

Digitale Identitäten und Blockchain

IHK Webinarreihe
„Blockchain für den Mittelstand“
15. Juni 2021

Frankfurt University of Applied Sciences

Prof. Dr. Nils Urbach

Kernkompetenzzentrum
Finanz- & Informationsmanagement

Projektgruppe Wirtschaftsinformatik
des Fraunhofer FIT

Professur für Wirtschaftsinformatik,
insbesondere Digital Business & Mobilität

www.fim-rc.de

www.wirtschaftsinformatik.fraunhofer.de

www.frankfurt-university.de

Digitale Identitäten spielen im Internet eine zentrale Rolle, weisen jedoch Herausforderungen auf

„The internet was built without an identity layer“

2018, Sovrin Foundation, Whitepaper: What Goes on The Ledger



5 Jul 1993, The New Yorker, by Peter Steiner



Süddeutsche Zeitung

6. März 2021, 19:16 Uhr Datensouveränität

Wettlauf um das digitale Ich



ÖKOSYSTEM DIGITALE IDENTITÄTEN

Digitalisierung im Alltag voranbringen

Das Fehlen digitaler Nachweise ist eines der drängendsten Digitalisierungshemmnisse unserer Zeit. Gemeinsam mit namhaften Partnern aus der Wirtschaft will die Bundesregierung noch in diesem Jahr den Grundstein zum Aufbau eines Ökosystems digitaler Identitäten legen und bis zu zehn Anwendungsfälle mit hoher Alltagsbedeutung umsetzen. Ein erstes Pilotprojekt vereinfacht das Hotel-Check-in für Firmenreisende.

heise online heise+

heise online › News › 03/2021 › Digitaler Corona-Impfpass: IBM, Ubirch und fünf Blockchains

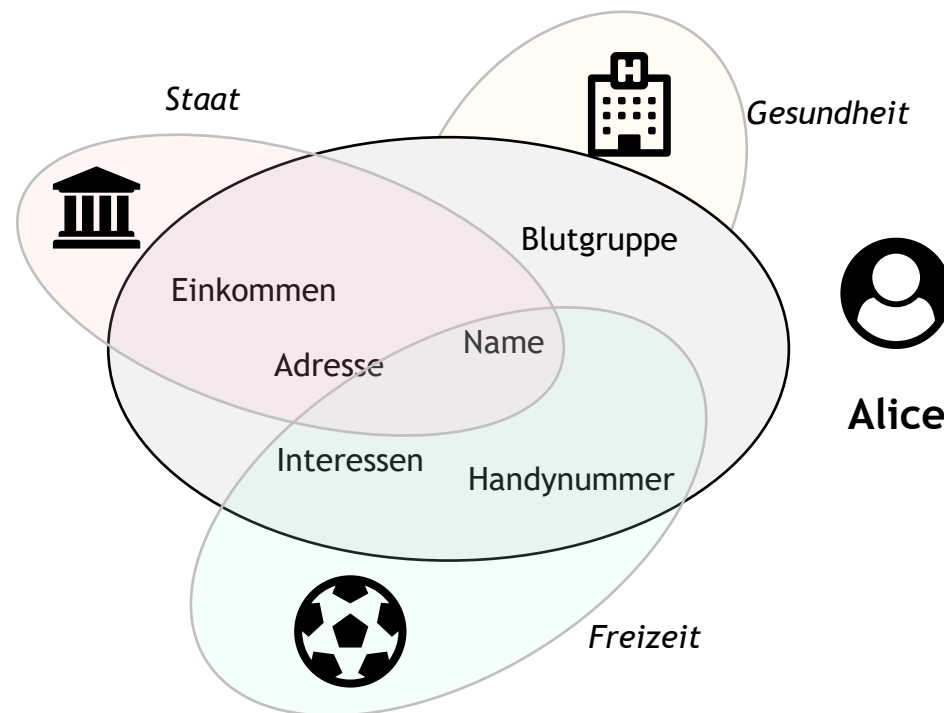
Digitaler Corona-Impfpass: IBM, Ubirch und fünf Blockchains

Die Bundesregierung hat IBM und der Firma Ubirch den Zuschlag für die Entwicklung eines digitalen Impfpasses gegeben.

Identitäten bestehen aus „partiellen Identitäten“

Alle Teilmengen der Identität repräsentieren die Person (oder Komponenten der Person). Einige dieser 'Teilidentitäten' identifizieren die Person eindeutig, andere nicht. Je nach Situation und Kontext kann die Person durch verschiedene Teilidentitäten repräsentiert werden.

