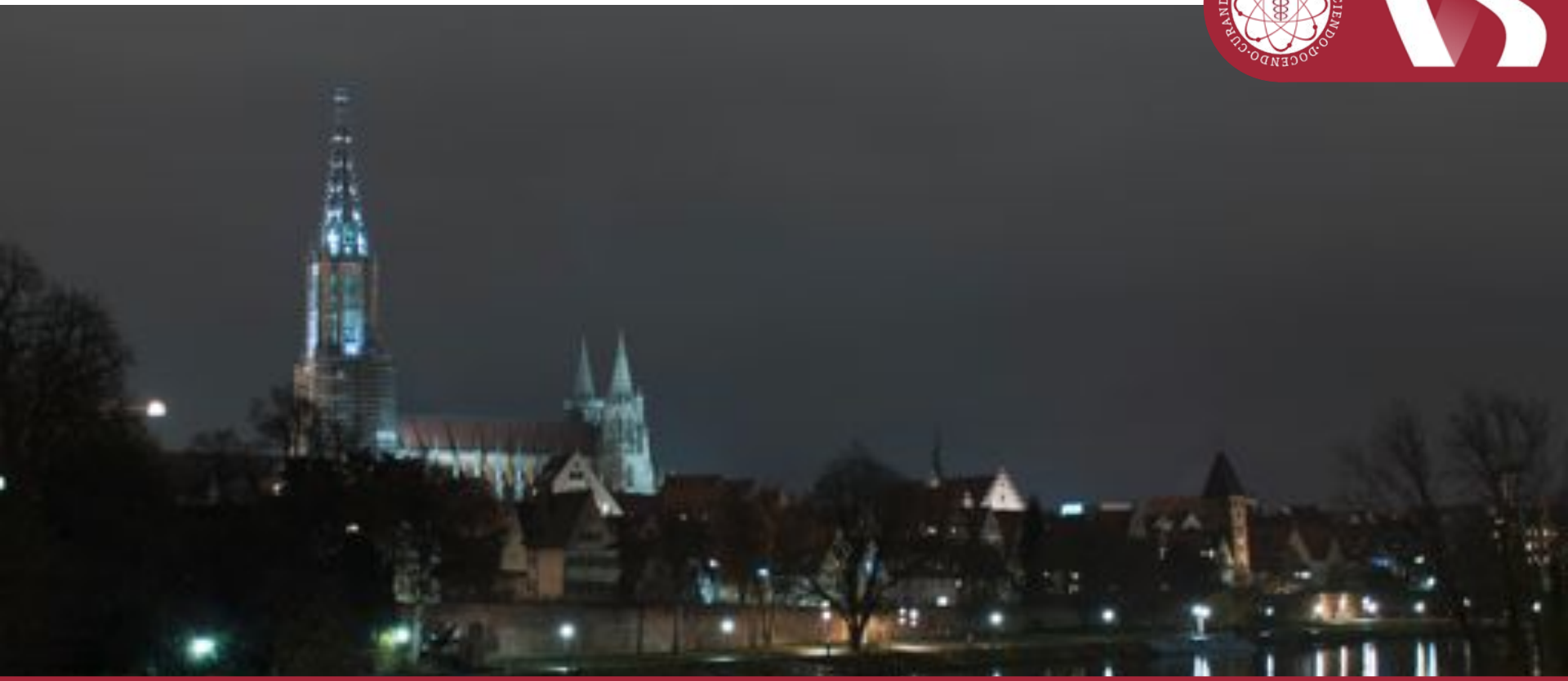


David Mödinger | 02.03.2017 | Fachgruppentreffen Betriebssysteme

PriCloud

and the Institute of Distributed Systems of Ulm University

The Institute of Distributed Systems

Research Interests and Strength

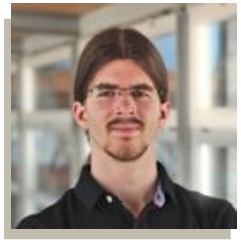
- Security and Privacy
  - automotive systems, CPS, IoT
  - privacy engineering, PETs
  - blockchain architectures
  - security in high-speed networks
- Distributed Graph Computing

Prof. Frank Kargl

- Dependable systems
  - SMR, consensus, deterministic scheduling
- Special-purpose middleware
  - real-time and distributed scheduling
  - anonymous communication
  - mobile sensing

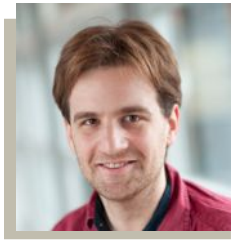
Prof. Franz J. Hauck

Baden-Württemberg Stiftung
Audi
DAIMLER
bwNET 100G+
SIEMENS
arago The Automation Experts
PRIPARE
CRISALIS SECURING CRITICAL INFRASTRUCTURES
PRESERVE preparing secure v2x communication systems
CONVERGE
SAMPL SECURE 3D PRINTING
CAR 2 CAR COMMUNICATION CONSORTIUM
ETSI World Class Standards
OptSCORE
ARTOS
Cosca
Instant-X



