ONIONS ADVENTURES

HOW TO USE ONION SERVICES AND THE  NETWORK IN YOUR WEB ENDEAVORS

hiro@torproject.org
https://mastodon.social/@nopressure
https://twitter.com/nopressure

HI! 

TOR BOOTH IN BUILDING K

(we have stickers)

RELAY OPERATOR MEETUP

15.00 SUNDAY - FEB 3RD

BUILDING H - ROOM 3244

HI, I AM SILVIA..

- Some known me as **Hiro**.
- I work at **the Tor Project.**
- I am also part of the Information Security Group in the Department of Telematics Engineering at UPC-**Barcelona** where I got my Ph.D.

KNOW YOUR ONIONS

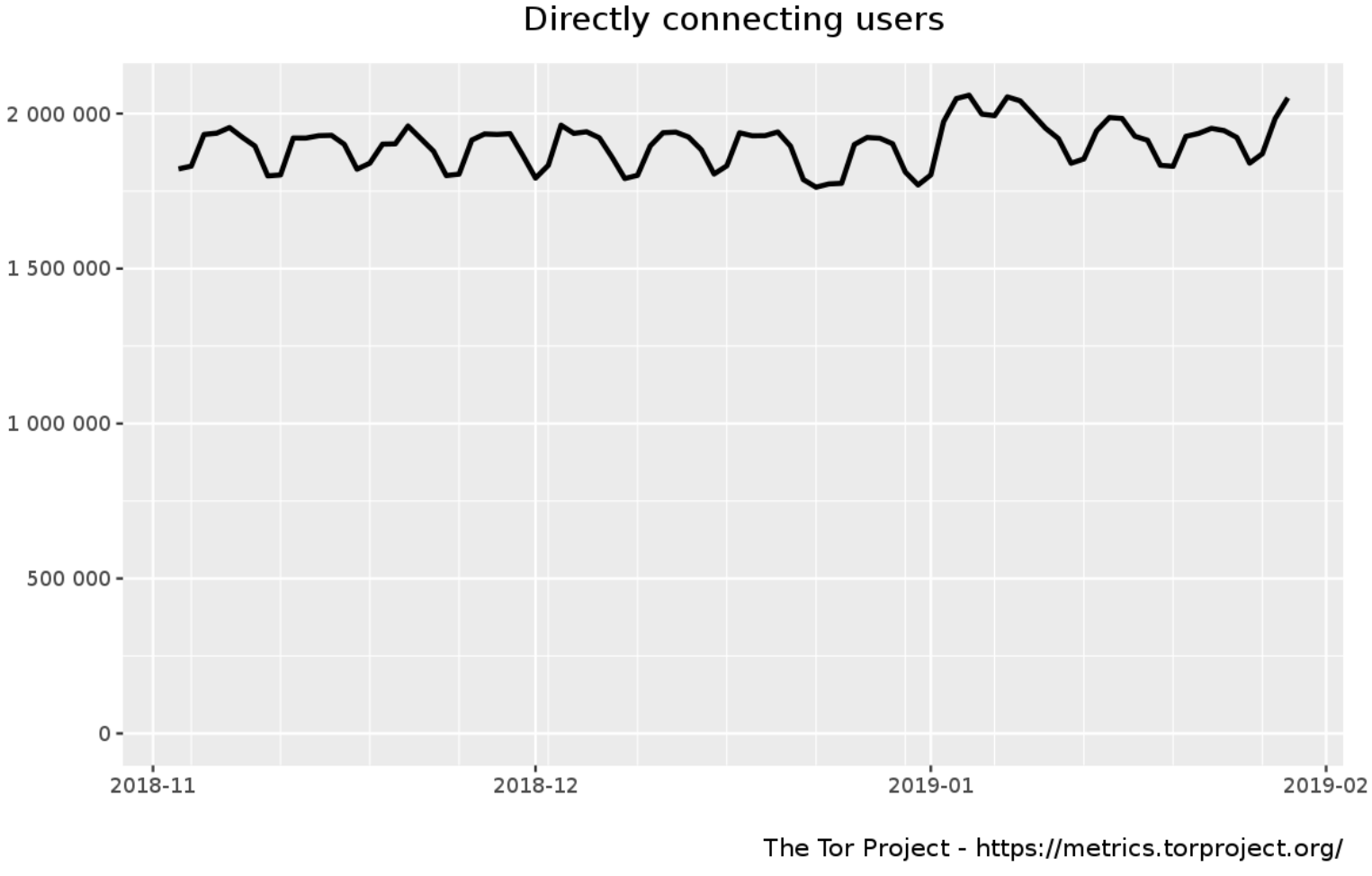
- What is Tor and **what it can do for you.**
- **Onion services** and bidirectional anonymity.
- Using onion services in your **personal** and **web projects.**

