TEXTE
162/2026

Abschlussbericht

Distributed Ledger Technology (DLT) im Rahmen der Lieferketten

von:

Carsten Stöcker, Johannes Ebert
Spherity GmbH

Steffen Schwalm, Tim Taschau
msg security advisors

Prof. Dr. Wolfgang Prinz, Mirko Mollik
Fraunhofer FIT

Herausgeber:
Umweltbundesamt

Für Mensch & Umwelt

Umwelt Bundesamt

TEXTE 162/2026

Ressortforschungsplan des Bundesministeriums für
Umwelt, Naturschutz, nukleare Sicherheit und
Verbraucherschutz

Forschungskennzahl 3723 11 101 2

Abschlussbericht

Distributed Ledger Technology (DLT) im Rahmen der Lieferketten

von

Carsten Stöcker, Johannes Ebert
Spherity GmbH

Steffen Schwalm, Tim Taschau
msg security advisors

Prof. Dr. Wolfgang Prinz, Mirko Mollik
Fraunhofer FIT

Im Auftrag des Umweltbundesamtes

Impressum

Herausgeber
Umweltbundesamt
Wörlitzer Platz 1
06844 Dessau-Roßlau
Tel: +49 340-2103-0
Fax: +49 340-2103-2285
buergerservice@uba.de
Internet: www.umweltbundesamt.de

Durchführung der Studie:
msg systems ag
Amelia-Mary-Earhart Straße 14
60549 Frankfurt

Abschlussdatum:
Dezember 2024

Redaktion:
Fachgebiet Z 2.3 Digitale Transformation und Beratungsstelle Green IT
Dirk Osiek

DOI:
https://doi.org/10.60810/openumwelt-8114

ISSN 1862-4804

Dessau-Roßlau, November 2026

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autorinnen und Autoren.

Kurzbeschreibung: Distributed Ledger Technology (DLT) im Rahmen der Lieferketten

Das Dokument beschreibt auf Basis der wesentlichen regulatorischen Anforderungen, wie eine Lieferkettennachverfolgung anhand von DLT erfolgen könnte. Zunächst wird ein Überblick über die technischen Grundlagen der DLT gegeben, einschließlich einer Bewertung ihrer Eignung für Nachweiszwecke, wie sie in der Lieferkette erforderlich sind.

Diesem Rahmen folgt die fundierte Beschreibung der regulatorischen Anforderungen. Dies beginnt mit den allgemeinen Vorgaben aus der Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS-Verordnung) sowie der Datenschutz-Grundverordnung (DSGVO), gefolgt von fachspezifischen Maßgaben. Dabei werden neue Entwicklungen und Projekte wie der neue qualifizierte Vertrauensdienst für Electronic Ledger oder laufende Forschungsprojekte zur Lieferkettennachverfolgung in Europa betrachtet.

Auf dieser regulatorischen wie fachlichen und technischen Grundlage beinhaltet der Bericht einen Vergleich von DLT und herkömmlichen Verfahren zur Lieferkettennachverfolgung einschließlich einer Bewertung und Zusammenfassung der Ergebnisse. Der Bericht beinhaltet darüber hinaus in der Anlage beispielhafte Fallstudien zum Einsatz von DLT im Rahmen der Lieferketten.

Abstract: Distributed Ledger Technology (DLT) in the context of supply chains

The document describes how supply chain tracking could be carried out using DLT based on the key regulatory requirements. This begins with an overview of the technical fundamentals of DLT, including an assessment of the technology for verification purposes, as is necessary for the supply chain.

This framework is followed by a well-founded description of the regulatory requirements. This begins with the general requirements specified in the Regulation on electronic identification and trust services (eIDAS) and the General Data Protection Regulation (GDPR), followed by subject-specific requirements. New developments and projects such as the new qualified trust service for electronic ledgers or ongoing research projects on supply chain tracking in Europe are considered.

On this regulatory, professional and technical basis, the report contains a comparison of DLT and conventional supply chain tracking methods, including an assessment and summary of the results. The report further includes exemplary case studies on the use of DLT in supply chains in the appendix.

Inhaltsverzeichnis

Abbildungsverzeichnis ... 8
Tabellenverzeichnis ... 8
Abkürzungsverzeichnis ... 9
Zusammenfassung ... 10
Summary ... 16
1 Einführung in Distributed Ledger Technologien ... 22
1.1 Electronic Ledger und Distributed Ledger ... 22
1.2 Einführung in DLT ... 22
1.3 Wesentliche Sicherheitsmerkmale von DLT ... 24
1.3.1 Grundsatz ... 24
1.3.2 Berechtigungsmanagement in DLT ... 26
1.3.2.1 Permissionless DLT ... 26
1.3.2.2 Permissioned DLT ... 28
1.4 Smart Contracts ... 29
1.5 Kurzüberblick wesentlicher Protokolle ... 31
1.5.1 Token in DLT ... 32
1.6 Unterschiede zwischen DLT und traditionellen Datenbanken ... 34
1.7 DLT und Nachweisfähigkeit ... 34
1.7.1 Grundsatz ... 34
1.7.2 Nachweisfähigkeit in DLT ... 35
1.8 Herausforderungen und Stand der Technik von DLT ... 36
1.9 Wesentliche DLT-Netzwerke in Europa ... 38
1.9.1 European Blockchain Service Infrastructure ... 38
1.9.2 Weitere Netzwerke ... 39
2 Anforderungen an ein System zur Lieferkettennachverfolgung ... 41
2.1 Regulatorische Anforderungen ... 41
2.1.1 eIDAS Verordnung ... 41
2.1.2 Lieferkettensorgfaltspflichtengesetz ... 43
2.1.3 Datenschutzgrundverordnung (DSGVO) ... 44
2.1.4 Verordnung „Recht auf Reparatur“ ... 45
2.1.5 EU-Batterieverordnung ... 45
2.1.6 Weitere Vorgaben in Europa ... 46
2.1.7 Internationale Vorgaben: FDA ... 47

2.1.8 Fachspezifische Anforderungen ... 48
2.1.9 Technische Anforderungen ... 50
2.1.10 Zusammenfassung ... 52
3 Vergleich DLT und herkömmliche Verfahren ... 54
3.1 Vorgehensweise und wesentliche Maßgaben ... 54
3.2 Ergebnisse ... 55
3.2.1 Regulatorische Anforderungen ... 55
3.2.2 Fachliche Anforderungen ... 56
3.2.3 Technische Anforderungen ... 56
3.3 Zusammenfassung ... 58
4 Fazit ... 59
5 Bibliographie ... 60
A Anhang 1: Fallstudien zur Lieferkettennachverfolgung mit DLT ... 64
A.1 Fallstudie 1: Lieferkettennachverfolgung in Übereinstimmung mit der EU-Batterieverordnung ... 64
A.2 Fallstudie 2: FSC DLT ... 68
A.3 Zusammenfassung der Fallstudien ... 70

Abbildungsverzeichnis

Abbildung 1: Arten von DLT 11
Abbildung 2: Types of DLT 16
Abbildung 3: Arten DLT im Überblick 23
Abbildung 4: Aufbau EBSI 58
Abbildung 5: TUFF DLT 66
Abbildung 6: FSC Supply Chain 69
Abbildung 7: FSC DLT 70

Tabellenverzeichnis

Tabelle 1: Unterschiede DLT und traditionelle Datenbanken 11
Tabelle 2: Bewertung DLT/DLT hinsichtlich geschäftsrelevanter Aufzeichnungen 12
Tabelle 3: Anforderungen an die Lieferkette 13
Tabelle 4: rough differences between DLT and traditional data bases 17
Tabelle 5: Asessment DLT against Records Management 18
Tabelle 6: Fundamental Requirements on Supply Chain 19
Tabelle 7: Vergleich Ethereum, Hyperledger Fabric und R3 Corda 31
Tabelle 8: Vergleich der Token in Ethereum, Hyperledger Fabric und R3 Corda 32
Tabelle 9: Wesentliche Unterschiede DLT und traditionelle Datenbanken 34
Tabelle 10: Bewertung DLT hinsichtlich signifikanter Eigenschaften geschäftsrelevanter Aufzeichnungen 35
Tabelle 11: Überblick internationale Standardisierung zu DLT (Auswahl) 37
Tabelle 12: Anwendbarkeit QTSP for Ledger 43
Tabelle 13: Überblick Anforderungen zum Vergleich DLT vs. herkömmliche Verfahren 54

Abkürzungsverzeichnis

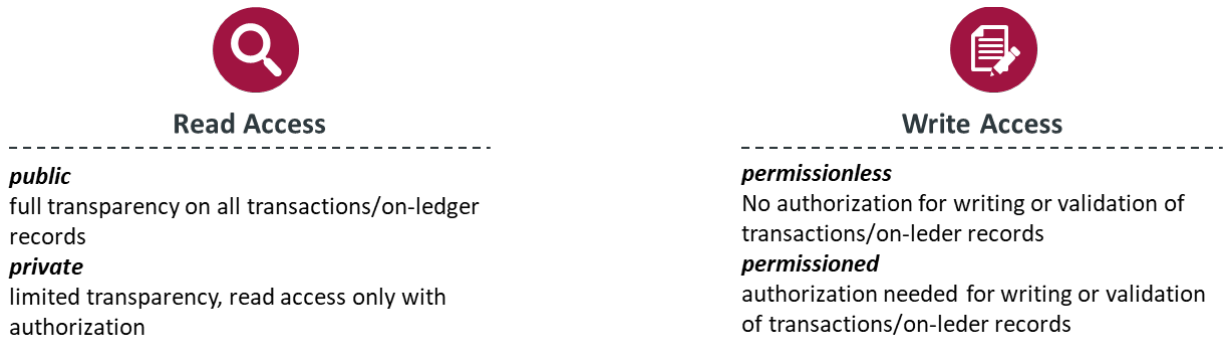
BFT	Byzantine Fault Tolerance
DID	Decentralized Identifier
DLT	Distributed Ledger Technologie
DPP	Digitaler Produktpass
DSGVO	Datenschutz-Grundverordnung
EBSI	European DLT Service Infrastructure
EDIC	The European Digital Infrastructure Consortium
eIDAS	Regulation on electronic identification and trust services
ESPR	Ecodesign for Sustainable Products Regulation
EUDIW	EUDI Wallet
GDPR	General Data Protection Regulation
ISMS	Informationssicherheitsmanagementsystem
JadES	JSON Advanced Electronic Signatures
JTC	Joint Technical Committee
MiCAR	Verordnung über Märkte für Kryptowerte
NFT	Non-fungible token
PKI	Public-Key-Infrastruktur
PoA	Proof of Authority
PoE	Proof of Existence
PoS	Proof of Stake
PoW	Proof-of-Work
QEAA	Qualifizierte Attributsbescheinigung
QES	Qualifizierte elektronische Signatur
QSeal	Qualifizierte elektronische Siegel
QTSP	Qualifizierter Vertrauensdienst
QWAC	Qualifizierte Websitezertifikate
TC	Technical Committee
UTXO	Unspent Transaction Output
WORM	Write Once Read Many

Zusammenfassung

Einführung in DLT

Grundsätzlich ist DLT ein dezentral verteiltes Peer-to-Peer-Netzwerk aus technischen Knoten für den Datenaustausch und die Ausführung von Transaktionen. Gemäß ISO 22739 wird ein Distributed Ledger von mehreren DLT-Knoten gemeinsam geführt und über einen Konsensmechanismus synchronisiert. Der Konsensmechanismus stellt sicher, dass alle Transaktionen gültig und unverändert sind. Wie ein Konsens erreicht wird, hängt von der Art des DLT ab. Das weit verbreitete Vorurteil, dass DLT einen sehr hohen Energiebedarf impliziert, trifft nur auf einige Konsensmechanismen zu. Insbesondere Proof of Work (PoW) ist energieintensiv. Andere Konsensmechanismen sind deutlich effizienter, vor allem in zugangsbeschränkten DLT-Systemen, etwa Byzantine Fault Tolerance (BFT), Proof of Authority (PoA) oder Proof of Stake (PoS). DLT-Netzwerke ermöglichen die Übertragung von Daten oder Werten von einer Partei zur anderen, ohne dass Zwischenhändler beteiligt sind. Sobald Transaktionen in das Ledger geschrieben sind, sind sie im Allgemeinen unveränderlich, was hauptsächlich auf dem Hash-Schutz der auf dem DLT gespeicherten Daten beruht. Jede Transaktion kann zuverlässig verfolgt werden. Wenn die tatsächlich verteilten Datensätze oder Transaktionen in sequenziell verknüpften Blöcken gebündelt sind, spricht man von einer Blockchain, einer speziellen Form von DLT. Die Blöcke enthalten in der Regel den Hash des vorherigen Blocks. Durch diese Hashverkettung sowie durch DLT-Zeitstempel wird die Unveränderlichkeit sichergestellt. DLT-Zeitstempel und DLT-kryptografische Signaturen unterscheiden sich von denen gemäß eIDAS und verwandten Standards. Bei den Zeitstempeln fehlt, sofern nicht durch einen (qualifizierten) Vertrauensdienst (QTSP) erzeugt, eine vertrauenswürdige Zeitquelle, den Signaturen, sofern nicht auf einem durch einen QTSP erzeugten Zertifikat beruhend, der sog. Proof of Existence, der von einem Dritten statt vom DLT-System selbst erstellt wird. Der hashbasierte Integritätsschutz jedes Blocks basiert auf Merkle-Bäumen. Dies bedeutet, dass Authentizitäts- oder Existenznachweise innerhalb von DLT-Systemen – sofern erforderlich – durch (qualifizierte) Vertrauensdiensteanbieter ergänzt werden müssen. Ähnliche Herausforderungen treten auf, wenn die an einer Transaktion beteiligten Parteien nachgewiesen werden sollen. In diesem Fall muss DLT mit externen Systemen kombiniert werden, um eine eindeutige und vertrauenswürdige Identifizierung von juristischen und/oder natürlichen Personen zu gewährleisten. Im Vergleich zu den ursprünglichen Ideen öffentlicher, erlaubnisfreier DLTs erfordert DLT nicht zwingend die Eliminierung eines Betreibers oder Konsortiums, das das verteilte Netzwerk bereitstellt. Dies hängt von der Art der DLT ab, die sich in Bezug auf Zugriffsrechte und Transaktionstransparenz unterscheiden kann. Bei einer öffentlichen DLT kann jeder alle Transaktionen und Daten einsehen, d. h. es herrscht vollständige Transparenz, bei privater DLT dürfen nur autorisierte Benutzer Transaktionen lesen oder ausführen. Bei permissionless DLT darf jeder Benutzer Transaktionen validieren und speichern, bei permissioned DLT hängt dies von den Zugriffsrechten und Governance-Richtlinien ab. Das nachstehende Bild zeigt die grundlegenden Arten von DLT im Überblick.

Abbildung 1: Arten von DLT



Quelle: eigene Darstellung, msg systems ag

Die wesentlichen Unterschiede zwischen DLT und traditionellen Datenbanken zeigt die folgende Übersicht.