Henning Kopp

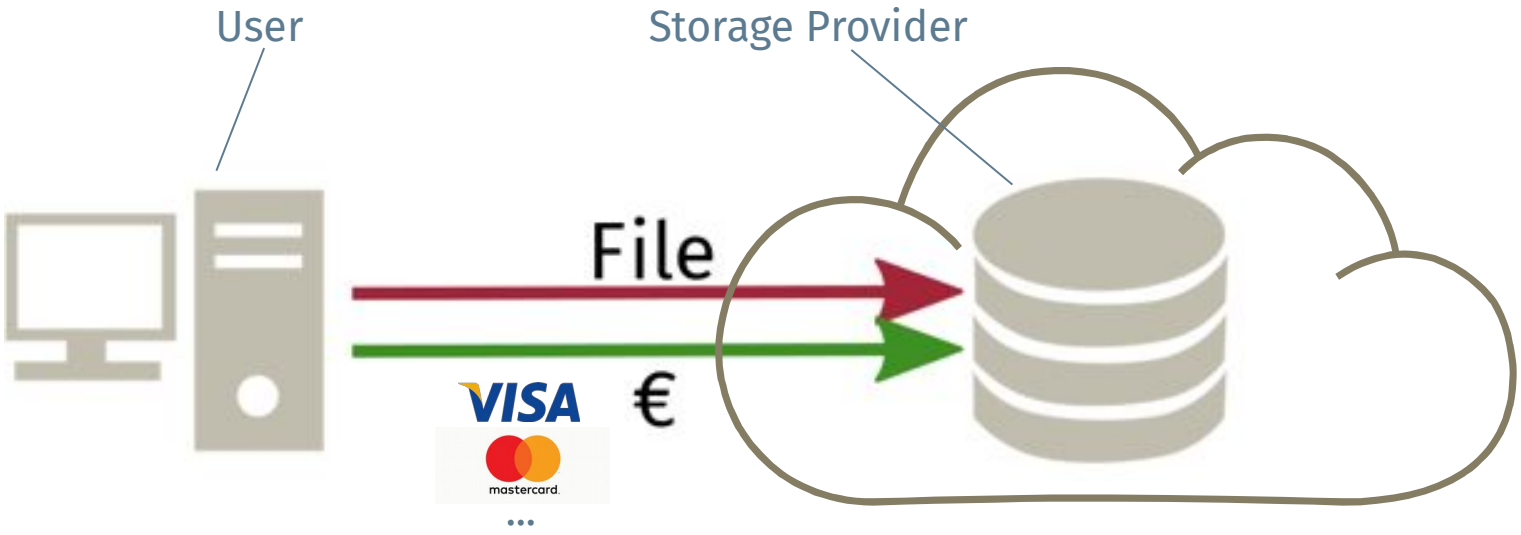
David Mödinger



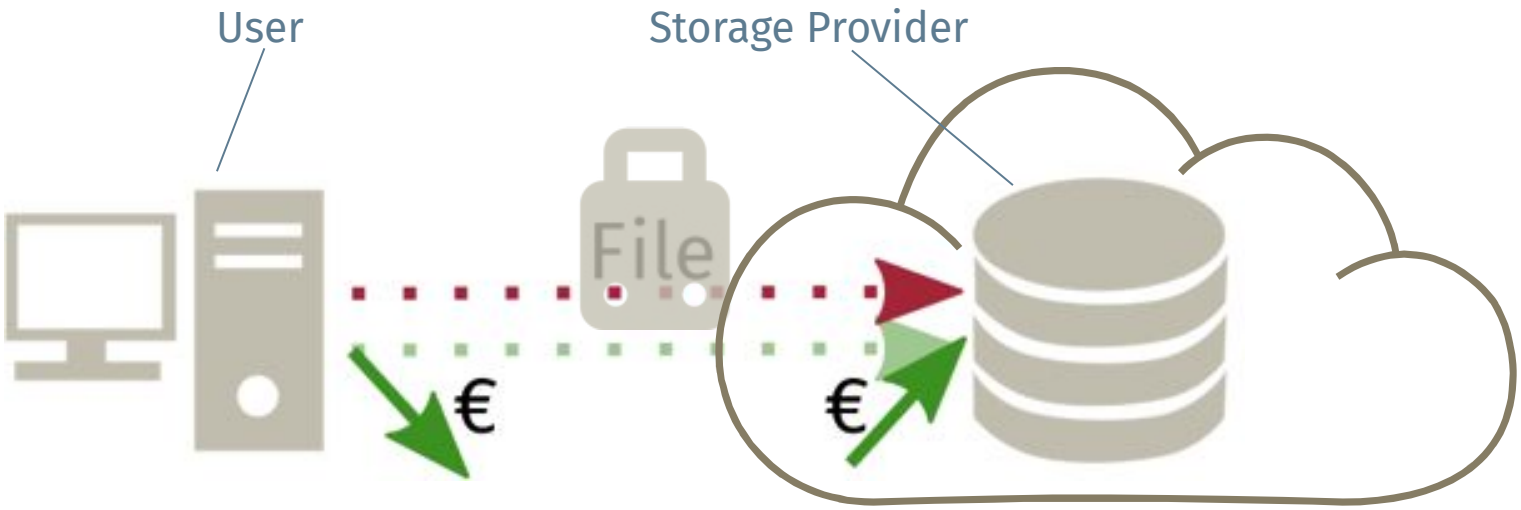
Storing Private Data

Work in Progress

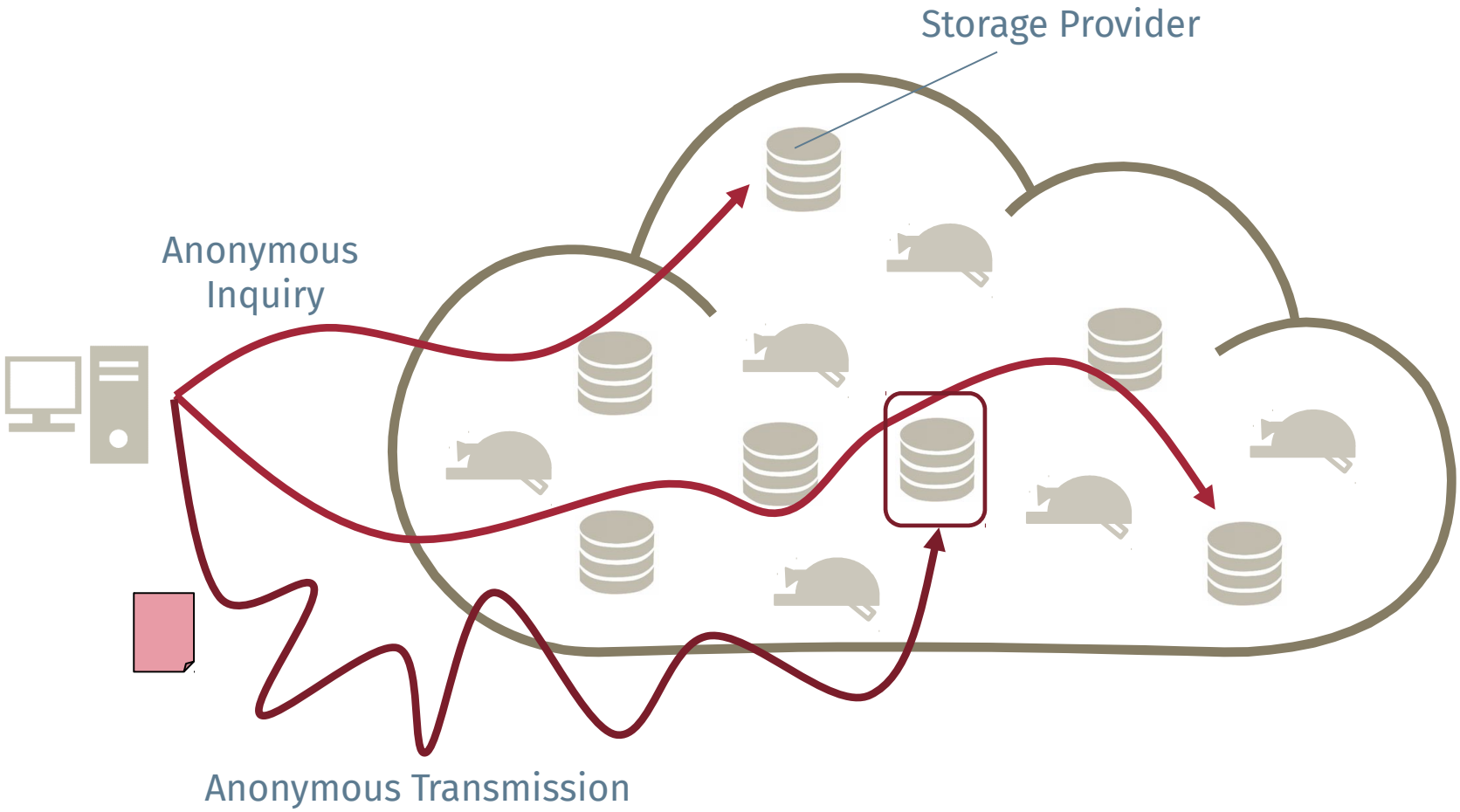
