Freenet / Hyphanet: the long game

Wann immer eine neue Art Datenschutzverletzung bekannt wird,
erinnern sich einige an das **Freenet Projekt**,
aber wenige kennen es wirklich.
Ändern wir das.
Vision, Grundlagen und Neuerungen

Dr. Arne Babenhauserheide

Warum Freenet?

Wann immer neue Arten der Datenschutzverletzung bekannt werden, erinnern sich einige an das Freenet Projekt, aber wenige kennen es wirklich.

Daher liefert dieser Vortrag einen Einstieg in die heutigen Fähigkeiten von Freenet.[1] Er erklärt, warum Freenet existiert und welche Vision all seine Weiterentwicklungen leitet, liefert ein Grundverständnis seiner Funktionsweise und der Werkzeuge, die es bietet, und zeigt die Fortschritte der letzten 15 Jahre.

Ein verteiltes Netz zum Schutz freier Kommunikation, eine Struktur ohne zentralisierte Macht, ein Ort zum Koordinieren der Arbeit für digitale Freiheit, wenn die Kämpfe um ein freies Netz zeitweise verloren werden sollten, ein Plan B für ein Internet, in dem Kommunikation funktioniert, ohne sich ständig verkaufen zu lassen.

Eine Aufnahme dieses Vortrages gibt es bei den SUMA-Kongress 2022 Videos.

Warum Freenet?

Warum Freenet?

"There is now no shield from forced exposure... The foundation of Groklaw is over... the Internet is over" –Groklaw, *Forced Exposure (2013-08-20)*

Warum ich?

- Seit 20 Jahren in der Entwicklung von peer-to-peer Netzen
- Freenet Release-Manager seit 2017
- Vorlesung zu Verteilten Systemen an der DHBW
- 2015 den SUMA Award für Freenet entgegengenommen

Fragen

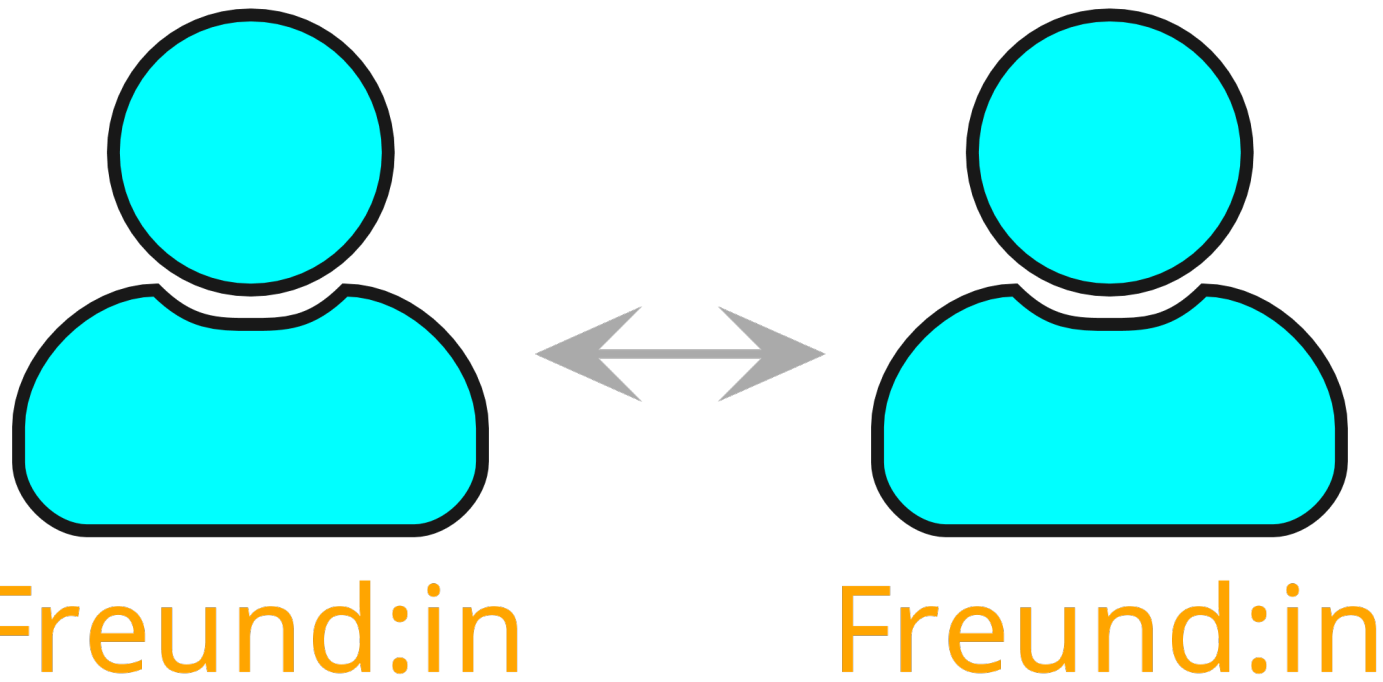
- Warum gibt es Freenet?
- Wie funktioniert Freenet?
- Was ermöglicht Freenet?
- Was hat sich geändert?

Warum Freenet? Was bringt es?

- Vertraulich oder pseudonym kommunizieren.
- Technischer Grundpfeiler für den Schutz gegen Zensur.
- Dafür: Hohes Datenschutzniveau.

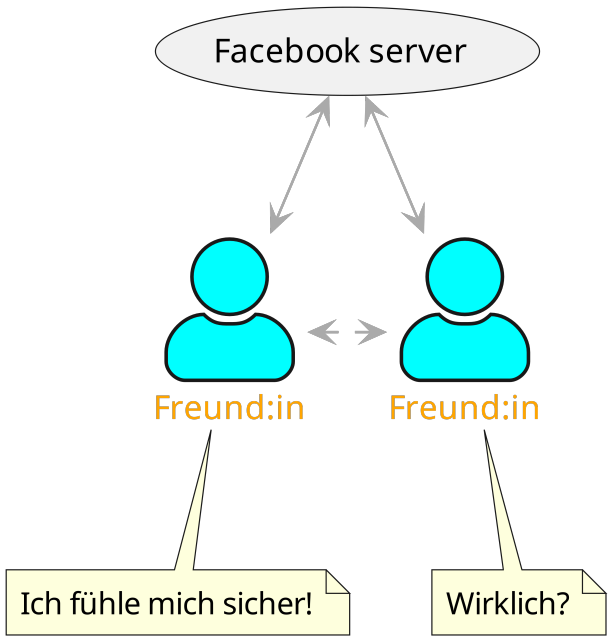
"Covers the needs for protection expected from a secure data broker for Multi-Party Data Exchange in IoT for Health" (**?**, Uni Bern) — Artikel

