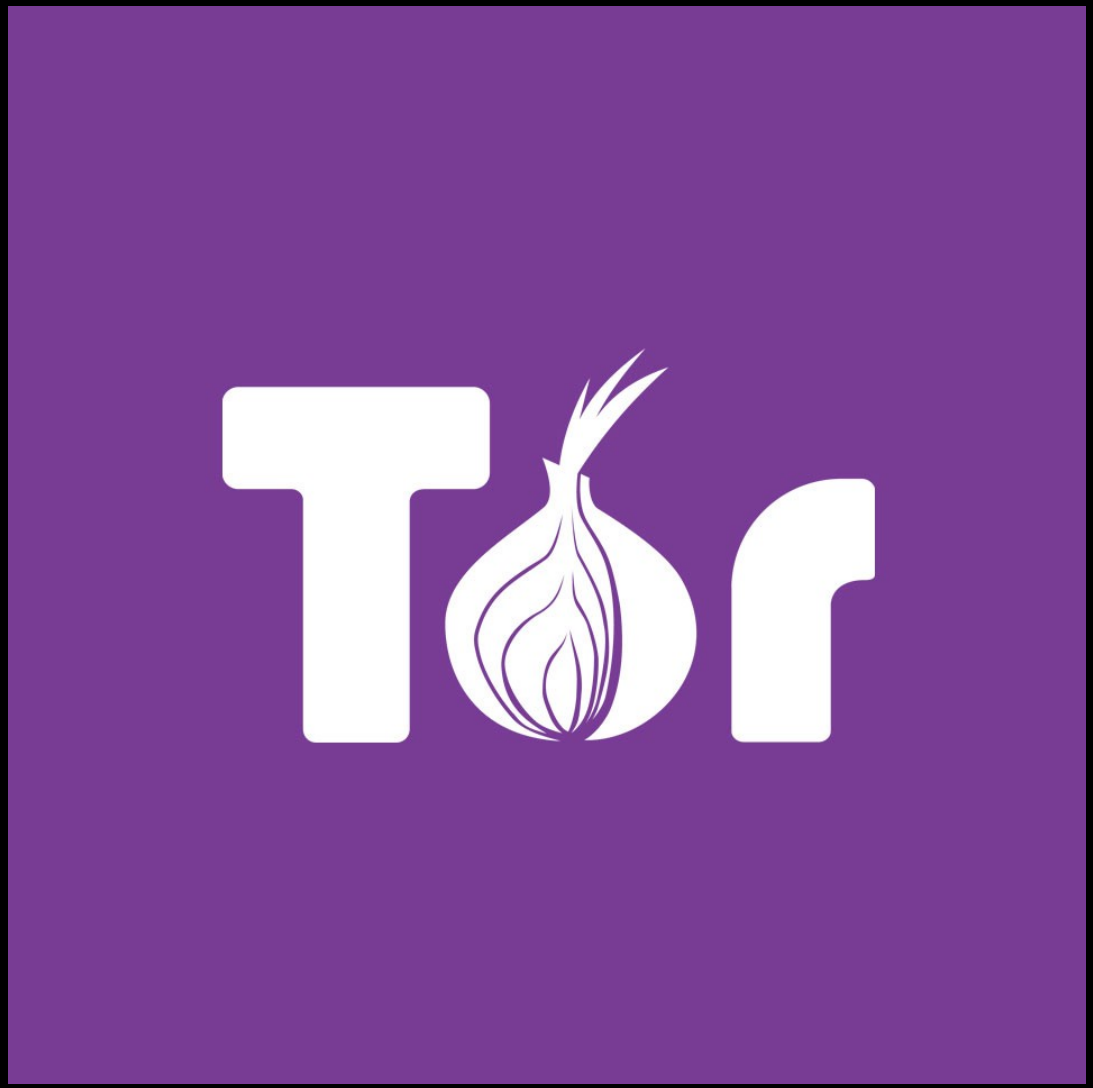
The Design and Implementation of the Tor Network

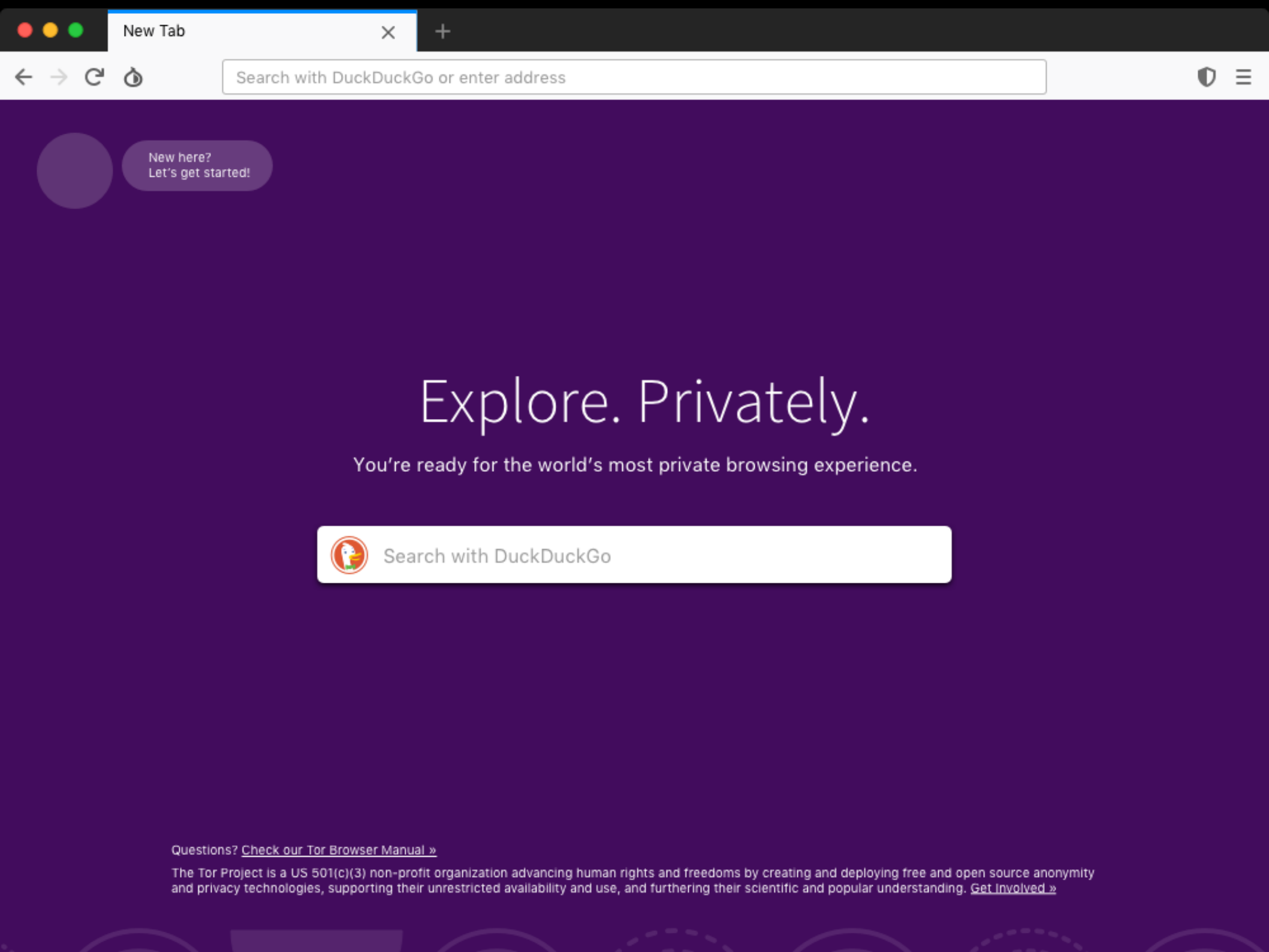


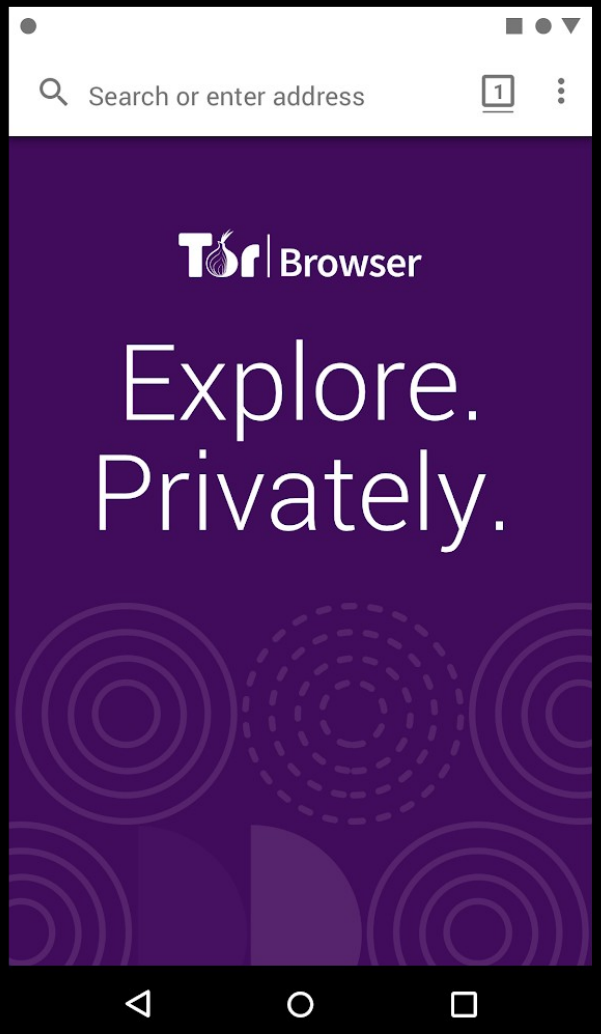
- Online Anonymity & Censorship Circumvention
  - Free Software
  - Open Network
- Community of researchers, developers, users and relay operators.
- U.S. 501(c)(3) non-profit organization

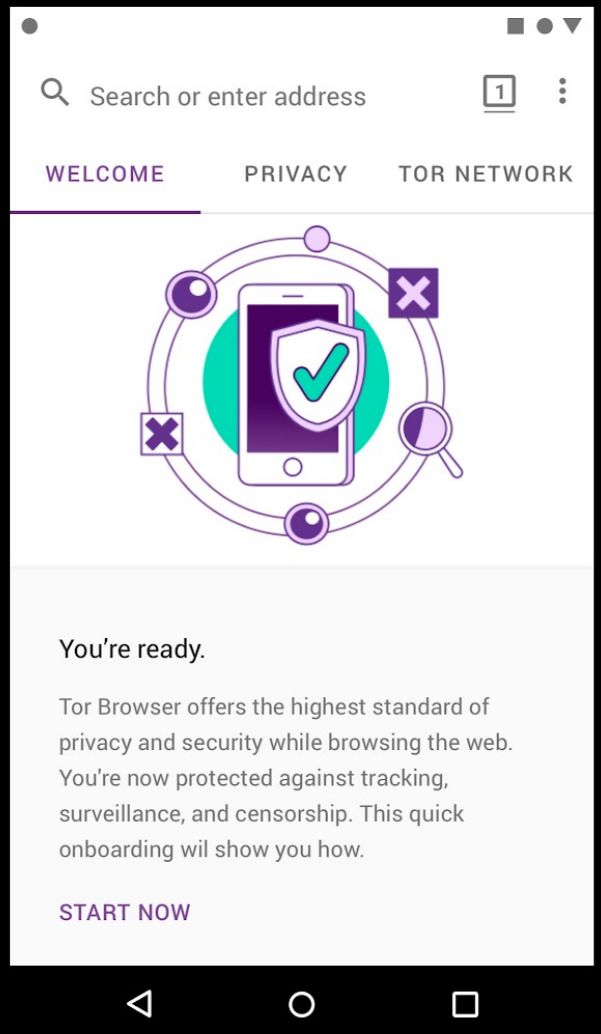
Tor’s History

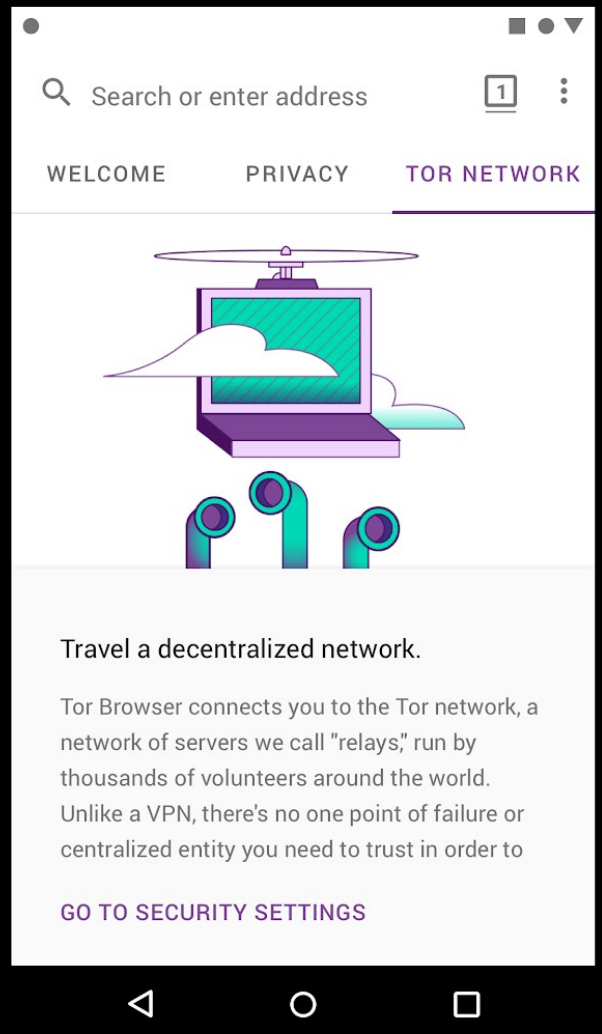
- 1990s: Onion routing for privacy online
- Early 2000s: Working with NRL
- 2004: Sponsorship by EFF
- 2006: The Tor Project, Inc became a nonprofit
- 2007: Expansion to anti-censorship
- 2008: Tor Browser development
- 2010: Arab spring
- 2013: Snowden revelations


Estimated 2,000,000 to
8,000,000
daily Tor users

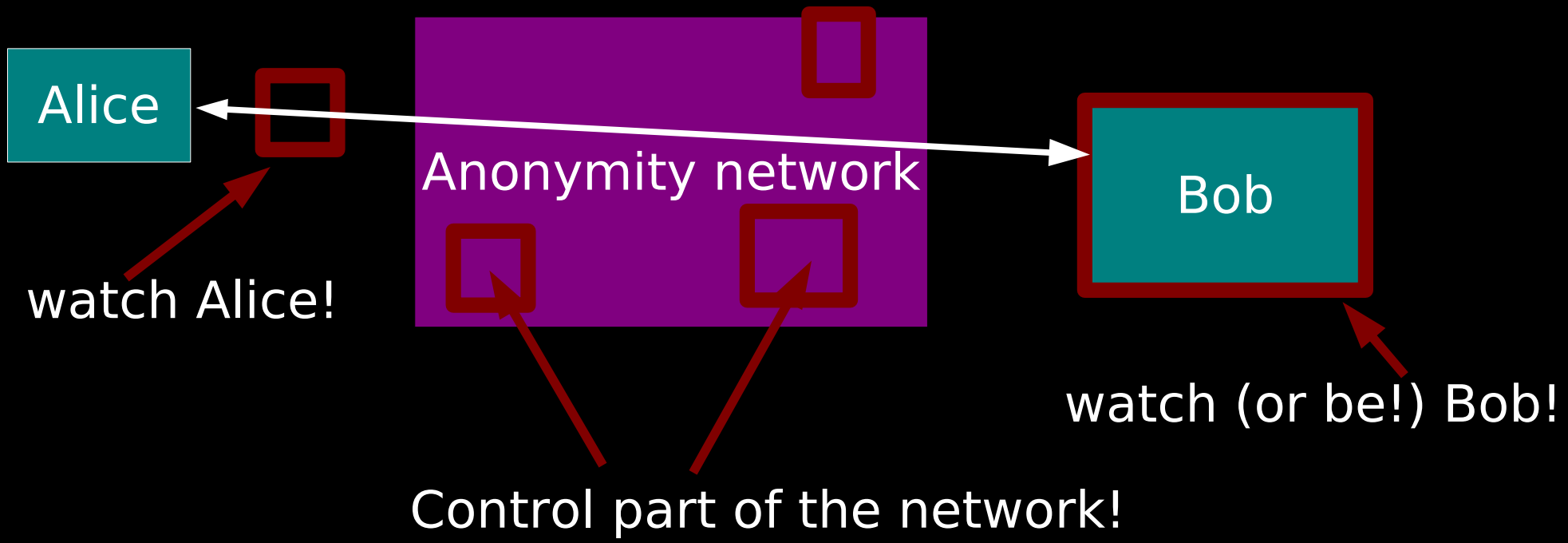

New Tab
Search with DuckDuckGo or enter address
New here?
Let's get started!
Explore. Privately.
You're ready for the world's most private browsing experience.
Search with DuckDuckGo
Questions? Check our Tor Browser Manual »
The Tor Project is a US 501(c)(3) non-profit organization advancing human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding. Get Involved »


Search or enter address
Tor Browser
Explore.
Privately.