Tabelle 1: Unterschiede DLT und traditionelle Datenbanken

Merkmal	DLT	Traditionelle Datenbank
Dezentralisierung	Verteilt auf mehrere Knoten	Zentralisiert auf einem Server
Veränderbarkeit	Unveränderlich	Veränderbar
Transparenz	Öffentlich einsehbar (bei Public DLT)	Zugriffskontrolle
Sicherheit	Abhängig von Sicherheitsmaßnahmen	Abhängig von Sicherheitsmaßnahmen
Skalierbarkeit	Komplex aber skalierbar durch Hardware	Skalierbar durch Hardware

Als wesentliches DLT-Netzwerk ist in Europa insbesondere die European Blockchain Service Infrastructure (EBSI) zu benennen. EBSI ist ein paneuropäisches DLT-Netzwerk, das von den Mitgliedstaaten bereitgestellt wird. Das bedeutet, dass die neue Betriebsorganisation Europeum/EDIC, die Hauptknoten und die Basisinfrastruktur betreibt und grundlegende Sicherheit, Geschäftskontinuität und Servicelevel gewährleistet.

Nachweisfähigkeit in der Lieferkette

Der Sinn einer Lieferkettennachverfolgung besteht im Kern im Nachweis der gesetzlichen Vorgaben[1] anhand der im Prozess entstehenden Aufzeichnungen. Es geht also darum, die Vertrauenswürdigkeit der Lieferkette nachzuweisen. Hierfür muss der eindeutige wie auch verlustfreie Nachweis der Authentizität, Integrität und Zuverlässigkeit der bei der Transaktionsabwicklung entstehenden oder empfangenen geschäftsrelevanten Aufzeichnungen bis zum Ablauf der geltenden Aufbewahrungsfristen gegenüber Gerichten, Prüfbehörden und sonstigen Dritten erbracht werden. Wesentlich hierfür ist die Erfüllung der weiteren Schutzziele Vertraulichkeit und Verfügbarkeit einschließlich der Verkehrsfähigkeit der Aufzeichnungen. Der

[1] Vgl. Kap. 2

Nachweis wird gegenüber vertrauenswürdigen Dritten anhand der Aufzeichnungen erbracht. Die folgenden Anforderungen stellen damit wesentliche Eigenschaften geschäftsrelevanter Aufzeichnungen dar:

- Authentizität
- Integrität
- Zuverlässigkeit
- Vertraulichkeit
- Verfügbarkeit
- Verkehrsfähigkeit

Die folgende Tabelle zeigt einen Überblick, wie DLT diese Anforderungen derzeit mit oder ohne zusätzliche Maßnahmen erfüllt oder nicht erfüllt. Eine Bewertung der DLT anhand dieser Anforderungen führt zu folgendem Ergebnis:

Tabelle 2: Bewertung DLT/DLT hinsichtlich geschäftsrelevanter Aufzeichnungen

Kernanforderung	Erfüllung	Begründung
Integrität	Bedingt	Unveränderlichkeit wird durch die kryptographische Sicherung der Blöcke (DLT) resp. der Transaktionen (DLT) erreicht Keine Langzeitstabilität, aufgrund des fehlenden Rehashings und Proof of Existence
Authentizität	Bedingt	Keine standardisierten Werkzeuge zur eindeutigen Zuweisbarkeit von Transaktionen und Daten zum Aussteller/Absender Ergänzung bedarf eindeutiger Identifizierung der Aussteller/Absender, was nur in *permissioned* DLT und nur mit Zusatzmitteln möglich ist
Vertraulichkeit	Bedingt	Nur in *permissioned* DLT möglich Erfüllung der Rechte des Betroffenen (Löschung, Datenübermittlung, Berichtigung etc.) nur bei *off-chain*-Speicherung der Inhaltsdaten möglich; Nachweisführung (Informationspflicht, Einwilligung) bedarf zusätzlicher Maßnahmen
Verfügbarkeit	Bedingt	Effektive Skalierbarkeit nur bei *off-chain*-Speicherung der Inhaltsdaten möglich Zugriff nur in DLT, d.h. keine standardisierten Mittel zum Datenexport *on-chain* gespeicherter Aufzeichnungen keine standardisierten Mechanismen zum Langzeiterhalt der in DLT abgelegten Daten
Zuverlässigkeit	Bedingt	Nur in *permissioned* DLT; vollständige Dokumentation bedarf zusätzlicher Maßnahmen durch Metadaten, Protokollinformationen etc., die in DLT nicht vorhanden sind

Kernanforderung	Erfüllung	Begründung
Verkehrsfähigkeit	Bedingt	Keine standardisierten Werkzeuge zum Datenexport aus DLT vorhanden nur bei *off-chain*-Speicherung für die außerhalb der DLT gespeicherten Daten möglich

Anforderungen an die Lieferkettennachverfolung

Als wesentliche Anforderungen lassen sich festhalten:

Tabelle 3: Anforderungen an die Lieferkette

Art der Anforderung	Inhalt
Regulatorisch	eIDAS
	DSGVO
	Lieferkettenspezifische Regelung
Fachlich (abgeleitet aus regulatorischen Vorgaben)	Nachweisfähigkeit (Integrität, Authentizität, Verfügbarkeit etc.)
	Prozessintegration
Technisch	Identifizierung und Authentisierung
	Langfristige Lesbarkeit und Prüfbarkeit der Nachweisdaten
	Vermeidung Single Point of Failure
	Backup & Recovery
	Cybersicherheitsanforderungen
	Systemintegration
	Datenintegration
	Betrieb

Die Erfüllung der regulatorischen, fachlichen und technischen Anforderung erfordern das Vorhandensein eines oder mehrerer Betreiber eines Systems zur Lieferkettennachverfolgung. Dies limitiert den Einsatz von DLT de facto auf permissioned DLT. Darüber hinaus wird die Umsetzung durch den neuen qualifizierten Vertrauensdiensteanbieter (Qualified Trust Service Provider, nachfolgend QTSP) für Ledger nach eIDAS erleichtert, da ein direkter Betreiber mit klarer Haftung und geprüfter Sicherheit (Konformitätsbewertung nach eIDAS) vorliegt.

Vergleich DLT und herkömmliche Verfahren zur Lieferkettennachverfolgung

Vergleichsgegenstand ist die Lieferkettennachverfolgung. Hierfür ist es grundlegend erforderlich, zum einen die verantwortliche juristische Person sowie deren handelnde Personen und ggf. das betroffene Produkt resp. dessen Teile eindeutig zu identifizieren und dem

betreffenden produzierenden Unternehmen zuzuordnen (Produktpass) sowie die eigentliche Lieferkette (Supply Chain, also den Prozess nachzuweisen und dem Produkt und beteiligten Unternehmen eindeutig zuzuordnen.

Als Verfahren wurden gewählt:

- DLT: Europäische Blockchain Service Infrastructure
  - Für die DLT wurde die EBSI als Beispiel gewählt, da diese als paneuropäische DLT-Infrastruktur der Mitgliedstaaten aufgebaut wird. Zudem wird die Lieferkettennachverfolgung durch verschiedene Projekte aktuell auf der EBSI pilotiert, so z.B. TRACE4EU[2], EBSI ELSA[3]
  - Es gelten damit die organisatorischen (Governance) und technischen Rahmenbedingungen der EBSI[4].
- Herkömmliches Verfahren

Für das herkömmliche Verfahren wurde von einem verteilten Datenbanksystem ausgegangen, bei dem für den Prozess der Lieferkette ein Workflowsystem verwendet wird.

Zusammenfassend lässt sich festhalten, dass EBSI vor allem hinsichtlich der Datenverteilung, Traceability und Prüfung des Prozesses einer Lieferkette, der Systemredundanz, Backup & Recovery oder Prozessnachweis, aufgrund der der DLT immanenten Eigenschaften, herkömmlichen Verfahren gegenüber von Vorteil ist. Nachteilig bleiben für DLT im Allgemeinen und EBSI im Besonderen, die derzeit noch fehlenden Sicherheitsstandards sowie Schwächen bei Servicemanagement und Skalierung. Mit dem QTSP für Ledger schafft die Neufassung der eIDAS klare Regelungen für Haftung, Betrieb und prüfbare Sicherheit in DLT. Sobald die notwendigen technischen Standards vorliegen, dürften die diesbezüglichen Nachteile behoben und DLT eine tatsächliche Alternative für herkömmliche Verfahren zur Lieferkettennachverfolgung darstellen. Dies gilt umso mehr, als dass die regulatorischen Vorgaben durch beide Verfahrensarten umsetzbar sind. Grundlegend ist jedoch festzustellen, dass DLT nur als Permissioned DLT die Anforderungen an die Lieferkettennachverfolgung erfüllen kann.

Herkömmliche Verfahren sind deutlich im Vorteil bei Fragen des Betriebs sowie der Informationssicherheit und Einsatz kryptographischer Mittel zum Authentizitäts- und Integritätsnachweis gemäß eIDAS. Dies liegt vor allem daran, dass diese Methoden für bestehende Verfahren etabliert, erprobt und umfänglich genutzt sind. Darüber hinaus sind herkömmliche Verfahren vorteilhaft bei weniger komplexen, also weniger verteilten Lieferketten, wo der hohe Aufwand eines verteilten Prozesses weniger ins Gewicht fällt. Des Weiteren sind die einfachere Nutzung von Identifizierungs-/ Authentisierungsmechanismen sowie etablierte Methoden für die langfristige Lesbarkeit und Prüfbarkeit zu nennen, was angesichts teilweise umfangreicher Aufbewahrungsfristen im Falle der Lieferkettennachverfolgung nicht zu unterschätzen ist.

Fazit

Mit dem QTSP für elektronische Ledger etabliert eIDAS einen dedizierten (qualifizierten) Vertrauensdienst für DLT. Durch die Integration von DLT in das eIDAS-Vertrauensrahmenwerk gelten alle Anforderungen an QTSP wie Haftung, Konformitätsbewertung durch unabhängige

[2] Vgl. https://trace4eu.eu/ - abgerufen am 23.02.2026

[3] Vgl. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI-ELSA+EUIPO - abgerufen am 23.02.2026

[4] Vgl. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home bzw. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/What+is+ebsi und https://hub.ebsi.eu/vc-framework - abgerufen am 23.02.2026

Konformitätsbewertungsstellen auch für DLT-Systeme, die von QTSP bereitgestellt werden. Dies gewährleistet nachgewiesene Sicherheit und das rechtliche Vertrauen, wie es u.a. für die Lieferkettennachverfolgung essentiell ist. Insofern kann QTSP für Ledger ein entscheidender Faktor für Industrie 4.0 sein, insbesondere in Sektoren wie Energie, Lieferkette und Fertigung. Industrielle Anwendungsfälle wie Third-Party Risk Management, Smart Manufacturing, digitale Produktpässe (DPPs) und Lieferkettenoptimierung können von einer qualifizierten DLT-Infrastruktur profitieren.

Wesentliche Voraussetzung für eine Anwendung der DLT für die Lieferkette bilden valide europäische Standards, die die eIDAS Verordnung technisch untersetzen und Interoperabilität mit der internationalen Standardisierung aufweisen. Diese sind aktuell in CEN JTC 19 (Europa) und ISO Tc 307 (international) in Entwicklung. Hinzu kommen die laufenden europäischen Projekte, die die Anwendung der DLT für die Lieferkette pilotieren. Diese Erfahrungen müssen in die Entscheidungsfindung zur Nutzung von DLT einfließen.

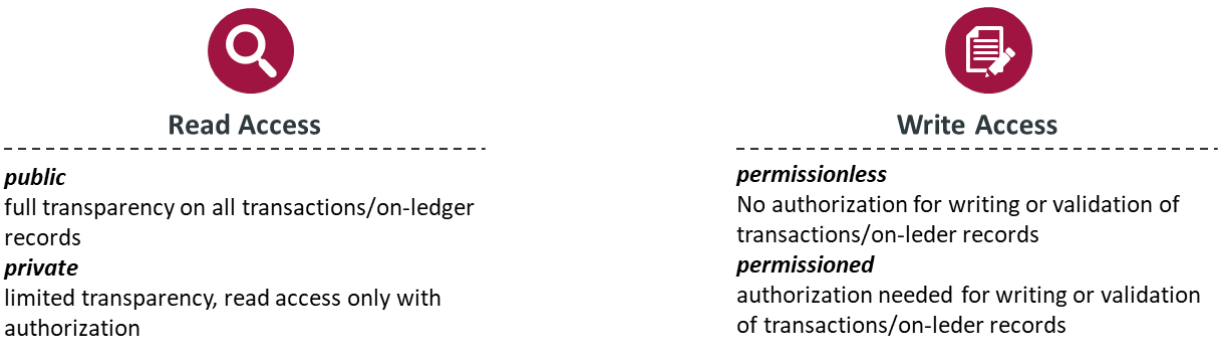
Zusammenfassend schafft eIDAS die Grundlage für eine sichere Nutzung von DLT u.a. für die Lieferkette. Für die praktische Anwendung über Forschungsprojekte hinaus sollten jedoch die Standardisierung sowie die Durchführungsrechtsakte der eIDAS (EUDI-Wallet und QEAA: November 2024) bzw. QTSP für Ledger (Mai 2025), die auf konkrete technische Standards verweisen werden, sowie die Anwendung von ETSI/CEN-Standards als Voraussetzung für EUDI-Wallet und qualifizierte Vertrauensdienste, abgewartet werden. Ohne diese Vorbedingungen erscheint eine Nutzung von DLT aufgrund mangelnder unabhängig geprüfter Sicherheit, fehlender klarer Haftungsregeln für den/die Betreiber des DLT-Systems sowie der mangelnden europäische Rechtsgrundlage, wie sie die eIDAS darstellt, für die Lieferkette kritisch. Dies bedeutet, dass DLT nur als Permissioned DLT die Anforderungen an die Lieferkettennachverfolgung erfüllen kann.