(Clauß & Köhntopp, 2001)



Ein Identitätsmanagementsystem erlaubt die Verwaltung von Teilidentitäten

“

*Ein Identitätsmanagementsystem stellt die Werkzeuge für die **Verwaltung von Teilidentitäten** in der digitalen Welt bereit. [...] Identitätsmanagementsysteme ermöglichen dem Benutzer, die **Art und Menge** der freigegebenen persönlichen Informationen **zu kontrollieren**. Dies ist ein wichtiges Merkmal für die **informationelle Selbstbestimmung**.*

(Clauß & Köhntopp, 2001)

Analoges Identitätsmanagement besitzt eine Reihe inhärenter Nachteile



Ineffizienzen

- Oftmals papierbasierte Prozesse für Bescheinigungen und Nachweise, welche aufwendige Folgeprozesse und Medienbrüche zur Folge haben
- Manuelle Bearbeitungen führen zu einer geringen Datenqualität



Manipulationsgefahr

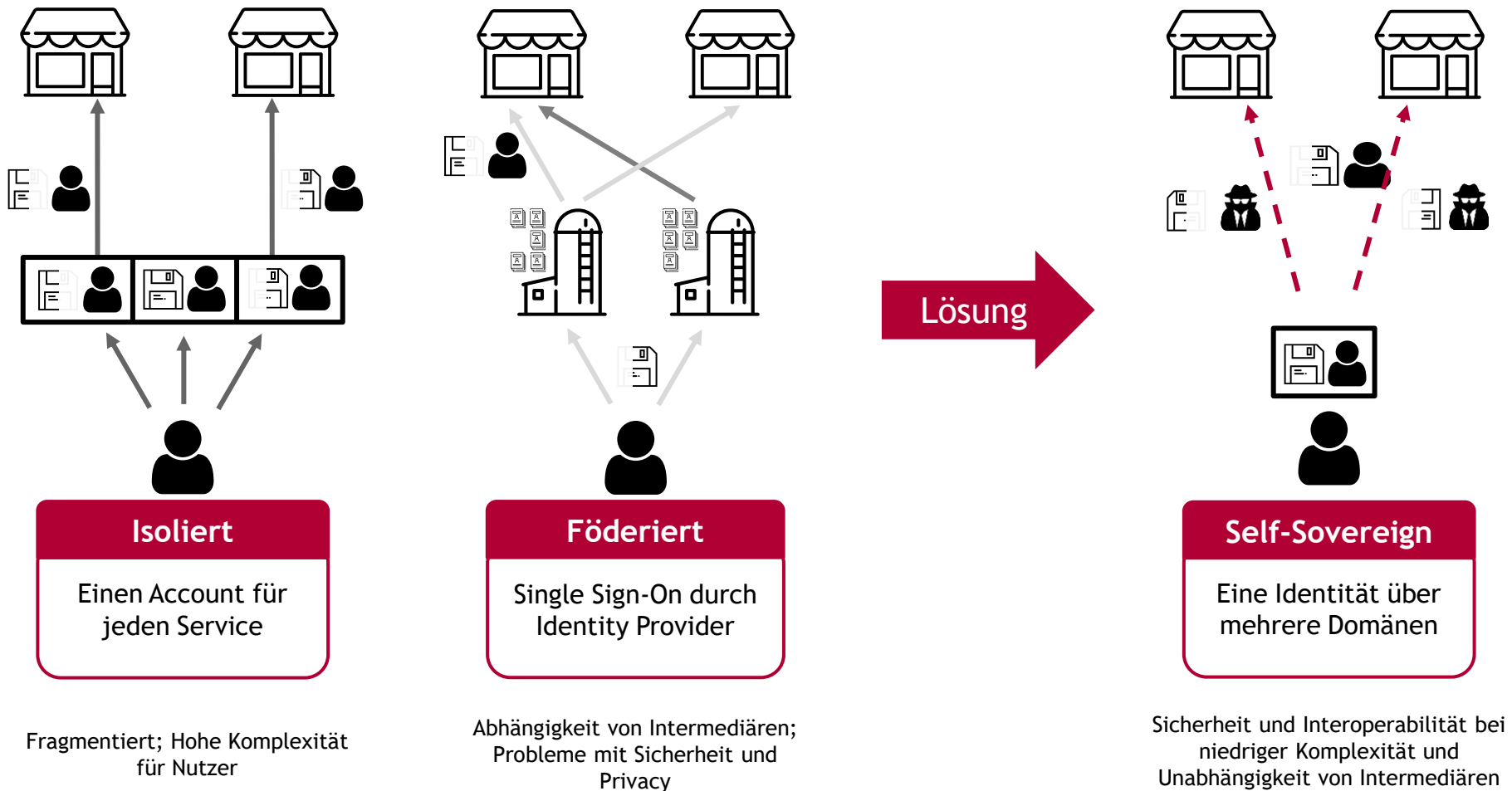
- Papierbasierte Bescheinigungen und Nachweise sind anfällig für Fälschungen und Missbrauch
- Papierbasierte Bescheinigungen können oftmals nicht zurückverlangt werden
- Durch organisationsseitige Verantwortung für Datenhaltung hohe Kosten für Compliance und Risiken von Datenschutzverletzungen



