Защита данных через P2P-сети и SAFE Network

Никита Баксаляр — @nbaksalyar

DEF CON NN

Текущее состояние Интернета

- Воровство и утечки личных данных

Текущее состояние Интернета

- Воровство и утечки личных данных

«Yahoo подтвердил утечку 500 млн учётных записей»

— *OpenNET, 22.09.2016*

Текущее состояние Интернета

- Воровство и утечки личных данных

«117 млн паролей от LinkedIn выставлены на продажу»

— *Xakep.ru, 19.05.2016*

Текущее состояние Интернета

- Воровство и утечки личных данных

«Данные более 100 млн аккаунтов «Вконтакте» продаются в сети за 1 биткоин»

— *GeekTimes, 06.06.2016*

Текущее состояние Интернета

- Цензура и государственный контроль

Текущее состояние Интернета

- Цензура и государственный контроль

  2012: Закон о блокировках в России

Текущее состояние Интернета

- Цензура и государственный контроль

  2012: Закон о блокировках в России
  2013: Сноуден

Текущее состояние Интернета

- Цензура и государственный контроль

  2012: Закон о блокировках в России
  2013: Сноуден
  2016: Закон Яровой

Текущее состояние Интернета

- Централизованность и отсутствие анонимности

Вопросы

- Кто виноват?
- Что делать?

Решение — оверлейные сети

- «Луковая» и «чесночная» маршрутизация (Tor и Onion, I2P)

- Не панацея: не спасают от воровства данных

Решение — P2P-сети

- IPFS, ZeroNet, SAFE
- BitTorrent на стероидах
- Данные хранятся не в цельном виде,
  а в зашифрованном и по кусочкам

Маршрутизация

- **Kademlia DHT**.
  Распределенная таблица хэшей, используемая в протоколе BitTorrent

- Заменяет слой маршрутизации по IP-адресам на XOR-метрику

Маршрутизация

- Bootstrap: процесс присоединения к сети
- Запрашивая данные из сети, узел добавляет информацию о себе в хэш-таблицу
- В BitTorrent: информация о сидах от трекера или от точки входа DHT — router.bittorrent.com

Адресация в Интернете (URL)

```
http://petya.ru/movie.mp4

                    ->

                              192.168.255.1:80

                              GET /movie.mp4
```

Адресация в P2P-сетях (URI)

```
$ sha1sum movie.mp4
```

->

0xa03daa..b2ce7

Адресация в P2P-сетях (URI)

```
$ sha1sum movie.mp4
```

->

```
01101110…01001
```

P2P-адресация — XOR-метрика

- ID ноды = 160 бит

Петя = **0xCAFE...1337**

Вася = **0x0001...4242**

P2P-адресация — XOR-метрика

- ID ноды = 160 бит

Петя = **101111…0010**

Вася = **101001…0101**

Как найти файл?

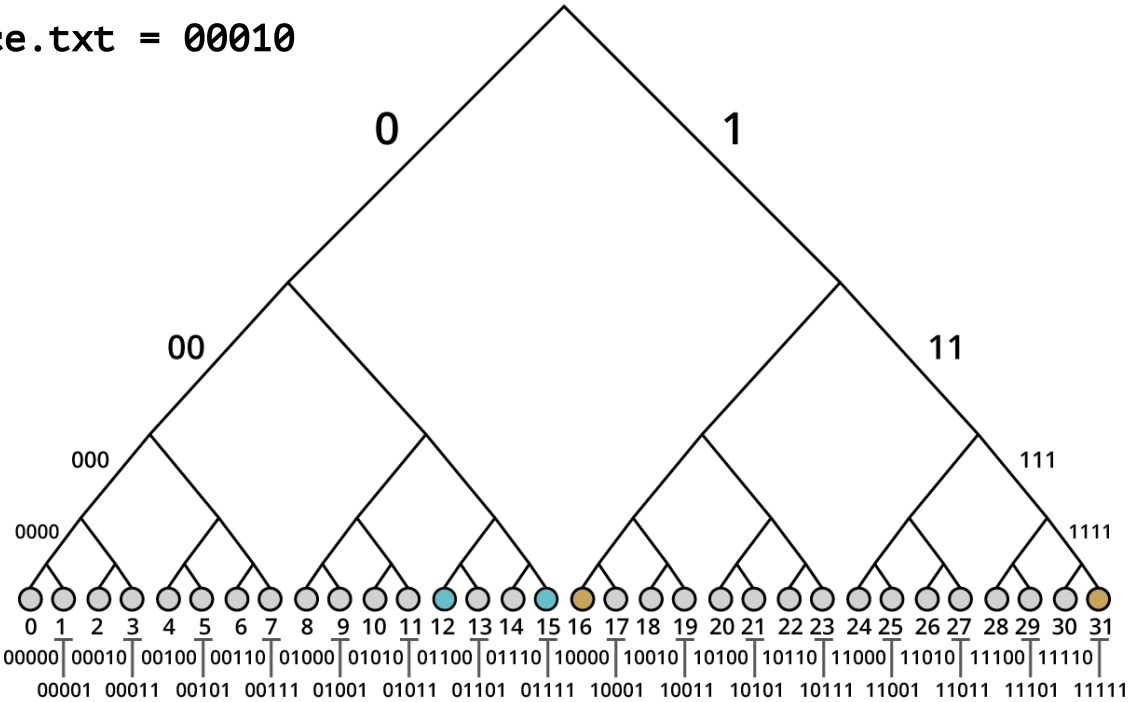
- Дистанция = XOR(хэш файла, ID узла)

