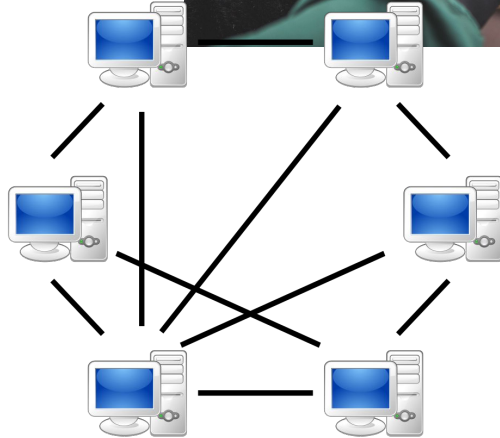


# Privacy Preserving DHT

**FOSDEM**'19



# Privacy Preserving DHT

**Why**

**How**

Open **challenges** + next up

**p3lib** <https://github.com/hashmatter/p3lib>

Privacy Preserving DHT **Why**

**Metadata leaks** in collaborative  
crowds

P2P networks can deliver the best privacy online



# Privacy Preserving DHT **Why**

## **Metadata leaks** in collaborative crowds

P2P networks can deliver the best privacy online

But naïve implementations will make it worse 🙄

*P2P and the "property extreme"*





Privacy Preserving DHT **Why**

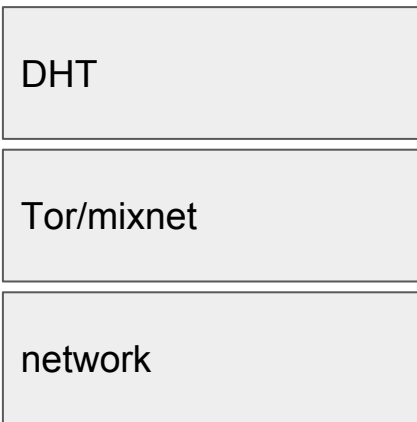
**Metadata resistant DHT lookup**



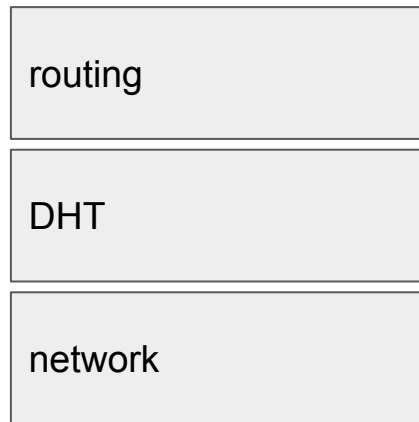
# Privacy Preserving DHT **How**

**Tor** (how about Tor itself?)

**Mix networks** (slow af)



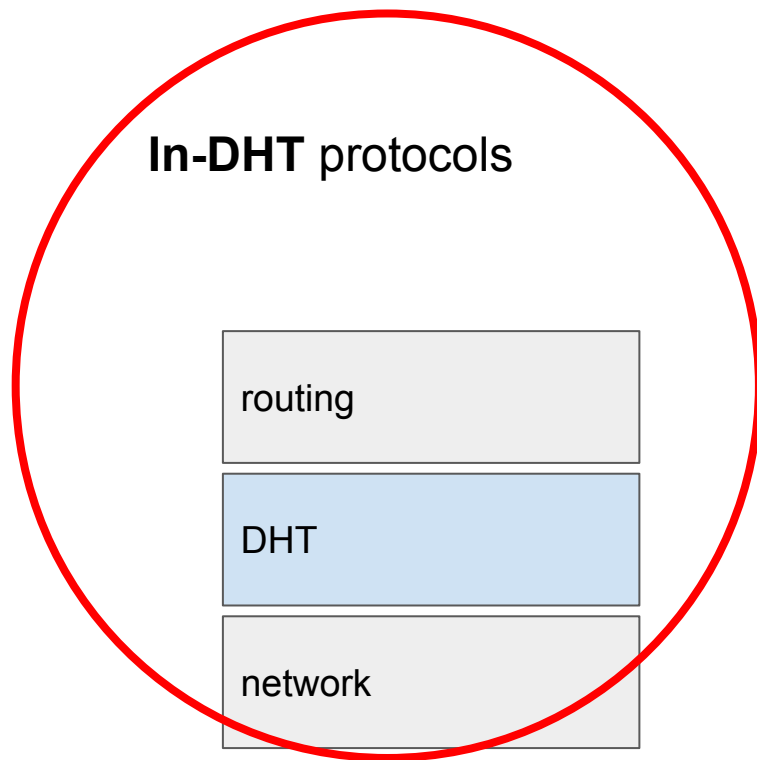
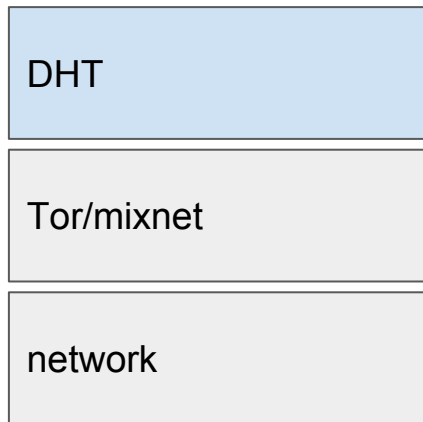
**In-DHT** protocols