Im Freundeskreis sprechen: Vertraulich

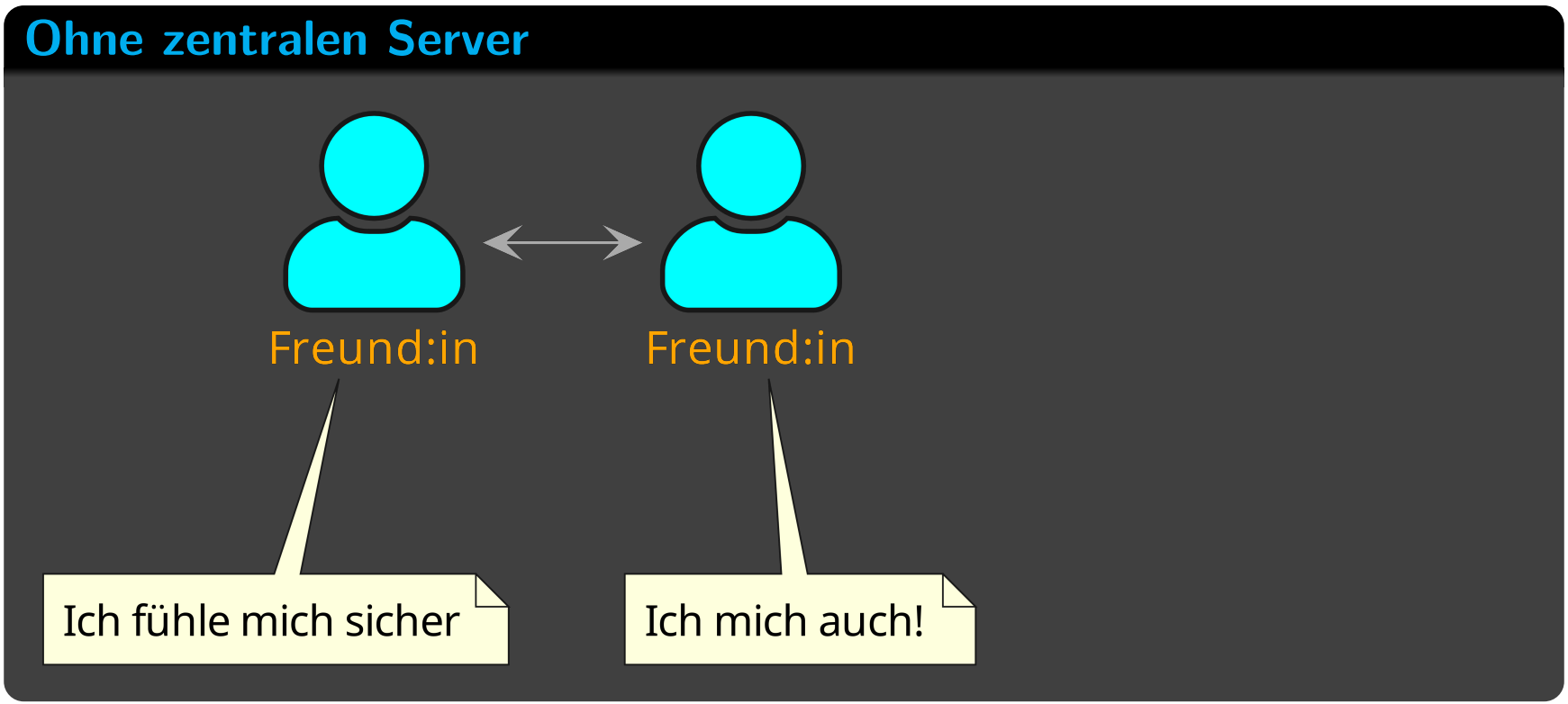


Was bietet Freenet?

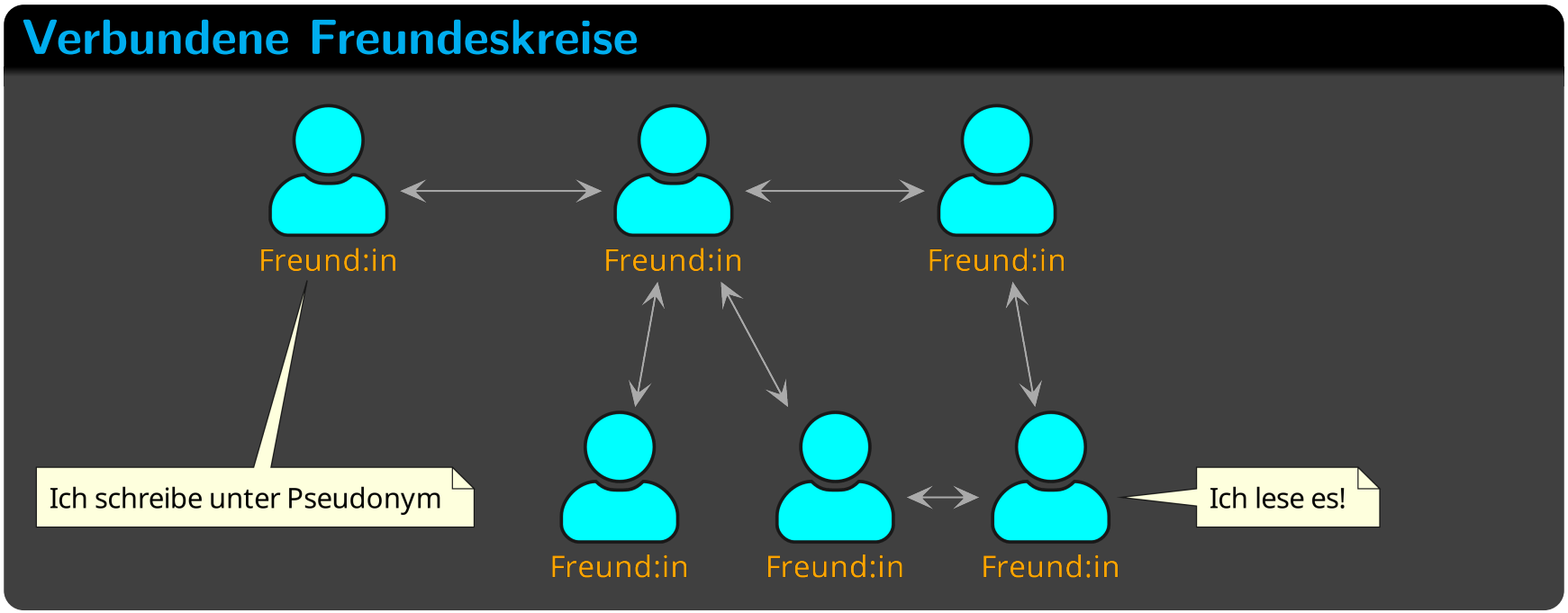
Sprechen wie mit . . .



