



JOLOCOM

Digitalisierung der Energiewende: Digitale Identitäten für Dezentrale Anlagen

by Irene Adamski, LL.M.



BLOCKCHAIN
BUNDESVERBAND

Chair INATBA WG Energy
General Secretary of German Blockchain Association
OECD BEPAB Member

Teil 1

Herausforderungen in der Energiewende

Teil 2

Erfordernisse Dezentraler Anlagen

Teil 3

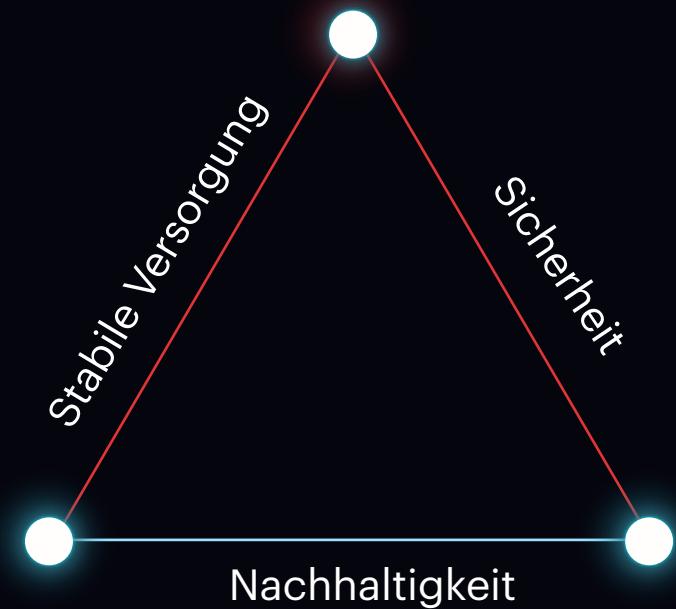
Digitale Identitäten als Lösungen

Das Trilemma kritischer Infrastrukturen

Das Kernproblem der Energiewende



Unser derzeitiges, auf fossilen Brennstoffen beruhendes Energiesystem ist sicher und stabil, aber nicht nachhaltig



Energiesysteme, die 100% auf Erneuerbaren Energien basieren, sind nachhaltig, aber weniger stabil und sicher.

Die verfügbaren Stellschrauben im Energie Sektor

LASTENSTEUERUNG

Lastensteuerung: abregeln bei Über- und Unterversorgung

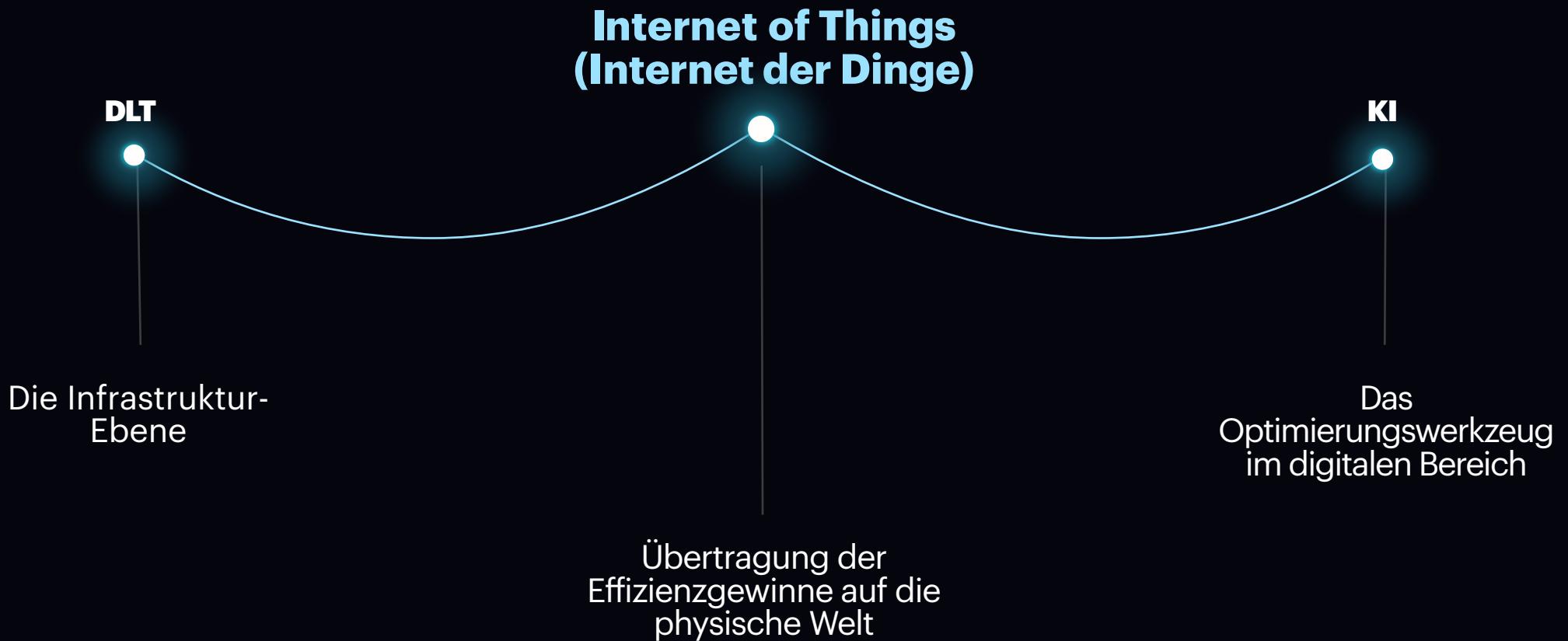
MARKTREGULIERUNG

Marktregulierung: soziale Verträglichkeit, Flexibilität und ökonomische Anreizsetzung

NETZAUSLASTUNG UND -AUSBAU

Netz: gleichmäßige Auslastung und Ausbau vorantreiben, wenn der Bedarf es erfordert

Der Dreiklang der Digitalisierung im Energiesektor



Teil 1

Herausforderungen in der Energiewende

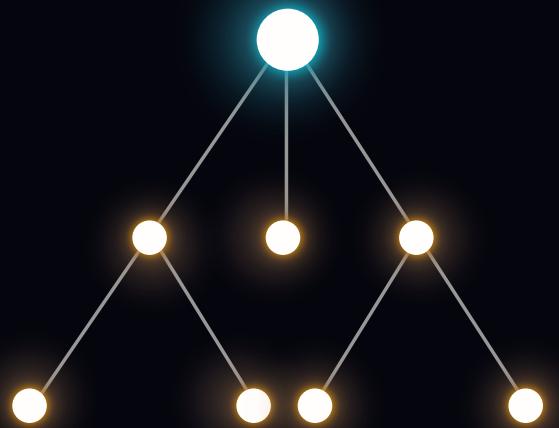
Teil 2

Erfordernisse Dezentraler Anlagen

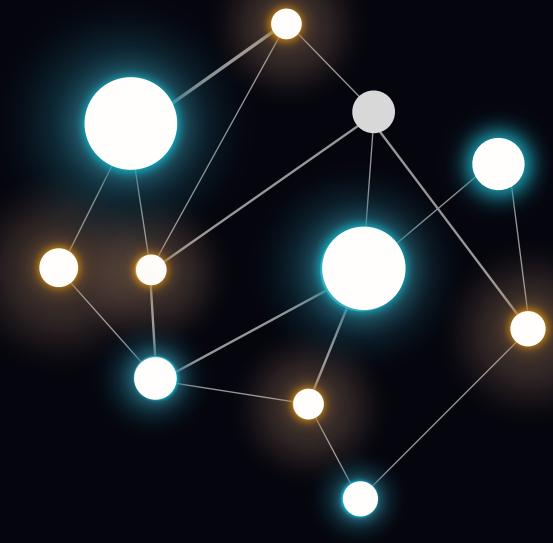
Teil 3

Digitale Identitäten als Lösungen

Eine zentralisierte Systemarchitektur wird dezentral



**Dezentrale Anlagen
restrukturieren ein
bisheriges Oligopol zu
einem Sektor mit Millionen
von dezentralen Geräten
und Akteuren**



Eine zentralisierte Systemarchitektur wird dezentral



Neue Akteure, wie der Prosument, müssen in das Stromnetz integriert werden

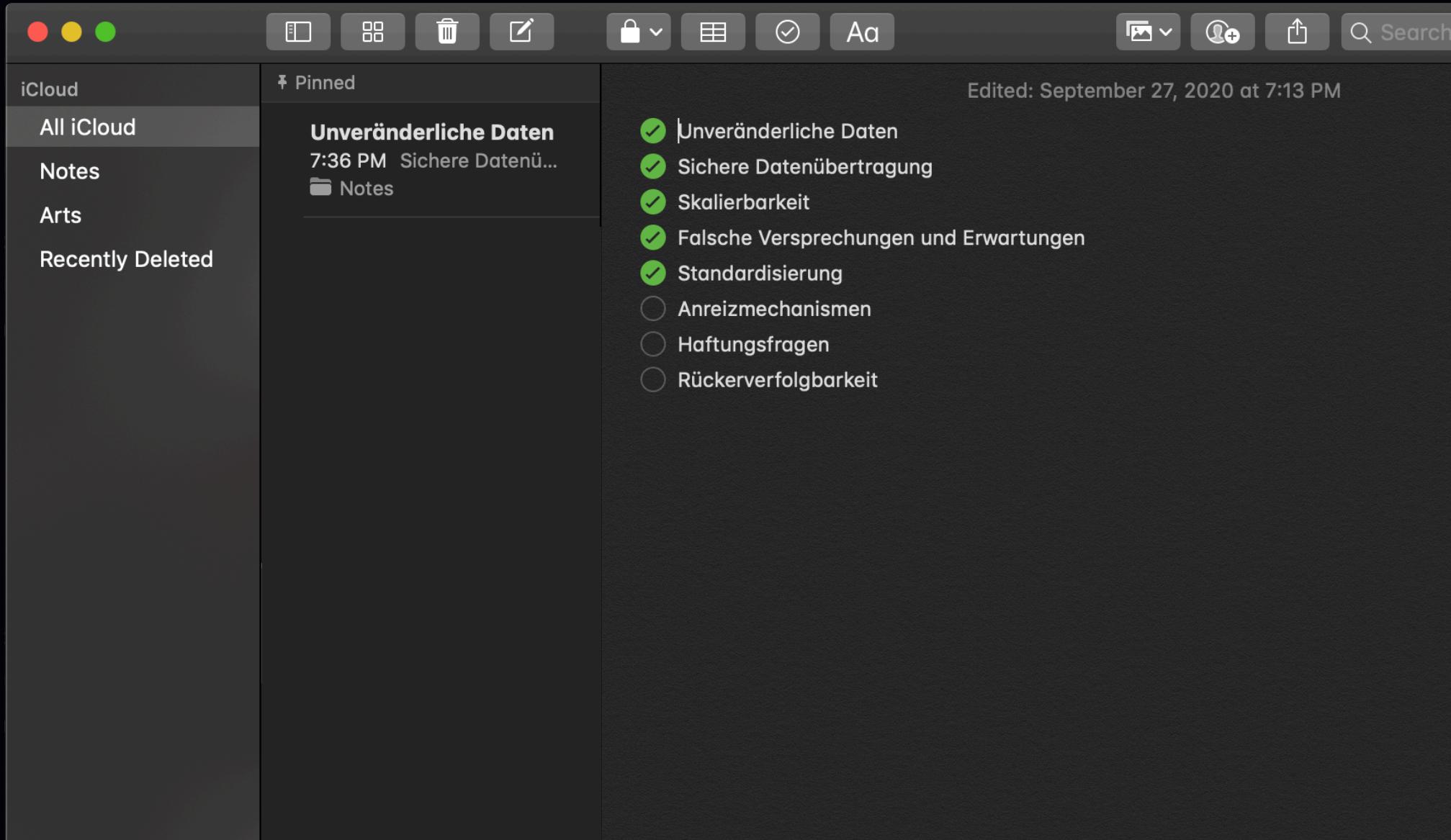
ökonomisch, flexibel und sicher

Eine zentralisierte Systemarchitektur wird dezentral



**Wie können Millionen neuer Akteure sinnvoll,
praktisch und sicher integriert werden?**

Reifegrad der Technologie und offene Fragen



A screenshot of a Mac OS X Notes application window. The window has a dark background. On the left is a sidebar with the following items: iCloud, All iCloud (which is selected), Notes, Arts, and Recently Deleted. The main area shows a pinned note titled "Unveränderliche Daten" with a timestamp of 7:36 PM and a note type of "Sichere Datenü...". Below the title is a "Notes" icon. To the right of the note is a list of bullet points under the heading "Edited: September 27, 2020 at 7:13 PM". The list contains the following items:

- Unveränderliche Daten
- Sichere Datenübertragung
- Skalierbarkeit
- Falsche Versprechungen und Erwartungen
- Standardisierung
- Anreizmechanismen
- Haftungsfragen
- Rückverfolgbarkeit

Teil 1

Herausforderungen in der Energiewende

Teil 2

Erfordernisse Dezentraler Anlagen

Teil 3

Digitale Identitäten als Lösungen

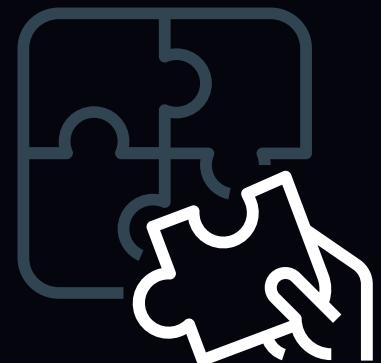
Identifizierung von Akteuren und Geräten

Optimierung der Märkte und Ihrer Regulierung

Granulare Datensätze für die Vorhersagemodelle von
ÜNBs und BKVs

Praktisch-umsetzbare Prüf- und Aufsichtsverfahren

Detaillierte Datensätze
Automatisierung
Differenzierung



Zentralisierte und Dezentralisierte Identitätsmodelle

SELBST-SOUVERÄNE IDENTÄTEN

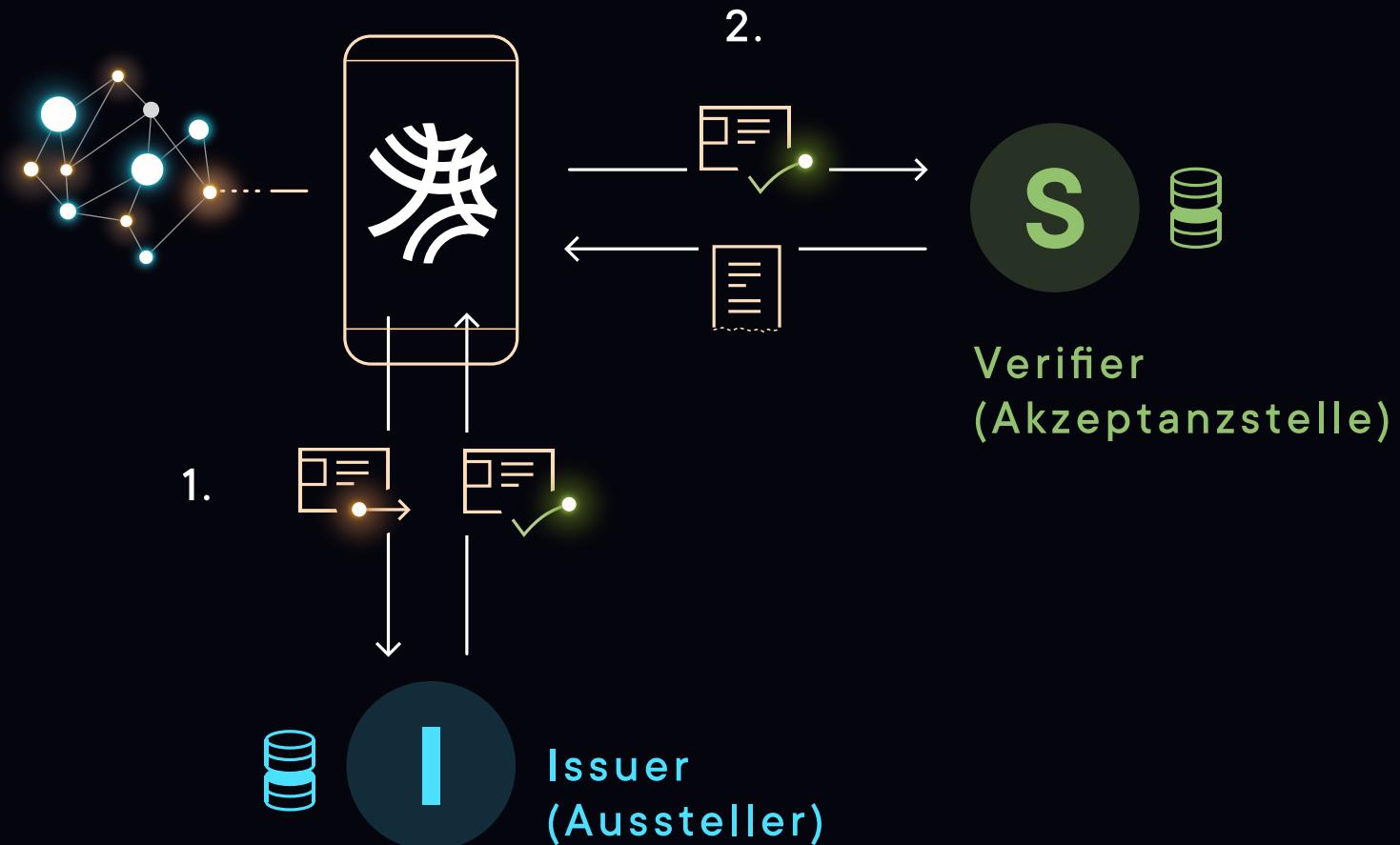
Dezentralisierter Ansatz bei dem der Endnutzer **völlig selbst-bestimmt** handelt, mit allen Rechten, Pflichten und Verantwortungen