Summary

Introduction to DLT

Basically, DLT is a decentralized distributed peer-to-peer network of technical nodes for exchanging data and executing transactions. According to ISO 22739, in this case a distributed ledger is shared by a number of DLT nodes and synchronized between the DLT nodes using a consensus mechanism. The consensus mechanism ensures that all transactions are valid and unchanged. How consensus is reached depends on the type of DLT. The common misconception that DLT implies very high energy requirements only applies to some consensus mechanisms. In particular, Proof of Work (PoW) is one such mechanism, others are significantly more efficient, especially those in DLT with restricted access such as Byzantine Fault Tolerance (BFT), Proof of Authority (PoA) and Proof of Stake (PoS). DLT networks allow data or value to be transferred from one party to another without the involvement of intermediaries. Once transactions are written to the ledger, they are generally immutable, which relies mainly on the hash protection of the data stored on the DLT. Each transaction can be reliably tracked. When the actual distributed records or transactions are bundled in sequentially linked blocks, this is called a blockchain, a special form of DLT. The blocks can also contain the hash of the previous block and achieve immutability via hash chaining of the blocks and DLT timestamps. DLT timestamps and DLT cryptographic signatures differ from those according to eIDAS and related standards. The timestamps, unless generated by a (qualified) trust service (QTSP), lack a trusted time source, and the signatures, unless based on a certificate generated by a QTSP, lack the so-called Proof of Existence, which is created by a third party rather than by the DLT system itself. The hash-based integrity protection of each block is based on Merkle trees. This means that if authenticity or proof of existence is required within DLT, these must be added by (qualified) trust service providers. Similar challenges arise when the parties involved in a transaction are to be proven. In this case, DLT must be combined with external systems to ensure unique and trustworthy identification of legal and/or natural persons. Compared to the original ideas of public, permissionless DLTs, DLT does not necessarily require the elimination of an operator or consortium providing the distributed network. This depends on the type of DLT, which can differ in terms of access rights and transaction transparency. With public DLT, anyone can see all transactions and data, i.e. there is complete transparency, with private DLT only authorized users are allowed to read or execute transactions. With permissionless DLT, any user is allowed to validate and store transactions, with permissioned DLT this depends on the access rights and governance policies. The image below shows the basic types of DLT at a glance.

Abbildung 2: Types of DLT



Source: own illustration, msg systems ag

The following overview shows the main differences between DLT and traditional databases.

Tabelle 4: rough differences between DLT and traditional data bases

Attribute	DLT	Traditional database
Decentralization	Distributed betweeen nodes	Centralized on 1 or more servers
Alteration	Imutable	Not immutable
Transparency	Public (in case of public DLT)	Public (in case of public DLT)
Security	Depend on security measures	Depend on security measures
Scalability	Complex but scalable through hardware	Scalable through hardware

The European Blockchain Service Infrastructure (EBSI) is a key DLT network in Europe. EBSI is a pan-European DLT network provided by the member states. This means that the new operating organization Europeum/EDIC operates the main nodes and the basic infrastructure and ensures basic security, business continuity and service levels.

Proof of compliance in the supply chain

The purpose of supply chain tracking is essentially to prove compliance with legal requirements based on the records created in the process. It is therefore about proving the trustworthiness of the supply chain. To do this, clear and lossless proof of the authenticity, integrity and reliability of the business-relevant records created or received during transaction processing must be provided to courts, audit authorities and third parties until the applicable retention periods expire. It is essential for this to meet the additional protection goals of confidentiality.

Proof is provided to trusted third parties based on the records. The following requirements therefore constitute significant characteristics of business-relevant records:

- Authenticity
- Integrity
- Reliability
- Confidentiality
- Availability
- Transferability

The following table provides an overview of how DLT currently meets or fails to meet these requirements with or without additional measures. An assessment of DLT against these requirements leads to the following result:

Tabelle 5: Asessment DLT against Records Management

Requirements	Fulfilment	Justification
Integrity	Limited	Integrity is achieved through cryptographic security of the blocks (DLT) or transactions (DLT) No long-term stability due to the lack of rehashing and proof of existence
Authenticity	Limited	No standardized tools for the unambiguous assignment of transactions and data to the issuer/sender Additionally, clear identification of the issuer/sender is required, which is only possible in permissioned DLT and only with additional resources
Confidentiality	Limited	Only possible in permissioned DLT Fulfillment of the data subject's rights (erasure, data portability, rectification, etc.) is only possible if the content data is stored off-chain; Providing proof (duty to inform, consent) requires additional measures.
Availability	Limited	Effective scalability only possible with off-chain storage of content data Access only in DLT, i.e. no standardized means for data export of on-chain stored records no standardized mechanisms for long-term preservation of data stored in DLT
Reliability	Limited	Only in permissioned DLT; complete documentation requires additional measures through metadata, protocol information, etc., which are not available in DLT/DLT
Transferability	Limited	No standardized tools available for data export from DLT only possible with off-chain storage for data stored outside the DLT

Requirements on Supply Chain

Fundamental Requirements are:

Tabelle 6: Fundamental Requirements on Supply Chain

Category	Content
Regulatory	eIDAS
	DSGVO
	Supply Chain specific
Professional (based on regulation)	Burden of proof
	Process integration
Technical	Identification and Authenticiation
	Long-term preservation and provability
	Avoidance Single Point of Failure
	Backup & Recovery
	Cybersecurity
	System Integration
	Data Integration
	Operations and Business Continuity

Fulfilling the regulatory, professional and technical requirements requires the existence of one or more operators of a supply chain tracking system. This de facto limits the use of DLT to permissioned DLT. In addition, implementation is made easier by the new QTSP for ledgers according to eIDAS, as there is a direct operator with clear liability and tested security (conformity assessment according to eIDAS).

Comparison of DLT and conventional methods for supply chain tracking

The subject of the comparison is supply chain tracking. For this, it is fundamentally necessary to clearly identify the responsible legal entity and its acting persons and, if applicable, the affected product or its parts and to assign them to the relevant manufacturing company (product passport) as well as to prove the actual supply chain (i.e. the process) and to clearly assign it to the product and the companies involved.

The following methods were chosen:

- DLT: Europäische Blockchain Service Infrastructure
  - The EBSI was chosen as an example for DLT because it is being built up as a pan-European DLT infrastructure for the member states. In addition, supply chain tracking is currently being piloted on the EBSI by various projects, such as TRACE4EU, EBSI ELSA
  - The organisational (governance) and technical framework conditions of the EBSI apply.

- Conventional System

The conventional method was based on a distributed database system in which a workflow system is used for the supply chain process.

In summary, it can be said that EBSI has advantages over conventional methods, especially in terms of data distribution, traceability and testing of the supply chain process, system redundancy, backup & recovery or process proof, due to the inherent properties of DLT. The disadvantages for DLT in general and EBSI in particular remain the currently lacking security standards and weaknesses in service management and scaling. With the QTSP for ledgers, the new version of eIDAS creates clear regulations for liability, operation and verifiable security in DLT. As soon as the necessary technical standards are in place, the disadvantages in this regard can be remedied and DLT can represent a real alternative to conventional supply chain tracking methods. This is all the more true as the regulatory requirements can be implemented using both types of method. It should be noted, however, that DLT can only meet the requirements for supply chain tracking as permissioned DLT.

Conventional methods have a clear advantage when it comes to questions of operation and information security and the use of cryptographic means to prove authenticity and integrity in accordance with eIDAS. This is mainly because these methods are established, tested and widely used for existing procedures. In addition, conventional methods are advantageous for less complex, i.e. less distributed, supply chains, where the high cost of a comprehensive distributed process is less of an issue. Furthermore, the simpler use of identification/authentication mechanisms as well as established methods for long-term readability and auditability should be mentioned, which should not be underestimated in view of the sometimes extensive retention periods in the case of supply chain tracking.

Conclusion

With the QTSP for electronic ledgers, eIDAS is establishing a dedicated (qualified) trust service for DLT. By integrating DLT into the eIDAS trust framework, all QTSP requirements such as liability and conformity assessment by independent conformity assessment bodies also apply to DLT systems provided by QTSP. This ensures proven security and legal trust, which is essential for supply chain tracking, among other things. In this respect, QTSP for ledgers can be a decisive factor for Industry 4.0, especially in sectors such as energy, supply chain and manufacturing. Industrial use cases such as third-party risk management, smart manufacturing, digital product passports (DPPs) and supply chain optimization can benefit from a qualified DLT infrastructure.

An essential prerequisite for the application of DLT for the supply chain is valid European standards that technically support the eIDAS regulation and demonstrate interoperability with international standardization. These are currently being developed in CEN JTC 19 (Europe) and ISO Tc 307 (international). In addition, there are ongoing European projects that are piloting the application of DLT for the supply chain. These experiences must be incorporated into the decision-making process for the use of DLT.

In summary, eIDAS creates the basis for the secure use of DLT, among other things, for the supply chain. For practical application beyond research projects, however, standardization and the implementing acts of eIDAS (EUDI Wallet and QEAA: November 2024) or QTSP for Ledger (May 2025), which will refer to specific technical standards and define the application of ETSI/CEN standards as a prerequisite for EUDI Wallet and qualified trust services, should be awaited. Without these preconditions, the use of DLT for the supply chain appears critical due to the lack of independently verified security, the lack of clear liability rules for the operator(s) of

the DLT system and the lack of a European legal basis such as that provided by eIDAS. However, this means that DLT can only meet supply chain tracking requirements as permissioned DLT.

1 Einführung in Distributed Ledger Technologien

Distributed Ledger Technologien (DLT) sind ein Konzept, das das Potenzial hat, die Art und Weise, wie wir Informationen und Werte austauschen, grundlegend zu verändern. Im Gegensatz zu traditionellen Datenbanken, die zentralisiert verwaltet werden, werden DLT in einem dezentralisierten Netzwerk repliziert, das von mehreren Teilnehmern gemeinsam betrieben wird. Diese dezentrale Natur bietet eine Reihe von Vor- und Nachteilen, darunter erhöhte Sicherheit, Transparenz und Effizienz.

Ein wichtiger Bestandteil von DLT ist das Konzept des Konsenses. Jeder Teilnehmer im Netzwerk muss sich auf den aktuellen Zustand der Datenbank einigen. Dies wird durch verschiedene Algorithmen erreicht, die sicherstellen, dass alle Transaktionen validiert und in das Ledger aufgenommen werden. Dieser Konsensmechanismus macht DLT resistent gegen Manipulationen und Datenverluste, da es keine zentrale Stelle gibt, die kontrolliert oder verändert werden kann.

1.1 Electronic Ledger und Distributed Ledger

Die ISO 22739:2024[5] definiert die weltweite Terminologie im Themenkontext Ledger und Distributed Ledger. Sie wurde ins europäische Normungswerk übernommen und ist insofern Stand der Technik in Europa. Dementsprechend gelten die folgenden Definitionen:

- Ledger: Informationsspeicher, der Aufzeichnungen von Transaktionen speichert, die endgültig, definitiv und unveränderlich sein sollen
- Distributed Ledger: Ledger, der von einer Reihe von DLT-Knoten gemeinsam genutzt und mithilfe eines Konsensmechanismus zwischen den DLT-Knoten synchronisiert wird

Das bedeutet, dass DLT technisch gesehen nur eine spezielle Art von Ledger ist und die grundlegenden Eigenschaften wie Unveränderlichkeit sowie die Tatsache, dass Ledger-Aufzeichnungen per Definition endgültig sind, für jede Art von Ledger gelten. Der einzige Unterschied zwischen einem Ledger und einem Distributed Ledger ist die verteilte Organisation.

Der weithin bekannte Terminus Blockchain bezeichnet einen Distributed Ledger (3.23) mit bestätigten Blöcken, die in einer nur ergänzten, aber nicht veränderbaren, sequentiellen Kette mit Hash-Links organisiert sind. Das bedeutet, Blockchain ist eine DLT, die in Blöcken organisiert ist. Da dies nur auf eine Minderheit von DLT zutrifft, wird im Dokument der generelle Begriff DLT verwendet.

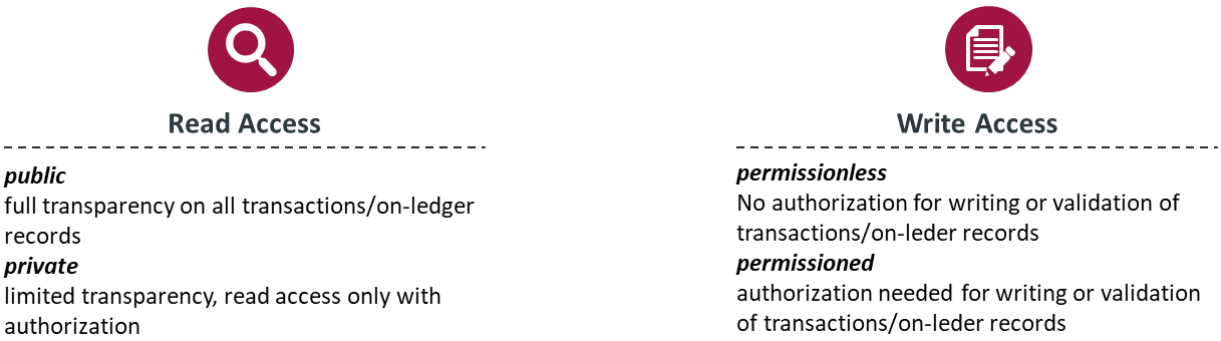
1.2 Einführung in DLT

Grundsätzlich ist DLT ein dezentral verteiltes Peer-to-Peer-Netzwerk aus technischen Knoten für den Datenaustausch und die Ausführung von Transaktionen. Gemäß ISO 22739 wird in diesem Fall ein Distributed Ledger von einer Reihe von DLT-Knoten gemeinsam genutzt und mithilfe eines Konsensmechanismus zwischen den DLT-Knoten synchronisiert. Der Konsensmechanismus stellt sicher, dass alle Transaktionen gültig und unverändert sind. Wie ein Konsens erreicht wird, hängt von der Art des DLT ab. Das weit verbreitete Vorurteil, dass DLT einen sehr hohen Energiebedarf impliziert, trifft nur auf einige Konsensmechanismen zu. Insbesondere Proof of Work (PoW) ist energieintensiv; andere Mechanismen sind deutlich effizienter, insbesondere solche in DLT mit eingeschränktem Zugriff wie Byzantine Fault Tolerance (BFT), Proof of Authority (PoA) und Proof of Stake (PoS). DLT-Netzwerke

[5] Vgl. https://www.iso.org/obp/ui/en/#iso:std:iso:22739:ed-2:v1:en- abgerufen am 23.02.2026

ermöglichen die Übertragung von Daten oder Werten von einer Partei zur anderen, ohne dass Zwischenhändler beteiligt sind. Sobald Transaktionen in das Ledger geschrieben sind, sind sie im Allgemeinen unveränderlich, was hauptsächlich auf dem Hash-Schutz der auf dem DLT gespeicherten Daten beruht. Jede Transaktion kann zuverlässig verfolgt werden. Wenn die tatsächlich verteilten Datensätze oder Transaktionen in sequenziell verknüpften Blöcken gebündelt sind, spricht man von einer Blockchain, einer speziellen Form von DLT. Die Blöcke können auch den Hash des vorherigen Blocks enthalten und über die Hashverkettung der Blöcke und DLT-Zeitstempel die Immutabilität erreichen. DLT-Zeitstempel und DLT-kryptografische Signaturen unterscheiden sich von denen gemäß eIDAS und verwandten Standards. DLT-Zeitstempeln fehlt – sofern sie nicht durch einen (qualifizierten) Vertrauensdiensteanbieter (QTSP) erzeugt wurden – eine vertrauenswürdige externe Zeitquelle. Ebenso fehlt kryptografischen Signaturen innerhalb von DLT-Systemen – sofern sie nicht auf einem durch einen QTSP ausgestellten Zertifikat beruhen – ein externer, rechtlich anerkannter Nachweis („Proof of Existence"), der durch einen unabhängigen Dritten erbracht wird. Der hashbasierte Integritätsschutz jedes Blocks basiert auf Merkle-Bäumen. Dies bedeutet, dass, wenn Authentizität oder Existenznachweis innerhalb von DLT erforderlich sind, diese von (qualifizierten) Vertrauensdiensteanbietern hinzugefügt werden müssen. Ähnliche Herausforderungen treten auf, wenn die an einer Transaktion beteiligten Parteien nachgewiesen werden sollen. In diesem Fall muss DLT mit externen Systemen kombiniert werden, um eine eindeutige und vertrauenswürdige Identifizierung von juristischen und/oder natürlichen Personen zu gewährleisten. Im Vergleich zu den ursprünglichen Ideen öffentlicher, erlaubnisfreier DLTs erfordert DLT nicht zwingend die Eliminierung eines Betreibers oder Konsortiums, das das verteilte Netzwerk bereitstellt. Dies hängt von der Art der DLT ab, die sich in Bezug auf Zugriffsrechte und Transaktionstransparenz unterscheiden kann. Bei öffentlicher DLT kann jeder alle Transaktionen und Daten einsehen, d. h. es herrscht vollständige Transparenz, bei privater DLT dürfen nur autorisierte Benutzer Transaktionen lesen oder ausführen. Bei permissionless DLT darf jeder Benutzer Transaktionen validieren und speichern, bei permissioned DLT hängt dies von den Zugriffsrechten und Governance-Richtlinien ab. Das nachstehende Bild zeigt die grundlegenden Arten von DLT im Überblick.