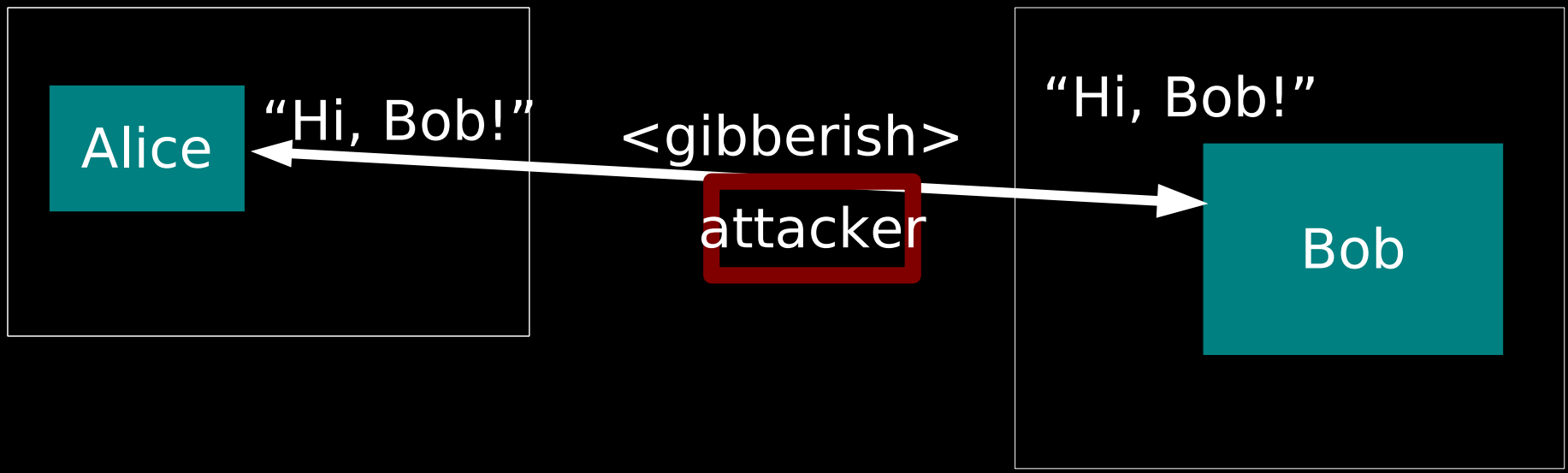

Search or enter address
WELCOME
PRIVACY
TOR NETWORK
You're ready.
Tor Browser offers the highest standard of privacy and security while browsing the web. You're now protected against tracking, surveillance, and censorship. This quick onboarding wil show you how.
START NOW


Search or enter address
WELCOME
PRIVACY
TOR NETWORK
Travel a decentralized network.
Tor Browser connects you to the Tor network, a network of servers we call "relays," run by thousands of volunteers around the world. Unlike a VPN, there's no one point of failure or centralized entity you need to trust in order to
GO TO SECURITY SETTINGS

Threat model: what can the attacker do?



Anonymity isn't encryption: Encryption just protects contents.



Metadata

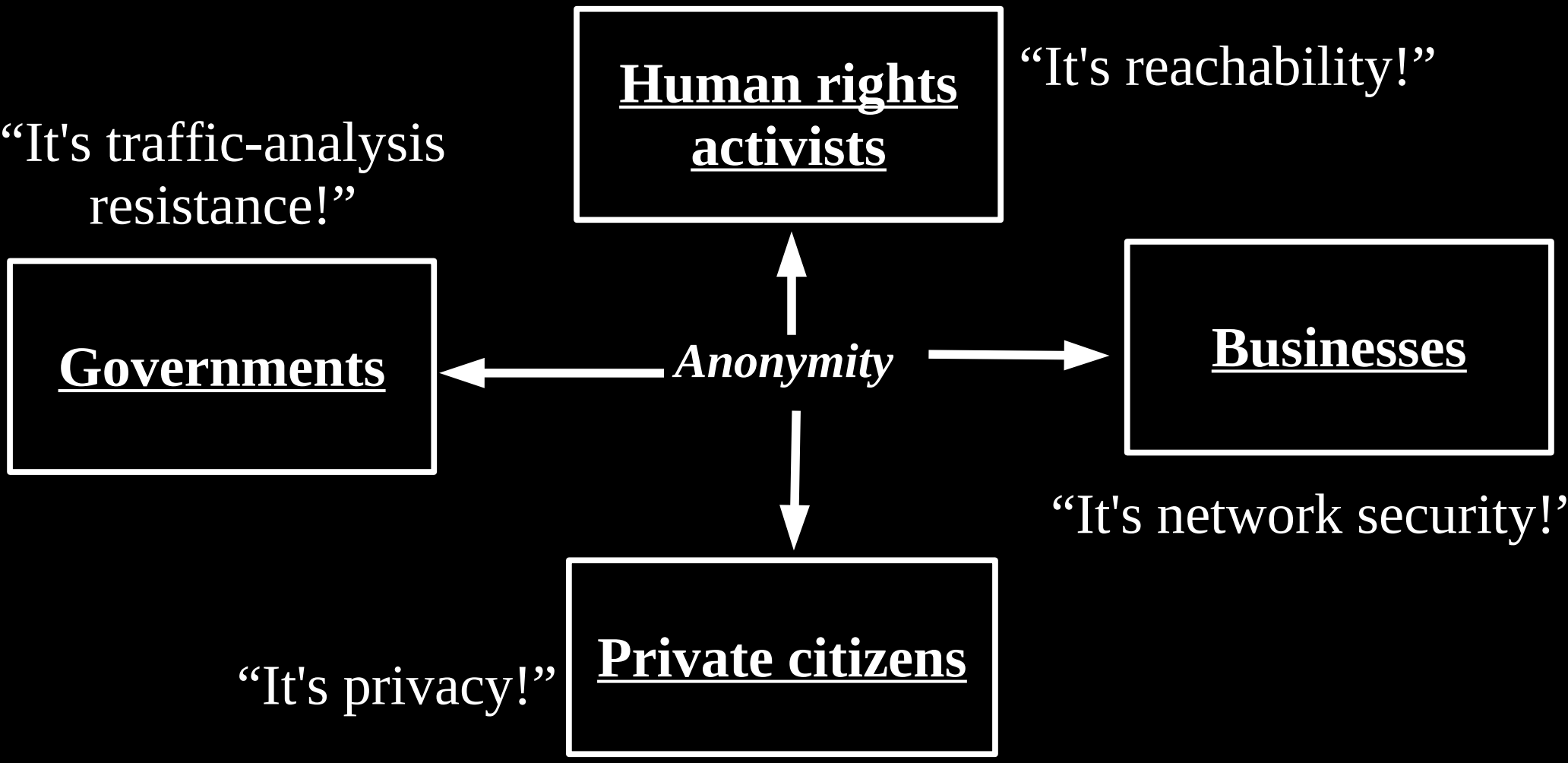
Data about data

"Metadata was traditionally in the card catalogs of libraries"

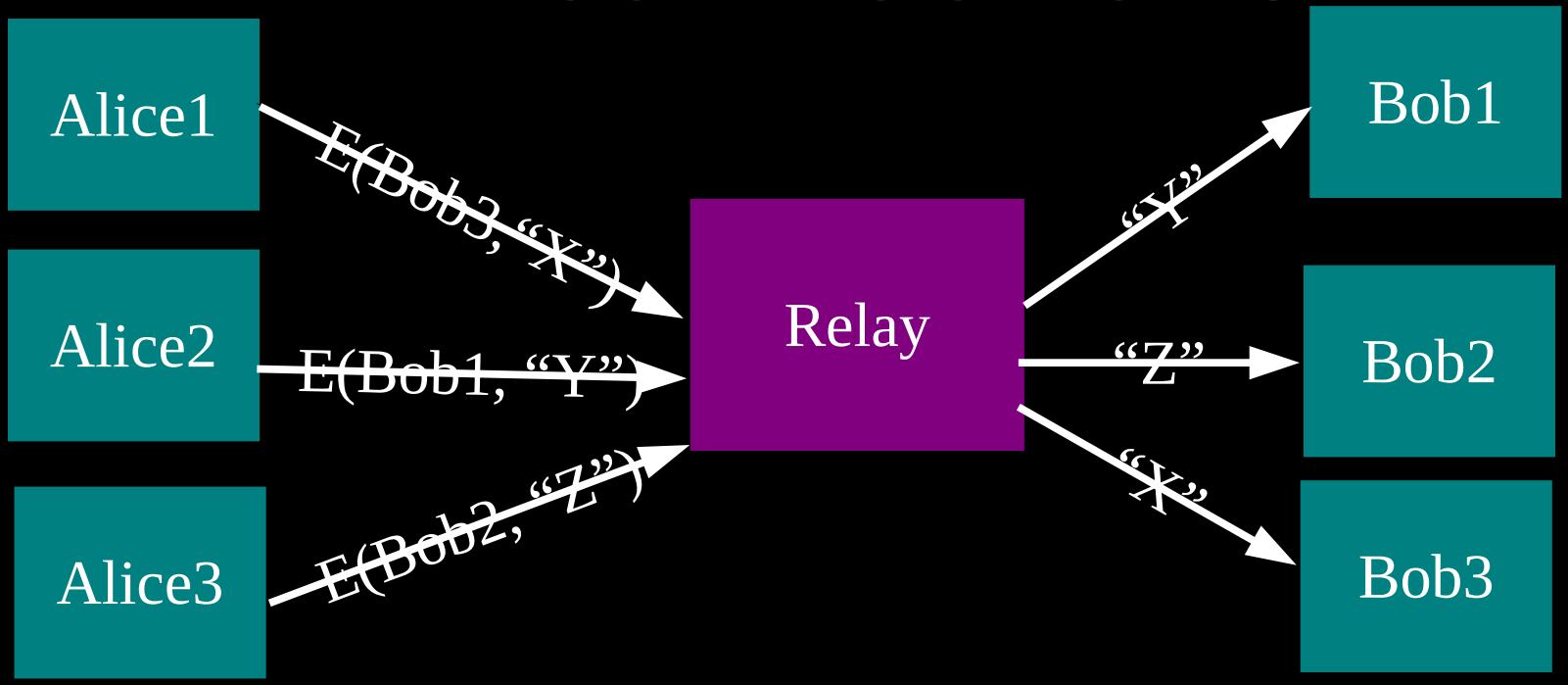
-- Wikipedia

"We kill people based on metadata"

Anonymity serves different interests for different user groups.

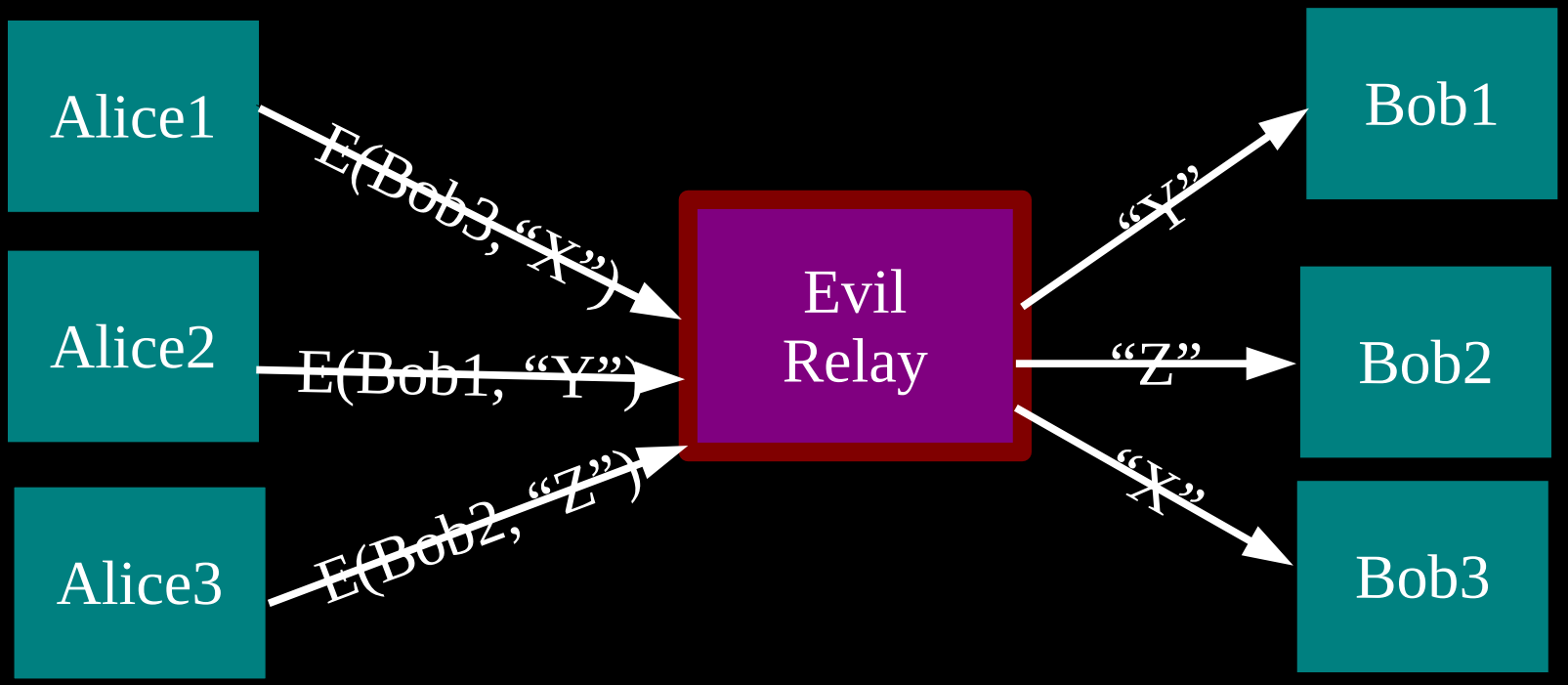


The simplest designs use a single relay to hide connections.