WHAT IS  AND
WHAT IT CAN DO FOR YOU

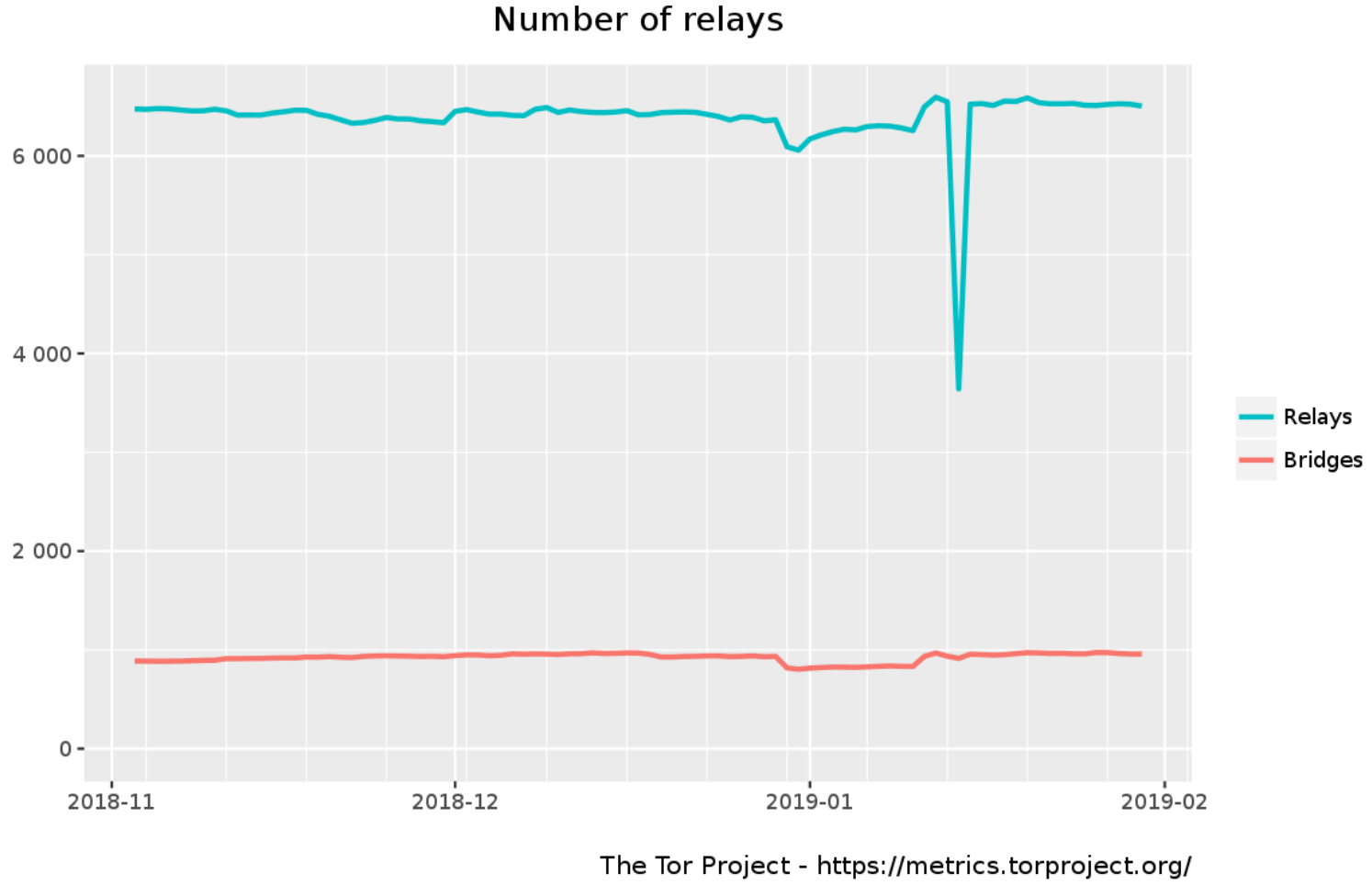
TOR IS A PRIVACY TOOL

- Tor is **free software**.
- Tor is a **community** made up of a diverse group of developers, researchers, relay operators, volunteers.
- Tor is an open **network.**
- Tor is a **non-profit.**

TOR IS ABOUT 2M DAILY USERS USING THE NETWORK!



TOR IS ABOUT 1K BRIDGES AND 6K RELAYS



WHAT DOES TOR DO?

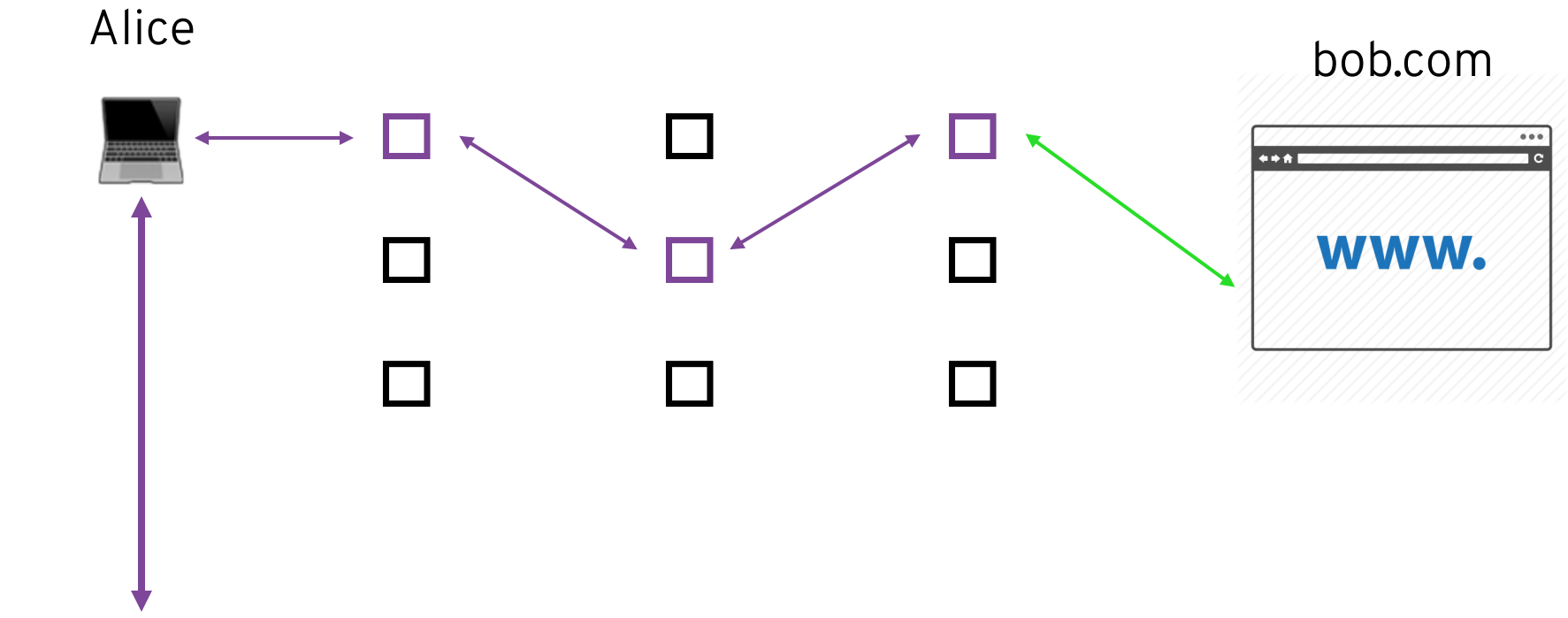
- Tor provides **privacy.**
- Tor provides **anonymity.**
- Tor provides **communication security.**
- Tor provides a **traffic analysis resistant communication network.**
- Tor provides **reachability against censorship**.

