



## [ Prof. Dr. Hannes Hartenstein // Dezentrale Systeme und Netzdienste ]

Hannes Hartenstein ist seit Oktober 2003 Leiter der Forschungsgruppe „Dezentrale Systeme und Netzdienste“ (DSN). Von Oktober 2010 bis September 2013 war er Geschäftsführender Direktor des Steinbuch Centre for Computing (SCC), von Oktober 2015 bis März 2017 Dekan der Fakultät für Informatik und von April 2017 bis April 2020 Bevollmächtigter für die Informationsverarbeitung und -versorgung (IV-B) des KIT.

74

Er studierte Mathematik an der Universität Freiburg. Seine Promotion erlangte er 1998 am dortigen Institut für Informatik über ein Thema zur Kompression von Bildern. Anschließend arbeitete er im Bereich „Mobile Networks“ in der Forschungsabteilung von NEC Europe Ltd. in Heidelberg mit Fokus auf Vehicular Ad Hoc Networks und Vehicle-to-X Communication.

Hannes Hartenstein ist Principal Investigator im Helmholtz-Topic „Engineering Secure Systems“ im Programm „Engineering Digital Futures“. Darüber hinaus ist er u. a. Mitglied der ständigen Kommission „Digitalisierung“ der Hochschulrektorenkonferenz, des Ausschusses für Recht und Sicherheit des Deutschen Forschungsnetzes sowie des Aufsichtsrats des Leibniz-Zentrums für Informatik Schloss Dagstuhl.

### // Überblick und Allgemeines

Die Forschungsgruppe „Dezentrale Systeme und Netzdienste“ untersucht Möglichkeiten und Grenzen dezentraler Systeme, d. h. verteilter und vernetzter technischer Systeme, die von mehreren Parteien weitestgehend unabhängig voneinander betrieben werden. Im Fokus stehen derzeit Blockchains und Distributed Ledger Technologies,

Broadcast- und Konsensverfahren, sichere Smart Contracts, Peer-to-Peer-Netze und ihr Monitoring, dezentrales Messaging am Beispiel von Matrix, Identitätsmanagement und Zugriffskontrolle sowie sichere und privatsphärengerechte Datenverarbeitung in bedingt vertrauenswürdigen Umgebungen.

### // Einblicke in Forschung und Projekte

Seit dem Jahr 2015 beobachten wir das Bitcoin Peer-to-Peer-Netz (siehe <https://www.dsn.kastel.kit.edu/bitcoin/>). Aktuelle Beobachtungen zeigen etwa Sicherheitsvorfälle, die ihrerseits wiederum zu Erkenntnissen über das Peer-to-Peer-Netz führen. So konnte beispielsweise eine massive Spamwelle im Jahr 2021 genutzt werden, um den Knotengrad der Bitcoin-Peers in bisher unerreichter Genauigkeit festzustellen.

Wir analysieren die theoretischen Eigenschaften der populären dezentralen Messaging-Plattform Matrix und konnten nachweisen, dass es sich bei der zugrundeliegenden Datenstruktur um einen sogenannten Conflict-Free Replicated Data Type handelt, der sogar die Eigenschaft der Toleranz gegen byzantinische Angreifer vorweisen kann.

Im Rahmen des Helmholtz-Topics „Engineering Secure Systems“ forschen wir an

Sicherheit und Privatsphäre am Beispiel von Mobility-as-a-Service. Wir entwickeln und untersuchen Systeme, die unabhängigen Parteien eine schnelle Konsensfindung ermöglichen, ohne dabei Geheimnisse offenbaren zu müssen, sowie Systeme, mit denen Bezahlungen effizient ausgeführt und abgerechnet werden können. Für die Konsensfindung evaluieren wir den Nutzen von Trusted Execution Environments, die die Verwendung von effizienteren Konsensalgorithmen ermöglichen. Für die Bezahlung von Tickets untersuchen wir die Verwendung von Payment Channel Networks.

Wir erforschen zudem die Tauglichkeit von dezentralen Plattformen wie Ethereum zur Erstellung und Nutzung von Softwareidentitäten. Basierend auf diesen Softwareidentitäten haben wir ein Konzept entwickelt und implementiert, mit denen digitale Objekte einem unabhängigen Review-Prozess unterzogen werden können, der auf einer öffentlichen Blockchain koordiniert und dokumentiert wird. So können Softwareidentitäten mit unabhängig überprüften Attributen hinsichtlich ihrer Sicherheitseigenschaften oder Funktionalität versehen werden.

Wir sind am vom BMWK geförderten Forschungsprojekt Software-Defined Car (SofDCar) beteiligt. Weil im Lebenszyklus automobiler Software verschiedene Parteien Informationen über die Software sammeln sowie Entscheidungen über ihren Einsatz treffen müssen, untersuchen wir dezentrale Ansätze für das Management von Identitäten und Zugriffen automobiler Software.

Im von der Carl-Zeiss-Stiftung geförderten Projekt „JuBot: Jung bleiben mit Robotern“ forschen wir an humanoiden Assistenzrobotern, die in Pflegeeinrichtungen und Haushalt in vielseitiger Weise die zu pflegenden als auch die betreuenden Personen unterstützen können. Unser Ziel ist das Co-Design von physischen Räumen, Assistenzrobotern und zugehörigen virtuellen Räumen hinsichtlich Zutritts-, Zugriffs-, und Nutzungsverfahren.



## // Ausgewählte Publikationen 2022

M. Grundmann, M. Baumstark und H. Hartenstein, „On the Peer Degree Distribution of the Bitcoin P2P Network,“ 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022, S. 1–5

F. Jacob, S. Bayreuther und H. Hartenstein, „On CRDTs in Byzantine Environments: Conflict Freedom, Equivocation Tolerance, and the Matrix Replicated Data Type,“ Sicherheit 2022: Sicherheit, Schutz und Zuverlässigkeit. Hrsg.: C. Wressnegger, Gesellschaft für Informatik e. V., 2022, S. 113–128

M. Leinweber, N. Kannengießer, H. Hartenstein, A. Sunyaev, „Leveraging Distributed Ledger Technology for Decentralized Mobility-as-a-Service Ticket Systems,“ in Towards the New Normal in Mobility. Hrsg.: H. Proff, erscheint bei Springer, 2022

O. Stengele, C. Westermeyer and H. Hartenstein, „Decentralized Review and Attestation of Software Attribute Claims,“ in IEEE Access, vol. 10, 2022, S. 66694-66710

S. Bayreuther, F. Jacob, M. Grotz, R. Kartmann, F. Peller-Konrad, F. Paus, H. Hartenstein, and T. Asfour, “BlueSky: Combining Task Planning and Activity-Centric Access Control for Assistive Humanoid Robots,“ in Proc. 27th ACM on Symposium on Access Control Models and Technologies (SACMAT ’22). ACM, New York, NY, USA, 2022, S. 185–194.

## // Mitarbeiterinnen und Mitarbeiter

**Verwaltungspersonal**  
Astrid Hopprich

**Wissenschaftliches Personal**  
Matthias Grundmann  
Florian Jacob  
Marc Leinweber  
Oliver Stengele  
Christina Westermeyer

// Website  
[dsn.kastel.kit.edu](https://dsn.kastel.kit.edu)