Scenario: Current Storage Solutions



Scenario: Improved Privacy

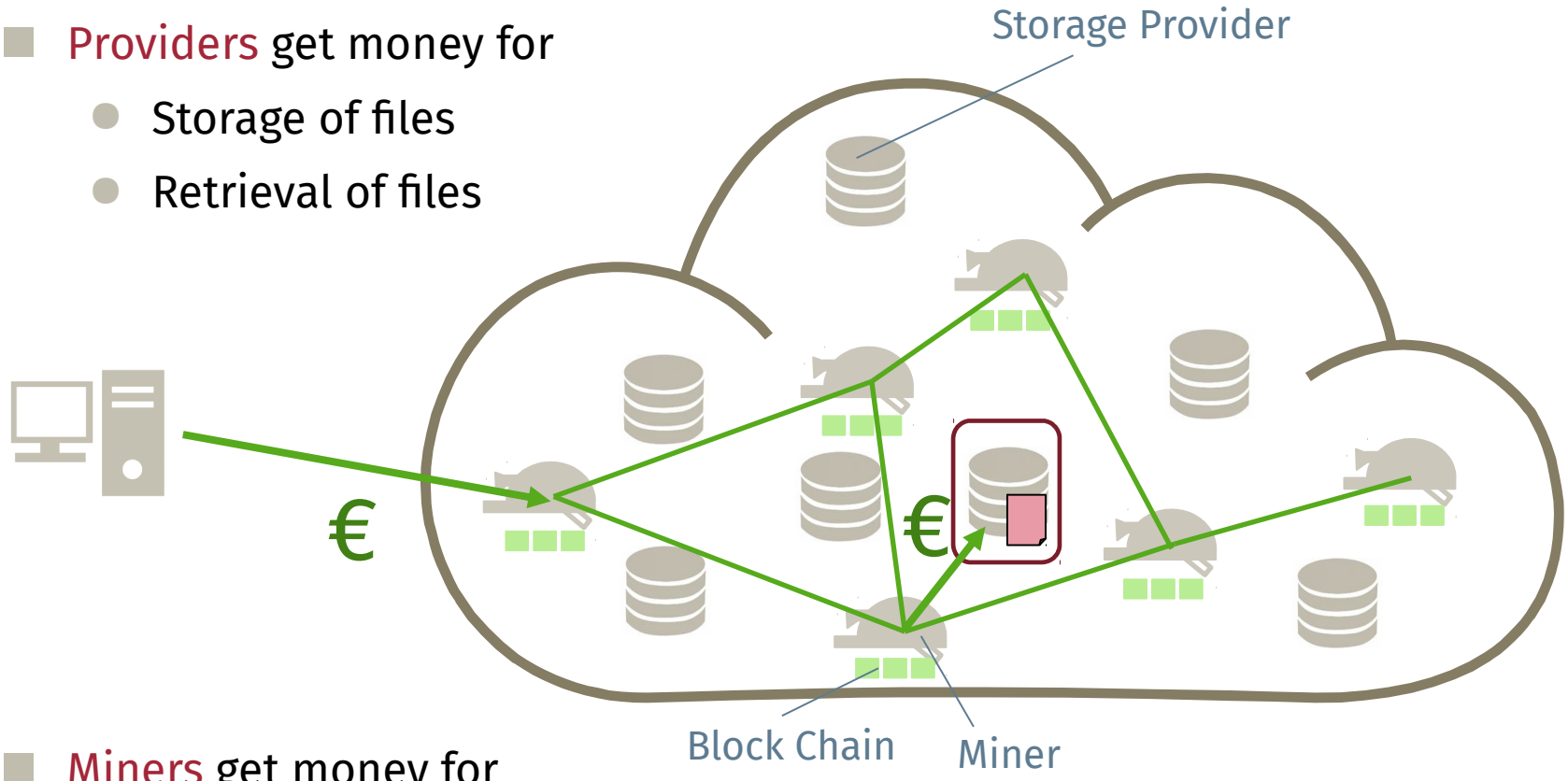


Funcionality



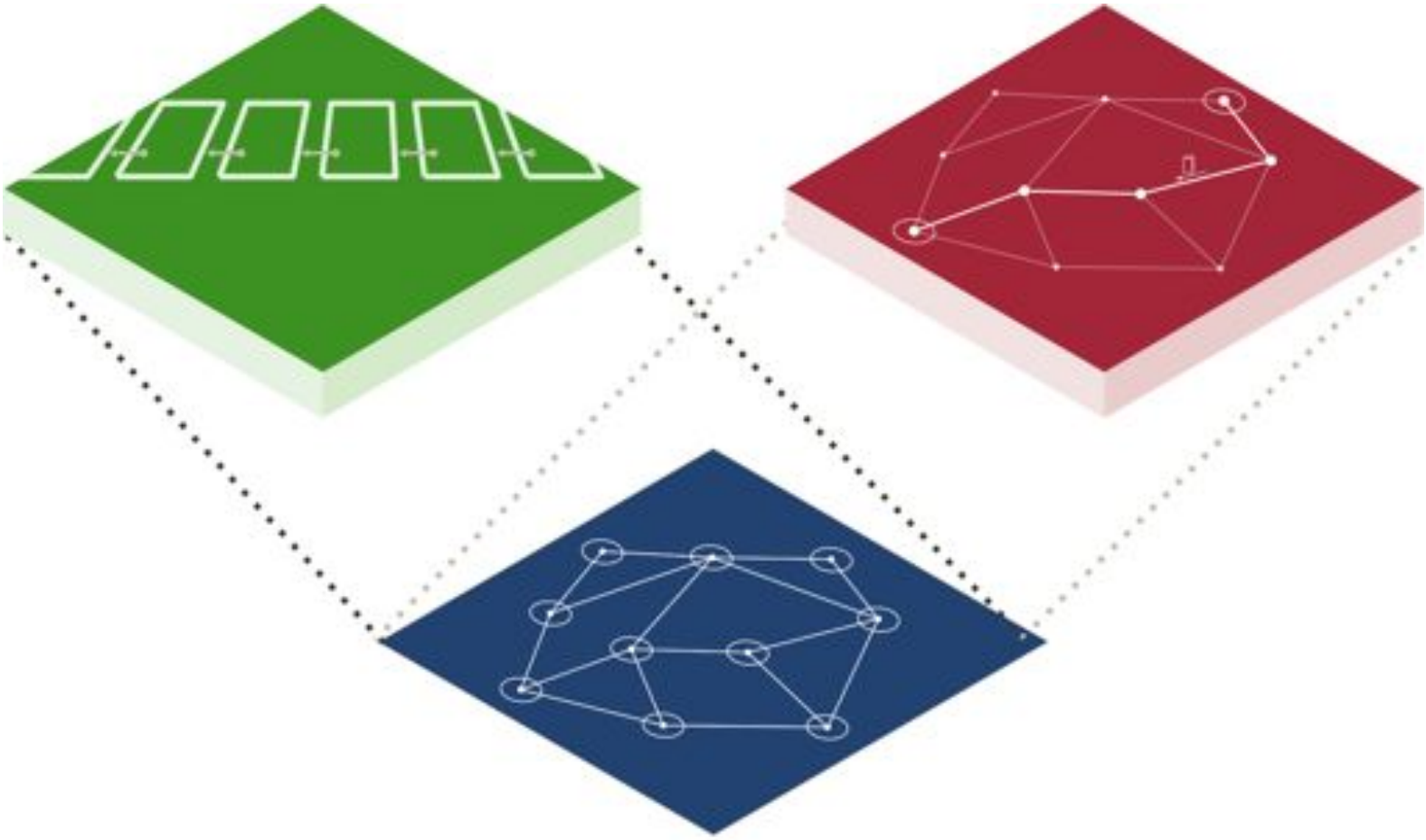
Payments