VERMITTLER-SYSTEM

zentralisierter Ansatz bei dem ein Dienstleister als **Intermediär zwischen Nutzer und Netz** agiert, was Rechte und Möglichkeiten einschränkt, aber Pflichten und Verantwortlichkeiten vollständig überträgt

- ✓ **Anreizmechanismen**
- ✓ **Haftungsfragen**
- ✓ **Rückerverfolgbarkeit**

Vertrauensmodelle Digitaler Identitäten



Zusammenfassung: integrierende Energiewende

1

**Integration neuer
Akteure
(Prosumenten, IoT-
Geräten) in das Netz**

2

**Sichere und
granulare Daten um
das dezentrale
System praktisch
handhabbar und
sicher zu machen**

3

**Anreize schaffen
über direkte
Beteiligung und
selbstbestimmte
Handlungsoptionen**

Möglichkeiten, sich aktiv mit Dezentralen Identitäten zu beschäftigen

Standardisierung



DIF



W3C

Pilotprojekte



eSSIF



SDI

Communities



VSDI



Bundesblock



INATBA

Vielen Dank für Ihre Aufmerksamkeit!

Irene Adamski, LL.M.

Irene@jolocom.com

Chair INATBA WG Energy
General Secretary of German Blockchain Association
OECD BEPAB Member





Decentralized Digital Identities in Mobility

Trust as the Key Concept
in the Internet of Things

Peter Busch

Product Owner DLT Mobility

 @pbusch42

The Bosch Group – Four Business Sectors

Key figures 2019*

BOSCH Group

- ~78 billion EUR in sales
- ~400.000 associates
- 280 plants in 60 countries

Mobility Solutions

- One of the world's largest suppliers of mobility solutions



84% share of sales



Industrial Technology

- Leading in drive and control technology, packaging, and process technology



Energy and Building Technology

- One of the leading manufacturers of energy-efficient heating products, security and communication technology



16% share of sales



Consumer Goods

- Leading supplier of power tools and accessories
- Leading supplier of household appliances



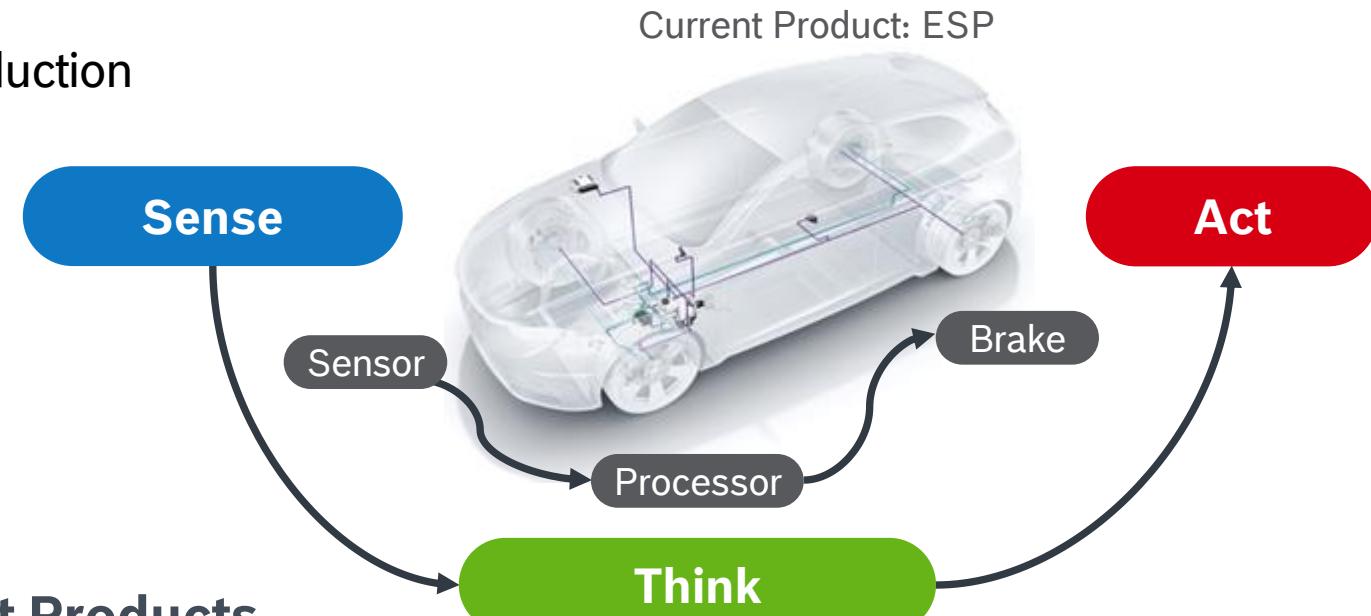
* as of 12.19

Expanding the Internet of Things Vision Chances for BOSCH (and the Industry)

We **connect** our products and their production
with the **Internet of Things (IoT)**

Artificial Intelligence (AI) enables
complex functionality based on data

IoT and **AI** are the basis for **intelligent Products**



Bosch IoT Vision: *All electronic products connected in 2020*

All products either posses **AI** or are created by utilizing **AI** in **2025**

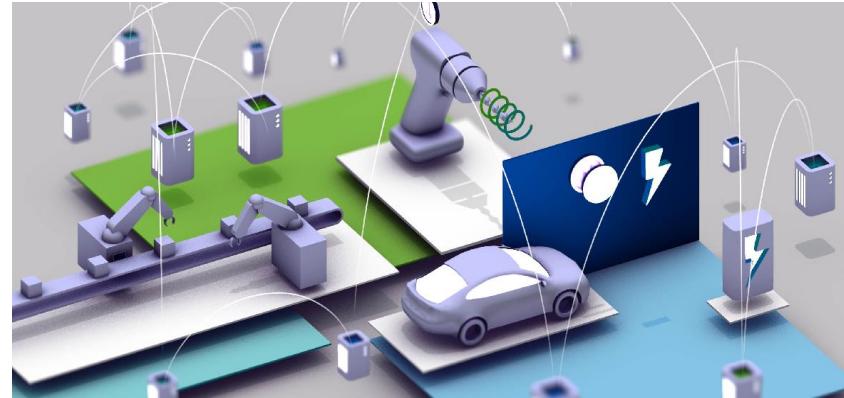
Distributed Ledger Technology - Project “Economy of Things”

An Alternative Approach to Centralized Platform Monopolies

INTERNET OF THINGS



- > All domains get connected
- > Massive DATA gets created
- > DATA enables new products



ECONOMY OF THINGS

- > CONNECTED devices as ECONOMIC devices
- > Devices do seamless BUSINESS
- > Towards AUTONOMOUS, LEGAL entities

*DISTRIBUTED LEDGER TECH

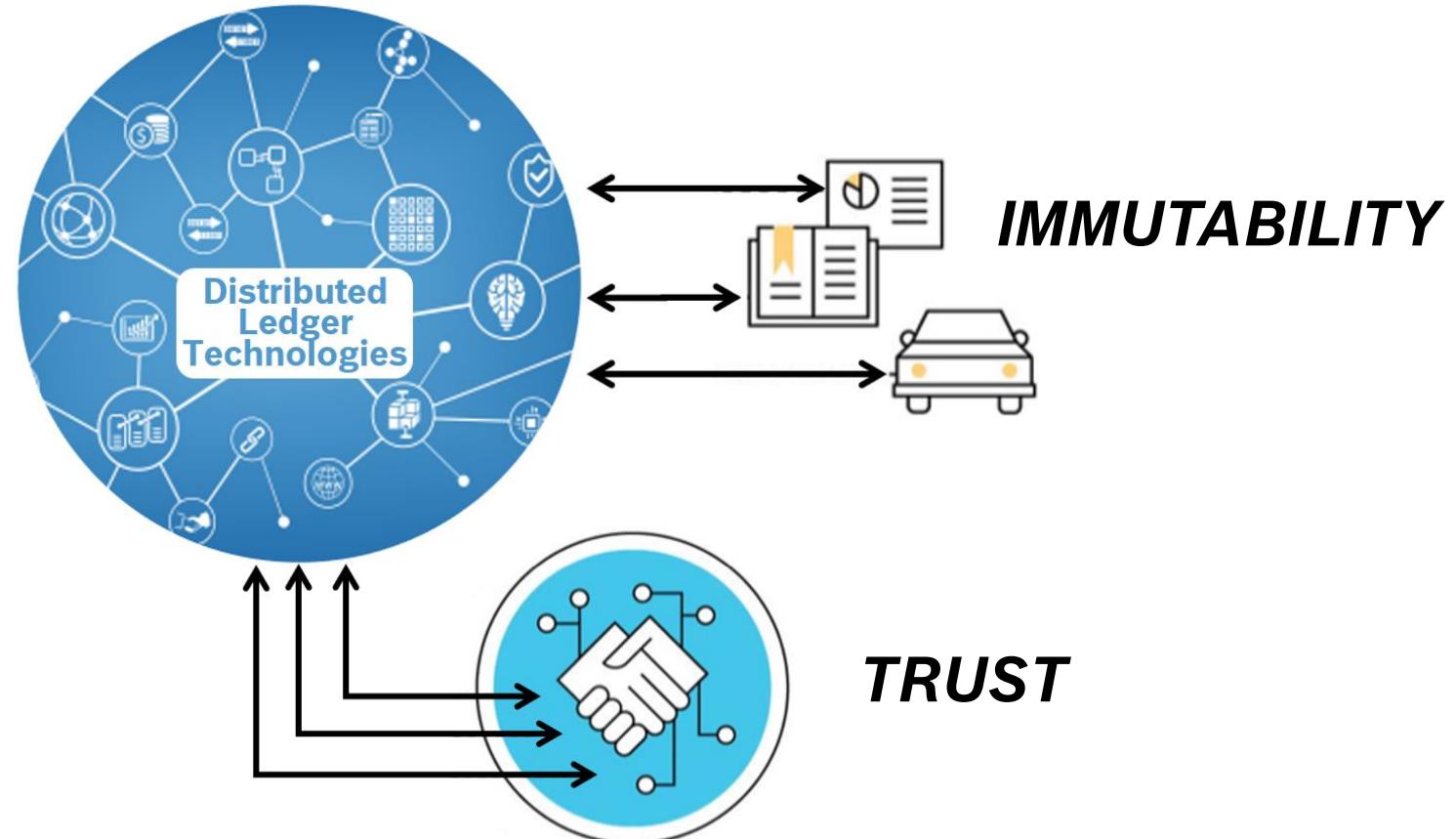


- > Foundation of crypto-currencies
- > Decentralization and Trust
- > Machine2Machine Value Exchange

Distributed Ledger Technology - Project “Economy of Things”

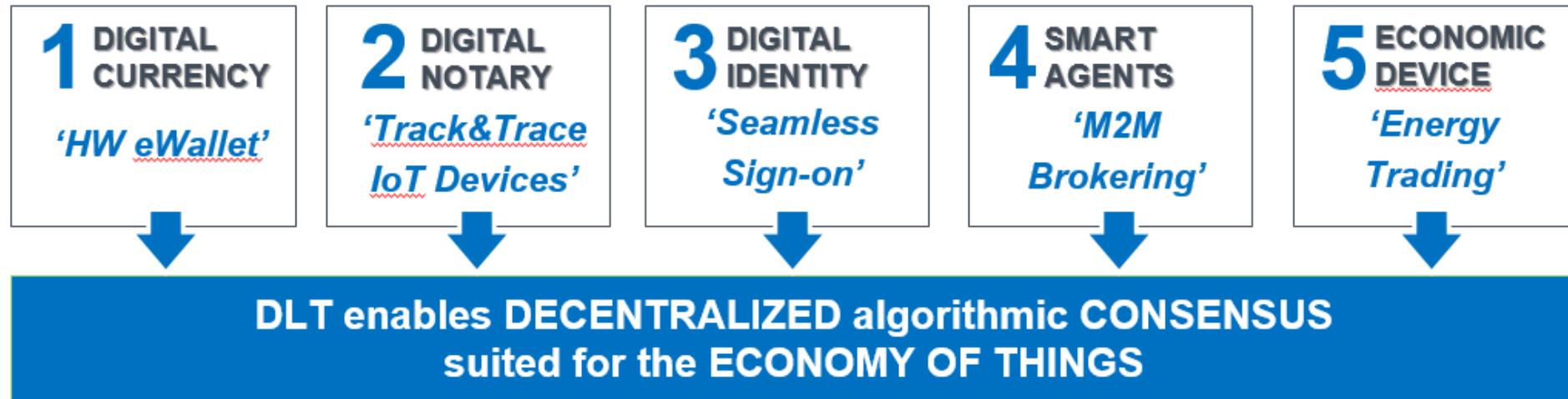
An Alternative Approach to GAFA* Platform Monopolies

DECENTRALIZATION



Distributed Ledger Technology - Project “Economy of Things”

5-Steps Strategy of Bosch’s DLT-Project



Everybody wants to own the platform

plus

Nobody wants to be locked in on other platforms

results in

Small platforms without benefits of scaling networks

A new concept to break this deadlock

The Economy of Things

Houston, we have a problem! The Internet was built WITHOUT an Identity Layer

Problem

- There isn't one identity provider that works for all



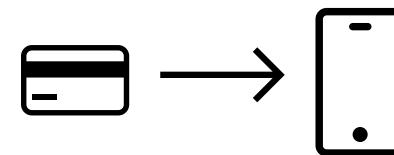
- Growing threats to our internet privacy/security



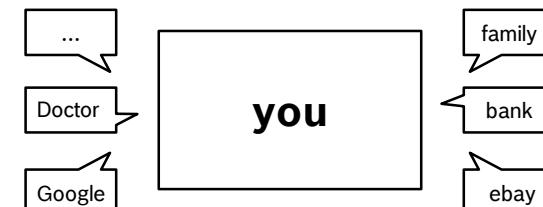
Current model of Identity

Solution

- Decentralized Digital Identity: moving the physical Identity credentials to our digital devices