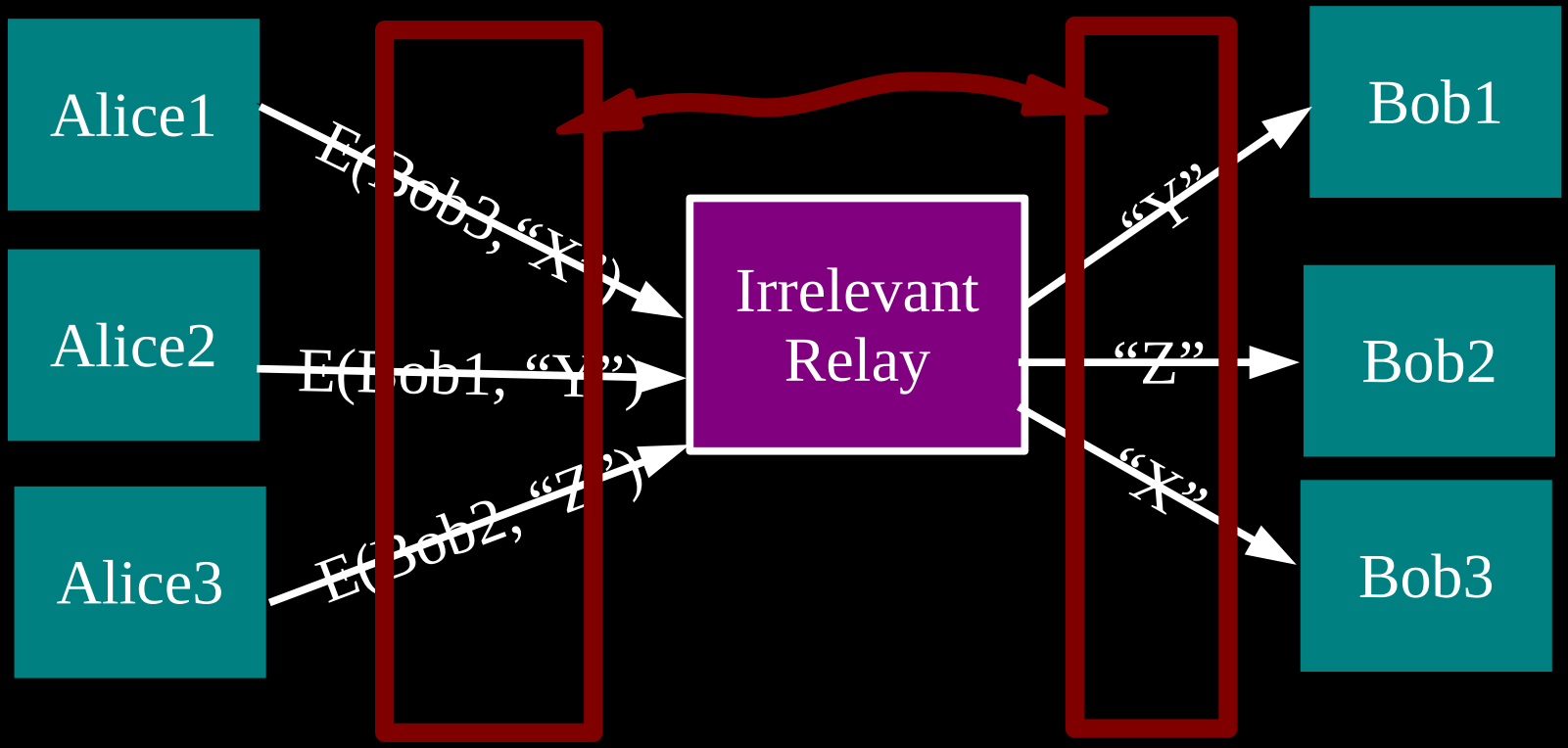


(example: some commercial proxy providers)

But a central relay is a single point of failure.

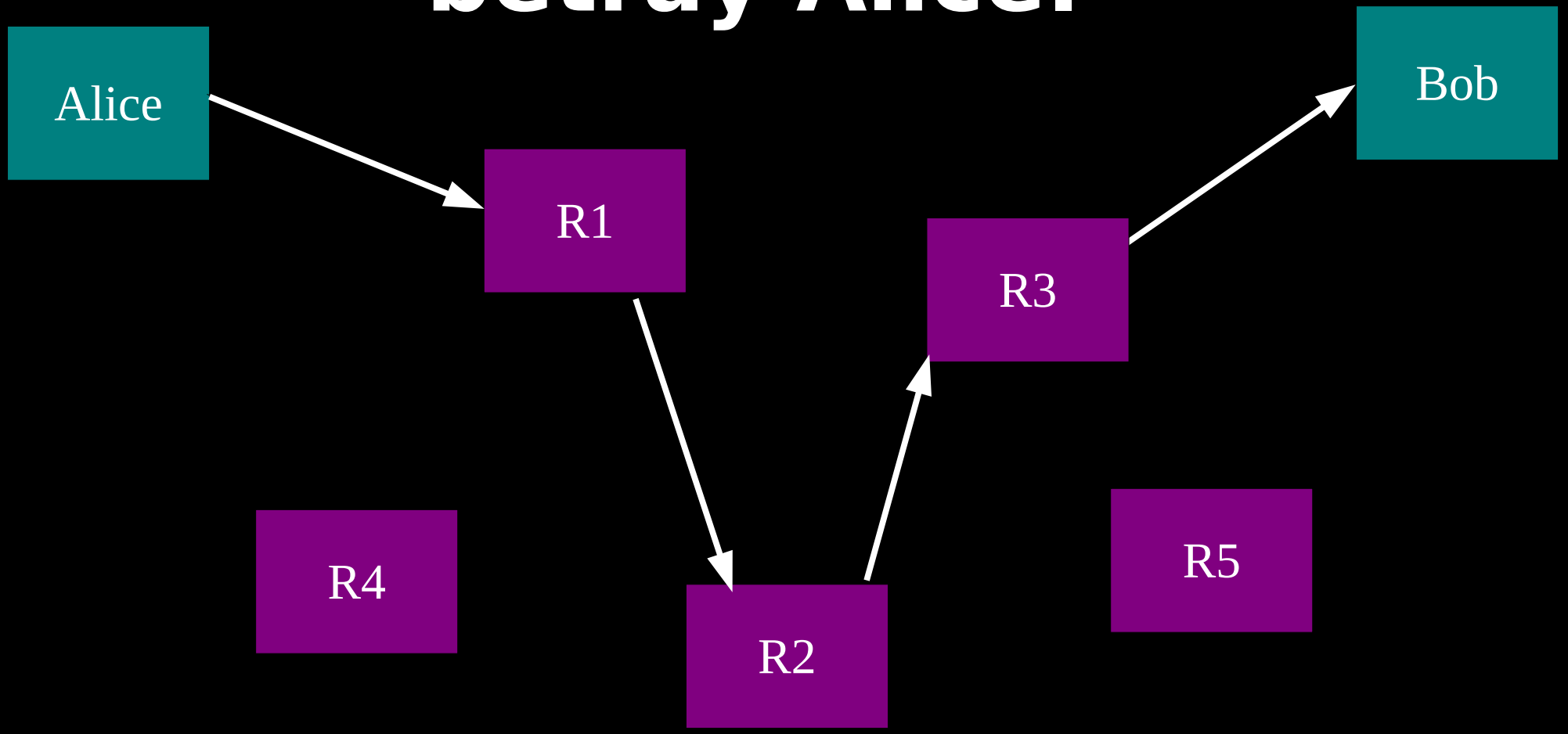


… or a single point of bypass.

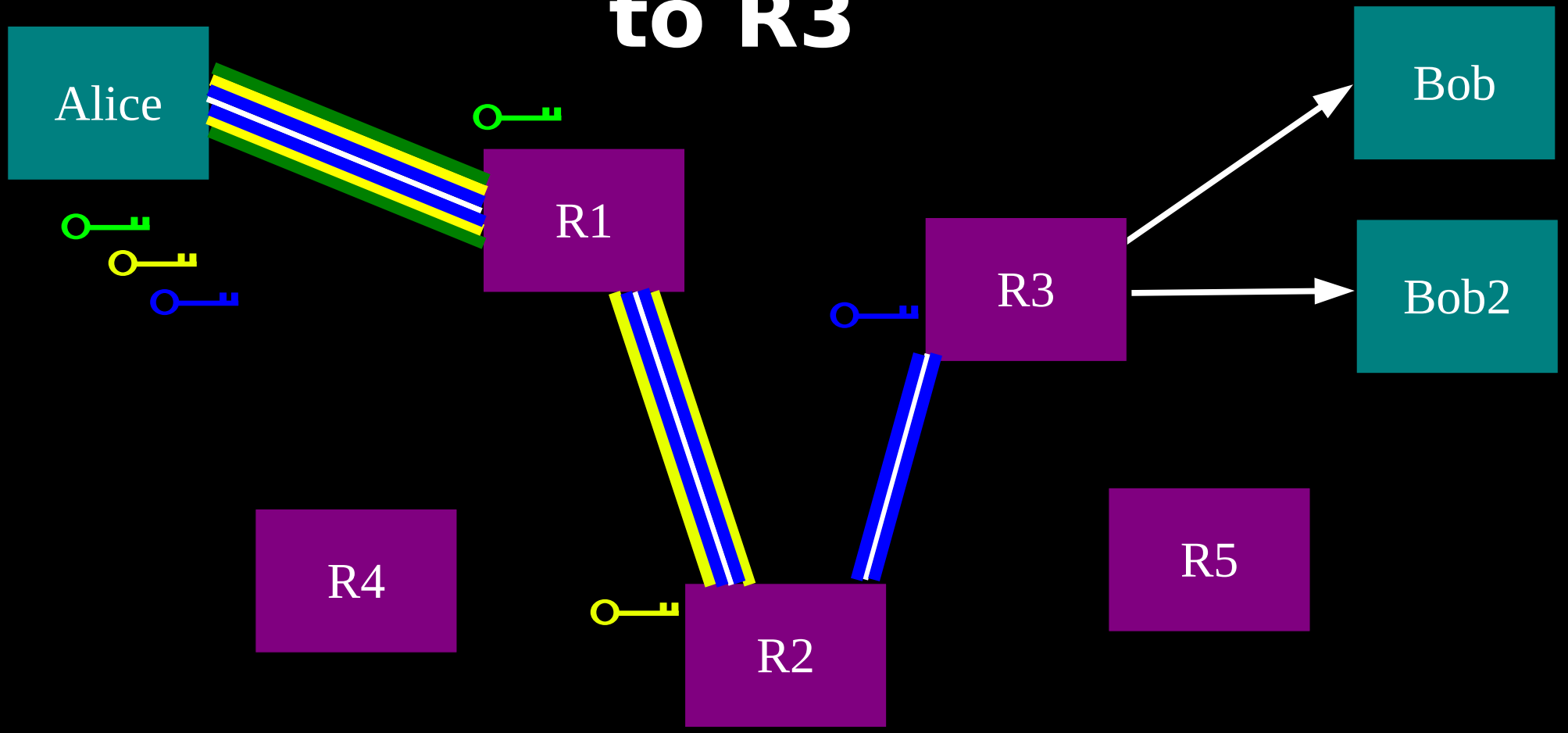


Timing analysis bridges all connections through relay ⇒ An attractive fat target

So, add multiple relays so that no single one can betray Alice.

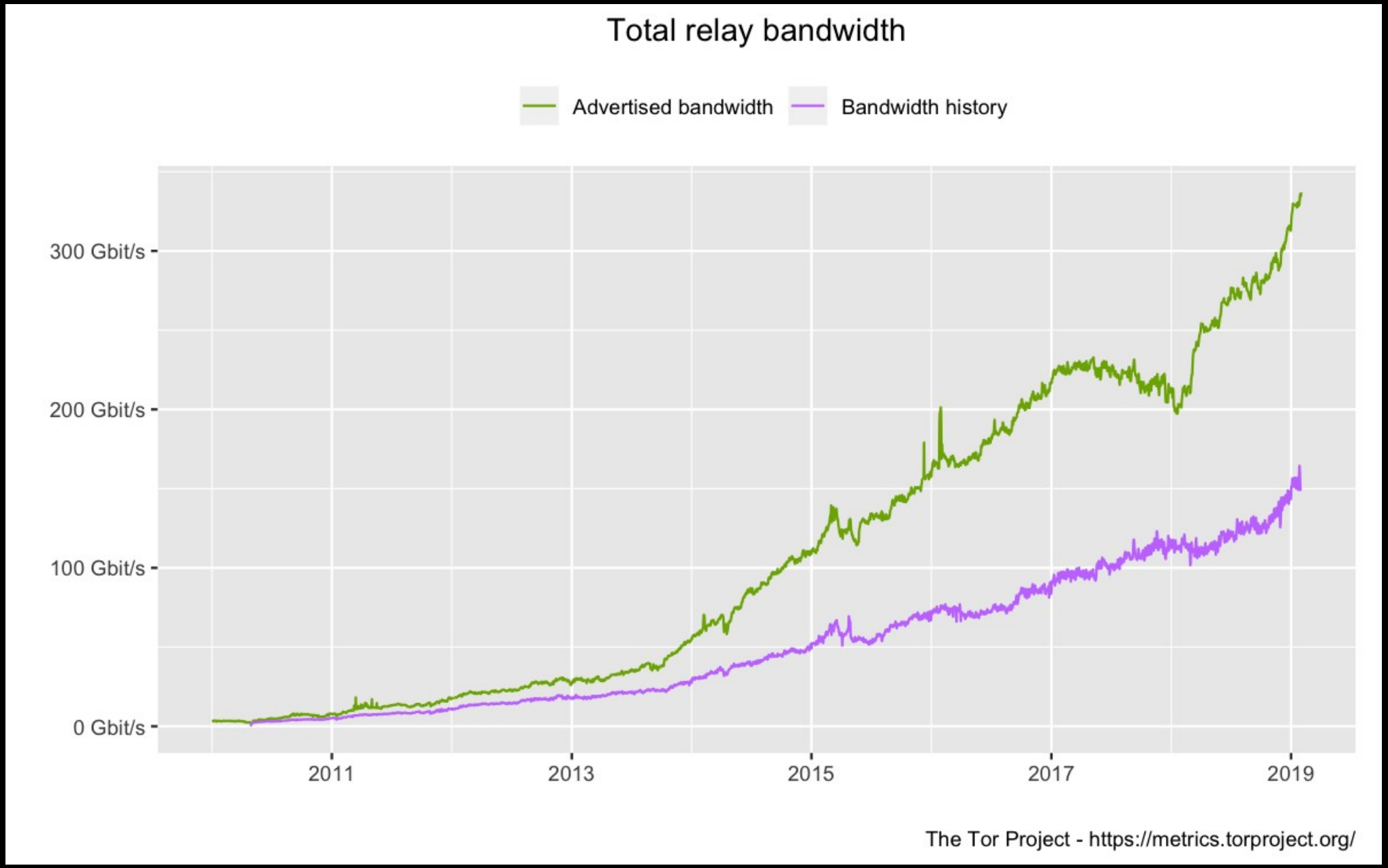


Alice makes a session key with R1 ...And then tunnels to R2...and to R3



The Network

- Between 6000 and 7000 relays online.
- Hosted by different organizations, companies, and individuals.
- 9 Directory Authorities and 1 Bridge authority.


