Freenet

Ein anonymes, dezentrales Filestorage System

Freenet – Überblick

- Motivation
  - Informationsfreiheit
  - Ein dezentrales System
- Architektur der Knoten
  - GUID Keys
  - Nachrichten
  - Datenaustausch

Freenet – Überblick

- Architektur des Netzes
  - Knoten einfügen, entfernen
  - Routing
  - Speicherplatzverwaltung
- Analyse
  - Performance
  - Fehlertoleranz
  - Angriffe
- Zusammenfassung

Freenet – Motivation

- Erfinder: Ian Clarke
  - Diplomarbeit 1999, Universität Edinburgh
  - Implementiert in Java
- Ziel
  - Nichtzensierbarer Datenspeicher

`http://www.freenetproject.org`

Freenet – Motivation

- Informationsfreiheit
  - Anonymität im Internet?
  - Überwachung
  - Zensur

Freenet – Motivation

- Ein dezentrales System
  - Ausfallsicherheit
  - Fehlertoleranz
    - Verbindungsprobleme
  - Korruption
  - Monopole

Freenet – Architektur

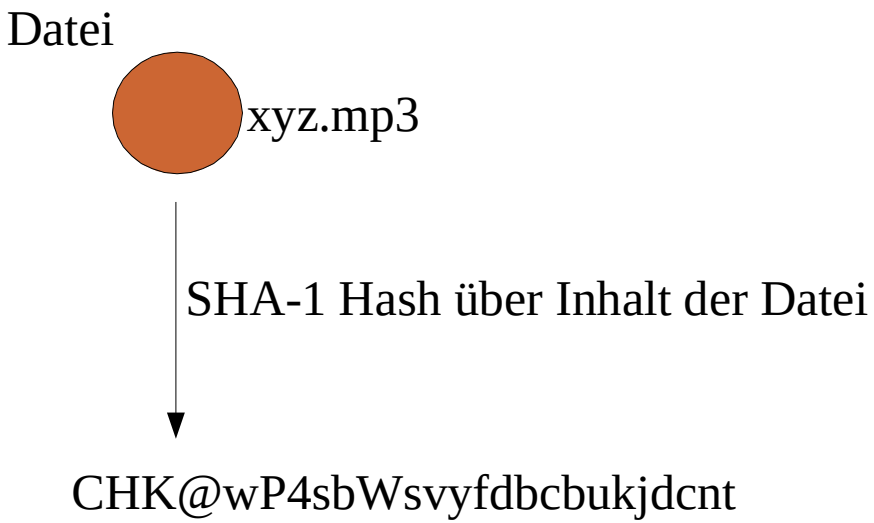
- Allgemeine Architektur
  - Völlig dezentral, kein Vermittlungsserver
  - Anonymität (Informationskonsument und -anbieter)
  - Datenspeicher
  - Erweiterbarkeit

Freenet – Architektur

- GUID Keys
  - *Global Unique Identifier*
  - Erzeugt mit SHA-1 Verfahren
  - CHK – Content Hash Keys
  - SSK – Signed Subspace Keys