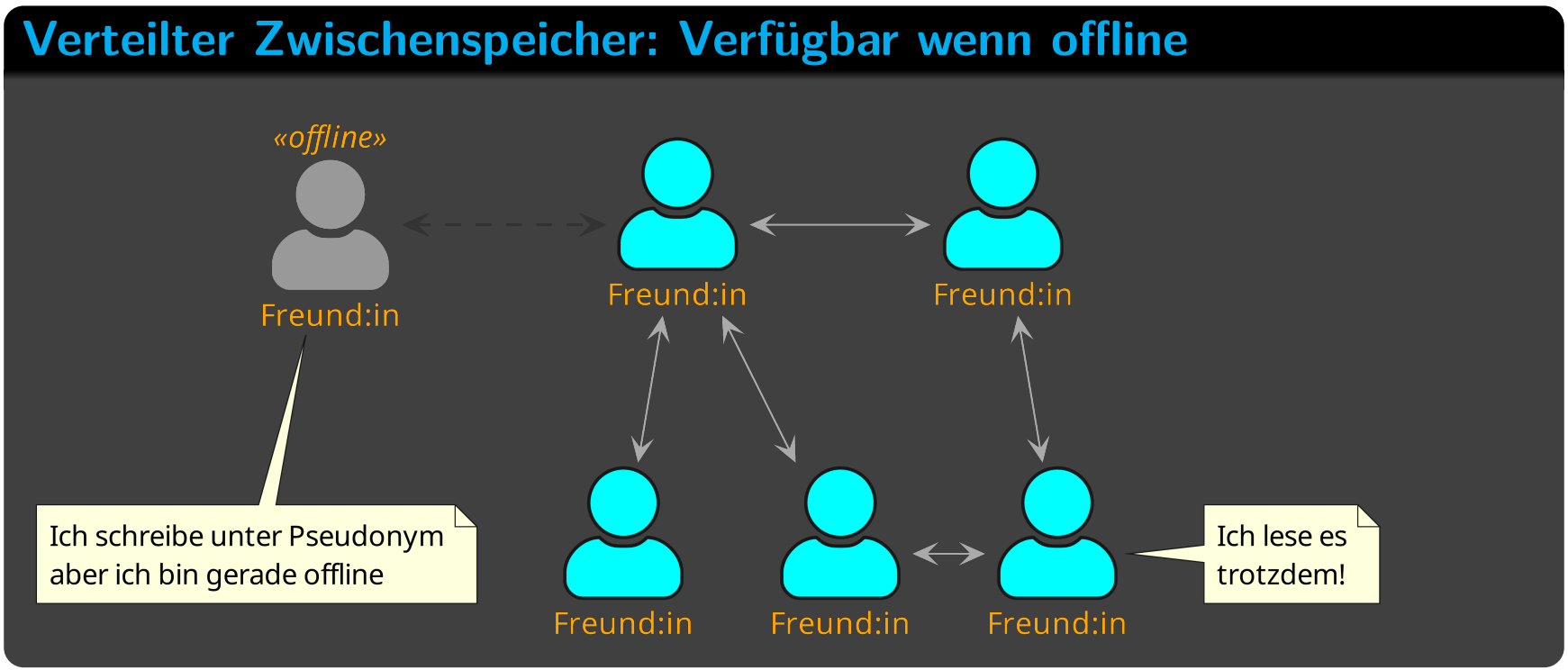
. . . aber ohne den Überwachungs-Server



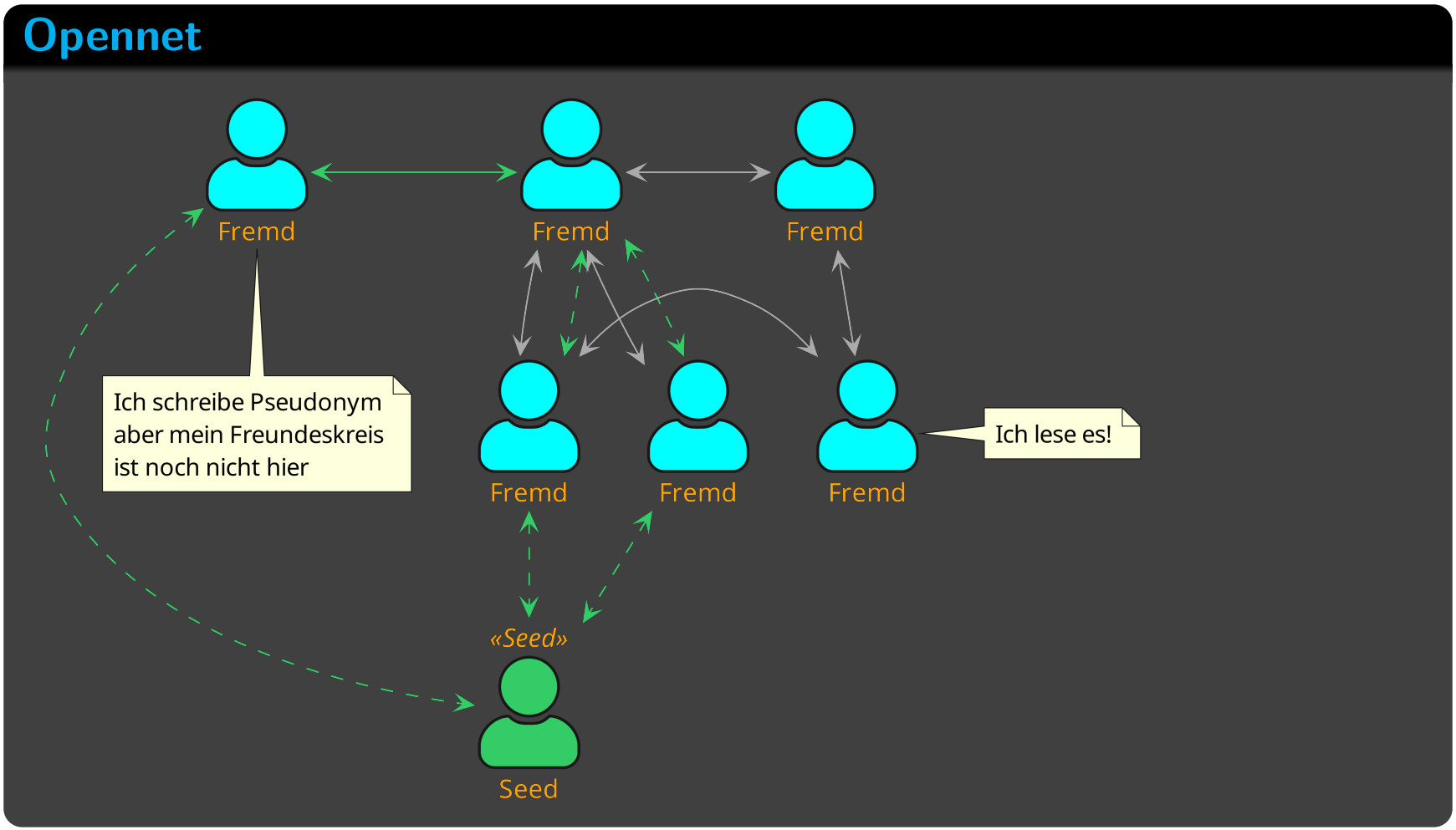
Mit Fremden sprechen



Ohne Server

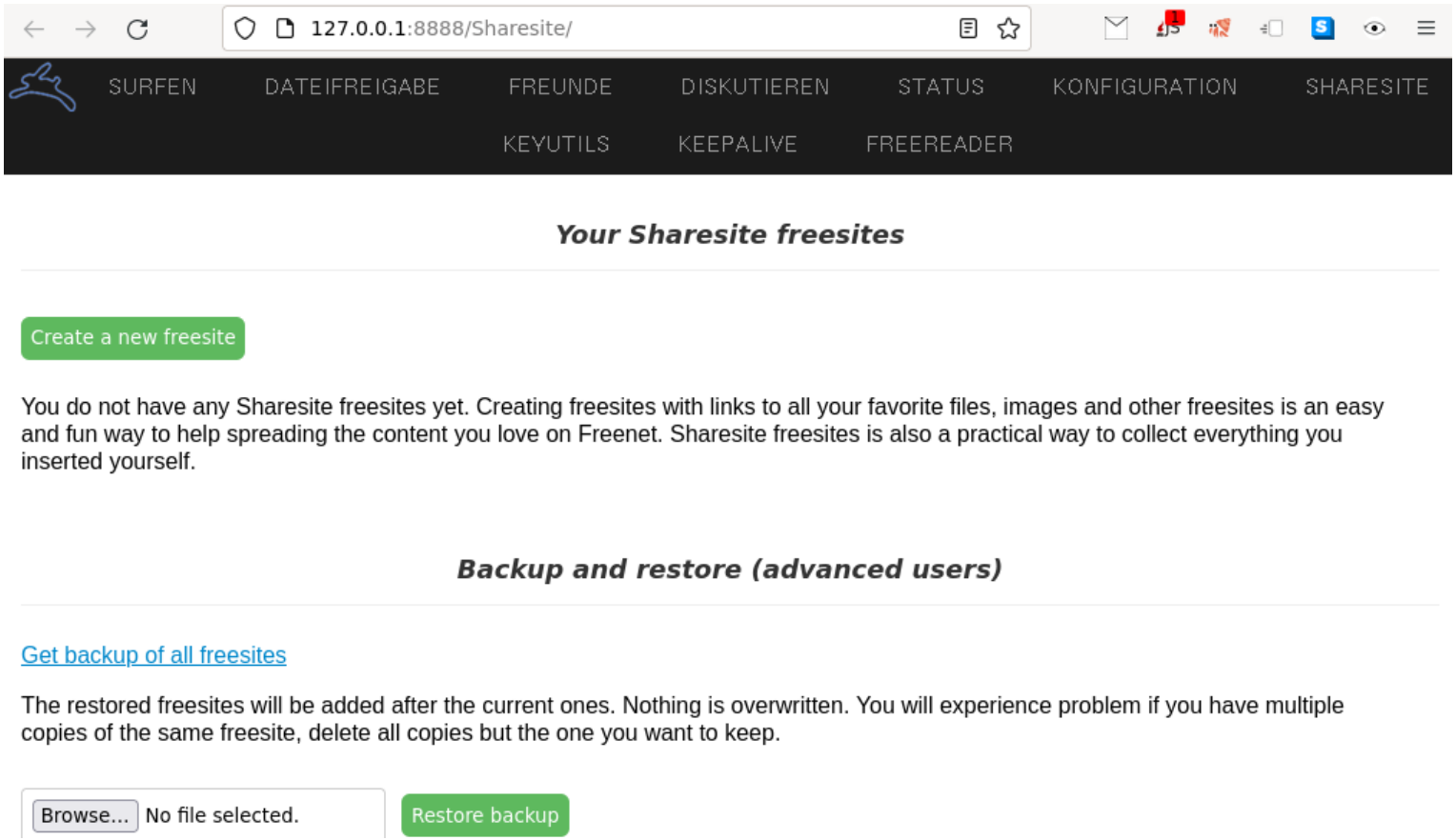

Verteilter Zwischenspeicher: Verfügbar wenn offline
«offline»
Freund:in
Freund:in
Freund:in
Ich schreibe unter Pseudonym
aber ich bin gerade offline
Freund:in
Freund:in
Freund:in
Ich lese es
trotzdem!