# Privacy Preserving DHT **How**

**Tor** (how about Tor itself?)

**Mix networks** (slow af)



Privacy Preserving DHT **How**

Onion routing over DHT

Mixnet over DHT

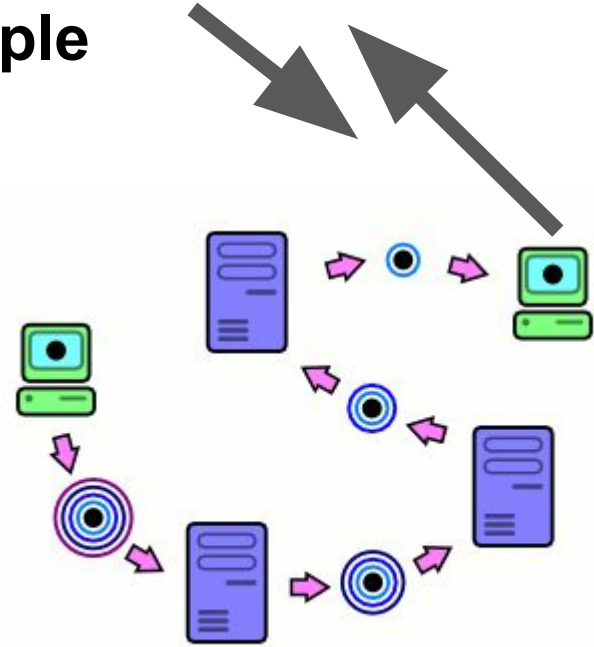
F2F routing (it's a small world!)





# Privacy Preserving DHT **Lookup** example

1. Select **DHT nodes** as relayers  
(partial view, security, anonymity => ZK!)
2. Construct secure and leak-proof packet with DHT lookup
3. **Delegate lookup:** forward & relay over circuit
4. Response package
5. Reliable and fail-proof circuits



# Privacy Preserving DHT Lookup example

## 1. Select **DHT nodes** as relayers

ShadowWalker [1], ... (anonymity => ZK!)

## 2. Construct secure and reliable circuit with DHT lookup

Sphinx [2], ...

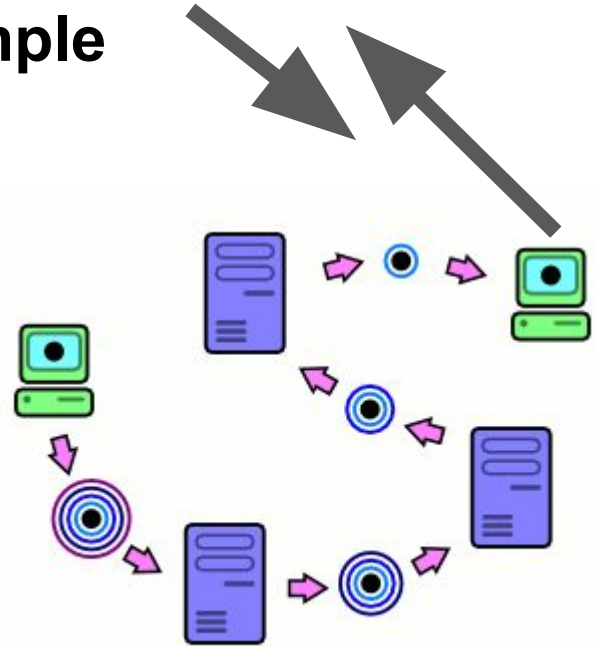
## 3. Delegate lookup: find next hop in circuit

HORNET [3], ...

## 4. Response package

## 5. Reliable and fail-proof circuits

TAP [4], ...

