Lehrstuhl für Software und Systems Engineering
Fakultät für Informatik
Technische Universität München

Decentralized Inverse Transparency With Blockchain

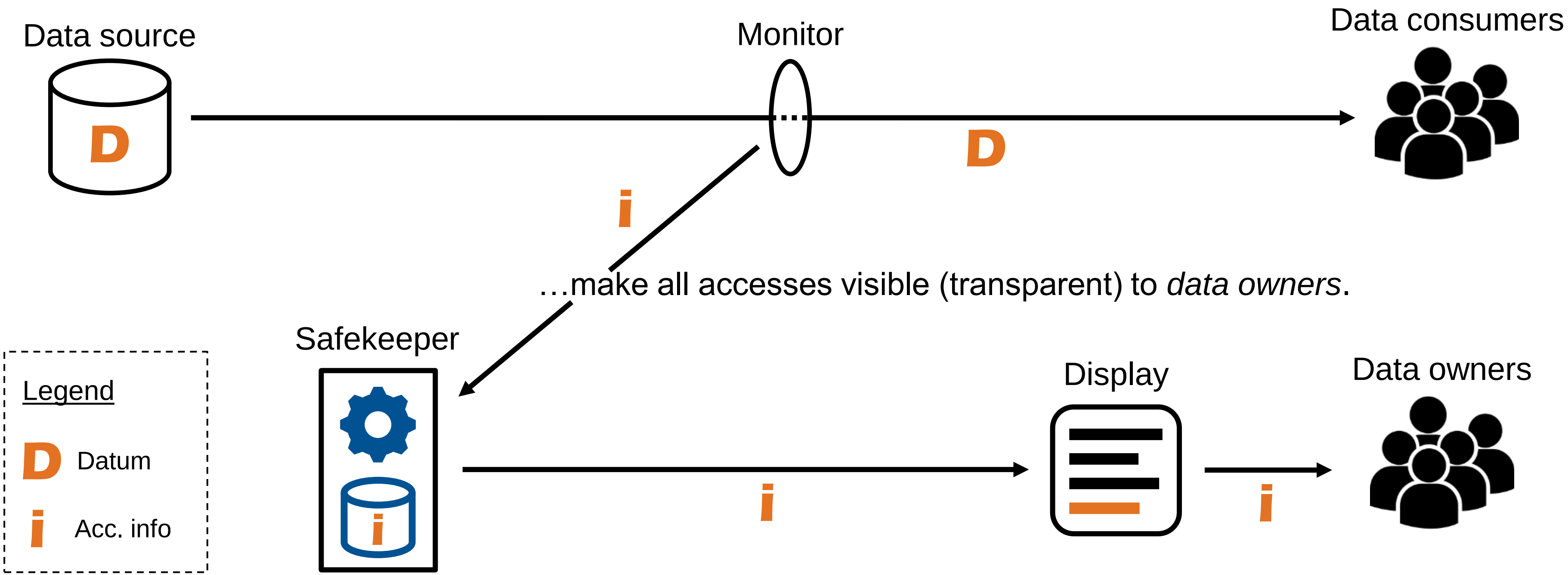
TUM Blockchain Salon

Valentin Zieglmeier

11th May 2023

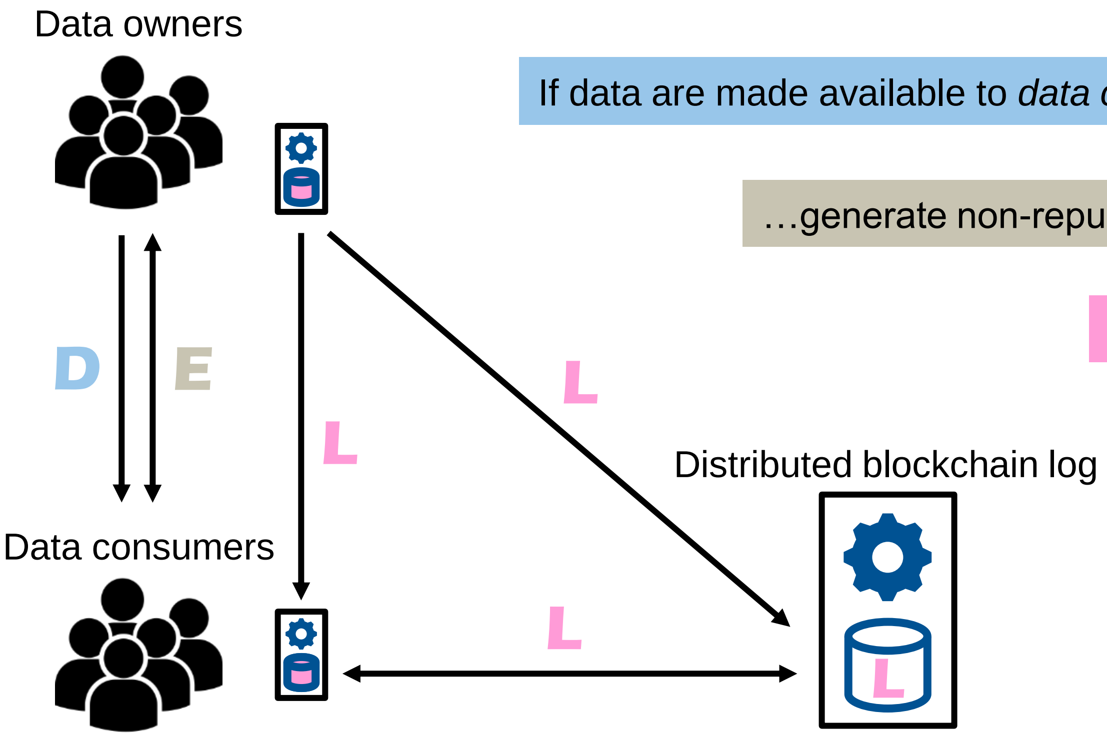
Use case: Secure usage logging

If data are made available to *data consumers*…



…make all accesses visible (transparent) to *data owners*.

Decentralized inverse transparency



If data are made available to *data consumers* directly…

…generate non-repudiable evidence of the exchange…

…to record the usage for *data owners*.

<u>Legend</u>

D Datum

E Evidence

L Access log