Pionier im Freundeskreis?



Einwurf: Wir starten eine Sharesite-Seite!

http://127.0.0.1:8888/Sharesite



Warum brauchen wir das?

Spiegelbild der Welt

Durch die steigende Vermengung des digitalen Lebens mit dem Analogen wird Analoge Kommunikation zu einem Spiegelbild des beschränkten Lebens im Netz.

— Arne Babenhauserheide, Suma e.V. Kongress 2015 :-)

Das Netz verbreitet sich

Ohne pseudonyme Kommunikation und ohne vertrauliche Kommunikation im Internet, werden wir sie auch in der Analogen Welt verlieren.

Analoge Kommunikation

Vertraulich

Im kleinen Rahmen
Direkter Kontakt

Analoge Kommunikation

Vertraulich

Im kleinen Rahmen
Direkter Kontakt

Offiziell

Selbstzensur
Fremdbestimmt

Analoge Kommunikation

Vertraulich

Im kleinen Rahmen
Direkter Kontakt

Offiziell

Selbstzensur
Fremdbestimmt

Pseudonym

Stetig auf der Hut
Quellenschutz!

Analoge Kommunikation

Im Überwachten Netz

Offiziell

Selbstzensur
Fremdbestimmt

Stichwort: Panoptikum

Die Dystopie: Verlust der Pressefreiheit

> *I worry about my child and the Internet all the time, even though she's too young to have logged on yet. Here's what I worry about. I worry that 10 or 15 years from now, she will come to me and say 'Daddy, where were you when they took freedom of the press away from the Internet?' –Mike Godwin, Electronic Frontier Foundation, "Fear of Freedom" (1995)*

Das Ziel des Freenet-Projektes ist es, den freien Informationsfluss zu gewährleisten.

Auch dann noch, wenn Kriminelle journalistisch Arbeitende und ihre Quellen bedrohen.

Technik und Politik

Tech alleine reicht nicht

Totale Überwachung und Kontrolle sind möglich.

Politik alleine reicht nicht

Wenn Überwachung und Zensur trivial sind, werden sie genutzt.

Tech und Politik

Technologie liefert die Grundlage, auf der Politik arbeiten kann: Überwachung und Zensur so aufwändig und teuer machen, dass wir den politischen Kampf gewinnen können.

> *The NSA surveillance doesn't scale.*
> *– Constanze Kurz (EuroPython 2014)*

Zensurfreiheit

- Kern von allem in Freenet
- Alle Möglichkeiten und Entwicklungen dienen diesem Ziel
- Artikel 5 GG: eine Zensur findet nicht statt

Folgerungen: Herrschaftsfreiheit

Niemand darf Macht über die Kommunikation anderer haben. Einige der Risiken für Kommunikation:

Direkte Zensur entfernt Beiträge durch Drohung oder Löschung

Schikane oder Hetze schließt Leute aus und treibt sie raus

Fluten mit Irrelevantem macht Wichtiges unauffindbar

Zerrüttung der Gesprächskultur verhindert Evolution von Ideen

Braucht das nicht Moderation?

Freenet ermöglicht Moderation ohne zentrale Macht

Wähle selbst, wer für dich blocken kann.
Wenn dein pseudonymer Freundeskreis ein Pseudonym blockt, wird es für dich automatisch auch unsichtbar, es sei denn, du hast es explizit freigeschaltet.
Das Anti-Spam-System skaliert besser als Spam. Auch ohne ein Heer ausgebeuteter Content-Moderationsteams aus Billiglohnländern (weiter: Arte: „The cleaners“).
Heutige verteilte Plattformen ziehen langsam nach.

Und Hetze?

Den Opfern helfen Pseudonyme mehr als den Tätern

Wer Gewalt fürchten muss, kann ohne Pseudonym nicht öffentlich kommunizieren. Überwachung hilft so immer den Tätern.

Unter Klarnamen sind Leute aggressiver

> *Results show that in the context of online firestorms, non-anonymous individuals are more aggressive compared to anonymous individuals*

- *Katja Rost et al.: Digital Social Norm Enforcement: Online Firestorms in Social Media*

Weiterlesen: Klarnamenspflicht schadet der Online-Kommunikation

Und Propaganda?

Propaganda will Herrschaft

Q: *"Can I prevent someone from commenting in my thread?"*
A: *"You did understand the part about no power over others?"*

Herrschaft ist zentralisierte Macht

Tik Toks Algorithmen treiben Leute in ein Labyrinth aus Desinformation. Selbst zu entscheiden, welchen Einflüssen wir uns aussetzen, ist eine Frage Kommunikativer Selbstbestimmung.

Und Radikalisierung?

Soziale Medien machen alles — und schlimmeres — was Leute jemals bei Freenet befürchtet haben. Außer Zugriff auf brisante Informationen wo Leute sie wirklich bräuchten.

Und außer der Möglichkeit, aggressiven Propagandisten verbal die Stirn zu bieten, ohne sich in Gefahr zu bringen.

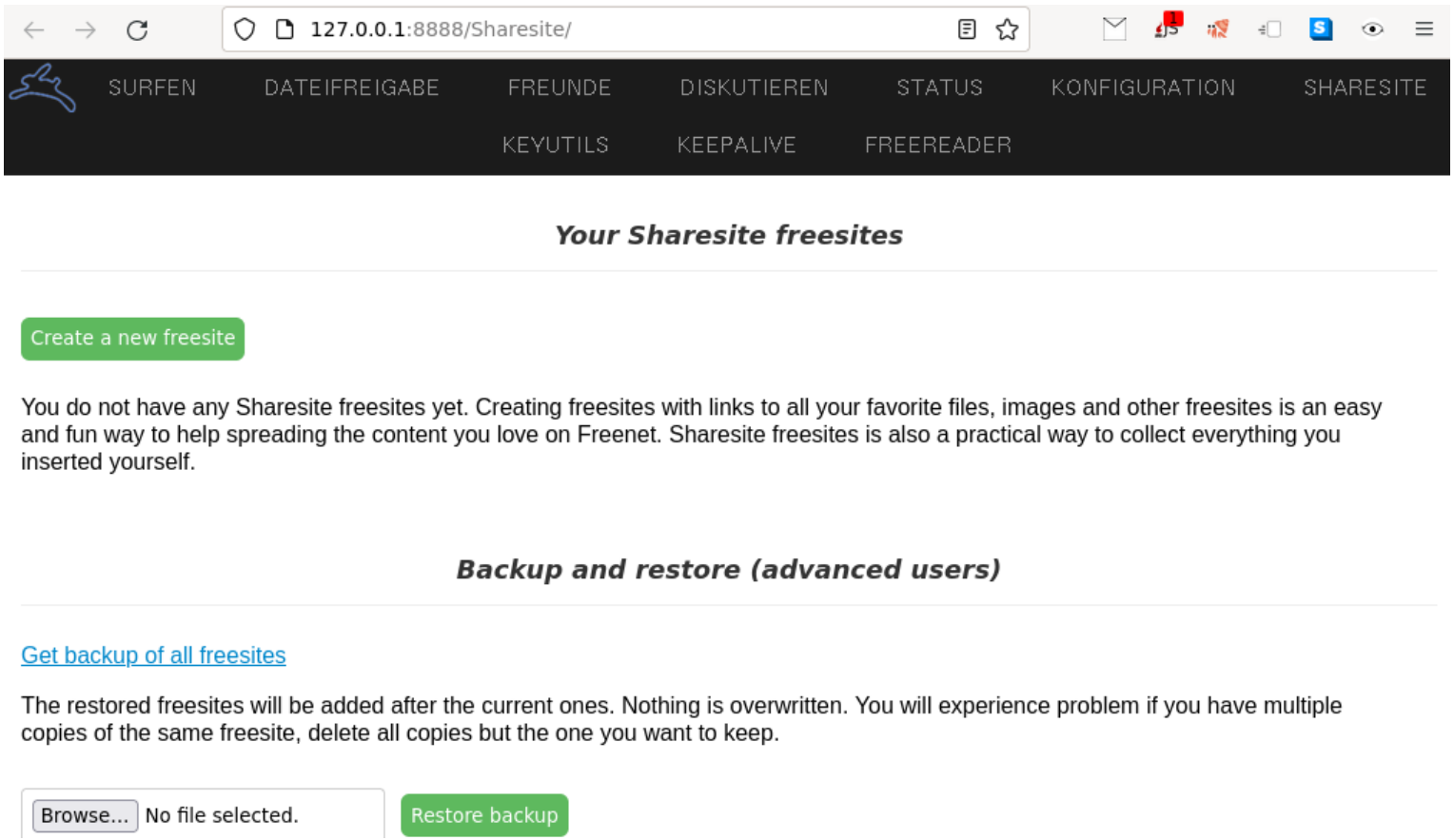
Zusammenfassung

- Zensurfreiheit
- Datenschutz
- Vertrauliche Kommunikation
- Pseudonyme

Eine technische Säule für Informationelle Selbstbestimmung.