- Providers get money for
  - Storage of files
  - Retrieval of files



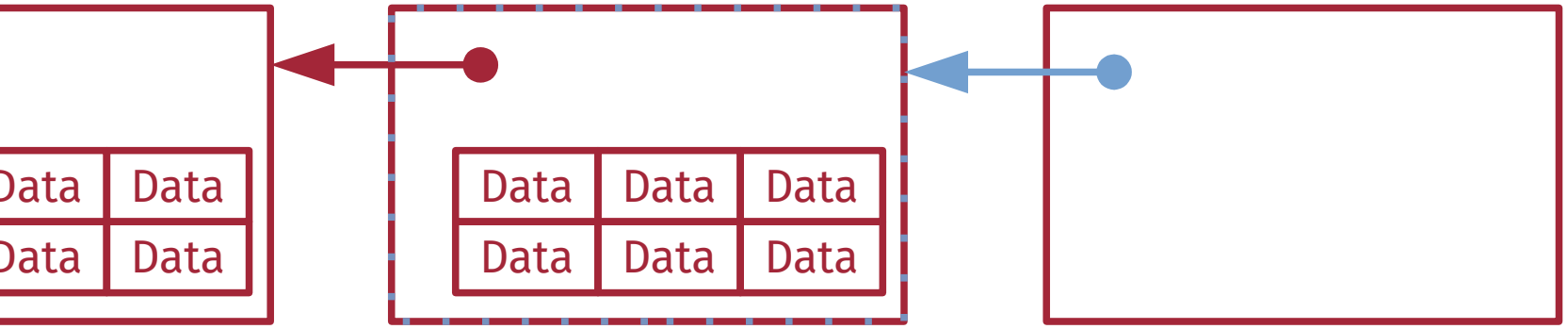
- Miners get money for
  - validating transactions
  - mining of blocks