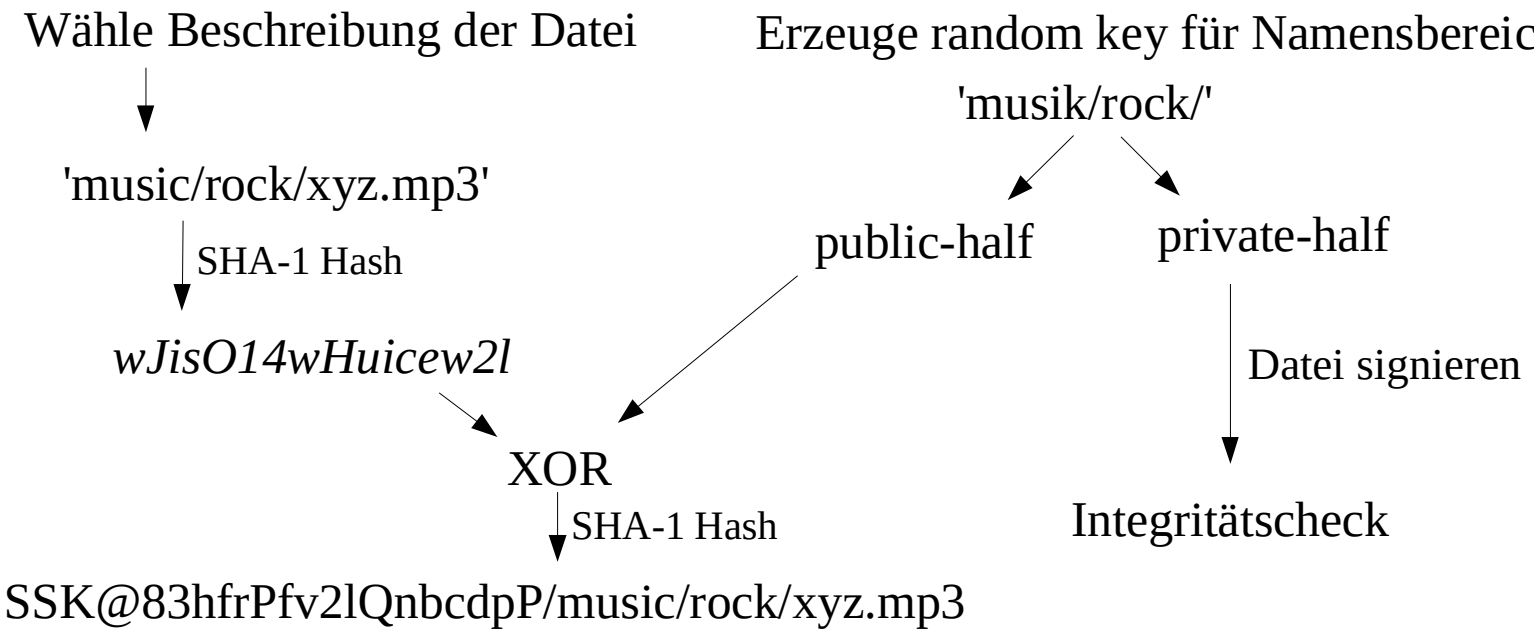
Freenet – Architektur

- Content Hash Key



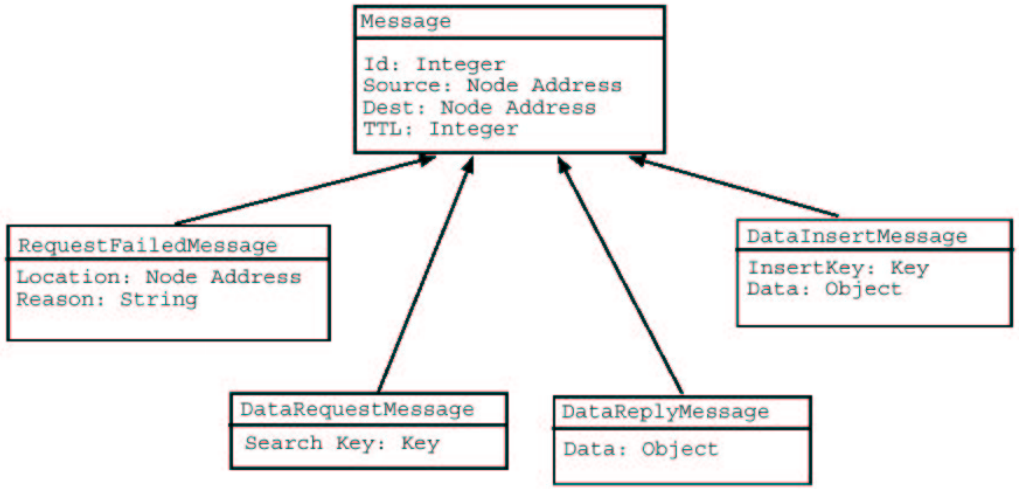
Freenet – Architektur

- Signed Subspace Key



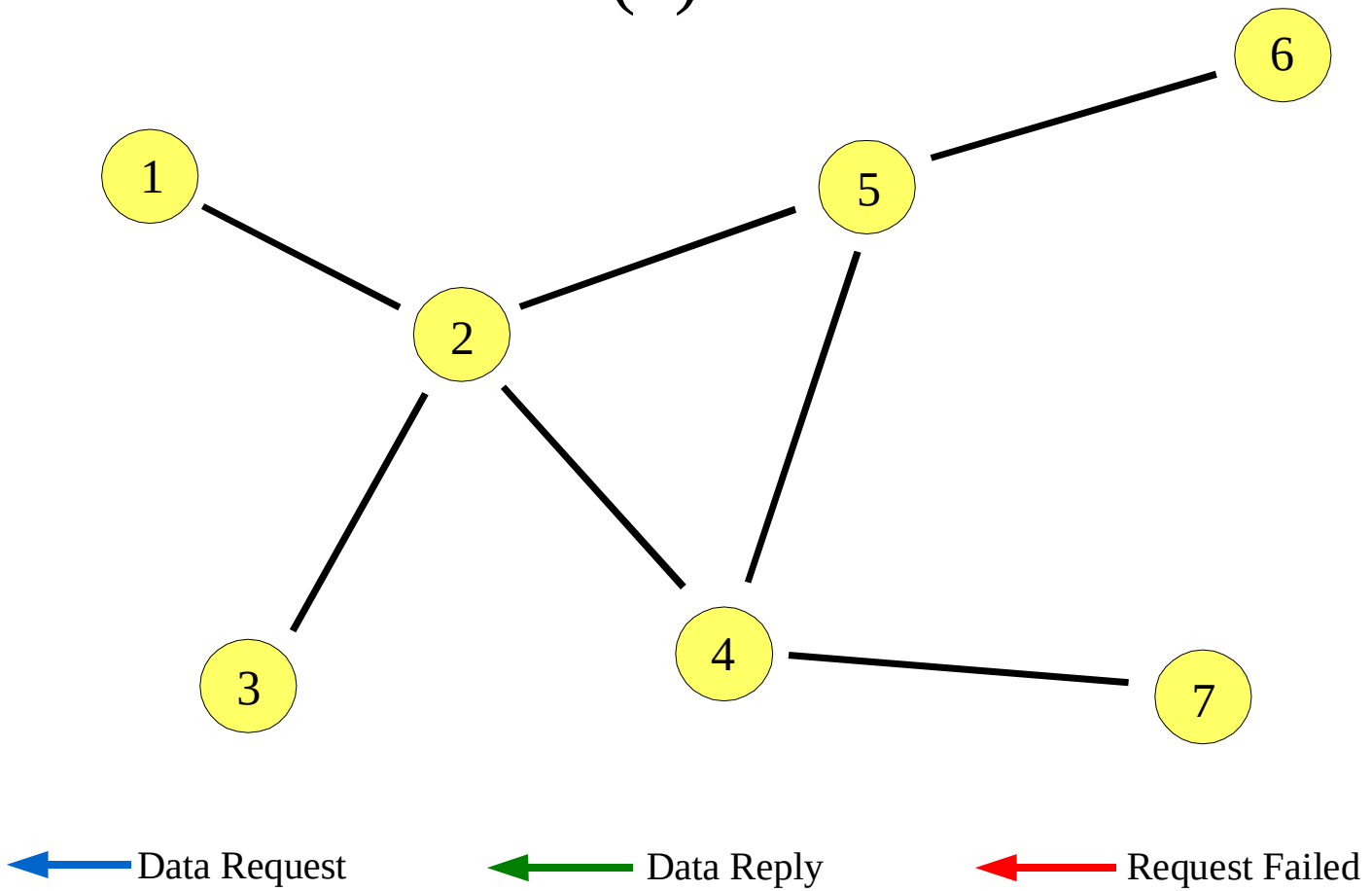
Freenet – Architektur

- Nachrichten
  - Data Request
  - Data Reply
  - Data Insert
  - Request Failed



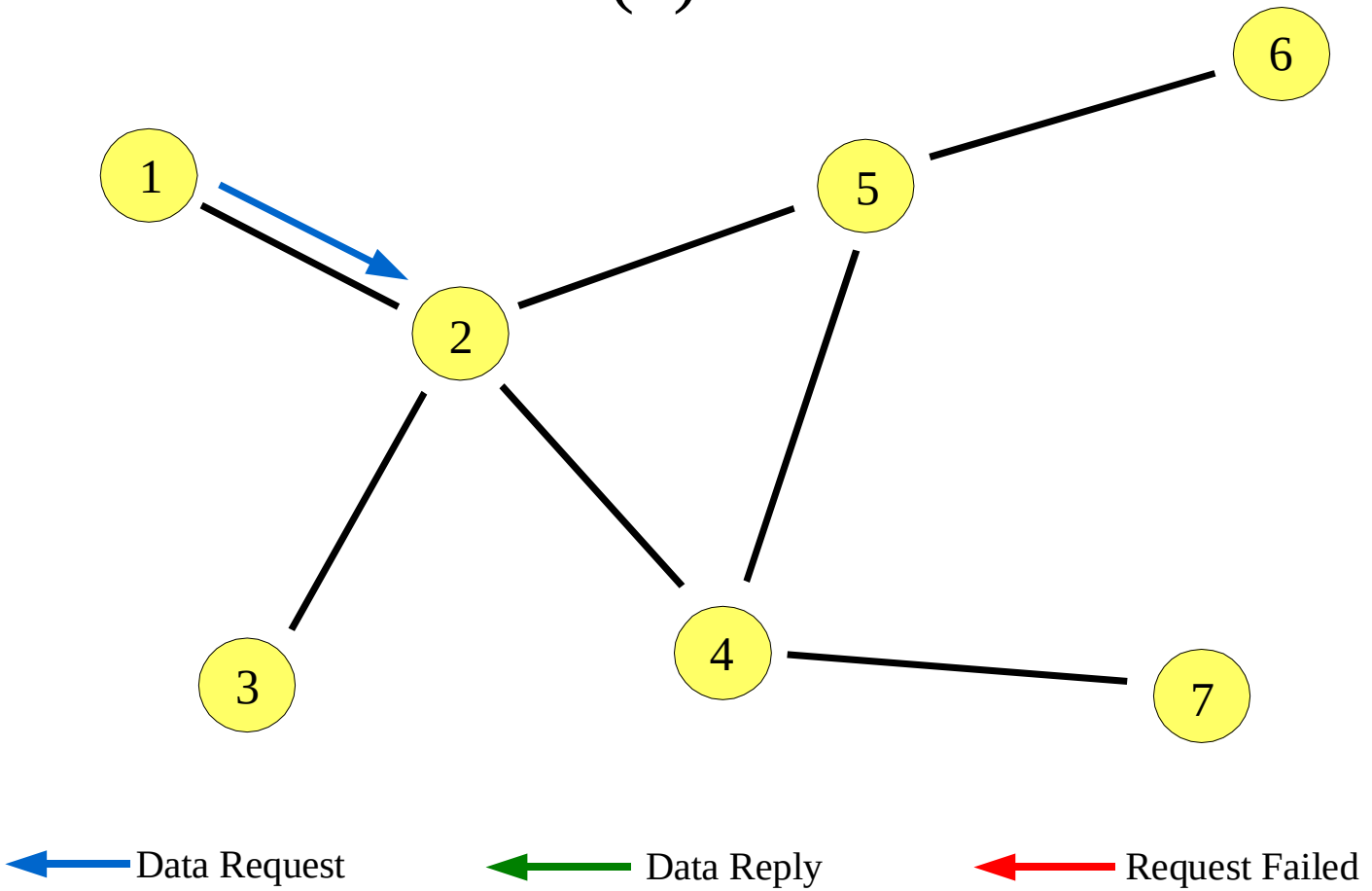
Freenet – Architektur

- Daten anfordern (1)