Петя = **101111…0010**
movie.mp4 = **011011…0100**

XOR = **110100…0111**
= **210427**

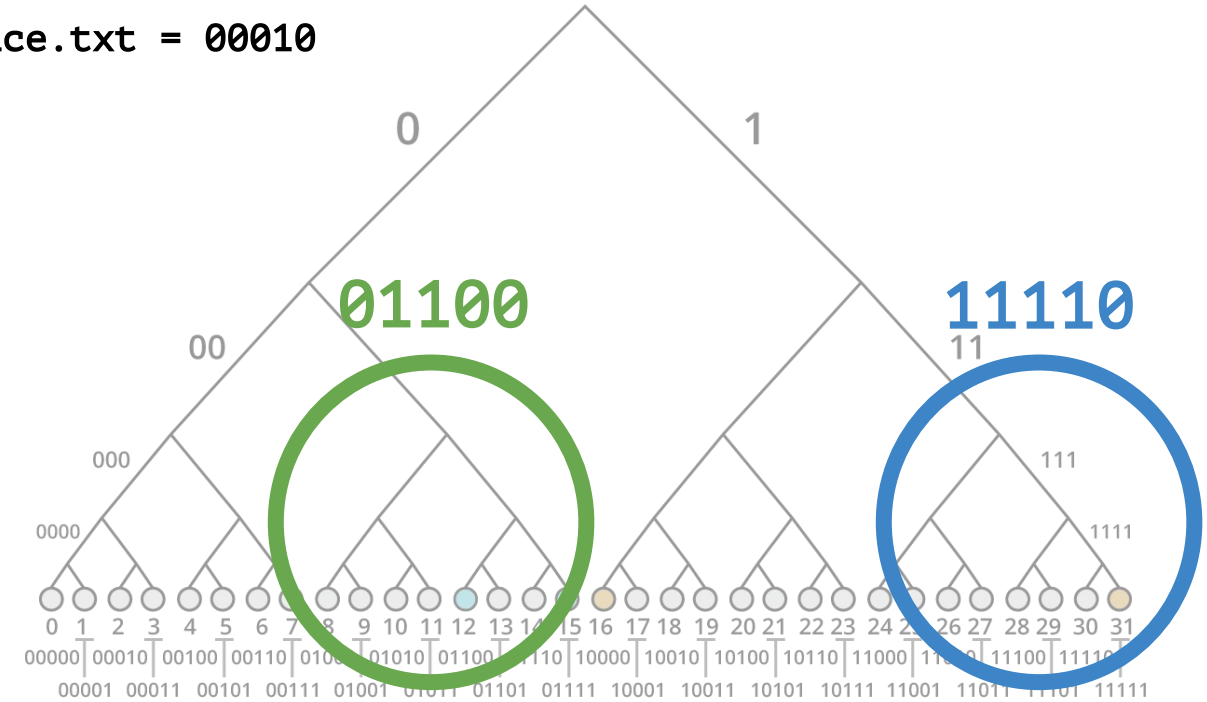
P2P-адресация — XOR-метрика

```
war_and_peace.txt = 00010
```



