Fraunhofer
IAO

Workshop IV:
»Sichere Identitäten für Personen und Dinge durch Blockchain und Distributed Ledgers«

Der Workshop gliederte sich in einen etwa 20-minütigen inhaltlichen Input von Dr. Heiko Roßnagel, Leiter des Team Identitätsmanagement des Fraunhofer IAO und einen etwa 70-minutigen Gruppenworkshop.

Input

Herr Dr. Roßnagel umriss zunächst knapp auf die Grundlagen des Identitätsmanagements (IdM), wobei er auf die Bedeutung des Identitätsmanagement-Lifecycles hinwies, ehe er aktuelle Entwicklungen und Herausforderungen im B2B-, sowie B2C-IdM hervorhob (etwa organisationsübergreifendes IdM in komplexen Wertschöpfungsketten, der anhaltende Erfolg zentraler Identitätsprovider im Web-IdM). Anschließend skizzierte er, weshalb die Blockchain-Technologie für IdM von Interesse ist und ging auf gegenwärtige Entwicklungen im Kontext des blockchain-basierten IdM ein (Self-Sovereign Identities, W3C Decentralized Identifiers (DID) Spec). Als Beispiele wurden Sovrin/Hyperledger Indy für Self-Sovereign Identities sowie ein alternativer, hierarchisch organisierter Ansatz (nach Mell et al. 2019) vorgestellt, und auf Blockchain/DLT-basiertes IdM für das IoT eingegangen. Bevor es in den Gruppenworkshop ging, stellte Herr Dr. Roßnagel schließlich noch gegenwärtige Herausforderungen für blockchain-basiertes IdM vor. Hierbei betonte er, dass diese nicht ausschließlich technisch (beispielsweise Handling von Credentials bei Verlust, Skalierbarkeit…), sondern insbesondere auch in sozioökonomischen Aspekten zu verorten sind (Mehrseitiger Markt, Business Case…).

Gruppenworkshop

In vier Gruppen befassten sich die Teilnehmenden (divers zusammengesetzt aus kleineren und Großunternehmen, Ministerien, Beratungen, zivilgesellschaftlichen Organisationen und einem Blockchain-IdM Startup) gemeinsam mit je einem Fraunhofer Experten eingehender mit Anwendungsszenarien für blockchain-basiertes IdM. Sie erarbeiteten pro Gruppe Anforderungen für je ein Szenario und diskutierten dessen Eignung für blockchain-basiertes IdM bzw. in wieweit die besonderen Eigenschaften der Blockchain-Technologie für das Szenario vorteilhaft sind oder aber auch eine Herausforderung darstellen. Außerdem skizzierten sie knapp, wie ein solches IdM-System gestaltet werden könnte, um die Anforderungen zu erfüllen und die identifizierten Herausforderungen bewältigt werden könnten. Die vier Szenarien und einige der von den Gruppen erarbeiteten und zum Abschluss des Workshops präsentierten Ergebnisse lauteten:

1. Blockchain-basiertes Identitätsmanagement im B2C e-Business
   In diesem Szenario wurde auf Wunsch der Teilnehmer weiter auf eine elektronische Patientenakte fokussiert. Hiermit ergaben sich entsprechend besondere Herausforderungen hinsichtlich des Datenschutzes. Eine solche Patientenakte müsste dann den selektiven Zugriff auf bestimmte Attribute/Patienteninformationen ermöglichen. Diskutiert wurde außerdem, wie eine Wiederherstellung von Credentials

bei Verlust und die Möglichkeiten und Grenzen von Social-Recovery-Funktionen diskutiert.

2. Blockchain-basierte Identitäten für Geflüchtete bzw. Menschen ohne Identitätsnachweise
   Als besondere Herausforderung wurden hier Datenschutzaspekte identifiziert, weshalb personenbezogene Daten unbedingt off-chain gehalten werden müssen. Des Weiteren stellt sich der Umgang mit verlorenen oder gestohlenen Credentials als herausfordernd dar.
3. Blockchain-basierte Identitäten als Ergänzung (Ersatz?) staatlicher IDs
   Im Zuge der Diskussion wurde bezweifelt, dass blockchain-basierte Identitäten ein Ersatz staatlicher IDs darstellen könnten, für bestimmte Anwendungsfälle könnten abgeleitete Identitäten jedoch durchaus hilfreiche Dienste leisten. Hier wurden etwa privatsphärenfreundliche Altersnachweise und ähnliche Use Cases genannt. Hinsichtlich des Verhältnis zu staatlichen IDs wurde die Bedeutung des EU eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste betont.
4. Blockchain-basiertes Identitätsmanagement für Dinge
   Für dieses Szenario diskutierte Anforderungen waren etwa technische wie auch die Skalierbarkeit der Zahl der Identitäten, die ökonomische und ökologische Effizienz, sowie die Manipulationssicherheit. Hinsichtlich letzterer wurde deutlich, dass die Blockchain zwar die Manipulationssicherheit der gespeicherten Informationen gewährleisten kann, es aber eine Herausforderung darstellt, einen manipulationssicheren Link zwischen »offline Dingen« und auf die Chain geschriebenen Informationen herzustellen.