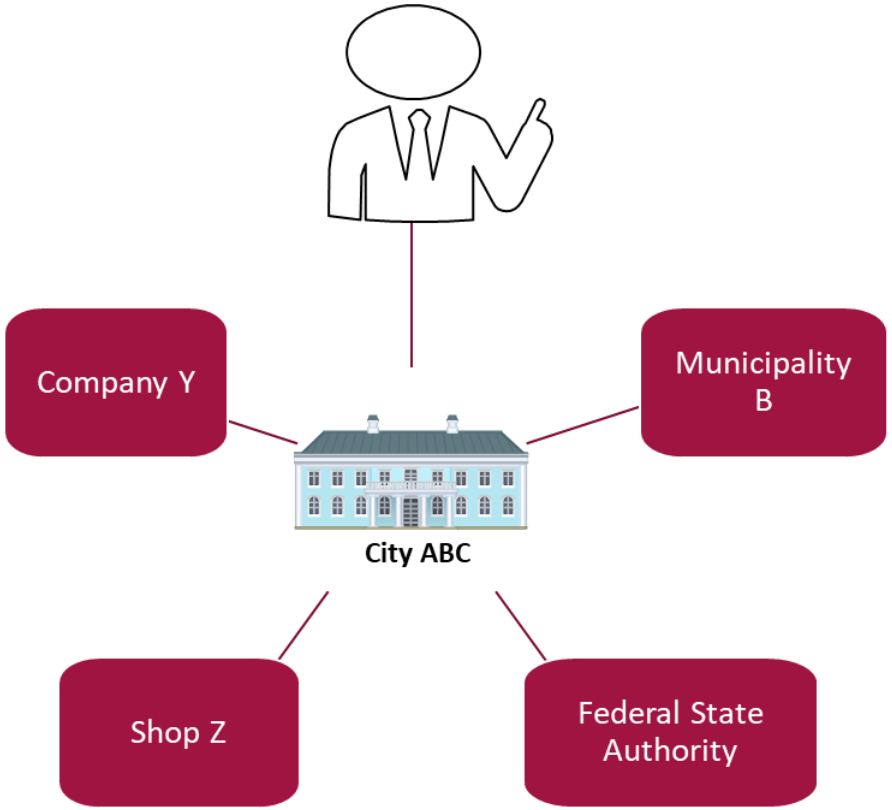
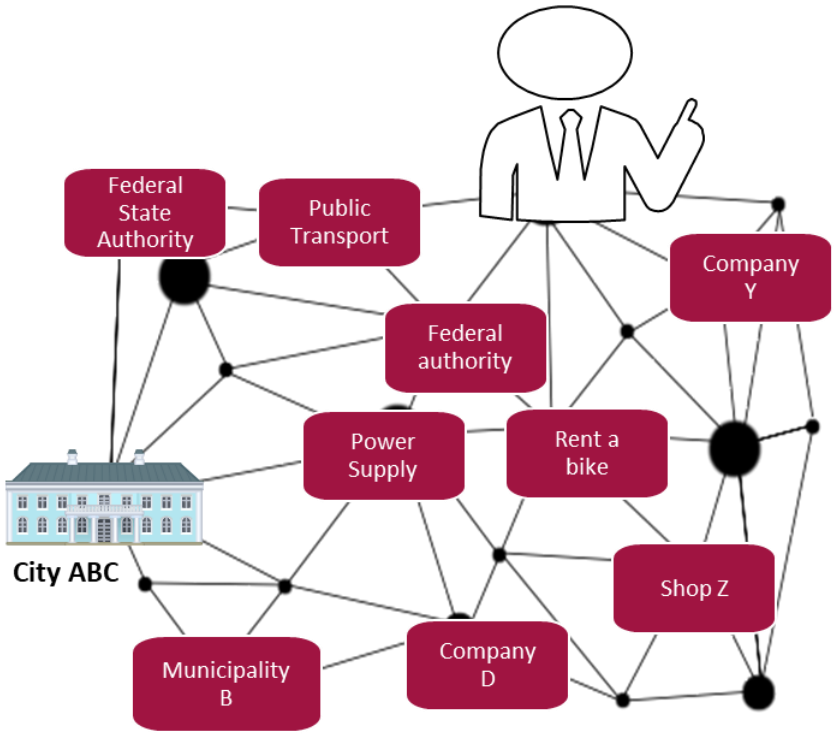
Kriterien für vertrauenswürdige digitale Prozesse – Records Management und beweissichere Aufbewahrung in Blockchain/DLT

