RWTH AACHEN UNIVERSITY

Decentralized Service Registry and Discovery in P2P Networks Using Blockchain Technology

ICWE 2019

Daejon, Korea
13.06.2019

Peter de Lange

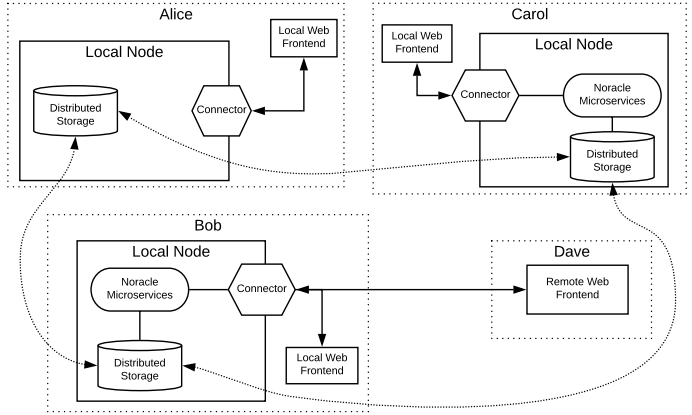
RWTH Aachen University

lange@dbis.rwth-aachen.de

Peter de Lange
RWTH Aachen University, Germany

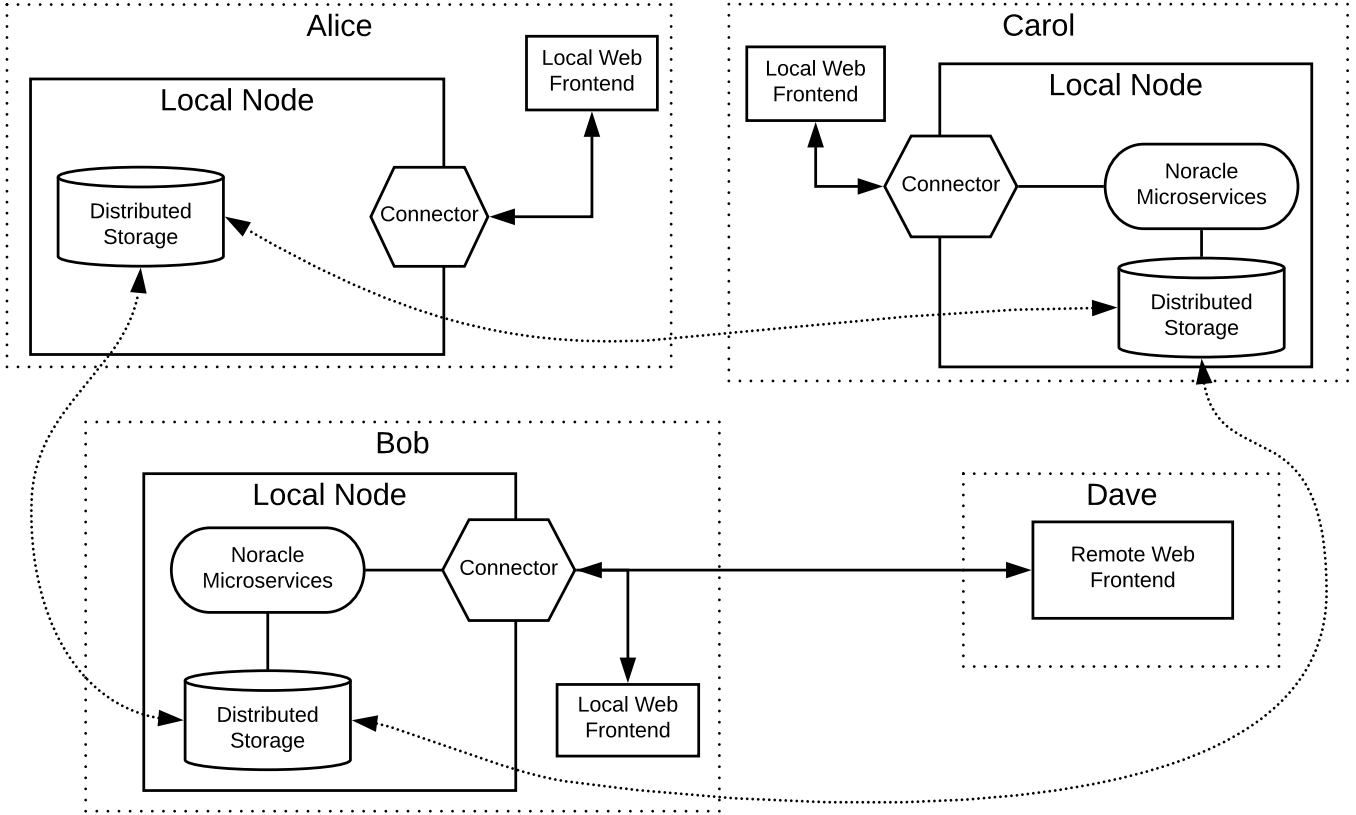
Motivation

- Communities of Practice (CoPs)[Wenger98] benefit from decentralized infrastructure
  - shared burden of hosting
  - natural scalability with community growth
  - self-governance and control over own data
- Previous work: Microservice Infrastructure for distributed CoPs[de Lange et al.18]
  - Self-hosted infrastructure for European Voluntary Service (EVS) training courses
  - Various evaluations with several communities over the course of a two year usage span



Peter de Lange
RWTH Aachen University, Germany

An Idealized Scenario...

