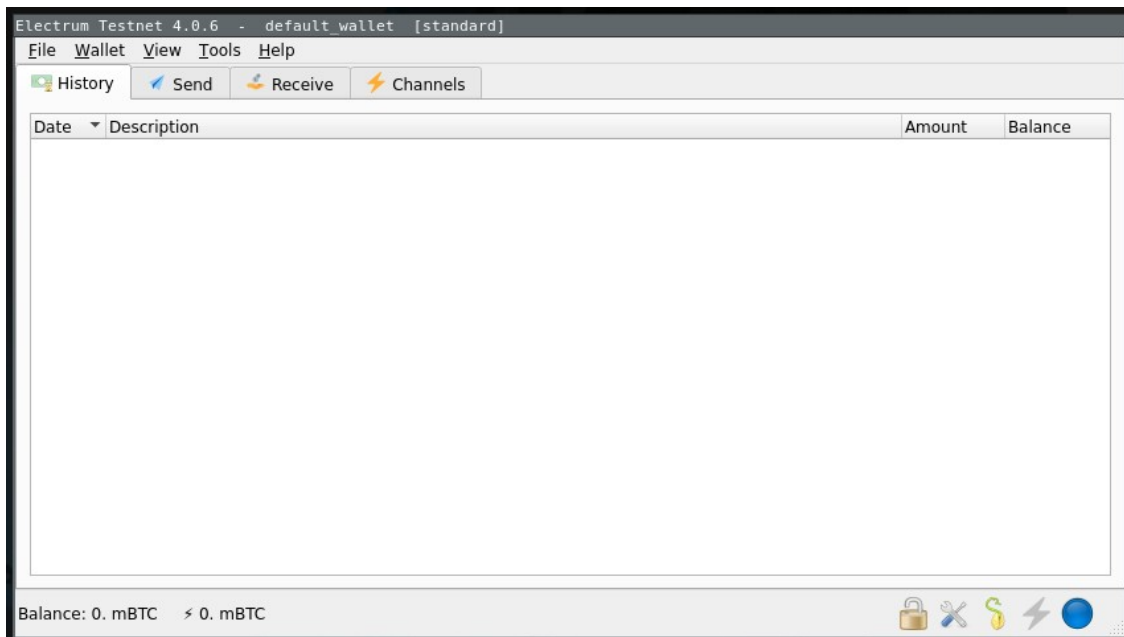
18 Whistleblower

19 Edward Snowden

20 Silk Road

21 Darknet Diaries





راهنمای تصویری اتصال کیف پول الکترام  
به سرورهای عمومی الکترام از طریق سرویس‌های لایه‌ای شبکه تور

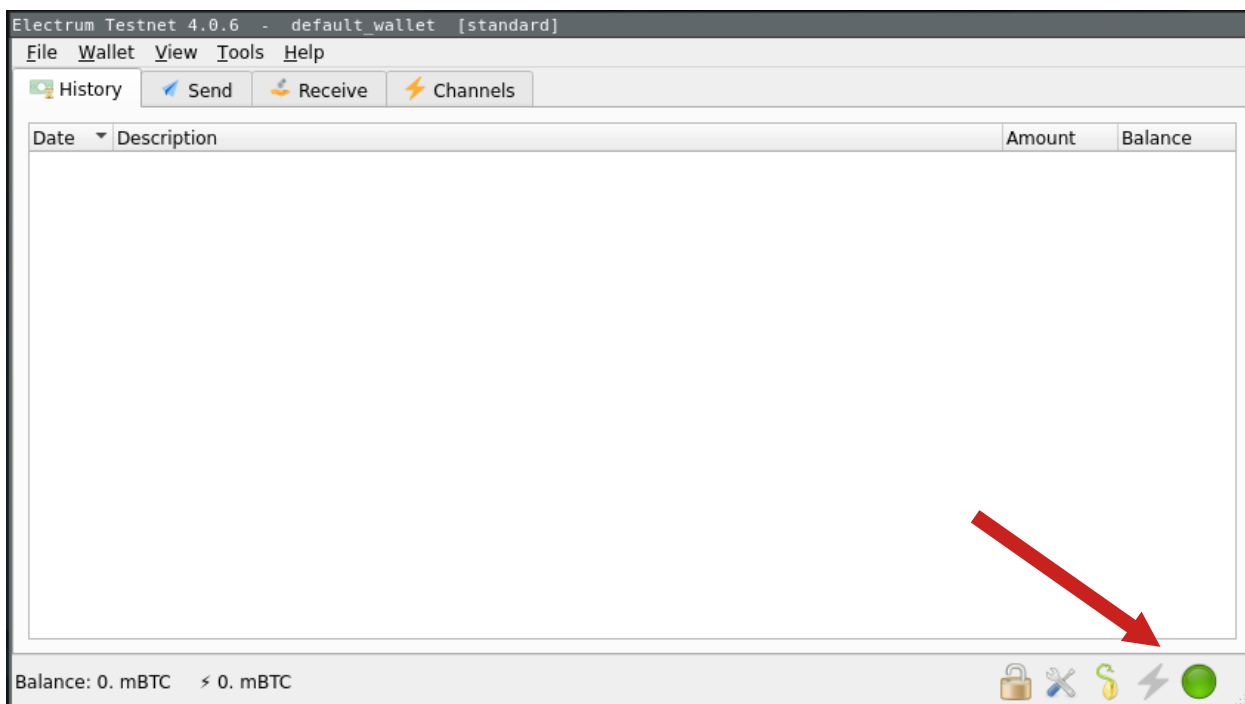
همان‌طور که قبلاً در مورد شبکه تور توضیح دادیم می‌توان از این شبکه برای اتصال ناشناس و ارتقای حریم خصوصی در اینترنت استفاده کرد. شما وقتی برای دریافت لیست تراکنش‌های کیف پول الکترام خود به یکی از سرورهای عمومی الکترام وصل می‌شوید در واقع دو داده خصوصی خود را برای آن‌ها ارسال می‌کنید.