Steffen Schwalm, Principal Business Consultant, msg group

Blockchain/DLT ´vernetzt Unternehmen, Behörden, Bürger in digitalen Ökosystemen durch Dezentralisierung und Datensouveränität





Beispielhafte UseCases (Vgl. u.a. Blockchainstrategie der Bundesregierung, European Blockchain Service Infrastructure etc.)

SSI & Datenaustausch

- COVID19 Impfpass, Schnelltestpass
- SmartCity, Smart Mobility,
- GAIA-X, Maschinen-/Datenhandelsplattformen (G2B2C2Machine) etc.
- Digitale Nachweise (Führerschein, Studentenausweis, Zeugnisse etc.)
- Ticketing, Telemedizin, Patientenakte, Zertifikate

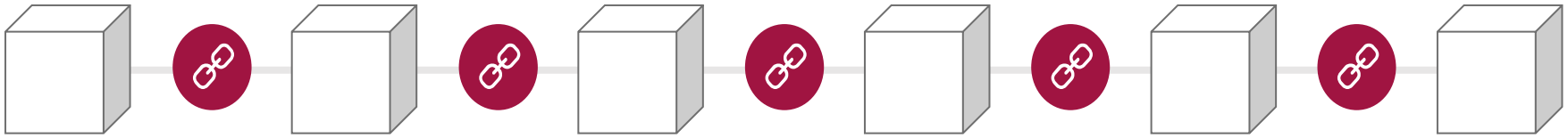
Datenvalidierung

- Digitale Nachweise
- Herkunftsnachweise
- Notarisation, Zertifikate

Digitale Ökosysteme

- Supply Chain (Nachverfolgung von Produktionsketten)
- Registerautomatisierung
- Kryptowährungen
- Banken-/Zahlungsnetzwerke
- Digitale Register, Stromhandel, Zertifikatshandel

Blockchain – Aufbau



Blockchain ist eine dezentrale, verteilte Liste von Datensätzen, die in Blöcken gebündelt und sequentiell aneinander gereiht sind. Blockchain ist die bekannteste Form der Distributed-Ledger-Technology (DLT).

Jeder Teilnehmer besitzt eine identische Kopie des Ledgers. Wenn ein neuer Block erzeugt wurde, wird dieser an alle Teilnehmer verteilt.

Ein **Ledger** ist ein Buch mit Datensätzen, wobei jede Seite eine Liste von Transaktionen enthält.

Ein Block in der Blockchain ist wie eine Seite im Ledger.

Jeder **Block** enthält eine gebündelte Liste von Daten.

Diese Daten können Transaktionen oder ein Smart Contract sein.

Jeder Block ist durch einen **Hashwert** gesichert, der eine unbemerkte Änderung der Daten in der Kette verhindert und große Anstrengungen erfordert, um die Daten zu ändern.

Was beinhaltet ein Block?