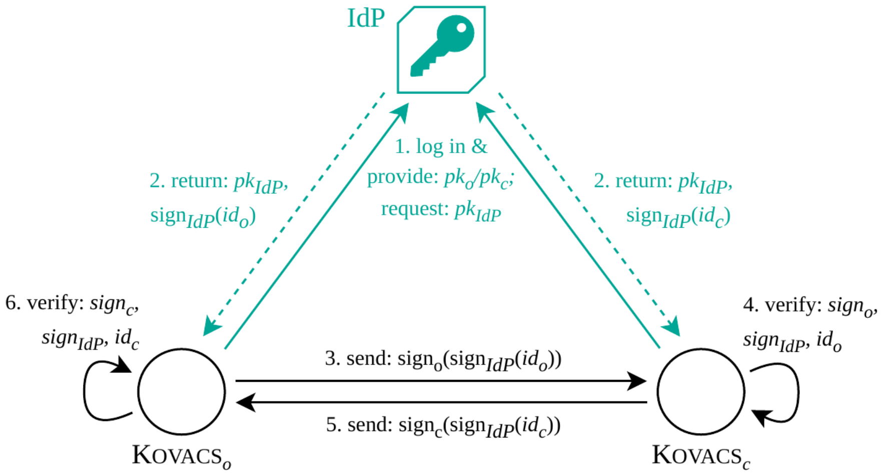
Motivation: Decentralized inverse transparency

- **Problem:** Having to trust any third party means manipulation is always a possibility
- **Blockchain as supporting technology:**
  - Advantages: immutable and decentralized ⇒ forward security, no trusted third party
  - Drawback: Not correctible, no arbiter
- **Solution:** KOVACS data exchange and usage logging system
  - Non-repudiable data exchange ⇒ accountability
  - Decentralized and private usage logs in blockchain ⇒ proof of ownership and unlinkability
- **Impact:** KOVACS enables fully decentralized inverse transparency
  - GDPR-compliant solution
  - Independent of utilized blockchain software