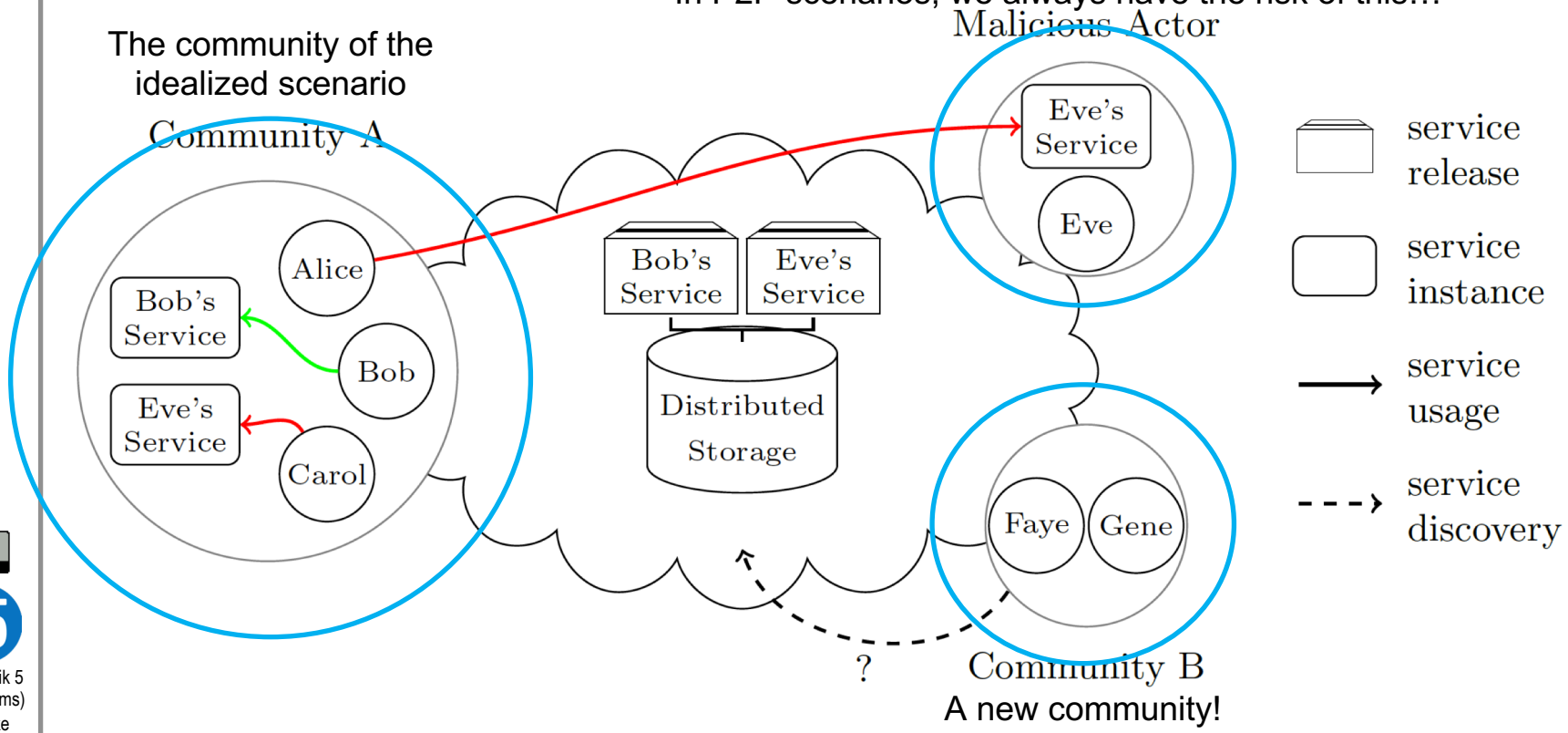


Lehrstuhl Informatik 5
(Information Systems)
Prof. Dr. M. Jarke

Peter de Lange
RWTH Aachen University, Germany

A More Realistic Scenario…

In P2P scenarios, we always have the risk of this…



Research Questions

1. How can we design a decentralized service registry that facilitates trust between service authors, users, and the published services?

2. How can we help users discover relevant services both within and beyond community boundaries?

Peter de Lange
RWTH Aachen University, Germany

Thus We Need A Decentralized Service Registry That...

- Gives authors control over service update process and the ability to establish a reputation
- Lets users verify origin and history of service releases
- Enables service discovery
    1. programmatically (via an API)
    2. for humans (via Web-based node front-end)

Peter de Lange
RWTH Aachen University, Germany

So Why Not Use The DHT?

- DHT lacks wildcard queriability → no search
- Sybil attacks:
  - create many “fake” identities in a network
  - influence majority decisions
- Byzantine fault:
  - nodes can exhibit arbitrary (mis-)behavior
  - misbehaving nodes can cooperate

Peter de Lange
RWTH Aachen University, Germany

Blockchain

- Decentralized data structure that is robust against Sybils and Byzantine faults (if majority of computing power “behaves”)
- Proof-of-Work consensus system
  - writing requires solving a cryptographic puzzle
  - “voting power” corresponds to computing power
- Ethereum: general purpose blockchain supporting smart contracts
  - scripts stored on the blockchain
  - their functions are invoked by special transactions
  - allow us to encode rules, such as ownership of entries

Peter de Lange
RWTH Aachen University, Germany

Two Smart Contracts: Decentralized Identity Management

- Secure identities are the foundation for trust
- Usernames can be registered on a first come, first served basis
- Stored on blockchain, smart contracts enforce ownership:
  - updating the entry requires private key
- Users have control over their data and can reveal as much as they like