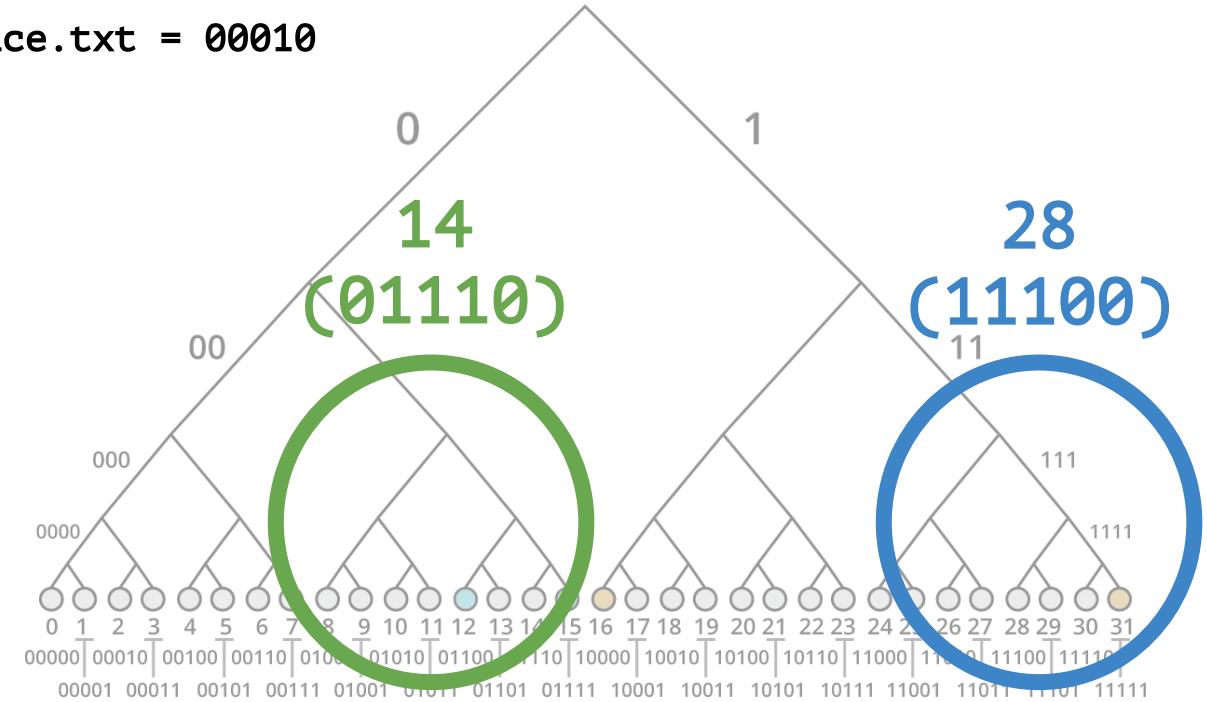
P2P-адресация — XOR-метрика

war_and_peace.txt = 00010



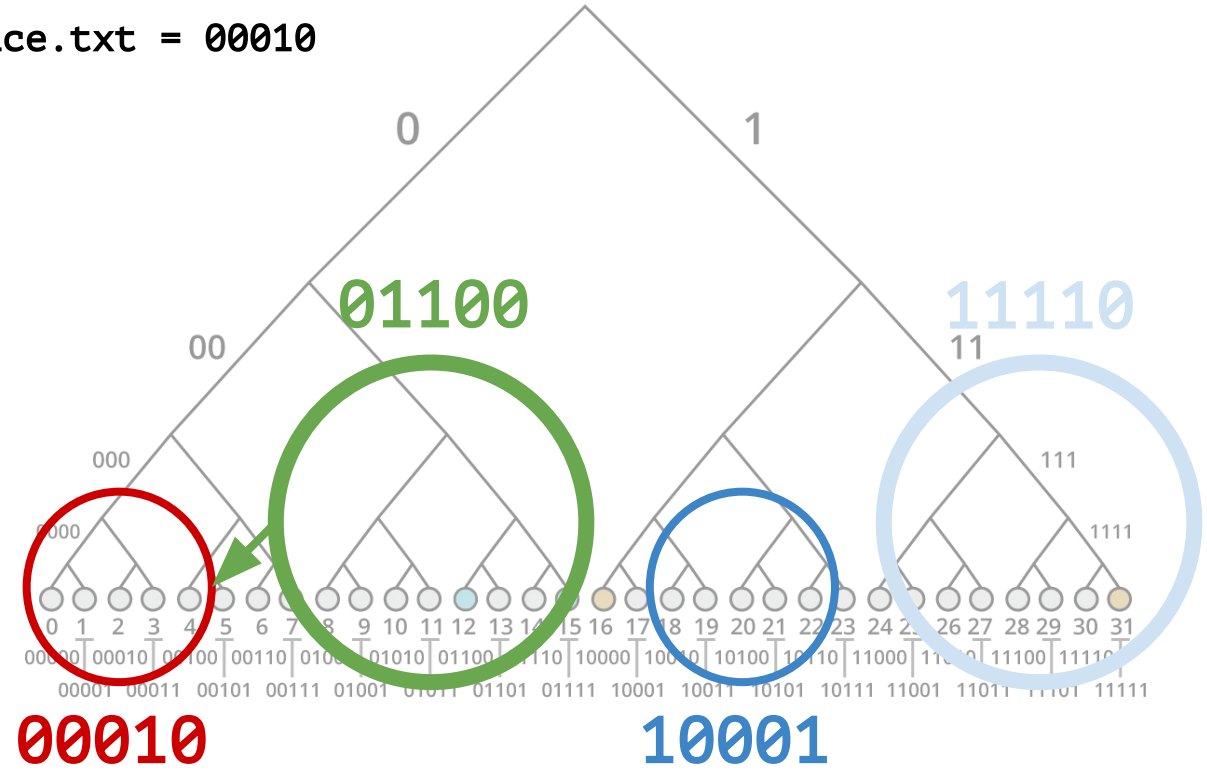
P2P-адресация — XOR-метрика

```
war_and_peace.txt = 00010
```