HOW DOES  PROVIDE PRIVACY AND ANONYMITY?

PRIVACY BY DESIGN

TOR PROVIDES PRIVACY BY DISTRIBUTING TRUST

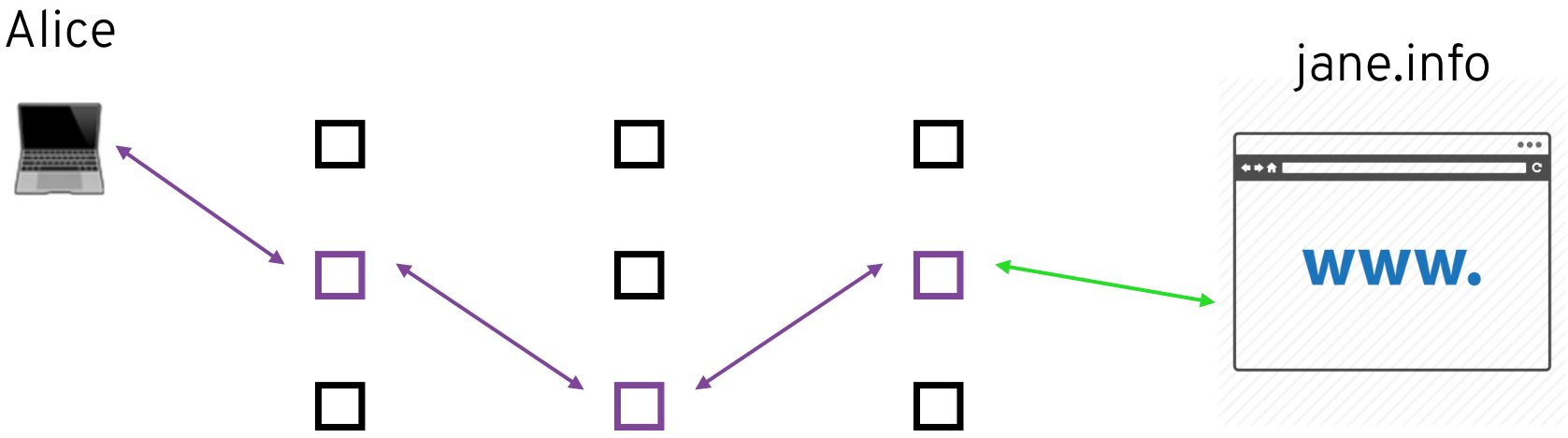
HOW TOR WORKS



Alice's Tor client obtains a list of Tor nodes from a directory server and picks a random path to destination server.

Alice wants to talk to some Bob. Alice also wants to stay safe.

HOW TOR WORKS



Alice's Tor client peaks another random path to destination server.

The connection between Alice and the tor network is encrypted.
The connection between the last exit node and Bob is not.

That's why it is important to use HTTPS!

ANONYMITY > ENCRYPTION

ANONYMITY > ENCRYPTION

- Encryption doesn't hide **conversations metadata**
- Encryption doesn't hide your **social graph**
- Encryption doesn't hide **network metadata**
- Encryption doesn't hide **your location**

USING Tor AT THE APP LAYER:

TOR BROWSER

WHAT IS TOR BROWSER

TOR BROWSER IS A MODIFIED FIREFOX ESR.

TOR BROWSER PACKAGES:

- TOR, TORBUTTON,
- TORLAUNCHER,
- NOSCRIPT,
- AND HTTPS-EVERYWHERE.

WHY TOR MAKES A BROWSER

Tor browser is designed to:

- Ensure the **safe use of Tor.**
- Reduce **linkability of user activities on different websites.**