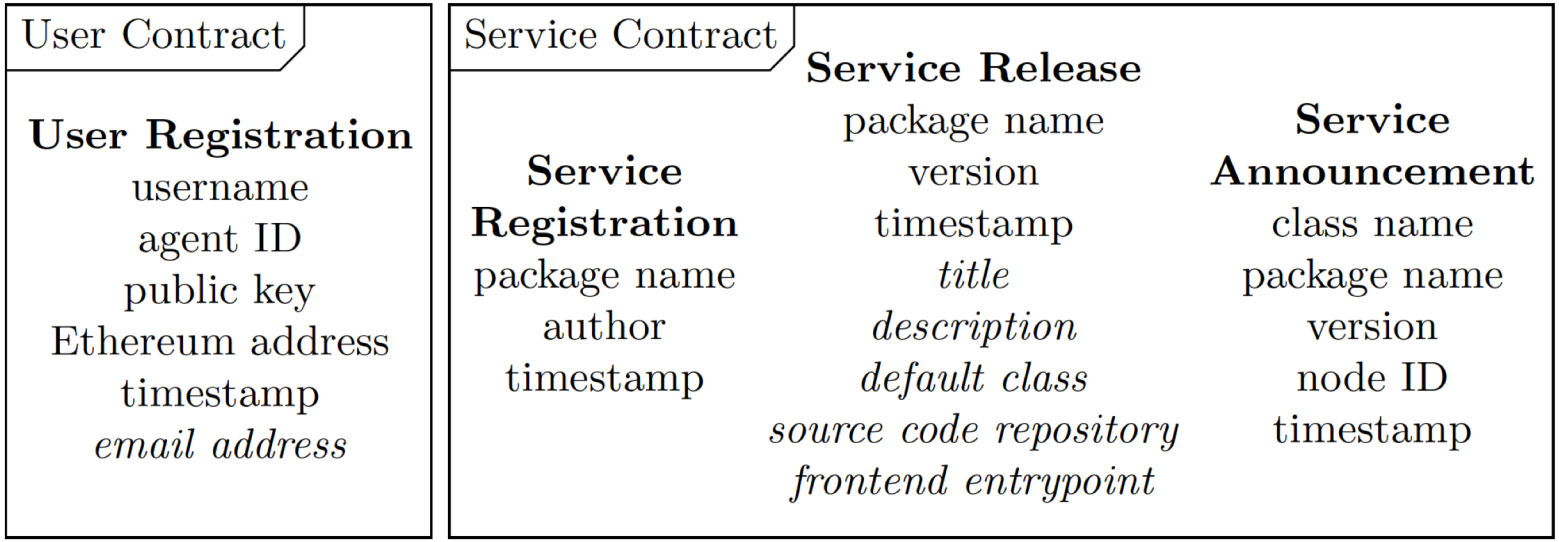
Peter de Lange
RWTH Aachen University, Germany

Two Smart Contracts: Service Registry

- Users can register service names
- The owner of a service name can then publish releases
- Releases include metadata for service discovery
  - for end-users: title, description, project URL
  - for services and developers: default class, entrypoint URL
- Running service instances are announced to the registry