۱. لیست آدرس‌های بیت‌کوین کیف پول خود (از طریق ارسال xpub)

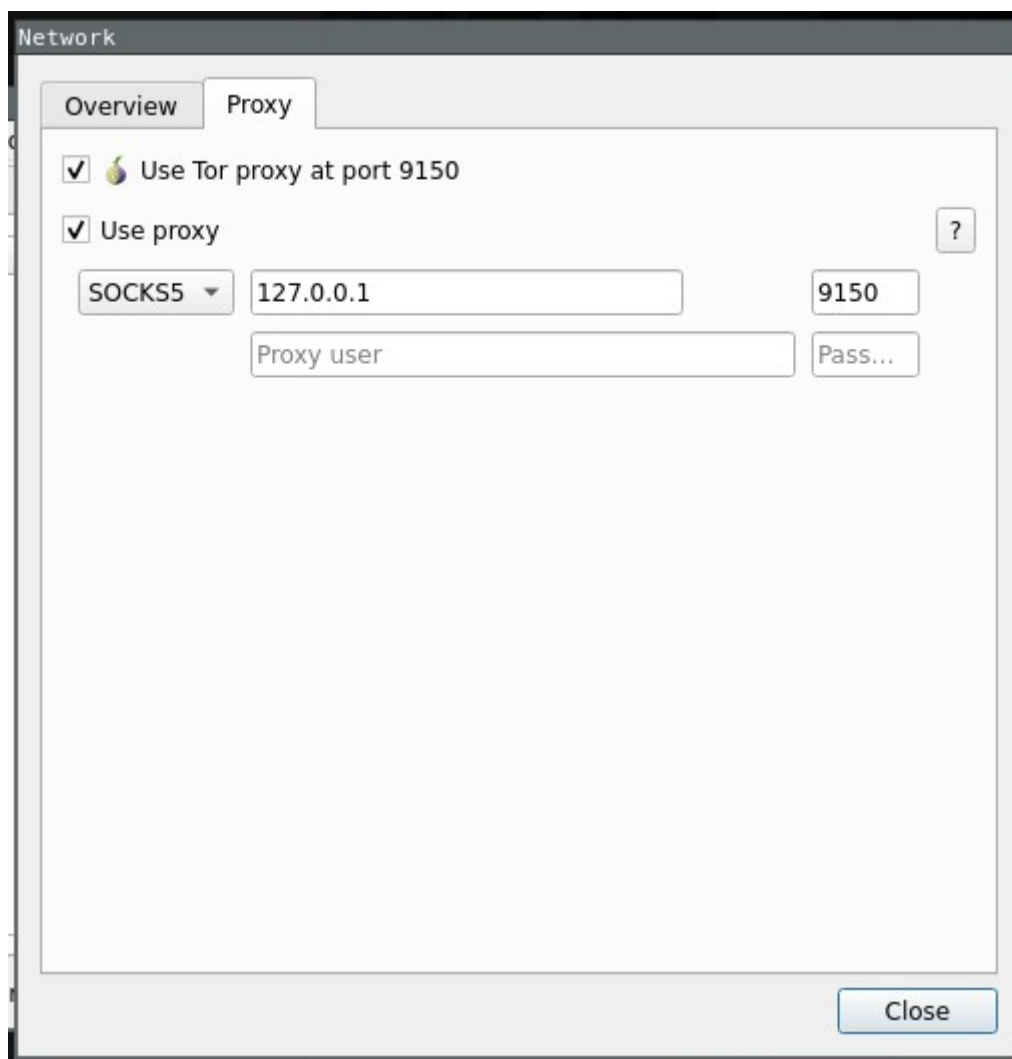
۲. موقعیت تقریبی خود با توجه به معلوم بودن IP شما

