Universität Bayreuth
Prof. Dr. Nils Urbach
Professur für Wirtschaftsinformatik
und Strategisches IT-Management

UNIVERSITÄT BAYREUTH

Ansprechpartner
Lehrkoordination WI

Telefon
+49 921 55 - 4705

E-Mail
wi-lehrkoordination@uni-bayreuth.de

Bachelorarbeit / Masterarbeit

Blockchain und Privacy - Die Bedeutung von Methoden des Privacy-Preserving Computings angesichts einer zunehmenden Verbreitung von DLT

Die Transparenz, die mit der Verwendung von Distributed Ledger Technologie (Blockchain) einhergeht, ist sowohl aus rechtlicher Sicht (DSGVO) als auch hinsichtlich der Interessen von Individuen und Unternehmen problematisch. Daher beschäftigen sich aktuell viele Forscher mit der Frage, wie es möglich ist, Daten trotz der mit DLT einhergehenden Transparenz nur in dem Umfang preiszugeben, der zwingend notwendig ist. Hierfür gibt es bereits zahlreiche Ideen und Methoden – die entsprechenden Konzepte sind in der Kryptographie bereits seit langem bekannt, aber in der Praxis noch nicht weit verbreitet. So könnten DSGVO-Aspekte durch Verschleierung von IP-Adressen in Kombination mit der Verwendung von Off-Chain-Speicherung und Hashwerten berücksichtigt werden. Auch die Verwendung von Zero-Knowledge-Proofs und Secure Multiparty Computation wird zunehmend diskutiert. Im Rahmen der Arbeit sollen diese Lösungsansätze gesammelt, anschaulich erklärt und sinnvoll strukturiert sowie hinsichtlich ihrer zukünftigen Relevanz auch im Lichte zunehmender Verbreitung der DLT bewertet werden.

Empfohlene Einstiegsliteratur:

- Vincent Schlatt, André Schweizer, Nils Urbach, Gilbert Fridgen: Blockchain: Grundlagen, Anwendungen und Potenziale.
  http://fim-rc.de/Paperbibliothek/Veroeffentlicht/642/wi-642.pdf
- Gilbert Fridgen, Nikolas Guggenberger, Thomas Hören, Wolfgang Prinz, Nils Urbach (Fraunhofer FIT im Auftrag des BMVI): Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik.
  https://www.bmvi.de/SharedDocs/DE/Anlage/DG/blockchain-gutachten.pdf?__blob=publicationFile
- Fraunhofer Blockchain Lab: Closing the Privacy Gap of Distributed Ledger Technology: An Introduction to Zero Knowledge Proofs and Secure Multiparty Computation
  https://medium.com/@FraunhoferLab/closing-the-privacy-gap-of-distributed-ledger-technology-an-introduction-to-zero-knowledge-proofs-bec67df2e241
- Bruce Schneier: Applied Cryptography: Protocols, Algorithms and Source Code in C. 20th anniversary edition

Betreuer: Sedlmeir, Johannes, M.Sc.

Universität Augsburg University · UNIVERSITÄT BAYREUTH · TUM · fim · Elitenetzwerk Bayern