



The Tor Project

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.

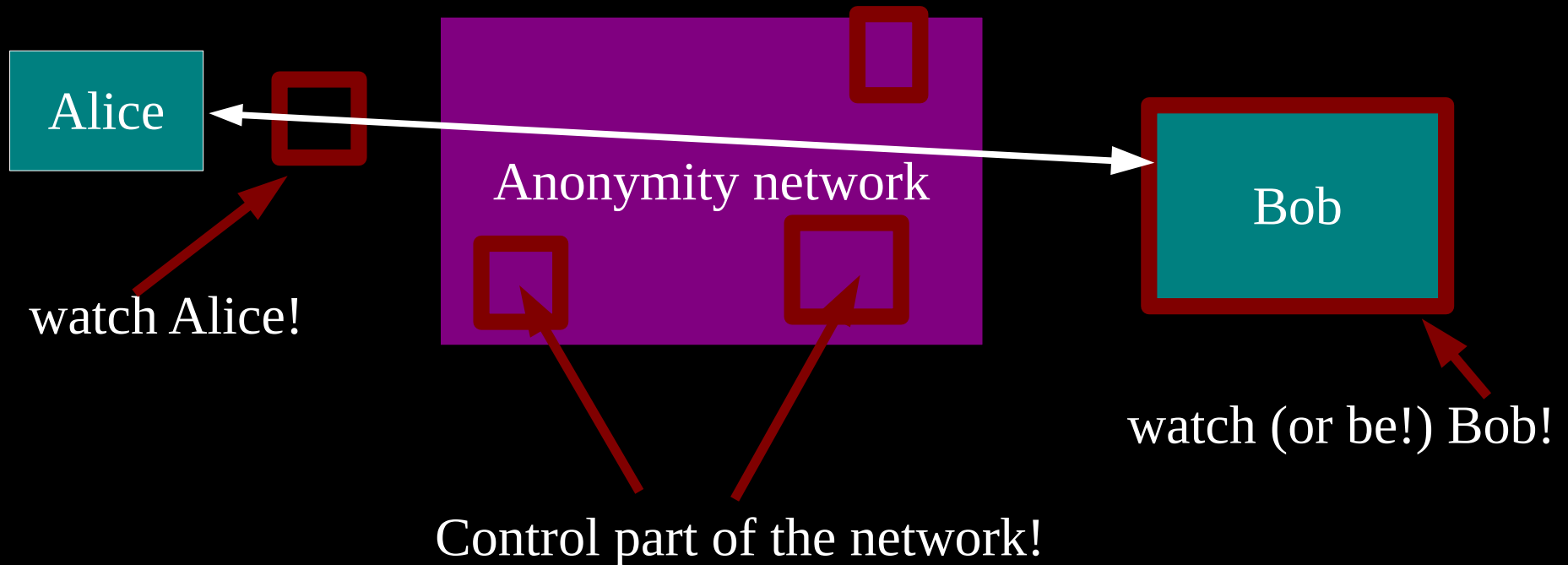


- Online Anonymity
 - Open Source
 - Open Network
- Community of researchers, developers, users and relay operators.
- U.S. 501(c)(3) non-profit organization

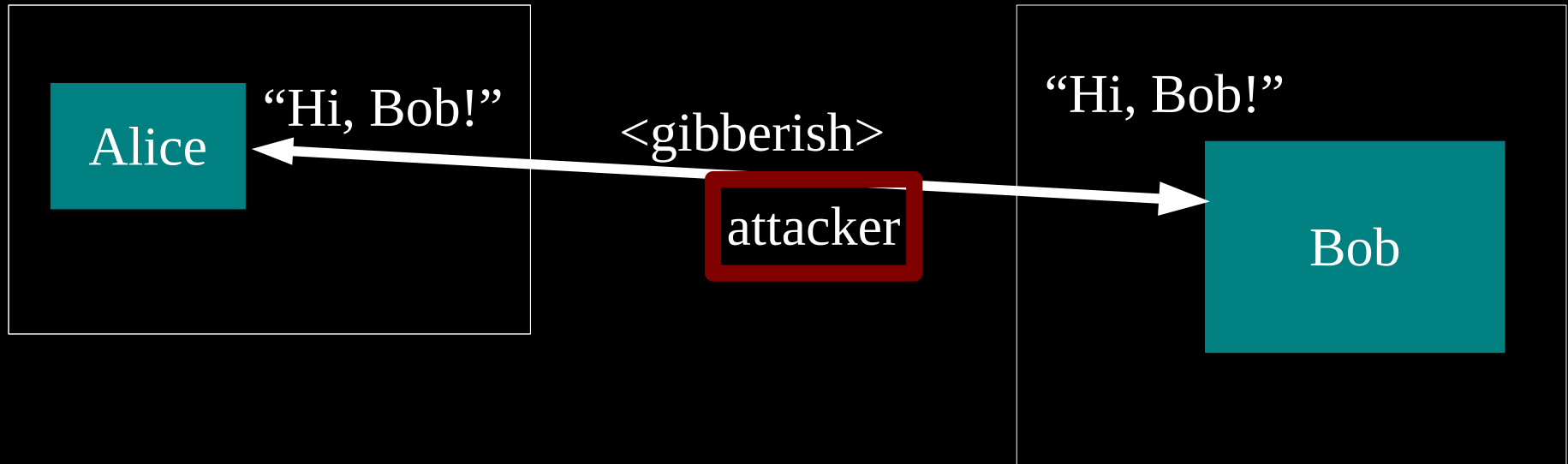
A photograph of a large, empty stadium with many rows of blue seats. The seats are arranged in a semi-circular pattern, and the stadium is completely devoid of people. The lighting is bright, and the overall tone is blue.

Estimated 2,000,000+
daily Tor users

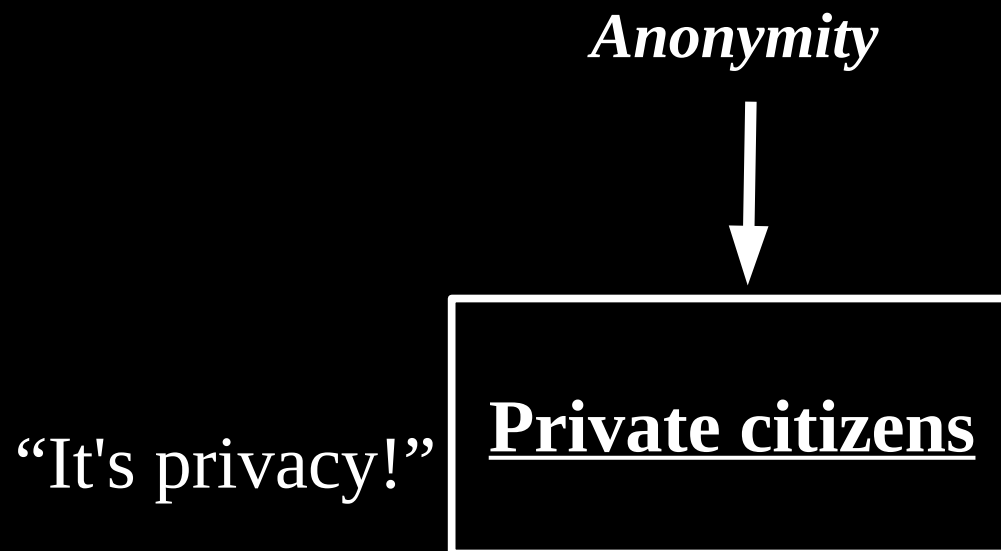
Threat model: what can the attacker do?



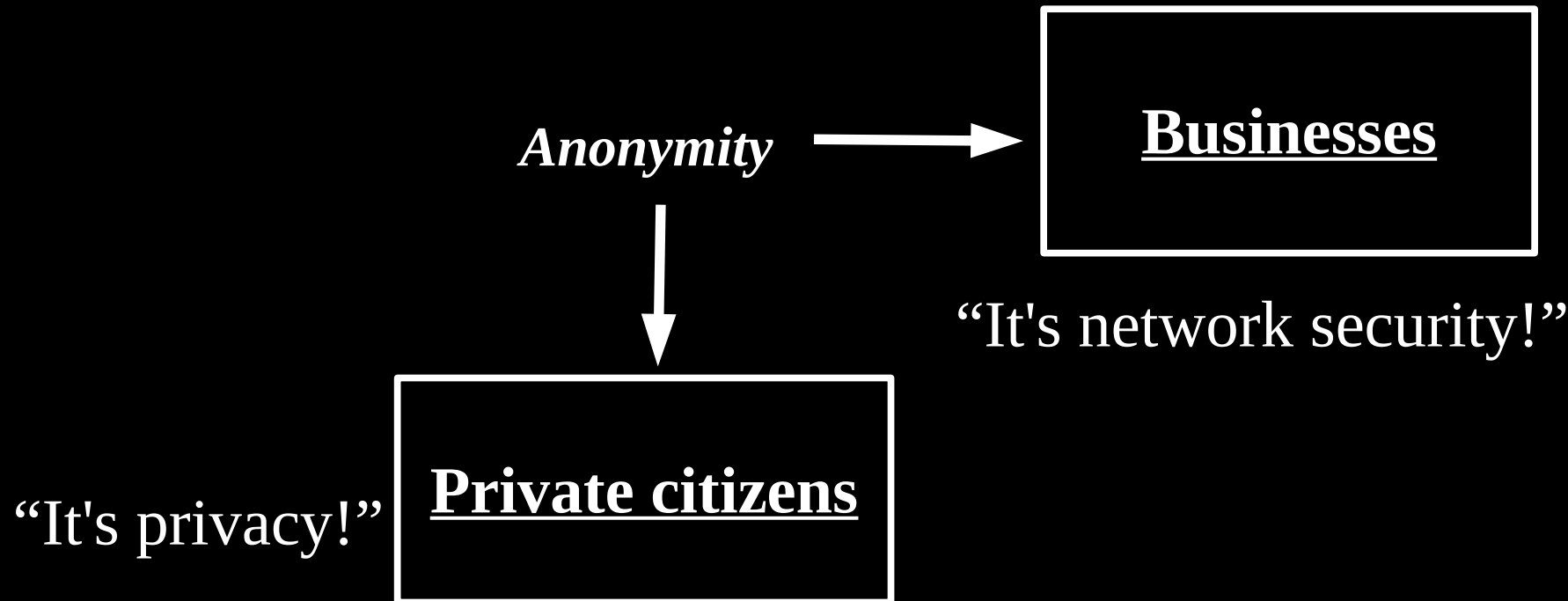
Anonymity isn't encryption: Encryption just protects contents.



Anonymity serves different interests for different user groups.



Anonymity serves different interests for different user groups.



Anonymity serves different interests for different user groups.

“It's traffic-analysis resistance!”