مورد اول فقط با راه انداختن یک فول نود شخصی حل می‌شود ولی برای حل مورد دوم می‌توان از شبکه تور استفاده کرد.

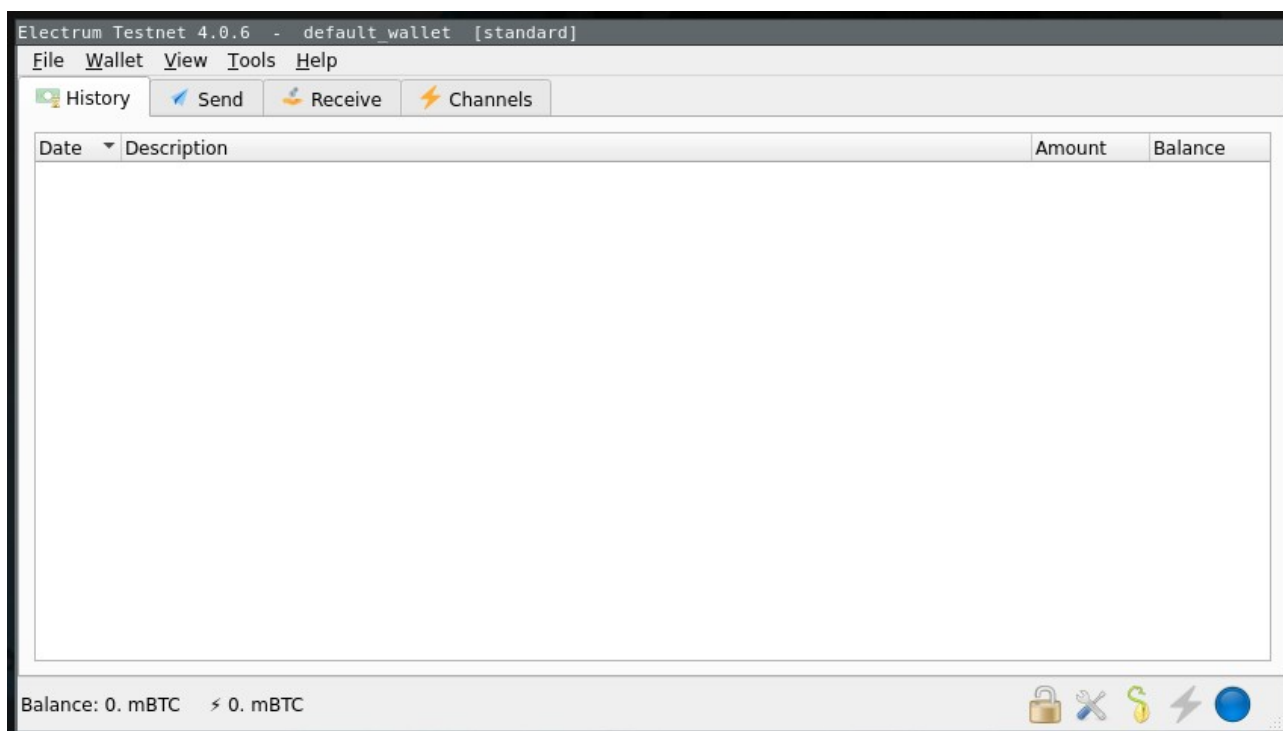
برای اتصال به سرورهای عمومی الکترام از طریق شبکه تور ابتدا مرورگر تور را اجرا کنید و از اتصال موفق آن به شبکه اطمینان حاصل کنید. سپس کیف پول الکترام را اجرا کنید و در بخش پایینی پنجره کیف پول روی آیکون سبز رنگ که نشانگر اتصال به شبکه است کلیک کنید.