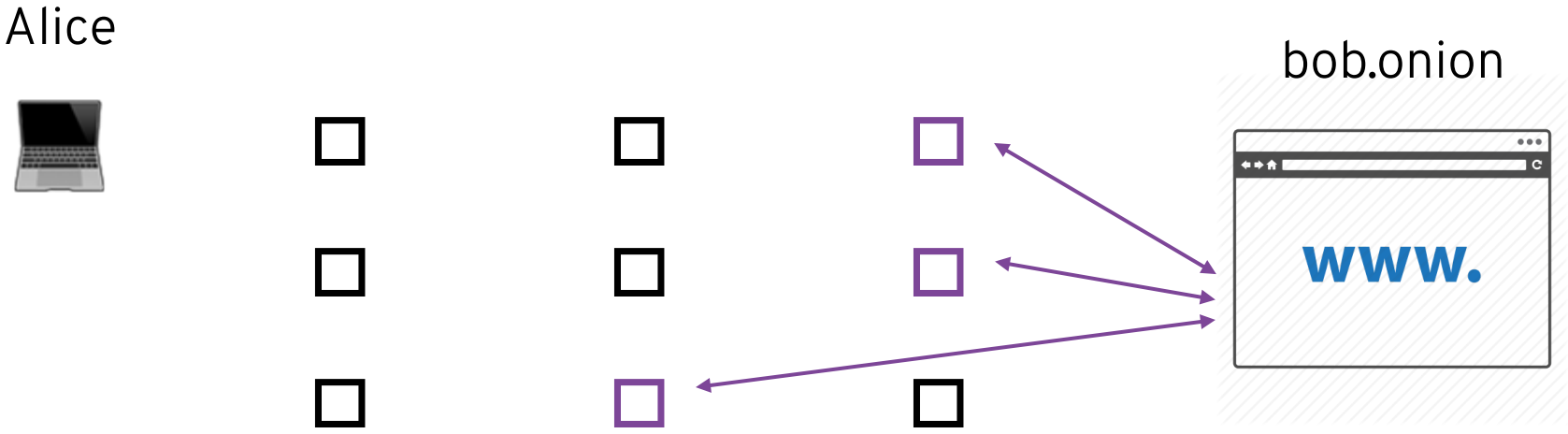
ONION SERVICES

PROVIDING BIDIRECTIONAL ANONYMITY

ONION SERVICES

- Onion services can be started from your computer
- Onion services are p2p
- Onion services are decentralised
- Onion services have a smaller attack surface
- Onion services provide by-directional anonymity
- Onion services addresses are 54 chars public keys [ed|curve25519 - Keccak(SHA3)]

HOW ONION SERVICES WORK

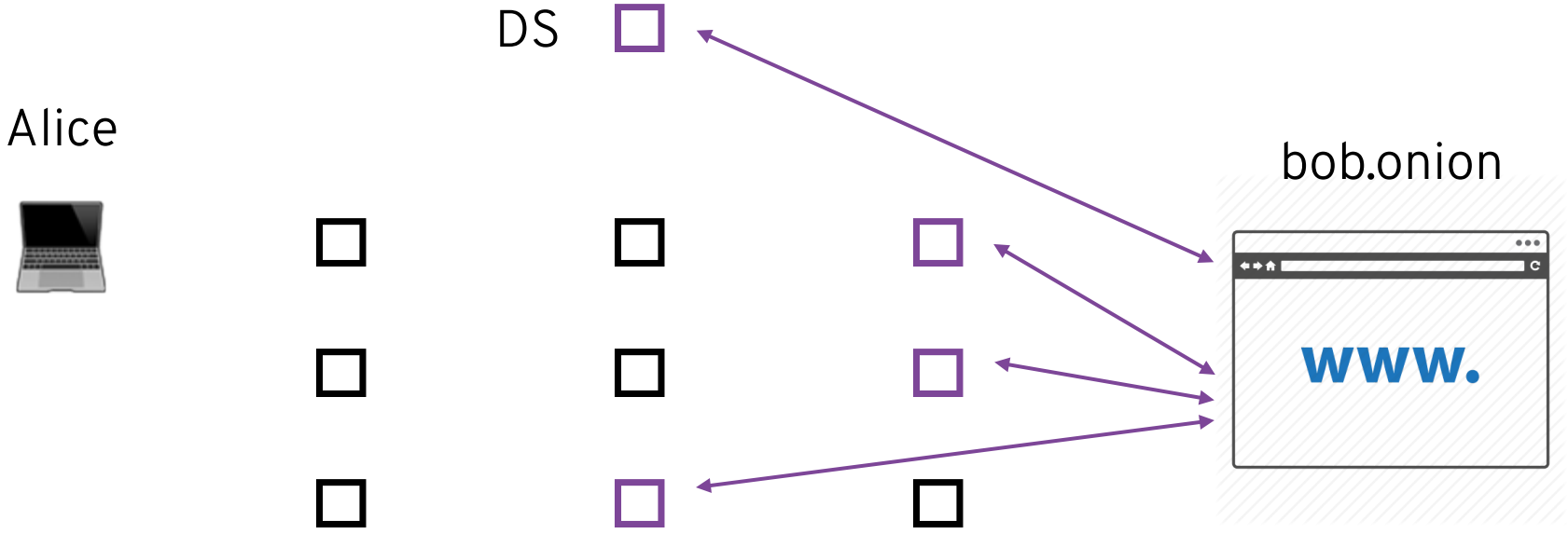


Bob picks some introduction points and builds a circuit to them...

Bob is an onion service and Alice a Tor Browser user.

Bob picks 3 introduction points and builds a circuit.