- The model that truly puts the Individual at the center



Self Sovereign Identity

Self-Sovereign Identity

Status-quo: Rise of Monopolistic Platforms



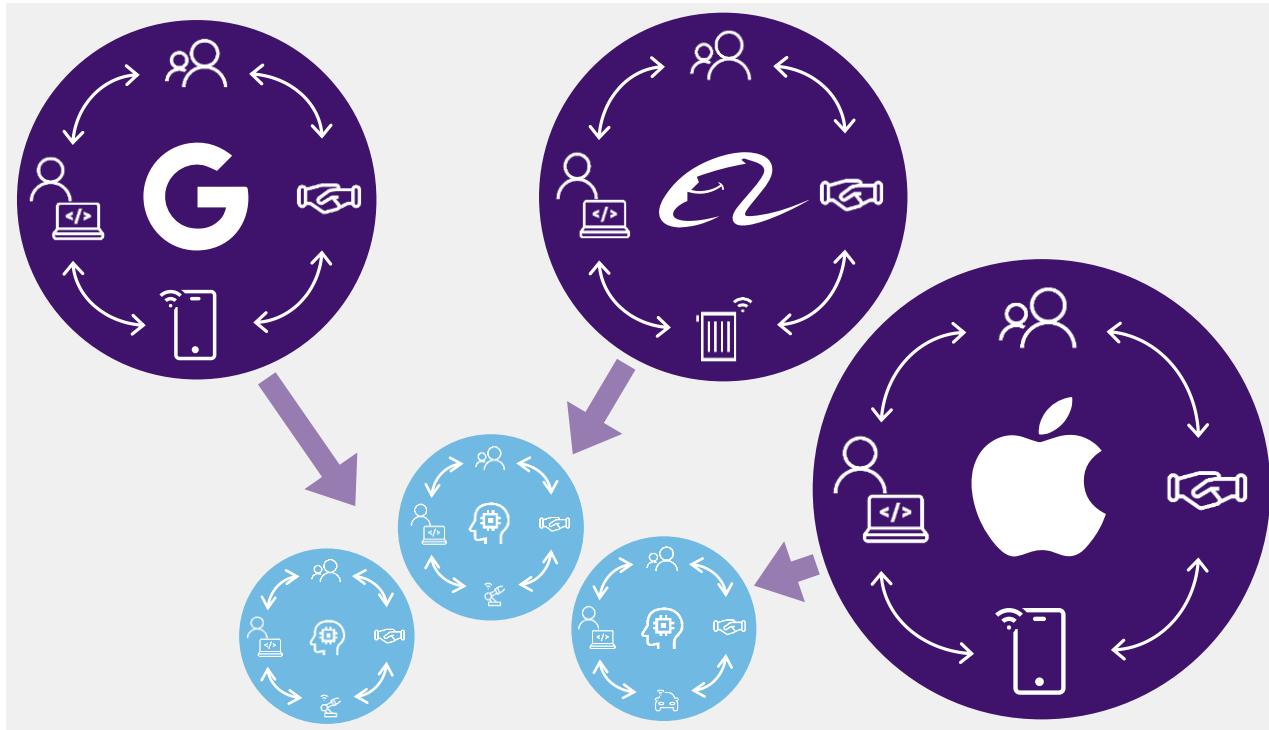
Risks

- ▶ **Monopolistic platforms regulate** an increasing share of business models through control of:
 - ▶ Distribution Channels,
 - ▶ Revenue Streams,
 - ▶ Customer Relationships
- ▶ **Hyperscalers compete with traditional companies** and leverage their power to attract new customers by subsidy of new business with traditional business

Monopolistic platforms and hyperscalers put competing market players and business models at risk.

Self-Sovereign Identity

Status-quo: Rise of Monopolistic Platforms



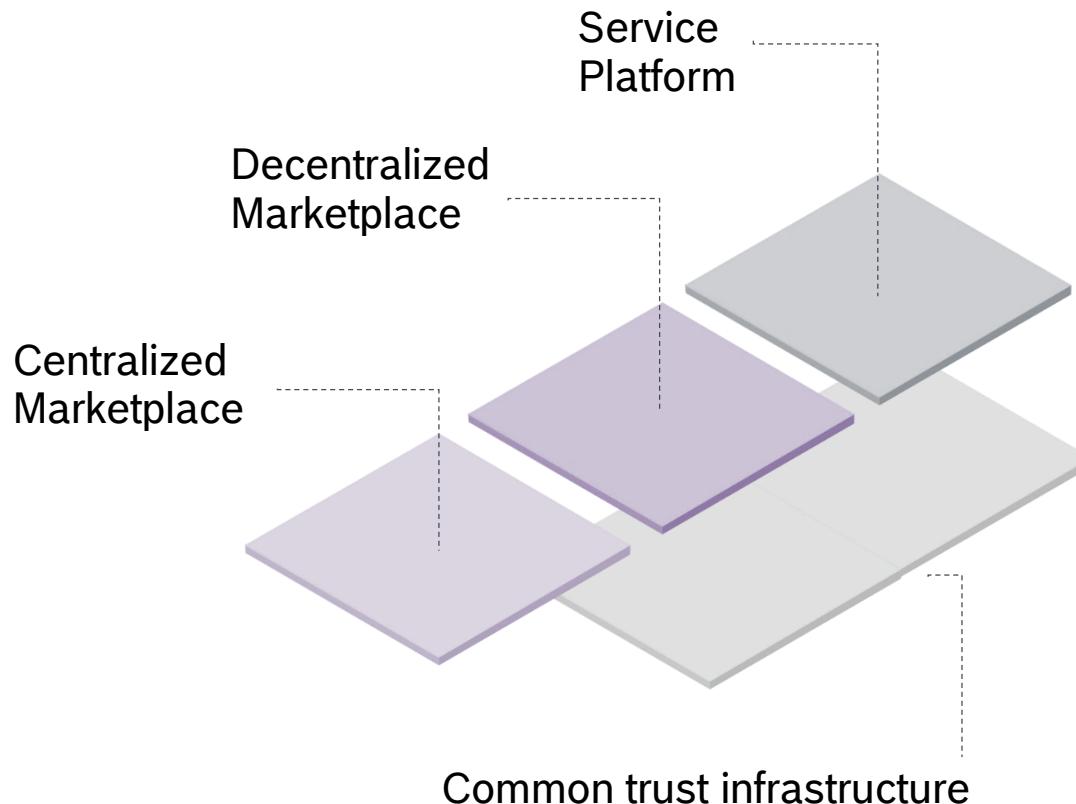
Risks

- ▶ **Monopolistic platforms regulate** an increasing share of business models through control of:
 - ▶ Distribution Channels,
 - ▶ Revenue Streams,
 - ▶ Customer Relationships
- ▶ **Hyperscalers compete with traditional companies** and leverage their power to attract new customers by subsidy of new business with traditional business

Monopolistic platforms and hyperscalers put competing market players and business models at risk.

Trust by Self-Sovereign Identity (SSI)

The Economy of Things needs a Trust Infrastructure



Decentralized Public Key Infrastructure (DPKI) (Distributed Ledger)

- ▶ Open Standards, not one platform
- ▶ Cryptographically-controlled Identifiers
- ▶ Cryptographically-verifiable Claims
- ▶ Privacy by Design

Emerging Open Standards for SSI

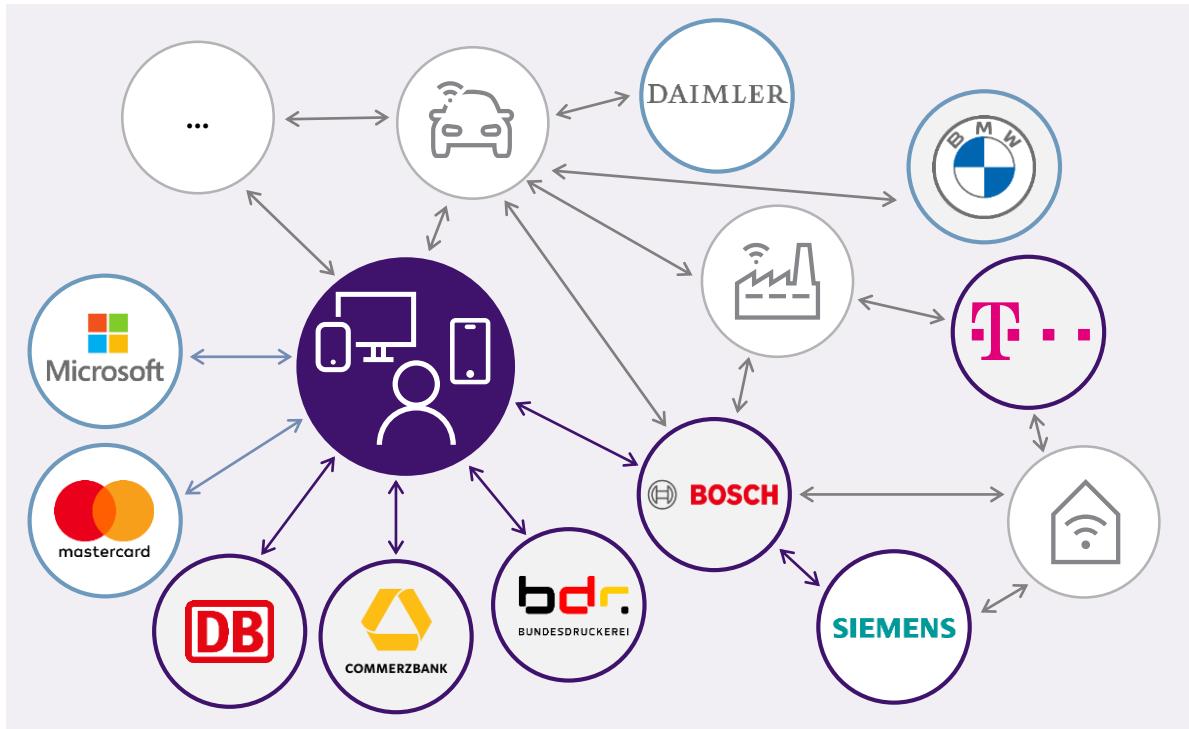
Verifiable Credentials
DID Auth
DKMS (Decentralized Key Management System)
DID (Decentralized Identifier)



Source: Drummond Reed / Evernym

SSIMeetup.org

Trust by Self-Sovereign Identity (SSI) Opportunities of an SSI Ecosystem



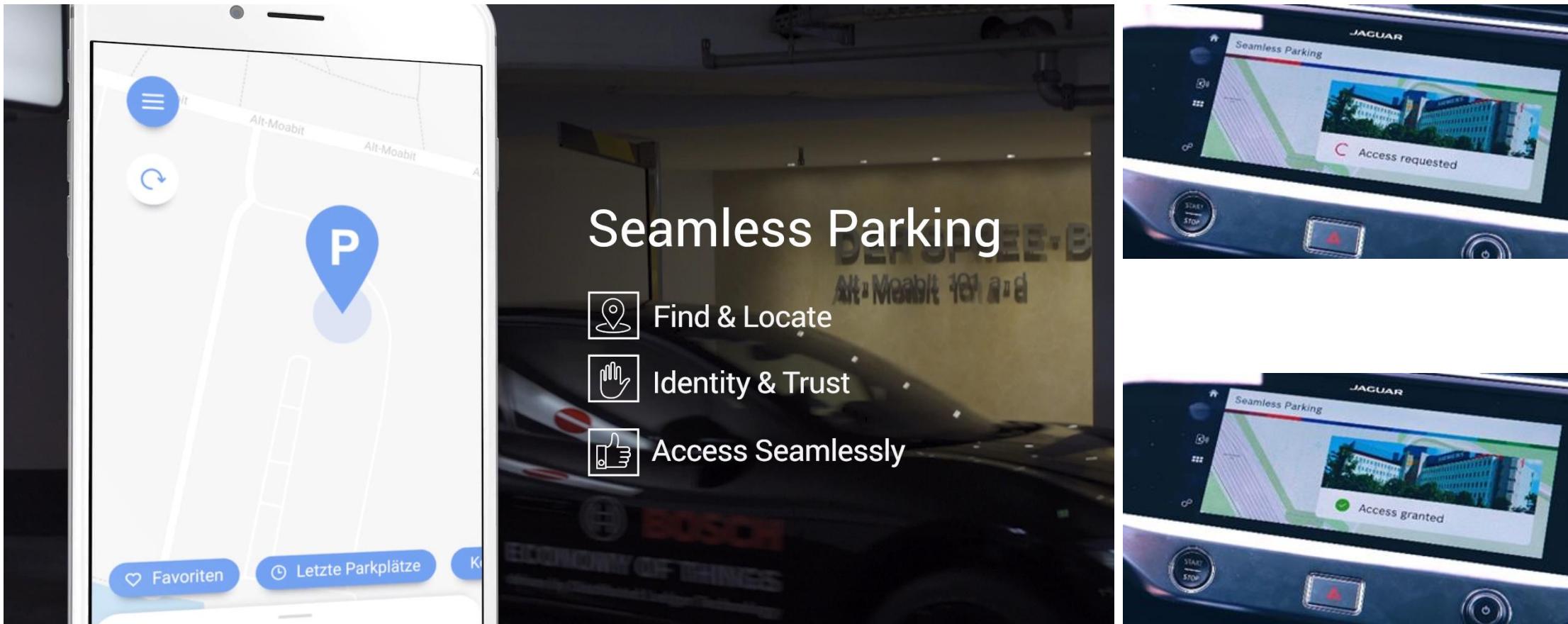
Opportunities

- ▶ Trusted digital relationships
 - ▶ Reduce risk of cybercrime by secure Authentication
 - ▶ Verifiable Credentials empower Authorization decisions allowing more automation of business processes
- ▶ Guarantees data sovereignty (GDPR)
 - ▶ Selective disclosure and consent management
- ▶ Cross-border Collaboration
 - ▶ Enable easy on-boarding of different entities to existing/new digital services and ecosystems
 - ▶ Supports different Solutions for different domains and entities (Organisation, Human, Machine)

Protects business data sovereignty and supports cross-border collaboration.