Total relay bandwidth
Advertised bandwidth
Bandwidth history
300 Gbit/s
200 Gbit/s
100 Gbit/s
0 Gbit/s
2011
2013
2015
2017
2019
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.

I'm a political activist, part of a semi-criminalized minority. In my younger years I entered the public debate openly, and as a result got harassed by government agencies. I later tried to obfuscate my identity, but I found that my government has surprisingly broad powers to track down dissidents.

Only by using anonymizing means, among which Tor is key, can I get my message out without having police come to "check my papers" in the middle of the night. Tor allows me freedom to publish my message to the world without being personally persecuted for it.

Being a dissident is hard enough, privacy is already heavily curtailed, so anonymized communication is a godsend.

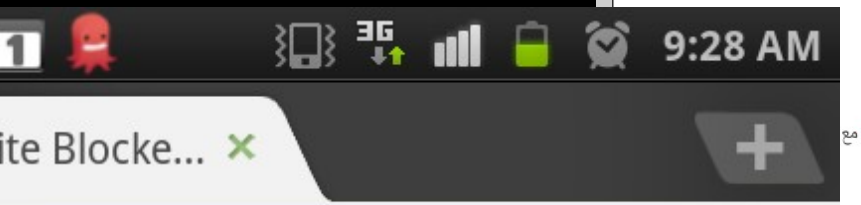
-Anonymous Tor User

I'm a doctor in a very political town. I have patients who work on legislation that can mean billions of dollars to major telecom, social media, and search concerns.

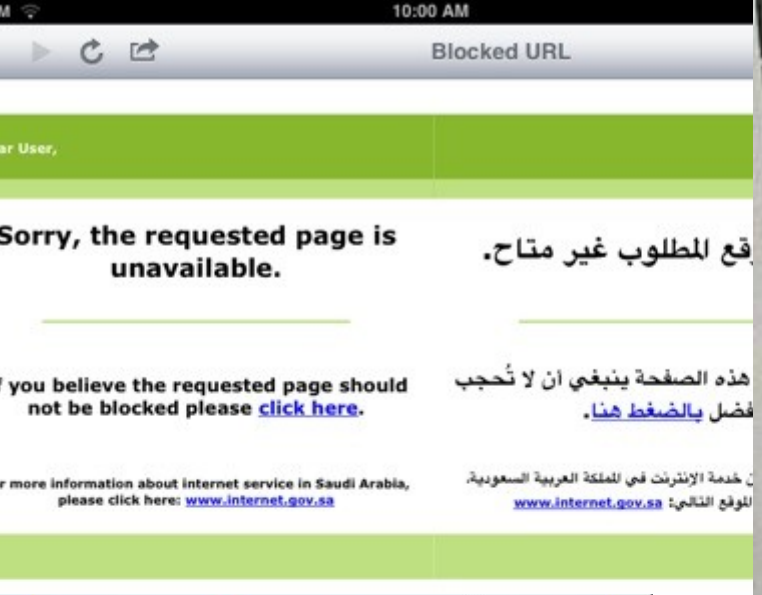
When I have to do research on diseases and treatment or look into aspects of my patients' histories, I am well aware that my search histories might be correlated to patient visits and leak information about their health, families, and personal lives. I use Tor to do much of my research when I think there is a risk of correlating it to patient visits.

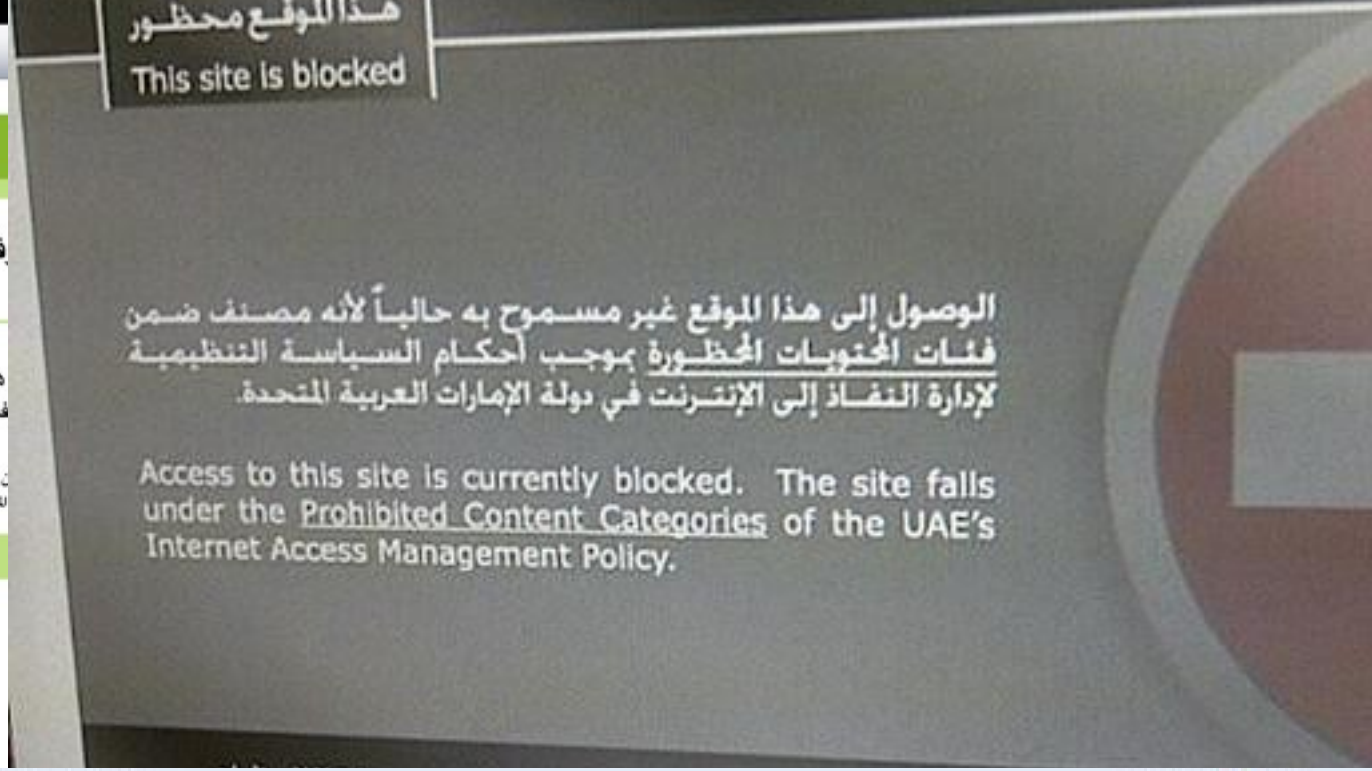
- Anonymous Tor User

Your request was denied because of its conte



ء على اللوائح والقوانين
مع unblock.kw@kw.zain


10:00 AM
Blocked URL
ar User,
Sorry, the requested page is unavailable.
you believe the requested page should not be blocked please click here.
r more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa
قع المطلوب غير متاح.
هذه الصفحة ينبغي أن لا تُحجب
فضل بالضغط هنا.
www.internet.gov.sa


This site is blocked
الوصول إلى هذا الموقع غير مسموح به حالياً لأنه مصنف ضمن فئات المحتويات المحظورة بموجب أحكام السياسة التنظيمية لإدارة النفاذ إلى الإنترنت في دولة الإمارات العربية المتحدة.
Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.


KT WATA...
٩:٢١ ص
87%
Tweet
Blocked by Mada Com...


مدى للإتصالات
mada Mada Communications
ان الموقع الذي تحاول زيارته محجوب
Access to this website is prohibited
SITE BLOCKED
This site is blocked according to the goverment filtering policy.
If you feel this page has been blocked in errors, kindly fill out the form and we will investigate .
Thank You .
Required fields are denoted by (*)
Full Name *
الإسم
Email *
العنوان البريدي
Blocked URL *
www.
.com
اسم النطاق
Comments
استفسارك
Submit

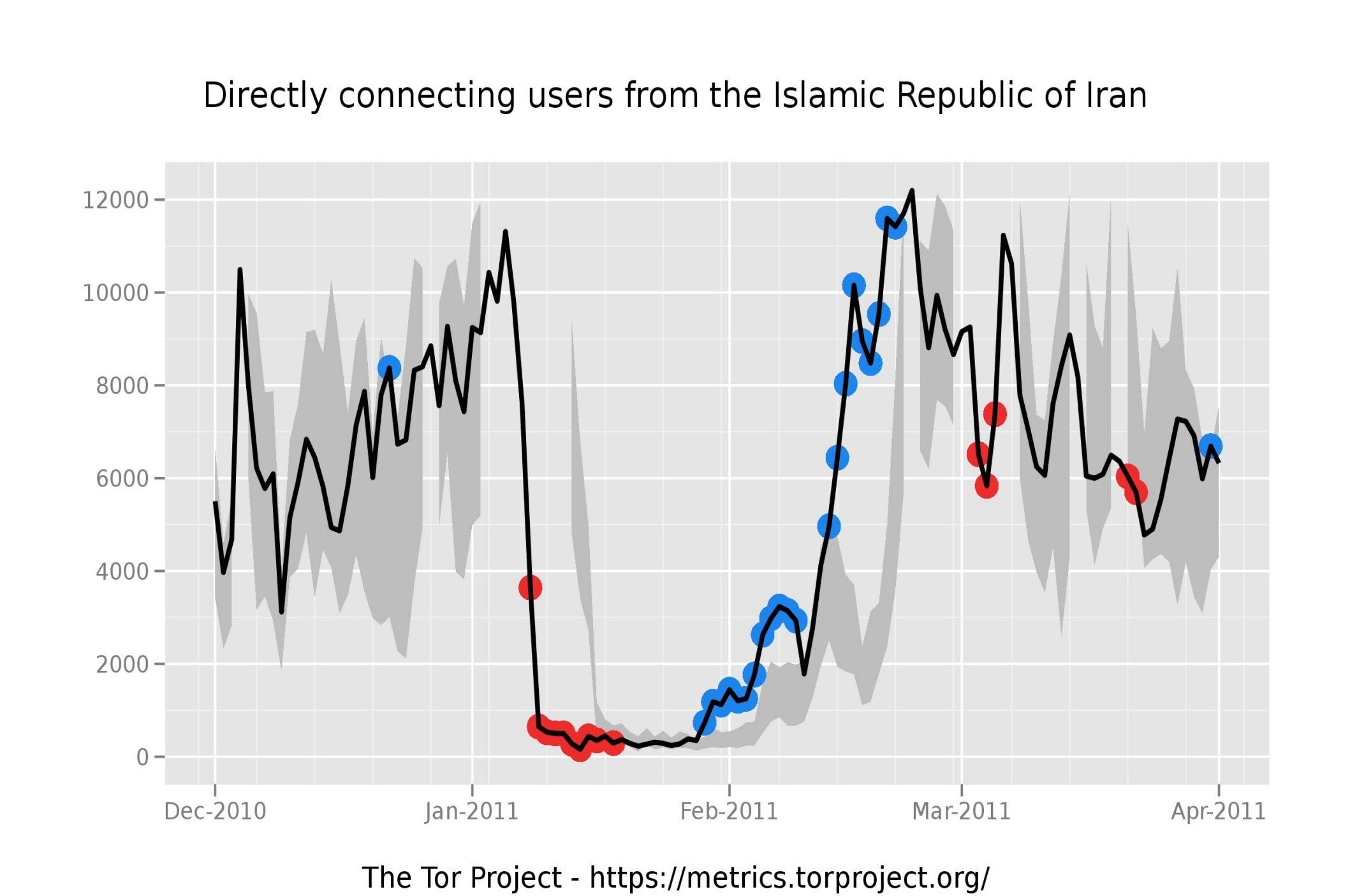

أفا oops
لقد تم منع الدخول إلى هذا الموقع
This site has been blocked
تم إيقاف عملية الدخول الى الموقع الذي تحاول زيارته نظراً لاحتوائه على محتويات محظورة
The web page you are trying to access has been blocked as the content contains prohibited materials
إذا كنت ترى أن هناك خطأ في ذلك - يرجى إرسال رسالة بريد إلكتروني إلى help@isp.qa
If you feel this is an error then please send

Building Secure Software

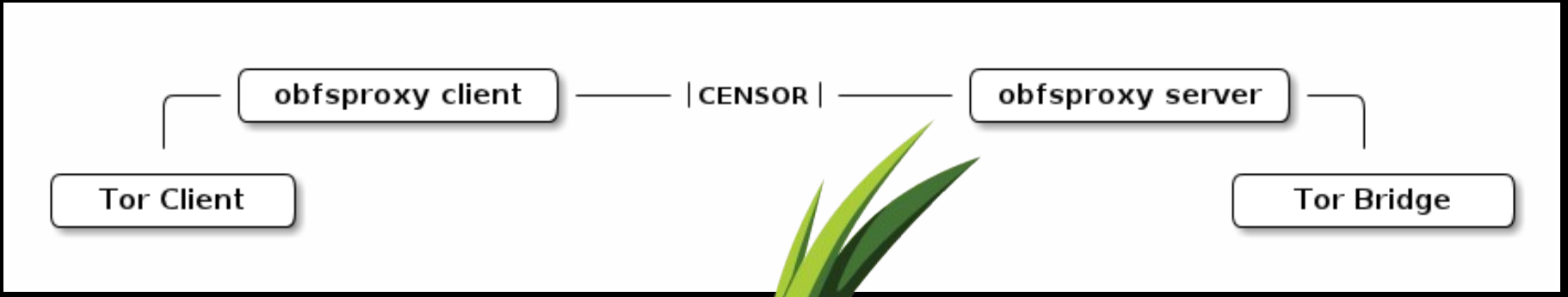
- Tor is written in the C programming language.
- Experiments with Mozilla's Rust programming language.
- Follow best practices: high coverage for tests, integration tests, coverity, static code analysis, code review policies.