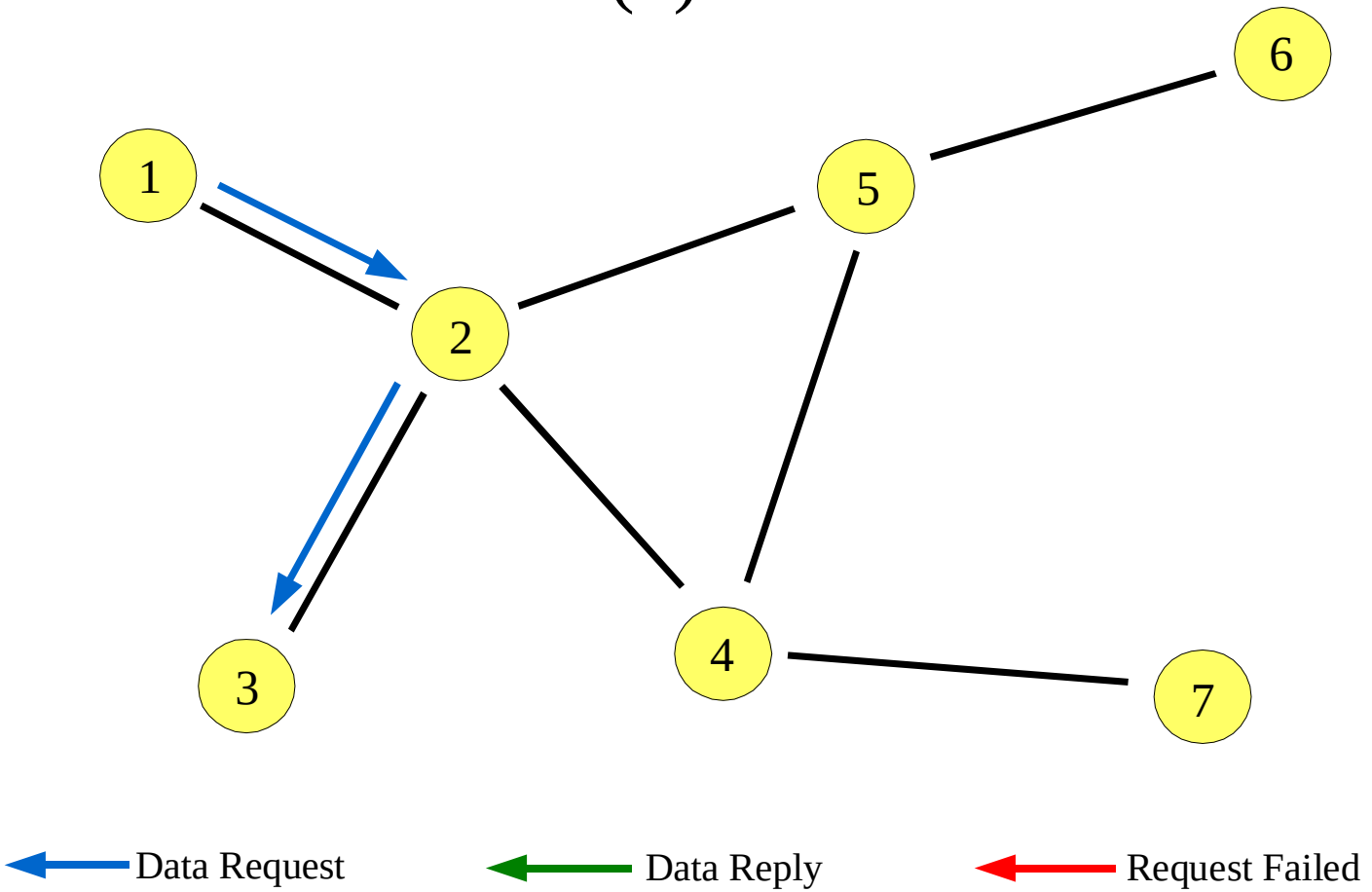
Freenet – Architektur

- Daten anfordern (2)



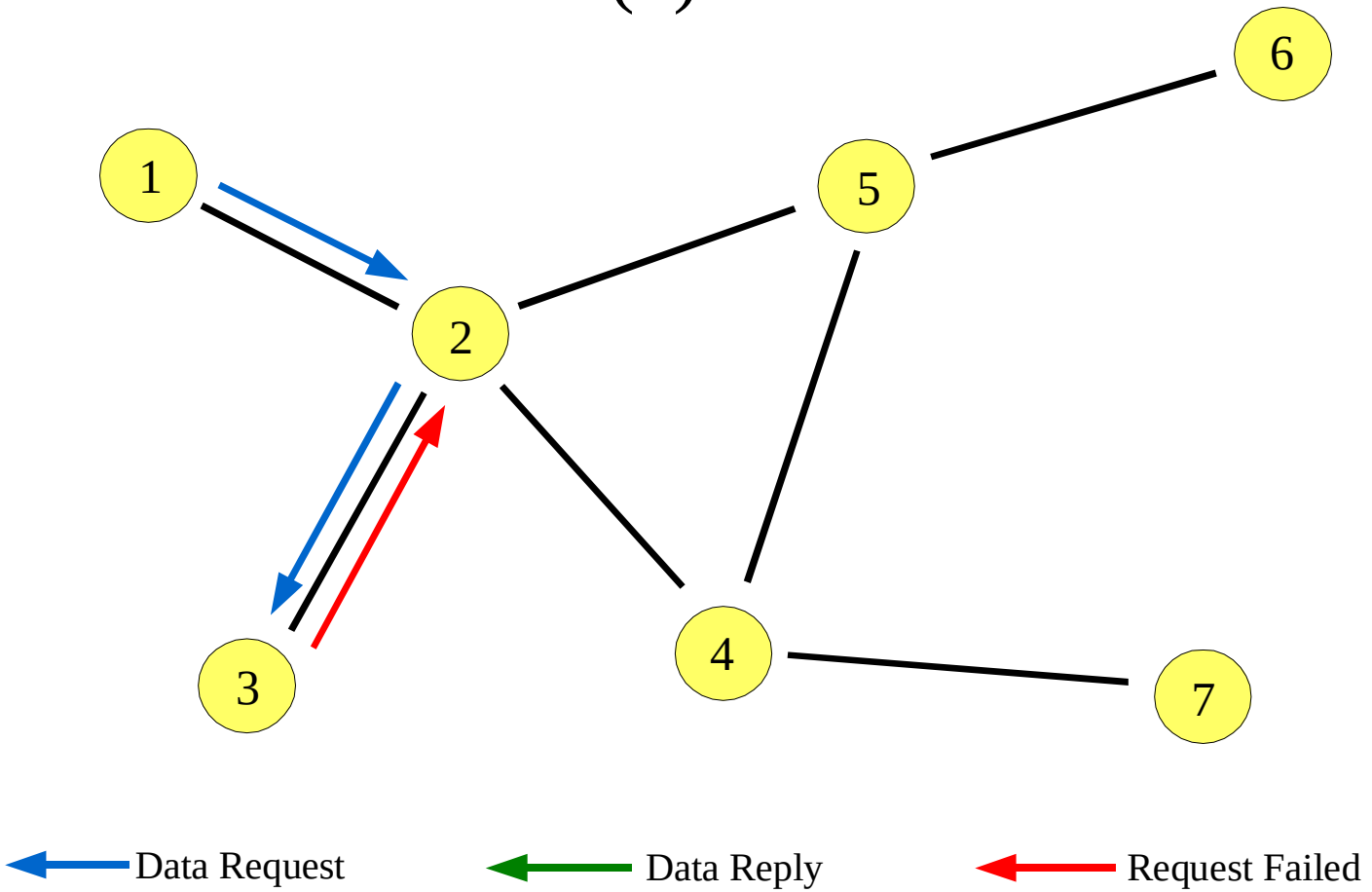
Freenet – Architektur

- Daten anfordern (3)