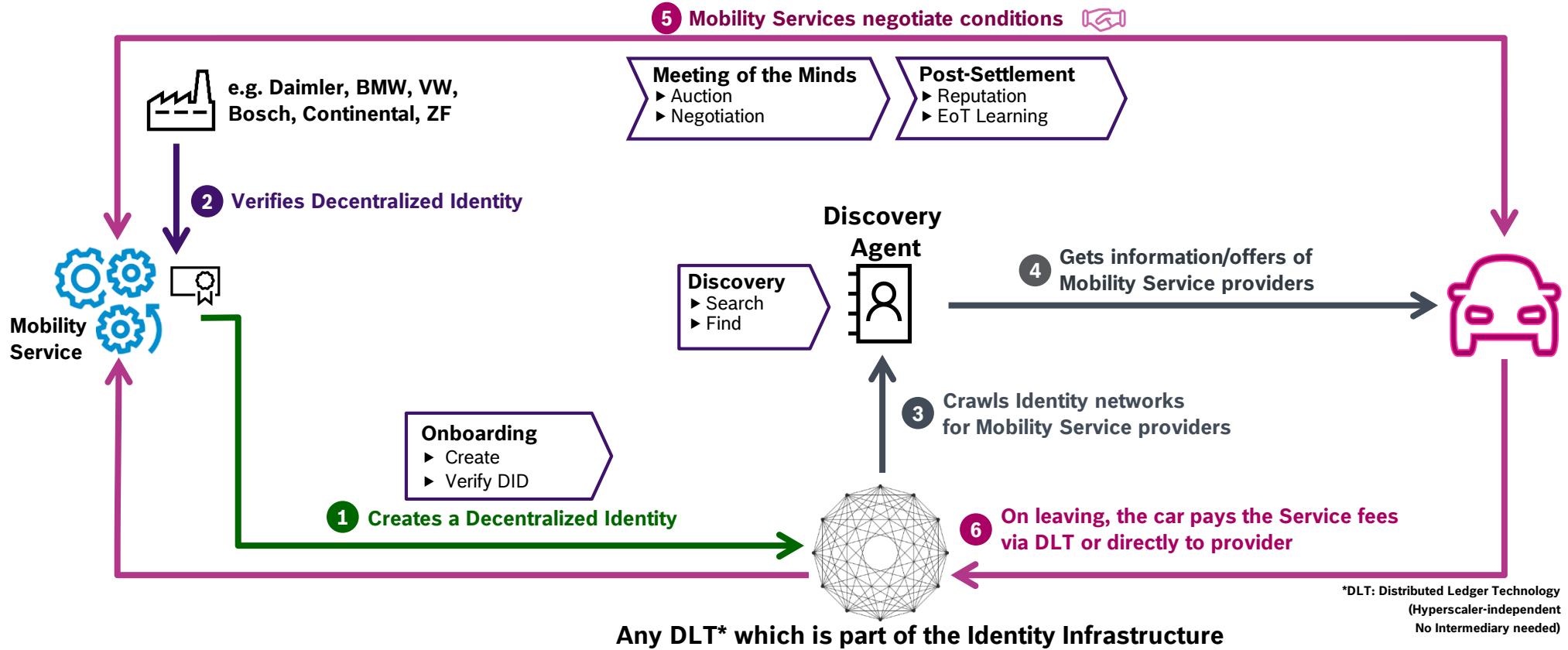
Self-Sovereign Identity Mobility Use Case

Finding Spots you never would have expected...



Seamless Mobility Services with Self-Sovereign Identity

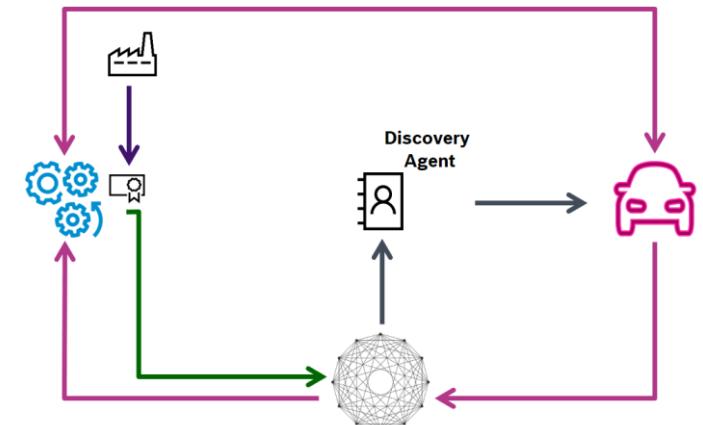
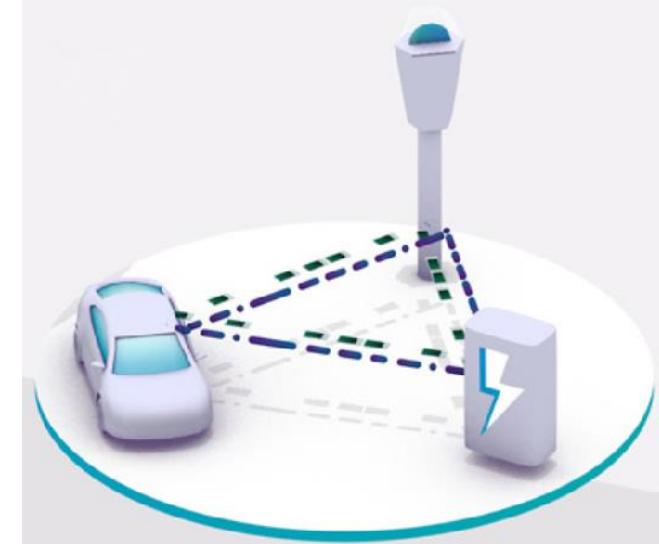
The Architecture...



Distributed Digital Identities in Mobility

Conclusion and Summary

- ▶ IoT will be the future of most industries
- ▶ Trust is the crucial concept of the IoT
- ▶ BUT: The Internet was built
WITHOUT an Identity Layer
- ▶ Decentralization is inevitable for Trust
- ▶ SSI may be one element of the Trust Infrastructure
for the IoT and Economy of Things
- ▶ We are starting to implement it in our IoT Vision



Thank YOU!



Peter Busch

Product Owner DLT Mobility

Peter.Busch@Bosch.com

@pbusch42

Blockchain Autumn School 2020

Self-Sovereign Identity in der praktischen Nutzung

Dr. André Kudra



Vorstellung esatus AG

Unser Beratungsportfolio



✓ Identity & Access



✓ Governance, Risk & Compliance



✓ IT Security



✓ Development Operations

Aktive Mitarbeit in relevanten Verbänden und Organisationen



SSI für Deutschland /
IDunion



SSI für Deutschland



Konsortialpartner



Assoziierte Partner



Ministerium für Wirtschaft, Innovation,
Digitalisierung und Energie
des Landes Nordrhein-Westfalen

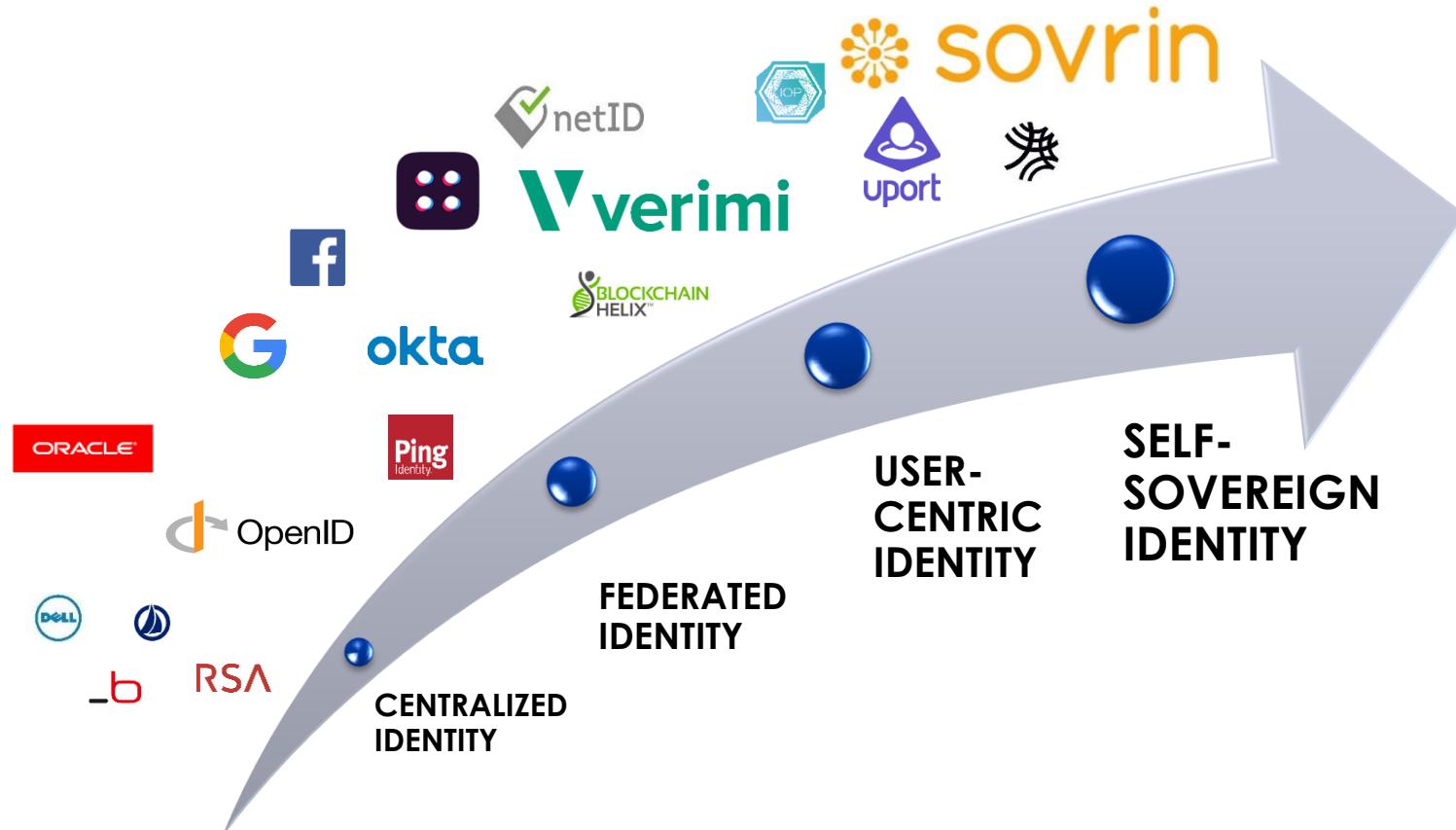


Gefördert durch:

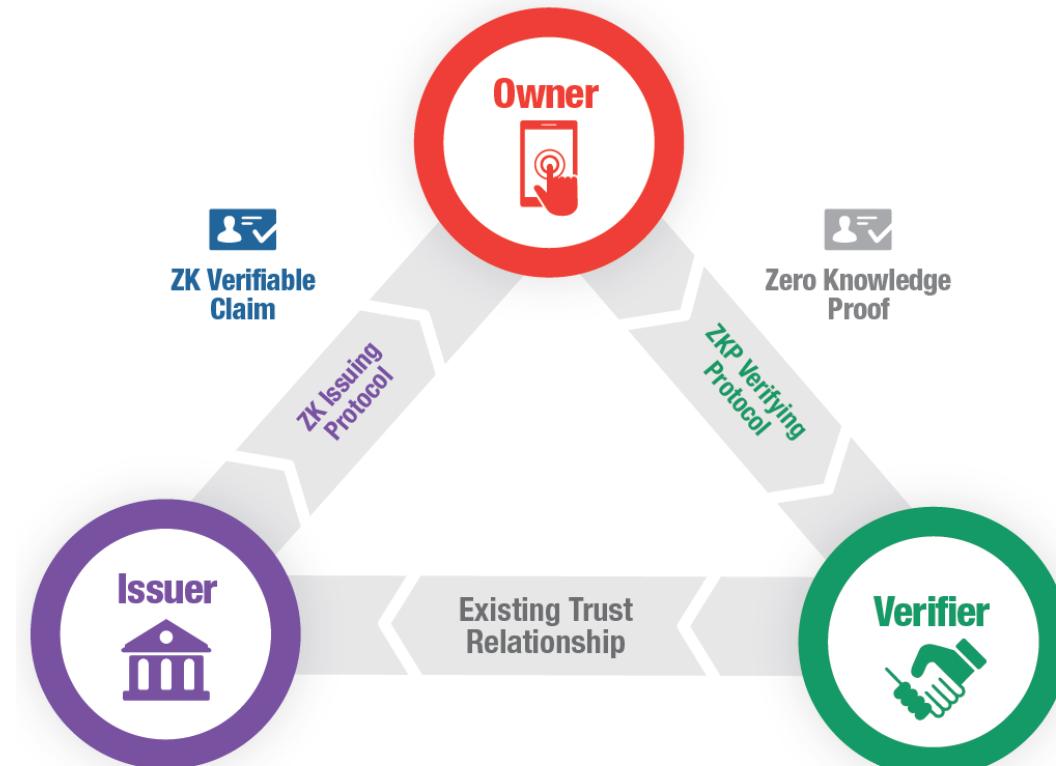


Einführung SSI

Die Entwicklung der digitalen Identität



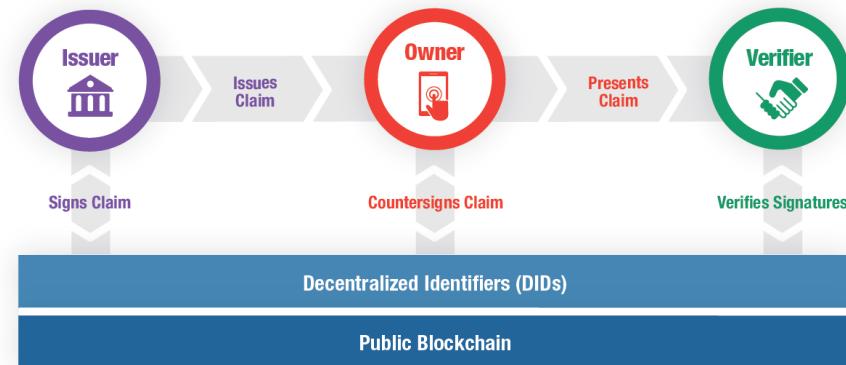
Vertrauensdreieck und Verifiable Credentials



Quelle: Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust - A White Paper from the Sovrin Foundation - Version 1.0 - January 2018

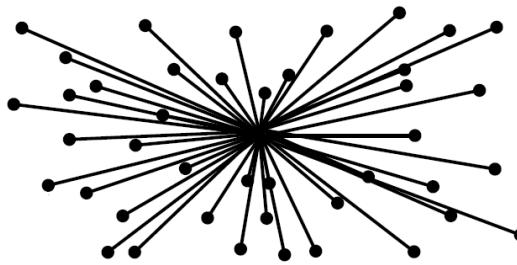
Self-Sovereign Identity, kurz SSI: Schon weit mehr als nur eine Idee

- **Konzept** einer echten selbstverwalteten und -kontrollierten digitalen Identität
- **Vertrauensnetzwerk**, das der vernetzten Welt noch immer fehlt
- **Recht auf digitale Identität** als öffentliches Gut für JEDEN
- **Technologie**, die den Nutzer in den Mittelpunkt stellt
- **Standards**, die alle relevanten Player schon jetzt verwenden „DIDs“ und „Verifiable Claims & Credentials“



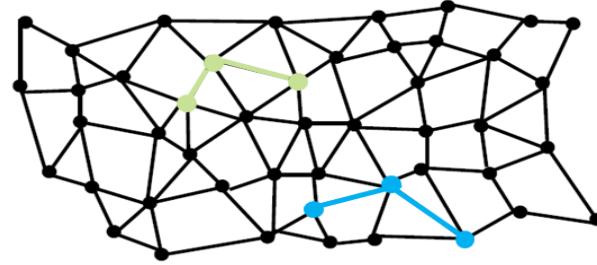
SSI löst mit Dynamik und Flexibilität zentralistische Single Points of Failure ab

Zentralistische Strukturen und technische Lösungen – wie bspw. Public Key Infrastrukturen (PKI) – lösen mit digitalen Zertifikaten spezifische funktionale Herausforderungen, insbesondere Verschlüsselung, Authentifizierung und elektronische Signatur. Dabei sind sie in der inhaltlichen Zertifikatsausgestaltung limitiert und stellen gleichzeitig einen Single Point of Failure dar. Mit der Self-Sovereign Identity tritt an deren Stelle ein flexibles und dynamisches Ökosystem, das verschiedene Anwendungsgebiete abdeckt.