Requirements: summary

- Forward security: Ensured by blockchain ✓
- Identity verification ⚠
- Non-repudiable data exchange ⚠
- GDPR compliance ⚠

Identity verification



- Needed to attribute logs to people
- Utilizes existing IdP
- Self-sovereign identities are requested once and reused for all future communications

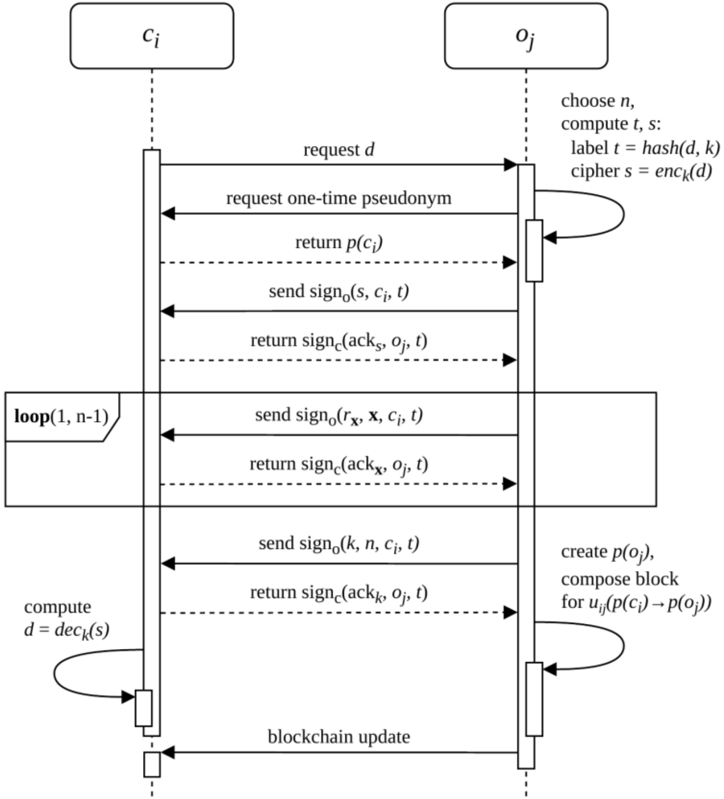
Implications:

- IdP knows of the <u>existence</u> of nodes
- IdP <u>does not</u> know who communicates with whom

See:

- *Mühle, A. et al. 2018. "A survey on essential components of a self-sovereign identity". Computer Science Review*
- *Preukschat, A. and Reed, D. 2021. "Self-sovereign identity". Manning.*