Einwurf: Unsere Sharesite!

http://127.0.0.1:8888/Sharesite



Funktionsweise von Freenet

- Grundkonzepte
- Schnittstellen
- Schutzmaßnahmen

Warum Funktionsweise betrachten?

- Quelle der Stärken von Freenet
- Verständnis notwendig für Effizienz

Alleinstellungsmerkmale

- Freund-zu-Freund Darknet (plus Opennet)
- Hosting ohne Server (hochladen und verschwinden)
- Stabile Pseudonyme (privater Schlüssel)
- Kryptografie über Links (einfach nutzbar)
- Dezentrale Spamresistenz (erprobt; hilft Kommunikationskultur)
- Nutzungsabhängige Lebenszeit (anonym)

Praktisch: Seit 23 Jahren durch Tausende genutzt.

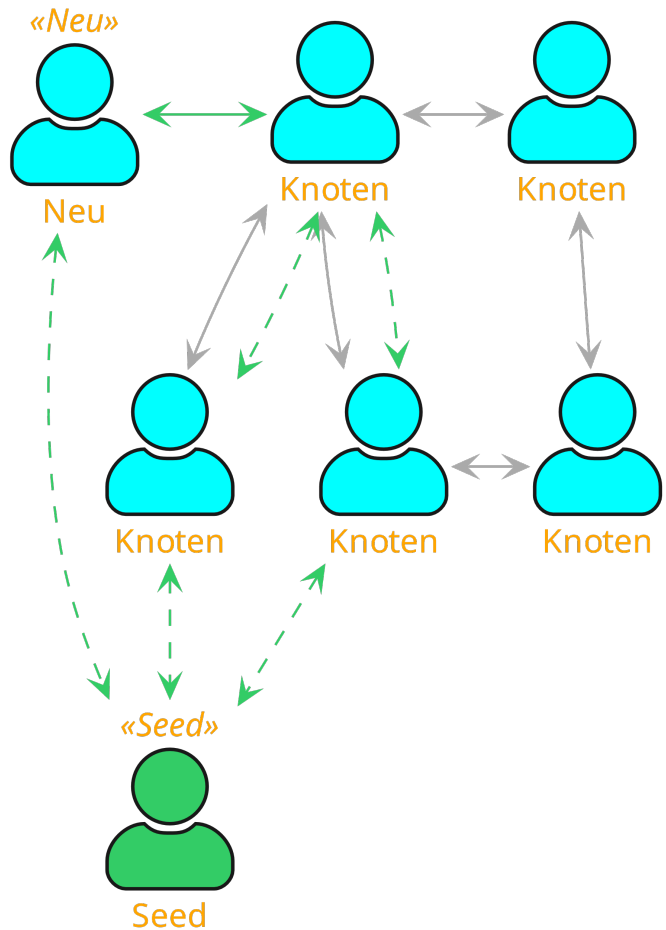
Grundkonzepte

- Zugriff auf Daten: dezentral und skalenfrei (small world)
- Referenzierung von Daten über Inhalts-Hash oder Öffentlichen Schlüssel
- Private und Öffentliche Schlüssel als Links
- Updates über Versionierung

Einstieg

- Mit Freunden verbinden[1] (sicherer), oder
- Mit Seednode verbinden

[1]: High Security Mode: nur mit Freunden verbinden



Small World / grob Skalenfreies Netz

- Verbunden zu vielen Nahen Knoten und wenigen entfernten
- 6 Degrees of Separation: Wie Briefe über Bekannte
- Ring: Location liegt zwischen 0.0 und 1.0
- Wer bei 0.3 ist, kennt v.a. Leute nahe 0.3
- Bei Opennet über den Einstieg realisiert
- Bei Friend-to-Friend über Tausch der Location

Dateien referenzieren: Schlüsseltypen

- CHK: Datei nach Inhalt
- SSK: Public/Private Key
  - USK: Aktualisierbar
  - KSK: Gemeinsames Passwort

CHKs sind 32kiB groß, SSKs 2kiB. Größere sind Bäume von CHKs mit SSK oder CHK für das Manifest.

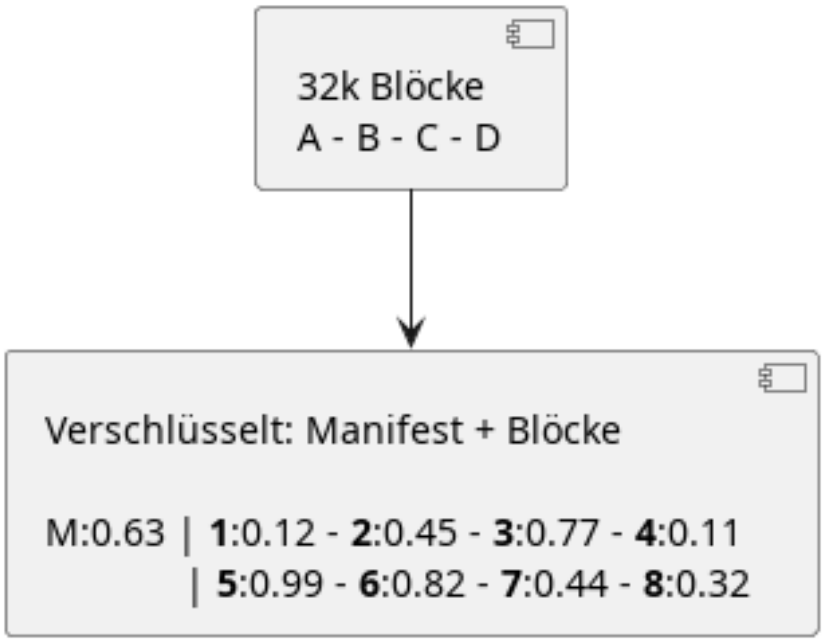
Struktur der Schlüsseltypen

```
CHK@<routing>,<encryption>,<flags>/<name>/[optional-path]
SSK@<routing>,<encryption>,<flags>/<name>/[optional-path]
USK@<routing>,<encryption>,<flags>/<name>/<version>/[optional-path]
KSK@<password>
```

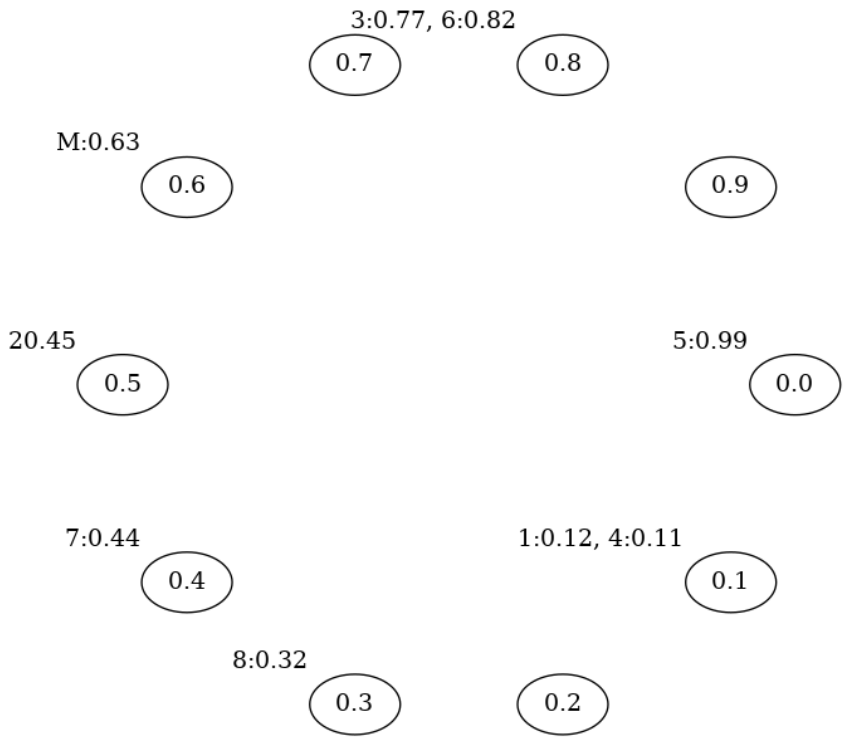
- CHK: CHK@7ER...,F2u...,AAMC–8/fetchpull-lifetime-realtime-success-count.png
- SSK: SSK@rQn...,I1v...,AQACAAE/gms-16/
- USK: USK@rQn...,I1v...,AQACAAE/gms/16/
- KSK: KSK@the-long-game

Nur <routing> wird ins Netz geschickt. <encryption> bleibt lokal.