Abbildung 3: Arten DLT im Überblick



Quelle: eigene Darstellung, msg systems ag

Darüber hinaus wird DLT hinsichtlich der Datenspeicherung unterschieden: On-Chain, wenn Daten im Ledger gespeichert werden, oder Off-Chain, wenn Daten in DLT nur durch Hash repräsentiert werden. Die Transaktionen in der DLT werden anhand der on-chain records und off-chain records nachgewiesen. Dabei ist der Stand der Technik zum Records Management zu gewährleisten.

Distributed Ledger Technologien funktionieren im Kern auf Basis eines dezentralisierten Netzwerks von Computern, die alle eine Kopie des Ledgers speichern. Dieses Netzwerk arbeitet

zusammen, um neue Transaktionen zu verifizieren und in das Ledger einzutragen. Der Prozess der Transaktionsverarbeitung ist in der Regel in mehrere Schritte unterteilt:

1. Transaktionserstellung: Ein Teilnehmer im Netzwerk initiiert eine Transaktion, beispielsweise eine Überweisung von Geld oder den Austausch von digitalen Vermögenswerten. Die Transaktion wird in einem bestimmten Format kodiert und an das Netzwerk gesendet.
2. Verifikation und Validierung: Die Transaktion wird von den Knoten im Netzwerk geprüft, um sicherzustellen, dass sie gültig ist und den Regeln des jeweiligen Konsensmechanismus entspricht. Die Knoten prüfen die Transaktionsdetails, die digitalen Signaturen und den verfügbaren Saldo des Absenders.
3. Konsensbildung: Die Knoten im Netzwerk müssen sich auf den aktuellen Zustand des Ledgers einigen. Dies erfolgt durch einen Konsensmechanismus, der je nach DLT-System variieren kann. Beliebte Mechanismen sind Proof-of-Work (PoW), Proof-of-Stake (PoS) oder Byzantine Fault Tolerance (BFT).
4. Blockbildung und -verankerung: Sobald ein Konsens über die Gültigkeit einer Transaktion erzielt wurde, wird sie in einen Block zusammengefasst. Dieser Block enthält weitere Transaktionen und Metadaten wie den Zeitstempel und den Hash des vorherigen Blocks. Der Block wird dann an das Ledger angehängt, wodurch die Daten dauerhaft und unveränderlich aufgezeichnet werden.
5. Verbreitung und Replikation: Der neue Block wird an alle Knoten im Netzwerk verteilt, wodurch alle Teilnehmer über die gleiche Version des Ledgers verfügen. Diese Replikation sorgt für die Sicherheit und Integrität des Ledgers.

Bei Netzwerken unterscheidet man zwischen asynchronem, partiell synchronem und synchronem Verhalten. Dies bezieht sich auf die Laufzeit von Nachrichten zwischen verschiedenen Knoten. Für das Fehlverhalten von Knoten stellen Crash-Fehler (einfacher Absturz) sowie byzantinische Fehler (beliebiges Verhalten inkl. gezielter Angriffe auf den Konsensmechanismus) die wesentlichen Optionen dar. Das angenommene Verhalten des Netzwerks, die Art des tolerierten Fehlverhaltens und die Anzahl der Knoten bestimmen die Ausfallsicherheit des Systems.

1.3 Wesentliche Sicherheitsmerkmale von DLT

1.3.1 Grundsatz

Die Sicherheit und Vertraulichkeit von Transaktionen in DLT-Netzwerken wird aktuell durch mehrere Mechanismen gewährleistet:

1. Kryptografische Absicherung

   DLT-Systeme beinhalten eine kryptographische Sicherung der on-chain records, die durch verkettete Hashwerte geschützt werden. Ein Proof of Existence in Form externer Zeitstempel besteht jedoch nicht.

2. Dezentrale Struktur

   Ein wesentliches Merkmal verteilter Ledger-Technologien ist die Dezentralisierung. Im Gegensatz zu traditionellen Systemen, die von einer zentralen Instanz kontrolliert werden, sind DLT in einem Netzwerk von Teilnehmern verteilt, die gemeinsam das

Ledger verwalten. Diese dezentrale Architektur trägt zur Widerstandsfähigkeit des Systems bei, da es keine einzelne Schwachstelle (Single Point of Failure) gibt, die angegriffen werden könnte. Selbst wenn ein Knoten kompromittiert wird, können andere Knoten die Integrität des Netzwerks aufrechterhalten.

3. Unveränderbarkeit / Sicherheit

   Distributed Ledger Technologien zeichnen sich durch ein hohes Maß an Sicherheit und Unveränderbarkeit aus. Diese Eigenschaften resultieren aus der dezentralen Architektur und den kryptografischen Verfahren, die bei DLT eingesetzt werden.

   Die Unveränderbarkeit der Daten in einem verteilten Ledger ist ein wesentlicher Vorteil. Sobald eine Transaktion in das Ledger aufgenommen wurde, gilt sie grundsätzlich als nicht mehr nachträglich veränderbar. Dieser Schutz vor Manipulationen ist auf die kryptografischen Hash-Funktionen zurückzuführen, die zur Verknüpfung der Blöcke in der DLT verwendet werden. Jede Änderung an einem Block würde den Hash des Blocks verändern, was wiederum die Hashes aller nachfolgenden Blöcke beeinflussen würde.

   Die Sicherheit von DLT wird durch die dezentrale Natur des Netzwerks und den Einsatz von kryptografischen Verfahren verstärkt. Da das Ledger in mehreren Kopien vorhanden ist, die von verschiedenen Teilnehmern verwaltet werden, ist es schwieriger, das System zu manipulieren oder Daten zu fälschen. Darüber hinaus ermöglichen kryptografische Verfahren wie digitale Signaturen und Verschlüsselung den sicheren Austausch von Informationen und die Authentifizierung von Teilnehmern.

   Die Sicherheit und Unveränderbarkeit von DLT bieten ein hohes Maß an Vertrauen und Zuverlässigkeit, das für verschiedene Anwendungsfälle unerlässlich ist. Dies ermöglicht den sicheren Austausch von Werten, die Verwaltung von digitalen Assets und die Durchführung von Transaktionen in einem transparenten und nachvollziehbaren Umfeld.

4. Zugriffskontrollen

   In geschlossenen (permissioned) DLT-Systemen können Zugriffsrechte fein granular gesteuert werden, um die Vertraulichkeit zu wahren.

5. Datenschutzmaßnahmen

   Einige DLT-Implementierungen ermöglichen es, dass nicht alle Daten bei allen Teilnehmern gespeichert werden, sondern in Unternetzwerken ausgetauscht werden, um die Vertraulichkeit zu erhöhen.

6. Auditfähigkeit

   Die Unumkehrbarkeit und Nachverfolgbarkeit jeder einzelnen Transaktion machen DLT-Systeme jederzeit auditfähig, was zur Sicherheit beiträgt.

1.3.2 Berechtigungsmanagement in DLT

Bei Distributed Ledger Technologien (DLT) können die Interaktionsrechte je nach Implementierung und Anwendungsfall variieren. Grundsätzlich lassen sich zwei Hauptkategorien von DLT-Systemen unterscheiden:

1. Permissionless DLT
2. Permissioned DLT

diese unterteilen sich jeweils in öffentliche und private DLT-Systeme:

1.3.2.1 Permissionless DLT

In diesen Systemen kann prinzipiell jeder teilnehmen und mit dem Netzwerk interagieren. Es wird unterschieden in:

Public Permissionless DLT

Die Teilnehmer haben folgende Rechte:

- Lesen der Daten im Ledger
- Schreiben von Daten auf den Ledger
- Initiieren von Transaktionen
- Validieren von Transaktionen
- Teilnahme am Konsensmechanismus

Eine **Public permissionless** DLT ist eine spezielle Form von DLT-Systemen mit folgenden Hauptmerkmalen:

- Öffentlicher Zugang: Jeder kann ohne Einschränkungen oder besondere Berechtigung am Netzwerk teilnehmen
- Anonymität: Teilnehmer können anonym oder pseudonym bleiben
- Hohe Dezentralisierung: Es gibt keine zentrale Kontrolle oder Autorität über das Netzwerk
- Transparenz: Alle Transaktionen sind für alle Teilnehmer sichtbar
- Konsensmechanismen: Entscheidungsfindung und Transaktionsverifizierung erfolgen durch Mechanismen wie Proof-of-Work oder Proof-of-Stake
- Open Source: Häufig basieren diese Systeme auf Open-Source-Code
- Hohe Performance: Durch die große Anzahl von Netzwerkknoten wird eine hohe Netzwerkstabilität erreicht
- Tokenisierung: Oft werden Token oder digitale Assets als Anreiz zur Teilnahme verwendet
- Beispiele: Bitcoin und Ethereum sind bekannte Vertreter von public permissionless DLTs
- Herausforderungen: Diese Systeme können Probleme mit Skalierbarkeit und Energieeffizienz haben, da die Verifizierung durch viele Teilnehmer ressourcenintensiv ist

Public permissionless DLTs bieten also maximale Offenheit und Dezentralisierung, was sie für Anwendungen attraktiv macht, die breite Teilnahme und Transparenz erfordern, aber möglicherweise weniger geeignet für Szenarien, die hohe Sicherheit, Nachvollziehbarkeit und Datenschutz erfordern, da hierfür insbesondere die Prüfbarkeit durch Dritte, die eindeutige Zuweisbarkeit von Transaktionen zu natürlichen und/oder juristischen Personen sowie ein differenziertes Zugangs- und Berechtigungsmanagement erforderlich sind.[6]

Private Permissionless DLT

Alle Teilnehmer haben folgende Rechte:

- Schreiben von Daten auf den Ledger
- Initiieren von Transaktionen

Nur berechtigte Nutzer besitzen folgende Rechte:

- Lesen der Daten im Ledger
- Validieren von Transaktionen

Ein **privates permissionless** DLT-System kombiniert Elemente von privaten und öffentlichen DLTs:

- Permissionless Zugang: Wie bei öffentlichen DLTs kann jeder einen Knoten betreiben und dem Netzwerk beitreten, ohne eine zentrale Autorität um Erlaubnis bitten zu müssen
- Private Daten: Im Gegensatz zu öffentlichen DLTs werden jedoch nicht alle Daten mit allen Teilnehmern geteilt. Stattdessen werden private Ad-hoc-Ketten für einzelne Smart Contracts erstellt.
- Zugriffskontrollen: Smart Contracts definieren nicht nur, wer Aktionen ausführen darf, sondern auch wer Zugriff auf die Vertragsdaten hat
- Mehrere Ketten: Ein einzelner Knoten kann mehrere dieser privaten Ad-hoc-Ketten enthalten, aber nie alle
- Hybride Architektur: Es wird eine Kombination aus privaten Event-Ketten und einer öffentlichen DLT-Ebene verwendet

Diese Architektur ermöglicht es, die Vorteile eines permissionless Systems (wie breite Teilnahme und Dezentralisierung) mit den Vorteilen privater DLT (wie Zugriffskontrollen) zu kombinieren. Dies unterscheidet sich von rein öffentlichen permissionless DLT-Protokollen wie Ethereum, wo alle Daten für alle Teilnehmer sichtbar sind. Dieser Ansatz zielt zudem darauf ab, die Skalierbarkeit beizubehalten.

Nachteile von Private Permissionless DLT sind u.a.:

- Eingeschränkte Transparenz der on-chain records

[6] Vgl. Kap. 1.7

- Abhängigkeit von einem oder mehreren Betreibern des DLT-Systems
- Eingeschränkte Dezentralisierung

1.3.2.2 Permissioned DLT

Hier wird der Zugang zum Netzwerk kontrolliert. Die Interaktionsrechte können je nach Rolle des Teilnehmers unterschiedlich sein:

- Lesezugriff: Berechtigung on-chain records einzusehen
- Schreibzugriff: Berechtigung, Transaktionen zu initiieren
- Validierungsrechte: Teilnahme am Konsensprozess zur Bestätigung von Transaktionen

Private Permissioned DLT

Eine Private permissioned DLT ist eine spezielle Form von Distributed Ledger Technologien mit folgenden Hauptmerkmalen:

- Geschlossenes Netzwerk: Im Gegensatz zu öffentlichen DLTs handelt es sich um geschlossene Netzwerke, zu denen nur ausgewählte Teilnehmer Zugang haben
- Zugriffskontrolle: Eine zentrale Autorität oder ein Konsortium bestimmt, wer am Netzwerk teilnehmen und Transaktionen validieren darf
- Teilweise Dezentralisierung: Das System ist über die bekannten Teilnehmer verteilt, aber nicht vollständig dezentralisiert wie öffentliche DLTs
- Kontrollierte Transparenz: Die Sichtbarkeit von Daten und Transaktionen wird basierend auf den Zielen der teilnehmenden Organisationen gesteuert
- Keine Anonymität: Die Identitäten der Teilnehmer sind bekannt
- Entwicklung durch private Einheiten: Diese Systeme werden in der Regel von Unternehmen oder Konsortien für spezifische Anwendungsfälle entwickelt
- Höhere Leistung und Skalierbarkeit: Da weniger Knoten Transaktionen validieren müssen, können diese Systeme oft schneller und effizienter arbeiten als öffentliche DLTs
- Verbesserte Privatsphäre: Sensible Geschäftsinformationen können besser geschützt werden
- Anwendungsfälle: Häufig eingesetzt für Supply Chain Management, Identitätsverifizierung oder Schadensregulierung in der Versicherungsbranche

Private permissioned DLTs bieten also mehr Kontrolle und Datenschutz als öffentliche Systeme, opfern dafür aber einen Teil der Dezentralisierung und Transparenz. Sie eignen sich besonders für Unternehmen und Organisationen, die sensible Daten verarbeiten und gleichzeitig die Vorteile der DLT-Technologie nutzen möchten. Wesentlicher Vorteil gegenüber zentralen Datenbanksystemen ist die Verteilung der Nodes über Jurisdiktionen und Organisationen hinweg sowie die lückenlose Dokumentation aller Transaktionen im Netzwerk.