Structure

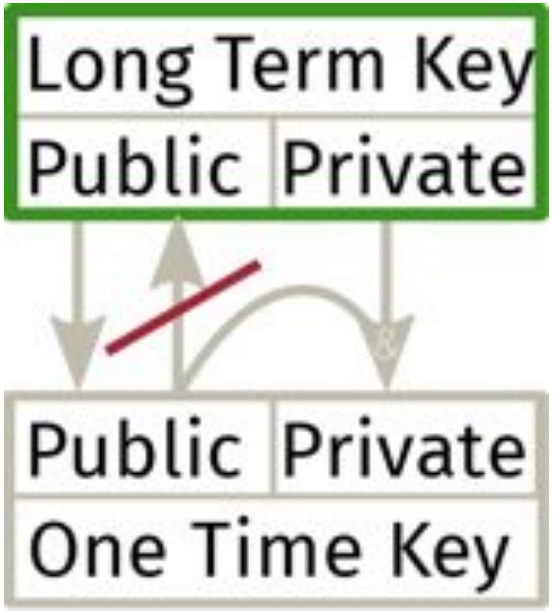


Area of Research: Blockchain and Applied Cryptogryphy

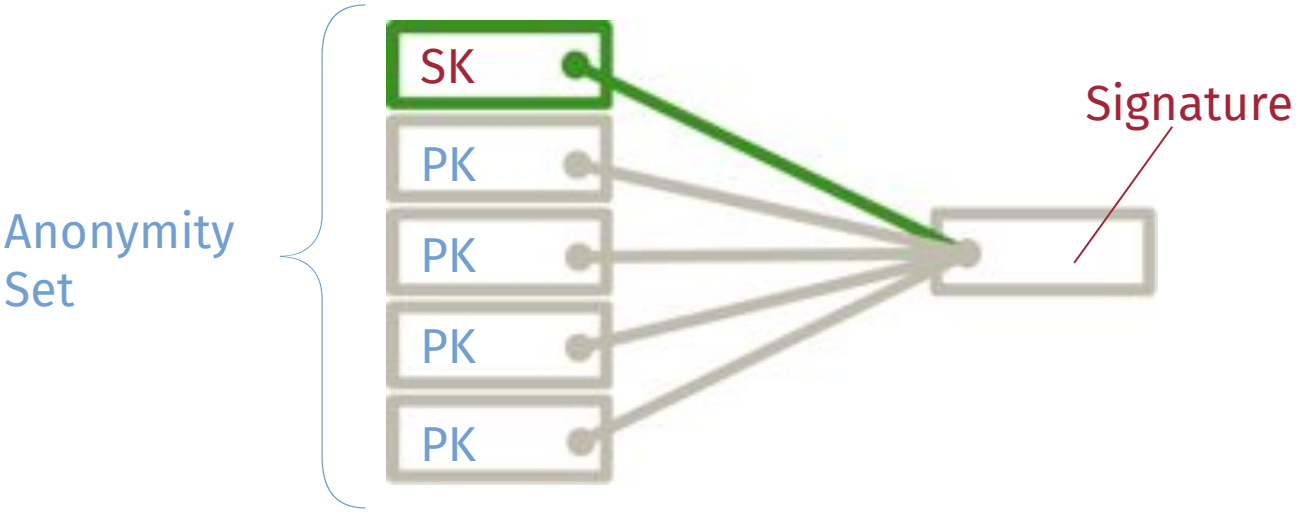
Blockchain



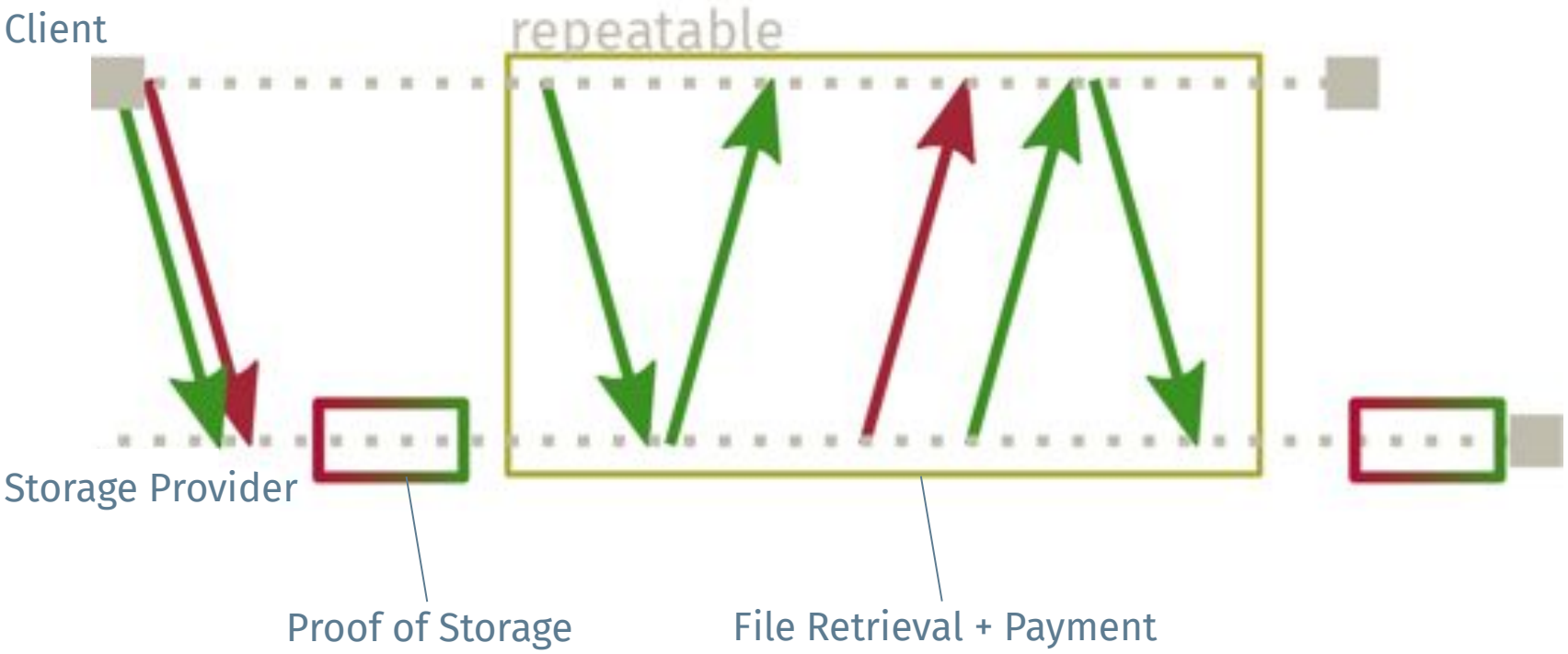
Privacy on the Blockchain: One Time Keys



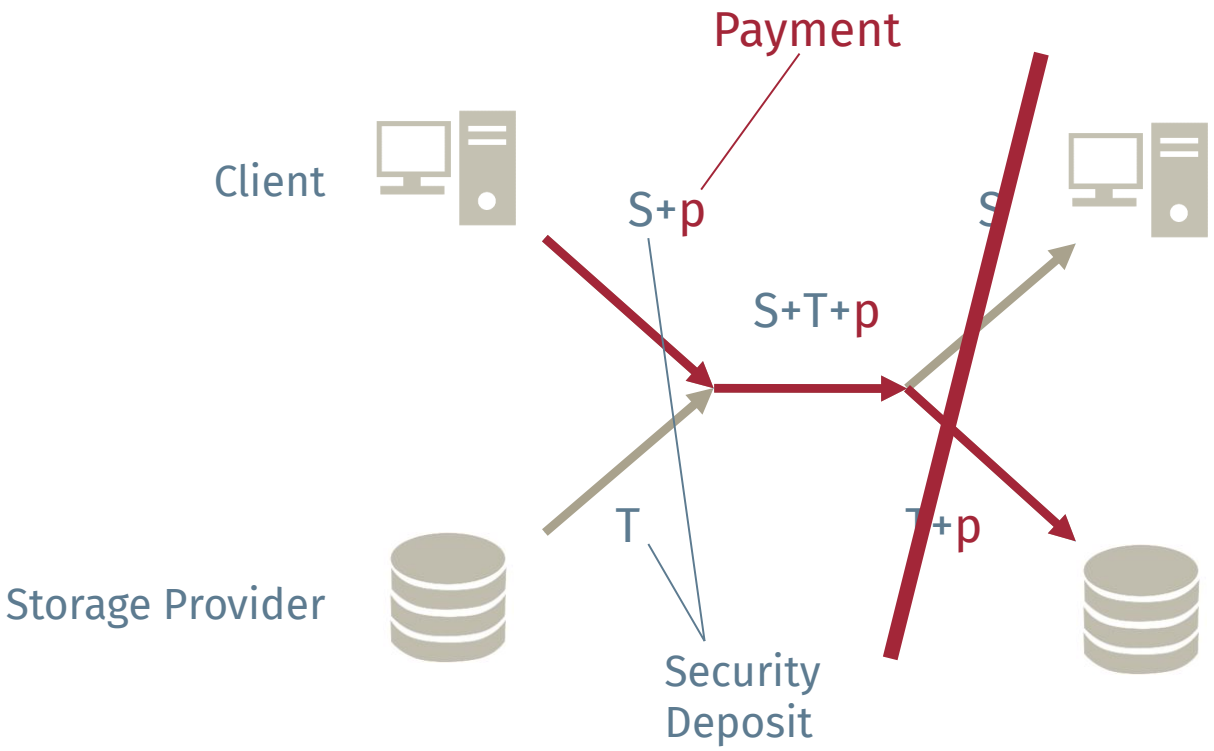
Privacy on the Blockchain: Linkable Ring Signatures