Hash des aktuellen Blocks

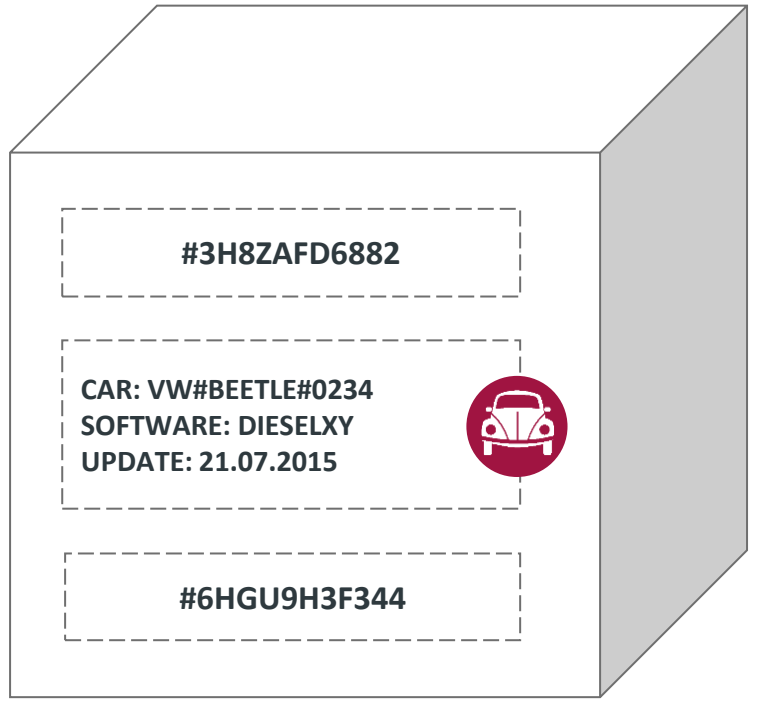
- Eindeutige Kennung des Blocks
- Hash wird basierend auf dem Hash des vorherigen Blocks und allen Daten des aktuellen Blocks erzeugt.

Daten

- Transaktionsdaten oder Datensätze werden im Block gebündelt.

Hash des vorherigen Blocks

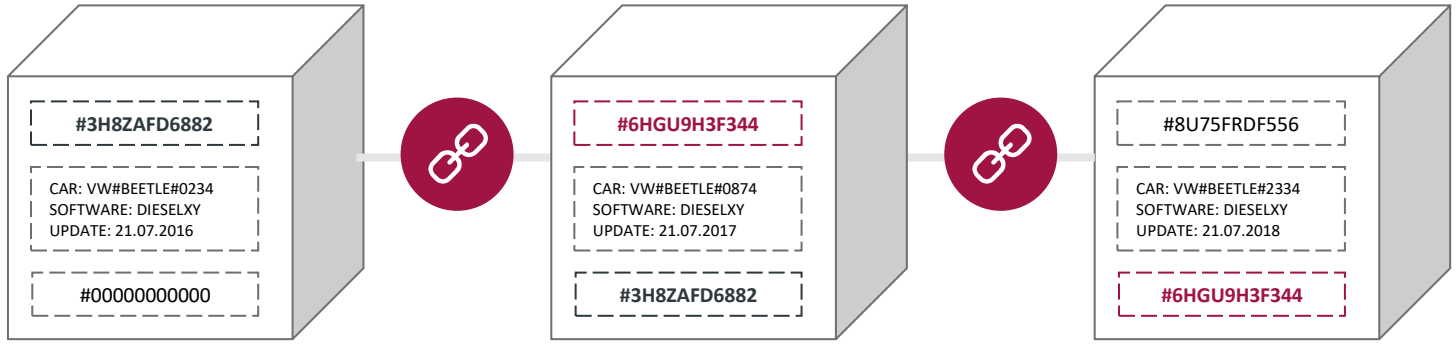
- Dieser Teil baut eine Verbindung zum vorherigen Block auf.