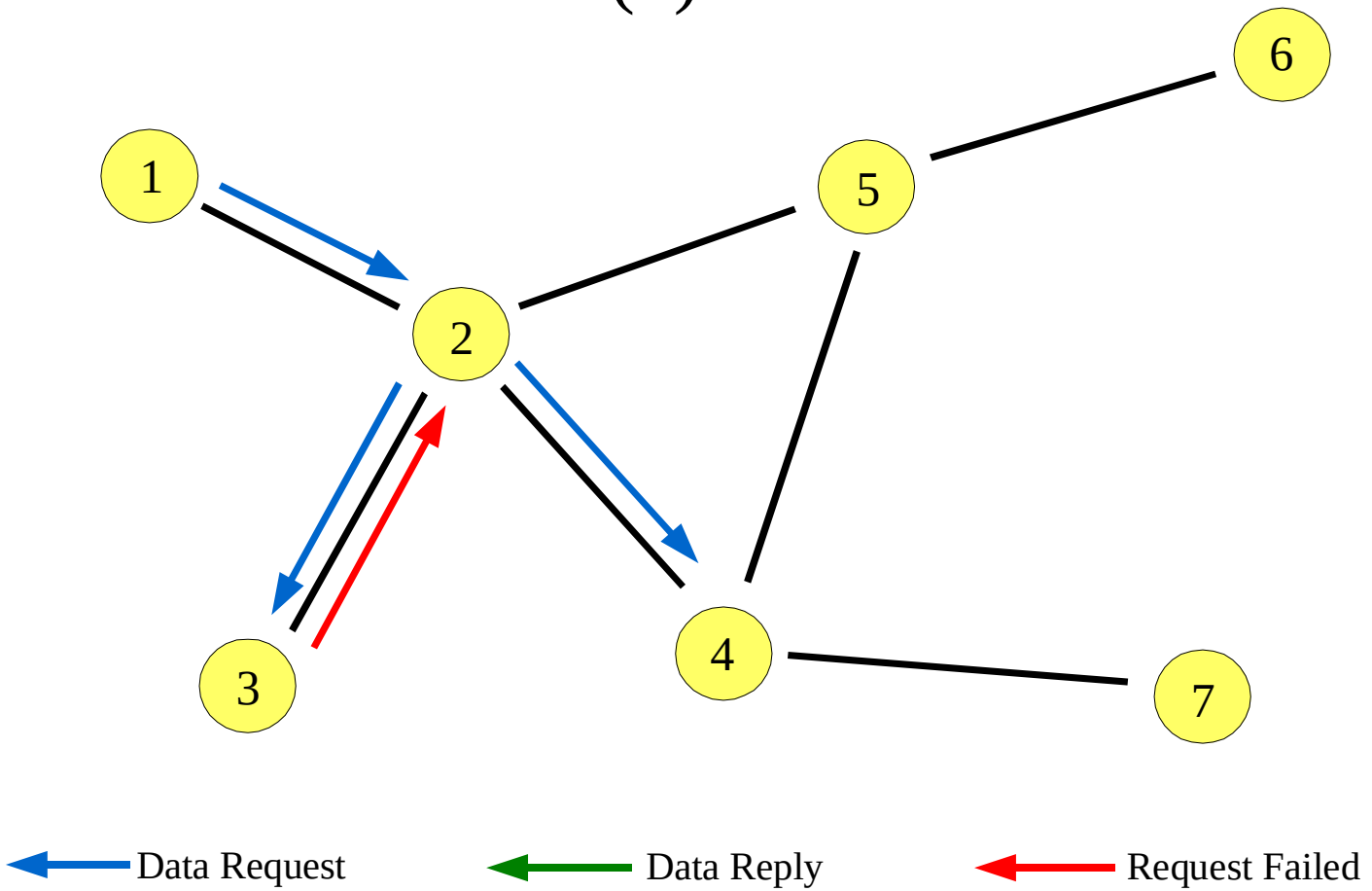
Freenet – Architektur

- Daten anfordern (4)



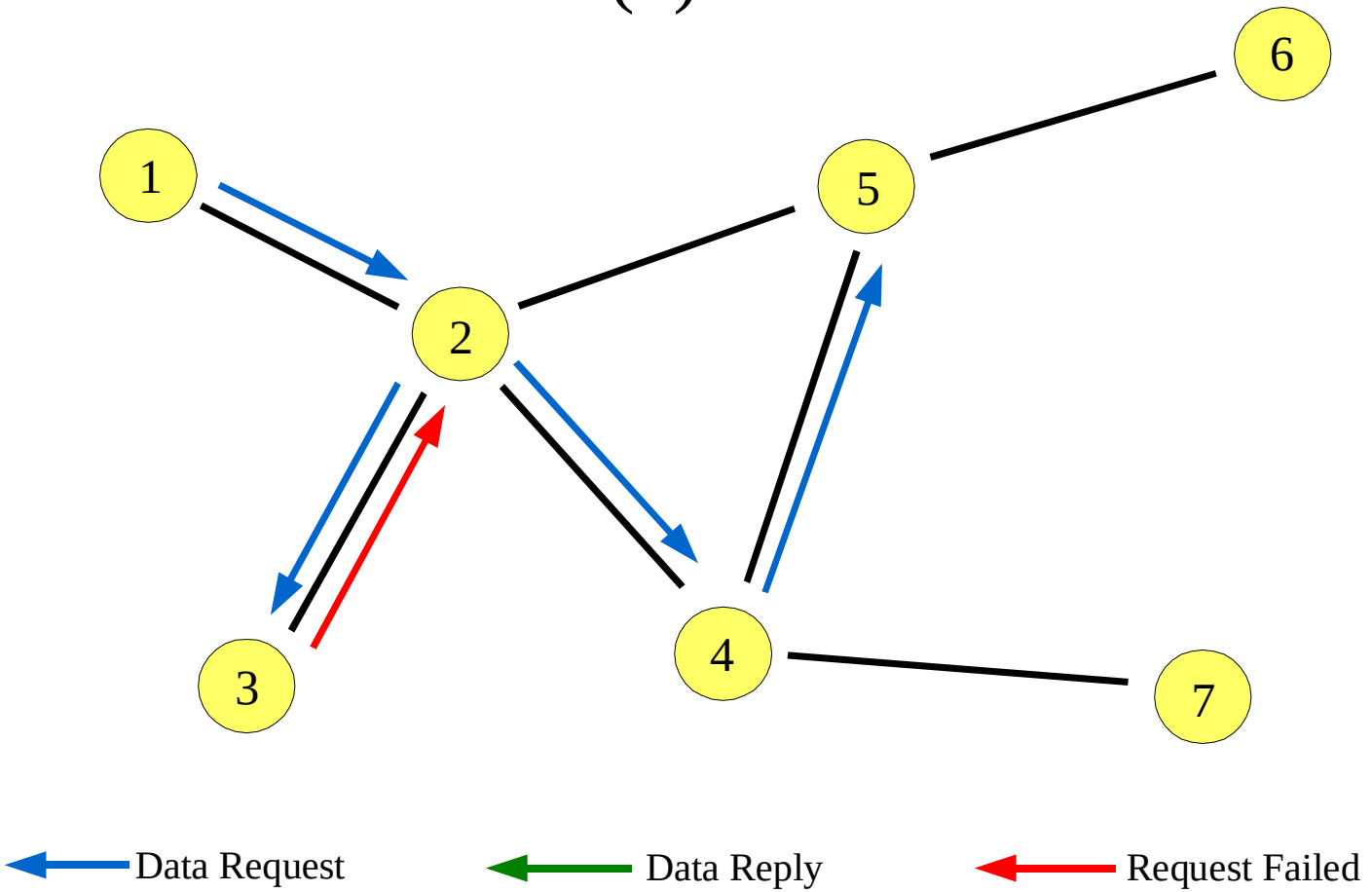
Freenet – Architektur

- Daten anfordern (5)