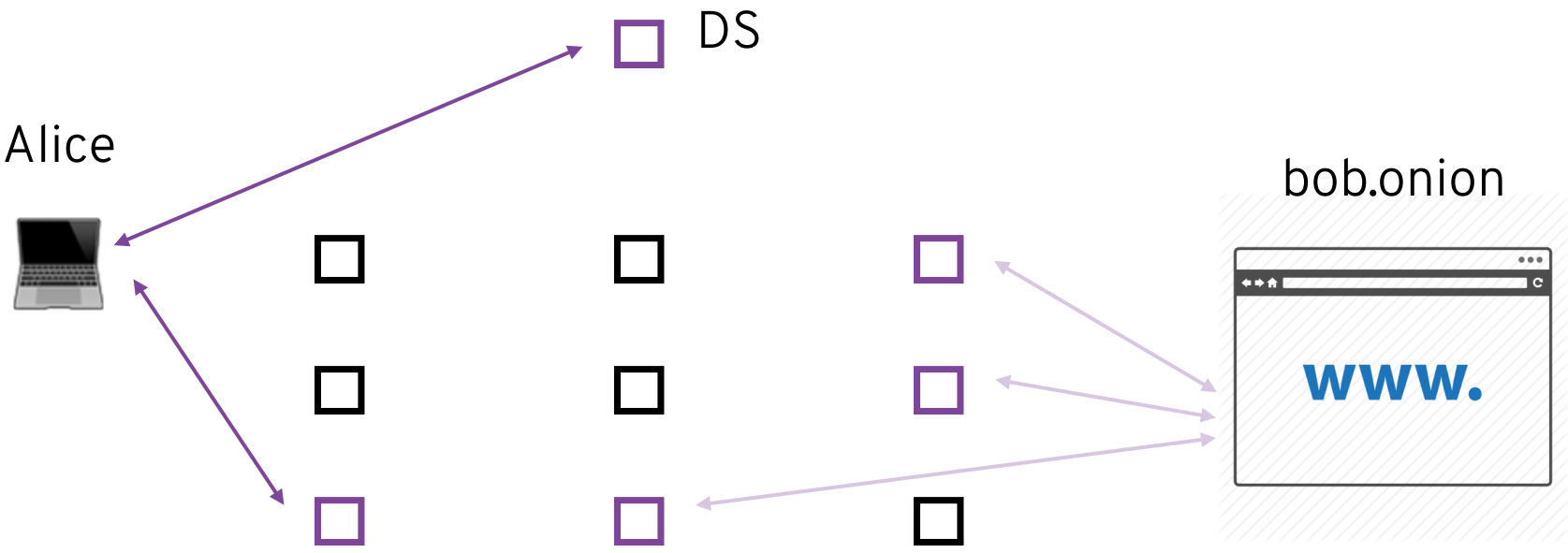
HOW ONION SERVICES WORK



Bob picks some introduction points and builds a circuit to them, then advertises its service at the database...

Bob builds a descriptor and uploads it to the directory

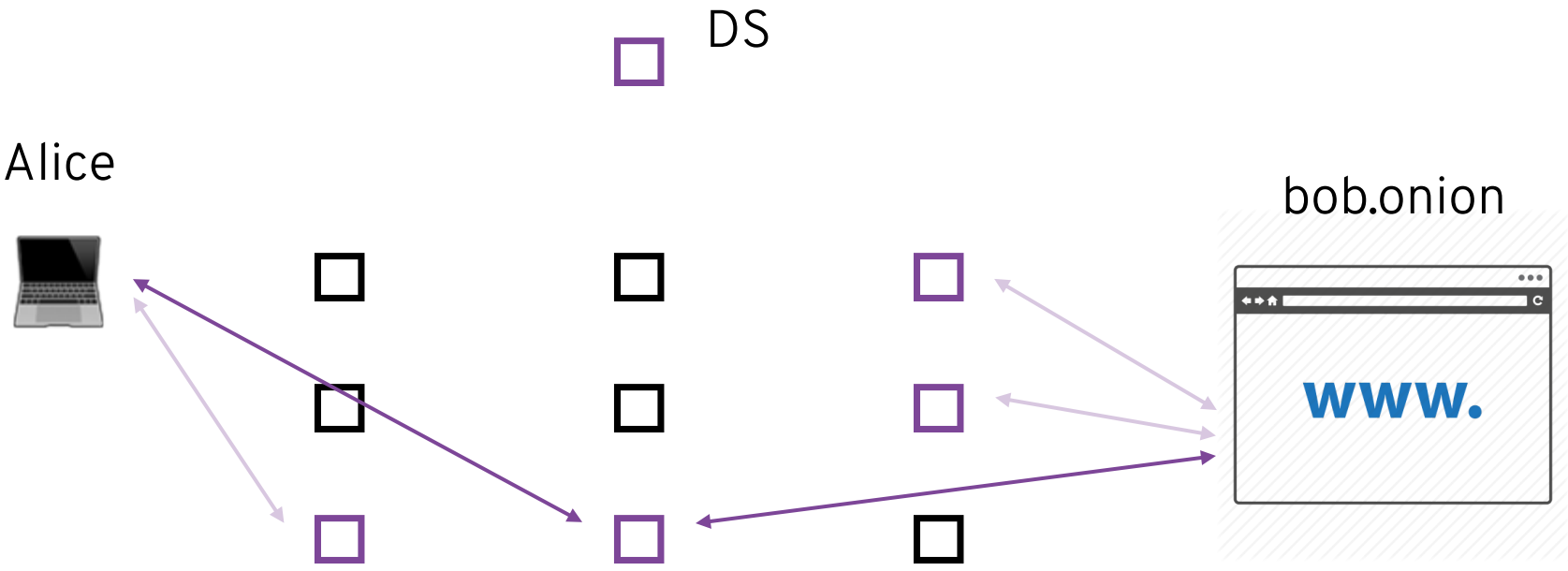
HOW ONION SERVICES WORK



Alice hears that bob.onion exists and they request more info from the database. They also setup a rendezvous point.

Alice fetches the descriptor from the directory and learns how to reach Bob.

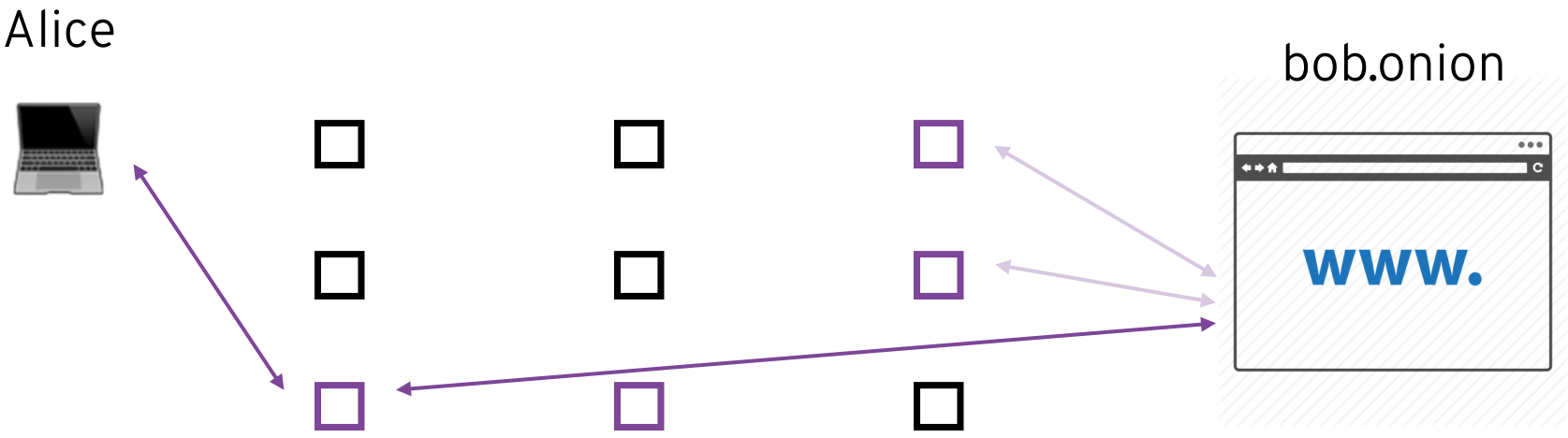
HOW ONION SERVICES WORK



Alice writes a message to Bob listing the rendezvous point and a one time secret, and asks an introduction point to deliver it to Bob.