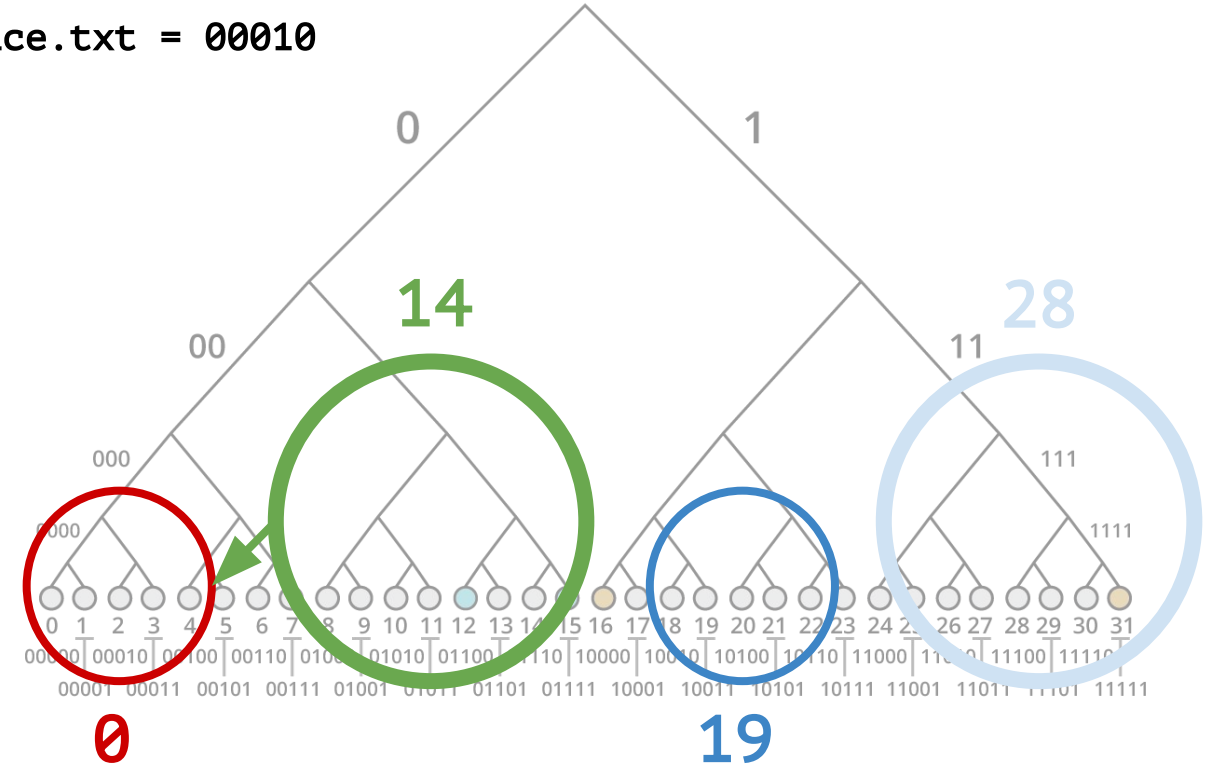
P2P-адресация — XOR-метрика

```
war_and_peace.txt = 00010
```



P2P-адресация — XOR-метрика

```
war_and_peace.txt = 00010
```



Практика: SAFE Network

- Безопасная маршрутизация на основе Kademlia
- Безопасное хранение зашифрованных данных
- Аутентификация и авторизация
- Платформа для безопасных приложений и веб-сайтов

- Весь код открыт под GPLv3

Практика: SAFE Network

- **Crust** — реализация соединений между нодами и обход NAT

- **Safe Client Libs** — API для подключения к сети пользователей и приложений
  Rust, C/C++, JavaScript, *Python, Ruby,* ...