Zentralistische PKI

- ➊ Standardisiertes Verfahren, globale produktive Anwendung
- ➋ Certificate Authorities (CAs) als Vertrauensdienstleister
- ➌ Regulatorische Rahmenbedingungen definiert
- ➍ Zertifikate inhaltlich fix definiert (X.509)
- ➎ Zentrale Stelle als Single Point of Failure



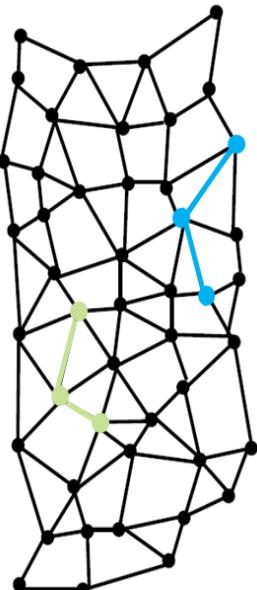
Dezentrales flexibles SSI-Netzwerk

- ➊ Jeder Teilnehmer kann Zertifikatsschemata definieren
- ➋ „Verifiable Credentials“ flexibel definier- und ausgestaltbar
- ➌ Jeder (!) kann Aussteller und Verifizierer sein
- ➍ CAs und Industriepartner bereits engagiert in SSI
- ➎ „DIDs“ als World Wide Web Consortium (W3C) Standard

SSI bietet unmittelbare Anknüpfungspunkte für aktuelle IDPs und hebt Integrationspotenziale



Der mit Self-Sovereign Identity proklamierte und praktisch realisierte Ansatz eines „Web-of-Trust“ verschafft für jeden Teilnehmer im Netzwerk unmittelbare Anknüpfungspunkte, auch und insbesondere für klassische, zentralistische Instanzen wie Certificate Authorities oder Identity Provider. Ein SSI-Ökosystem trägt dazu bei, alle Integrationspotenziale effizient und effektiv zu heben.



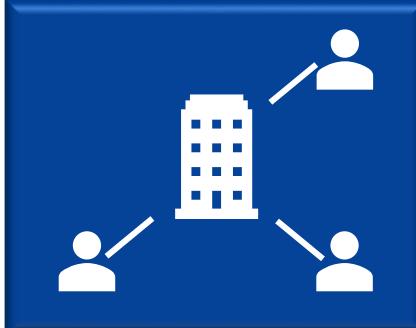
Self-Sovereign Identity

- ... ist das ideale Ökosystem zur Integration jeglicher Teilnehmer.
- ... integriert unkompliziert auch Teilnehmer, die bisher keine Interaktion hatten.
- ... liefert ein Integrationsgewebe, mit dem reale Vertrauensnetzwerke elektronisch abbildbar sind.
- ... transportiert Vertrauen und reicht es digital weiter.
- ... bietet Vertrauensdienstleistern eine Plattform für globale Diensteverbreitung (bspw. Verimi).
- ... passt sich domänen spezifischen Anforderungen flexibel an (bspw. „Know your customer“/KYC).
- ... nutzt bestehende Standards und stellt sie auf eine dezentralisierte Basis (bspw. PKI wird zur DPKI) .
- ... lässt sich leicht in gewachsene Strukturen integrieren (bspw. LDAP Berechtigungsmanagement).

SSI kompensiert die Nachteile zentralistischer Identity Provider und stärkt die Nutzerposition

	Internationale IDPs (Google, Facebook, Amazon, ...)	Lokale IDPs mit DE-Basis (Verimi, netID, id4me, ...)	Self-Sovereign Identity (Sovrin, uPort, Blockstack, ...)
Komfort	↑ Fast jeder Anwender nutzt Dienste bereits	↓ Anwender muss erst aufspringen	↓ Anwender muss erst aufspringen
Nutzungsraum	↑ Global	↓ Lokal (DE/EU)	↑ Global
Empowerment	↓ Anwender hat kaum Einfluss	↓ Anwender hat nur mittelbar Kontrolle	↑ Anwender hat vollständige Kontrolle
Datenablage	↓ Zentral bei IDP	↓ Zentral bei IDP (innerhalb EU)	↑ Ausschließlich beim Anwender
Skalierbarkeit	↑ Enorme Kapazitäten verfügbar	↑ Gegeben	↑ Design für globale Nutzung
Sicherheit	↓ Erfolgreicher Angriff kompromittiert alles	↓ Erfolgreicher Angriff kompromittiert alles	↑ Dezentralität erschwert Angriffe massiv
Datenschutz	↓ DSGVO wird ausgehebelt	↑ DSGVO glaubwürdig eingehalten	↑ Design für DSGVO-Konformität
Standards	↑ Standards verfügbar, produktiv genutzt	↑ Standards verfügbar, produktiv genutzt	↑ Standards verfügbar, prototypisch genutzt
Vertrauen	↓ Anwender ist „ausgeliefert“	↑ Informierte Anwender vertrauen bedingt	↑ Informierte Anwender vertrauen maximal

Die Self-Sovereign Identity Mission & Vision

Lokale Use Cases umsetzen	Kritische Masse erreichen	Internationale Use Cases umsetzen
		
SSI für I&A in Unternehmen nutzbar machen.	Unternehmen und Behörden verbinden um Begeisterungsmerkmale für Interessierte bereitzustellen.	Skalierung und kontinuierliche Verbesserung.

Status Quo Self-Sovereign Identity (SSI) – Beispiele internationaler Vorhaben und Projekte



- BMWi Förderaufruf Sichere Digitale IDs



- govdigital (Zusammenschluss öffentlicher IT-Dienstleister)
- SSI für Deutschland

- EMIL

- Digitales Corona Gesundheitszertifikat
- 5 Sovrin Stewards



- 5 Sovrin Stewards



- myIDsafe (SSI)
- 2 Sovrin Stewards



- uPort / Ethereum Foundation Zug
- 5 Sovrin Stewards



- SSI-Projekt mit Banken via Dutch Blockchain Coalition
- 5 Sovrin Stewards



- Sovrin-Credentials für Unternehmen, öffentliches Unternehmensregister
- Beantragung und Verwaltung von Zulassungen und Lizenzen
- 2 Sovrin Stewards



- EBSI eSSIF
- INATBA
- ID2020
- 25 Sovrin Stewards

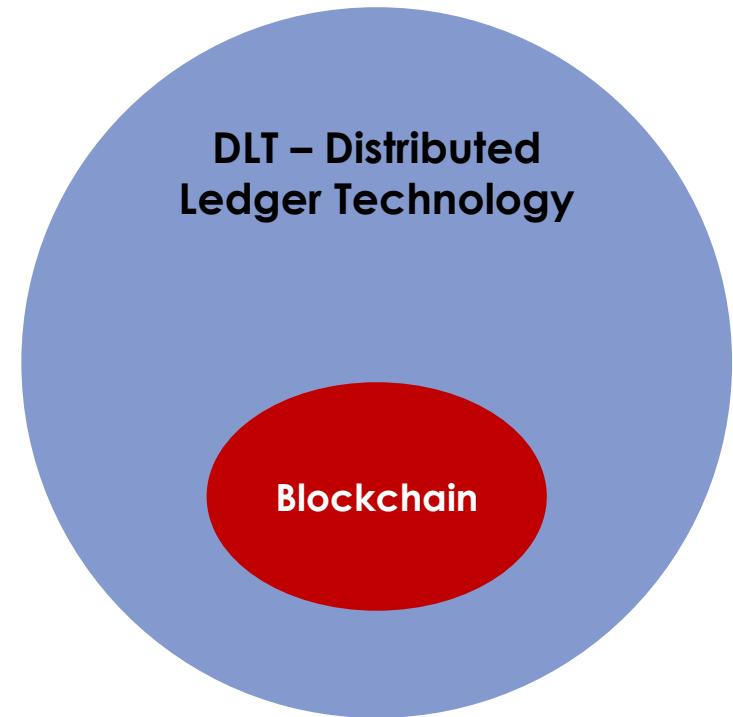


- Sovrin Network
- Trust over IP Foundation
- Covid Credentials Initiative (CCI)
- GLEIF Pilotprojekt (Organization Wallets)
- ~80 Sovrin Stewards

Blockchain Technologie

Nutzung der Distributed Ledger Technology für digitale Identitäten

- Dezentralisiertes Ledger
- Transaktionen bestätigt durch Konsens-Algorithmus
- Teilnehmer sind Nodes / Nutzer / Miner
- Alle Informationen befinden sich auf allen Nodes
- Integrität wird durch Verkettung sichergestellt
- Authentizität durch asymmetrische Verschlüsselung
- Technische Durchsetzung der CIA-Triade:
Confidentiality | Integrity | Availability
Vertraulichkeit | Integrität | Verfügbarkeit
- Geeignet für Kryptowährungen, Supply Chains, Nachverfolgungen und **digitale Identitäten!**



Blockchains sind nicht immer gleich: Öffentliches vs. Privates Blockchain-Netzwerk

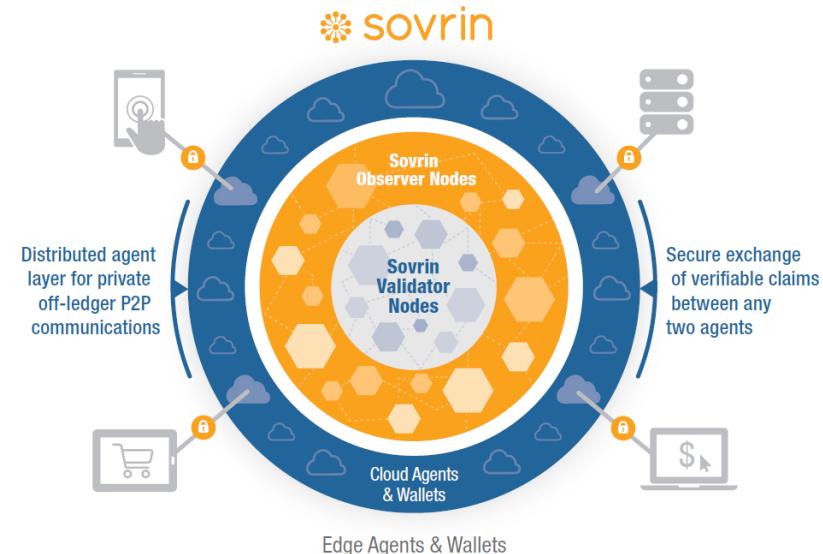
- ✓ Robustheit
 - ✓ Teure Angriffe
 - ✓ Transparenz
 - ✗ Träge Änderungen
 - ✗ Langsamer Konsens
-
- ✗ Kein sinnvolles Anwendungsszenario

		Wer kann validieren?	
		Permissionless	Permissioned
Wer hat Zugriff?	Public	„Jeder darf lesen und validieren“  https://bitcoin.org	„Jeder darf lesen, nur Berechtigte validieren“  https://sovrin.org
	Private	„Nur Berechtigte dürfen lesen, jeder darf validieren“	„Nur Berechtigte dürfen lesen und validieren“  https://www.corda.net

- ✓ Robustheit
 - ✓ Berechtigungen
 - ✓ Transparenz
 - ✓ Schneller Konsens
 - ✓ Rollback möglich
 - ✗ Missbrauch möglich
-
- ✓ Berechtigungen
 - ✓ Schneller Konsens
 - ✓ Rollback möglich
 - ✗ Missbrauch möglich
 - ✗ Erprobtere Datenbanken

Beispiel Sovrin: Modell für Self-Sovereign Identity & dezentralisiertes Vertrauen

- Globales DLT-basiertes Identitätsnetzwerk
- Nutzt dezentralisierte Identifikatoren (DIDs)
- Schneller und energiesparender Konsens (RBFT: Redundant Byzantine Fault Tolerance)
- Verwaltet durch Non-Profit-Organisation
- Diverse „Stewards“ verpflichten sich zu einem Trust Framework und betreiben die Nodes
- Cross-funktional mit anderen Identity Chains
- Open Source Softwarebasis
- Teil von Hyperledger Indy



Quelle: Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust - A White Paper from the Sovrin Foundation - Version 1.0 - January 2018

Methoden der Konsensfindung: PoX etc.

Proof-of-Work (PoW)

Proof-of-Stake (PoS)



Kryptographisches Rätsel – Wettlauf um einen Hashwert mit automatischer Anpassung des Schwierigkeitsgrades



Verwandt mit PoW, gewichtete Zufallsauswahl des Validierers, ausschlaggebend ist der „Stake“ eines Nutzers, also der Anteil an der gesamten Menge an Token, die er besitzt

Byzantine Fault Tolerance (BFT) Familie

Redundant BFT / Plenum

Proof-of-Authority (PoA)



Redundantes Protokoll für Maschinenreplikation mit eingebauter Toleranz für willkürlich auftretende Fehler – DLT, nicht Blockchain



Alternative zu Proof-of-Stake, die Vertrauenswürdigkeit einer Person/Organisation statt Teilnehmer mit hohem Vermögen als Validierer für die Blockchain ist ausschlaggebend

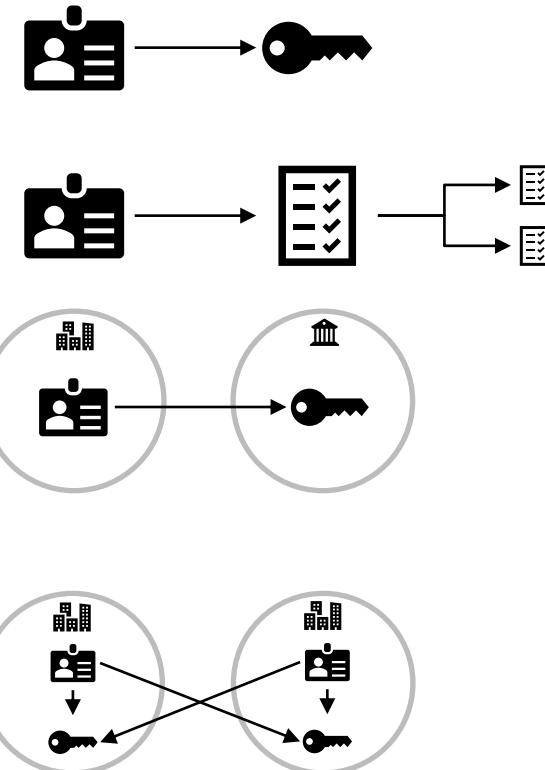
Vorstellung SeLF / Demo

SeLF Demo



Anwendungsbeispiele

- 🔒 Credentials führen zu Berechtigungen (auch physical access)
- 🔒 Credentials als Primary Source für Fakten
- 🔒 Credentials extern nutzen:
 - 🔒 Mitarbeiterangebote
 - 🔒 Nachweis des Anstellungsverhältnisses
- 🔒 Cross-Organisation Onboarding und Berechtigungsvergabe



Anbindung an Legacy und SSI-native Zielsysteme



Kompatibilitätsmatrix

	Authentication					Authorization					
	SAML	OAuth 2	OpenID Connect	SSSI-native	SAML	OAuth 2	OpenID Connect	LDAP	Active Directory	Azure AD	SSSI-native
Adobe Creative Cloud	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✗
Adobe ID Management	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✗
Alibaba Cloud Service	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
AssetSonar	✓	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗
Atlassian Confluence	\$	✓	\$	✗	\$	✓	\$	✓	✓	✓	✗
Atlassian Jira	\$	✓	\$	✗	\$	✓	\$	✓	✓	✓	✗
AuditBoard	✓	✗	✗	✗	✓	✗	✗	✗	✓	✓	✗
AWS Console	✓	✓	✓	✗	✓	✓	✗	✗	✗	✓	✗
Azure Cloud	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
Bloomberg Anywhere	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
Cisco Cloud	✓	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗
DB2	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗
Dropbox Business	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓	✗
esatus SeLF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Evernote	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓	✗
GitHub	✓	✓	✗	✗	✓	✗	✗	✓	✓	✓	✗
Google Cloud	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
Google ID Platform	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
HP Service Manager	✓	✗	✗	✗	✓	✗	✓	✓	✓	✓	✗