Nachteile von Private Permissioned DLT sind u.a.:

- Eingeschränkte Transparenz der on-chain records
- Abhängigkeit von einem oder mehreren Betreibern des DLT-Systems
- Eingeschränkte Dezentralisierung

Public Permissioned DLT

Eine public permissioned DLT kombiniert Elemente öffentlicher und privater DLT. Sie ist öffentlich zugänglich, erfordert aber eine Identitätsverifizierung der Teilnehmer.

- Offener Zugang: Jeder kann prinzipiell teilnehmen, muss aber bestimmte Voraussetzungen erfüllen und sich identifizieren
- Identitätsnachweis: Im Gegensatz zu public permissionless DLTs müssen Teilnehmer ihre Identität offenlegen
- Dezentrale Governance: Trotz Zugangskontrolle wird ein dezentrales Governance-Modell verwendet, ähnlich wie bei öffentlichen DLT
- Kontrolle und Transparenz: Es gibt eine Balance zwischen der Offenheit öffentlicher Netzwerke und der Kontrolle privater Konsortien
- Anwendungsbereich: Besonders geeignet für regulierte Bereiche wie die Finanzindustrie, wo Identitätsverifizierung wichtig ist

Public Permissioned DLT kombinieren im Kern die Sicherheit und Kontrolle privater DLTs mit der Offenheit und Dezentralisierung öffentlicher Systeme. Sie sind mit herkömmlichen Public Key-Infrastrukturen vergleichbar, die nach einem ähnlichen Berechtigungssystem funktionieren.

Nachteile von Public Permissioned DLT sind u.a.:

- Abhängigkeit von einem oder mehreren Betreibern des DLT-Systems
- Keine Dezentralisierung

1.4 Smart Contracts

Smart Contracts sind ein wichtiger Bestandteil von verteilten Ledger-Technologien (DLT). Sie sind im Wesentlichen selbstauführende Programme, die in der DLT gespeichert werden und die Ausführung von Vereinbarungen zwischen verschiedenen Parteien automatisieren. Diese Programme werden durch einen Code definiert, der die Regeln und Bedingungen des Vertrags festhält. Sobald ein Smart Contract in die DLT aufgenommen wurde, gilt er grundsätzlich als nicht mehr nachträglich veränderbar. Dies führt einerseits zu hoher Sicherheit und Zuverlässigkeit, erfordert andererseits jedoch ein komplexes Berechtigungssystem, um Fehleinträge im Ledger bzw. aufwändige Blacklisting-Verfahren zu vermeiden.

Smart Contracts weisen eine Reihe von Eigenschaften auf, die potenziell vorteilhaft sein können, darunter:

- Automatisierung: Sie automatisieren Prozesse und reduzieren den Bedarf an manuellen Eingriffen und Vermittlern.
- Transparenz und Nachverfolgbarkeit: Alle Aktionen und Daten, die mit einem Smart Contract verbunden sind, werden in der DLT aufgezeichnet und sind jederzeit nachvollziehbar.

- Sicherheit und Zuverlässigkeit: Smart Contracts sind unveränderlich und resistent gegen Manipulationen, was sie zu einer sicheren und zuverlässigen Grundlage für Vertragsabwicklung macht.
- Beschleunigung: Sie beschleunigen Transaktionen und Prozesse, wodurch die Abwicklung von Vereinbarungen schneller und potenziell effizienter wird.
- Reduzierte Kosten: Durch die Automatisierung von Prozessen und die Reduzierung des Bedarfs an Vermittlern können Smart Contracts die Kosten für Vertragsabwicklung senken.

Wesentliche Nachteile wären u.a.:

- Technische Komplexität
- Umfangreiches Berechtigungssystem im DLT-System notwendig
- Derzeit begrenzte Standardisierung[7]

Im Kern können Smart Contracts als Workflowanwendungen in DLT bezeichnet werden. Kritisch zu betrachten ist die Limitierung vieler DLT-Systeme, direkt auf Off-Chain-Daten zugreifen zu können. Konkrete Lösungen hierzu sind in der internationalen Standardisierung in Entwicklung.

[7] ETSI begann einen Technischen Report, Konkrete Standards sind in ISO Tc 307 erst in Entwicklung

1.5 Kurzüberblick wesentlicher Protokolle

Tabelle 7: Vergleich Ethereum, Hyperledger Fabric und R3 Corda (Stand 2019)

Typ	Ethereum	Hyperledger Fabric	R3 Corda
Entwicklung	Open-source	IBM, Open-source	R3, Open-source
Typ	Public, permissionless; Enterprise Versionen sind private oder public permissioned (dann als Hyperledger BESU)	Private, permissioned	Private, permissioned
Version	Constantinople (Istanbul in Okt 2019)	1.4.3 (Stable – Aug 2019) 2.0 (Alpha – Apr 2019)	4.1 (Juni 2019)
Messaging	Peer-to-peer, vollständige Übertragung	"Channel" peer-to-peer, vollständige Übertragung	Point-to-point
Vertraulichkeit	Vollständige Übertragung Transaktionen können verschlüsselt werden, so dass nur einige Knoten lesen können, aber alle Knoten haben eine Kopie. State Channels können für Vertraulichkeit genutzt werden. Volle Vertraulichkeit äquivalent Corda kann durch Hyperledger BESU erreicht werden, das auf Ethereum aufsetzt und mittlerweile meistgenutzte Ethereum Derivat darstellt.	Vollständige Übertragung im Channel Transaktionen können verschlüsselt werden, so dass nur einige Knoten lesen können, aber alle Knoten haben eine Kopie. Private Daten können Point-to-point zwischen Peers geteilt werden.	Volle Vertraulichkeit, nur beteiligte Knoten sehen die Transaktion. Transaktionen können auch verschlüsselt werden.
Transaktions-aufzeichnungen	Alle Knoten können alle Transaktionen sehen, inkl. Historie.	Alle Knoten in einem „Channel" können alle Transaktionen sehen, inkl. Historie.	Nur betroffene Knoten können Transaktionen sehen, an denen sie beteiligt sind.
Konsensmodell	Order – Execute – Validate	Order – Execute – Validate	Order – Execute – Validate
Verfügbare Konsens-algorithmen	Proof-of-Work Proof-of-Stake Proof-of-Authority (BFT) Raft (CFT mit Leader) Istanbul BFT (mit Endgültigkeit)	SOLO Kafka (CFT mit Leader) Raft (CFT mit Leader)	Notary

Typ	Ethereum	Hyperledger Fabric	R3 Corda
Smart Contract Sprache	Solidity, Serpent Deterministisch	FabToken verfügbar in Fabric 2.0 Alpha, aber nicht in 1.4.3 Stable	Token Anwendung verfügbar ab Corda 5.0

1.5.1 Token in DLT

Ein Distributed-Ledger-Token oder ein DLT-Token stellt die Abstraktion eines intrinsischen oder extrinsischen Vermögenswertes, einer Währung, von Rechten oder Eigentum dar. Sie werden bspw. in folgenden Anwendungsfällen verwendet:

- Crypto-Assets, im Sinne der MiCAR[8]
- Repräsentation geistigen oder realen Eigentums wie in den Projekten TRACE4EU[9] oder EBSI ELSA[10] pilotiert[11]
- Abbildung digitaler Zwillinge (Digital Twins)

Token können fungibel sein, sodass eine einzelne Einheit des Tokens ohne Unterschiede in Wert oder Funktion durch eine andere ersetzt werden kann, oder nicht fungibel, sodass jedes Token einzigartig und nicht austauschbar ist.

Ein Beispiel für einen fungiblen Token wäre ein Token, der den Anteil des Eigentums an einem Produkt repräsentiert, dessen Lieferkette über die DLT nachvollzogen werden soll, wobei jeder Token z.B. 10% des Eigentums am Produkt repräsentiert, also 10 Eigentumstoken existieren würden. Ein nicht fungibler Token (NFT) ist ein eindeutiger, nicht austauschbarer Token, der typischerweise einen bestimmten einzelnen Vermögenswert oder ein spezifisches Produkt repräsentiert. Diese beiden Tokens sind nicht austauschbar und jedes ist eine eindeutige Darstellung eines Vermögenswertes. Ebenso gilt Bargeld als fungibel, während Identität grundsätzlich nicht fungibel ist.

Token, die intrinsische Vermögenswerte darstellen, sind solche, bei denen das Eigentum innerhalb der DLT selbst gebunden ist. Auf diese Weise liegen das Eigentum und die Gewalt über den intrinsischen Vermögenswert im Private Key des Tokens. Extrinsische Vermögenswerte sind solche, bei denen die Rechtmäßigkeit oder Realität des Eigentums außerhalb der DLT liegt, die Vermögenswerte aber im Ledger abgebildet sind.

Tabelle 8: Vergleich der Token in Ethereum, Hyperledger Fabric und R3 Corda

Typ	Ethereum	Hyperledger Fabric	R3 Corda
Typ (Space)	Fungible und nicht fungible Token-Standards verfügbar	Nur Standard für fungiblen Token verfügbar	Fungible und nicht fungible Token-Standards verfügbar

[8] Vgl. REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

[9] Vgl. https://trace4eu.eu/ - abgerufen am 23.02.2026

[10] Vgl. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI-ELSA+EUIPO - abgerufen am 23.02.2026

[11] Vgl. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI+Ecosystem+Day+Agenda - abgerufen am 23.02.2026

Typ	Ethereum	Hyperledger Fabric	R3 Corda
Typ (Time)	Fixe und veränderliche Token-Funktionen in verschiedenen Standards verfügbar	Nur fixe Funktionen verfügbar	Fixe und veränderliche Token-Funktionen verfügbar
Tokenmodell	Token-Implementierung basierend auf dem Account-Modell	Token-Implementierung basierend auf dem UTXO-Modell	Token-Implementierung basierend auf dem UTXO-Modell
Standard Implementation	Uneingeschränkte Token-Implementierung durch Smart Contracts ohne Anforderungen an die Einhaltung von Standards	Uneingeschränkte Token-Implementierung mit Chaincode ohne Anforderungen an die Einhaltung von Standards	Uneingeschränkte Token-Implementierung mit States und Flows ohne Anforderungen an die Einhaltung von Standards, jedoch wurden die Standardbibliotheken aktualisiert (Corda 4.1), um Token-Datentypen aufzunehmen.
Standards	EIP-20, EIP-777, EIP-1155, EIP-721	FabToken	Corda Token Management System
Status des Standards	Production/Final	Alpha	Beta
Integration mit Protokoll	Integration auf Smart Contract Level, nicht Protokoll-Level	FabToken kann derzeit nicht mit Chaincode interagieren.	Integration mit States und Flows

1.6 Unterschiede zwischen DLT und traditionellen Datenbanken

Tabelle 9: Wesentliche Unterschiede DLT und traditionelle Datenbanken

Merkmal	DLT	Traditionelle Datenbank
Dezentralisierung	Verteilt auf mehrere Knoten	Zentralisiert auf einem Server
Veränderbarkeit	Unveränderlich	Veränderbar
Transparenz	Öffentlich einsehbar (bei Public DLT)	Zugriffskontrolle
Sicherheit	Abhängig von Sicherheitsmaßnahmen	Abhängig von Sicherheitsmaßnahmen
Skalierbarkeit	Komplex, aber skalierbar durch Hardware	Skalierbar durch Hardware

Die Tabelle verdeutlicht die wichtigsten Unterschiede zwischen DLT-Technologien und traditionellen Datenbanken. Während traditionelle Datenbanken zentralisiert und veränderbar sind, zeichnen sich DLTs durch Dezentralisierung, Unveränderlichkeit und Transparenz (für Public DLT) aus. Diese Eigenschaften machen DLT-Technologien besonders geeignet für Anwendungen, die Sicherheit, Transparenz und Vertrauen erfordern.

1.7 DLT und Nachweisfähigkeit

1.7.1 Grundsatz

Der Sinn einer Lieferkettennachverfolgung besteht im Kern im Nachweis der gesetzlichen Vorgaben[12] anhand der im Prozess entstehenden Aufzeichnungen. Es geht also darum, die Vertrauenswürdigkeit der Lieferkette nachzuweisen. Hierfür muss der eindeutige wie verlustfreie Nachweis der Authentizität, Integrität und Zuverlässigkeit der bei der Transaktionsabwicklung entstehenden oder empfangenen geschäftsrelevanten Aufzeichnungen bis zum Ablauf der geltenden Aufbewahrungsfristen gegenüber Gerichten, Prüfbehörden, Dritten erbracht werden. Wesentlich hierfür ist die Erfüllung der Schutzziele Vertraulichkeit und Verfügbarkeit einschließlich der Verkehrsfähigkeit der Aufzeichnungen. Der Nachweis wird gegenüber vertrauenswürdigen Dritten anhand der Aufzeichnungen erbracht. Die folgenden Anforderungen bilden damit signifikante Eigenschaften geschäftsrelevanter Aufzeichnungen:

- Authentizität
- Integrität
- Zuverlässigkeit
- Vertraulichkeit

[12] Vgl. Kap. 2

- Verfügbarkeit
- Verkehrsfähigkeit

Diese Anforderungen an vertrauenswürdige digitale Transaktionen sind technologieunabhängig und müssen auch in DLT-Systemen verlustfrei bis zum Ablauf der jeweiligen Aufbewahrungsfristen der einzelnen Aufzeichnungen gewährleistet werden. Es muss auch bei der Nutzung von DLT möglich sein, die darin abgewickelten Transaktionen anhand der signifikanten Eigenschaften geschäftsrelevanter Aufzeichnungen gegenüber vertrauenswürdigen Dritten nach dem Stand der Technik nachzuweisen. Dies ist so lange erforderlich, wie die geschäftsrelevanten Aufzeichnungen benötigt werden. Hierfür ist zum einen ein ordnungsgemäßes Records Management, zum anderen der verlustfreie Erhalt des Beweiswerts der Aufzeichnungen und Transaktionen anhand der eigentlichen Aufzeichnungen, also der on-chain records und off-chain records notwendig.