- **Safe Vault** — ноды, хранящие данные

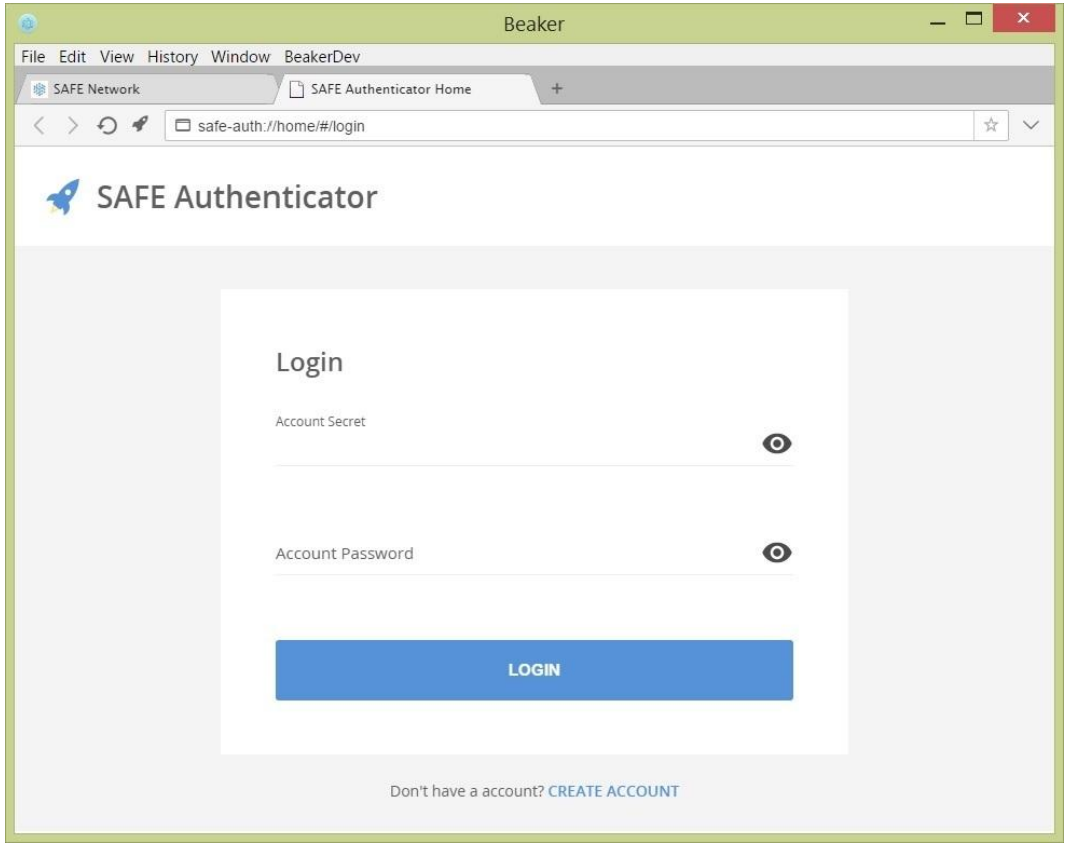
Как стать хранилищем?

- **Proof of resource**:
  Подтверждаем, что у нас достаточно ресурсов для хранения данных

- За хранение данных
  получаем печеньки — **SafeCoins**

Платформа для сайтов

- **SAFE Browser**



Платформа для сайтов

- Распределенная система доменных имен (DNS)
  safe://service.domain

- Домены — это тоже файлы
  SHA1(service.domain) = f66023...

Платформа для сайтов

- Статический контент (HTML, CSS, …)
  (и это тоже файлы)

- Динамический контент через JavaScript API — комментарии, чаты, форумы, …
  (и даже это — файлы)

Ресурсы

- Скачать: **http://maidsafe.net**
- Код: **http://github.com/maidsafe**
- Форум: **http://tinyurl.com/safenet-ru**
  http://safenetforum.org

Спасибо за внимание!
Вопросы?

Слайды будут доступны в Твиттере **@defcon_nn**
Телеграм **@defcon_nn**, ВК **https://vk.com/defcon_nn**

За кадром

- Достижение консенсуса
  (как ноды договариваются о том, что данные можно изменить)
- Отток (churn) и проблема сохранности данных
- Дедупликация
  (файлы во всей сети хранятся только в единственном экземпляре)