New-usage protocol

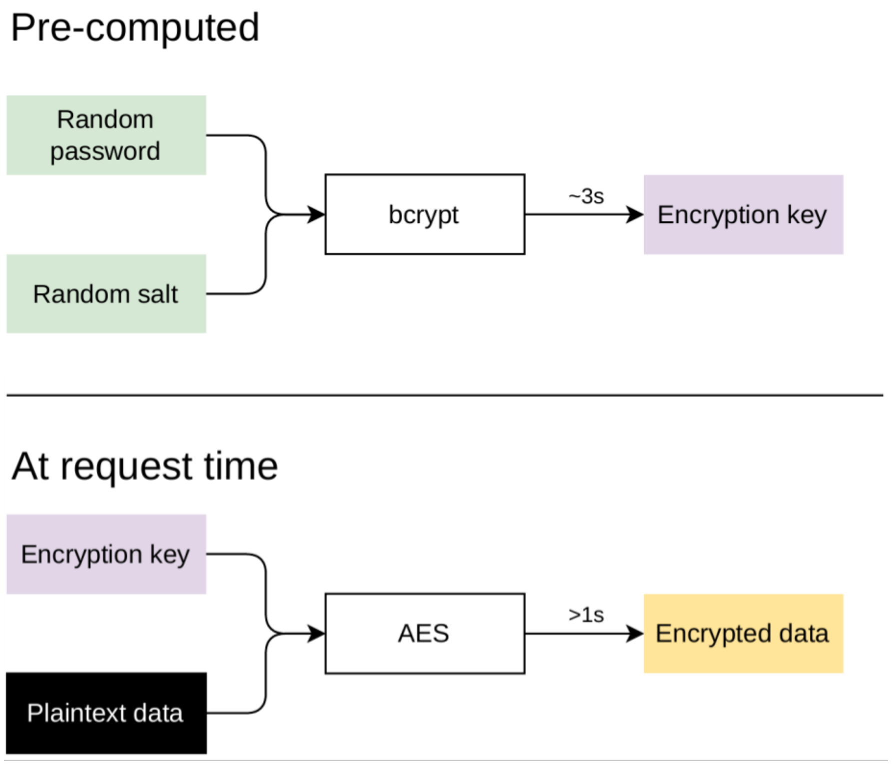


- **Start:** o(wner) holds datum (d), c(onsumer) holds nothing
- **Perform new-usage protocol**
  - core: protocol by Markowitch & Roggemann
  - adapted for blockchain context:
    - c and o generate individual pseudonym
    - o creates usage log and sends blockchain update
- **Result:**
  - both hold non-repudiation evidence (of origin / receipt)
  - usage is logged

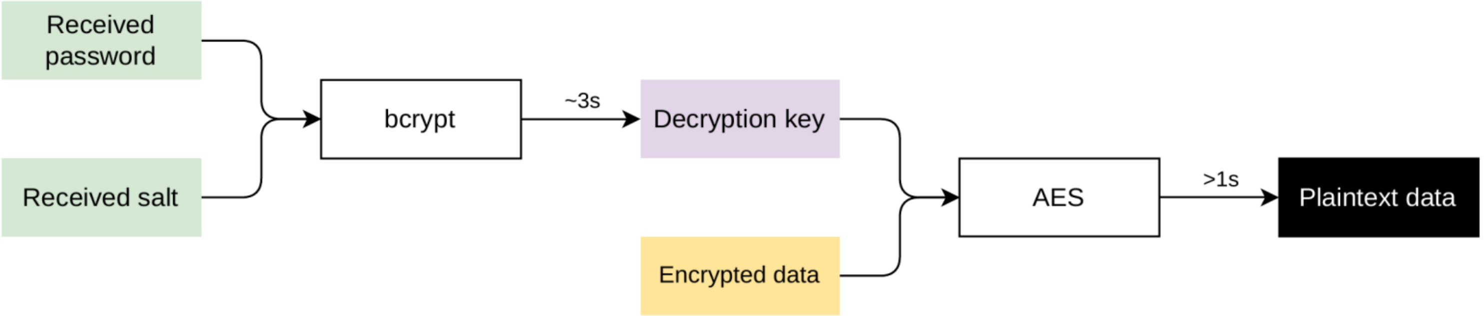
See:

- *Markowitch, O. & Roggemann, Y. 1999. "Probabilistic non-repudiation without trusted third party." Proc. 2nd Conference on Security in Communication Networks, pp. 25–36*
- *Kremer, S. et al. 2002. "An intensive survey of fair non-repudiation protocols." Computer Comm. 25, 17.*

Time-asymmetric encryption



Time-asymmetric decryption



See:

- *Kelsey, J. et al. 1998. "Secure applications of low-entropy keys". Proceedings of the 1st International Workshop on Information Security*
- *Provos N. and Mazieres D. 1999. "A future-adaptable password scheme". Proceedings of the FREENIX Track*
- *Dworkin M. 2007. "Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC". NIST Special Publication 800-38D*

Blockchain logs ↔ GDPR

Reduced **confidentiality**	↔	requirement to **protect** personal data	Problem
Immutability	↔	right to **erasure**	

Theory

- GDPR only applies to personally identifiable information
- Pseudonymized data are...
  - personally identifiable — if a link pseudonym ↔ real-world identity exists
  - anonymous — otherwise

⇒ Users **self-provision** pseudonyms guaranteeing **unlinkability** and **proof of ownership**