Peter de Lange
RWTH Aachen University, Germany

Smart Contracts

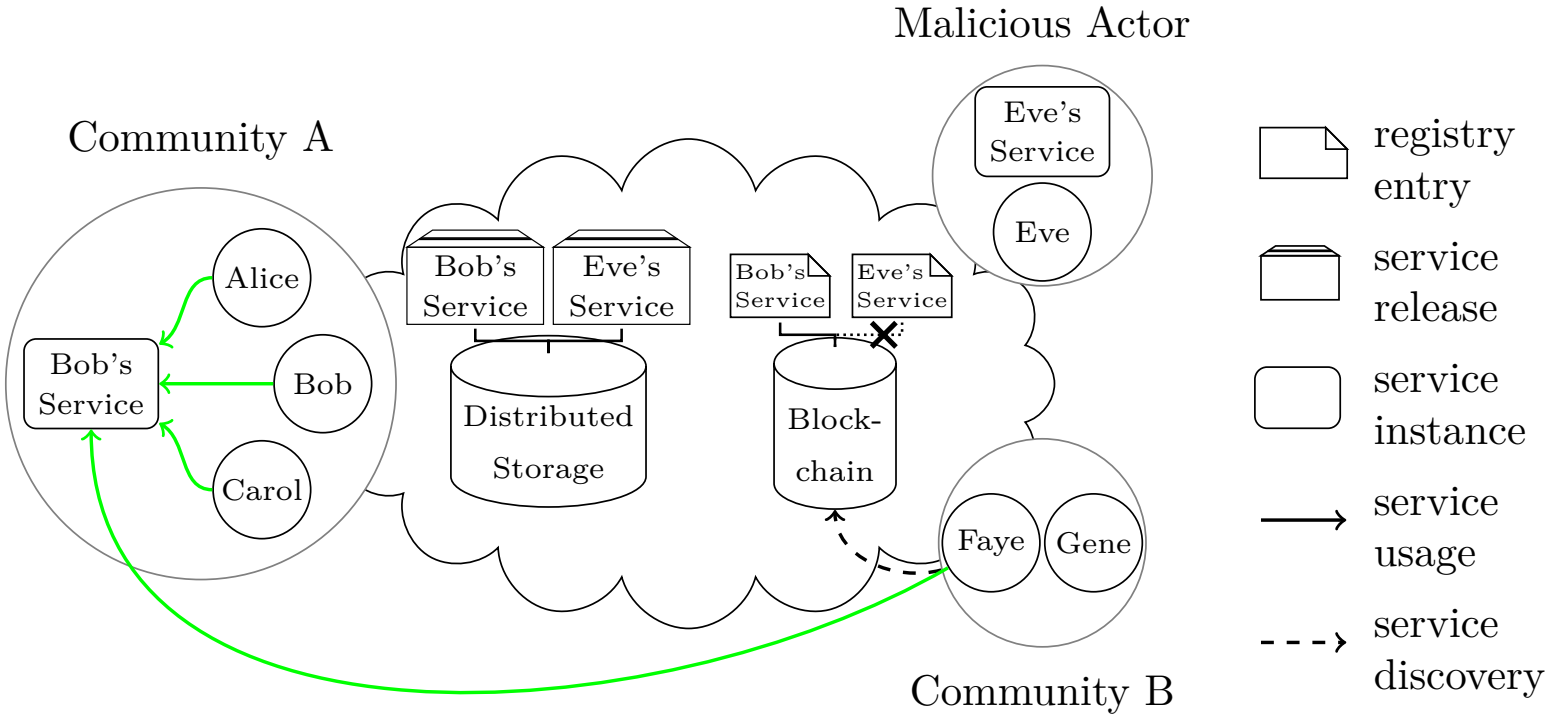


(entries in italics are stored as references to DHT)