Anonymity

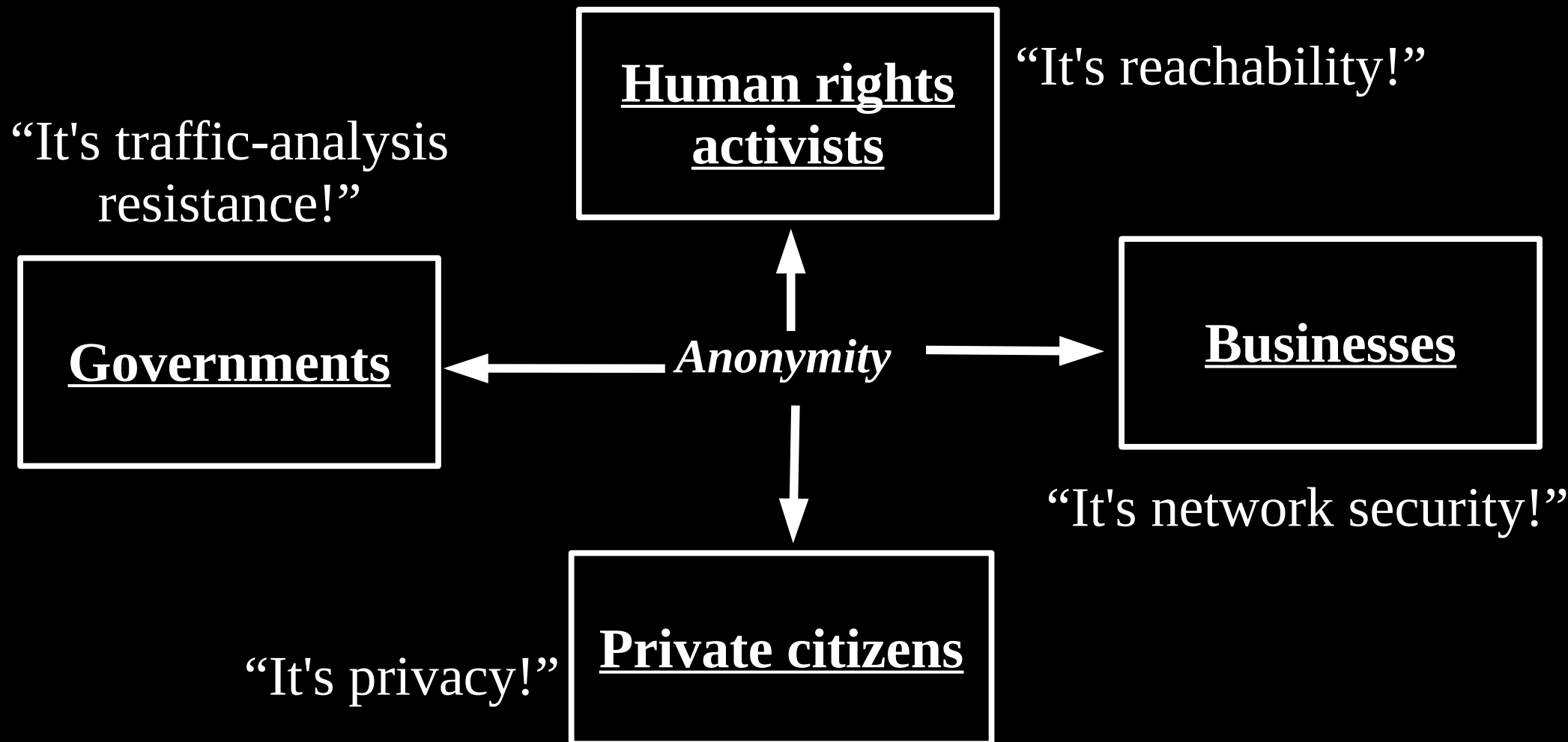


“It's network security!”

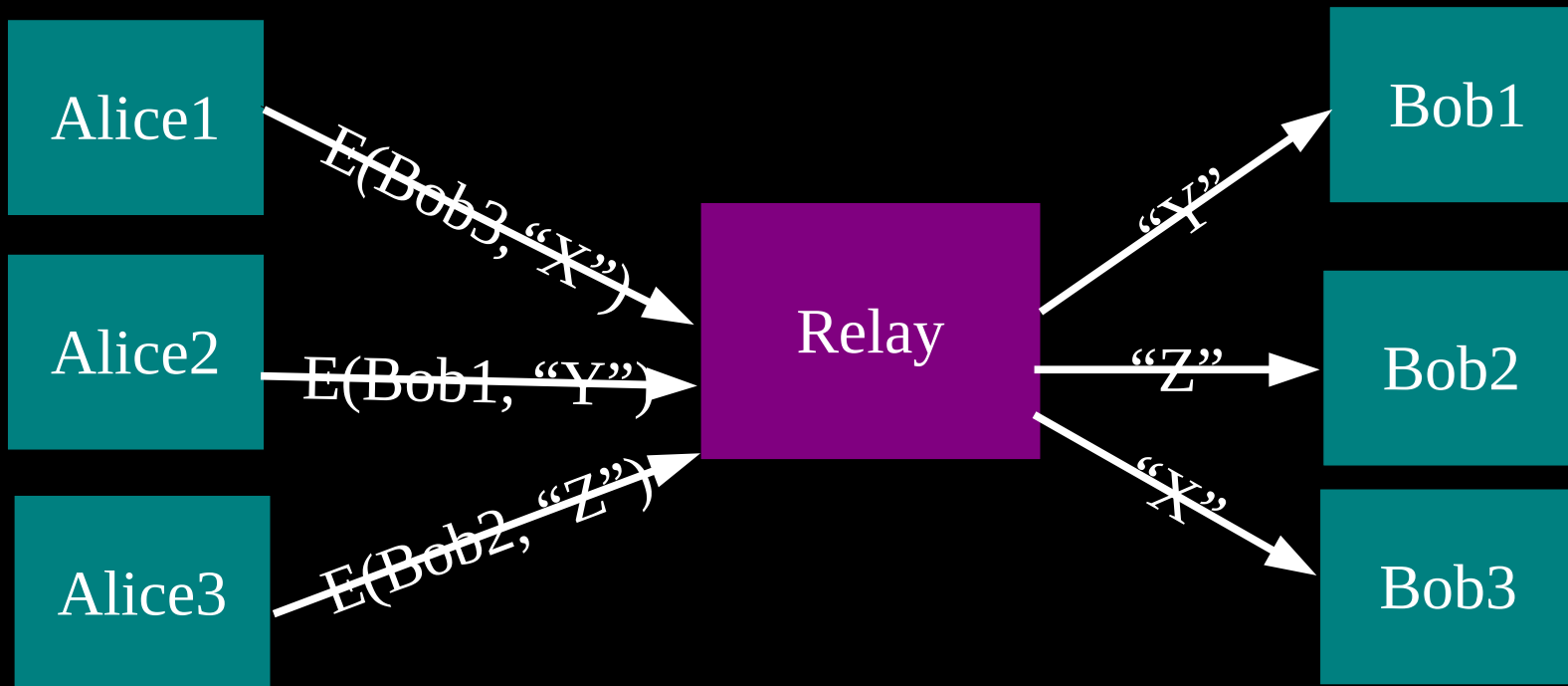
“It's privacy!”



Anonymity serves different interests for different user groups.

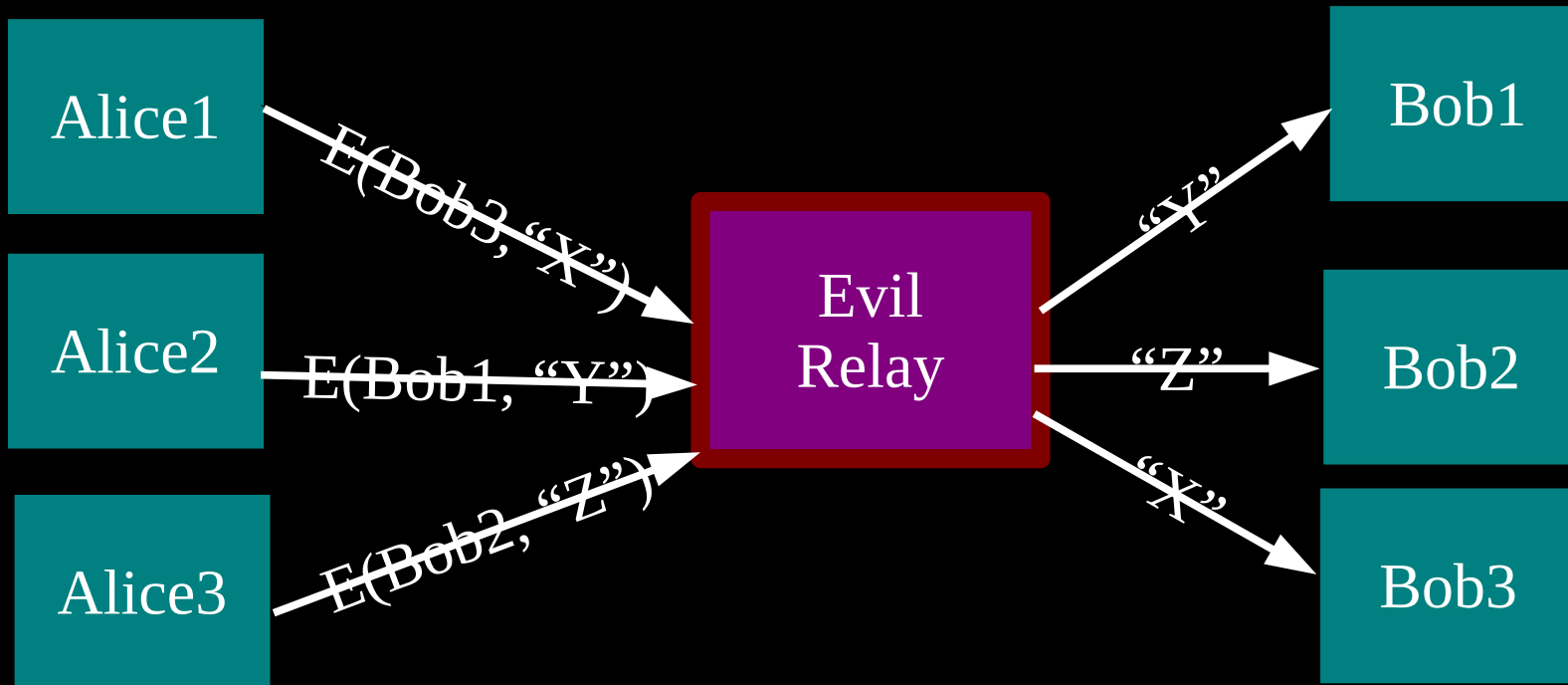


The simplest designs use a single relay to hide connections.