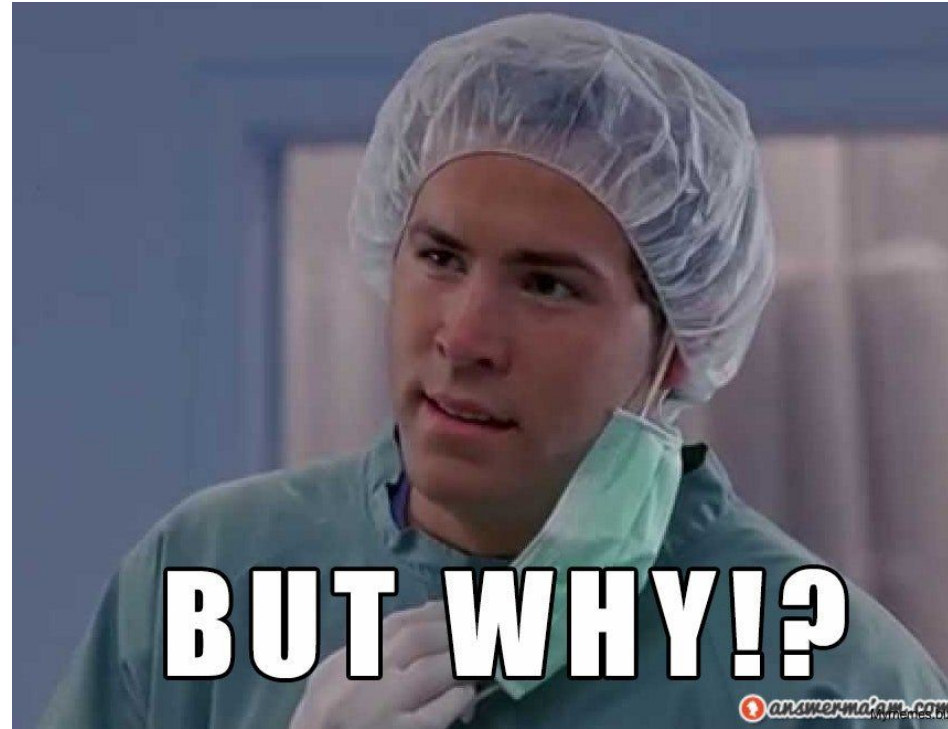


# Privacy Preserving DHT Lookup example



# Privacy Preserving DHT

- **Overall better unlikeability**
- Tor is not a good fit (overhead, censorship)
- Different needs >> different strategies
- **Selective privacy and consent**
- *"Entropy by diversion"* or protocol mux
- Maybe more resilient and efficient?



# Privacy Preserving DHT

- **Overall better unlikeability**
- Tor is not a good fit (overhead, censorship)
- Different needs >> different strategies
- **Selective privacy and consent**  

```
$ ipfs get QmYaaMBmXVgqNDURR2G8Y6cGLg5AfdLc2Pjh3584YVMoRQ --private
```
- *"Entropy by diversion"* or protocol mux
- Maybe more resilient and efficient?



# Privacy Preserving DHT

## **What I'd love to answer but I can't (yet)**

- Enough entropy?
- Overhead/how expensive?
- Secure relayer set construction?
- Incentives for relayers?
- Plug-and-play set of primitives for P2P privacy?



# Privacy Preserving DHT

**What I can tell you**



# Privacy Preserving DHT

**What I can tell you**

**We do have some options!!**



## Privacy Preserving DHT

### **Send traffic anonymously?**

- Onion routing (over DHT)
- Sphinx
- HORNET
- Octopus
- Phantom
- ...

# Privacy Preserving DHT

## Send traffic anonymously?

- Onion routing (over DHT)
- Sphinx
- HORNET
- Octopus
- Phantom
- ...



**How?  
Where?  
Waat??**

## Privacy Preserving DHT

### **Locate relays anonymously?**

- ShadowWalker
- Salsa + DHT "secure" lookups
- AP3 + stochastic based random walks
- ...

# Privacy Preserving DHT

## Locate relays anonymously?

- ShadowWalker
- Salsa + DHT "secure" lookups
- AP3 + stochastic based routing
- ...



**How?  
Where?  
Waat??**



# Privacy Preserving DHT

## **F2F/restricted topology?**

- Freenet's "*darkweb*" (not secure/private btw)
- Turtle F2F
- ...

# Privacy Preserving DHT

## F2F/restricted topology?

- Freenet's "*darkweb*" (not so)
- Turtle F2F
- ...



**How?**  
**Where?**  
**Waat??**

# Privacy Preserving DHT Networking

- Onion routing (over DHT)
- Sphinx
- HORNET
- Octopus
- Phantom
- ShadowWalker
- Sale
- AP3 +
- Freenet's
- Turtle
- ....

**How?**  
**Where?**  
**Waat??**

waaat?

waaat?

waaat?


waaat?