Lehrstuhl Informatik 5 (Information Systems)
Prof. Dr. M. Jarke

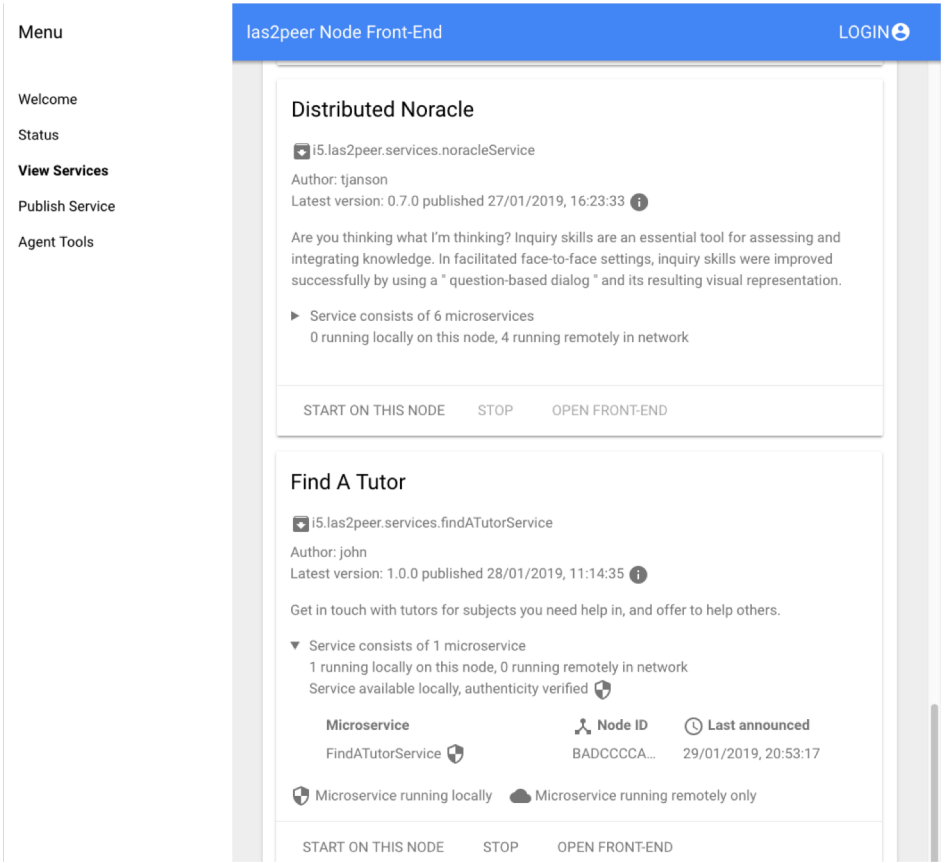
Peter de Lange
RWTH Aachen University, Germany