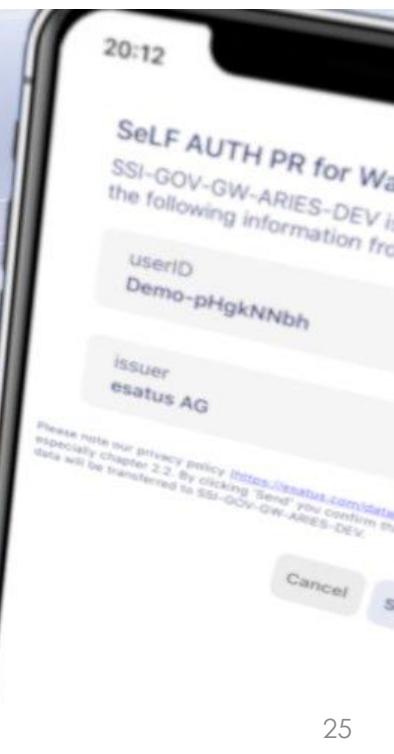
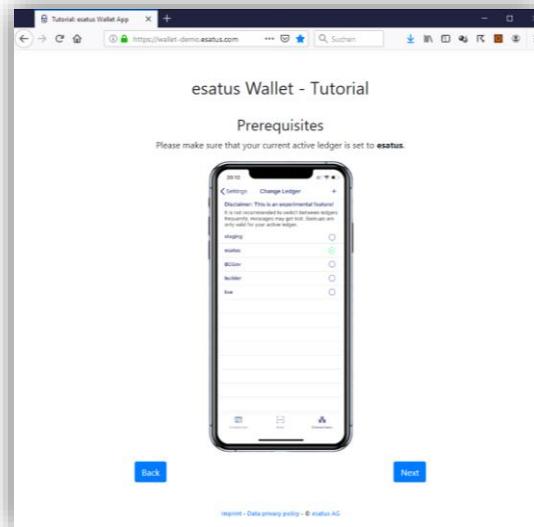
* All information is supplied without guarantee and is based on own research. ▲

	Authentication					Authorization					
	SAML	OAuth 2	OpenID Connect	SSSI-native	SAML	OAuth 2	OpenID Connect	LDAP	Active Directory	Azure AD	SSSI-native
Microfocus ALM	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗
Microsoft SQL Server	✓	✗	✗	✗	✓	✗	✗	✓	✓	✓	✗
MySQL	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Nextcloud	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
Oracle Database	✗	✓	✗	✗	✗	✓	✗	✓	✓	✓	✗
Rocket Chat	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
RSA Identity G&L	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗
Salesforce	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
SAP (various apps)	✓	✓	✗	✗	✗	✓	✗	✓	✓	✓	✗
SAP Cloud ID Platform	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗
ServiceNow	✓	✓	✗	✗	✓	✓	✗	✓	✗	✓	✗
SharePoint (local)	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Slack	✓	✗	✗	✗	✗	✓	✗	✗	✗	✓	✗
Sybase	\$	✓	✗	✗	\$	✓	✗	✓	✓	✓	✗
Trello	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗
Workday	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓	✗
Zendesk	✓	✓	✗	✗	✓	✗	✗	✓	✓	✓	✗

* All information is supplied without guarantee and is based on own research. ▲

Selbst ausprobieren?

<https://wallet-demo.esatus.com>



esatus SeLF Rollout



A screenshot of a whitepaper titled "How to Launch Self-Sovereign Identity Technology for Corporate IT Access". The page includes a header with the title, a bio for Dr. Achim Krämer, a call-to-action button "Klik hier voor SSI I&A", and a section titled "Jumping into practical SSI applications". The content discusses the development of a credential-based Identity & Access solution called SeLF, its integration with various partners like Hypersign, and its use in corporate environments. It also mentions the creation of a native mobile app for SSI access control.



https://esatus.com/files/whitepapers/esatus_SSI_Roll-out.pdf

<https://www.youtube.com/watch?v=WBiLpRK6PRU>



self-ssi.com



@esatus_SeLF



@esatuzzself

Fragen & Antworten



Ansprechpartner



CIO esatus AG

Dr. André Kudra

Tel.: +49 6103 90295-0

a.kudra@esatus.com

esatus AG | www.esatus.com

Copyright



Copyright © 2020 esatus AG. Alle Rechte vorbehalten

Alle Inhalte, Fotos und Grafiken sind urheberrechtlich geschützt. Sämtliche Teile dieses Dokuments dürfen nicht ohne vorherige schriftliche Genehmigung durch die esatus AG weder ganz noch auszugsweise kopiert, vervielfältigt, verändert oder übertragen werden.

Herausgeber: esatus AG

Copyright Fotos: Tomasz Zajda/Fotolia; bismillah_bd/Fotolia;
tostphoto/Fotolia; envfx/Fotolia



Self-sovereign Identity

Ideologie, Paradigma, Standards und aktuelle Entwicklungen

Christoph Menzer
Fakultät CB | BCCM

30. September 2020

Digitale Identität

Ansätze des Identitätsmanagements

Self-sovereign Identity

Definition, Prinzipien, Ideologie
Standards und Initiativen

Decentralized Identifiers (DIDs)

Architektur
DID-Document
DID-Method
DID-Resolution
Authentifizierung

Verifiable Credentials

Claims
Credentials
Presentations
Lebenszyklus
Anti-Korrelation

Literatur

Eine digitale Identität ist eine Sammlung elektronischer Daten zur Charakterisierung eines Internetnutzers mit einer physischen Identität.

Daten, die zu einer digitalen Identität gehören, sind z.B.:

- ▶ Nutzernname
- ▶ E-Mail-Adresse
- ▶ Wohnanschrift
- ▶ Kontonummer
- ▶ Passwort

(Tietz u. a. 2017, S. 13)

- ▶ jene Daten werden als Attribute bezeichnet
- ▶ ein physischer Nutzer kann sich im Internet mit vielen verschiedenen digitalen Identitäten bewegen (anderer Nutzernname, andere E-Mail usw.)
- ▶ es gibt verschiedene Rollen, z.B. „privat“, „staatlich“ und „geschäftlich“

Authentifizierung

- ▶ Bindung an den jeweiligen physischen Nutzer muss sichergestellt werden
- ▶ die Überprüfung findet in Form eines Anmeldeprozesses (Login) statt
- ▶ der Nutzer muss beweisen, dass er Besitzer einer digitalen Identität ist, d.h., er muss sich *authentifizieren*
- ▶ Passwörter, PIN, Fingerabdruck, Gesichtserkennung, Chipkarten usw.

(Tietz u. a. 2017, S. 13)

- ▶ isoliertes Identitätsmanagement
 - jeder Dienst verwaltet seine Nutzer selbst
 - am weitesten im Internet verbreitet
- ▶ zentralisiertes Identitätsmanagement
 - zentrale Einheit, die Nutzer verwaltet und Anmeldeprofile speichert, die andere Einheiten abrufen können
 - auch als Identitätsprovider (IdP) bezeichnet
 - z.B. Social-Logins, LDAP, Active Directory

(Tietz u. a. 2017, S. 13)

- ▶ dezentralisiertes Identitätsmanagement
 - mehrere Identitätsprovider, die benutzt werden können
 - der Dienst muss den Identitätsprovider im Vorfeld nicht kennen (Auflösung durch URL), jedoch auf seine Aussage vertrauen
 - z.B. OpenID
- ▶ föderiertes (federated) Identitätsmanagement
 - Föderation bzw. einen Vertrauenskreis (Circle of Trust) von Diensten und Identitätsprovidern, die gegenseitig ihren Identitätsinformationen vertrauen
 - z.B. WS-Federation, Kantara Initiative

(Tietz u. a. 2017, S. 13)

Self-sovereign Identity

Definition, Prinzipien, Ideologie

- ▶ Self-sovereign Identity (SSI, dt. Selbst-souveräne Identität)
- ▶ Modell für digitale Identitäten, bei dem der Nutzer einer Identität in die Lage versetzt wird, alle Handlungen und Informationen bezüglich seiner Identität selbst zu verwalten
- ▶ Über eine genaue Definition, was SSI ausmacht, herrscht noch kein Konsens
- ▶ Einen ersten allgemeingültigen Definitionsversuch unter Aufstellung von zehn Prinzipien, die diese auszeichnen, gibt Christopher Allen in seinem Blogpost „The Path to Self-Sovereign Identity“ (Allen 2016)

Prinzipien nach Allen (2016) I

Existence (Existenz) jeder Nutzer hat eine unabhängige Existenz, d.h eine SSI basiert auf einer realen/physischen Persönlichkeit und kann nicht ausschließlich in der digitalen Welt existieren.

Control (Kontrolle) jeder Nutzer sollte die alleinige Kontrolle über seine Identität haben.

Access (Zugriff) der Nutzer sollte zu jeder Zeit uneingeschränkten Zugriff zu seinen Daten haben. Das heißt allerdings nicht, dass der Nutzer seine Daten jederzeit bearbeiten kann.

Transparency (Transparenz) die Algorithmen, über die Identitäten verwaltet werden, müssen frei und quelloffen und weitestgehend unabhängig von speziellen Systemarchitekturen sein. Ähnliches gilt für die Netzwerke, die zur Identitätsverwaltung genutzt werden.

Self-sovereign Identity

Definition, Prinzipien, Ideologie

Prinzipien nach Allen (2016) II

Persistence (Persistenz) Identitäten sollten für immer, oder wenigstens so lange, wie der Nutzer es wünscht, gültig sein.

Portability (Portabilität) Identitäten sollten nicht an ein bestimmtes Netzwerk gebunden sein.

Interoperability (Interoperabilität) Identitäten sollten wenn möglich überall, d.h. über Landesgrenzen und Grenzen digitaler Systeme hinweg, nutzbar sein.

Consent (Zustimmung) jede Freigabe von persönlichen Informationen gegenüber Dritten erfordert die Zustimmung des Nutzers.

Prinzipien nach Allen (2016) III

Minimalization (Minimalismus) es sollte möglich sein, nur Informationen freizugeben, die unbedingt notwendig sind. Typisches Beispiel ist der Nachweis eines bestimmten Alters. Wenn nur gefragt ist, ob man älter als 18 Jahre alt ist, sollte auch nur diese Information zur Verfügung gestellt werden und nicht etwa das genaue Alter oder gar das Geburtsdatum.

Protection (Schutz) die Freiheiten und Rechte eines Nutzers wiegen höher als die Interessen des Identitätsnetzwerkes und sollten geschützt werden.

Self-sovereign Identity

Definition, Prinzipien, Ideologie

- ▶ weiterer Ansatz: „A Technology-Free Definition of Self-Sovereign Identity“ von Andrieu (2016)
- ▶ Blockchain Bundesverband (Kai Wagner u. a. 2018, S. 5):

We use the terminology of SSI, as an identity model that allows an individual or entity to have sole control of their digital identity expressed through the use of one or more decentralised identifiers or “DIDs.”

...

Self-sovereign Identity

Standards und Initiativen

- ▶ W3C Working Draft: *Decentralized Identifiers (DIDs) v1.0* (2019)
- ▶ Draft Community Group Report: *Decentralized Identifier Resolution (DID Resolution) v0.2* (2019)
- ▶ W3C Recommendation: *Verifiable Credentials Data Model 1.0* (2019)

- ▶ Decentralized Identity Foundation (DIF)
- ▶ Internet Identity Workshop (IIW)
- ▶ Rebooting Web-of-Trust (RWOT) Design Workshop
- ▶ SSI Meetup
- ▶ International Organization for Standardization (ISO)
- ▶ ID2020 Alliance
- ▶ Blockchain-Bundesverband

Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, „self-sovereign“ digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority.

Beispiel

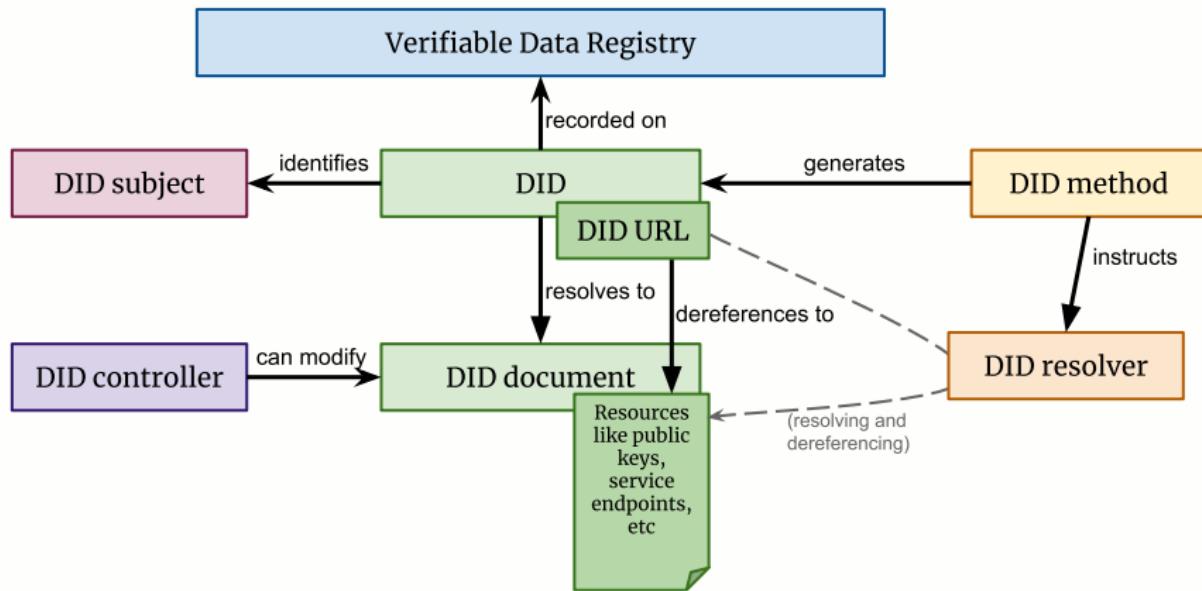
did:example:123456789abcdefghi

- ▶ eine DID besteht aus Schema:Methode:Identifier
- ▶ an eine DID ist ein DID Document gebunden
- ▶ DID enthält aufgrund der Methode bereits Routing-Informationen, damit ist sie an eine bestimmte *Verifiable Data Registry* gebunden
- ▶ Ähnlichkeit zur E-Mail-Adresse: 123456789abcdefghi@example.did
- ▶ in vielen DID-Methoden enthält der DID-Suffix kryptografisches Material (z.B. den Hash eines Öffentlichen Schlüssels)

(*Decentralized Identifiers (DIDs) v1.0 2019*)

Decentralized Identifiers (DIDs)

Architektur



(*Decentralized Identifiers (DIDs) v1.0 2019*)

Decentralized Identifiers (DIDs)

DID-Dокумент

A DID document is the resource that is **associated with** a decentralized identifier (DID). DID documents typically express **verification methods** (such as public keys) and **services** that can be used to interact with a DID controller.

- ▶ Context
- ▶ Subject
- ▶ Public Keys
- ▶ Authentication
- ▶ Authorization and Delegation
- ▶ Service Endpoints
- ▶ Created
- ▶ Updated
- ▶ Proof
- ▶ Extensibility

(Decentralized Identifiers (DIDs) v1.0 2019)

Decentralized Identifiers (DIDs)

DID-Documents

**Das DID-Document sollte/darf keine persönlichen Informationen
(personally identifiable information, PII) enthalten!**

Decentralized Identifiers (DIDs)

DID-Method

Schemas

- ▶ Die Methodenspezifikation muss genau ein bestimmtes DID-Schema definieren
- ▶ sie muss durch genau einen Methodennamen identifiziert werden können
- ▶ die DID-Methodenspezifikation für das spezifische DID-Schema muss angeben, wie die methodenspezifische ID-Komponente einer DID zu erzeugen ist
- ▶ dafür bedarf es keines zentralen Registrierungsdienstes

Operationen

- ▶ Erstellen (create)
- ▶ Aktualisieren (update)
- ▶ Abrufen (read/verify)
- ▶ Deaktivieren (deactivate)

(Decentralized Identifiers (DIDs) v1.0 2019)

Decentralized Identifiers (DIDs)

DID-Method

A DID method specification **MUST define exactly one method-specific DID scheme**, identified by exactly one method name. For more information, see the method-name rule in Section § 5.1 Generic DID Syntax.