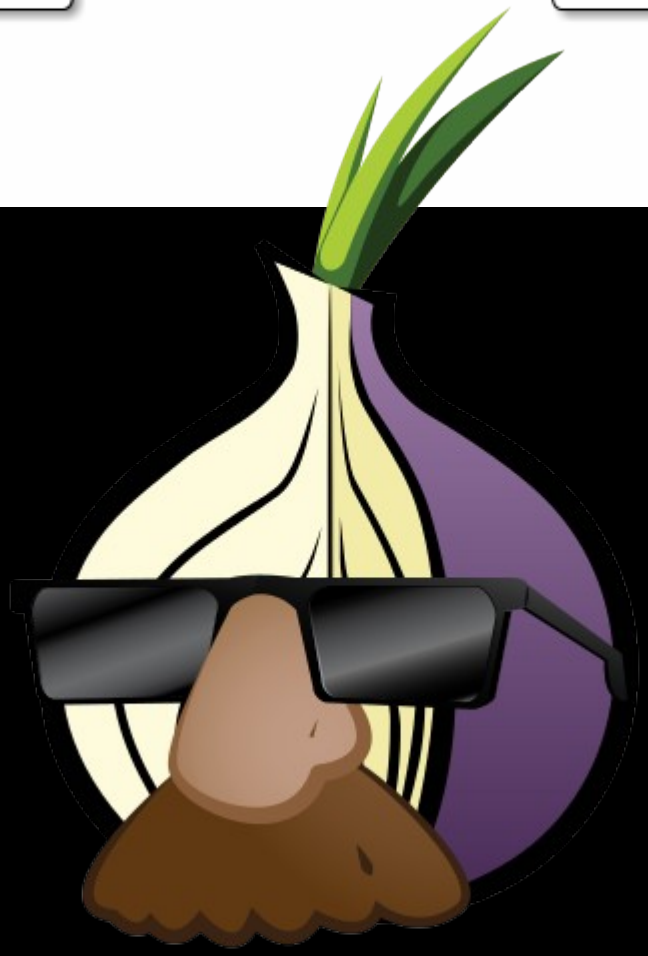
Anti Censorship

- Censors will apply censorship to nodes in the network.
- Same for **known** bridges.
- Solution: either make it hard to analyze the traffic or make it hard to block the bridges.


Directly connecting users from the Islamic Republic of Iran
12000
10000
8000
6000
4000
2000
0
Dec-2010
Jan-2011
Feb-2011
Mar-2011
Apr-2011
The Tor Project - https://metrics.torproject.org/

Pluggable Transports





The Obfourscator (obfs4)

- Does full x25519 handshakes, but uses Elligator2 to map elliptic curve points.
- Allows you to tune timers for traffic.

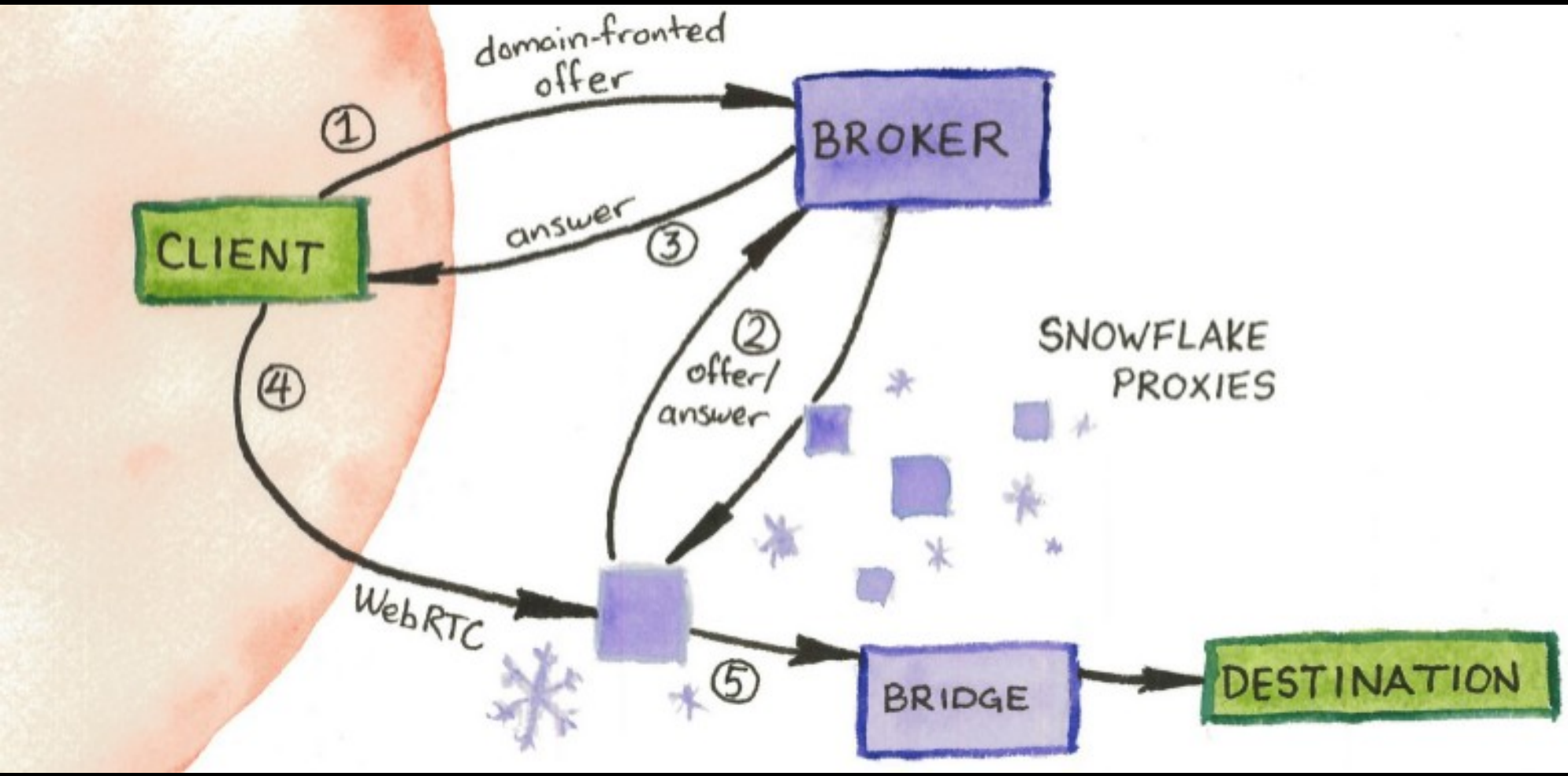
Domain Fronting (Meek)

- Connect with TLS with SNI set to some large user of the cloud provider.
- Inside your TLS connection you do a normal HTTP request, but with the Host header set to the server you want to reach inside the cloud.
- Efficient, but expensive :-(

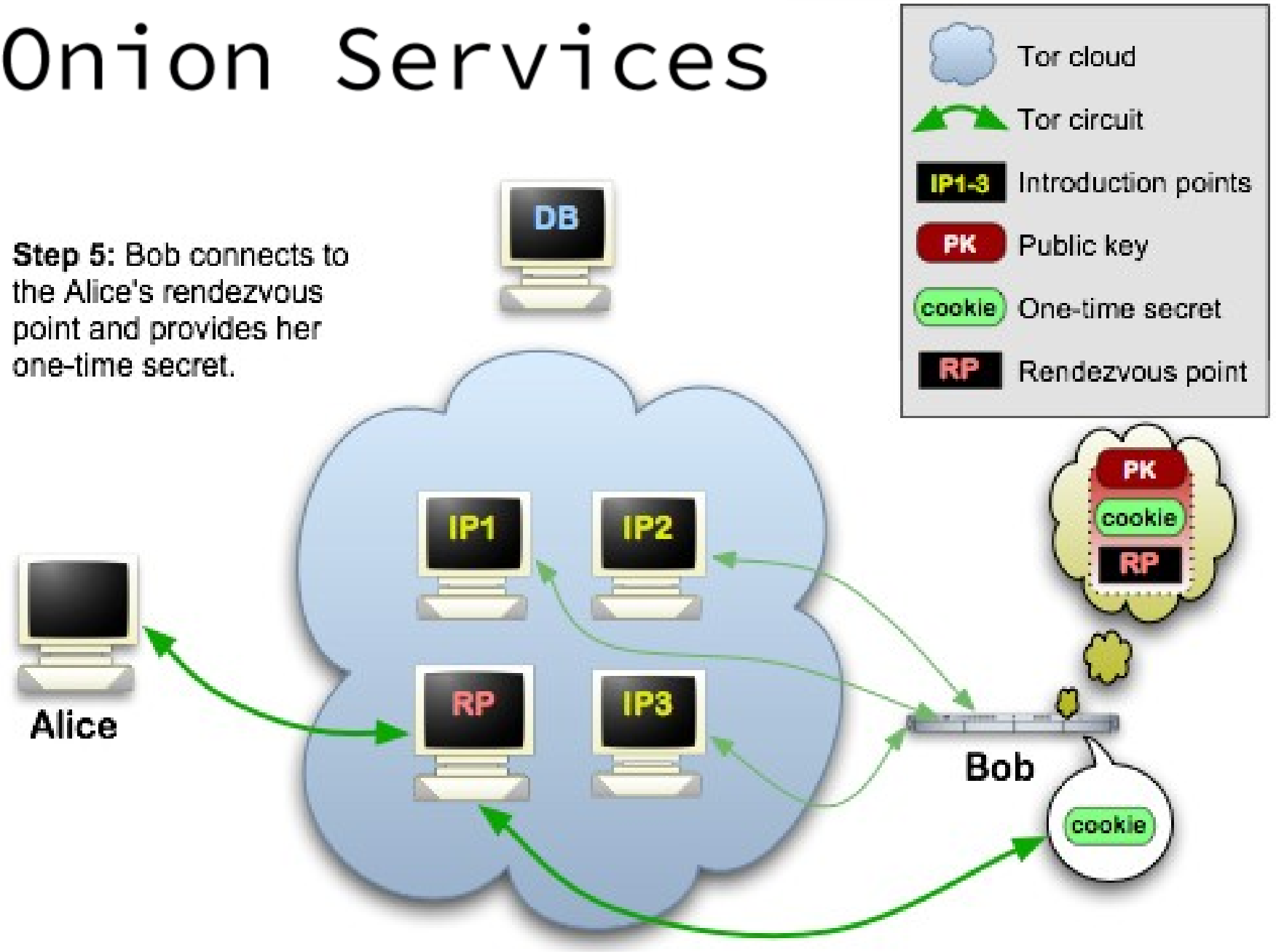
Domain Fronting

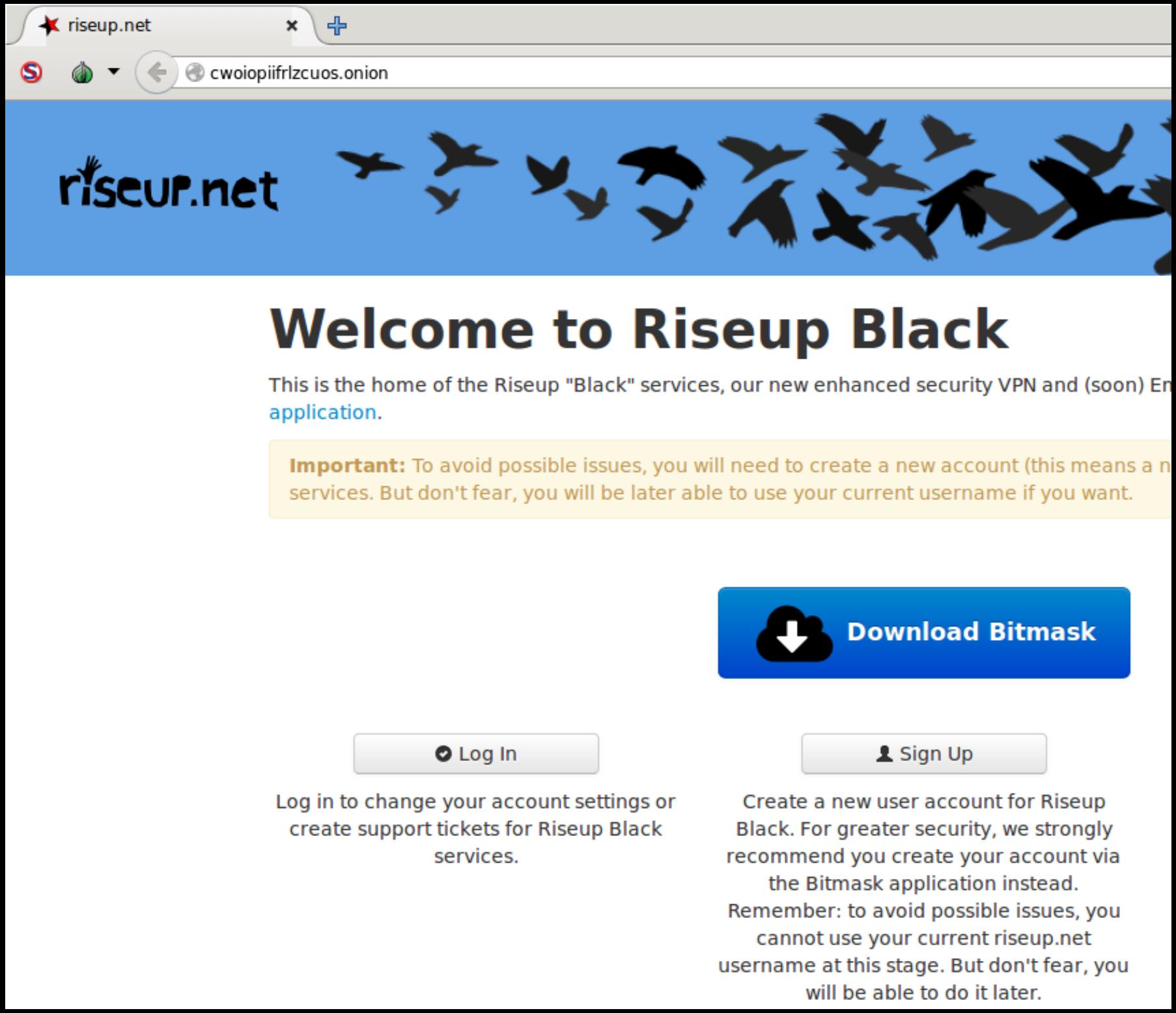
- Using ESNI?
- Using various cloud providers message queue services?
- Generally using large centralized services to give access to censored people.

Snowflake


domain-fronted
offer
1
BROKER
CLIENT
answer
3
2
offer/
answer
SNOWFLAKE
PROXIES
4
WebRTC
5
BRIDGE
DESTINATION

Onion Services




riseup.net
cwoiopiifrlzcuos.onion
riseup.net
Welcome to Riseup Black
This is the home of the Riseup "Black" services, our new enhanced security VPN and (soon) En
application.
Important: To avoid possible issues, you will need to create a new account (this means a n
services. But don't fear, you will be later able to use your current username if you want.
Download Bitmask
Log In
Log in to change your account settings or create support tickets for Riseup Black services.
Sign Up
Create a new user account for Riseup Black. For greater security, we strongly recommend you create your account via the Bitmask application instead. Remember: to avoid possible issues, you cannot use your current riseup.net username at this stage. But don't fear, you will be able to do it later.