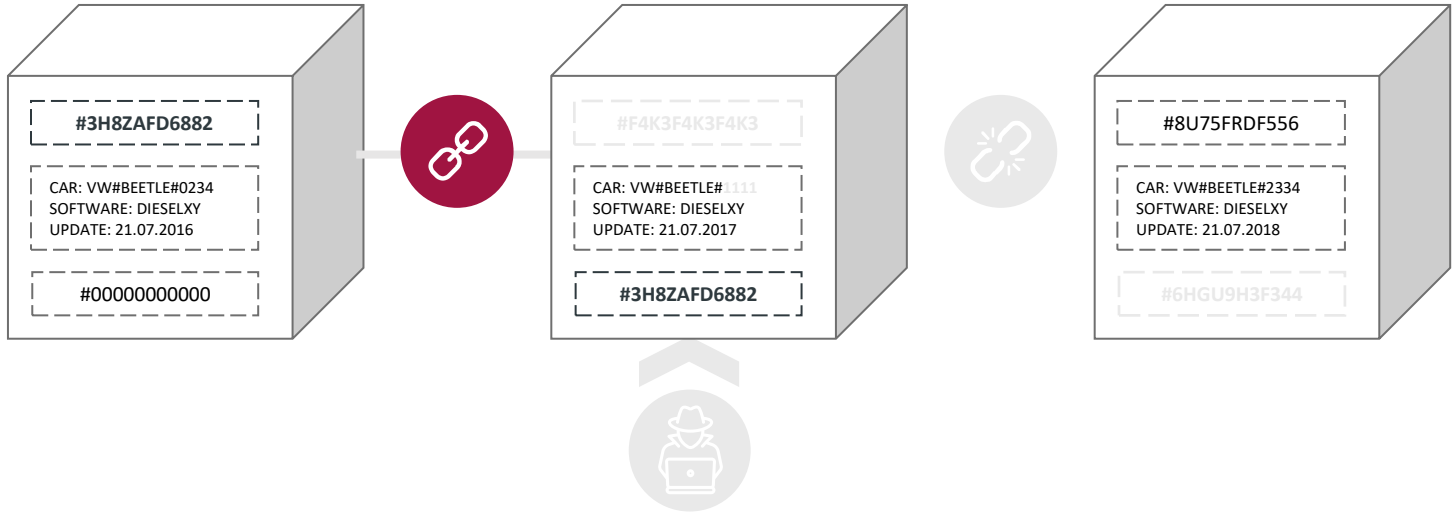
- On-Chain vs. off-chain (Ledger Records vs. Non-Ledger Records)
- Zusammenhang ist dauerhaft zu wahren

Wie sind die Blöcke miteinander verbunden und warum ist die Blockchain „sicher“?

Jeder Block ist mit dem vorherigen Block verbunden, da er den Hashwert des vorherigen Blocks enthält.



Wenn ein Angreifer Informationen in einem Block ändert, passt der ursprüngliche Hashwert nicht mehr und die Kette ist nicht länger verbunden.



Berechtigungen in Blockchain/DLT

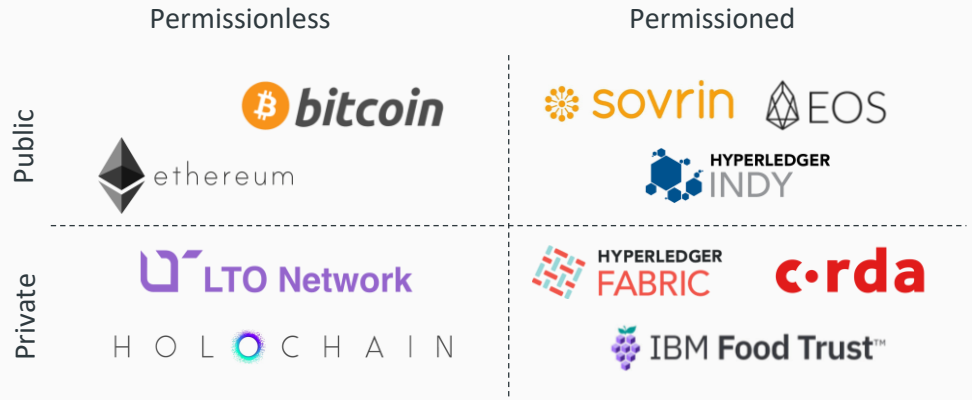
- Blockchains und DLT werden zusätzlich anhand Lese- und Schreiberechte unterschieden

Leserechte

public
Vollständige Transparenz und Einsicht aller Transaktionen
private
Eingeschränkt, nur eigene Transaktionen bzw. Einsicht nach Aufnahme

Schreiberechte

permissionless
Beteiligung bei Transaktionsvalidierung und Persistierung
permissioned
Eingeschränkte bzw. keine Berechtigung zu Validierung und Persistierung



Bei den in der Allgemeinheit bekanntesten Blockchains handelt es sich um public permissionless Ausprägungen, die so gänzlich ohne Kontrollhoheit auskommen.

Enterprise-Lösungen sind häufig private permissioned.