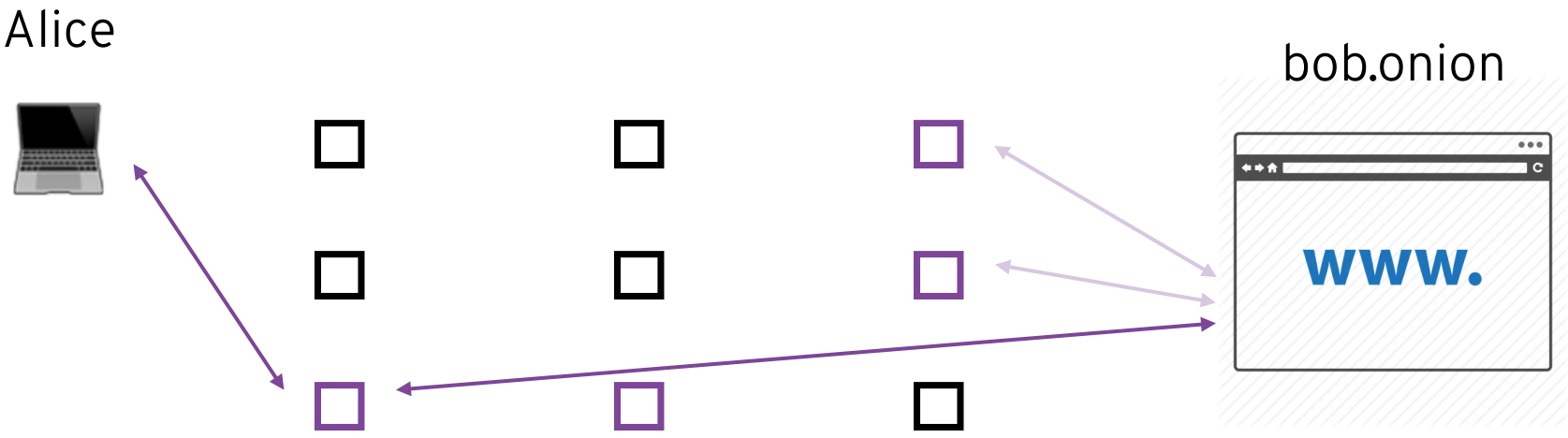
Alice tells Bob to meet her at the rendezvous point.

HOW ONION SERVICES WORK



Bob connects to Alice's rendezvous point and provides their one-time secret.

HOW ONION SERVICES WORK

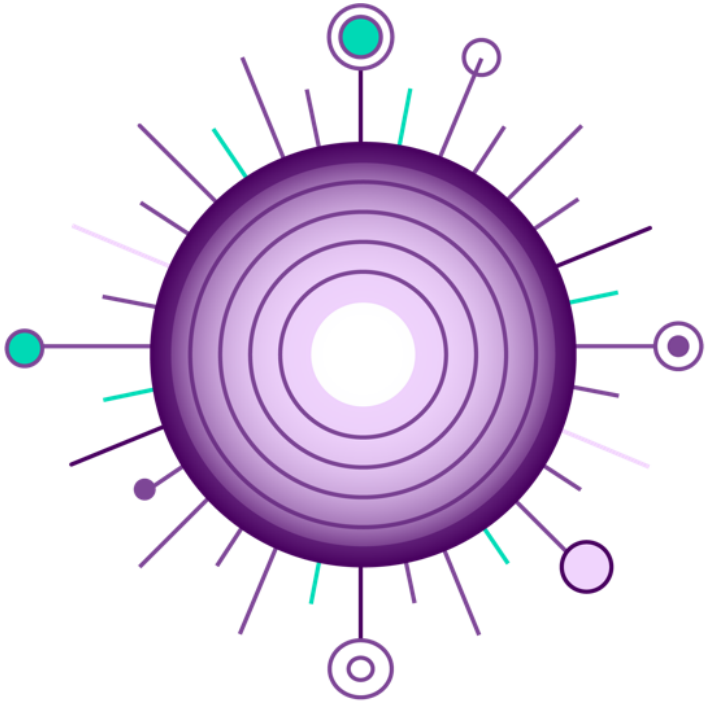


Bob and Alice use their circuit normally.

Both Alice and Bob connect with a 3 hops circuit to the RP.

TOR ECOSYSTEM

USING TOR WITHIN OTHER APPLICATIONS THROUGH ONION SERVICES.