Solution

P³ pseudonym provisioning

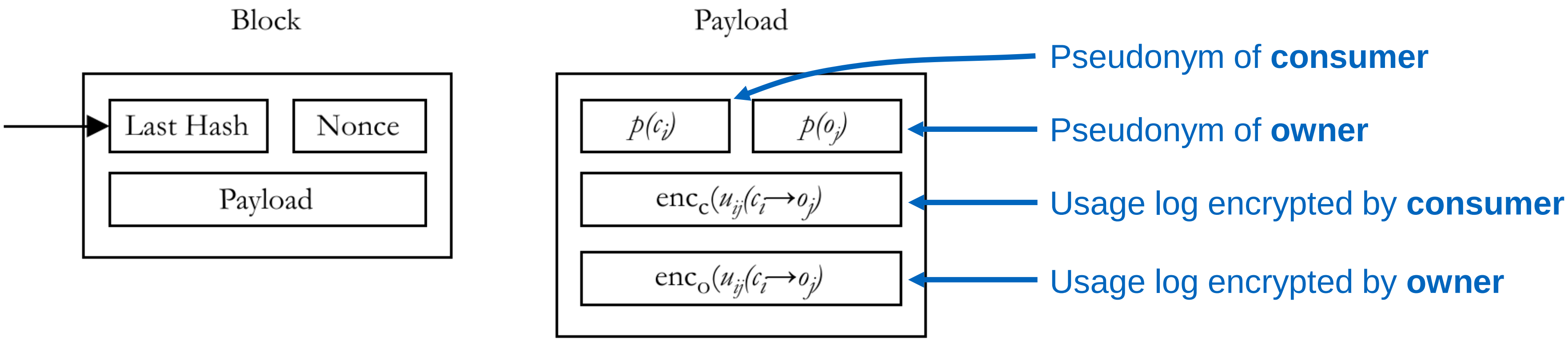
Generate RSA public/private key pair → Hash public key with BLAKE2s → Hash = one-time pseudonym

Resulting guarantees:

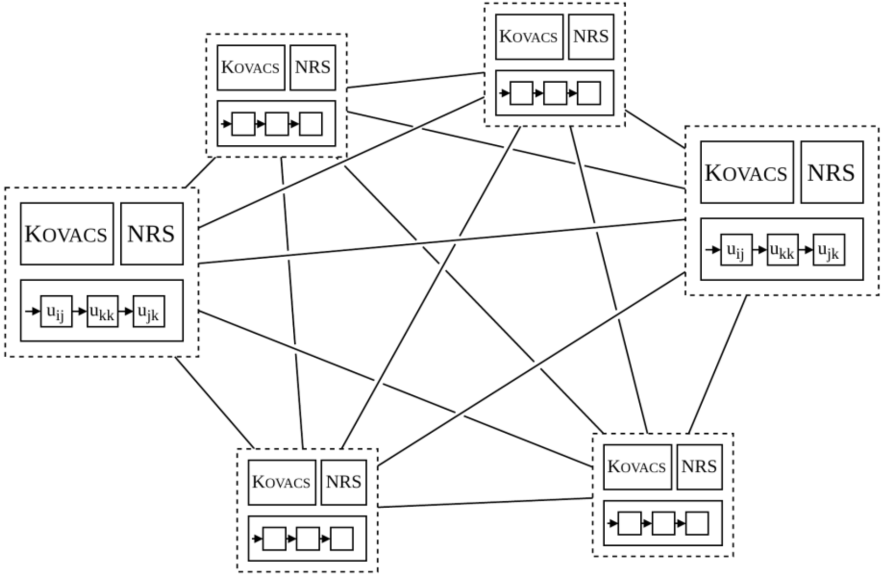
- **Unlinkability** (from BLAKE2s)
- **Proof of ownership** (via underlying key pair)

See:
- *Florian, M. et al. 2015. "Sybil-resistant pseudonymization and pseudonym change without trusted third parties." Proc.14th ACM Workshop on Privacy in the Electronic Society.*
- *Aumasson, J.-P. et al. 2013. "BLAKE2: simpler, smaller, fast as MD5." Proc. 11th International Conference on Applied Cryptography and Network Security.*
- *Applebaum, B. et al. 2017. "Low-complexity cryptographic hash functions." Proc. 8th Innovations in Theoretical Computer Science Conference.*