1.7.2 Nachweisfähigkeit in DLT

Aufgrund von Leistungseinschränkungen und Datenschutzgesetzen wie der DSGVO wird derzeit häufig Off-Chain-Speicherung verwendet. DLT kann als verteiltes System charakterisiert werden, das sein Vertrauen aus der durch kryptografische Verfahren gesicherten Unveränderlichkeit, der Integrität der Daten sowie der durch den Konsensmechanismus gewährleisteten Konsistenzprüfung (nicht jedoch einer Vollständigkeitsprüfung) bezieht. Jede unbefugte Änderung ist so transparent und im besten Fall ist keine zentrale Autorität oder kein Vermittler erforderlich. Dies bedeutet, dass DLT normalerweise nur in verteilten Ökosystemen mit mehr als zwei beteiligten Parteien (vorzugsweise privaten Institutionen) nützlich ist, wo die Verteilung sinnvoll ist und die Parteien einander normalerweise technisch nicht vertrauen, sodass Vertrauen in die Korrektheit der Technologie notwendig erscheint.

Wenn DLT für vertrauenswürdige digitale Transaktionen verwendet werden soll, ist es zwingend erforderlich, Anforderungen an das Records Management zu erfüllen, einschließlich der langfristigen Aufbewahrung der Beweise für maßgebliche Aufzeichnungen, auch gegenüber Dritten, bis zum Ende der geltenden Aufbewahrungsfristen. Dies bedeutet, dass ein ordnungsgemäßes Records Management einschließlich Beweissicherung obligatorisch ist. Die folgende Tabelle zeigt einen Überblick, wie DLT diese Anforderungen derzeit mit oder ohne zusätzliche Maßnahmen erfüllt oder nicht erfüllt. Eine Bewertung der DLT anhand dieser Anforderungen führt zu folgendem Ergebnis:

Tabelle 10: Bewertung DLT hinsichtlich signifikanter Eigenschaften geschäftsrelevanter Aufzeichnungen

Kernanforderung	Erfüllung	Begründung
Integrität	Bedingt	Unveränderlichkeit wird durch die kryptographische Sicherung der Blöcke (DLT) resp. der Transaktionen (DLT) erreicht. Keine Langzeitstabilität, aufgrund des fehlenden Rehashings und Proof of Existence
Authentizität	Bedingt	Keine standardisierten Werkzeuge zur eindeutigen Zuweisbarkeit von Transaktionen und Daten zum Aussteller/Absender

Kernanforderung	Erfüllung	Begründung
		Ergänzung bedarf eindeutiger Identifizierung der Aussteller/Absender, was nur in permissioned DLT und nur mit Zusatzmitteln möglich ist.
Vertraulichkeit	Bedingt	Nur in permissioned DLT möglich Erfüllung der Rechte des Betroffenen (Löschung, Datenübermittlung, Berichtigung etc.) nur bei off-chain-Speicherung der Inhaltsdaten möglich; Nachweisführung (Informationspflicht, Einwilligung) bedarf zusätzlicher Maßnahmen.
Verfügbarkeit	Bedingt	Effektive Skalierbarkeit nur bei off-chain-Speicherung der Inhaltsdaten möglich. Zugriff nur in DLT, d.h. keine standardisierten Mittel zum Datenexport on-chain gespeicherter Aufzeichnungen keine standardisierten Mechanismen zum Langzeiterhalt der in DLT abgelegten Daten
Zuverlässigkeit	Bedingt	Nur in permissioned DLT; vollständige Dokumentation bedarf zusätzlicher Maßnahmen durch Metadaten, Protokollinformationen etc., die in DLT/DLT nicht vorhanden sind.
Verkehrsfähigkeit	Bedingt	Keine standardisierten Werkzeuge zum Datenexport aus DLT vorhanden nur bei off-chain-Speicherung für die außerhalb der DLT gespeicherten Daten möglich

Als Schlussfolgerung anhand der wesentlichen Anforderungen an das Records Management zur Nachweisbarkeit digitaler Transaktionen wie der Lieferkettennachverfolgung kann festgestellt werden, dass DLT weitere, zusätzliche Maßnahmen benötigt, um die Durchführung vertrauenswürdiger digitaler Transaktionen zu ermöglichen. Darüber hinaus können derzeit nur DLT mit mindestens eingeschränkten Schreibrechten für die Teilnehmer, also public- oder private permissioned DLT, einschließlich einer Off-Chain-Speicherung der wesentlichen Datensätze empfohlen werden. Nur Daten über die Transaktion, nicht der Inhalt selbst, sollten On-Chain gespeichert werden.

1.8 Herausforderungen und Stand der Technik von DLT

Neben aktuell mangelnden Funktionen zum Nachweis digitaler Transaktionen umfasst DLT einige technische Herausforderungen, die die Anwendung im regulierten Umfeld wie z.B. Lieferkettennachverfolgung derzeit erheblich einschränken:

- Standardisierte Maßnahmen gegen allgemeine und Ledger-spezifische Cyberangriffe
- Stabilität der verwendeten Kryptoalgorithmen und Proof of Existence
- Sicherheit bei Smart Contracts, Konsensmechanismus
- Geschäftskontinuität und Migration im Falle einer Beendigung des Netzwerks

- Qualifizierung der DLT nativen Signaturen und Zeitstempel hinsichtlich der eIDAS Verordnung in Europa
- Audit und Zertifizierung eines DLT-Netzwerks hinsichtlich Informationssicherheit, Datenschutz, Business Continuity oder Service Management

Die notwendigen internationalen Standards zur Lösung dieser Herausforderungen befinden sich aktuell in der Entwicklung. Die nachstehende Tabelle gibt einen Überblick zum relevanten, aktuellen Standardisierungsrahmen hinsichtlich DLT in Europa und weltweit.

Tabelle 11: Überblick internationale Standardisierung zu DLT (Auswahl)

Gremium	Standard/Technischer Report
ISO Tc 307 (weltweit/publiziert)	ISO 22739:2024 Terminology
	ISO TR 23249:2022 Overview of existing DLT Systems for identity management
	ISO 23257:2022 Reference Architecture
	ISO TS 23635:2022 Guidelines for Governance
ISO Tc 46 Sc 11 (weltweit/publiziert)	ISO TR 24332 Blockchain and DLT in relation to authoritative records, records systems and records management (Nachweisfähigkeit in DLT)
ISO Tc 307 (weltweit/in Entwicklung)	ISO TS 23353 Auditing guidelines
	ISO 25126 Information security controls based on ISO/IEC 27002 for distributed ledger services
	ISO 24875-1 bis 4 Smart contract security
CEN JTC 19 (Europa)	CEN TS 18264 Policy and security requirements for trust services providing ledger services

Zudem gilt es hervorzuheben, dass mit der überarbeiteten eIDAS Verordnung erstmalig eine übergreifende europäische Regulierung vorliegt, die die Vertrauenswürdigkeit und prüfbare Sicherheit von DLT-Systemen und -Providern ermöglicht. Der bei CEN JTC 19 in Entwicklung befindliche Standard soll absehbar durch den verbindlichen Durchführungsrechtsakt für Art. 45l Abs. 3 eIDAS 2.0 referenziert und regulatorisch verbindlich werden. Dieser Standard wird konkrete Anforderungen zur Lösung der o.g. Herausforderungen beinhalten und durch den Durchführungsrechtsakt für die Zertifizierung qualifizierter Vertrauensdienste für Electronic Ledger durch die Konformitätsbewertungsstellen nach Art. 22 eIDAS 2.0 verbindlich. Insofern ist davon auszugehen, dass die genannten, derzeit noch bestehenden Schwächen von DLT perspektivisch adressiert werden. Die Frage der Veränderung oder Löschung von on-chain Daten kann beispielsweise durch Blacklisting erfolgen, also Sperren der vorherigen Transaktion, die in der Folge beim Konsensmechanismus nicht mehr berücksichtigt wird (vergleichbar mit sog. WORM-Speicher).

Details hierzu enthält Kap. 2.1.1.

1.9 Wesentliche DLT-Netzwerke in Europa

1.9.1 European Blockchain Service Infrastructure

Als wesentliches DLT-Netzwerk ist in Europa insbesondere die European Blockchain Service Infrastructure (EBSI) zu benennen. EBSI ist ein paneuropäisches DLT-Netzwerk, das von den Mitgliedstaaten bereitgestellt wird. Das bedeutet, dass die neue Betriebsorganisation Europeum/EDIC die Hauptknoten sowie die Basisinfrastruktur betreibt und grundlegende Sicherheit, Geschäftskontinuität und Servicelevels gewährleistet. Jede Anwendung, unabhängig davon, ob sie

- technisch (z. B. Smart Contracts) oder
- anwendungsfallbezogen (z. B. Supply Chain, digitale Nachweise, Tokenisierung)

ausgestaltet ist - wird immer auf der faktischen staatlichen Infrastruktur aufgebaut. Dies führt zu der Feststellung, dass EBSI standardmäßig auf einem staatlichen Vertrauensanker basiert.

EBSI verfügt über eine umfassende Governance-Sturkur, ein Vertrauensmodell sowie ein technisches Framework:

- definiertes Vertrauensmodell[13]
- umfassender technischer Rahmen für Formate, Protokolle, Schnittstellen, DID-Methoden[14], der bestehende Standards von ETSI und CEN wiederverwendet, insbesondere in Bezug auf Signaturen (JAdES), Widerruf usw.[15]
- vertrauenswürdiges Ausstellerregister, vergleichbar mit der TrustList nach Art. 22 eIDAS 2.0
- vertrauenswürdige Richtlinien, um zu definieren, wie Anwendungen auf EBSI bereitgestellt werden – vergleichbar mit den Trust Service Practice Statements und Trust Service Policies für QTSP in eIDAS
- Identitäts-, Zugriffs- und Autorisierungsmanagement
- Validierungsverfahren für überprüfbare Anmeldeinformationen[16]
- Konformitätstests für Wallets anhand dedizierter Spezifikationen[17]
- spezifische Schnittstellen oder nicht identitätsbezogene Anwendungsfälle, z. B.: Track and Trace für Rückverfolgbarkeitsanwendungsfälle wie digitale Produktpässe, Lieferkette[18]:
- Technologisch basiert EBSI auf Hyperledger BESU und stellt also eine public permissioned DLT dar, die auch als private permissioned verwendet werden kann.

Zusammenfassend enthält EBSI einen nachhaltigen organisatorischen und technischen Rahmen und eine Infrastruktur, die von den Mitgliedstaaten bereitgestellt wird und zum Aufbau kompletter Ökosysteme genutzt werden kann, beispielsweise für:

13 Vgl. https://hub.ebsi.eu/vc-framework/trust-model - abgerufen am 23.02.2026

14 Vgl. https://hub.ebsi.eu/vc-framework - abgerufen am 23.02.2026

15 Vgl. https://hub.ebsi.eu/vc-framework/credential-status-framework - abgerufen am 23.02.2026

16 https://hub.ebsi.eu/tools/vc-validator - abgerufen am 23.02.2026

17 https://hub.ebsi.eu/conformance - abgerufen am 23.02.2026

18 Vgl. https://hub.ebsi.eu/apis/pilot/track-and-trace - abgerufen am 23.02.2026

- dezentrale PKI zur Ausstellung und Überprüfung digitaler Nachweise bzw. Identitätsattribute (Qualified Attestations of Attributes, Zertifikate für QES/QSeal/QWAC, Qualifizierter Zeitstempel nach eIDAS[19])
- Infrastruktur für Anwendungsfälle wie Rückverfolgbarkeit, Tokenisierung, digitale Währungen kombiniert mit Smart Contracts usw.

Das bedeutet, dass EBSI nicht nur klassische Identitätsanwendungsfälle wie digitale Diplome ermöglicht, sondern auch Anwendungen, um Identität und Transaktionen selbst in einer Infrastruktur zu kombinieren, wie z. B.

- Digitaler Produktpass und Lieferkettennachverfolgung
  - Pilotiert aktuell z.B. im europäischen Konsortium TRACE4EU[20]
- Digitaler Frachtbrief
  - Pilotiert aktuell z.B. im europäischen Konsortium EBSI-ELSA[21]
- Eigentum und Handel mit in NFT digitalisierten Vermögenswerten und Produkten
  - Pilotiert aktuell z.B. im europäischen Konsortium TRACE4EU
- Digitale Währungen wie digitaler Euro und Zahlung[22]

Im Mai 2024 wurde außerdem EDIC als Betriebsgesellschaft der Mitgliedstaaten für EBSI gegründet, die sicherstellt, dass EBSI öffentliches Gut bleibt und nur von (privaten) EUDI-Wallet-Anbietern (vom Mitgliedstaat anerkannt) oder qualifizierten Vertrauensdiensteanbietern genutzt werden kann.

1.9.2 Weitere Netzwerke

Als weitere DLT-Netzwerke in Europa wären beispielhaft zu nennen:

- Alastria
  - Land: Spanien
  - Fokus: dezentrale digitale Identitäten und Nachweise
  - Technologie/Protokoll: Hyperledger BESU (Public/private permissioned)[23]
- ID Union
  - Land: Deutschland

19 Vgl. Kap. 2.1.1

20 Vgl. https://trace4eu.eu/ - abgerufen am 23.02.2026

21 Vgl. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI-ELSA+EUIPO - abgerufen am 23.02.2026

22 Einen Überblick über die aktuellen Pilotprojekte geben die folgenden Links:

https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Make+information+easy+to+verify+and+almost+impossible+to+fake - abgerufen am 23.02.2026

sowie

https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI+Ecosystem+Day+Contents?source=post_page-----5f17c5c75dd5 - abgerufen am 23.02.2026

23 Quelle: https://alastria.io/en/home/ - abgerufen am 23.02.2026

- Fokus: dezentrale digitale Identitäten, insbesondere Organisationsidentitäten
- Technologie/Protokoll: Hyperledger Indy, perspektivisch EBSI (Public/private permissioned)[24]

- Findynet
  - Land: Finnland
  - Fokus: dezentrale digitale Identitäten und Nachweise
  - Technologie/Protokoll: Hyperledger Indy (Public permissioned)[25]
- Comercio
  - Land: Italien
  - Fokus: anwendungsfallübergreifend
  - Technologie/Protokoll: Tendermint (eigenes Protokoll, Public permissioned)[26]
- Polygon
  - Land: UK
  - Fokus: anwendungsfallübergreifend, Web 3, Tokenization
  - Technologie/Protokoll: eigenes Protokoll basierend auf Ethereum (Public permissioned)[27]

Im Gegensatz zu EBSI werden alle diese Netzwerke von privaten Gesellschaften oder Genossenschaften betrieben. Eine Zertifizierung oder Compliance zu eIDAS und anderen für die Lieferkettennachverfolgung relevanten regulatorischen Rahmenbedingungen liegt, unabhängig von Marketingaussagen der Betreiber, aktuell noch nicht vor.