SSH ONION-SERVICES

```
ssh:
  container_name: onion_ssh
  hostname: onion_ssh
  build: ${PWD}/config/ssh
  command: /home/root/init.sh
  volumes:
    - ./config/ssh/tor/torrc:/etc/tor/torrc
    - ./config/ssh/keys/:/home/root/.ssh/keys
    - ./config/ssh/init.sh:/home/root/init.sh
    - ./config/ssh/sshd_config:/home/root/.ssh/ssh/sshd_config
  ports:
    - "2222:22"
```

```
FROM debian
MAINTAINER hiro <hiro@torproject.org>
RUN apt-get update
RUN apt-get install -y sudo vim openssh-server tor
USER root
RUN mkdir -p 700 /home/root/.ssh \
    && mkdir /var/run/sshd \
    && mv /etc/ssh /home/root/.ssh/ssh \
    && ln -s /home/root/.ssh/ssh /etc/ssh
WORKDIR /home/root
VOLUME /home/root
EXPOSE 22
```

SSH ONION-SERVICES

```
## /etc/torcc
##
############### This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

HiddenServiceDir /home/tor/onion_ssh_service/
HiddenServicePort 22 127.0.0.1:22
```

TORSOCKS

```
$ torsocks curl http://yjuwkcxlgo7f7o6s.onion/
```

- **Torsocks** is a wrapper use applications through the Tor network
- In this example, we **run curl through the tor network** and reach the onion address for archive.torproject.org
  - https://trac.torproject.org/projects/tor/wiki/doc/torsocks
- We have a **how-to torify apps** [WIP]
  - https://trac.torproject.org/projects/tor/wiki/doc/TorifyHOWTO

USING THE SOCKS5 PROXY

```
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import requests

proxies = {
    'http': 'socks5://127.0.0.1:9050',
    'https': 'socks5://127.0.0.1:9050'
}

r = requests.get('http://yjuwkcxlgo7f7o6s.onion/', proxies=proxies)
```

- We can use the **SOCKS5 proxy** provided by tor
- In this example, we fetch **archive.torproject.org** via its onion address

ONIONS FOR THE DECENTRALISED WEB

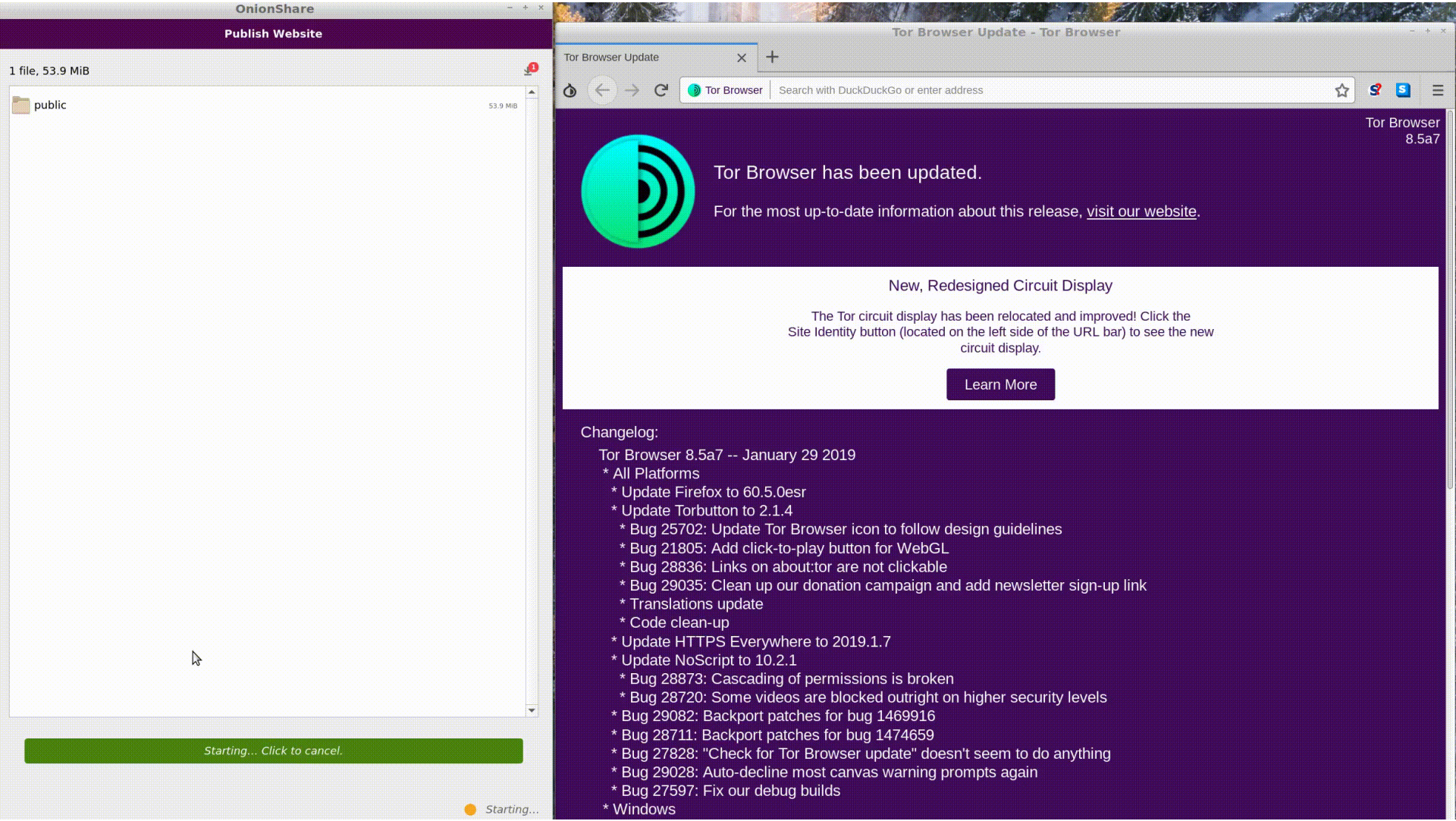
Onion services can also be used for **p2p applications**:

- **OnionShare** is a file sharing app that works by starting a web server, making it accessible as a Tor Onion Service, and generating an unguessable URL to access and download the files.
  - **https://onionshare.org**

NEXT STEP

Use Onionshare to share static websites.

ONIONS FOR THE DECENTRALISED WEB



ONIONS FOR THE DECENTRALISED WEB

NEXT STEP

Start a container from any device and share any kind of service and make this as easy as opening an app!

MyOnion is a proof of concept to run onion services into docker containers from your command line, via cli, or more simply via gui.