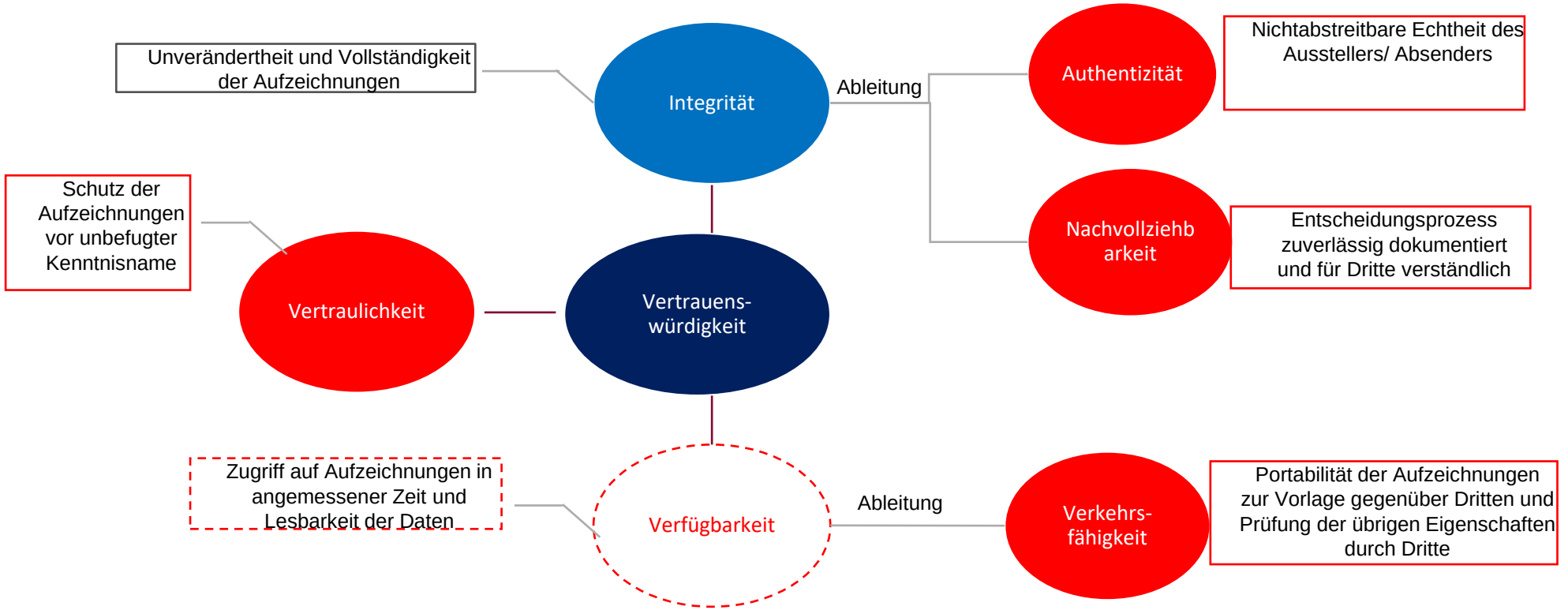
Wesentliche Herausforderungen an die Nutzung von Blockchain für vertrauenswürdige digitale Register/Verzeichnisdienste und Transaktionen

- Sichere Identifizierung und Authentisierung (sichere digitale Identität
- Datenschutz gem. DSGVO (z.B. Gewährleistung Rechte des Betroffenen)
- Vertrauenswürdigkeit/Nachweis des Abschlusses/Zeitpunkts und Zuordnung von Daten/Transaktion zum Aussteller/Organisation
- Langfristiger Nachweis und Sicherheit der Daten sowie Transaktion
- Legal Compliance, Machbarkeit und Vorteile der UseCases gegenüber „klassischen Technologien“

International Standardisierung schafft Lösungen zum Records Management und DLT.

ISO TR 24332 (Stage 20.20)
Blockchain and DLT in relation to authoritative records, records systems, and records management

Es gilt die Authoritativeness of records zu bewahren – allerdings erfüllt DLT die Anforderungen an authoritative records nur bedingt.