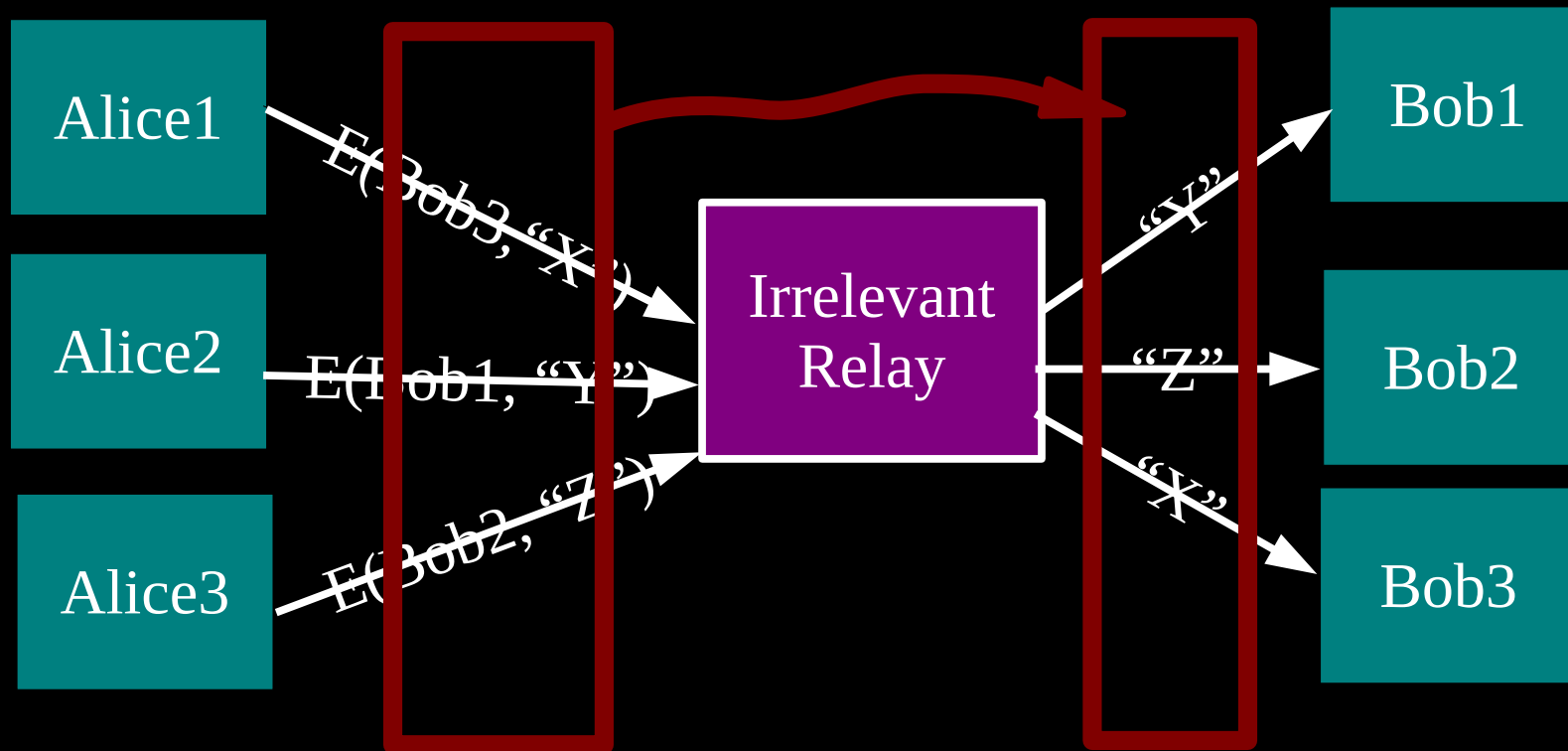


(example: some commercial proxy providers)

**But a central relay is
a single point of failure.**

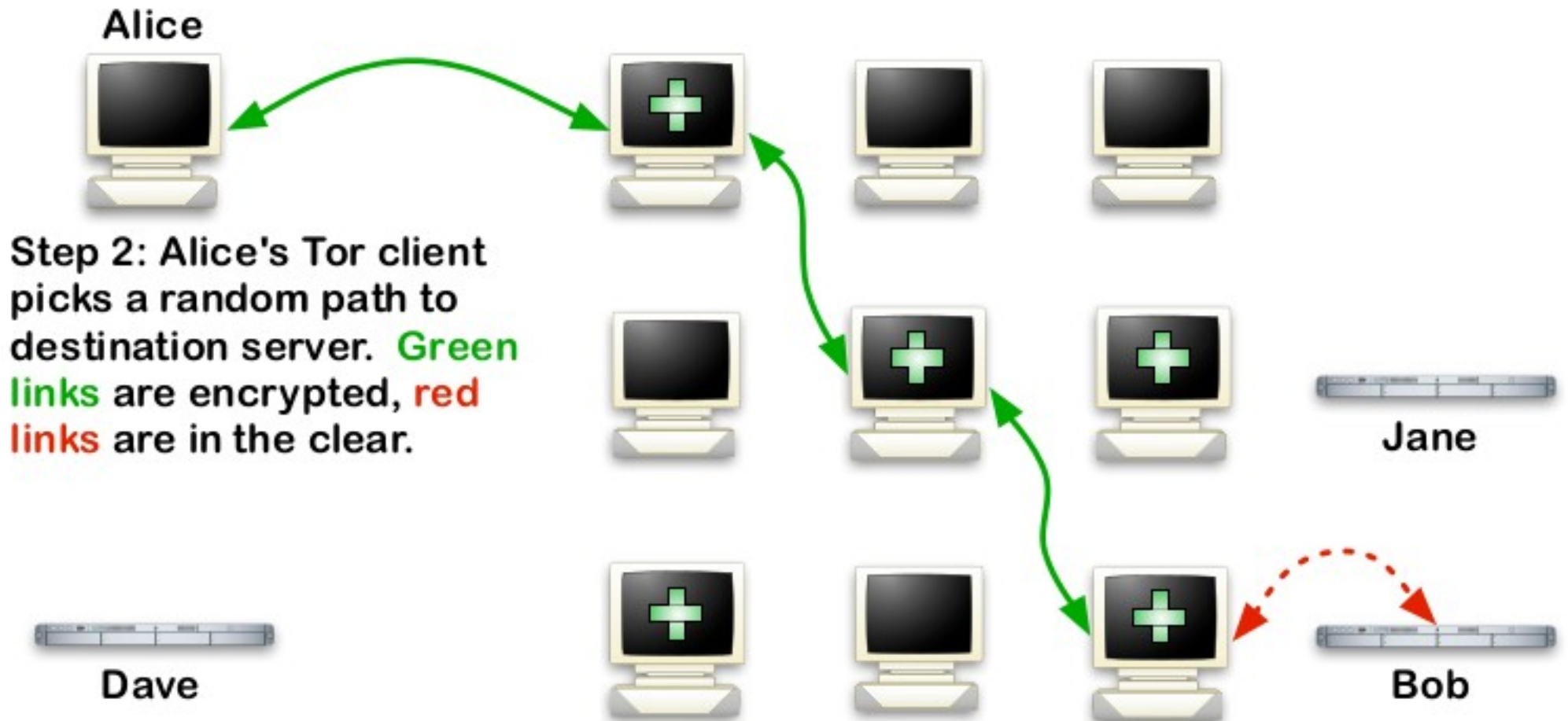
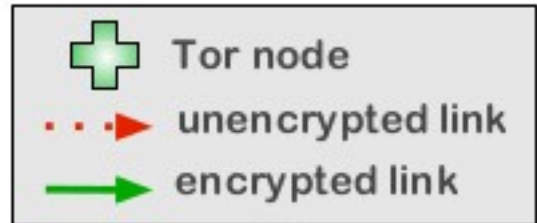


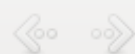
... or a single point of bypass.



Timing analysis bridges all connections through relay \Rightarrow An attractive fat target

EFF How Tor Works: 2





about:tor



Startpage

Tor Browser
3.5-Linux

New Identity

Cookie Protections

Preferences...

About Torbutton...

Open Network Settings...

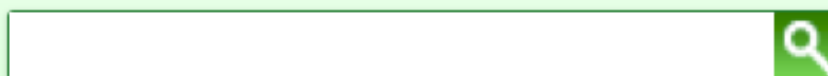


Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)



Search [securely](#) with [Startpage](#).

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

[Tips On Staying Anonymous »](#)

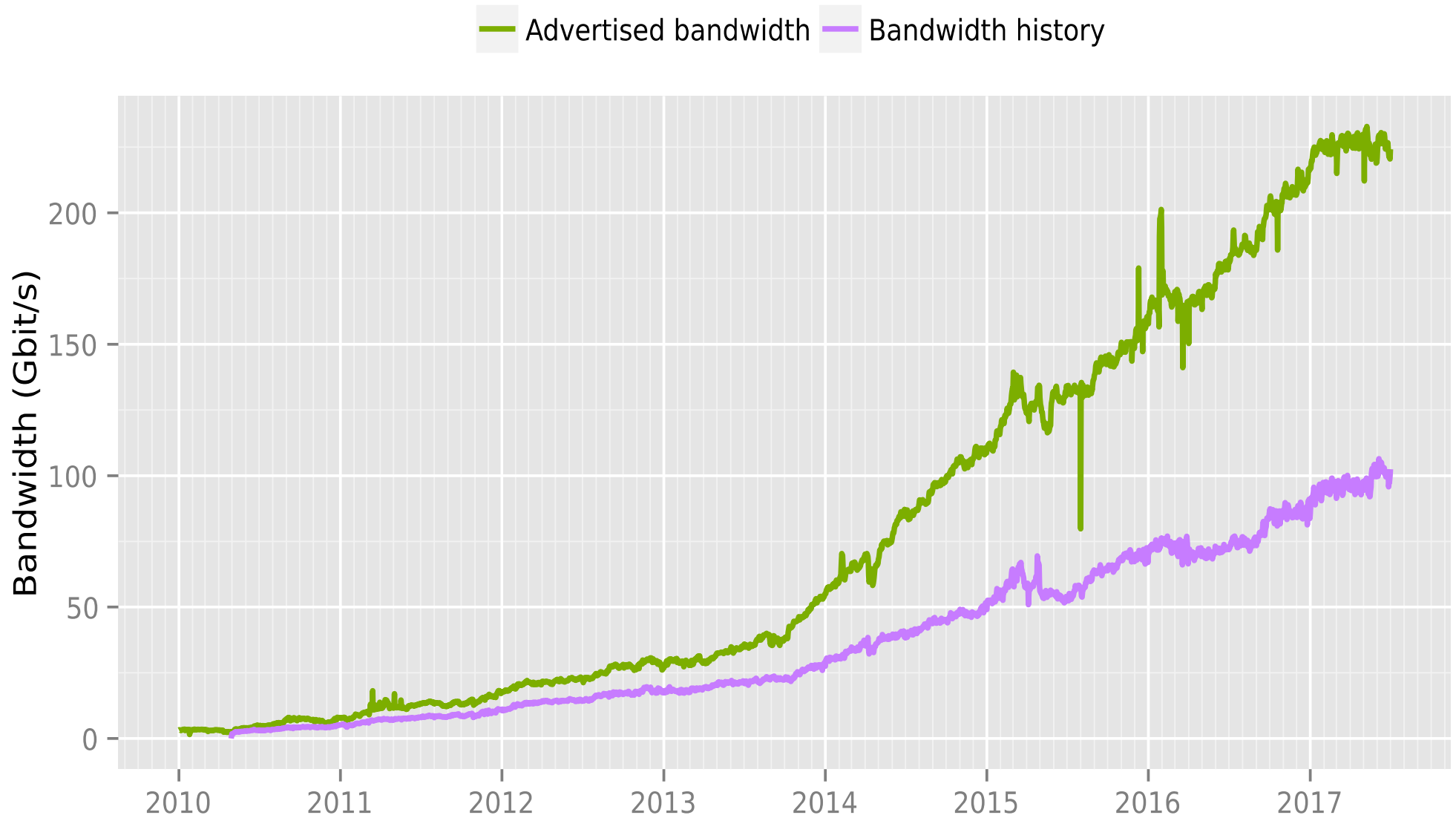
You Can Help!