Block structure

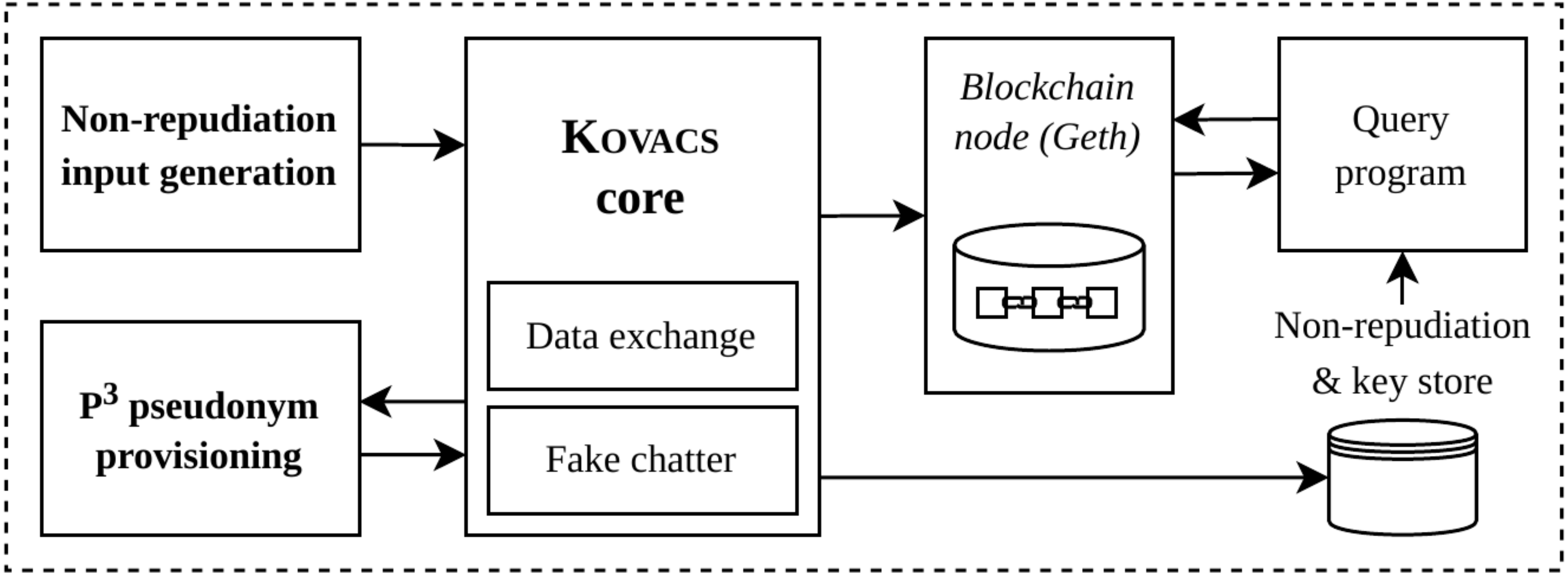


KOVACS: Deployment

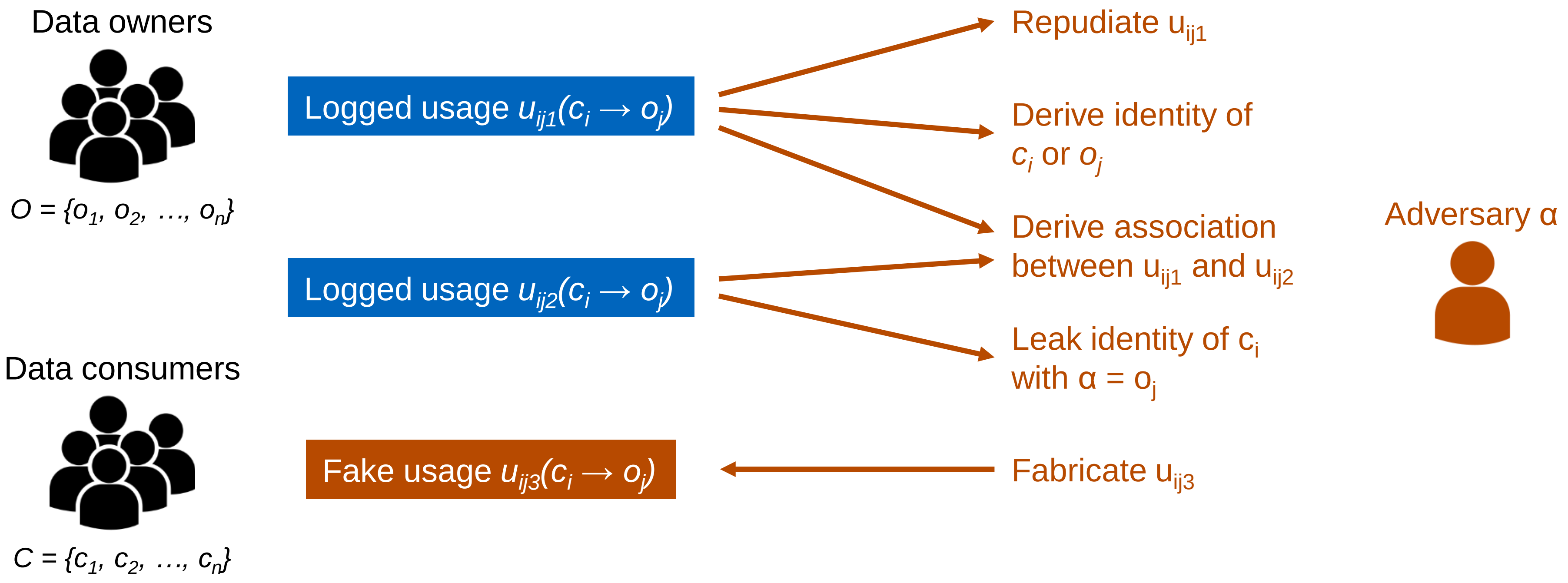


- Fully decentralized deployment
- Each node has own copy of blockchain
- Peer-to-peer data exchange
  - Blockchain updates
  - Data exchange

Summary: KOVACS system model



Analysis: Adversarial model



Analysis

Robustness against attacks

1. Repudiate usage

   ⇒ M&R hardness

   ⇒ technically infeasible

2. Derive identity

   ⇒ BLAKE2 hardness

   ⇒ technically infeasible

3. Associating usages

   ⇒ BLAKE2 + RSA hardness

   ⇒ technically infeasible

Protocol confidentiality

P2P, encrypted, no TTP

⇒ confidential

Optional hardening:

- Fake chatter (next slide)
- Random block publication

GDPR compliance

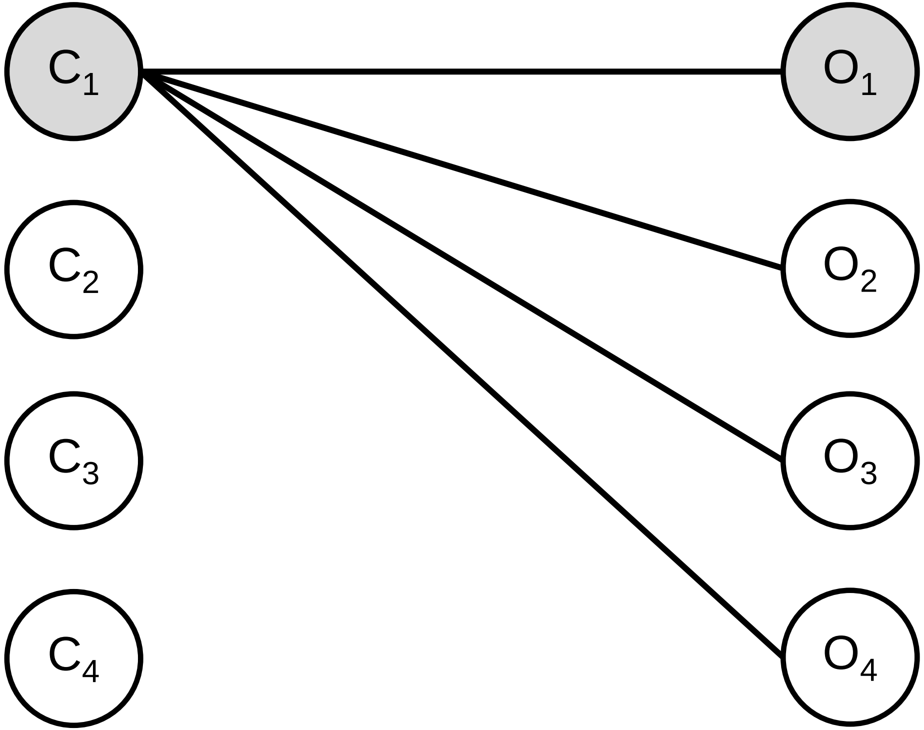
Encrypted payload

enables confidentiality ✓

Unlinkability & proof of ownership

enable right to erasure ✓

Fake chatter

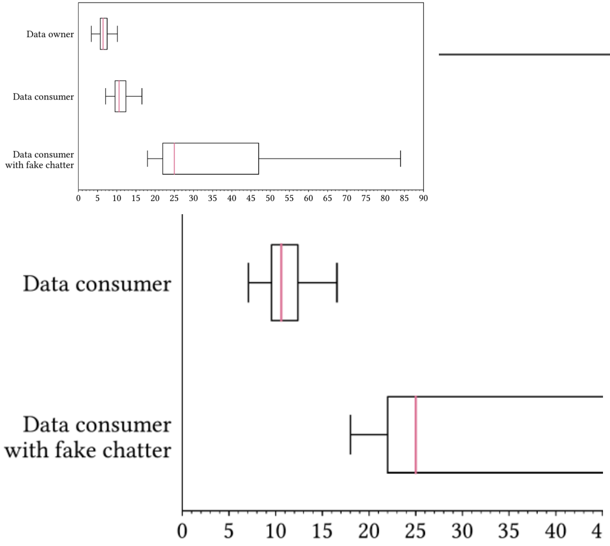


- Hide <u>relationship</u> of c to o
- Additional fake exchanges
- **Effect:** Communication hiden

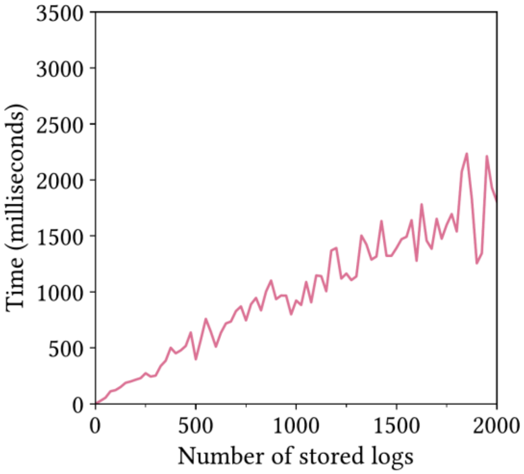
Benchmarks

Performance: exchange duration

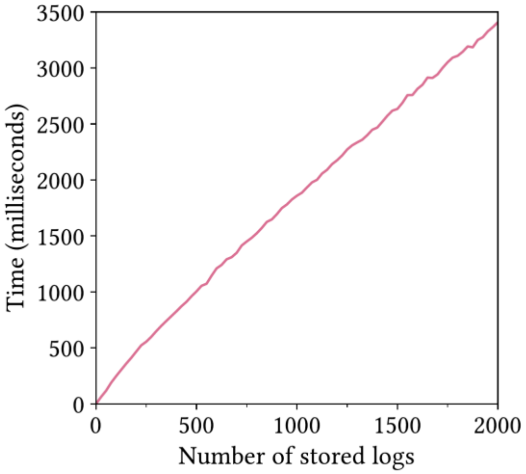
Network with 50 nodes | 2 second timeout | Ethereum (PoW)



(a) retrieve *single* log



(b) retrieve *all* logs



Summary

KOVACS enables…

- secure non-repudiable data exchanges
- fully decentralized deployment
- independence of the underlying blockchain solution

Practical implication: GDPR-compliant and scalable usage log storage on any blockchain

Academic impact: Paper published in *ACM Distributed Ledger Technologies* journal

Thank you for your attention.

Decentralized Inverse Transparency With Blockchain

Valentin Zieglmeier

Garching, 11th May 2023

Read the paper: https://mediatum.ub.tum.de/node?id=1706624