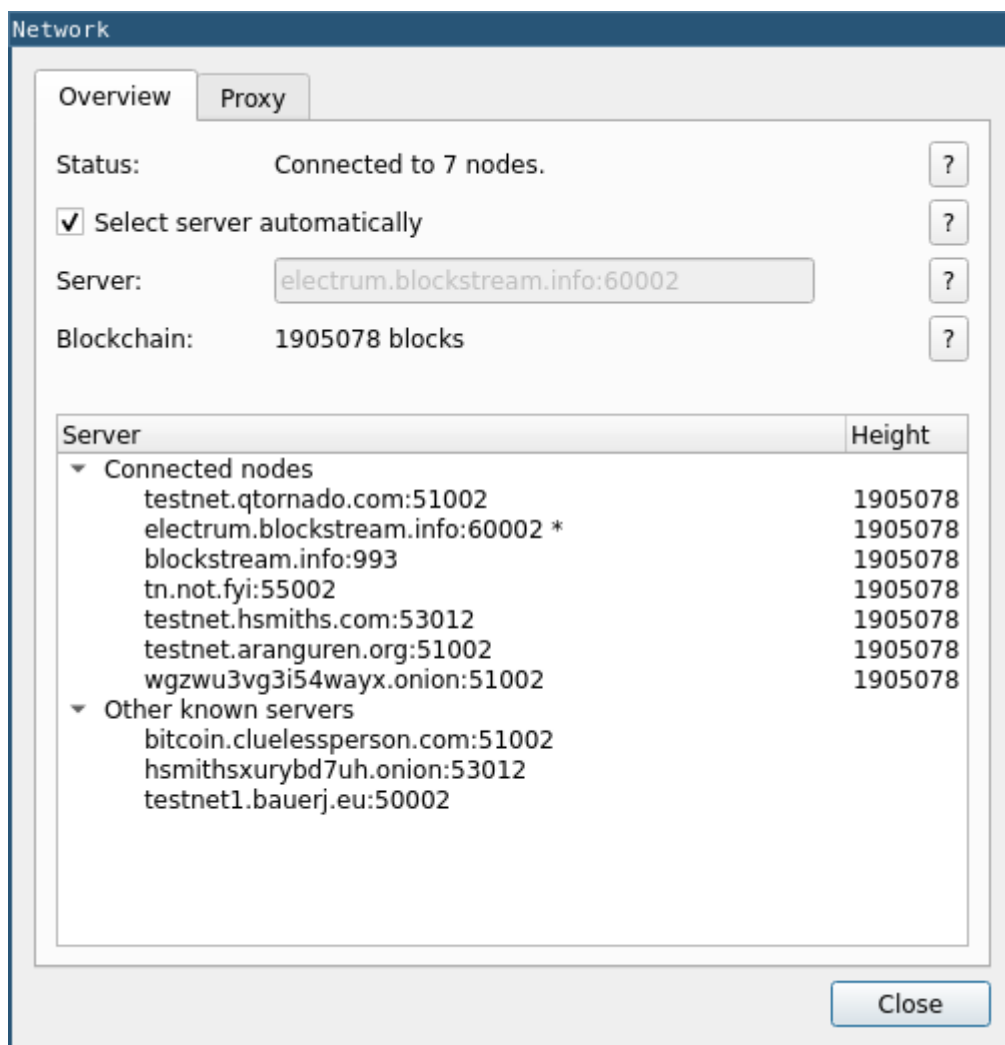
در این پنجره می‌توانید کیف پول الکترا را برای اتصال از طریق شبکه تور تنظیم کنید.  
فقط کافیست روی هر دو باکس کلیک کنید.



در نهایت آیکون اتصال به شبکه به رنگ آبی تغییر رنگ می‌دهد و نشان می‌دهد که شما از طریق شبکه تور به سرورهای عمومی الکترام متصل شده‌اید.



در بخش تنظیمات و سرورهایی که به صورت عمومی در دسترس کاربران هستند به آدرس‌های سرویس‌های `.onion` توجه کنید.



مشاهده می‌کنید که در این لیست آدرس‌های نسخه ۲ `.onion` و آدرس‌های دامین رایج بر پایه IP لیست شده‌اند.

سؤال برای خوانندگان: اتصال به یک سرور که سرویس `.onion` ارائه می‌کند با یک سرور معمولی چه تفاوتی دارد؟

هرگونه استفاده از این خودآموز برای همگان آزاد است.

گردآوری: ر.فرد

بازبینی و صفحه‌بندی: [@bitcoind\\_me](https://bitcoind.me)

زمستان ۱۳۹۹

# bitcoind.me

---

## منابع فارسی بیت‌کوین

معرفی کتاب‌ها، مقالات، خودآموزها، و بطور کلی منابع آموزشی و کاربردی معتبر حوزه بیت‌کوین، اقتصاد، و حریم خصوصی که توسط علاقمندان و فعالان جامعه فارسی‌زبان بیت‌کوین تالیف یا ترجمه شده‌اند