There are many ways you can help make the Tor Network faster and stronger:

- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)

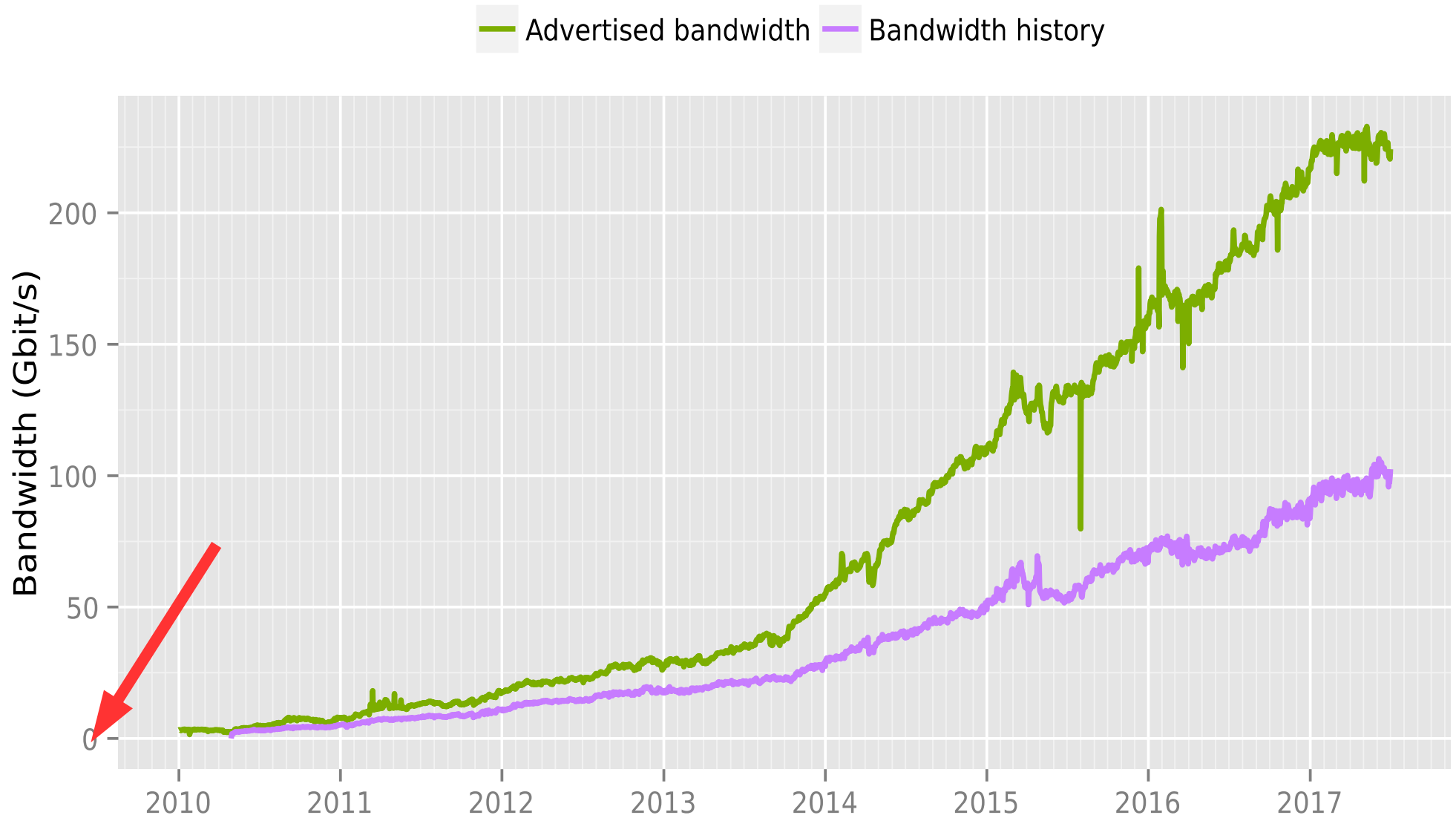
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

Total relay bandwidth



The Tor Project - <https://metrics.torproject.org/>

Total relay bandwidth



The Tor Project - <https://metrics.torproject.org/>

Tor's safety comes from diversity

- #1: Diversity of relays. The more relays we have and the more diverse they are, the fewer attackers are in a position to do traffic confirmation. (Research problem: measuring diversity over time)
- #2: Diversity of users and reasons to use it. 50000 users in Iran means almost all of them are normal citizens.

Transparency for Tor is key

- Open source / free software
- Public design documents and specifications
- Publicly identified developers
- Not a contradiction:
privacy is about choice!

But what about bad people?

- Remember the millions of daily users.
- Still a two-edged sword?
- Good people need Tor much more than bad guys need it.

Myth #1

- “I heard the Navy wrote Tor originally, so how can I trust it?”

Myth #2

- “I heard the NSA runs half the relays.”

Myth #3

- “I heard Tor is slow.”

Myth #4

- “I heard Tor gets most of its money from the US government.”

Myth #5

- “I heard 80% of Tor is bad people.”

Myth #6

- “I shouldn't use Tor, because if I do the NSA will watch me.”

Myth #7

- “I heard Tor is broken.”

riseup.net



cwoiopiifrlzcuos.onion

riseup.net



Welcome to Riseup E

This is the home of the Riseup "Black" services, our new enhanced application.

Important: To avoid possible issues, you will need to create new services. But don't fear, you will be later able to use your current