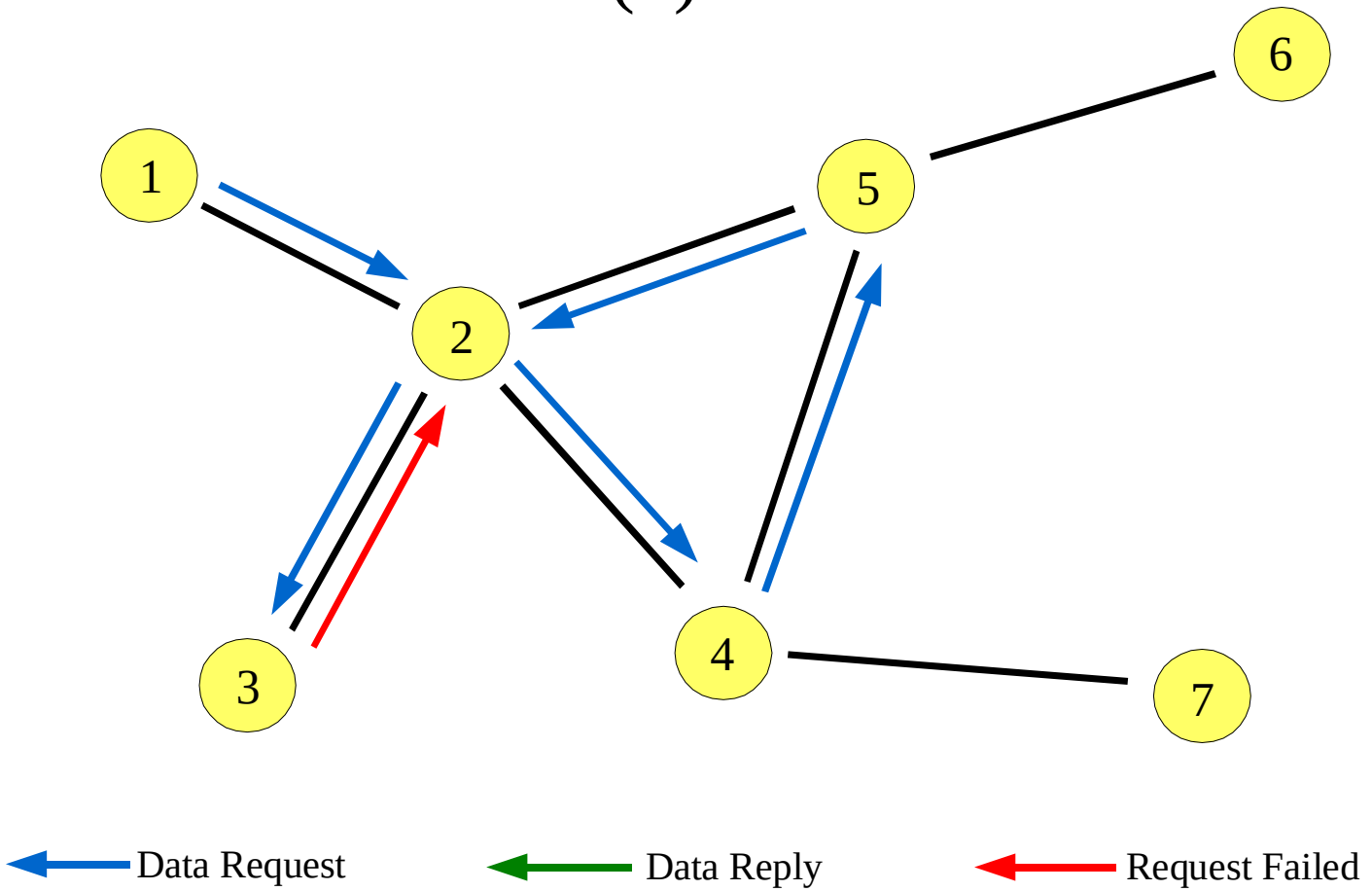
Freenet – Architektur

- Daten anfordern (6)



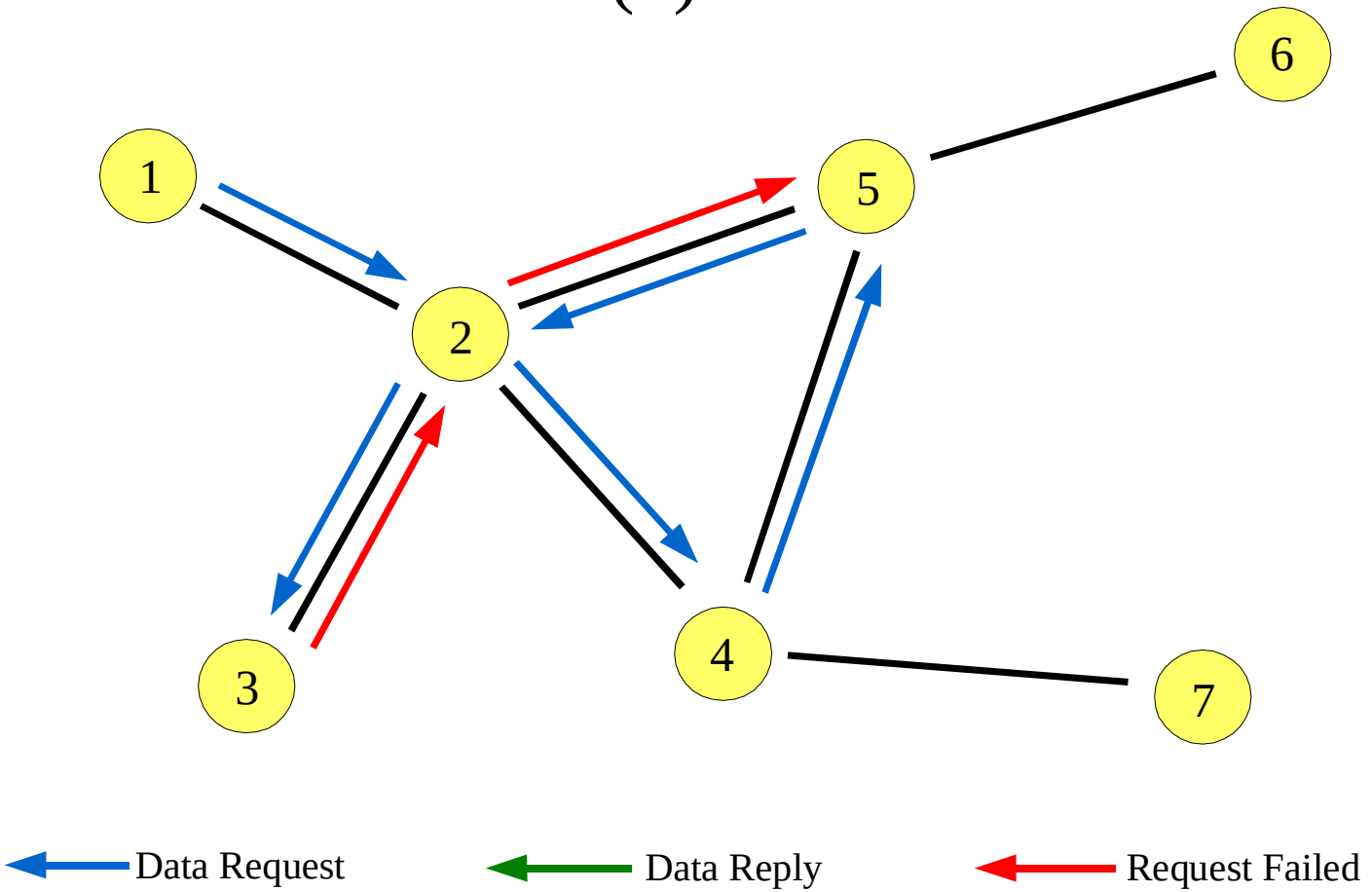
Freenet – Architektur

- Daten anfordern (7)



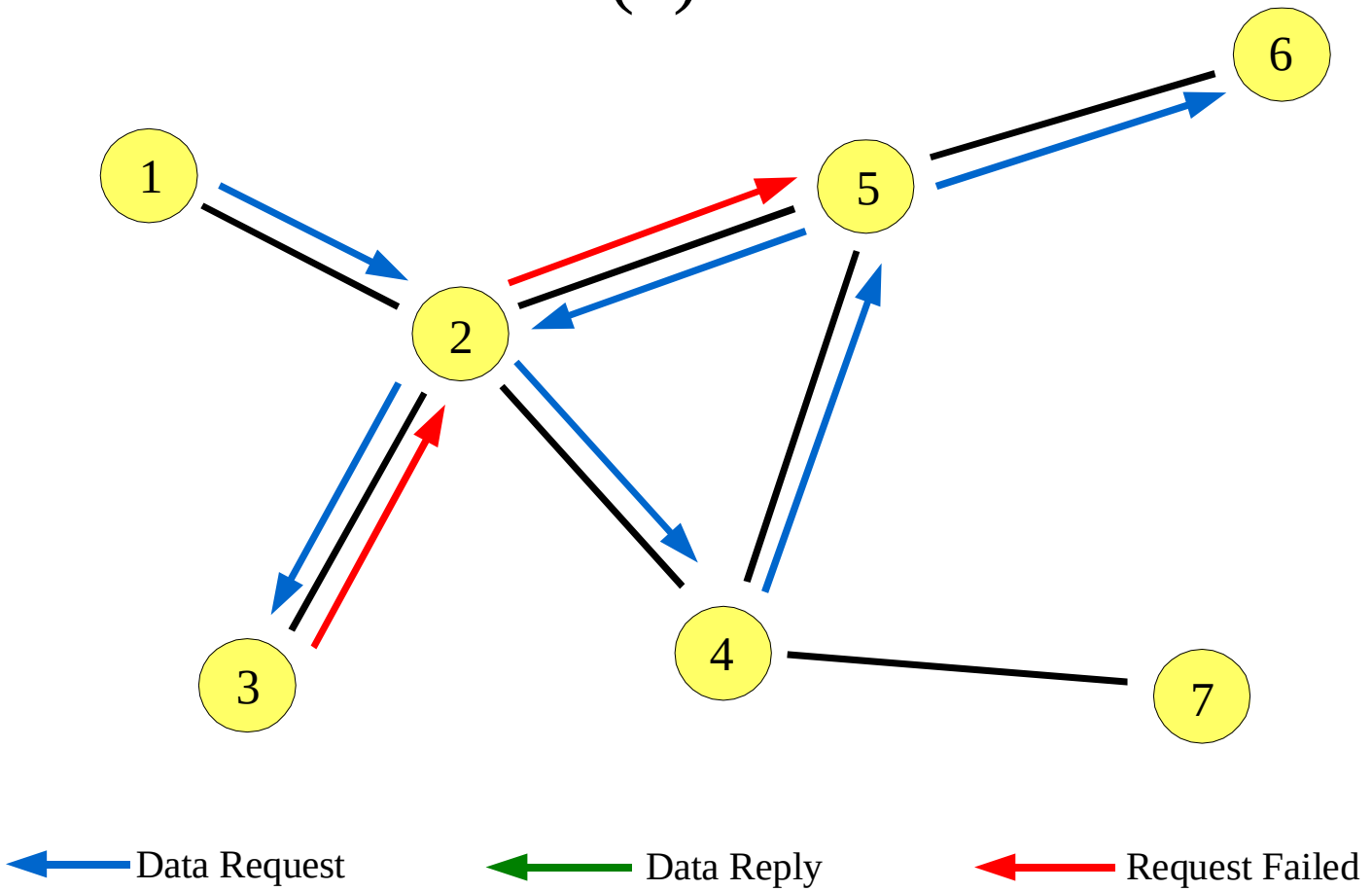
Freenet – Architektur

- Daten anfordern (8)