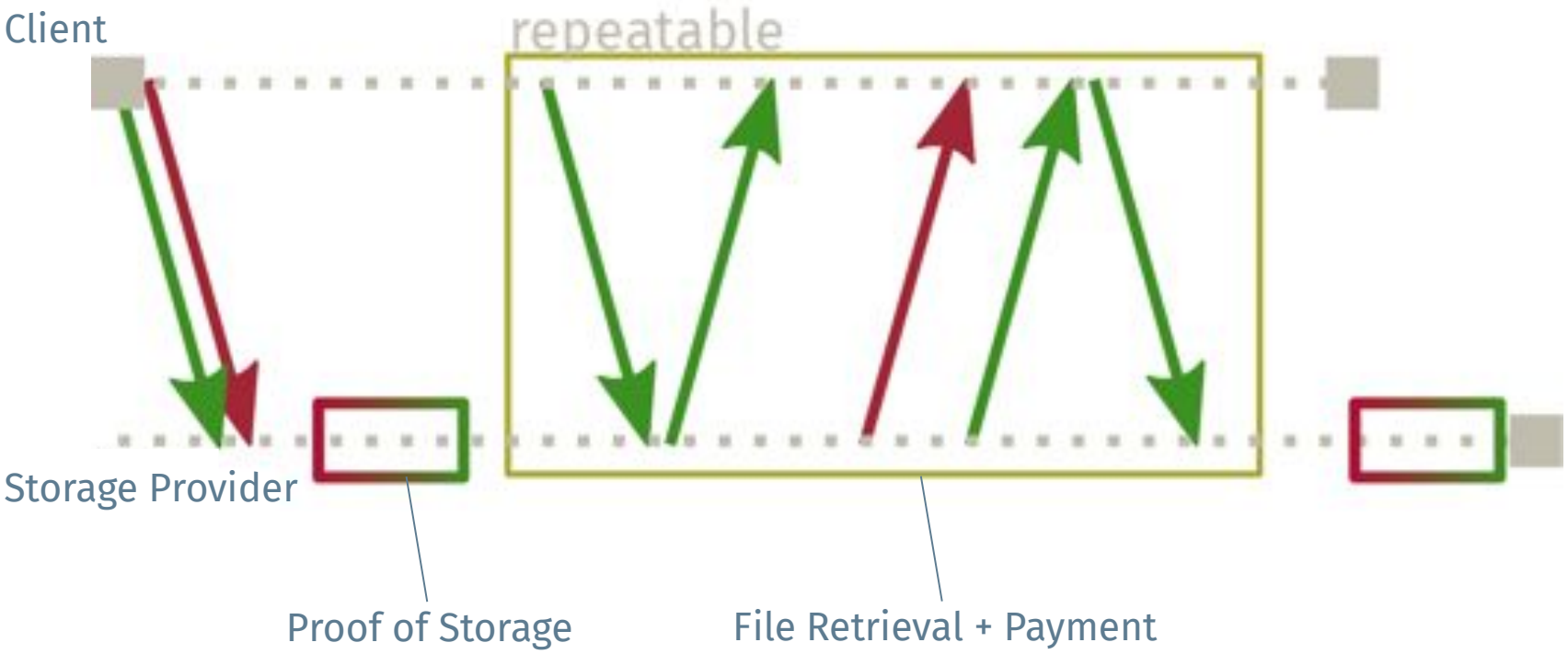
Blockchain: Smart Contracts



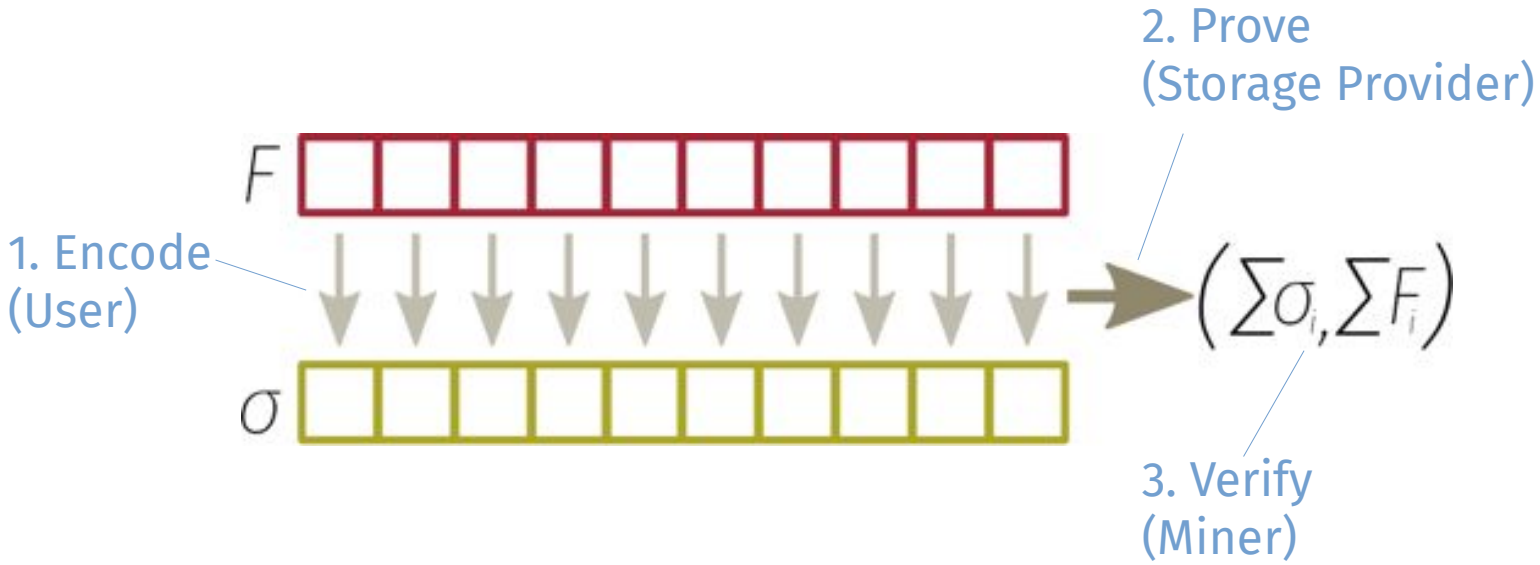
Blockchain: Economic Security



Blockchain: Smart Contracts