Onion service properties

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

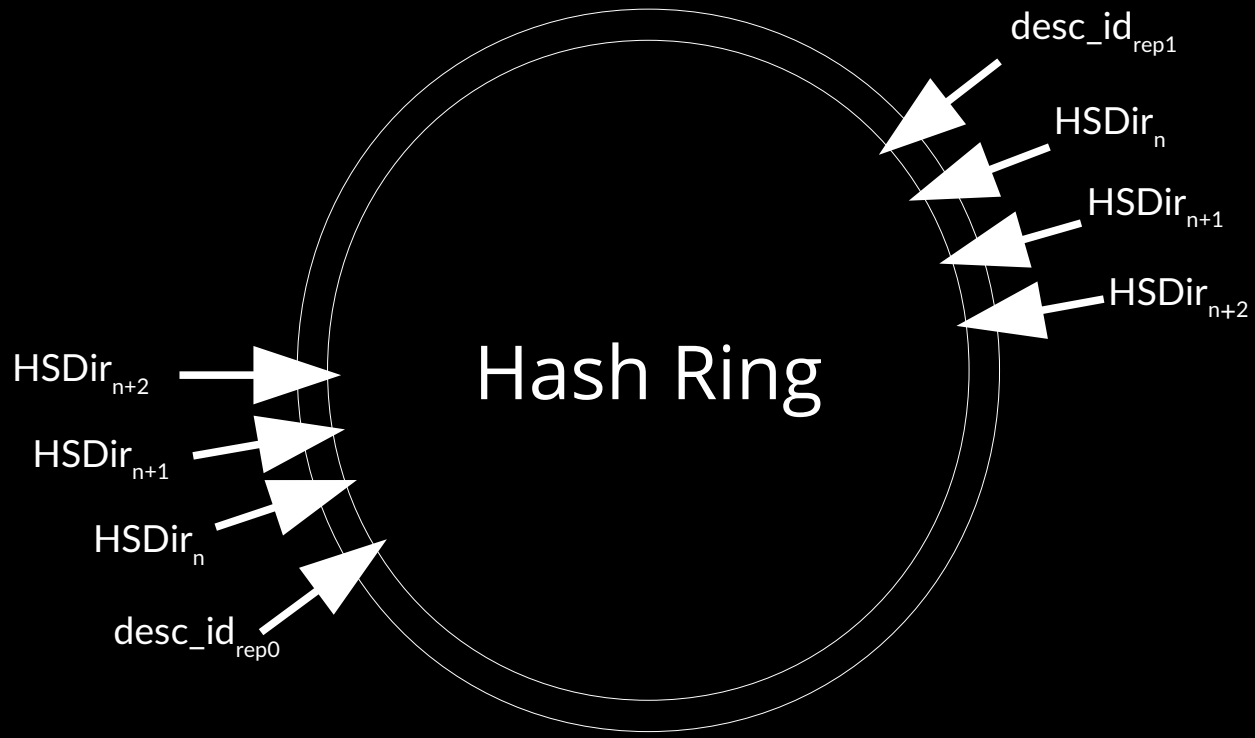
Onion service properties

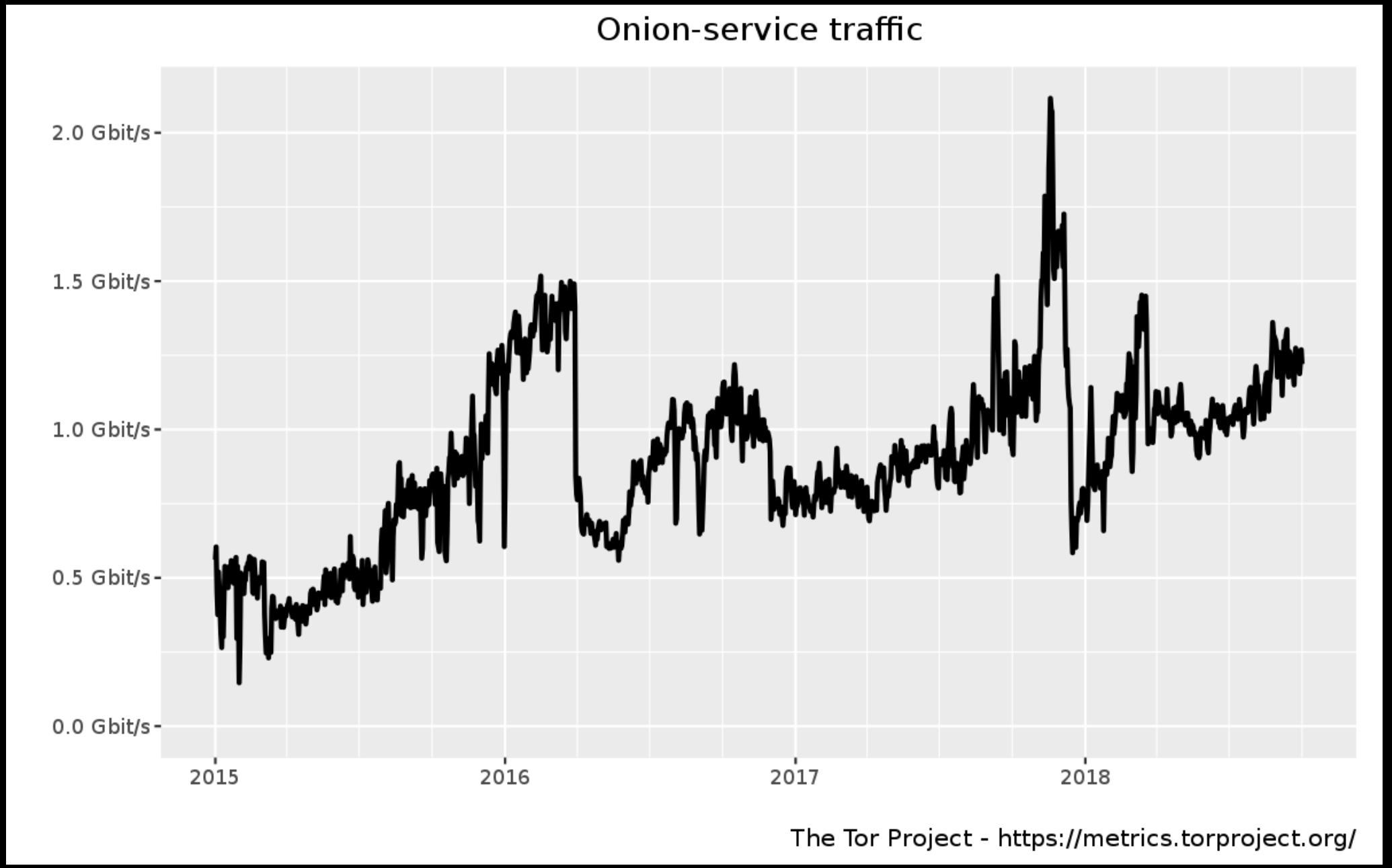
- Very long names – hard to remember for humans. V2 → V3 transition made names even longer.
- Should we have a secure and “fair” domain name system on top?

Onion service crypto

- V2: RSA-1024 + SHA-1 :-(
- V3: {ed|x}25519 + SHA-3.

Camping the Hash Ring



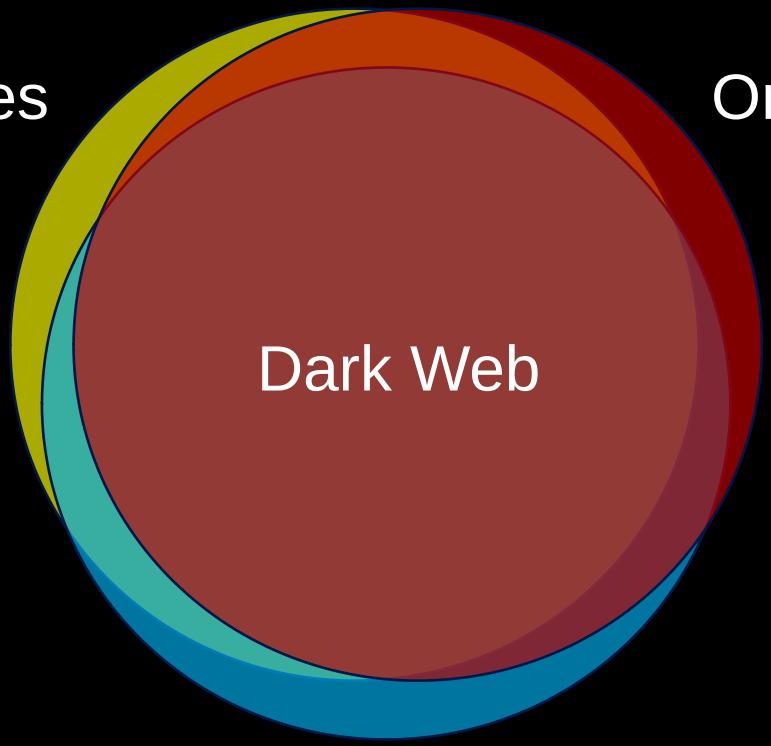

Onion-service traffic
2.0 Gbit/s
1.5 Gbit/s
1.0 Gbit/s
0.5 Gbit/s
0.0 Gbit/s
2015
2016
2017
2018
The Tor Project - https://metrics.torproject.org/