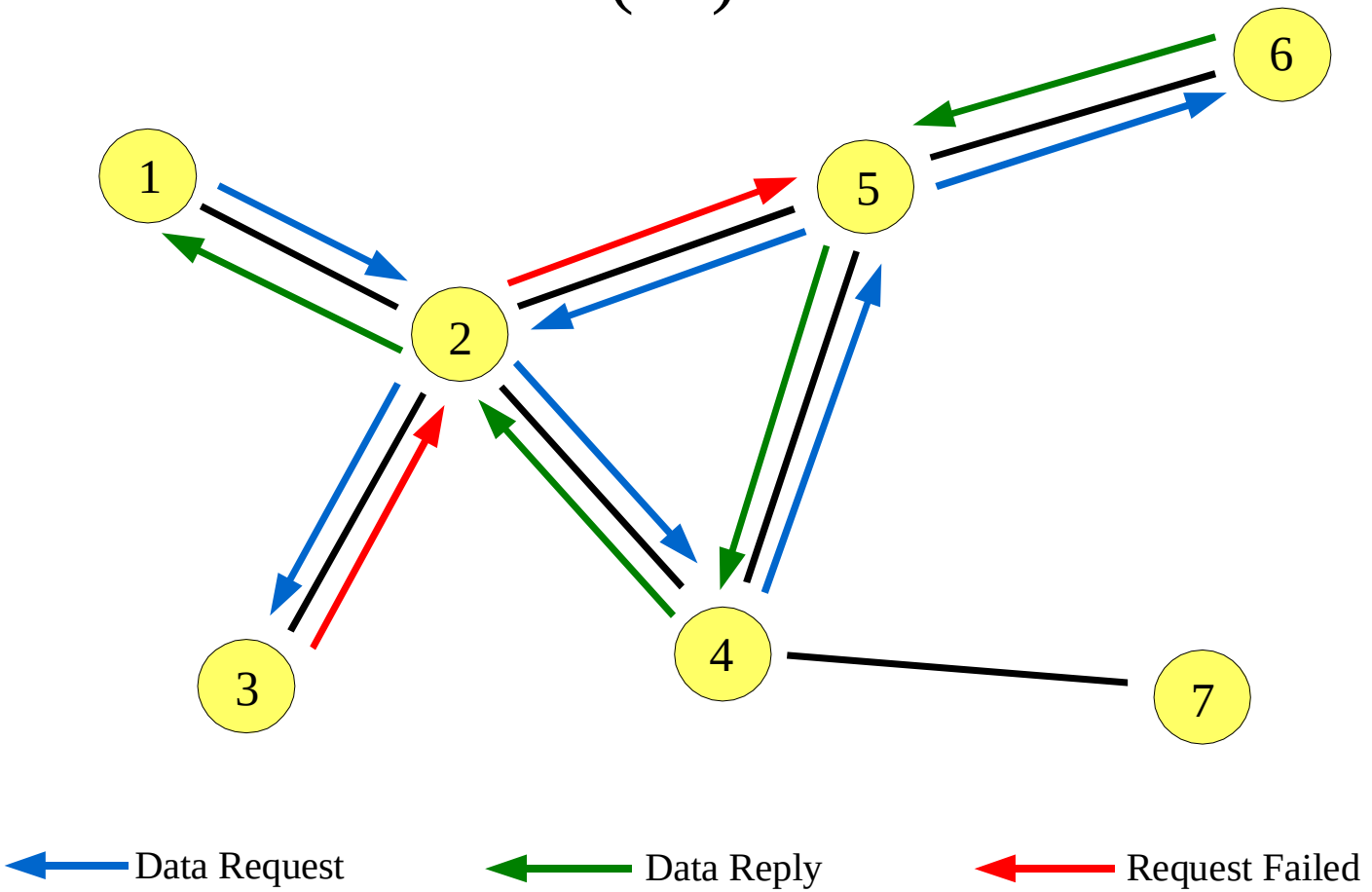
Freenet – Architektur

- Daten anfordern (9)



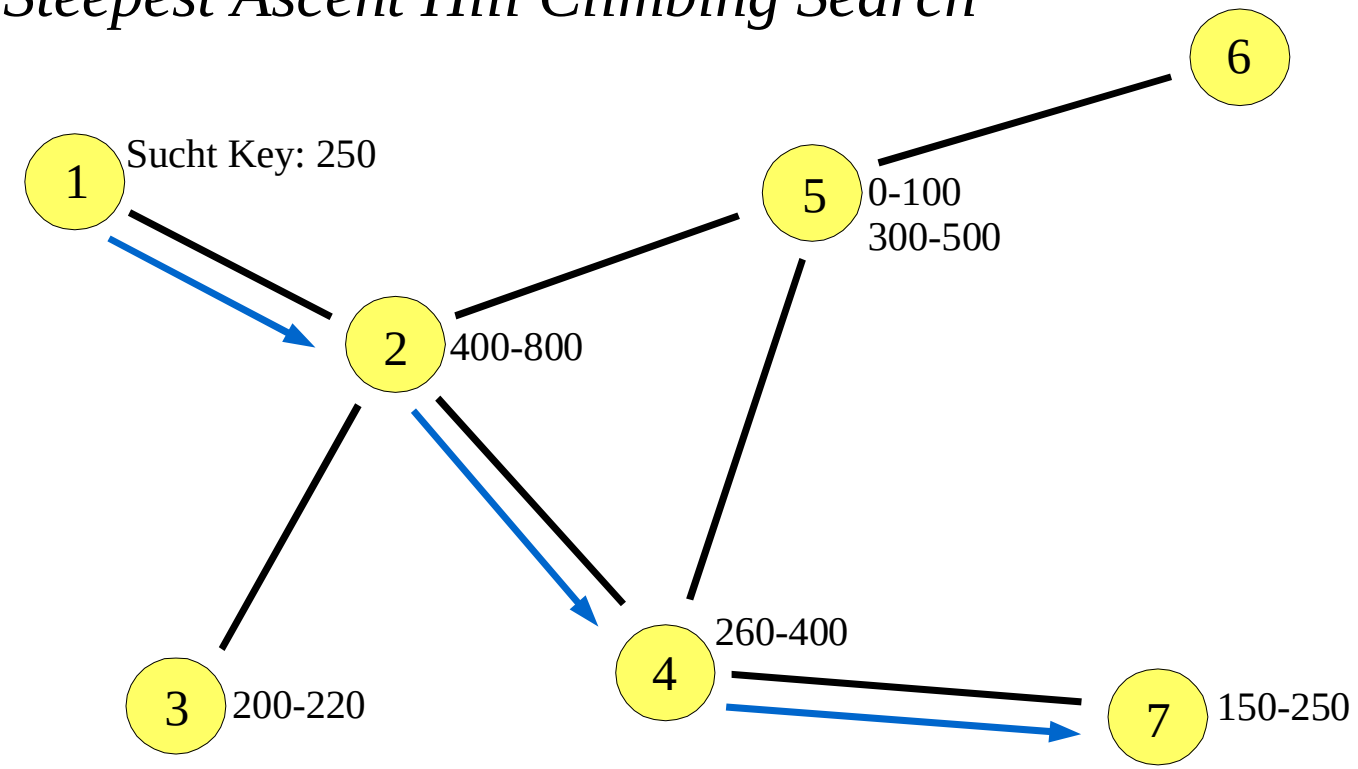
Freenet – Architektur

- Daten anfordern (10)