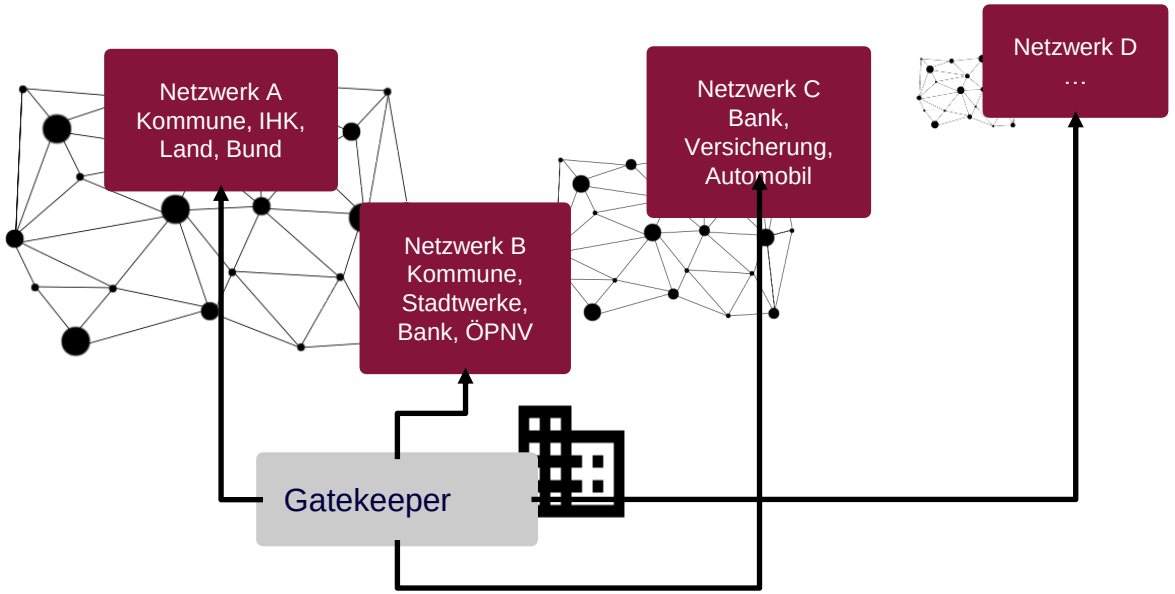
Gewährleistung durch definierte Prozesse, Organisation, Governance, IT (Records Management) im records system (jedes System, das [authoritative] records beinhaltet

Kriterien für vertrauenswürdige digitale Transaktionen — Records Management & Beweiswerterhaltung in Blockchain and Distributed Ledger Technology (DLT) DIN TS 31648 schafft Basis für DLT-Nutzung in Deutschland

- **Fundamentals on records management & trustworthines of digital transactions based on ISO-15489, ISO-303xx [ISO Tc 46 Sc 11), ETSI M460, ISO Tc 307, ESSIF, Federal Office for Information Security [Germany]**
- **Compliance & Governance (Regulatory Compliance, State of the Art technology, Policies, utilisation of trust services e.g. signatures/seals risk management Roles & Responsbilities, Certification & Audit)**
- **Life-Cycle of electronic records (storage location, description, Access Management, Identification & Onboarding, Privacy, Archiving & Preservation)**
- **Information Security (consensus, cryptographic mechanism, attack scenarios, crypto stability, Proof of Existence & evidence preservation etc.)**
- **Technical subjects (interoperability, scalability, reliability, maintainability etc.)**