Same Use Case With BC-Service Registry



Peter de Lange
RWTH Aachen University, Germany

Service Explorer



Lehrstuhl Informatik 5 (Information Systems)
Prof. Dr. M. Jarke

Peter de Lange
RWTH Aachen University, Germany

Implementation: Components & Technology

- Service registry (*Solidity – Smart contract scripting language*)
  - stores and retrieves data on/from private blockchain
- Registry gateway (*Java*)
  - middleware layer, interfacing with DHT storage and Ethereum client
  - stores data blobs in DHT, references them on blockchain
  - provides JSON-based API
- Service explorer (*LIT Element Web Component*)
  - added to existing node Web front-end

Peter de Lange
RWTH Aachen University, Germany

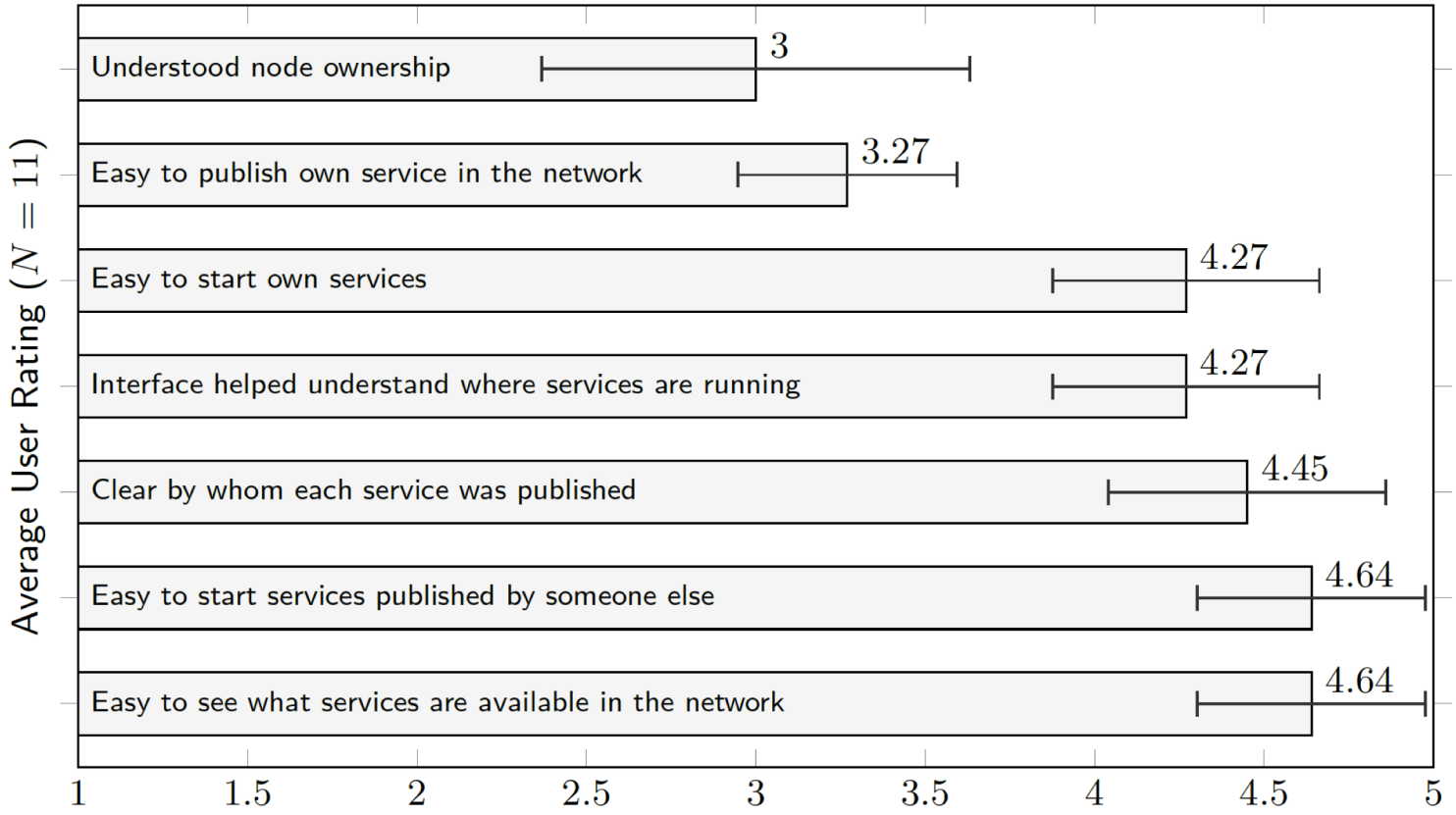
User Evaluation

- Do users understand and appreciate the service registry concept?
- What are their motivations, how do they benefit, and what improvements do they suggest?
- Sessions
  - 11 participants using a network of 5 permanent nodes
  - hands-on tasks using the Service Explorer: explore & discover, register, start & publish a service

Decentralized Service Registry

Peter de Lange
RWTH Aachen University, Germany

User Evaluation Results



Lehrstuhl Informatik 5
(Information Systems)
Prof. Dr. M. Jarke

Peter de Lange
RWTH Aachen University, Germany

Outcomes And Interpretation

- Participants considered service registry useful
- Most considered verified service authorship important
- Several participants were confused by concepts like nodes
  - need to improve UI for a non-technical audience
- Acceptable response time: 10 minutes or less