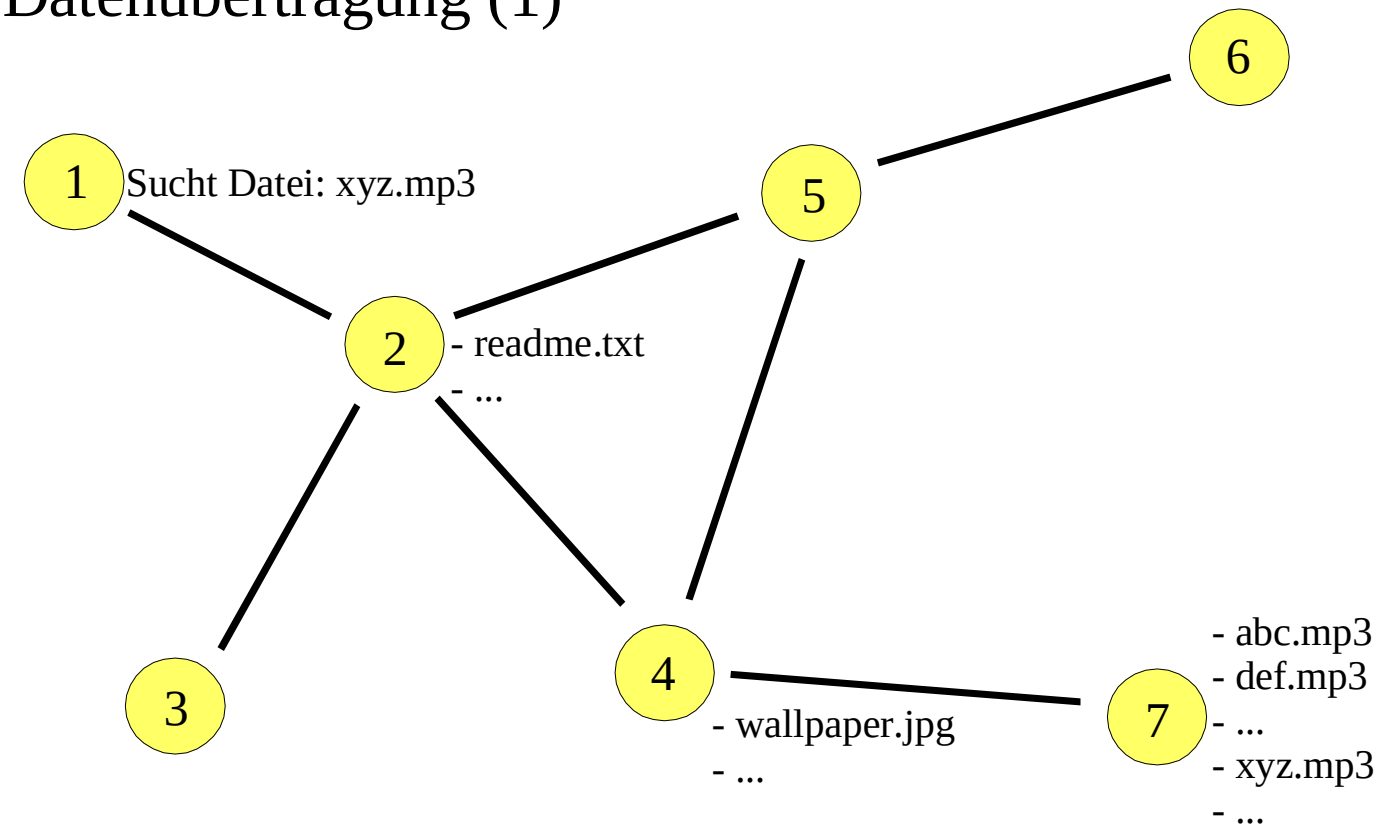
Freenet – Architektur

- Routing
  - *Steepest Ascent Hill Climbing Search*



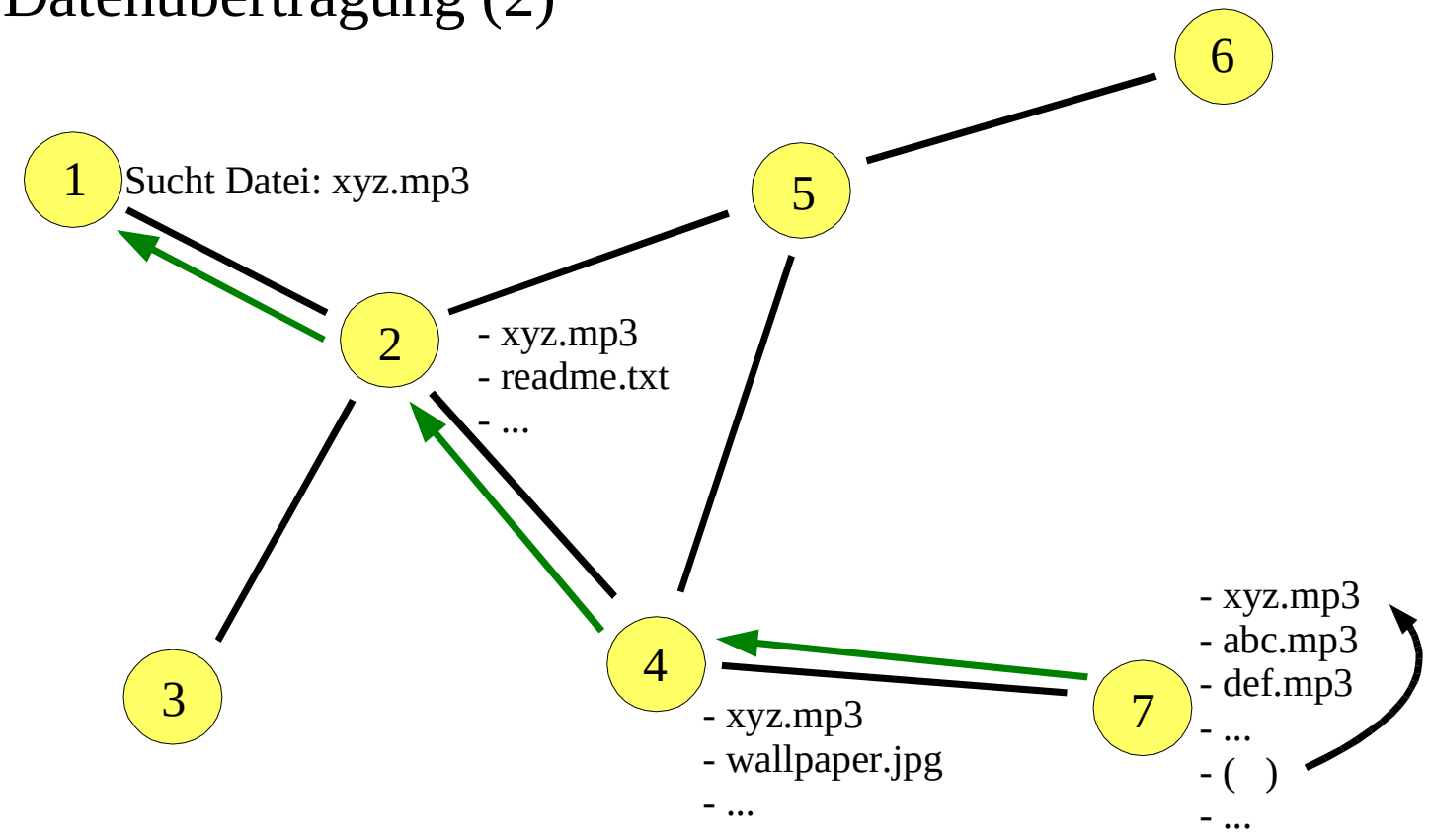
Freenet – Architektur

- Routing
  - Datenübertragung (1)



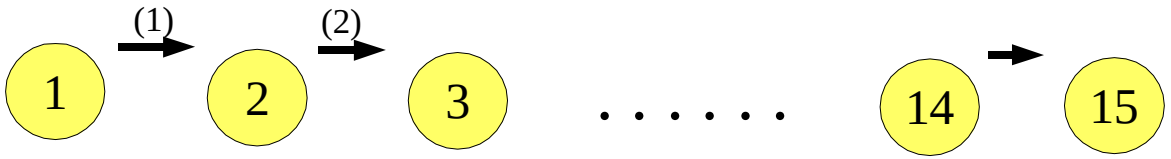
Freenet – Architektur

- Routing
  - Datenübertragung (2)