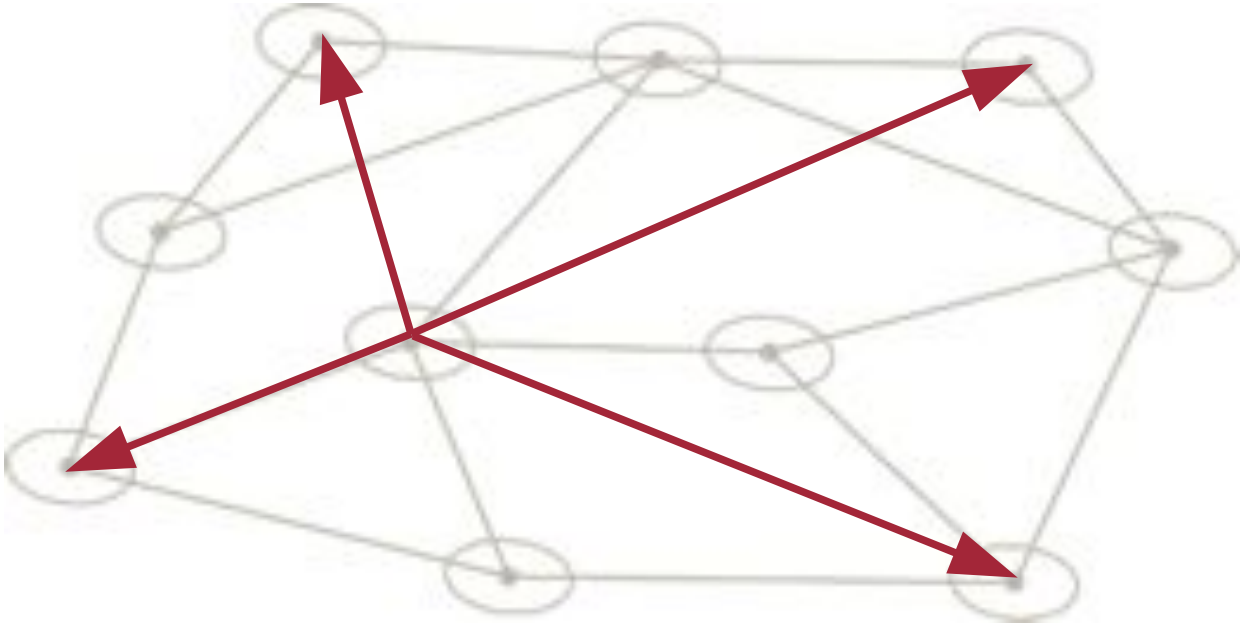
Proofs of Storage



Proofs of Storage: Efficiency of Encoding

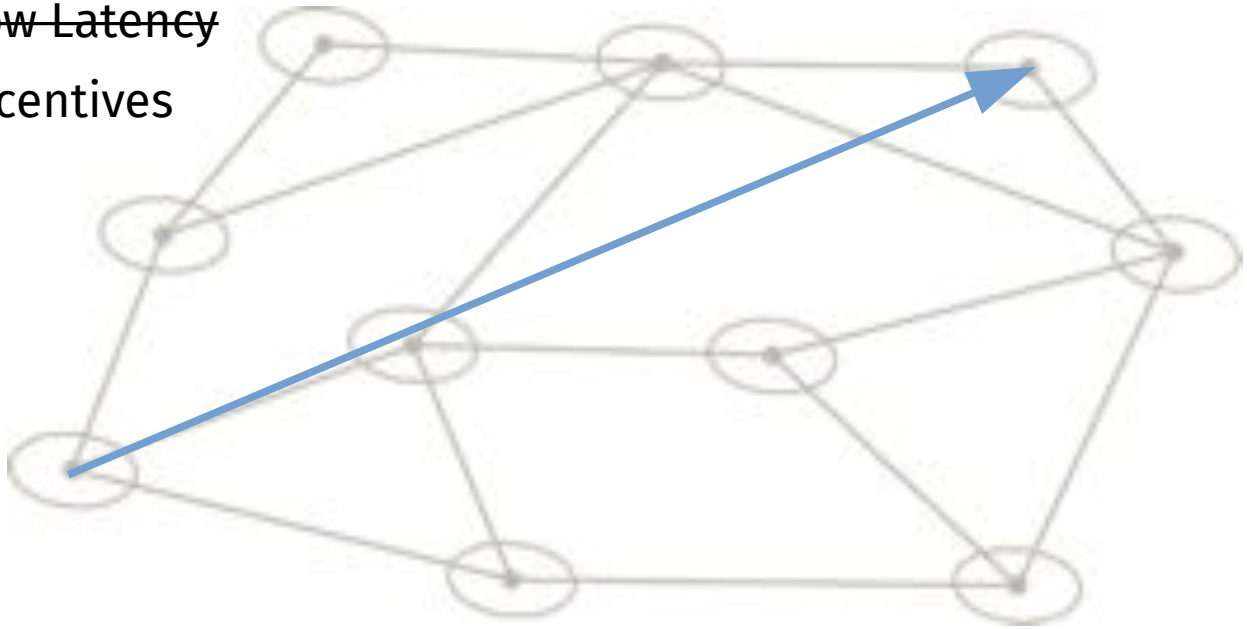
Area of Research: Peer-to-Peer Networking