The DID method specification for the method-specific DID scheme **MUST specify how to generate the method-specific-id component of a DID**.

The method-specific-id value **MUST** be able to be generated **without** the use of a **centralized registry service**.

(Decentralized Identifiers (DIDs) v1.0 2019)

Decentralized Identifiers (DIDs)

DID-Method

- ▶ der Methodename sollte eindeutig sein
- ▶ keine zentrale Behörde für die Zuweisung oder Genehmigung von DID-Methodennamen
- ▶ Die W3C Credentials Community Group führt eine nicht autorisierende Liste bekannter DID-Methodennamen
- ▶ mehr als 70 solcher Methoden bisher gelistet

Decentralized Identifiers (DIDs)

DID-Method

DID Method Registry

A registry for Decentralized Identifier Methods



Draft Community Group Report 17 January 2020

Latest editor's draft:

<https://w3c-ccg.github.io/did-method-registry/>

Editors:

[Manu Sporny](#) ([Digital Bazaar](#))
[Drummond Reed](#) ([Evernym](#))

Author:

[Credentials Community Group \(W3C\)](#)

Participate:

[GitHub w3c-ccg/did-method-registry](#)
[File a bug](#)
[Commit history](#)
[Pull requests](#)

Copyright © 2020 the Contributors to the DID Method Registry Specification, published by the [Credentials Community Group](#) under the [W3C Community Contributor License Agreement \(CLA\)](#). A human-readable [summary](#) is available.

(DID Method Registry 2019)

Decentralized Identifiers (DIDs)

DID-Resolution

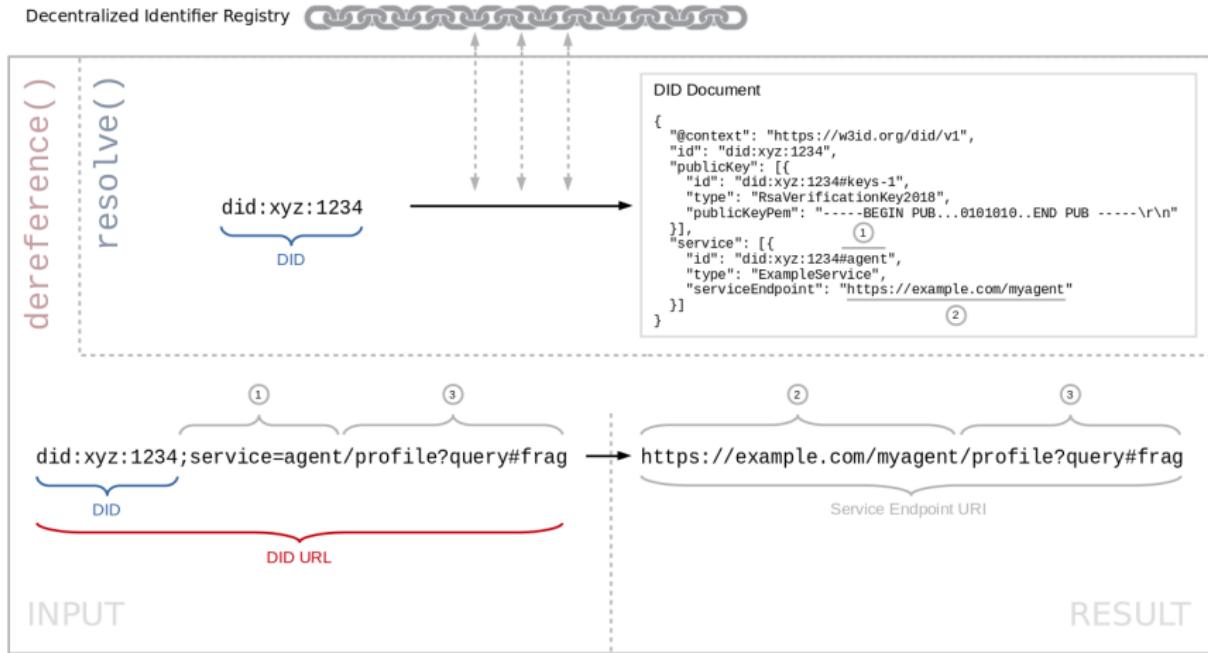
DIDs resolve to DID Documents – simple documents that describe how to use that specific DID.

- ▶ Auflösen von DIDs und Dereferenzierung von DID-URLs
- ▶ DID-Resolution ist der Prozess zur Erlangung eines DID-Dokuments für einen bestimmten DID
- ▶ DID-URL-Dereferenzierung ist der Prozess des Abrufs einer Repräsentation einer Ressource für eine bestimmte DID-URL
- ▶ Die Algorithmen müssen von einem konformen DID-Resolver implementiert werden.

(Decentralized Identifier Resolution (DID Resolution) v0.2 2019)

Decentralized Identifiers (DIDs)

DID Resolution



(Decentralized Identifier Resolution (DID Resolution) v0.2 2019)

Decentralized Identifiers (DIDs)

DID Resolution

*Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; **it can't be locked down to one site or locale.***

- Christopher Allen -

(vgl. Kai Wagner u. a. 2018)

Decentralized Identifiers (DIDs)

DID Resolution

*Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating user autonomy. To accomplish this, a self-sovereign identity must be transportable; **it can't be locked down to one site or locale.***

- Christopher Allen -

(vgl. Kai Wagner u. a. 2018)

Widerspruch?

Decentralized Identifiers (DIDs)

Authentifizierung

Was „verankert“ die Verifiable Data Registry eigentlich?

- ▶ sie stellt in erster Linie die Verbindung zwischen Identifier und Öffentlichen Schlüssel(n) her
- ▶ vgl. Zertifikat (z.B. x.509, PGP) und DID-Document

Wozu brauche ich das?

- ▶ die Öffentlichen Schlüssel für einen Identifier können sich im Laufe der Zeit ändern (Verlust, Diebstahl etc.)
- ▶ z.T. werden verschiedene Öffentliche Schlüssel für Signaturen und/oder zur Verschlüsselung benötigt
- ▶ nützliche Erweiterungen: z.B. Service Endpoints

- ▶ für Blockchains, die den *Elliptic Curve Digital Signature Algorithm (ECDSA)* verwenden, gilt: Transaktionen haben kein from-Feld, da sich der Öffentliche Schlüssel aus der Signatur berechnen lässt

Signature Prefix Value (v) und Public Key Recovery I

- ▶ Signatur besteht aus r (x-Koordinate) und s (Signatur)
- ▶ aus r können wir zwei Punkte auf der Kurve R und R' berechnen (Symmetrie zur X-Achse)
- ▶ r hat außerdem ein multiplikatives Inverses r^{-1}
- ▶ wir ermitteln weiterhin z , was das n -niedrigste Bit des Hashes der Nachricht ist, wobei n die Ordnung der Kurve ist

(Antonopoulos und Wood 2018, S. 120 ff.)

Signature Prefix Value (v) und Public Key Recovery II

- die möglichen Schlüssel berechnen sich dann aus

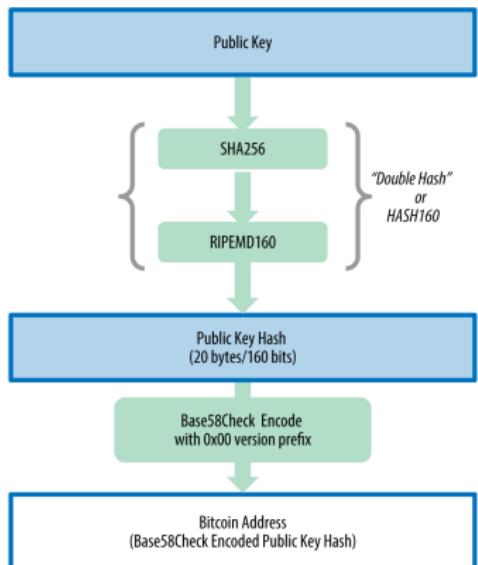
$$K_1 = r^{-1}(sR - zG) \text{ und } K_2 = r^{-1}(sR' - zG)$$

- G ist der Generator-Punkt der Kurve
- um nicht jedes Mal ausprobieren zu müssen, wurde zusätzlich zur Signatur der Prefix v eingeführt
 - wenn v gerade ist, dann ist R korrekt
 - wenn v ungerade ist, dann ist R' korrekt

(Antonopoulos und Wood 2018, S. 120 ff.)

Exkurs: Bitcoin-Adressen

Public Key to Bitcoin Address



- ▶ Bitcoin- oder ähnliche Adressen sind grundlegend ebenfalls Identifier

(Antonopoulos 2015, S. 72)

Decentralized Identifiers (DIDs)

Authentifizierung

- ▶ dieser Mechanismus lässt sich prinzipiell auch ohne eine Verifiable Data Registry zur Authentifizierung nutzen

Problem

- ▶ der Zusammenhang zwischen Öffentlichem Schlüssel und Identifier ist fix

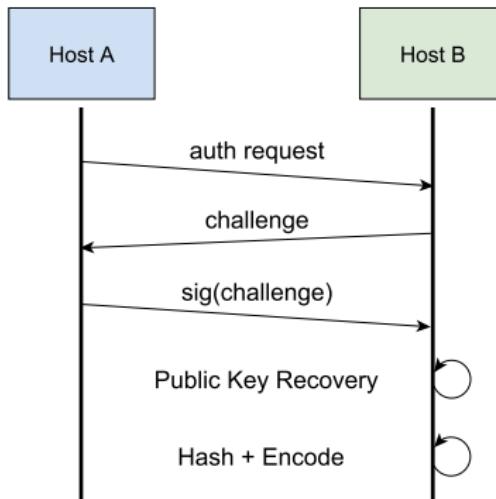
Lösungen

- ▶ sehr geschickt: BTCR-Methode (*BTCR DID Method 2019*)
- ▶ sehr flexibel: ETHR-Methode / *ERC-1056 (2018)*
- ▶ 2nd-Layer: Sidetree
- ▶ ohne Blockchain: Key Event Receipt Infrastructure (KERI, Smith 2019), Peer-DID (*Peer DID Method Specification 2020*)
- ▶ u.v.m.

Decentralized Identifiers (DIDs)

Authentifizierung

- ▶ einfache Authentifizierung mit Bitcoin- oder ähnlichen Adressen/Identifiern (u.a. DIDAuth)



Problem

- ▶ nicht resistent gegenüber *Men-in-the-Middle-Angriffen*

Lösungen

- ▶ DIDComm / DID Exchange (Aries RFC 0434, Aries RFC 0023)
- ▶ TLS (ungünstig)
- ▶ Challenge verschlüsseln (Auth-Request + PubKey)
- ▶ andere Kanalsicherungen, z.B. mit Diffie-Hellman-Schlüsselaustausch o.ä.

Verifiable Credentials

Verifiable Credentials

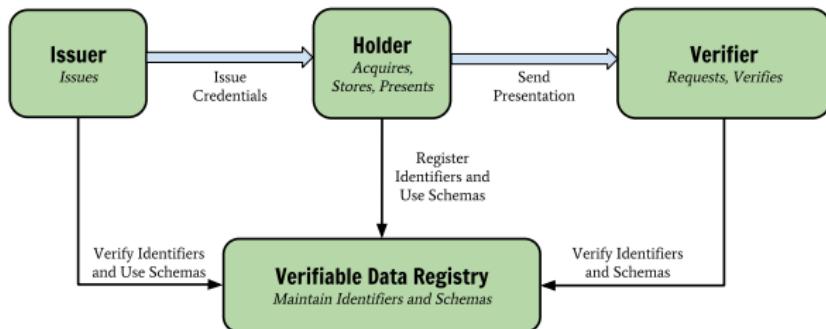
*A verifiable credential can represent all of the same information that a **physical credential** represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts.*

*Holders of verifiable credentials can generate **verifiable presentations** and then share these verifiable presentations with verifiers to prove they possess verifiable credentials with certain characteristics.*

(Verifiable Credentials Data Model 1.0 2019)

Verifiable Credentials

Rollen



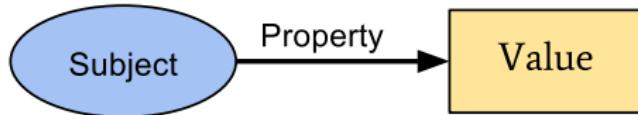
- ▶ Subject
- ▶ Holder/Owner
- ▶ Issuer
- ▶ Verifier
- ▶ Verifiable Data Registry

(*Verifiable Credentials Data Model 1.0 2019*)

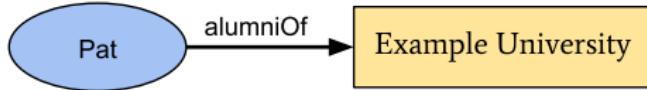
Verifiable Credentials

Claims

A *claim* is a statement about a subject. A *subject* is a thing about which claims can be made. Claims are expressed using subject-property-value relationships.



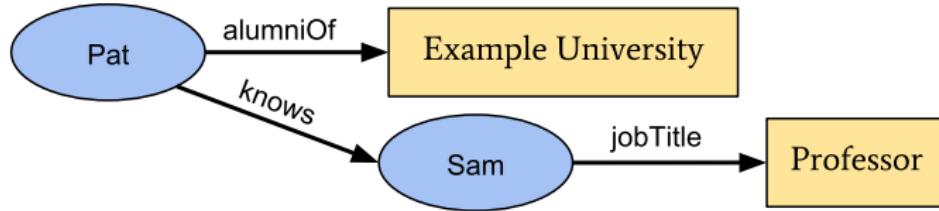
Beispiel



(*Verifiable Credentials Data Model 1.0 2019*)

Verifiable Credentials

Claims



(*Verifiable Credentials Data Model 1.0 2019*)

Verifiable Credentials

Claims

Beispiel

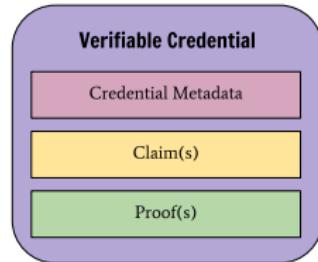
```
"alumniOf": {
    "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
    "name": [
        {
            "value": "Example University",
            "lang": "en"
        },
        {
            "value": "Exemple d'Université",
            "lang": "fr"
        }
    ]
}
```

Verifiable Credentials

Credentials

A credential is a set of one or more claims made by the same entity.