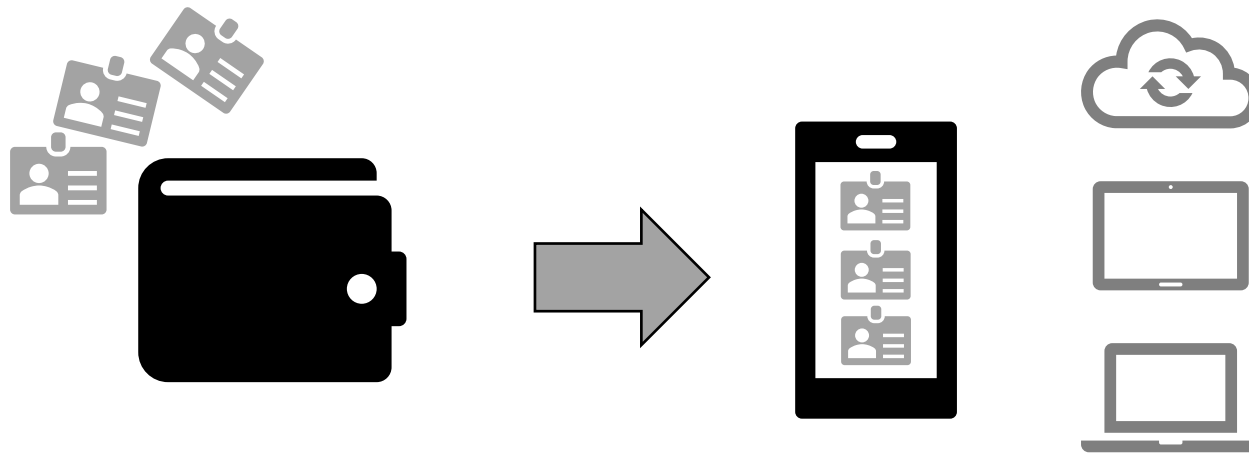
Komplexität und geringer Komfort

- Unterschiedliche Systeme zur Datenverarbeitung von Organisationen führen zu hoher Komplexität und Transaktionskosten
- Geringer Nutzerkomfort durch oftmals redundantes Teilen von Daten