# Privacy Preserving DHT    **Open challenges**


- "Cryptography is free, anonymity is not" aka **Incentives**
- **Metrics**/measurements
- What is actually **happening** in Real World™ ?
- Scalable and **secure** DHT
- Privacy preserving network **engineering** (r&d)


# Privacy Preserving DHT **p3lib**


 hashmatter / **p3lib**


 Unwatch ▾ | 1 |  Unstar | **10k** |  Fork | 1


 Code


 Issues 3

 Pull requests 0

 Projects 1

 Wiki

 Insights

 Settings

privacy preserving primitives and protocols (p3) for routing and messaging in P2P networks <https://hashmatter.com>

Edit


p2p


messaging


anonymous


privacy-enhancing-technologies


Manage topics

 11 commits

 1 branch

 0 releases

 1 contributor

 MIT

Branch: master ▾


New pull request

Create new file

Upload files

Find file

Clone or download ▾

 gpestana Merge pull request #5 from gpestana/crypto-ecdh ...

Latest commit 91f457e 6 hours ago

# Privacy Preserving DHT

w3f / messaging

Unwatch

19

Unstar

43

Fork

4

<> Code

Issues 14

Pull requests 0

Projects 0

Wiki

Insights

Messaging for Web3

39 commits

3 branches

0 releases

5 contributors

Branch: master

New pull request

Create new file

Upload files

Find file

Clone or download

robertkiel updated diagram

Latest commit 29ebb91 28 minutes ago

rewards-poe	Making way for rewards description	2 months ago
ADVERSARY.md	Cleanup, restructuring	2 months ago
README.md	updated diagram	28 minutes ago
REQUIREMENTS.md	Cleanup, restructuring	2 months ago
project.md	publish the initial description	2 months ago
rewards.md	Making way for rewards description	2 months ago

README.md

## A Decentralised Privacy-Preserving Communication Protocol

Messaging for Web3.



## Privacy Preserving DHT

















- Research vs Real World™
- Not even one (!) good solution out there
- A lot to research, to understand, to code and to measure

# IPFS Project Roadmap v0.4.0

---

## Table of Contents

---






- [IPFS Mission Statement](#)
- [2019 Priorities](#)
- [2019 Working Groups Roadmaps](#)
- [2019 IPLD & libp2p Roadmaps](#)
- [2019 Epics](#)
- [2019 Goals \(expanded\)](#)
  -  [Package Managers](#)
  -  [Large Files](#)
  -  [Decentralized Web](#)
- [2020+ Goals](#)
  -  [Encrypted Web](#)
  -  [Distributed Web](#)
  -  [Personal Web](#)
  -  [Sneaker Web](#)
  -  [Interplanetary Web - Mars 2024](#)
  -  [Packet Switched Web](#)
  -  [Data Web](#)
  -  [Package Switched Web](#)
  -  [Self-Archiving Web](#)
  -  [Versioning Datasets](#)
  -  [Interplanetary DevOp](#)
  -  [The World's Knowledge becomes accessible through the DWeb](#)
  -  [WebOS](#)

# IPFS Project Roadmap v0.4.0

---

## Table of Contents

---

- [IPFS Mission Statement](#)
- [2019 Priorities](#)
- [2019 Working Groups Roadmaps](#)
- [2019 IPLD & libp2p Roadmaps](#)
- [2019 Epics](#)
- [2019 Goals \(expanded\)](#)
  -  [Package Managers](#)
  -  [Large Files](#)
  -  [Decentralized Web](#)
- [2020+ Goals](#)
  -  [Encrypted Web](#)
  -  [Distributed Web](#)
  -  [Personal Web](#)
  -  [Sneaker Web](#)
  -  [Interplanetary Web - Mars 2024](#)
  -  [Packet Switched Web](#)
  -  [Data Web](#)
  -  [Package Switched Web](#)
  -  [Self-Archiving Web](#)
  -  [Versioning Datasets](#)
  -  [Interplanetary DevOp](#)
  -  [The World's Knowledge becomes accessible through the DWeb](#)
  -  [WebOS](#)

{  [Metadata resistant Web](#)

# Privacy Preserving DHT and P2P networking

<https://github.com/gpestana/p2psec> (paper reviews, notes, projects)

 [Privacy preserving DHT open research paper](#) (github)

 <https://github.com/hashmatter/p3lib>

<https://hashmatter.com>

# References

- [1] ShadowWalker: Peer-to-peer Anonymous Communication Using Redundant Structured Topologies (Prateek Mittal, Nikita Borisov)
- [2] Sphinx: A Compact and Provably Secure Mix Format (George Danezis, Ian Goldberg)
- [3] HORNET: High-speed Onion Routing at the Network Layer (Chen Chen, et al.)
- [4] TAP: A Novel Tunneling Approach for Anonymity in Structured P2P Systems (Yingwu Zhu, Yiming Hu)

For more: <https://github.com/gpestana/p2psec/tree/master/research>

# Privacy Preserving DHT

**FOSDEM**'19