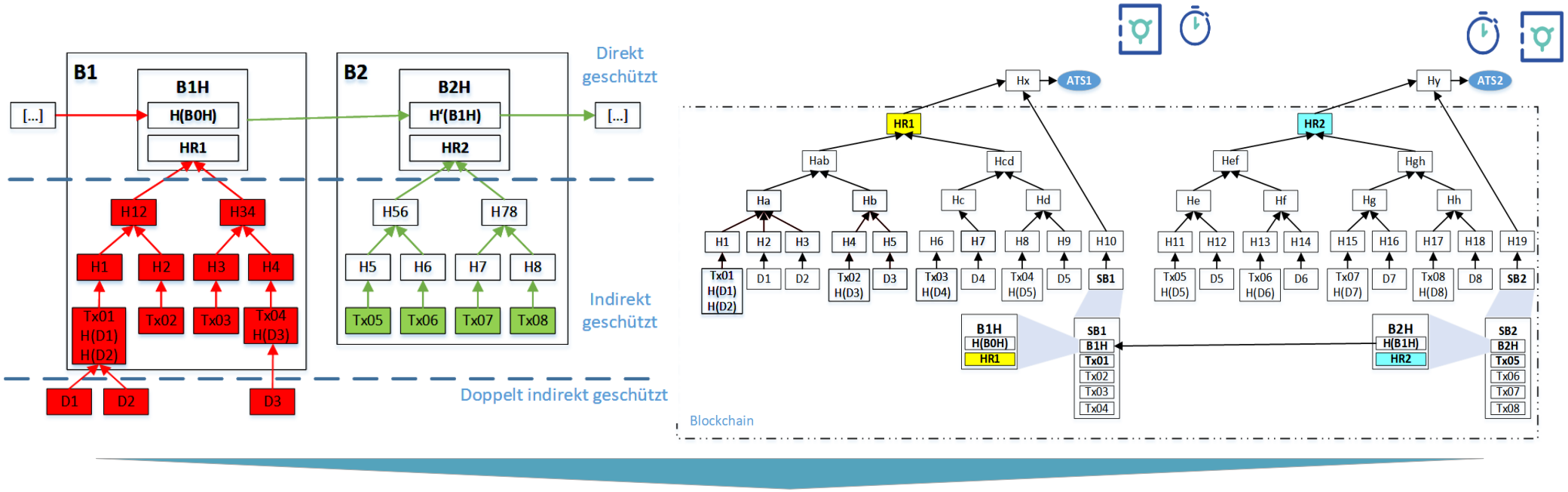
Quelle: DIN NID 15 WG 2 DIN TS 31648 Kriterien für vertrauenswürdige digitale Transaktionen. Beweiswerterhaltung und Records Management in Blockchain/DLT

Der (qualifizierte) Trust Service Provider acc. eIDAS enabled vertrauenswürdige Transaktionen in DLT/Blockchain (Vgl. auch eIDAS 2.0)