World Wide Web
Deep Web
Dark Web

The “Dark Web” as popularly depicted

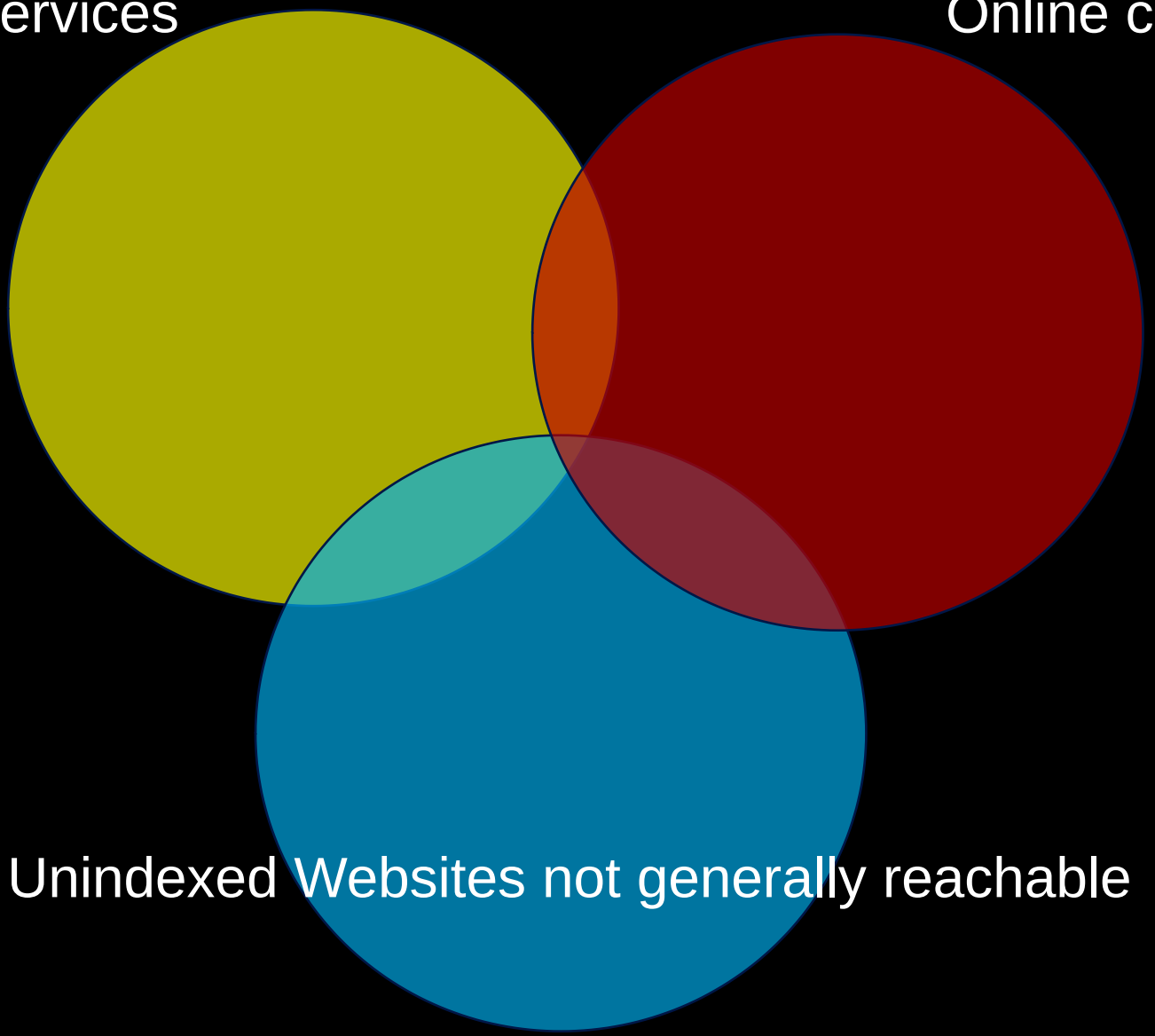
Onion services

Online criminal activity

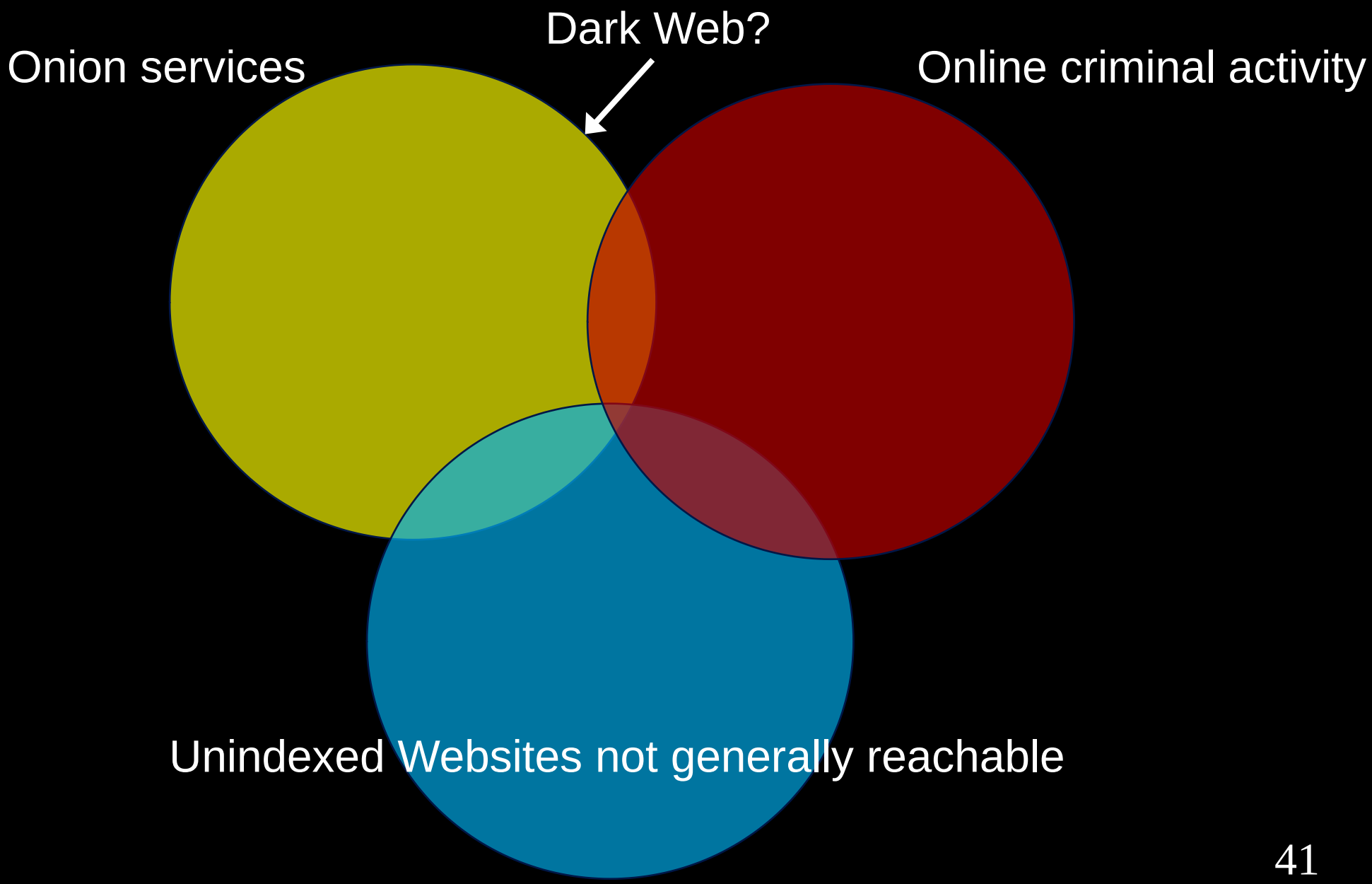


Unindexed Websites not generally reachable

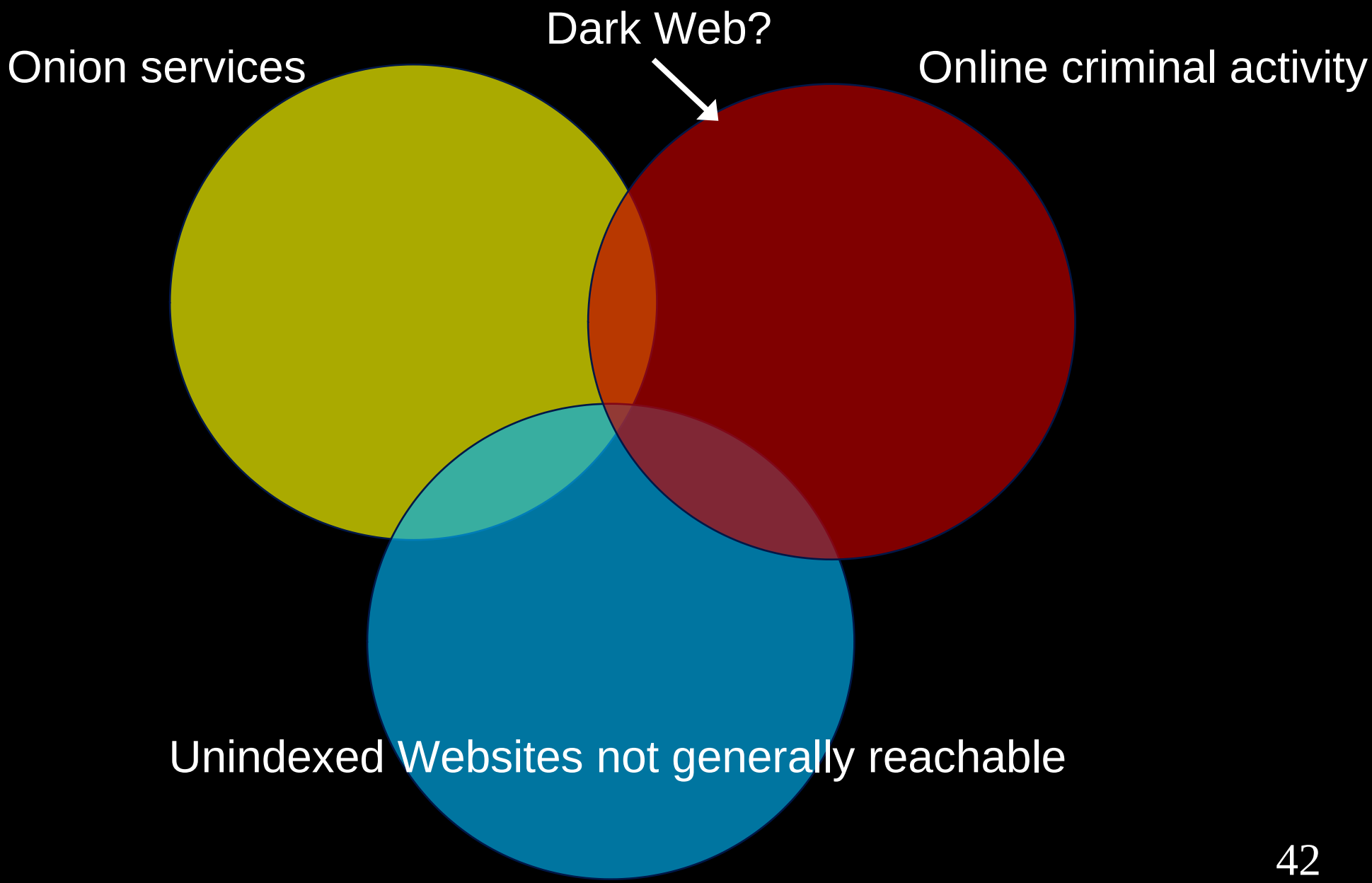
Reality


Onion services
Online criminal activity
Unindexed Websites not generally reachable

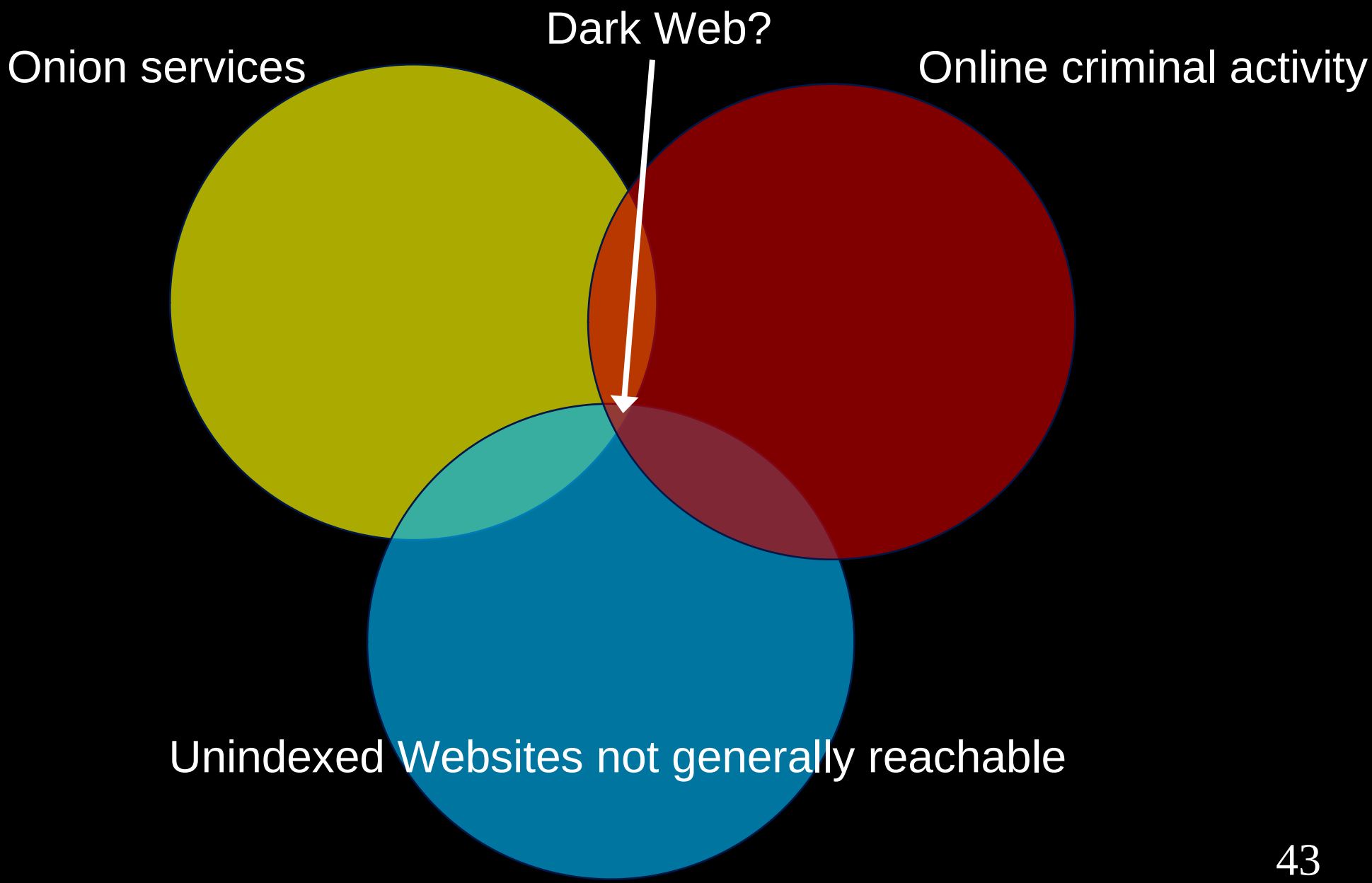
Reality


Dark Web?
Onion services
Online criminal activity
Unindexed Websites not generally reachable

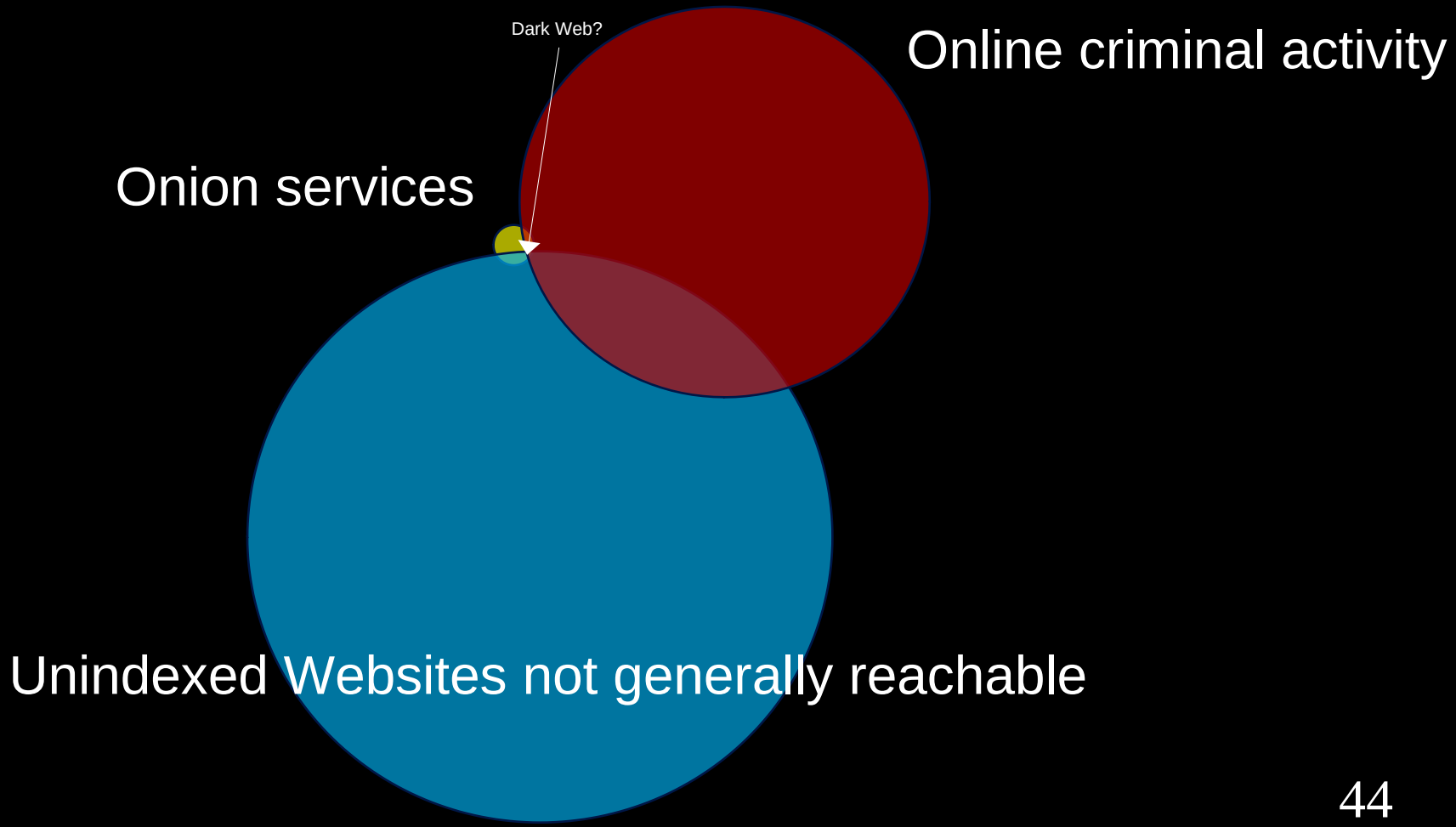
Reality

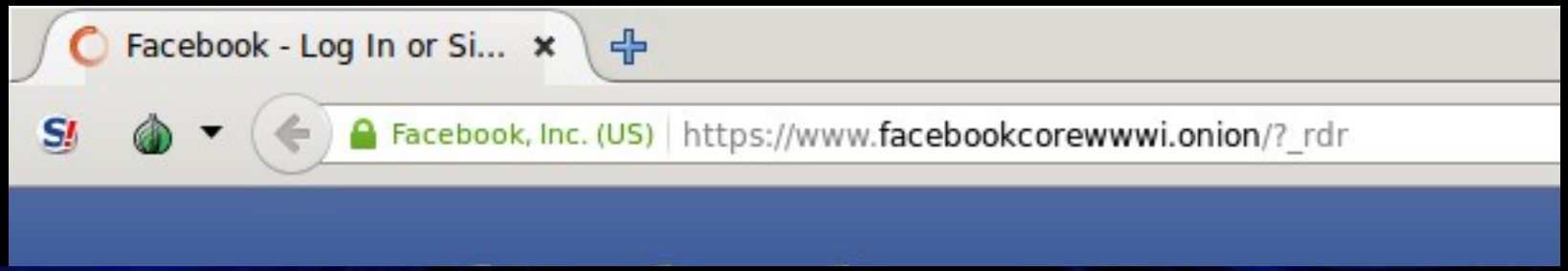

Dark Web?
Onion services
Online criminal activity
Unindexed Websites not generally reachable

Reality


Dark Web?
Onion services
Online criminal activity
Unindexed Websites not generally reachable

Scale also matters





1 Million People use Facebook over Tor

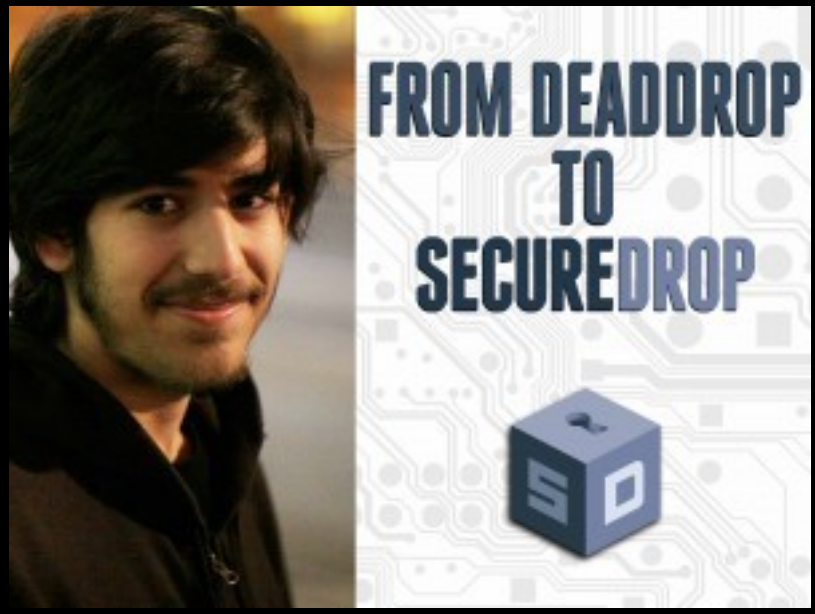
FACEBOOK OVER TOR · FRIDAY, APRIL 22, 2016

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.