Dateien aufteilen und hochladen

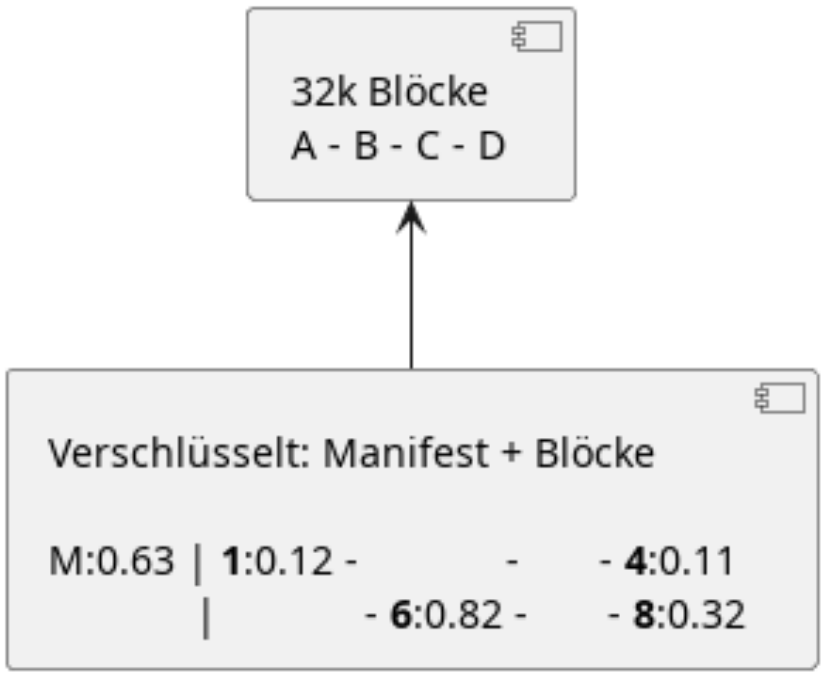


Schlüssel ist im Link (z.B. CHK).
Blöcke ohne Link nicht entschlüssel- oder erkennbar.

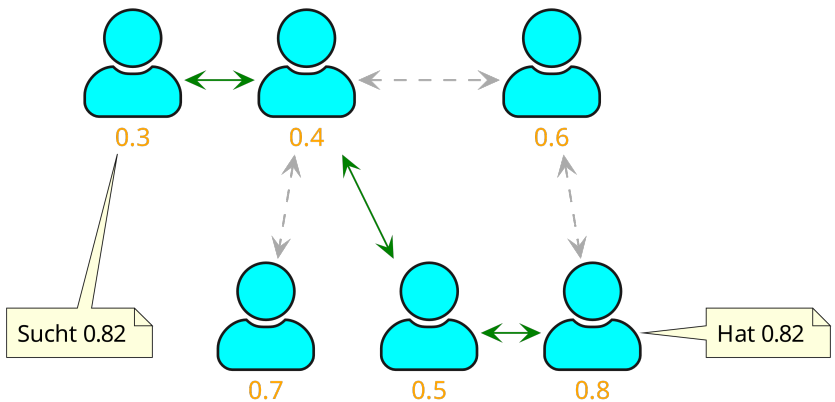


Blöcke zufällig überschreiben.

Blöcke finden und zusammenfügen

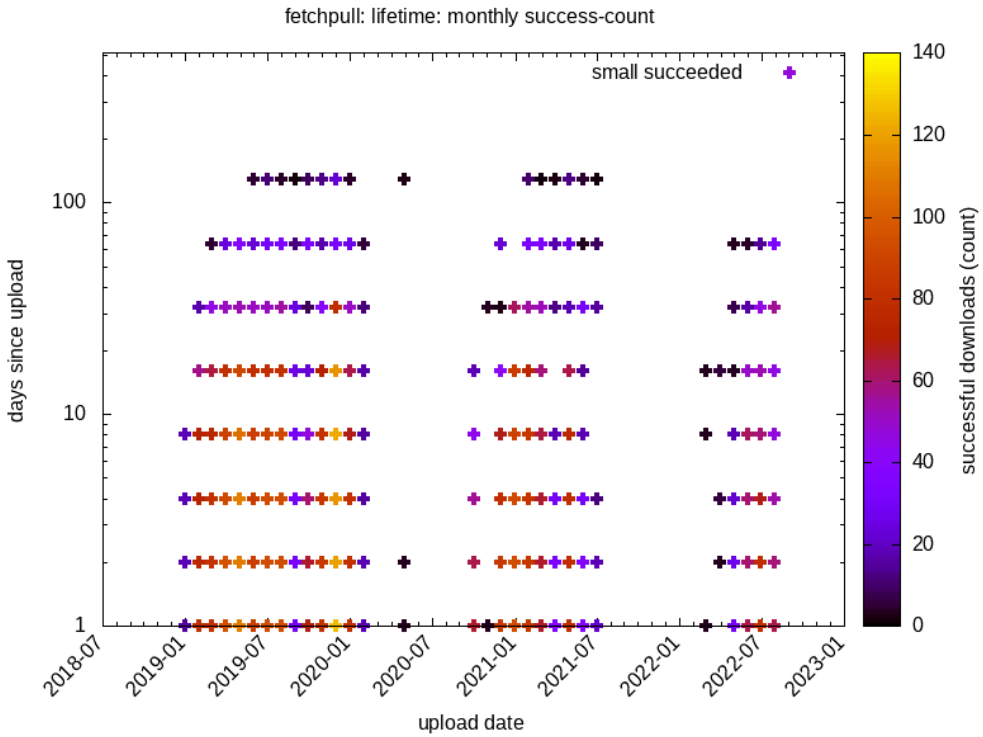


Verfügbar, solange 50% der Blöcke auffindbar sind.



Routing in Small-World Netzwerk über die Positionen der Freunde von Freunden (FOAF).

Lebenszeit



Jeder Zugriff startet die Uhr neu.

Recht auf Vergessen?

- Lebenszeit aus öffentlichem Interesse
- Recht auf Vergessen in Technologie
- Datenschutzfreundlich

Technischer Hintergrund: wichtigste Frage bei verteilten Speichernetzen: wie entscheiden wir, was wir löschen?