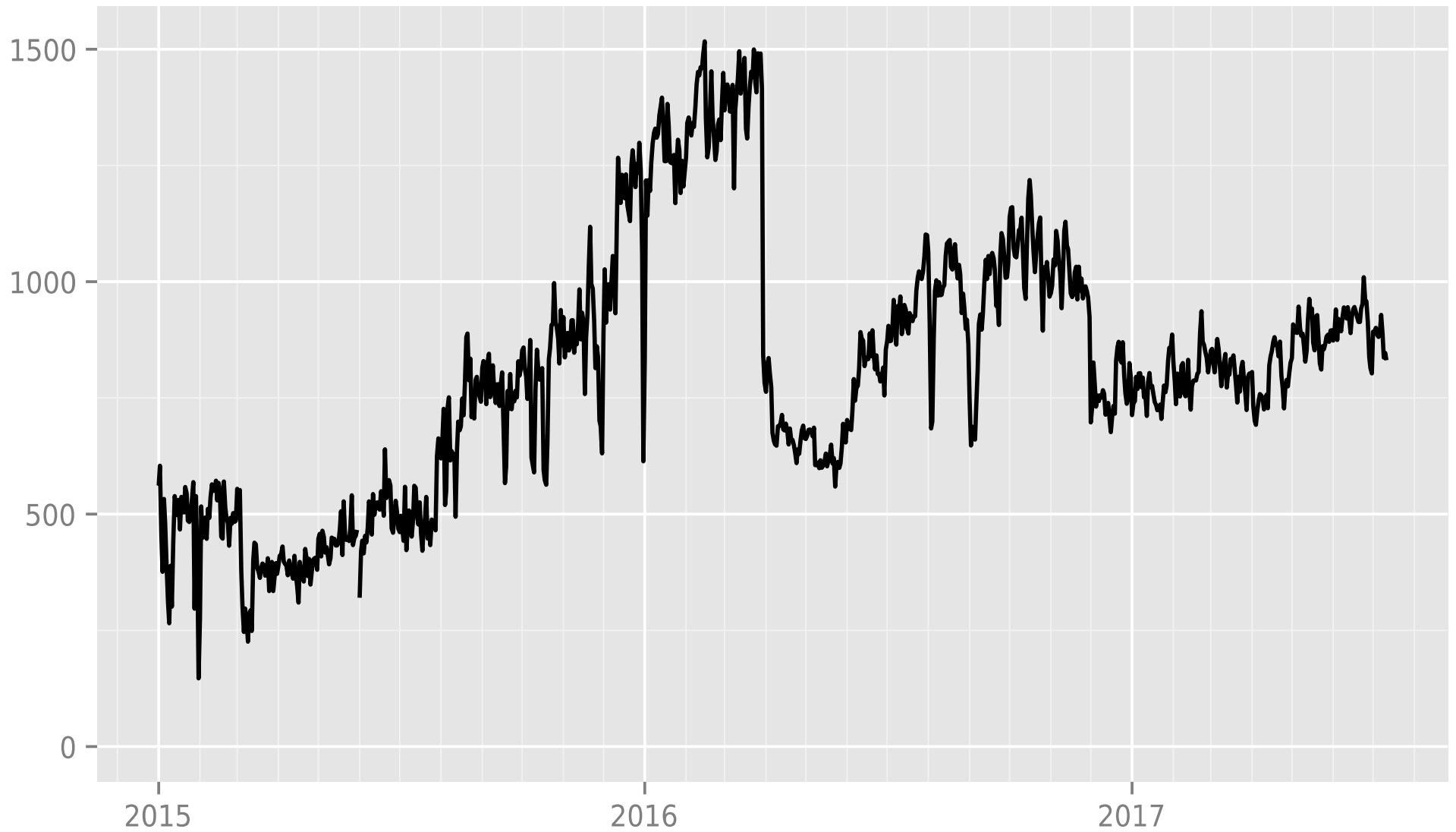


Do

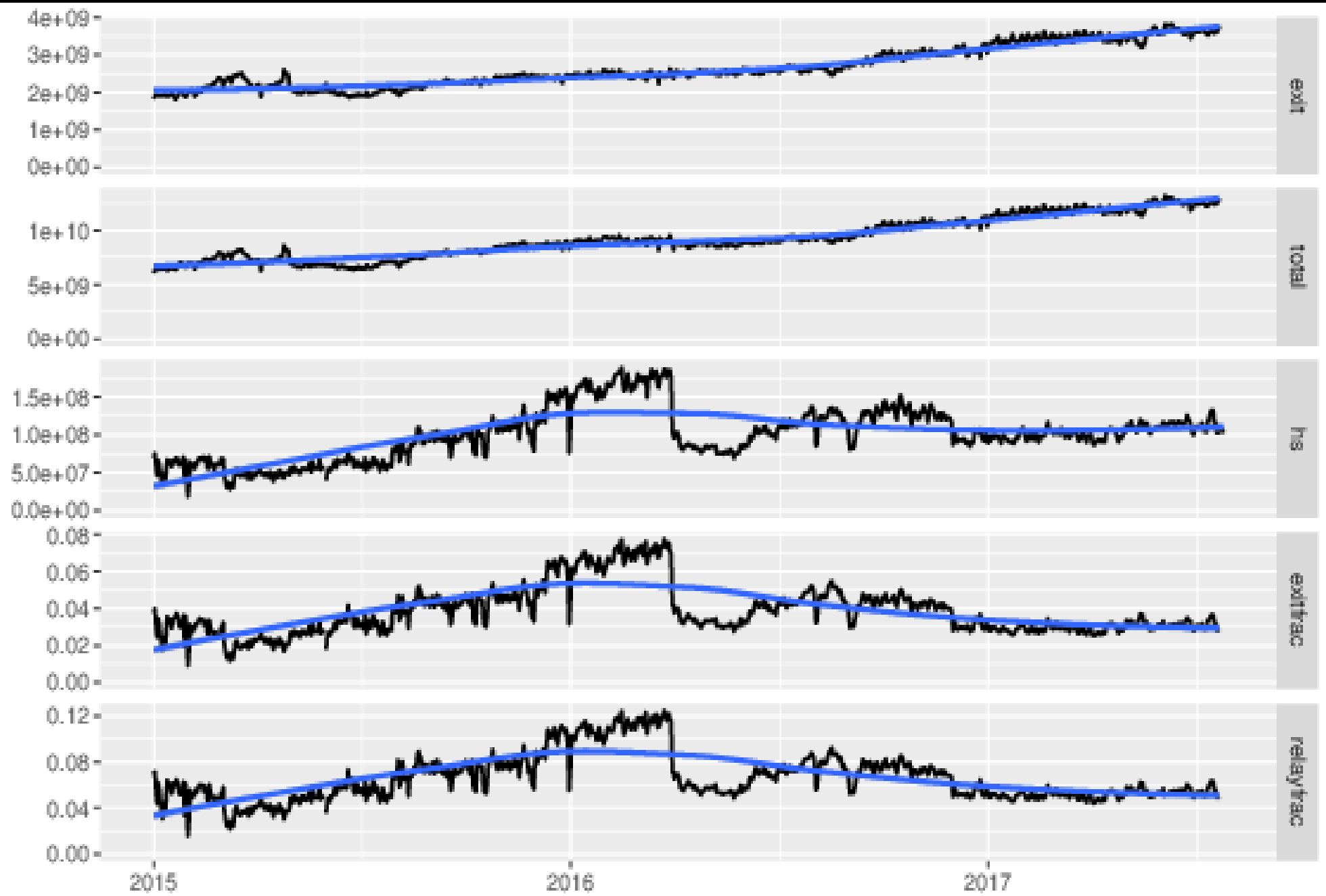
Onion service properties

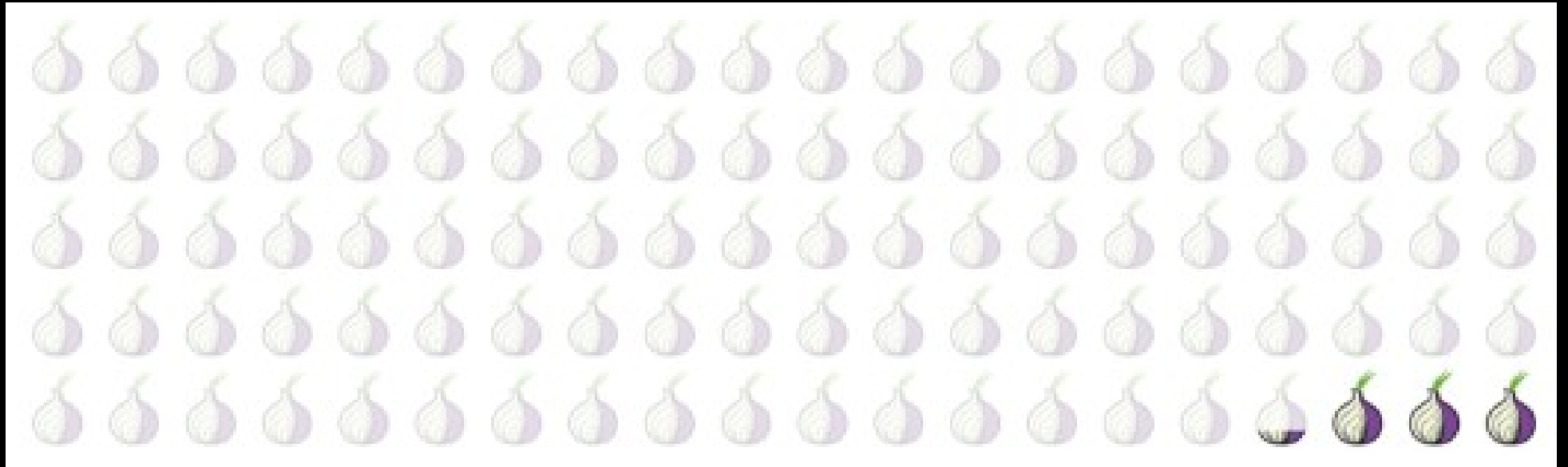
- Self authenticated
- End-to-end encrypted
- Built-in NAT punching
- Limit surface area
- No need to “exit” from Tor

Onion-service traffic in Mbit/s



The Tor Project - <https://metrics.torproject.org/>

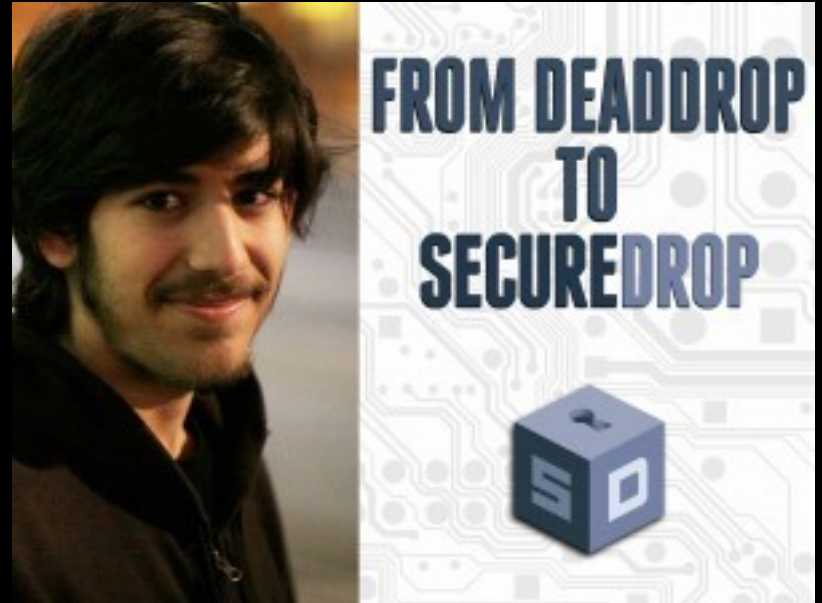






SecureDrop

THE NEW YORKER
STRONGBOX



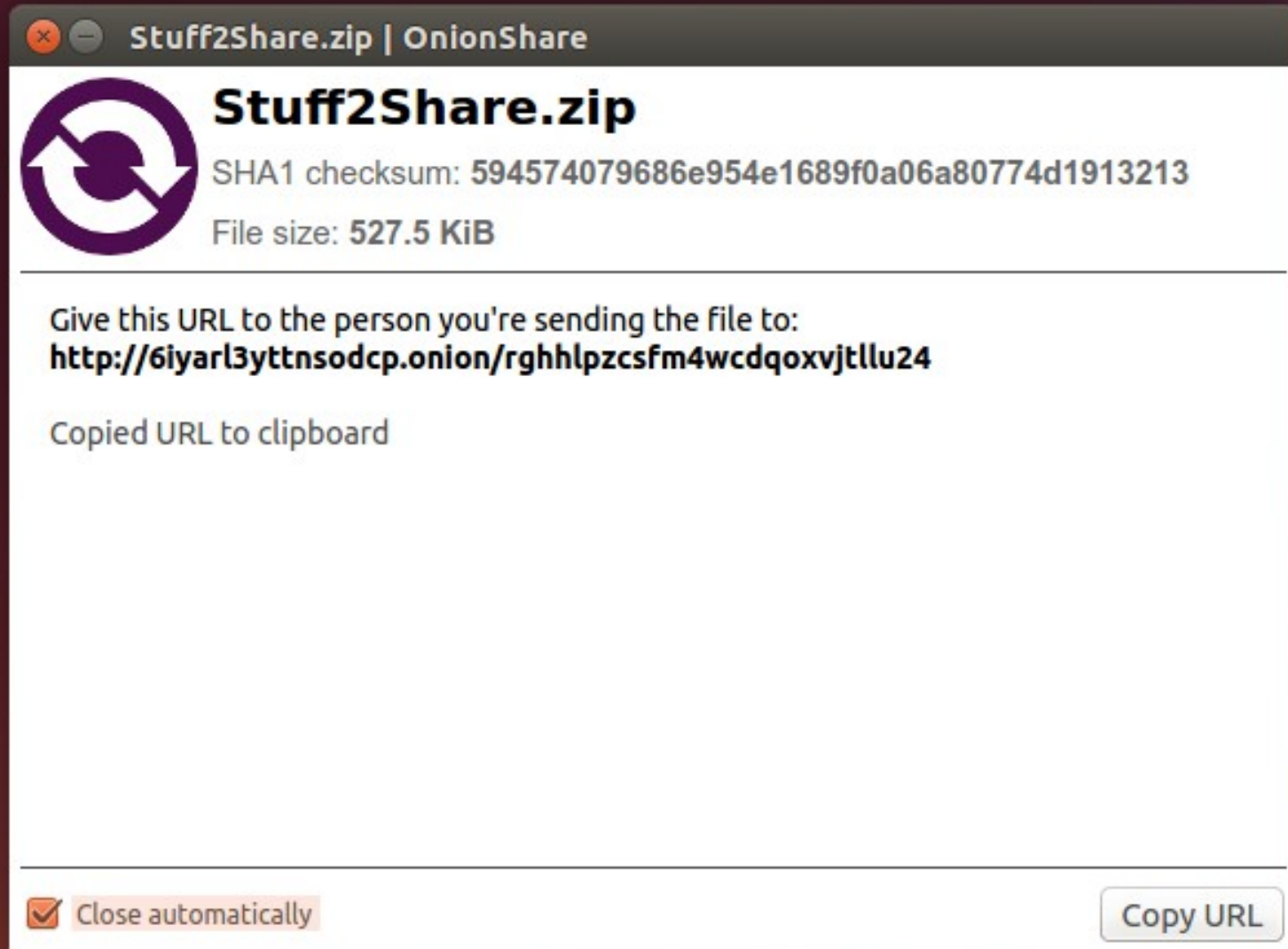
Today, 30+ organizations use SecureDrop

<https://securedrop.org/directory>

Ricochet



OnionShare



Services and Tools



All Riseup.net services are available using hidden service

<https://help.riseup.net/en/tor#riseups-tor-hidden-services>

... and many others



...



debian

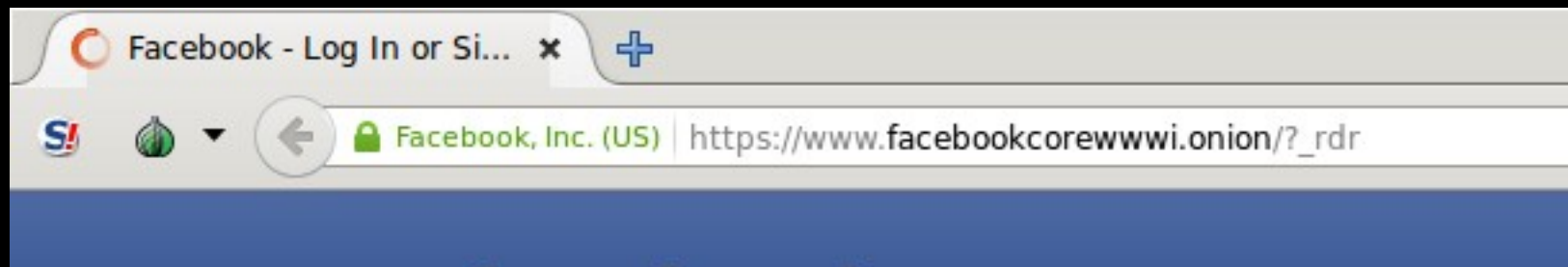
Package repository

<http://vwakviie2ienjx6t.onion/>

```
apt-get install apt-tor-transport
```

Anonymous updates are awesome

- Evil package repository can't target you with a bad update, because they don't know it's you
- Local observer can't learn what you're updating, so they can't target you for being out of date



1 Million People use Facebook over Tor

 FACEBOOK OVER TOR · FRIDAY, APRIL 22, 2016

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've [written previously](#) it's important to us to provide methods for people to use our services securely – particularly if they lack reliable methods to do so.

This is why in the last two years we built [the Facebook onion site](#) and [onion-mobile site](#), helped [standardise the “.onion” domain name](#), and implemented Tor connectivity [for our Android mobile app](#) by enabling connections through [Orbot](#).

Tor Hidden Services: 1

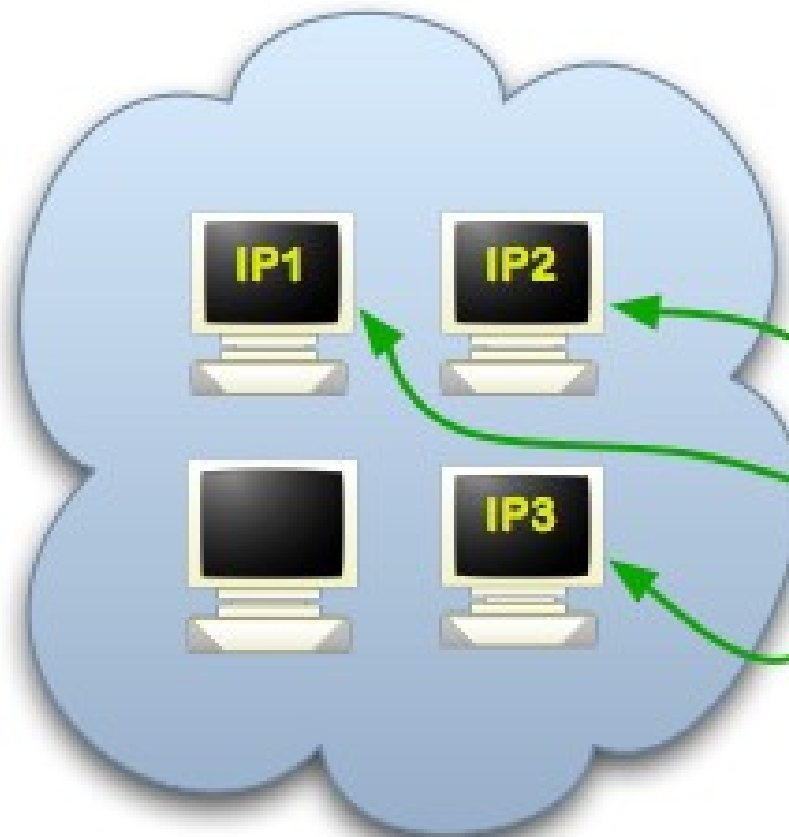
Step 1: Bob picks some introduction points and builds circuits to them.