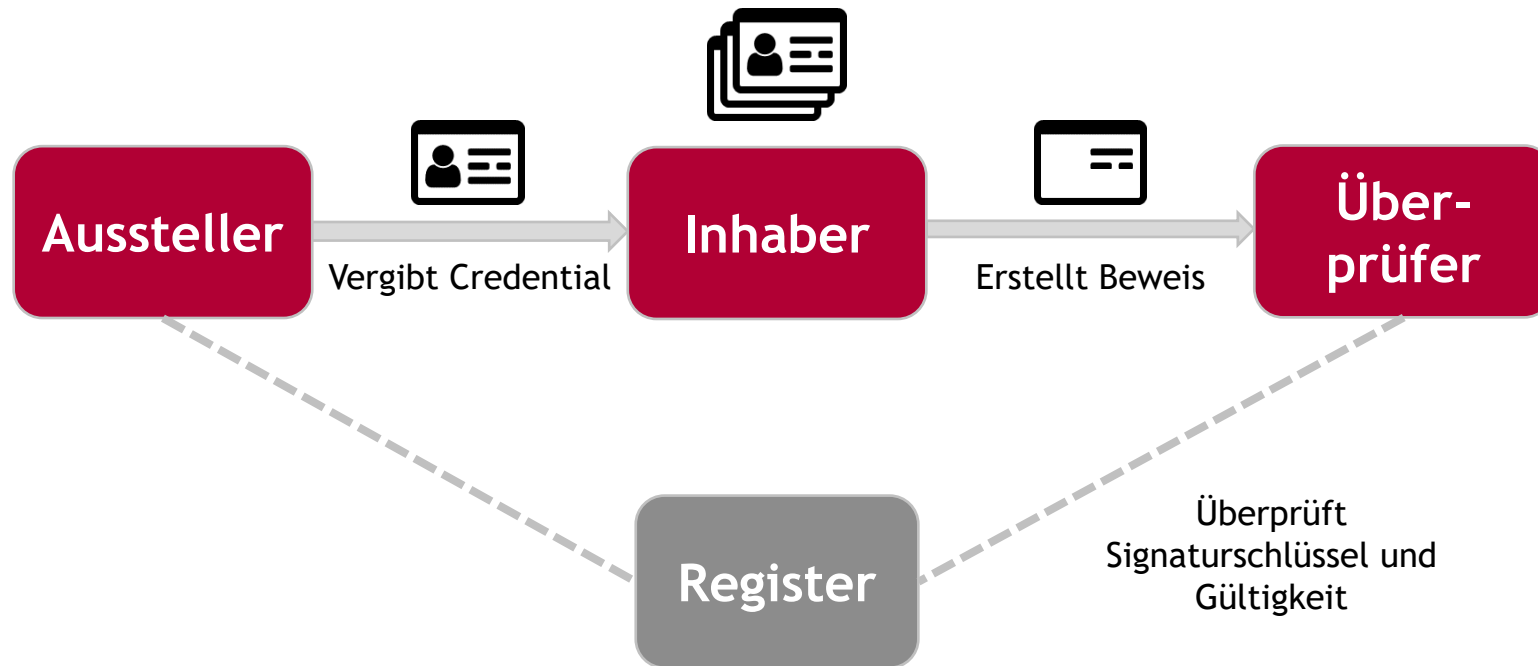
Auch digitale Lösungen sind nicht perfekt und besitzen Herausforderungen



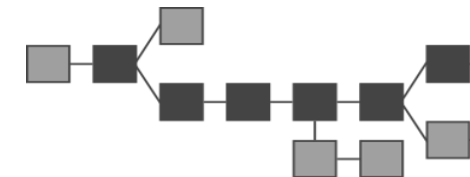
Im Wesentlichen sind selbstsouveräne Identitäten wie Nachweise in einer Brieftasche