Network: Anonymous Information Dissemination

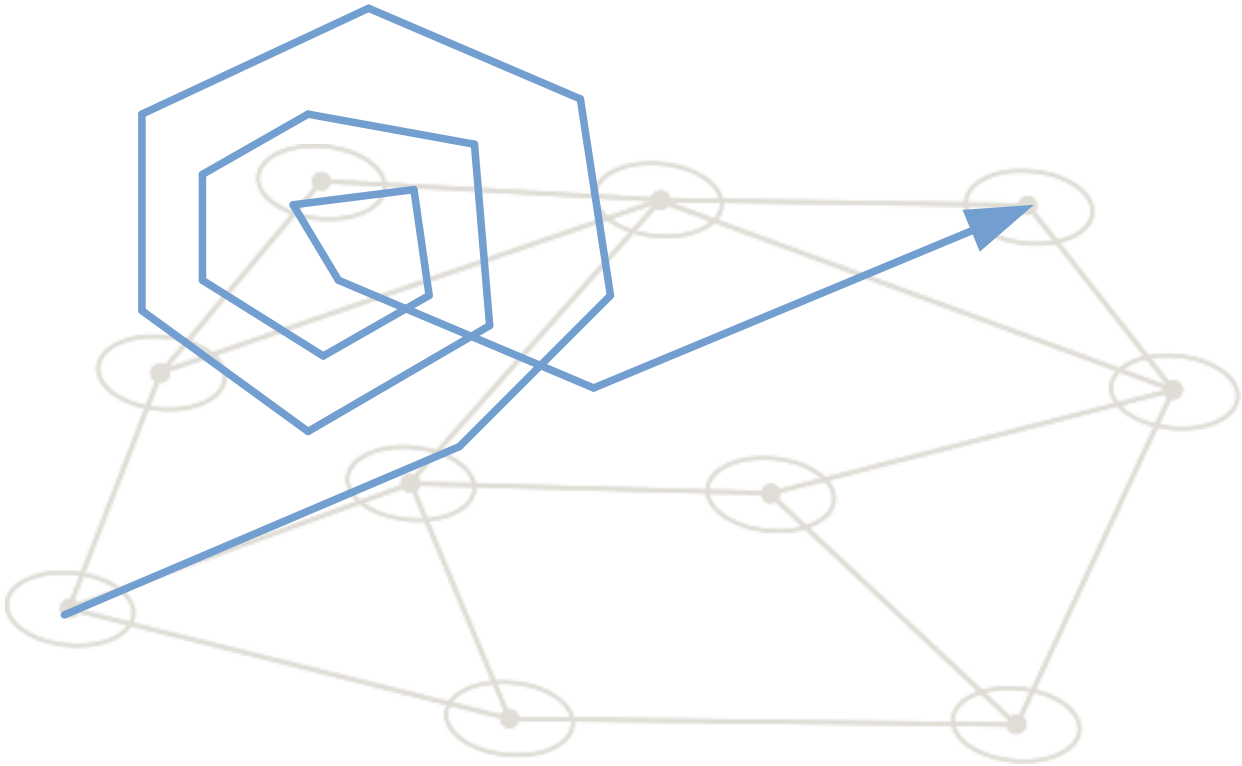


Network: Anonymous Data Transmission

- TOR not enough!
  - Attack Model
  - ~~Low Latency~~
  - Incentives



Network: Efficiency



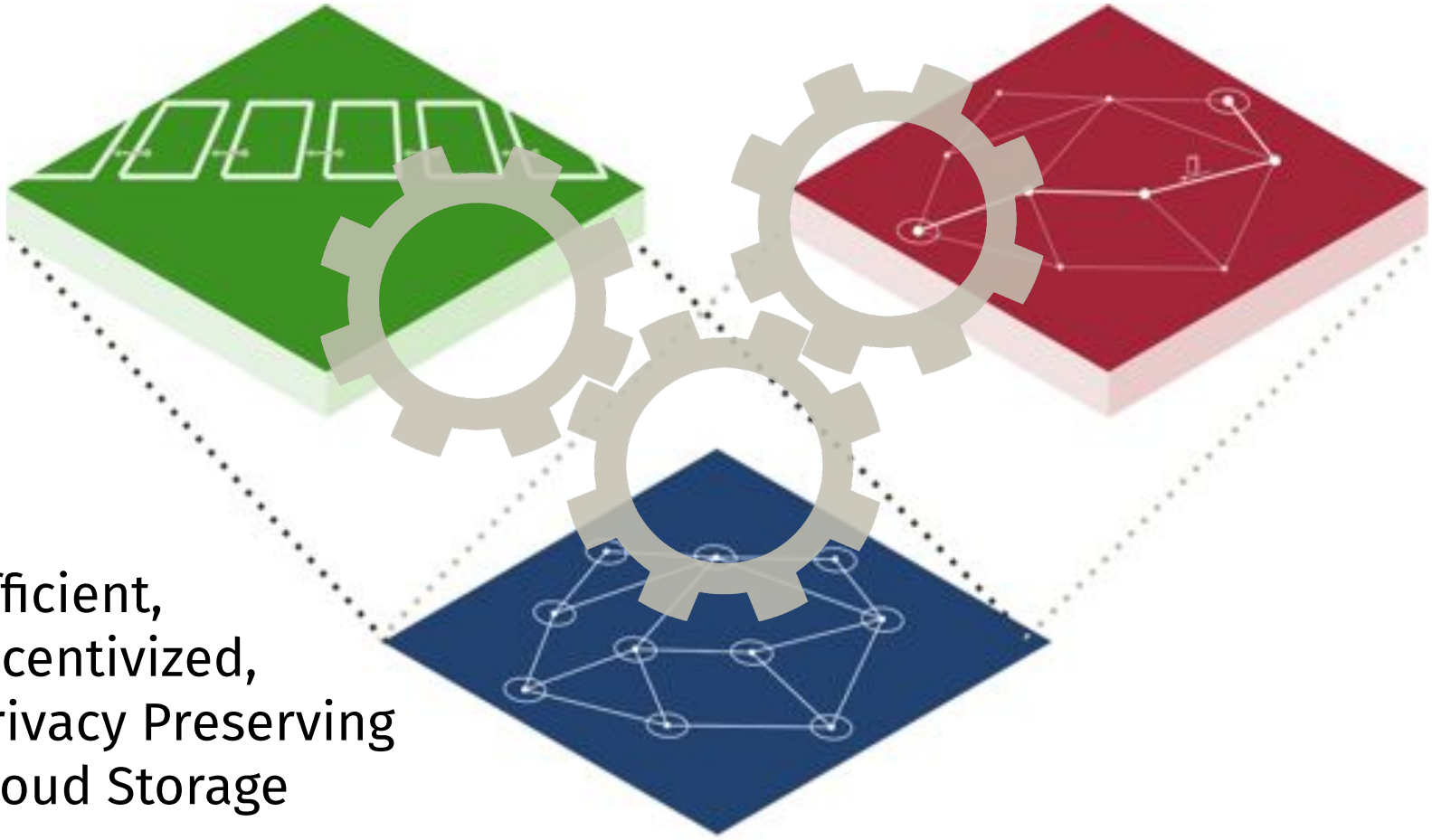
Incentivizing Participation

- Providers have an incentive
- Miners have an incentive
- Users get value

But why would they participate in the anonymity net?

Summary

Improvements by Coupling



Efficient,
Incentivized,
Privacy Preserving
Cloud Storage

Questions