Und Update-Infos? In konstanter Zeit: Date Hints

- Nutzer: `SSK@.../meine-seite-1/...` → `SSK@.../meine-seite-2/activelink.png`
- Entwickler: `USK@.../meine/seite/1`
  - `SSK@[key]/[sitename]-DATEHINT-[year]`

```
HINT
46
2013-7-5
```

DATEHINT-[year], DATEHINT-[year]-WEEK-[week], DATEHINT-[year]-[month], DATEHINT-[year]-[month]-[day]

Ordner in Freenet: Manifest-Daten

- Ein Archiv (Tarball), transparenter Zugriff

Ordner in Freenet: Als Manifest

Explore a site

List the content of a manifest
Freenetkey to explore: SSK@LHeuG-SU5ZvYQXTu8Y9mhjCYyQxB-m-W~ryElufr-2M,Ij9l0U1Wa~FQu7GFBf~ciwUbCwj Explore!
☐ parse manifest recursive (include multilevel metadata/subcontainers)

Key: SSK@LHeuG-SU5ZvYQXTu8Y9mhjCYyQxB-m-W~ryElufr-2M,Ij9l0U1Wa~FQu7GFBf~ciwUbCwpTFv6mWZkS1YuoxQk,AQACAAE/arnebab-org-413 (Manifest)

	Type	Name	Size	Mime	Target
0-R	[s] SMF		(34 Items)		
0-0	[c] SYS	/		<NoMime>	->index.html
0-0	[c] AMR	/software		<NoMime>	.metadata-0

USK@LHe. . . ,Ij9. . . ,AQACAAE/arnebab-org/413/

Schnittstellen

- Browser
- Verteilte Datenbank für Programme
- Plugins

Der Browser

- Zugriff üblicherweise auf `http://localhost:8888`
- freenetbrowser (automatisch generiertes Firefox-Profil) für bessere Sicherheit
- Optimierungen für Pre-Fetching und Media-Streaming

http://localhost:8888/USK@rQn...,I1v...,AQACAAE/gms/16/

Externe Programme

- Server für Foren/NNTP (FMS) und IRC (FLIP)
- GUI-Programme (jSite)

Externe Programmier-Schnittstellen

- FCP: Freenet Client Protokoll
  - HTTP-Ähnlich: `Key: value` Zeilenweise, Optional Data-Bytes am Ende
  - https://github.com/freenet/wiki/wiki/FCPv2
- Bibliotheken
  - Maintained: Java, Python
  - Unmaintained or experimental: ruby, go, C++
  - https://github.com/freenet/wiki/wiki/Projects#libraries
- Plugins
  - https://github.com/freenet/wiki/wiki/Plugin-API
  - github.com/freenet/wiki/wiki/Projects#plugins

Schnittstelle: FCP

Async für Programme:

- Put/Putdir/Get
- Subscribe to key
- Plugins kontrollieren

```
ClientHello
Name=My Client
ExpectedVersion=2.0
EndMessage
NodeHello
...
EndMessage
ClientPut
URI=CHK@
UploadFrom=disk
Filename=/tmp/debian-dvd1.iso
Identifier=sarge-disk-1
Global=true
EndMessage
```

Latenz in der Praxis

- Bis zu 2kiB, raw, realtime mode: <30s
- Große Dateien, im Manifest: ~5 min

Realtime

```
PriorityClass . 2 ;; high
MaxRetries . 0 ;; default: 10
RealTimeFlag . true
DontCompress . true
ExtraInsertsSingleBlock . 0
ExtraInsertsSplitfileHeaderBlock . 0
```

Bulk

```
PriorityClass . 3 ;; medium
RealTimeFlag . false
DontCompress . false
```

Schnittstelle: Plugins

- In die Web-Oberfläche integriert
- Schwache Abstraktion
- Zugriff auf das Innenleben (riskant)
- Leichtester Einstieg: Bestehendes Plugin anpassen

Beispiele: Sone oder Sharesite

Grundlagen der Kommunikation über Freenet

- Einstieg: Seed-keys + Captcha-Queue: KSK-Prefix
- Suche: Nutzerspezifische Seiten mit Links, Update-Infos
- Verteilung: Gossip keys, Dateien einfach hochladen
- Störungsresistenz: Web of Trust mit langsam steigender Sichtbarkeit

Einwurf: Konstruktive Spammer: https://xkcd.com/810/

Schutzmaßnahmen

- Datenschutz trotz Browser
- Abstreitbarkeit
- Spam-Abwehr

Content Sanitizing: Vor dem Browser schützen

Browser und Media-Player: Anderes Bedrohungs-Szenario

$\Rightarrow$ Inhalte filtern, um Zugriffe auf Clearnet-Resourcen zu vermeiden

Beispiel: Album-Art einer Radiosendung über URL nachladen.

Abstreitbarkeit: Das war jemand anders

- Anfragen haben Hops to Live (HTL)
- Mit jedem Schritt um 1 verringert
- HTL 18 wird nur bei 50% der Verbindungen verringert — Wahl bleibt über die Dauer der Verbindung bestehen
  $\Rightarrow$ Anfragen mit HTL 18 können immer von einem anderen Knoten kommen

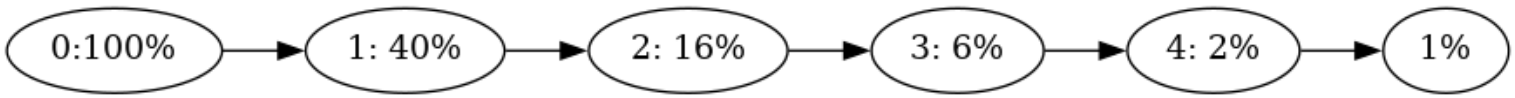
Spam-Abwehr

WoT (Web of Trust): Eine von zwei praktisch genutzten Möglichkeiten. Die andere ist FMS (Freenet Message System).

- ID = USK
- Trust -100 bis 100
- Rank: Distanz → capacity
- Score: Summe über alle Wertungen: trust * rank
- Skaliert bei 22 Nachrichten pro Tag[2] (Dunbar-Zahl)

[2] https://www.draketo.de/english/freenet/deterministic-load-decentralized-spam-filter

Capacity



- Rank 1 40 %. rank 1: 100 trust, 40 Punkte als Score.
- Rank 2 16 %
- Rank 3 6 %
- Rank 4 2 %
- Rank 5 und niedriger: 1 %

Integer-Mathematik: `2 * 6 / 100 = 0`.

Zusammenfassung

- Freundeskreis / Opennet,
- Ohne Server,
- Schlüssel als Pseudonym,
- Spamresistenz,

- Small-World
- Schlüsseltypen (CHK: Inhalt, USK: Aktualisierbar, KSK: Passwort)
- Dateien werden aufgeteilt, Redundanz
- Lebenszeit nach Zugriffshäufigkeit
- Ordner
- Schnittstellen
- Schutzmaßnahmen

Werkzeuge

Sieht spannend aus, aber was kann ich mit Freenet praktisch machen?

Der Browser

- Browse
- Hoch-/Herunterladen
- Plugins
- Freund-zu-Freund-Nachrichten
- Lesezeichen mit Update-Info (5 min Latenz)
- Indexe mit Listen von Seiten (pseudonym betriebene Crawler)

Sharesite: Einfachstes pseudonymes Veröffentlichen

http://127.0.0.1:8888/Sharesite

FMS and Flip: pseudonyme Foren and IRC

- FMS: http://127.0.0.1:8888/USK@OnpnMrqZNKRCRoGojZV93UNHCMN-6UU3rRSAmP6jNLE,~BG-edFtdCC1cSH4O3BWdeIYa8Sw5DfyrSV-TKdO5ec,AQACAAE/fms/153/
- FLIP: http://127.0.0.1:8888/USK@pGQPA-9PcFiE3A2tCuCjacK165UaXO7AQYw98iDQrNA,8gwQ67ytBNRO3hNj7JU~ceeew22HVq6G50dcEeMcgks,AQACAAE/flip/17/

Sone: pseudonymes Microblogging

Beispiele: USK@nwa. . . ,DuQ. . . ,AQACAAE/sone/82/

Freemail: vertrauliche E-Mail

http://127.0.0.1:
8888/USK@M0d8y6YoLpX0eQGxu0-IDg8sE5Yt~Ky6t~GPyyZe~zo,
KlqIjAj3~dA1Zf57VDljkmp3vHUozndpxnH-P2RRugI,AQACAAE/
freemail/8/

Shoeshop: Sneakernet mit Freenet

http://127.0.0.1:8888/USK@MYLAnId-ZEyXhDGGbYOa1gOtkZZrFNTXjFl1dibLj9E,Xpu27DoAKKc8b0718E-ZteFrGqCYROe7XBBJI57pB4M,AQACAAE/Shoeshop/3/

jfniki: Wiki über Freenet

http://127.0.0.1:8888/USK@jZVIWXW-5nl4Bco~7lWbVazRzFQv78X9RnJsWWKdWm4,zBn2IimGcyEQ7mh~w~tRABGAYH6F4Zwoqfh8Cv7tVhY,AQACAAE/jFniki.Index/12/Contributing.html

KeyUtils: Technische Details über Uploads

http://127.0.0.1:8888/KeyUtils/

Keepalive: Ein paar Dateien verfügbar halten

http://127.0.0.1:8888/KeepAlive/

Freereader: RSS über Freenet verbreiten

http://127.0.0.1:8888/freereader/feeds

pyFreenet: Kommandozeilenwerkzeuge

https://github.com/freenet/pyFreenet

infocalypse: Versionsverwaltung über Freenet

https://hg.sr.ht/~arnebab/infocalypse/browse/Readme.txt

jSite: Webseiten hochladen mit GUI

http://127.0.0.1:8888/USK@1waTsw46L9-JEQ8yX1khjkfHcn--gOMlMsTlYHax9zQ,oYyxr5jyFnaTsVGDQWk9e3ddOWGKnqEASxAkO8MHT2Y,AQACAAE/jSite/15/

Neuerungen

Was sich in 15 Jahren seit dem Rewrite in 0.7 getan hat.