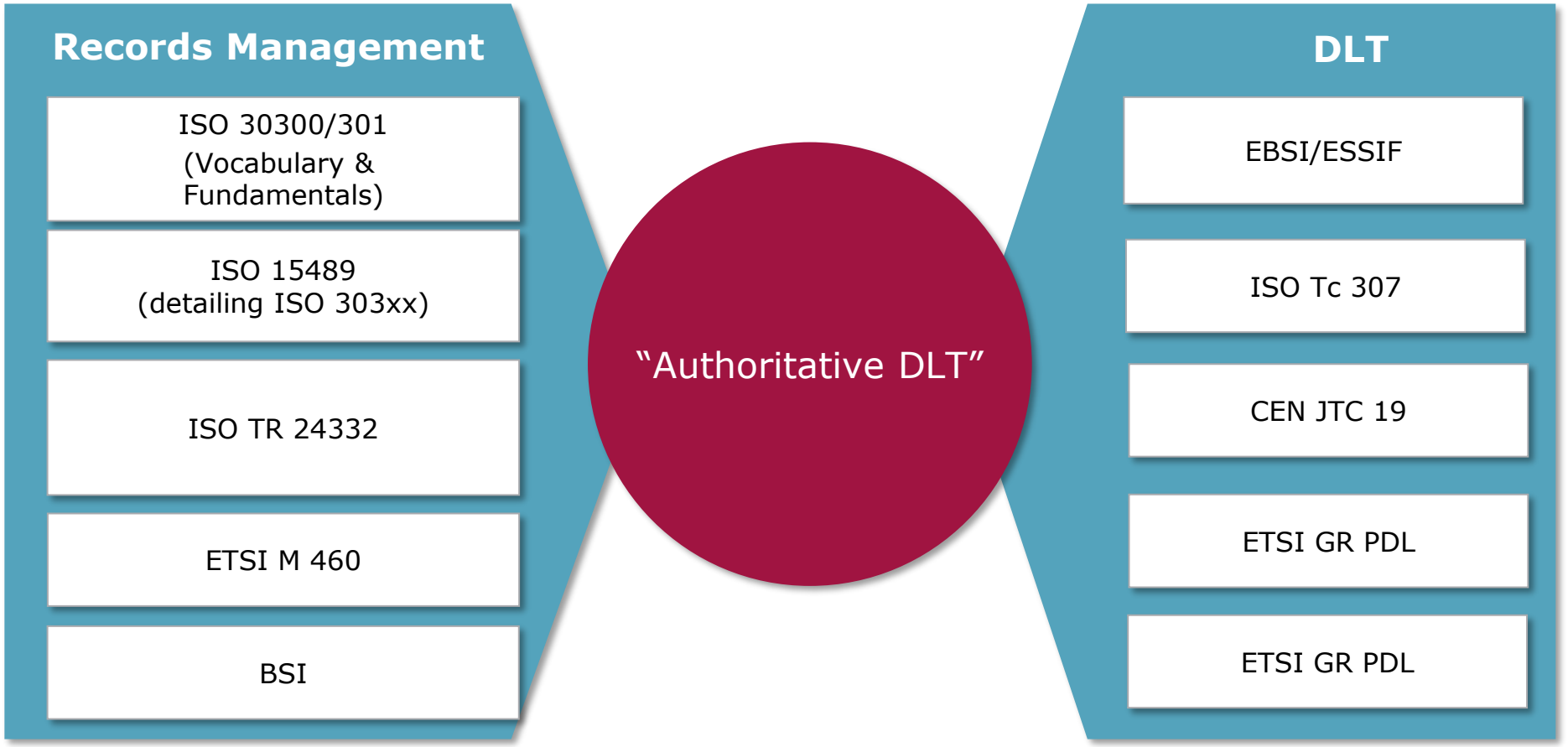
Beweiswerterhaltung und langfristige Kryptostabilität durch Kombination DLT mit etablierten Standards & Normen.

Wesentliche Maßgabe: aufbewahrungspflichtige Daten befinden sich außerhalb der Blockchain, Blockchain beinhaltet nur Hashwerte der Daten



- ETSI TS 119 511 und 512 schaffen Grundlage für (qualifizierte) Bewahrungsdienste und Bewahrung (Beweiswerterhaltung) in Europa
- BSI TR 03125 TR-ESOR floss in ETSI-Vorgaben unmittelbar ein und nimmt diese auf
- Nutzung etablierter Verfahren zum Beweiswerterhalt sicher auch Beweiswert in DLT

Wesentliche Standards



Diskussionsthesen

1. DLT ermöglicht digitale Geschäftsmodelle & Ökosysteme die (derzeit) keine andere Technologie realisiert und beschleunigt so eine sichere wie nachhaltige Digitalisierung
2. DLT unterstützt Datensouveränität & unterstützt Demokratisierung
3. DLT erfordert völlig neues Governance-Modelle – Records Management durch Beteiligte eines Netzwerks
4. Auch vollständig anonyme Transaktionen erzeugen, speichern und sichern authoritative records
   Klassische Berechtigungsmechanismen sind zu überdenken
5. DLT allein ist weder sicher noch vertrauenswürdig, erst durch Ergänzung notwendiger Dienste und adäquater Sicherheitsmaßnahmen wird Records Management nach Stand der Technik erreicht

Steffen Schwalm
Principal Business Consultant
Information Security & Compliance

Convenor ISO Tc 46 Sc 11 JWG 1
(ISO TR 24332)
Expert CEN/CENELEC e.g. JTC 19
Deputy Leader DIN NID 15
Experte u.a. ISO Tc 307, ETSI, DIN NIA 43,
DIN NIA 27

+49 (0) 162 280 6472
steffen.schwalm@msg.group

https://www.researchgate.net/profile/
Steffen_Schwalm/research

msg systems ag
Amelia-Earhart-Str. 14
60549 Frankfurt am Main

http://www.msg.group