Es gibt drei zentrale Rollen im Kontext von selbstsouveränen Identitäten



Credentials müssen widerrufen werden können

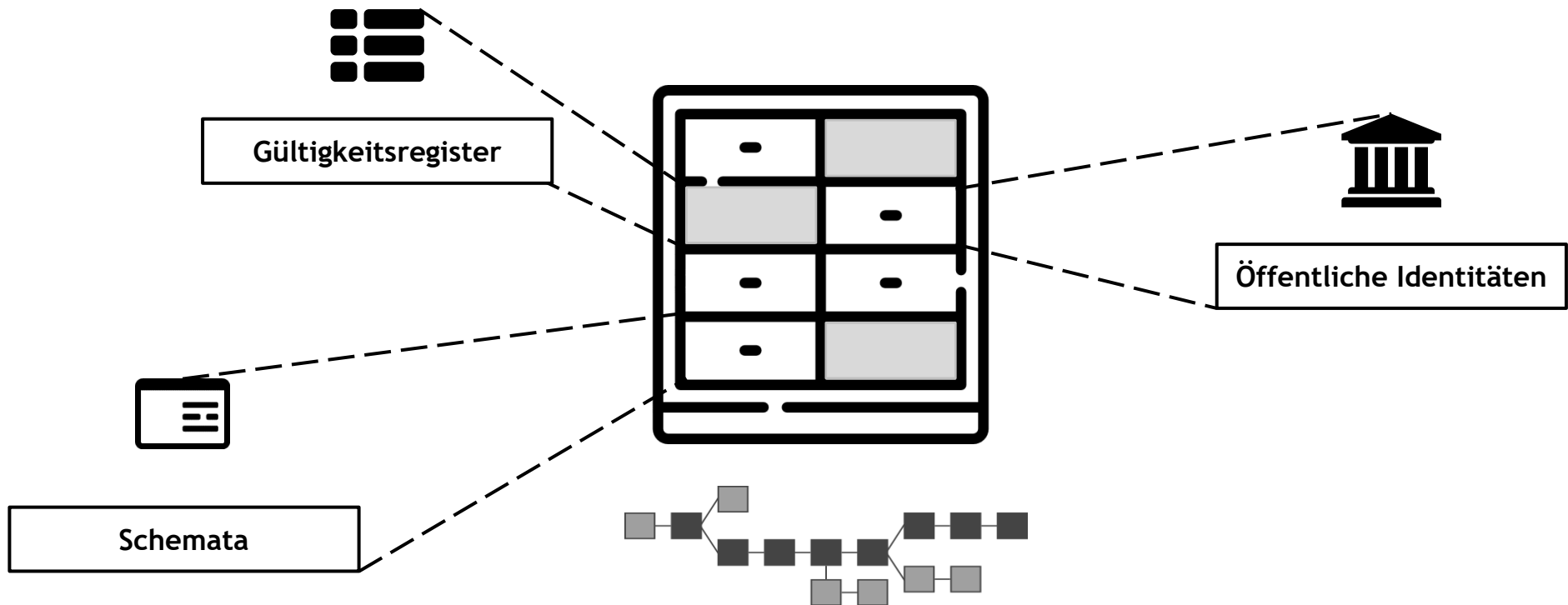


Attribute wie z.B. Verfallsdaten können in einem Verifiable Credential enthalten sein.

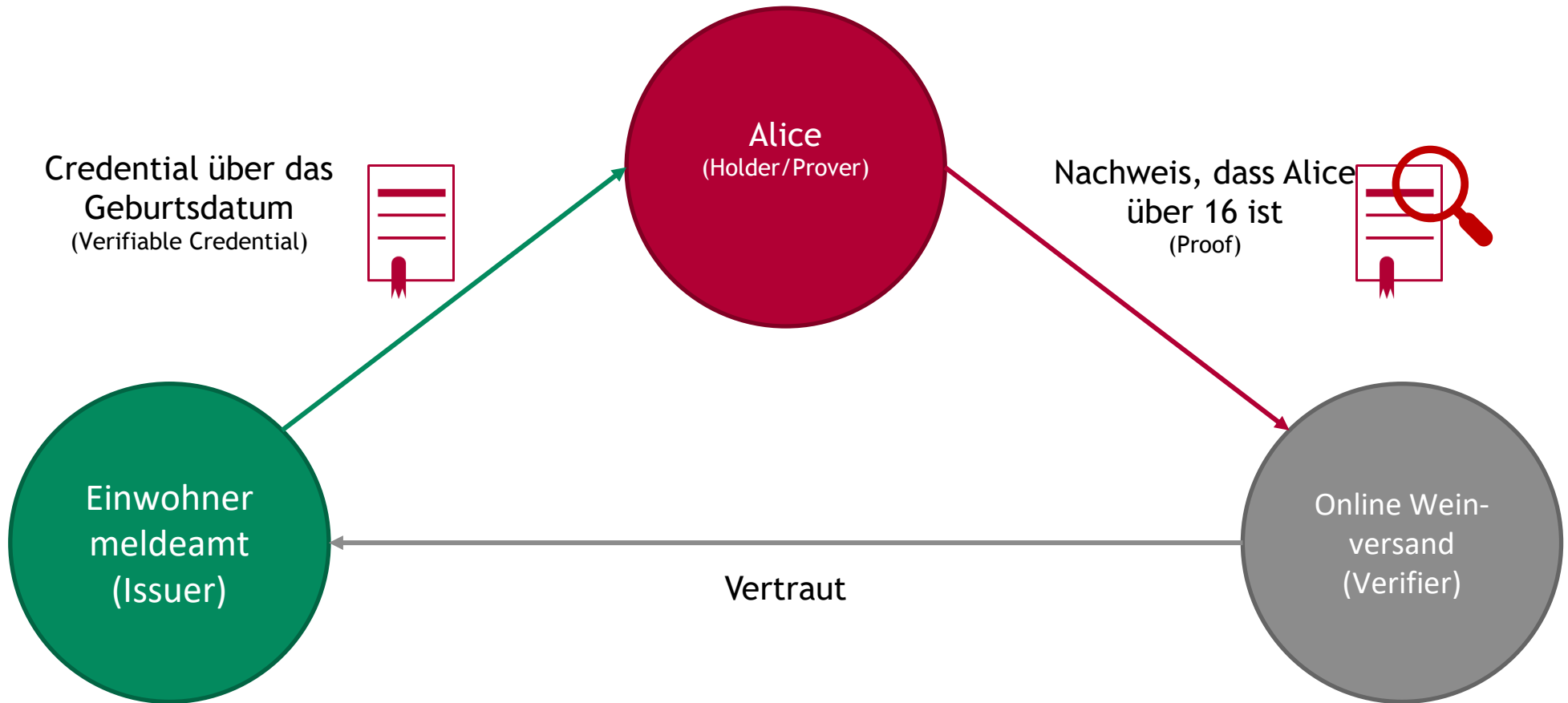
Für den Fall, dass das Credential ad hoc widerrufen werden muss, erlaubt ein dezentralisiertes Berechtigungssystem nicht, das Credential des Inhabers lokal zu löschen.