24 Quelle: https://idunion.org/ - abgerufen am 23.02.2026

25 Quelle: https://findynet.fi/en/ - abgerufen am 23.02.2026

26 Quelle: https://commercio.network/ - abgerufen am 23.02.2026

27 Quelle: https://polygon.technology/ - abgerufen am 23.02.2026

2 Anforderungen an ein System zur Lieferkettennachverfolgung

2.1 Regulatorische Anforderungen

2.1.1 eIDAS Verordnung

Die eIDAS-Verordnung ist ein Regelwerk der Europäischen Union, dessen erste Version 2014 eingeführt wurde, um die Sicherheit und das Vertrauen in elektronische Transaktionen im europäischen Binnenmarkt zu erhöhen. eIDAS steht für elektronische Identifikation, Authentifizierung und Vertrauensdienste. Die Verordnung hat wesentliche Auswirkungen auf Unternehmen, insbesondere im Kontext digitaler Lieferketten:

- Elektronische Identifikation (eID): eIDAS ermöglicht es Bürgern und Unternehmen der EU, ihre nationale elektronische Identifikation in anderen EU-Ländern zu nutzen. Das erleichtert die grenzüberschreitende Authentifizierung und fördert den digitalen Handel.
- Vertrauensdienste: Die Verordnung standardisiert verschiedene Vertrauensdienste, einschließlich elektronischer Signaturen, elektronischer Siegel, Zeitstempel, Einschreibedienste und Zertifikatdienste für die Authentifizierung von Websites. Diese Dienste sind entscheidend für die Sicherheit und Integrität elektronischer Transaktionen.
- Rechtsverbindlichkeit und Anerkennung: Elektronische Signaturen und andere Vertrauensdienste, die unter eIDAS zertifiziert sind, haben die gleiche Rechtskraft wie handschriftliche Signaturen und sind in der gesamten EU anerkannt. Dies ist besonders wichtig für Verträge und Vereinbarungen in der Lieferkette.
- Datenschutz und Sicherheit: eIDAS legt strenge Standards für die Sicherheit von elektronischen Identifikations- und Vertrauensdiensten fest. Dies trägt dazu bei, das Vertrauen in digitale Prozesse zu stärken und gleichzeitig den Datenschutz zu gewährleisten.
- Effizienz in der Lieferkette: Durch die Vereinfachung und Sicherung elektronischer Transaktionen erleichtert eIDAS die digitalen Interaktionen zwischen Unternehmen, Verbrauchern und Behörden. Das verbessert die Effizienz in der gesamten Lieferkette, von der Auftragserteilung bis zur Lieferung.

Die eIDAS 2 als überarbeitete Version zielt darauf ab, die bestehende Verordnung zu erweitern und sich an die ändernden digitalen Anforderungen und die Weiterentwicklung der Technologien anzupassen. Hier wurde der private Sektor mehr in den Fokus genommen sowie das Konzept von Wallets in Form des EUDI Wallets mit aufgenommen, sodass digitale Identitäten und Vertrauensdienste im digitalen Binnenmarkt und damit bei Lieferketten genutzt werden können. In der Lieferkette ist eIDAS daher eine wichtige Anforderung, da sie Transparenz, Sicherheit und Vertrauen in digitale Prozesse bringt. Dies ist besonders relevant in einem internationalen Kontext, wo die Einhaltung unterschiedlicher nationaler Gesetze und Standards eine Herausforderung darstellen kann. Mit eIDAS werden grenzüberschreitende digitale Transaktionen vereinfacht und standardisiert, was für Unternehmen in der EU und darüber hinaus von Vorteil ist.

Mit Section 11 führt die Neufassung der eIDAS auch (qualifizierte) Vertrauensdienste für elektronische Register ein (Art. 45h ff.). eIDAS definiert, dass qualifizierte Register „von einem oder mehreren qualifizierten Vertrauensdiensteanbietern erstellt und verwaltet werden, den Ursprung der Datensätze im Register feststellen, die eindeutige chronologische Reihenfolge der

Datensätze im Register sicherstellen und Daten so aufzeichnen, dass jede spätere Änderung der Daten sofort erkennbar ist, wodurch ihre Integrität im Laufe der Zeit gewährleistet wird“. Obwohl eIDAS technologieneutral ist, entspricht die Beschreibung in Art. 45i der Definition von DLT in internationalen Normen wie ISO 22739 und enthält Kerneigenschaften von DLT. Da eIDAS die Anforderung verbindlicher Durchführungsrechtsakte mit Verweis auf europäische Normen enthält, gewährleistet es einen kohärenten technischen Rahmen für DLT. Da die Anforderungen an QTSP auch für QTSP für Register gelten, werden diese Normen auch die Grundlage für die Zertifizierung durch unabhängige Konformitätsbewertungsstellen sein und so nachgewiesene Sicherheit und Vertrauen in DLT gewährleisten. Es muss darauf hingewiesen werden, dass sich Abschnitt 11 auf alle Anwendungsfälle konzentriert, die nicht von EUDIW oder allen anderen (qualifizierten) Vertrauensdiensten abgedeckt sind, also z. B. (qualifizierte) Signaturen, Siegel, Zeitstempel, Bescheinigungen für elektronische Zustellung usw. Dies bedeutet, dass DLT als Infrastruktur für jedes EUDIW sowie für jeden anderen QTSP verwendet werden kann – die Sicherheit wird im Rahmen der Konformitätsbewertung nachgewiesen, aber es besteht keine Notwendigkeit, QTSP für Ledger als Voraussetzung für die Bereitstellung eines anderen (qualifizierten) Vertrauensdienstes oder eines EUDIW zu verwenden. Diese Differenzierung ist wichtig, da sie zu den wichtigsten Anwendungsfällen für QTSP für elektronische Ledger führt, wie z. B. Tokenisierung oder digitale Vermögenswerte, Kryptowährungen oder Rückverfolgbarkeit in Lieferketten und digitale Produktpässe. Die folgende Tabelle zeigt die möglichen Anwendungsszenarien für elektronische Ledger (DLT) innerhalb des eIDAS-Ökosystems.

Tabelle 12: Anwendbarkeit QTSP for Ledger

Nr	Thema	Beispiele	Section 11 anwendbar
1	EUDI-Wallet	eID TrustList	Nein
2	Qualifizierte Vertrauensdienste	QES QSeal Qualifizierte Zeitstempel Validierung Bewahrung Archivierung eDelivery Management of secure signature creation devices Qualifizierte Attributsbescheinigungen TrustList	nein
3	Qualifizierter Vertrauensdienst für Electronic Ledger	Traceability Lieferketten Digitaler Produktpass Tokenization Smart Contracts	ja

2.1.2 Lieferkettensorgfaltspflichtengesetz

Das „Lieferkettensorgfaltspflichtengesetz“, oft auch als Lieferkettengesetz bezeichnet, ist ein deutsches Gesetz, das darauf abzielt, die Menschenrechtsstandards und Umweltschutzmaßnahmen in globalen Lieferketten zu verbessern. Es wurde im Juni 2021 vom Deutschen Bundestag verabschiedet und ist seit Januar 2023 in Kraft. Hier sind einige Kernpunkte des Gesetzes:

- Geltungsbereich: Das Gesetz gilt für Unternehmen mit Sitz oder Zweigniederlassung in Deutschland, die mehr als 3.000 Mitarbeitende haben (ab 2024 gilt es für Unternehmen mit mehr als 1.000 Mitarbeitenden).
- Sorgfaltspflichten: Unternehmen sind verpflichtet, Sorgfaltspflichten in ihren Lieferketten zu erfüllen. Dazu gehört die Einführung und Durchführung von Risikomanagementsystemen, die regelmäßige Durchführung von Risikoanalysen, die Ergreifung präventiver Maßnahmen bei festgestellten Menschenrechtsverletzungen und die Einrichtung eines Beschwerdemechanismus.
- Menschenrechte und Umweltschutz: Das Gesetz konzentriert sich auf die Einhaltung von Menschenrechtsstandards und Umweltschutznormen. Unternehmen müssen sicherstellen, dass ihre Lieferanten diese Standards einhalten und keine Menschenrechtsverletzungen wie Kinderarbeit, Zwangsarbeit oder Umweltzerstörung verursachen.
- Dokumentation und Berichterstattung: Unternehmen müssen ihre Bemühungen dokumentieren und regelmäßig über ihre Maßnahmen zur Einhaltung der Sorgfaltspflichten berichten.

- Haftung und Sanktionen: Bei Verstößen gegen das Gesetz können Unternehmen mit Sanktionen belegt werden. In schwerwiegenden Fällen kann dies auch zivilrechtliche Haftungsansprüche nach sich ziehen.

Das Gesetz ist ein wichtiger Schritt zur Stärkung der unternehmerischen Verantwortung in Bezug auf Menschenrechte und Umweltschutz in internationalen Lieferketten. Es spiegelt einen wachsenden Trend in der globalen Wirtschaft wider, bei dem Unternehmen zunehmend für die Auswirkungen ihrer Geschäftstätigkeiten auf die Gesellschaft und die Umwelt verantwortlich gemacht werden.

2.1.3 Datenschutzgrundverordnung (DSGVO)

Die Datenschutzgrundverordnung der Europäischen Union spielt eine zentrale Rolle bei der Nachverfolgung von Lieferketten, insbesondere wenn personenbezogene Daten verarbeitet werden. Hier sind einige Gründe, warum die Einhaltung der DSGVO in diesem Kontext relevant ist:

- Verarbeitung personenbezogener Daten: In der Lieferkette können personenbezogene Daten an verschiedenen Punkten verarbeitet werden, z.B. beim Versand, bei Kundeninteraktionen oder bei der Überwachung der Mitarbeitendenleistung. Die DSGVO fordert, dass solche Datenverarbeitungen rechtmäßig, transparent und sicher sind.
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen: Die DSGVO verlangt, dass Datenschutzmaßnahmen von Anfang an in die Gestaltung von Verarbeitungssystemen und -prozessen integriert werden (Privacy by Design). Außerdem müssen datenschutzfreundliche Voreinstellungen (Privacy by Default) angewendet werden. Für Lieferketten bedeutet das, dass die Systeme und Prozesse zur Überwachung und Steuerung von Anfang an datenschutzkonform gestaltet sein müssen.
- Rechenschaftspflicht und Dokumentation: Unternehmen müssen nachweisen können, dass sie die Grundsätze der DSGVO einhalten (Rechenschaftspflicht). Dies beinhaltet die ordnungsgemäße Dokumentation von Datenverarbeitungsaktivitäten und die Implementierung und Aufrechterhaltung von Datenschutzmaßnahmen.
- Rechte der betroffenen Personen: Die DSGVO stärkt die Rechte von Einzelpersonen in Bezug auf ihre Daten, einschließlich des Rechts auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung. Unternehmen müssen sicherstellen, dass diese Rechte im Kontext der Lieferkettenüberwachung respektiert werden.
- Grenzüberschreitende Datenübertragungen: Da Lieferketten oft international sind, können Daten über Landesgrenzen hinweg übertragen werden. Die DSGVO setzt strenge Regeln für die Übertragung personenbezogener Daten außerhalb der EU, was für Unternehmen, die global agieren, relevant ist.
- Risikomanagement und Datenschutzfolgenabschätzung: Für bestimmte Arten von Datenverarbeitungen, insbesondere solche, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen, verlangt die DSGVO eine Datenschutzfolgenabschätzung. Dies könnte für komplexe oder umfangreiche Lieferkettenaktivitäten erforderlich sein.

Insgesamt ist die Einhaltung der DSGVO bei der Lieferkettennachverfolgung entscheidend, um das Risiko von Datenschutzverletzungen zu minimieren und das Vertrauen aller Stakeholder,

einschließlich Kunden, Lieferanten und Mitarbeitenden, zu wahren. Verstöße gegen die DSGVO können zu erheblichen Bußgeldern und Reputationsschäden führen.

2.1.4 Verordnung „Recht auf Reparatur“

Die EU Richtlinie EU 2024/1799, das sogenannte "Right to Repair" (Recht auf Reparatur), als regulatorische Anforderung, hat weitreichende Auswirkungen auf Lieferketten, vor allem in der Art und Weise, wie Produkte entworfen, produziert, vertrieben und gewartet werden. Hier sind einige Gründe, warum das Recht auf Reparatur als regulatorische Anforderung im Kontext von Lieferketten relevant ist:

- Produktdesign und Herstellung: Hersteller müssen ihre Produkte so entwerfen, dass sie leichter reparierbar sind. Dies kann bedeuten, dass die Produkte modular aufgebaut sind, Ersatzteile standardisiert werden, und Reparaturanleitungen zur Verfügung gestellt werden müssen. Solche Designänderungen haben direkte Auswirkungen auf die Lieferkette, da sie die Beschaffung von Materialien, die Produktionsprozesse und die Auswahl der Zulieferer beeinflussen können.
- Ersatzteillogistik und Verfügbarkeit: Ersatzteile und Reparaturinformationen müssen unter festgelegten Bedingungen verfügbar sein.. Dies erfordert eine effektive Planung und Verwaltung der Lieferketten für Ersatzteile, einschließlich Lagerhaltung und Distribution.
- Dienstleistungsnetzwerke und Support: Um Reparaturen zu ermöglichen, müssen Unternehmen möglicherweise umfangreichere Support-Netzwerke aufbauen, einschließlich qualifizierter Reparaturdienste und Kundensupport. Dies erfordert zusätzliche Ressourcen und Koordination innerhalb der Lieferkette.
- Nachhaltigkeit und Kreislaufwirtschaft: Das Recht auf Reparatur fördert die Nachhaltigkeit, indem es zur Langlebigkeit von Produkten beiträgt und den Abfall reduziert. Unternehmen müssen ihre Lieferketten möglicherweise anpassen, um diese nachhaltigeren Praktiken zu unterstützen, was sich auf Materialauswahl, Verpackung und Transportmethoden auswirken kann.
- Compliance und Risikomanagement: Die Einhaltung von Reparaturgesetzen erfordert ein effektives Compliance- und Risikomanagement in der gesamten Lieferkette. Unternehmen müssen sicherstellen, dass sie die gesetzlichen Anforderungen erfüllen und mögliche Risiken, wie z.B. Versorgungsengpässe oder regulatorische Änderungen, proaktiv managen.
- Kundenerwartungen und Marktstrategien: Da Verbraucher zunehmend Produkte bevorzugen, die reparierbar und nachhaltig sind, müssen Unternehmen ihre Marktstrategien entsprechend anpassen. Dies kann Einfluss auf das Branding, Marketing und den Kundenservice haben, was wiederum die Lieferkette betrifft.

Zusammenfassend ist das Recht auf Reparatur eine regulatorische Anforderung, die Unternehmen dazu veranlasst, ihre Lieferketten zu überdenken und anzupassen. Es beeinflusst, wie Produkte entworfen, hergestellt und unterstützt werden und fördert gleichzeitig nachhaltigere Geschäftspraktiken.

