

# Cypherpunkts und Privatsphäre

- Prof. Dr. Florian Tschorsch
- Cypherpunks
  - Was sind Cypherpunks?
  - Wie hat sich die Bewegung entwickelt?
  - Wichtige Personen und Projekte
- Forschungsfrage

- Informatik-Studium an der Heinrich-Heine-Universität Düsseldorf
- Promotion an der Humboldt-Universität zu Berlin in 2016
- Seit 2017 Juniorprofessor an der Technischen Universität Berlin
- Forscht an anonymer Kommunikation und Blockchain



Quelle: [https://pbs.twimg.com/profile\\_images/824000575083790340/hclYN\\_4Q\\_400x400.jpg](https://pbs.twimg.com/profile_images/824000575083790340/hclYN_4Q_400x400.jpg)

A person who uses encryption when  
accessing a computer network  
in order to ensure privacy,  
especially from government authorities.

(laut Oxford Dictionary [<https://en.oxforddictionaries.com/definition/cypherpunk>])

# Einwurf: Privatsphäre

- Begriff verwirrt oft als das er beschreibt
- Am besten als „shorthand umbrella term“ benutzt
- „Der Bereich, in dem eine Person selbst bestimmt [...], wem sie wann und warum welche Information über sich selbst zugänglich macht“

# Einwurf: Geheimhaltung

- „Ein Geheimnis ist eine meist sensible Information, die einem oder mehreren Eigentümern zugeordnet ist“
- Aufbewahren von Geheimnissen, damit diese nicht in fremde Hände geraten

# Cypherpunk Manifest

- Privatsphäre ist wichtig für offene Gesellschaft
- Privatsphäre  $\neq$  Geheimhaltung
- Werkzeuge: Anonyme Transaktionssysteme & Verschlüsselung
- Jede Person muss eigene Privatsphäre verteidigen
- Cypherpunks schreiben Code für eigene und Privatsphäre anderer
- Wichtig: Gesellschaft muss sich auf Privatsphäre als allgemeines Gut einigen



# Einige wichtige Projekte



„Tor logo“ by [The Tor Project, Inc.](#),  
licensed under [CC BY 3.0 US](#)



[https://github.com/WhisperSystems/Signal-iOS  
/blob/master/Signal/iTunesArtwork%403x.png](https://github.com/WhisperSystems/Signal-iOS/blob/master/Signal/iTunesArtwork%403x.png)



„New bitcoin logo“ by Bitboy,  
licensed under CC0

# Einige wichtige Personen



Bild: Wikipedia / Tobias Klenze / [CC-BY-SA 4.0](#)



„Moxie Marlinspike“ by [Knight Foundation](#),  
licensed under [CC-BY-SA 2.0](#)

Satoshi Nakamoto

Eric Hughes

Ich habe doch nichts zu verbergen!

# Weiterführende Links

- Seite von Prof. Dr. Florian Tschorsch (<http://www.dsi.tu-berlin.de/menue/arbeitsgruppe/tschorsch/>)
- Cypherpunk Manifest (<https://www.activism.net/cypherpunk/manifesto.html>)
- Englischer Wikipedia-Artikel zu Cypherpunk (<https://en.wikipedia.org/wiki/Cypherpunk>)
- Spiegel Online Artikel zu Cryptopartys (<http://www.spiegel.de/netzwelt/netzpolitik/cryptoparty-bewegung-die-cypherpunks-sind-zurueck-a-859473.html>)

# Weitere Quellen

- <https://en.oxforddictionaries.com/definition/cypherpunk> (zuletzt abgerufen am 13.12.2017)
- <https://twitter.com/flotschorsch> (zuletzt abgerufen am 13.12.2017)
- <https://de.wikipedia.org/wiki/Geheimnis> (zuletzt abgerufen am 13.12.2017)
- Solove, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, p. 745, 2007; GWU Law School Public Law Research Paper No. 289. Available at SSRN: <https://ssrn.com/abstract=998565>

# Weitere Quellen (Fortsetzung)

- Prof. Dr. Lutz Prechelt: „Vorlesung Anwendungssysteme: Privatsphäre“