Alice



DB



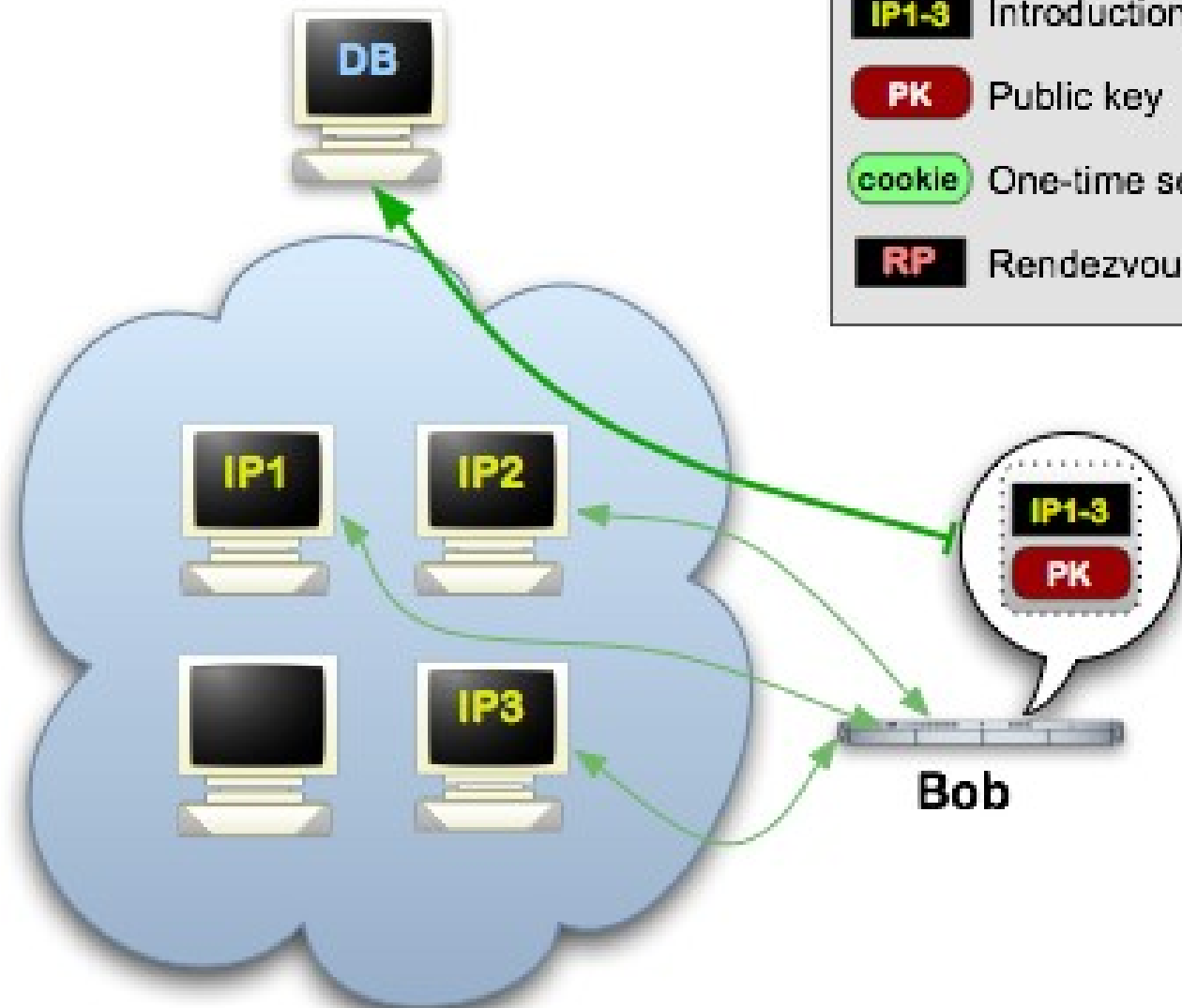
-  Tor cloud
-  Tor circuit
- IP1-3** Introduction points
- PK** Public key
- cookie** One-time secret
- RP** Rendezvous point





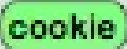

Tor Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



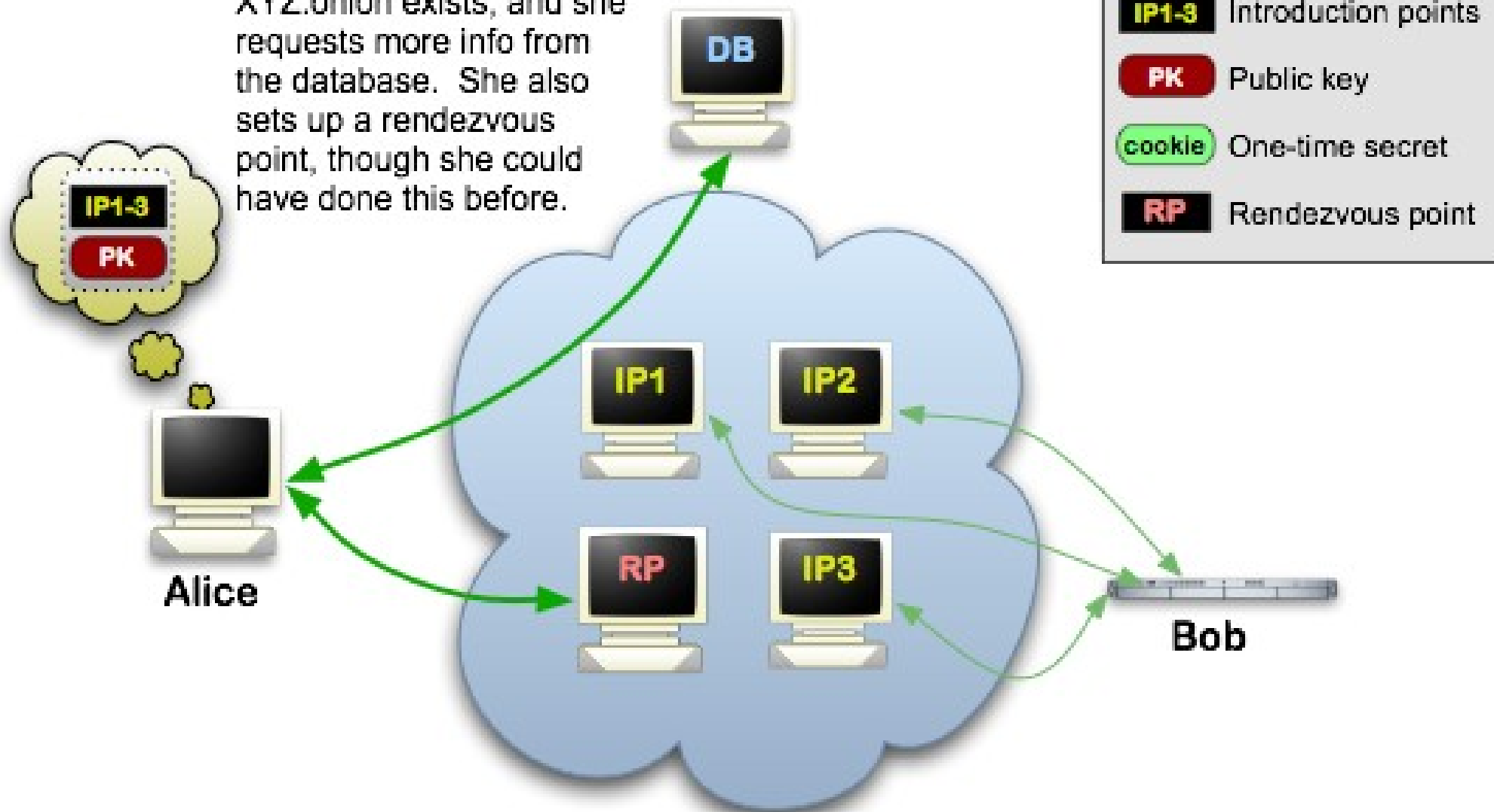
Alice



-  Tor cloud
-  Tor circuit
-  Introduction points
-  Public key
-  One-time secret
-  Rendezvous point

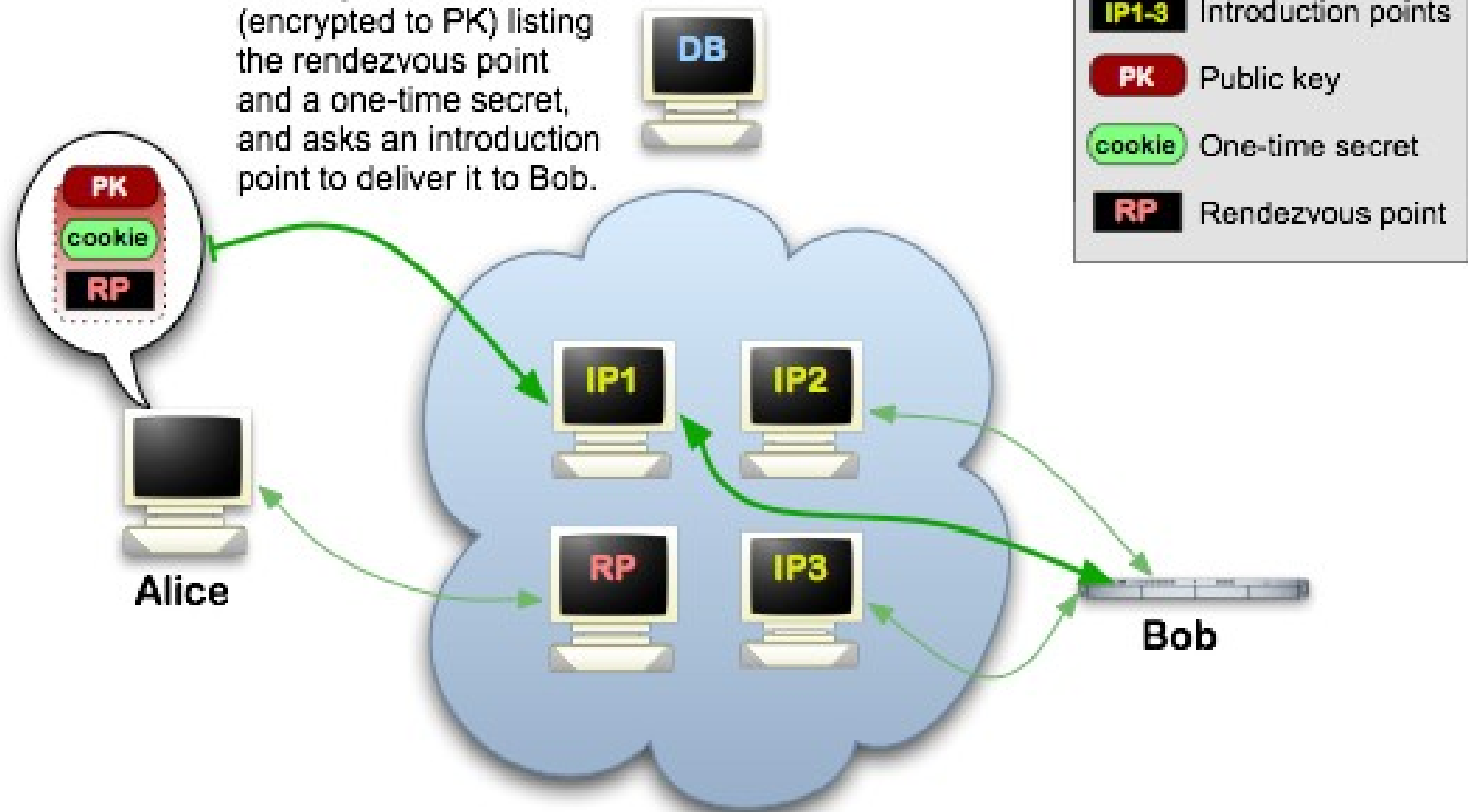
Tor Hidden Services: 3

Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.