One secret of success: relentless optimization.

Pitch-Black Attack

2007 haben Christian Grothoff et al. eine Schwachstelle gefunden und belegt.

Routing in the Dark: Pitch Black

Nathan S. Evans Chris GauthierDickey Christian Grothoff

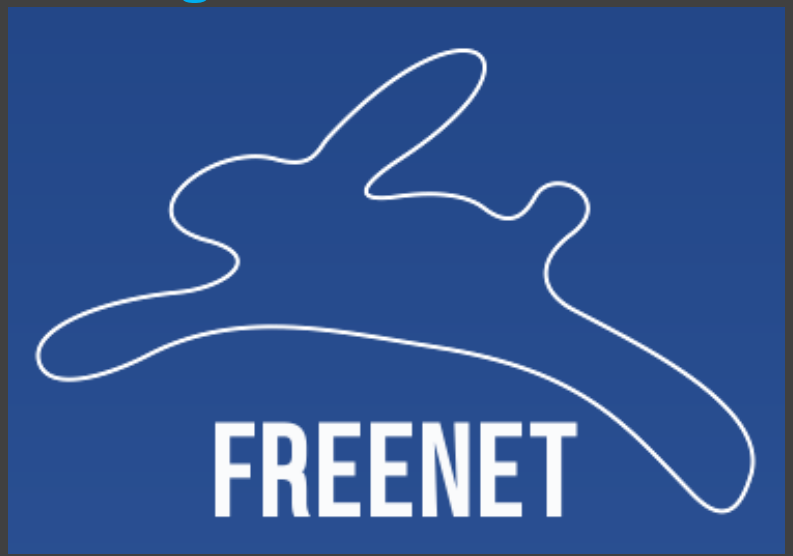
Colorado Research Institute
for Security and Privacy

Department of Computer Science
University of Denver, USA
{natevans,chrisg,grothoff}@cs.du.edu

Pitch black gelöst

The mitigation

2021 haben wir sie endlich **gefixt.**



→ **build 1490: “pitch black streaming”** ←

WoT: Precisely updating and subscription-based

OPTIMIZING A DISTRIBUTED SPAM FILTER FOR FREENET

AKA

THE WEB OF TRUST DEVELOPER'S MANUAL

Dr. Arne Babenhauserheide

Bessere Geschwindigkeit

- Von 10kiB/s bis 11MB/s (und mehr)
- Unterstützt bis zu 15.000 Subscriptions: Binnen 5 Minuten Updates sehen
- 30 Sekunden Round-Trip-Zeit für Chat

Mehr HTML and CSS

- Unterstützung für Teile von CSS3.
- Nur, bei was die Sicherheit garantiert werden kann.

Audio streaming

http://127.0.0.1:8888/USK@~22K5...,IwY...,AQACAAE/stream-radiocc-again/15/

Mit Live-Streaming:

https://github.com/freenet/re-stream-into-freenet

Beispiel:

http://127.0.0.1:8888/USK@j1V...,vsk...,AQACAAE/futo-ian-interview-2022/3/

Video on demand

http://localhost:8888/USK@rQn...,I1v...,AQACAAE/gms/16/

via https://github.com/hyphanet/generate-media-site/

mobile-node: Freenet auf Android

https://freenet-mobile.github.io/app/

FreeChat: Chat auf Android

https://github.com/freenet/free-chat-2

icicles: Nachrichten von Freunden und Knoten verbinden

https://github.com/freenet/icicle

Offene Fragen

- Besseres Routing? (dank Pitch Black mitigation wurden auch neue Strukturen möglich)
- Freund-zu-Freund Verbindungen über tor und i2p? (braucht UDP!)
- Steganographic Transport Plugins (HTTP3?)
- Dezentrale Suche in Freenet (Spider/Library optimierungsbedürftig)

Pläne

No plan survives contact with reality, but a good plan provides set-pieces for the path you might actually walk.

- High-Impact Tasks
- High-Level Roadmap — structured by major version
- Bugtracker-Roadmap — very detailed but outdated

Zusammenfassung 1

Warum gibt es Freenet? Freie Kommunikation

Was ermöglicht Freenet? Vertraulich und Pseudonym, ohne zentrale Server, Datenschutzfreundliche Datenbank für verteilte Programme.

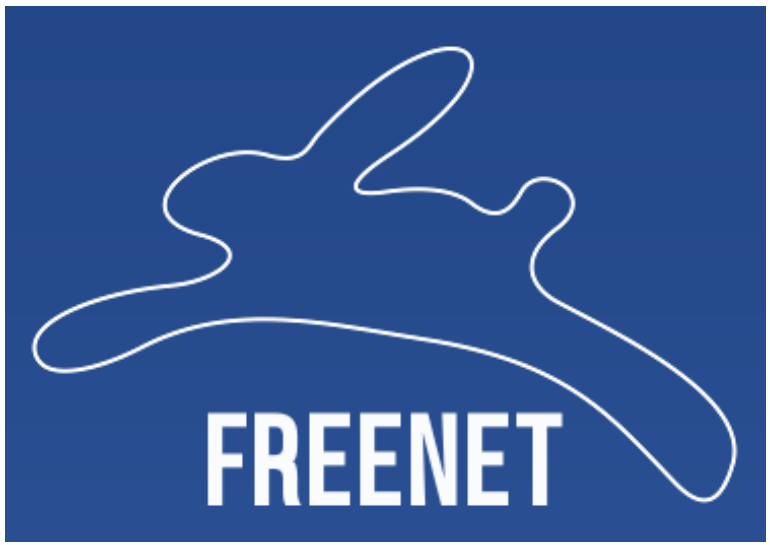
Wie funktioniert Freenet? -

- Einstieg: Freund-zu-Freund (High Security) oder über Seednode (Opennet)
- Routing: Small-World mit FOAF-Routing
- Dateien: Aufteilen, Verschlüsseln, 100% Redundanz, Verfügbar solange genutzt.

Zusammenfassung 2

Was hat sich geändert? Pitch Black gelöst, Spam-Schutz über WoT/Sone und FMS, schneller, IRC Chat, Multimedia-Streaming, Android-Unterstützung, Sharesite für einfachste Webseiten, Stetige Optimierung in praktischer Nutzung.

Nutzt Freenet / Hyphanet!



- Sharesite
- Sone
- Verbindung im Freundeskreis

freenetproject.org

Andere Projekte

- Tor mit SecureDrop, z.B. auf https://taz.de/investigativ
  (wechselt auf den Tor Browser, bevor ihr auf die Seite geht!)

Quellen

Bilder: Hase unter GPL, alle weiteren cc by.

- https://www.flickr.com/photos/anonymous-munich/3282278914
- https://www.flickr.com/photos/gruenejugendffm/6272541036
- https://www.flickr.com/photos/eppofficial/13564824463
- https://www.flickr.com/photos/maguide/6092244239

Quellen 2

- https://www.flickr.com/photos/okubax/15814107199
- https://www.flickr.com/photos/okubax/14248440483
- https://www.flickr.com/photos/okubax/15812839470
- https://www.flickr.com/photos/digitpedia/4709307610

Quellen 3

- https://www.flickr.com/photos/focusc/4758319160
- https://www.flickr.com/photos/amitd/4693814169
- commons.wikimedia.org/wiki/File:International_newspaper,_Rome_May_20
- commons.wikimedia.org/wiki/File:Edward_Snowden_2013-10-9_%281%29_%28cropped%29.jpg

Quellen 4

Lizenzen:

- https://creativecommons.org/licenses/by/2.0/deed.en
- https://gnu.org/l/gpl

(und neuere Versionen)

References I