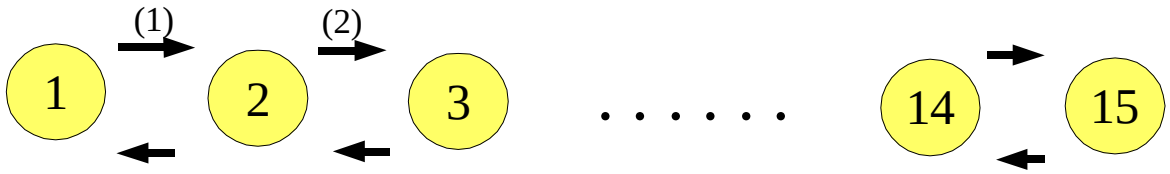
Freenet – Architektur

- Daten einbringen
  - Explizit einfügen
  - Keys erzeugen



Freenet – Architektur

- Neue Knoten
  - *New Node Announcement*
  - Keyspace aushandeln



Freenet – Architektur

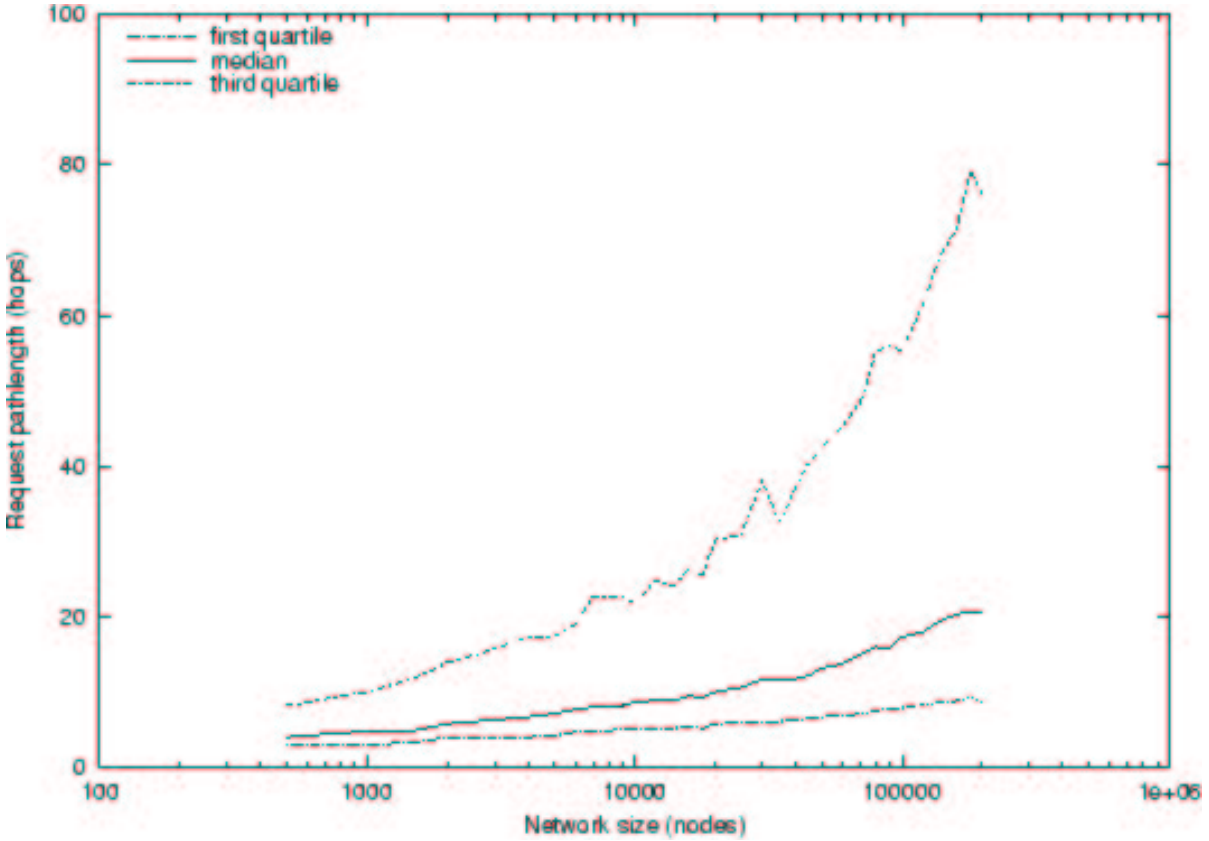
- Knoten trainieren
  - Viele Dateien einbringen
    - Routingtabellen (eigene und Nachbarknoten) werden erweitert
    - Auf Dauer erhält Knoten mehr Suchanfragen
  - Erfolgreiche Suchanfragen
    - Neue Knoten kennenlernen

Freenet – Architektur

- Speicherplatzverwaltung
  - *File-storage System*
    - ➔ Problem bei Ungleichheit Datendurchsatz/Speicherplatz
  - LRA – Least Recently Accessed
  - Populäre Daten fördern

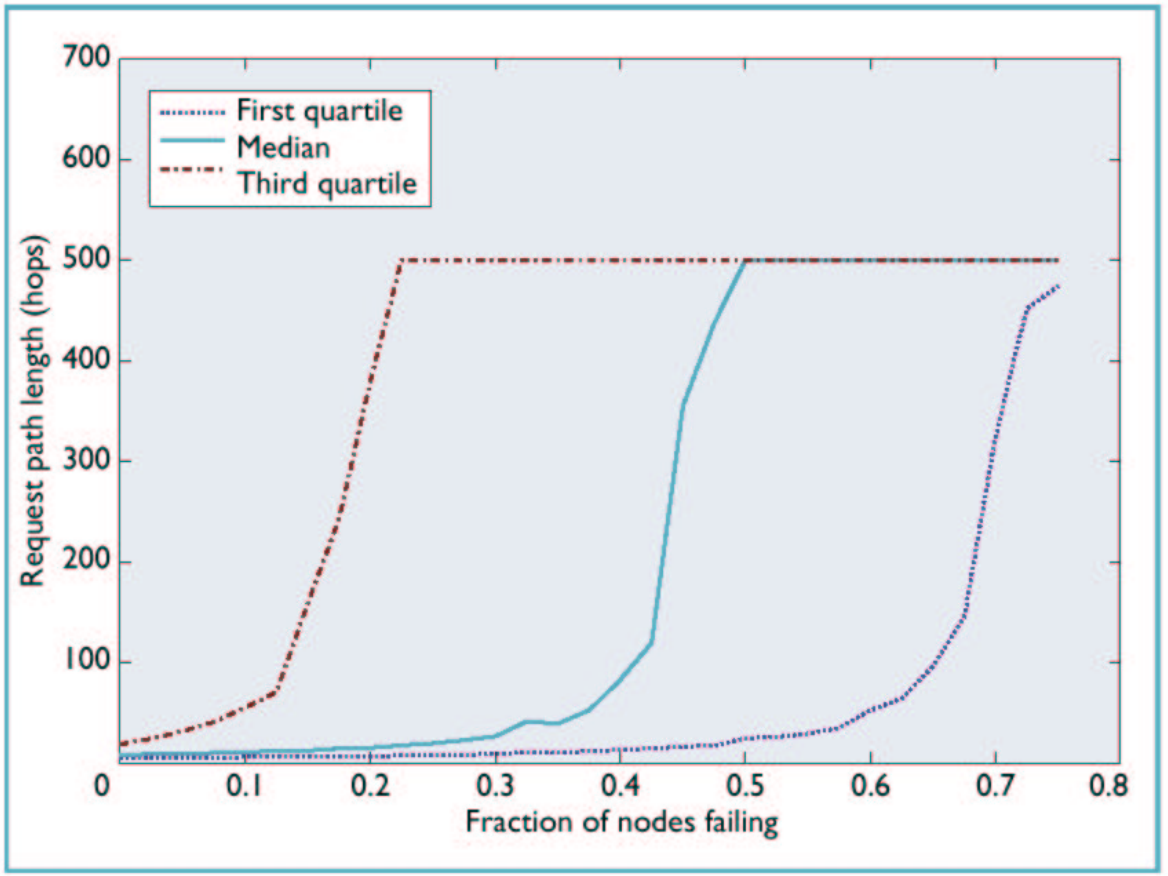
Freenet – Analyse

- Performance



Freenet – Analyse

- Fehlertoleranz



Freenet – Analyse

- Angriffe
  - Knoten löschen
  - Knoten 'flooden'

Freenet

- Zusammenfassung
  - Absolut Anonym
  - Schwachstellen?
  - Komplex
  - Suchmaschine fehlt