This project explore the idea of running ephemeral onion services on the Tor network.

https://github.com/hiromipaw/myonion/

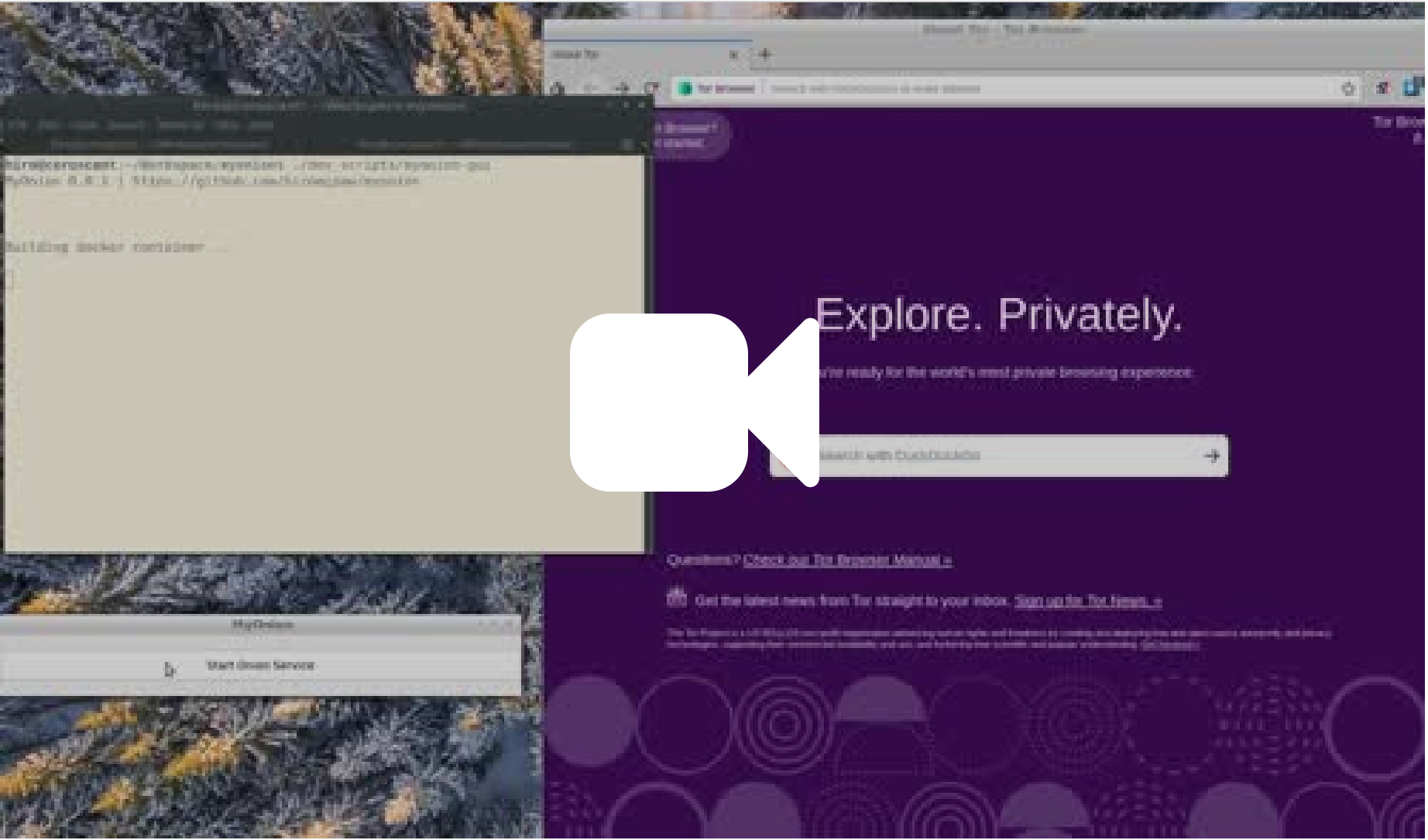
ONIONS FOR THE DECENTRALISED WEB

```
api_client = docker.APIClient(base_url='unix://var/run/docker.sock')

client = docker.from_env()

build = [line for line in
api_client.build(
path=self.common.get_resource_path('containers/website'), tag='website', dockerfile='./Dockerfile'
)

]

container = client.containers.run('website:latest', detach=True)
```

ONIONS FOR THE DECENTRALISED WEB

```
FROM debian

RUN \
    apt-get update && \
    apt-get install -y nginx tor && \
    rm -rf /var/lib/apt/lists/* && \
    echo "\ndaemon off;" >> /etc/nginx/nginx.conf && \
    chown -R www-data:www-data /var/lib/nginx

COPY tor/torrc /etc/tor

COPY default /etc/nginx/sites-available/

...
```

ONIONS FOR THE DECENTRALISED WEB



ONIONS FOR THE DECENTRALISED WEB

Because .onion services live on the Tor network, you do not need hosting or a public ip address to offer some service via .onion address.

This means .onion services are a gateway to a decentralised, peer-to-peer internet, where you regain control on the content you create and who you are sharing it with.

The .onion is hosted on your computer for the time you desire, allowing the people visiting your site to remain anonymous, and also you.

We believe anonymity to be very important since it can free people, allowing them to decide how to expose themselves or to make themselves visible on their own terms.

“ Cyberspace.
A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts...

A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...

William Gibson, Neuromancer

LEARN MORE...

- **www.torproject.org**
- **Tor Browser design doc**
  - [www.torproject.org/projects/torbrowser/design/]
- **Mozilla Firefox Extended Support Release**
  - [www.mozilla.org/en-US/firefox/organizations/]
- **Tor Projects**
  - [www.torproject.org/projects/projects]
- **Tor Rendezvous Specification - Version 3**
  - [gitweb.torproject.org/torspec.git/tree/rend-spec-v3.txt]
- **Secure Messaging with Onion Services, a How-To**
  - [blog.torproject.org/secure-messaging-onion-services-how]