  - a large minority voted for 10 seconds

Peter de Lange
RWTH Aachen University, Germany

Technical Evaluation: Requirements

- Block time of < 1s used during evaluation proved infeasible
  - storage requirement too large
  - network synchronization issues
- Further evaluation yielded base storage requirements of
  - 3.7GB per year for 9.3s block time
  - 125MB per year for 271s (4.5min) block time

  → block times between 10s and 1min are feasible and would fulfill most users' expectations

Technical Evaluation: Security and Limitations

- Any attacker controlling the majority of mining power in the network can censor future transactions (e.g., exclude a particular user)
- Regardless of the blockchain-based registry, disruption of the network is easily possible by attacking the shared storage
- But: “Rewriting history” (e.g., changing ownership of a service) is quite expensive
  - an attacker twice as powerful as the existing network needs exactly one month to rewrite a block that is one month in the past

Conclusion

- Blockchain-based username and service registry is secure and feasible under realistic conditions
  - evaluation participants found the system useful
  - storage requirements are feasible, if response time requirements are not “real-time”

Future Work

- Service explorer only a first step
  - personalized recommendations, tagging, and community analysis
- Contributions, in their various forms (providing computing resources, authoring services), should be recognized and rewarded
  - blockchain cryptocurrency may form the basis of a reputation system
  - bounties could be awarded for desired contributions