SecureDrop

THE NEW YORKER
STRONGBOX

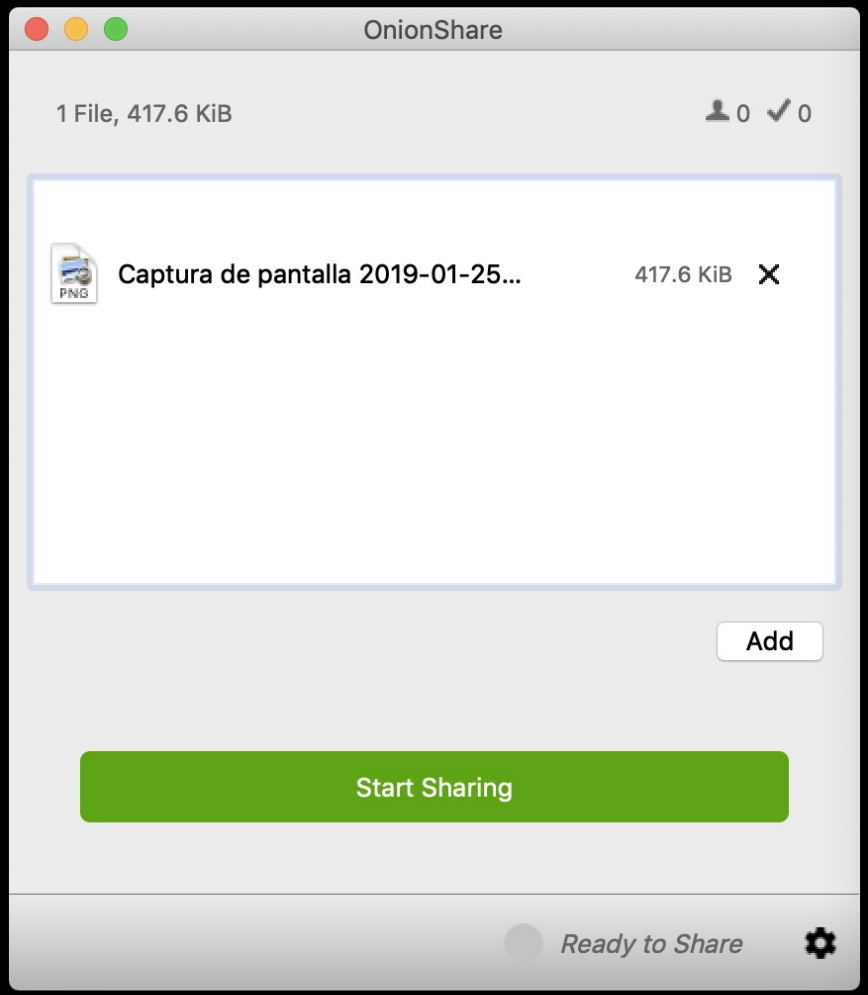


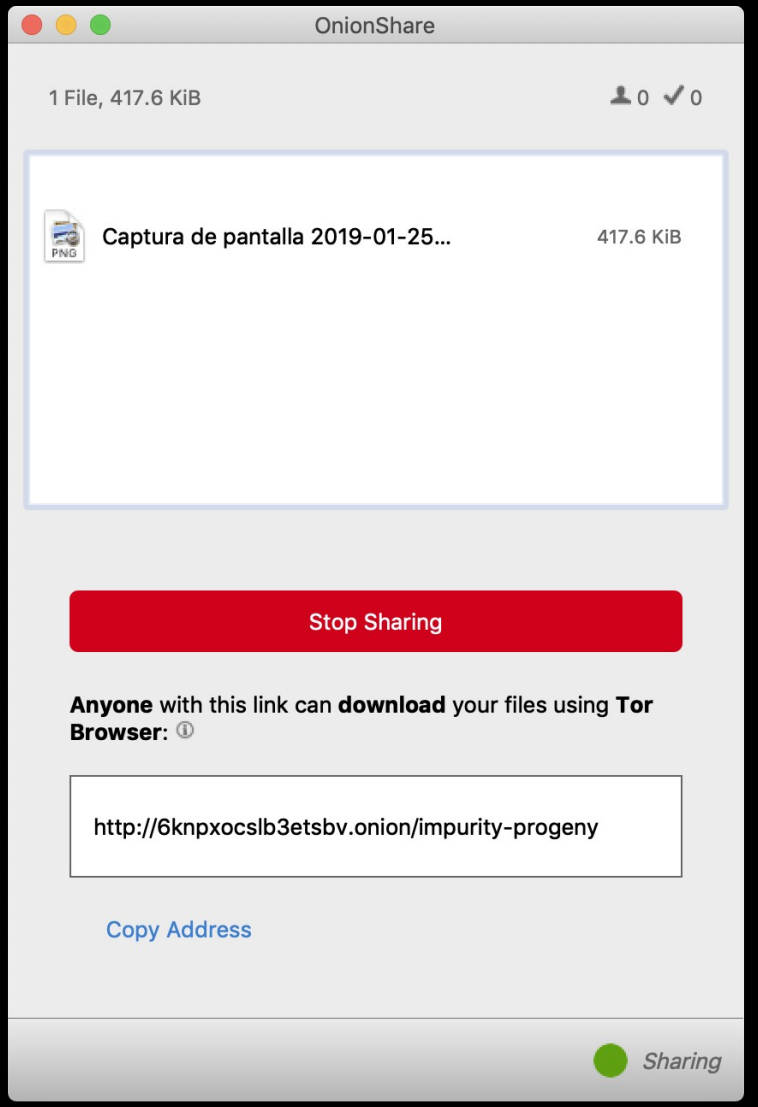
SECUREDROP

Today, 75+ organizations use SecureDrop

https://securedrop.org/directory

OnionShare


OnionShare
1 File, 417.6 KiB
0 0
Captura de pantalla 2019-01-25...
417.6 KiB
Add
Start Sharing
Ready to Share


OnionShare
1 File, 417.6 KiB
0 0
Captura de pantalla 2019-01-25...
417.6 KiB
Stop Sharing
Anyone with this link can download your files using Tor Browser:
http://6knpxocslb3etsbv.onion/impurity-progeny
Copy Address
Sharing

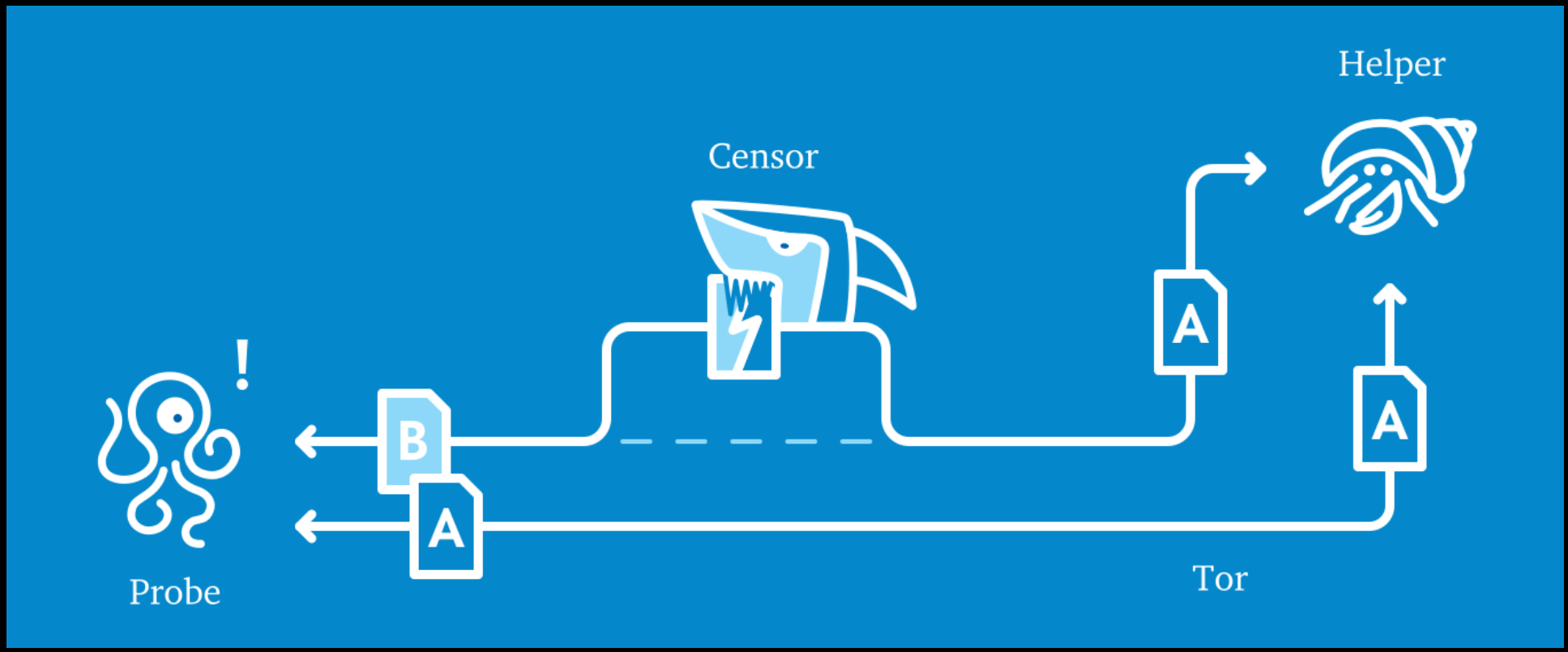
Tor isn't foolproof

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

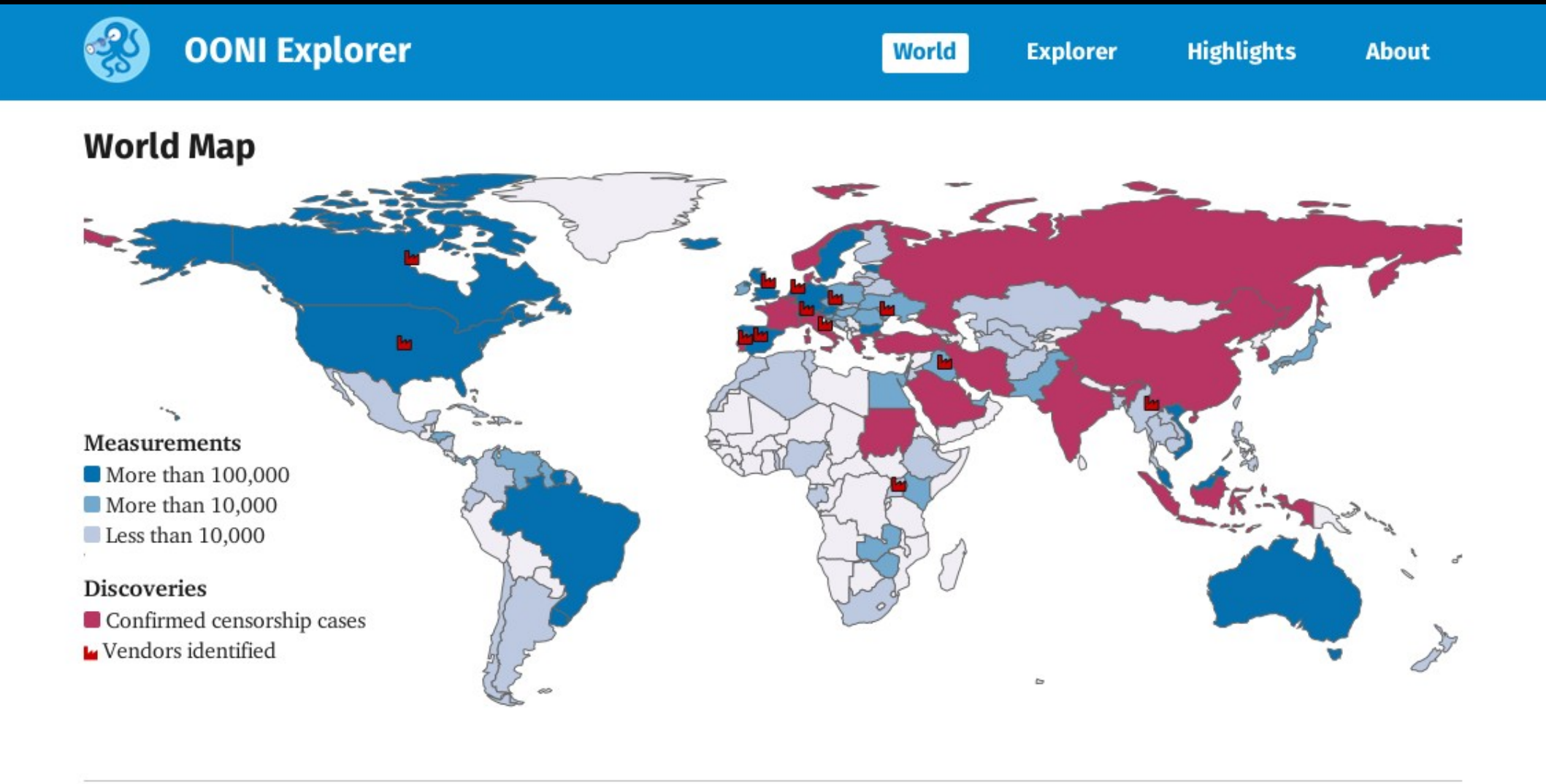
How can you help?

- 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
- Donating to the project: https://donate.torproject.org/

ooni.torproject.org



explorer.ooni.torproject.org



Questions?