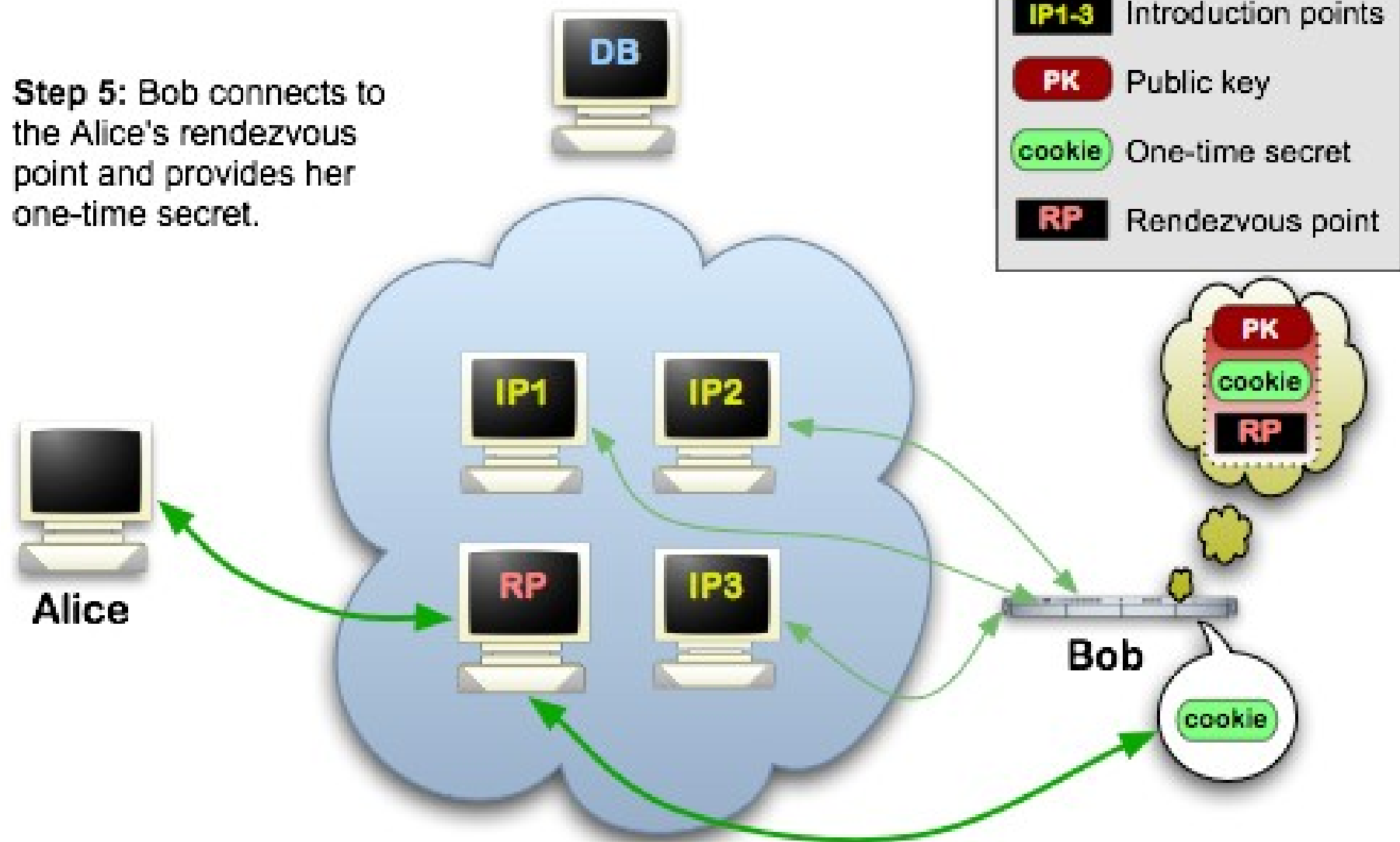
Tor Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



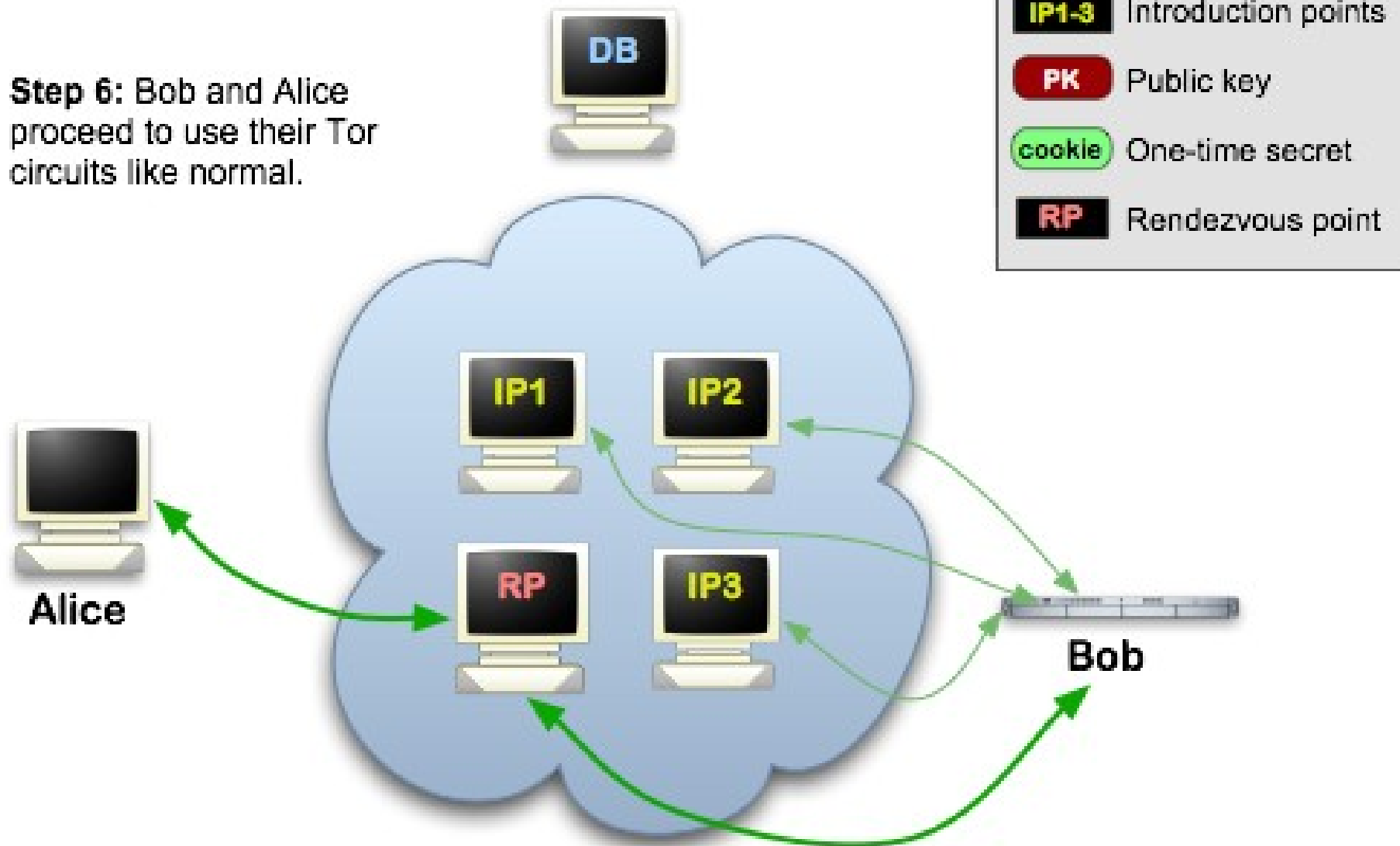
Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



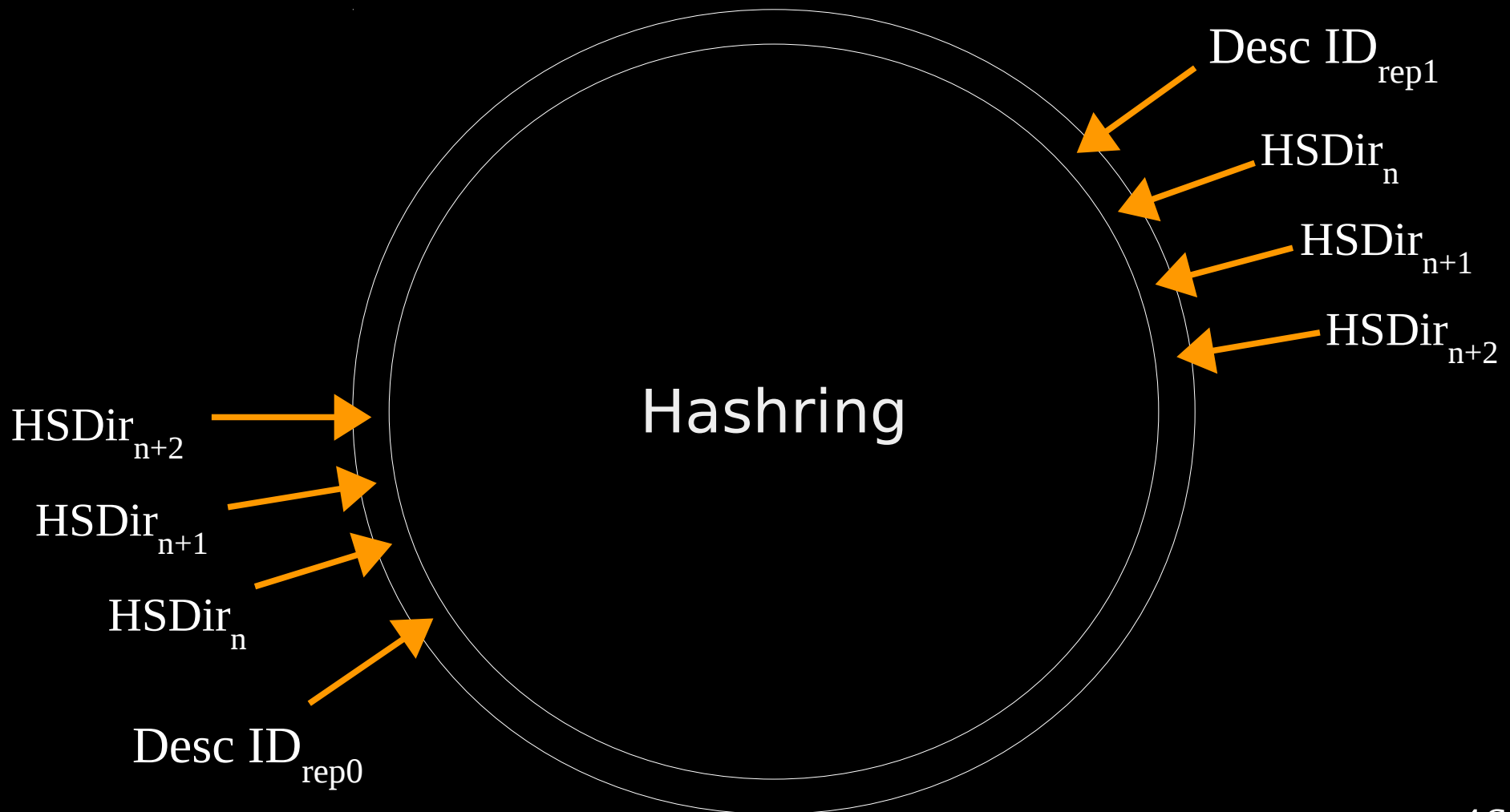
Tor Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