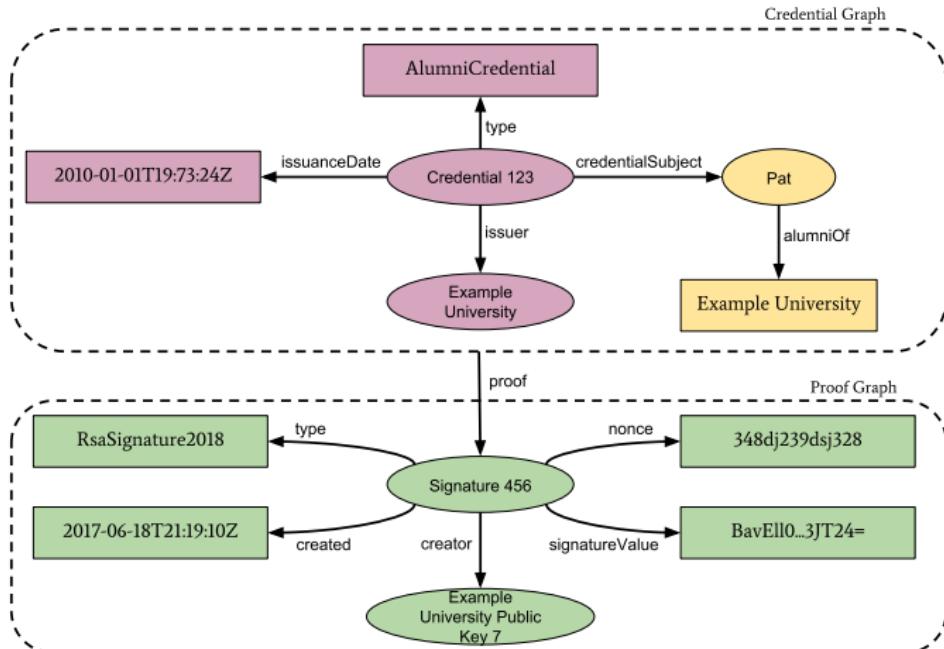
- ▶ kann auch einen Identifikator und Metadaten zur Beschreibung der Eigenschaften enthalten:
 - Ablaufdatum und -zeit
 - ein repräsentatives Bild
 - einen öffentlichen Schlüssel für Verifizierungszwecke
 - den Widerrufsmechanismus
- ▶ Metadaten können ebenfalls vom Issuer signiert sein
- ▶ manipulationssichere Claims und Metadaten, die kryptografisch belegen, wer sie ausgestellt hat



(*Verifiable Credentials Data Model 1.0 2019*)

Verifiable Credentials

Credentials



(Verifiable Credentials Data Model 1.0 2019)

Verifiable Credentials

Credentials

Beispiel

```
{  
  "issuer": "https://example.edu/issuers/565049",  
  
  "credentialSubject": {  
  
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",  
  
    "alumniOf": {  
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",  
      "name": [{  
        "value": "Example University",  
        "lang": "en"  
      }, {  
        "value": "Exemple d'Université",  
        "lang": "fr"  
      }]  
    },  
    "proof": {  
      ...  
    }  
  }  
}
```

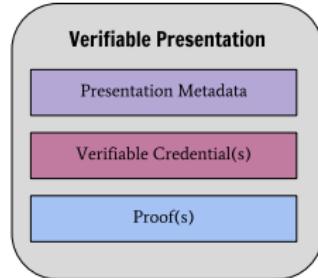
Verifiable Credentials

Presentations

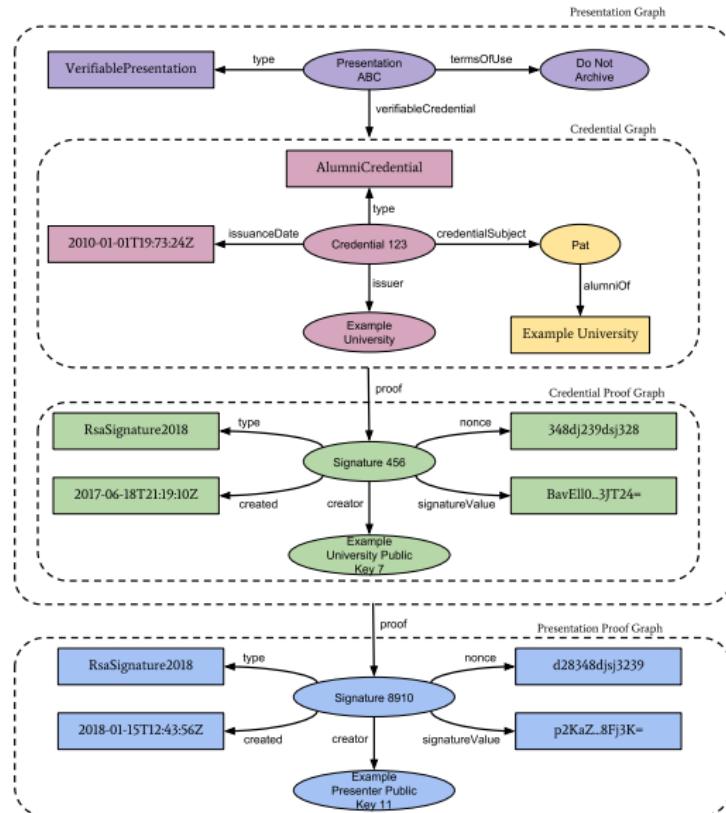


A verifiable presentation expresses data from one or more verifiable credentials, and is packaged in such a way that the authorship of the data is verifiable.

- ▶ die Daten in einer Präsentation beziehen sich oft auf dasselbe Subjekt, können aber von mehreren Ausstellern ausgegeben worden sein
- ▶ die Aggregation dieser Informationen drückt typischerweise einen Aspekt einer Person, Organisation oder Einheit aus
- ▶ auch Präsentationen mit mehreren Credentials über verschiedene Subjekte sind möglich



(*Verifiable Credentials Data Model 1.0 2019*)



(*Verifiable Credentials Data Model 1.0 2019*)

Verifiable Credentials

Presentations

Beispiel I

```
{  
  "type": "VerifiablePresentation",  
  
  "verifiableCredential": [{  
  
    "issuer": "https://example.edu/issuers/565049",  
  
    "credentialSubject": {  
  
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",  
  
      "alumniOf": {  
        "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",  
        "name": [{  
          "value": "Example University",  
          "lang": "en"  
        }],  
      },  
    },  
  },  
]
```

Verifiable Credentials

Presentations

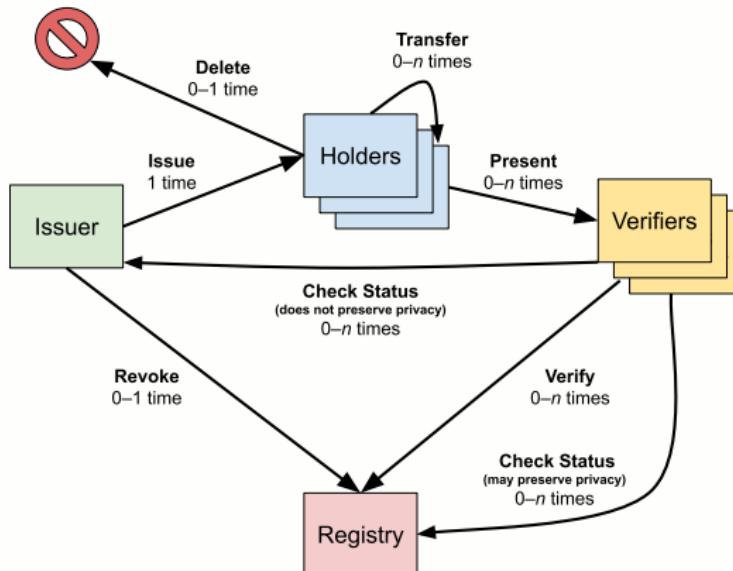
Beispiel II

```
{
  "value": "Exemple d'Université",
  "lang": "fr"
}
},
"proof": {
  }
},
"proof": [
  {}
}
```

Verifiable Credentials

Lebenszyklus

Life of a Single Verifiable Credential



(Verifiable Credentials Data Model 1.0 2019)

Verifiable Credentials

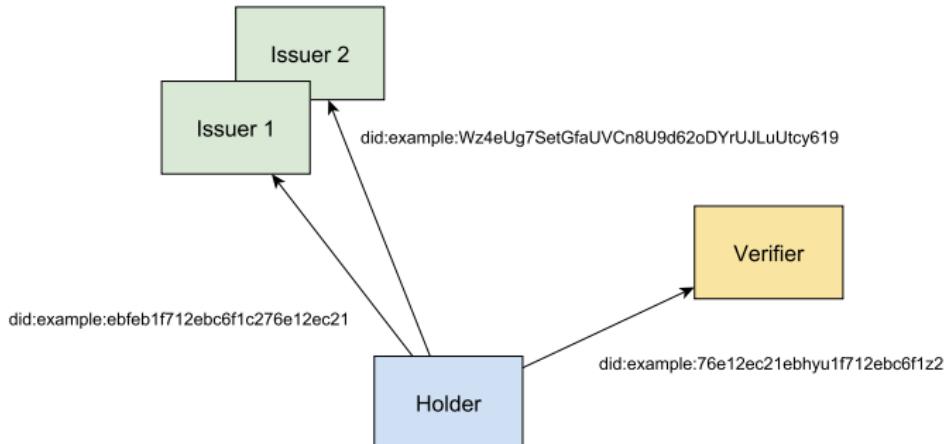
Lebenszyklus

- ▶ ein Issuer stellt einem Holder ein Verifiable Credential aus. Die Ausstellung erfolgt immer vor allen anderen Aktionen, die ein Credential betreffen
- ▶ ein Holder kann einen oder mehrere seiner Credentials auf einen anderen Inhaber übertragen
- ▶ ein Inhaber legt einen oder mehrere seiner Credentials einem Verifier vor, optional innerhalb einer Verifiable Presentation
- ▶ ein Verifier überprüft die Authentizität der vorgelegten Presentation und der Credentials. Dazu sollte auch die Überprüfung des Status für den Widerruf der Credentials gehören.
- ▶ ein Issuer könnte ein Credential widerrufen
- ▶ ein Inhaber kann ein Credential löschen.

Verifiable Credentials

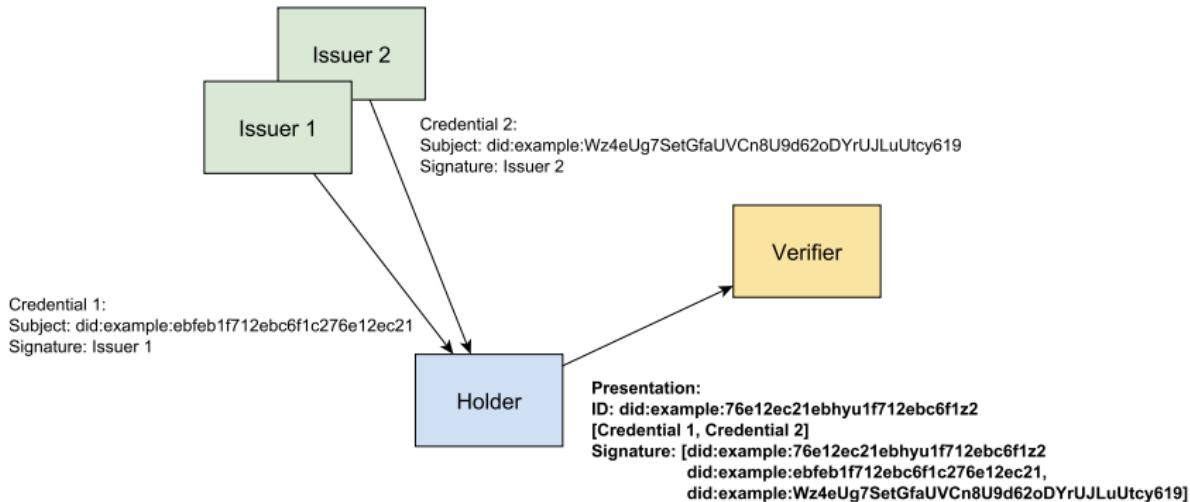
Anti-Korrelation

- ▶ Credentials könnten für unterschiedliche DIDs ausgestellt werden
- ▶ Nachweis der Eigentümerschaft durch mehrere Signaturen/Self-issued-Credentials in der Presentation (Pairwise DIDs)
- ▶ verhindert Korrelation nur gegenüber den Issuern, aber nicht in jedem Fall gegenüber den Verifiern



Verifiable Credentials

Anti-Korrelation



- DID könnte nun als URI/URL eines jeweiligen Credentials gesehen und zum Eigentümer aufgelöst werden (Service Endpoints evtl. nützlich)

Zusammenfassung

- ▶ Benutzer können ihre digitale Identität nicht kontrollieren. Im besten Fall kontrollieren sie ihre Geräte/Software, und diese kontrollieren die digitale Identität
- ▶ eine digitale Identität besteht aus einem Identifier und verifizierbaren Eigenschaften
 - der Identifier wird durch einen Decentralized Identifier (DID) dargestellt
 - Eigenschaften werden durch Verifiable Credentials (VCs) ausgedrückt
- ▶ einmal offengelegte Informationen (in VCs) können nicht entzogen oder zurückgezogen werden
- ▶ öffentlich zugänglich müssen sein:
 - letzte Rotation/Änderung von Schlüsseln
 - Widerrufslisten/Zertifikatssperrlisten (Revocation Lists) von Credentials
 - Credential-Schemas und deren Semantik

Was fehlt...

- ▶ Decentralized Key Management Systems (DKMS; z.B. Secret-Sharing, Multisig etc.)
- ▶ Vertrauensmodelle/Trust-Frameworks
- ▶ Herstellung von Vertrauen in die Anwendersoftware
- ▶ Bereitstellung von Revocation Lists
- ▶ Bereitstellung von Credential-Schemas und deren Semantik
- ▶ sichere Speicherung von Credentials (lokal, Hubs, Backups usw.)
- ▶ CL-Signaturen und Zero-Knowledge-Proofs

Was bleibt...

- ▶ Vielen Dank für Ihre Aufmerksamkeit
- ▶ Bei Fehlern, Anmerkungen oder Kritik: kommen Sie gern auf mich zu

Vielen Dank

Christoph Menzer
Projektmitarbeiter

Hochschule Mittweida | University of Applied Sciences
Technikumplatz 17 | 09648 Mittweida
Fakultät CB| BCCM

T +49 (0) 3727 58-1175
F +49 (0) 3727 58-21175

menzer@hs-mittweida.de
<https://blockchain.hs-mittweida.de/>

Haus 6 | Grunert de Jácome Bau | Raum 6.04.23
Technikumplatz 17| 09648 Mittweida

Allen, Christopher (25. Apr. 2016). *The Path to Self-Sovereign Identity*. URL: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html> (besucht am 27.04.2020).

Andrieu, Joe (Okt. 2016). *A Technology-Free Definition of Self-Sovereign Identity*. URL: <https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/topics-and-advance-readings/a-technology-free-definition-of-self-sovereign-identity.pdf> (besucht am 27.09.2020).

Antonopoulos, Andreas M. (2015). *Mastering Bitcoin*. First edition. Sebastopol CA: O'Reilly. 272 S. ISBN: 978-1-4493-7404-4
978-1-4919-0260-8.

Antonopoulos, Andreas M. und Gavin A. Wood (4. Dez. 2018). *Mastering Ethereum: Building Smart Contracts and DApps*. 1. Aufl. Farnham: O'Reilly UK Ltd. 384 S. ISBN: 978-1-4919-7194-9.

BTCR DID Method (8. Aug. 2019). URL:

<https://w3c-ccg.github.io/didm-btcr/> (besucht am 14.07.2020).

Decentralized Identifier Resolution (DID Resolution) v0.2 (2019). URL:

<https://w3c-ccg.github.io/did-resolution/> (besucht am 03.12.2019).

Decentralized Identifiers (DIDs) v1.0 (2019). URL:

<https://w3c.github.io/did-core/> (besucht am 12.11.2019).

DID Method Registry (2019). URL:

<https://w3c-ccg.github.io/did-method-registry/> (besucht am 13.11.2019).

ERC-1056 (3. Mai 2018). *ERC: Lightweight Identity · Issue #1056 ·*

Ethereum/EIPs. URL:

<https://github.com/ethereum/EIPs/issues/1056> (besucht am 04.06.2020).

Kai Wagner u. a. (23. Okt. 2018). *Self-Sovereign Identity.* URL: <https://www.bundesblock.de/wp-content/uploads/2019/01/ssi-paper.pdf> (besucht am 15.10.2019).

Peer DID Method Specification (2020). URL:

<https://identity.foundation/peer-did-method-spec/> (besucht am 29.09.2020).

Smith, Samuel (3. Juli 2019). *Key Event Receipt Infrastructure (KERI).*

Tietz, Christian u. a. (2017). *Management digitaler Identitäten: aktueller Status und zukünftige Trends*. Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam 114. Potsdam: Universitätsverlag Potsdam. 66 S. ISBN: 978-3-86956-395-4.

Verifiable Credentials Data Model 1.0 (2019). URL:
<https://www.w3.org/TR/vc-data-model/> (besucht am 04.12.2019).