Credentials müssen auf öffentlich zugänglichen Listen durch den Issuer oder autorisierte Behörden widerrufen werden.

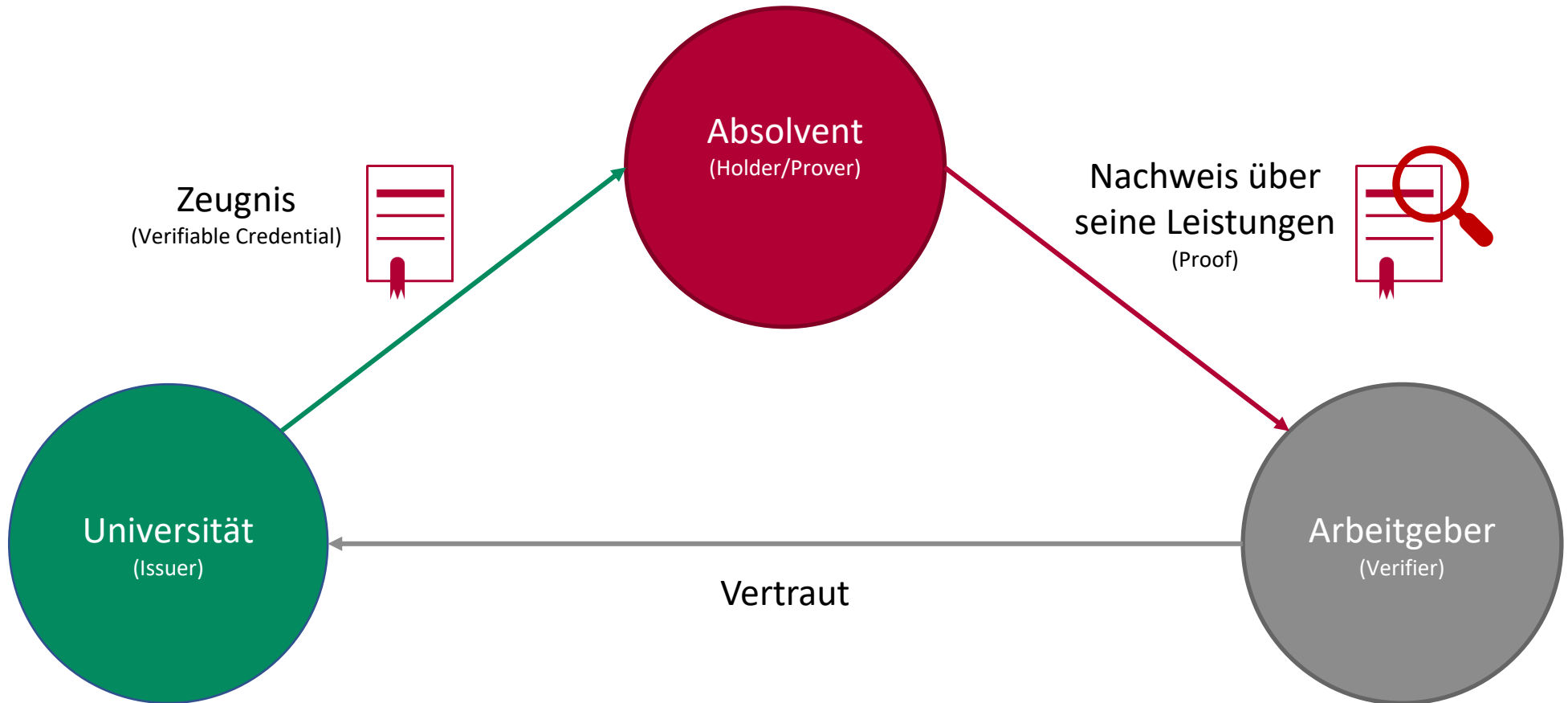
Häufig werden Blockchains als Register für Gültigkeiten, Schemata und öffentliche Identitäten genutzt