HS Directory

Desc ID = $H(\text{onion-address} \mid H(\text{time-period} \mid \text{descriptor-cookie} \mid \text{replica}))$



#1: Old onion keys are weak

- “The first 80 bits of the SHA-1 of the 1024-bit RSA key” :(
- The new system uses ED25519 (i.e. much stronger ECC keys)

New keys => longer onion addresses

From 16 characters:

nzh3fv6jc6jskki3.onion

... to 52 characters:

a1uik0w1gmfq3i5ievxdm9ceu27e88g6o7pe0rffdw9jmntwkdsd.onion

(ed25519 public key base32 encoded)

The HSDir relays are too predictable

- The six daily HSDirs for a given onion address are predictable into the future
- So a bad guy can run six relays with just the right keys to target a specific future day...to censor or to measure popularity
- People – we don't know who – were doing this attack in practice

#2: Global shared random value

- The solution: make the HSDir mapping include a communal random value that everybody agrees about but that nobody can predict
- The directory authorities pick this value each day as part of their consensus voting process

HSDirs get to learn onion addresses

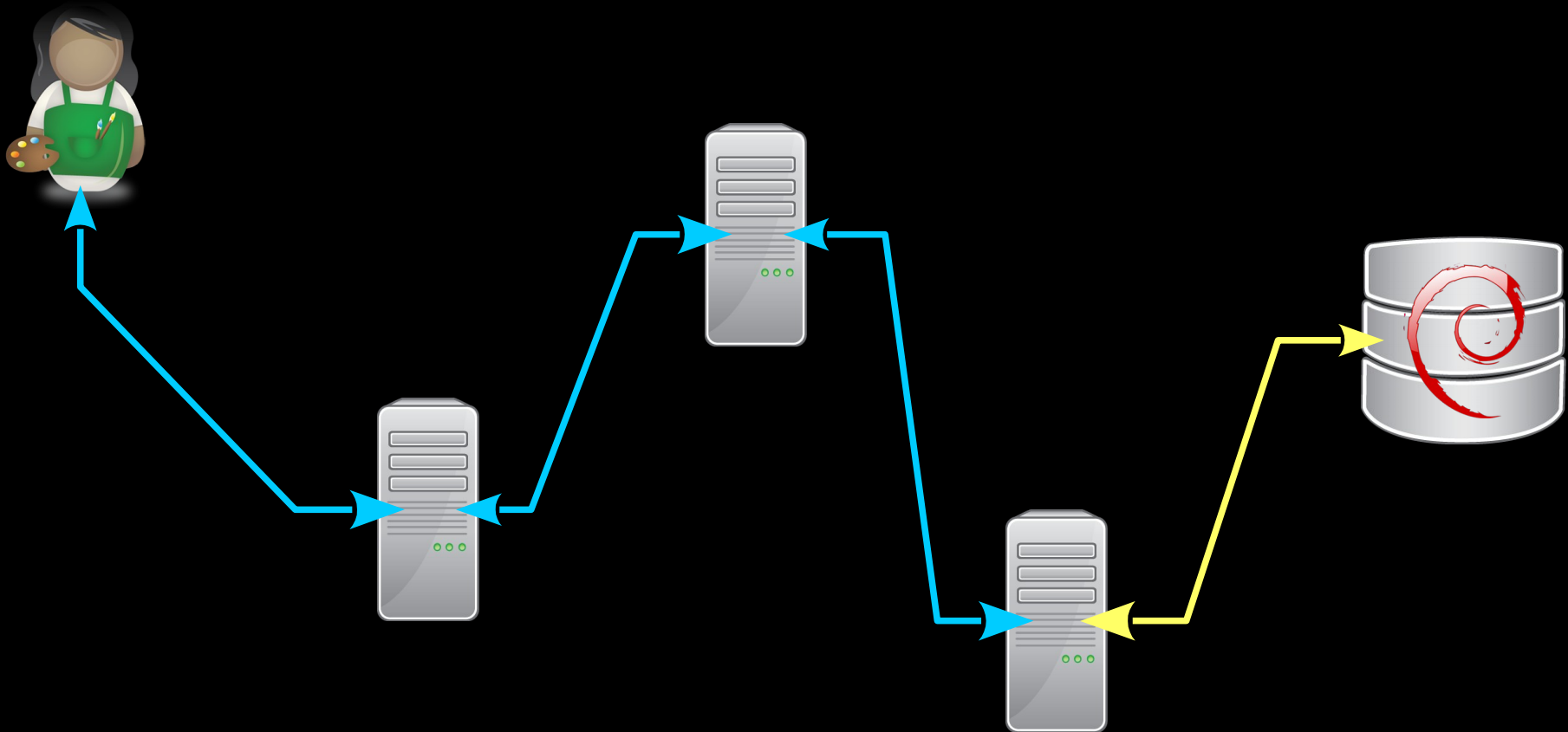
- The onion service descriptor (which gets uploaded to the HSDir) includes the public key for the service (so everybody can check the signature)
- So you can run relays and discover otherwise-unpublished onion addresses
- “Threat intelligence” companies have been trying to do just that

#3: New crypto hides the address

- The solution: the new cryptosystem has a cool feature where you can sign the onion descriptor with a subkey
- So everybody can check the signature but nobody can learn the main key from the subkey or signature
- Should finally kill the arms race with jerks running relays to gather onions

#4: Rendezvous Single Onion Services

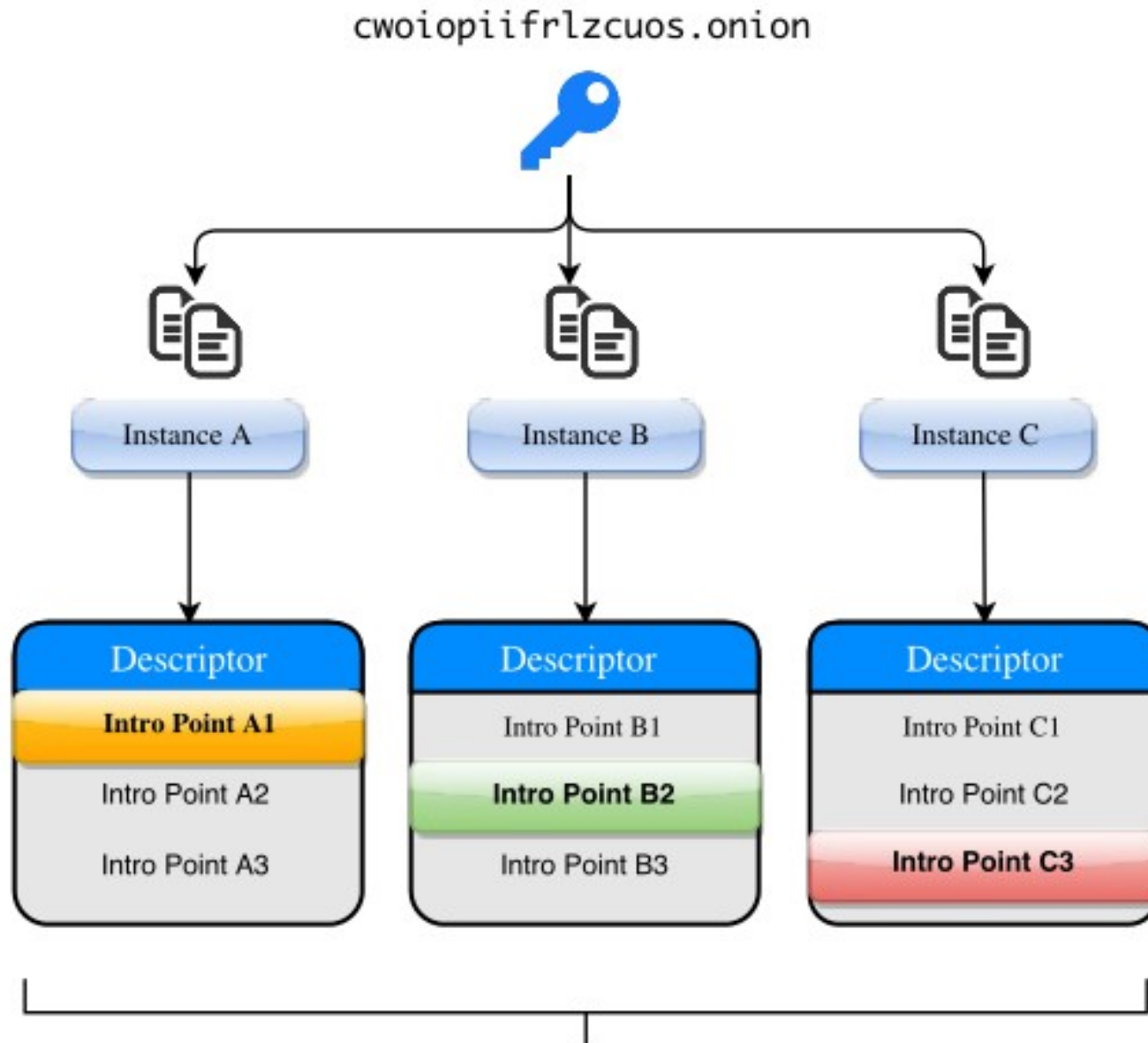
Proposal 260



Rendezvous Point

OnionBalance

<https://onionbalance.readthedocs.org>



#5: Guard discovery is a big deal

- Your Tor client uses a single relay (called a Guard) for the first hop in all your paths, to limit exposed surface area
- But there are relatively easy attacks to learn a user's guard, and for onion services that can be especially bad

Vanguards (Tor proposal 271)

- Multiple layers of guards protect better against Sybil+compromise attacks
- Path selection is still a huge open research area

Deployment timeline

- HSDir side: deployed in Tor 0.3.0
- Relay side: deployed in Tor 0.3.0
- Client side: upcoming in Tor 0.3.2
- Service side: upcoming in Tor 0.3.2

Try it at

```
% git clone https://git.torproject.org/arma/tor.git  
% git checkout dc25
```

This is the example page for [Tor's](#) rendezvous points system.

Read [Thomas Paine's Common Sense](#).

Or read [The Federalist papers](#), which were also originally published

(If you were sent here by the Tor help desk, your Tor Browser is acting normally. If you still cannot reach a particular hidden service, then

Tor isn't foolproof

- Opsec mistakes
- Browser metadata fingerprints
- Browser exploits
- Traffic analysis

How can you help?

- Run a relay (or a bridge)
- Teach your friends about Tor, and privacy in general
- Help find -- and fix -- bugs
- Work on open research problems (petsymposium.org)
- donate.torproject.org



“Still the King of high secure,
low latency Internet Anonymity”

“There are no contenders for the throne”