Beispielhafte Anwendung von selbstsouveränen Identitäten im E-Commerce



Beispielhafte Anwendung von selbstsouveränen Identitäten durch Universitäten



Self-Sovereign Identity bringt Vorteile sowohl für Organisationen als auch Privatpersonen



Effizienz

- Offene Standards ermöglichen ein interoperables, Blockchain-basiertes Ökosystem und verbessern die Datenqualität und -verfügbarkeit
- Nutzerzentrierung minimiert das Teilen von redundanten Daten zwischen Organisationen
- Standardisierte Interaktionsmuster reduzieren die Komplexität von Systemen und Transaktionskosten



Sicherheit

- Fälschungssichere Zertifikate verhindern Missbrauch von Daten
- Dezentralisierte Identifier (DIDs) ermöglichen sichere bilaterale Kommunikation
- Nutzerverantwortung für die Daten reduziert die Kosten für Compliance und minimiert die Auswirkungen von Datenverletzungen



Nutzererfahrung

- Kryptografische Verfahren erhöhen die Privatsphäre
- Tragbare Lösungen ermöglichen eine komfortable Bedienung
- Interoperabilität reduziert die Komplexität der Anwendung



Prof. Dr. Nils Urbach

Projektgruppe WI des Fraunhofer FIT
Kernkompetenzzentrum FIM
Frankfurt University of Applied Sciences
nils.urbach@fim-rc.de

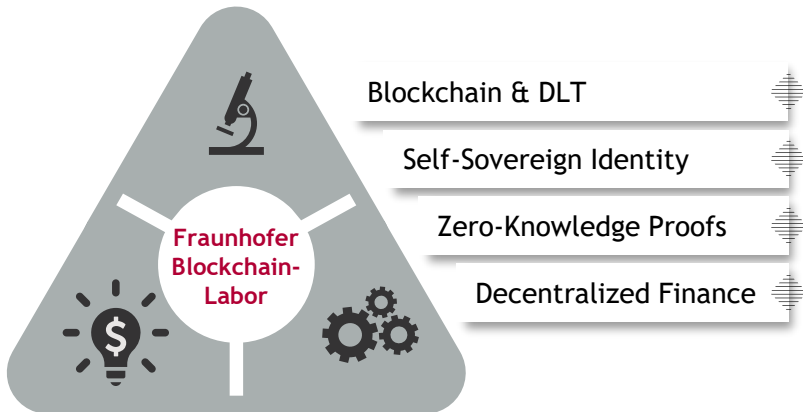


Das Fraunhofer Blockchain-Labor erforscht verschiedene Anwendungen im Kontext von Blockchain

Fraunhofer Blockchain-Labor

Unser Leistungsspektrum

- Das Fraunhofer Blockchain-Labor ist eine multidisziplinäre Einrichtung zur **Konzeption, Entwicklung und Evaluation von Blockchain-Lösungen und dezentralen Systemen.**
- Wir bieten **nachhaltige, innovative und wertstiftende IT-Lösungen für allen Branchen.**



Workshops,
Vorträge &
Schulungen



Konzepte,
Analysen
& Studien



Prototypen,
MVP &
Netzwerkaufbau



Publikationen &
Wissenschaftliche
Community



Wissenschaftliche Begleitung

- Anwendung wissenschaftlicher Methoden im interdisziplinäre Umfeld
- Überführung aktueller Erkenntnisse aus der Forschung in praxistaugliche, integrative Anwendungen

#State-of-The-Art



Geschäftsmodell-Entwicklung

- Begleitung aus rechtlicher, ökonomischer und technischer Perspektive
- Anforderungs- und Potentialanalysen neuer Technologien
- Einordnung und Entwicklung von disruptiven Geschäftsmodellen

#Value-Driven



Technologie-Implementierung

- Konzeptionierung technischer Systeme aufbauend auf Blockchain und anderen dezentralen Lösungen
- Implementierung von Prototypen mit Hilfe agiler Methoden sowie deren technische Evaluierung

#Cutting-Edge