2.1.5 EU-Batterieverordnung

Eine branchenspezifische Verordnung ist zum Beispiel die EU-Batterieverordnung. Sie gibt verschiedene regulatorische Vorgaben vor, die von Herstellern, Importeuren, Händlern und Verbrauchern von Batterien und Akkumulatoren beachtet werden müssen. Diese Vorgaben

dienen dem Umweltschutz und der Förderung der Kreislaufwirtschaft. Zu den wichtigsten Vorgaben gehören:

- Rücknahmepflicht: Hersteller und Vertreiber sind verpflichtet, gebrauchte Batterien und Akkus unentgeltlich zurückzunehmen. Dies gilt sowohl für den Einzelhandel als auch für den Online-Handel.
- Kennzeichnung und Beschränkungen: Batterien müssen mit dem Symbol einer durchgestrichenen Mülltonne gekennzeichnet sein, um darauf hinzuweisen, dass sie nicht im Hausmüll entsorgt werden dürfen. Zudem müssen sie bei Überschreitung bestimmter Schadstoffgrenzwerte (Quecksilber, Blei, Cadmium) entsprechend gekennzeichnet sein.
- Registrierungspflicht: Hersteller, die Batterien oder Akkus erstmals in Deutschland in Verkehr bringen, müssen sich bei der zuständigen Behörde registrieren. Dies dient der Überwachung des Marktes und der Sicherstellung der Einhaltung der gesetzlichen Vorschriften.
- Informationspflichten: Hersteller und Händler müssen Verbraucher über die Rückgabemöglichkeiten von Altbatterien und die Bedeutung der Batteriesymbole informieren.
- Pfandpflicht für Autobatterien: Für Fahrzeugbatterien besteht eine Pfandpflicht, um die Rückgabe und das Recycling zu fördern. Käufer erhalten das Pfand zurück, wenn sie eine gebrauchte Batterie zurückgeben.
- Berichtspflichten: Hersteller müssen regelmäßig über die in Verkehr gebrachten und zurückgenommenen Batteriemengen berichten.
- Umweltgerechte Entsorgung: Es müssen geeignete Maßnahmen getroffen werden, um die umweltgerechte Entsorgung von Altbatterien sicherzustellen.

Diese Vorgaben sind darauf ausgerichtet, die Umweltauswirkungen von Batterien zu reduzieren, insbesondere durch Förderung ihrer Rücknahme und des Recyclings. Nichtbeachtung dieser Vorschriften kann zu rechtlichen Konsequenzen führen, einschließlich Bußgeldern.

2.1.6 Weitere Vorgaben in Europa

Der europäische Green Deal 2019 hat verschiedene gesetzgeberische Maßnahmen eingeleitet, um Nachhaltigkeit und Zirkularität in Lieferketten für Produkte zu fördern, die auf den europäischen Markt gelangen. Zu den wichtigsten Verordnungen, die sich derzeit in verschiedenen Phasen des Gesetzgebungsprozesses befinden, gehören:

- Green Claims-Richtlinie
- EU-Richtlinie zur unternehmerischen Nachhaltigkeitssorgfaltspflicht
- EU-Gesetz über kritische Rohstoffe
- Ökodesign-Verordnung für nachhaltige Produkte (ESPR)

Insbesondere die neue Batterieverordnung und die ESPR sind weitreichende Verordnungen, die sich auf Rückverfolgbarkeitsprozesse und Datenaustauschpraktiken zwischen den Beteiligten in der Lieferkette auswirken werden und daher einen genaueren Blick verdienen.

Die neue EU-Batterieverordnung ist am 17. August 2023 in Kraft getreten und mitlerweile in nationales Recht umgesetzt[28]. Sie ist eine wichtige Initiative zur Verbesserung der Nachhaltigkeit und Zirkularität der Batterielieferkette und zur Erhöhung der Ressourcenunabhängigkeit Europas. Sie gilt für alle Batterien mit einer Kapazität von mehr als 2 kWh, die auf den europäischen Markt gelangen. Neben der Festlegung einer Liste von Anforderungen in Bezug auf ESG-Aspekte und Mindestmengen an recyceltem Inhalt ist diese Verordnung die erste, die einen digitalen Produktpass (DPP) vorschreibt (Artikel 65). Der Batteriepass soll Informationen zum Batteriemodell und spezifische Informationen zur einzelnen Batterie enthalten, die ihre gesamte Wertschöpfungskette abdecken. Er wird als Compliance-Tool für die Batterieverordnung dienen und Batteriedaten über den gesamten Batterielebenszyklus hinweg registrieren und zugänglich machen können.

Die Verordnung hat bereits mehrere Initiativen zur weiteren Spezifizierung des DPP ausgelöst, die sich in der Arbeit der Global Battery Alliance und öffentlich finanzierten Projekten wie Battery Pass und CIRPASS widerspiegeln. Darüber hinaus hat sie auch zur Entstehung von industriegetriebenen Ökosystemen zum Datenaustausch wie Catena-X geführt.

Es ist zu erwarten, dass die Erkenntnisse und Erfahrungen mit der Verordnung die Umsetzung der Rückverfolgbarkeit und der Offenlegung von Produktinformationen in anderen Produktkategorien stark beeinflussen werden.

Die Ökodesign-Verordnung für nachhaltige Produkte ist eine ehrgeizige EU-Initiative, um nachhaltige Produkte zur Norm in der EU zu machen. Sie deckt fast alle auf den Markt gebrachten Produkte ab, wobei nur wenige Ausnahmen bestehen (z. B. Lebensmittel, Futtermittel, Arzneimittel). Sie wird eine breite Palette von Aspekten ansprechen, um Produkte langlebiger, zuverlässiger und kreislauffähiger zu machen und ihre Umweltauswirkungen während des gesamten Lebenszyklus zu minimieren. Sie legt Anforderungen an Haltbarkeit, Mindestmengen an Recyclingmaterial, Wiederverwendbarkeit, Aufrüstbarkeit, Reparaturfähigkeit, Vorhandensein von Stoffen, die die Kreislauffähigkeit beeinträchtigen, Energie- und Ressourceneffizienz, Wiederaufbereitung, Recycling und CO2-Fußabdruck fest. Sie wird sich auch auf die soziale Nachhaltigkeit von Produkten und Due-Diligence-Aspekte sowie wichtige Zertifizierungen entlang der Lieferkette konzentrieren.

Spezifische Anforderungen für jede Produktkategorie werden in speziellen Rechtsakten festgelegt, die nach der Ratifizierung der Rahmenverordnung erlassen werden. Die ersten delegierten Rechtsakte, die erlassen werden, werden wahrscheinlich Textilien betreffen.

Um die Prüfung, Offenlegung und den Austausch dieser Informationen zwischen den Beteiligten der Lieferkette zu ermöglichen, schreibt die ESPR einen digitalen Produktpass für alle Produkte vor.

2.1.7 Internationale Vorgaben: FDA

Mit der Betrachtung der Lieferkette nicht nur auf EU-Ebene, sondern auch international, können weitere rechtliche Vorgaben wie aus den Vereinigten Staaten relevant werden. Die Anforderungen der US-amerikanischen Food and Drug Administration (FDA) sind für die Lieferkettenverfolgung insbesondere in der Lebensmittel-, Pharma- und Medizinprodukteindustrie von großer Bedeutung. Die FDA setzt strenge Standards für

[28] Redaktioneller Hinweis: Nachträgliche Änderung nach Abnahme des Berichts. Zur Abnahme des Berichts war diese noch nicht umgesetzt. https://www.umweltbundesamt.de/themen/abfall-ressourcen/produktverantwortung-in-der-abfallwirtschaft/batterien-altbatterien?utm_source=chatgpt.com#gesetzliche-grundlagen

Sicherheit, Wirksamkeit und Qualität in diesen Sektoren. Hier sind einige Aspekte, in denen die FDA-Anforderungen für die Lieferkettenverfolgung relevant sind:

- Good Manufacturing Practice (GMP): Die FDA fordert die Einhaltung der Good Manufacturing Practice-Regeln, die eine hohe Qualität und Sicherheit bei der Herstellung von Arzneimitteln, Lebensmitteln und Medizinprodukten sicherstellen. Dazu gehört die lückenlose Dokumentation von Produktionsprozessen und Materialquellen.
- Traceability-Anforderungen: In der Lebensmittelindustrie müssen Unternehmen in der Lage sein, die Herkunft ihrer Produkte zu verfolgen und zu dokumentieren. Dies hilft bei der schnellen Identifizierung und Rückverfolgung von Produkten im Falle von Lebensmittelsicherheitsproblemen.
- Drug Supply Chain Security Act (DSCSA): Für die Pharmaindustrie schreibt der DSCSA vor, dass Unternehmen Systeme zur Rückverfolgung von verschreibungspflichtigen Medikamenten implementieren müssen. Dies umfasst Anforderungen an die Kennzeichnung und elektronische, interoperable Systeme zur Verfolgung von Arzneimittelbewegungen durch die Lieferkette.
- Unique Device Identification (UDI): In der Medizinprodukteindustrie fordert die FDA die Verwendung eines Unique Device Identification-Systems. Jedes Gerät muss eine eindeutige Kennung haben, die während seiner gesamten Lebensdauer verfolgt werden kann.
- Meldepflicht bei Qualitätsproblemen: Unternehmen müssen der FDA über Probleme mit der Produktqualität oder Sicherheit berichten. Dies erfordert effektive Überwachungs- und Rückverfolgungssysteme innerhalb der Lieferkette.
- Importkontrolle: Die FDA überwacht importierte Produkte und kann die Einfuhr von Produkten verbieten, die nicht ihren Standards entsprechen. Dies erfordert, dass internationale Lieferketten den FDA-Vorschriften genügen.

Die Einhaltung dieser FDA-Anforderungen ist entscheidend, um Compliance-Risiken zu vermeiden und die Sicherheit und Qualität von Produkten zu gewährleisten. Unternehmen, die in den USA oder für den US-Markt produzieren, müssen sicherstellen, dass ihre Lieferketten diese Anforderungen erfüllen, um Zulassungs- und Betriebsgenehmigungen zu erhalten und aufrechtzuerhalten.

2.1.8 Fachspezifische Anforderungen

Konkrete fachspezifische Anforderungen variieren je nach Branche und lassen sich teilweise aus den regulatorischen Anforderungen ableiten. Im Folgenden sind einige Branchen mit ihren jeweiligen Anforderungen aufgelistet.

Lebensmittelindustrie:

- Hazard Analysis and Critical Control Points (HACCP): Dies ist ein präventives Risikomanagementsystem, das dazu dient, Lebensmittelsicherheit zu gewährleisten. Unternehmen müssen potenzielle Gefahren analysieren und kritische Kontrollpunkte in ihren Produktionsprozessen identifizieren und überwachen, um Lebensmittelverunreinigungen zu verhindern.
- Kühlkettenmanagement: Für viele Lebensmittel ist es entscheidend, dass sie kontinuierlich bei bestimmten Temperaturen gelagert und transportiert werden. Das Management der

Kühlkette umfasst die Überwachung und Aufrechterhaltung optimaler Temperaturbedingungen vom Produzenten bis zum Endverbraucher.

- Rückverfolgbarkeit: Die Fähigkeit, den Weg eines Lebensmittels von der Quelle bis zum Verbraucher nachzuverfolgen, ist für die Lebensmittelsicherheit wesentlich. Im Falle eines Lebensmittelsicherheitsvorfalls müssen Unternehmen schnell die Herkunft des Produkts identifizieren können.

Pharmaindustrie:

- Good Manufacturing Practice (GMP): GMP sind Richtlinien, die sicherstellen, dass pharmazeutische Produkte konsequent mit hoher Qualität produziert werden. Sie umfassen Aspekte wie Hygiene, Rohmaterialqualität, Prozessvalidierung und Mitarbeiterqualifikation.
- Kontrollierte Substanzen: Für den Umgang mit verschreibungspflichtigen Medikamenten und Betäubungsmitteln gelten strenge Vorschriften. Dazu gehören sichere Lagerung, genaue Buchführung und kontrollierte Distribution.
- Kühlketten für biologische Produkte: Biologische Produkte wie Impfstoffe erfordern oft spezielle Lager- und Transportbedingungen, um ihre Wirksamkeit zu bewahren. Dies kann präzise temperaturgesteuerte Umgebungen während der gesamten Lieferkette beinhalten.
- Food and Drug Administration: In den USA ist die FDA über die Zulassung von Lebensmitteln und Medikamenten zuständig. Hier werden in Teil 11 Vorgaben für elektronische Aufzeichnungen und Signaturen definiert, damit eine Gleichwertung zu den papierbasierten Verfahren sichergestellt werden kann.

Automobilindustrie:

- Just-In-Time (JIT) und Just-In-Sequence (JIS): JIT minimiert Lagerbestände, indem Materialien und Teile genau zum benötigten Zeitpunkt geliefert werden. JIS bezieht sich auf die Lieferung von Teilen in der exakten Reihenfolge, in der sie in der Produktion benötigt werden.
- IATF 16949:2016: Diese Norm legt spezifische Anforderungen für das Qualitätsmanagementsystem in der Automobilproduktion fest, einschließlich Design, Entwicklung, Produktion und, wenn relevant, Installation und Service von Automobilprodukten.

Elektronikindustrie:

- RoHS (Restriction of Hazardous Substances): Diese Richtlinie beschränkt die Verwendung bestimmter gefährlicher Stoffe in elektrischen und elektronischen Geräten. Sie zielt darauf ab, die Umweltauswirkungen dieser Produkte zu reduzieren und die Gesundheit der Verbraucher zu schützen.
- E-Waste-Management: Die ordnungsgemäße Entsorgung und das Recycling von Elektronikschrott sind entscheidend, um Umweltverschmutzung zu vermeiden und wertvolle Ressourcen zurückzugewinnen.

Textil- und Bekleidungsindustrie:

- Soziale Compliance: Diese umfasst die Einhaltung von Standards für Arbeitsbedingungen, wie angemessene Bezahlung, Arbeitszeiten, keine Kinder- oder Zwangsarbeit und sichere Arbeitsumgebungen.
- Ökotextilien-Zertifizierung: Zertifizierungen wie der Global Organic Textile Standard (GOTS) stellen sicher, dass Textilprodukte unter Einhaltung von ökologischen und sozialen Kriterien produziert werden.

Luft- und Raumfahrt:

- AS9100: Dieses Qualitätsmanagementsystem wurde speziell für die Luft- und Raumfahrtindustrie entwickelt. Es umfasst Anforderungen an die Qualitätssicherung in Design, Entwicklung, Produktion und Wartung.
- NADCAP: Dieses Programm akkreditiert spezielle Prozesse und Produkte in der Luft- und Raumfahrtindustrie, wie Schweißen, Wärmebehandlung und Beschichtungen, um sicherzustellen, dass diese den hohen Qualitätsstandards entsprechen.

EASA: die Agentur der Europäischen Union für Flugsicherheit definiert die Vorschriften für die Zulassung von Luftfahrzeugprodukten in Europa. Part 21 bezieht sich dabei auf die Anforderungen und das Management der Lieferkette, indem Standards für Qualität, Sicherheit und Konformität in der Produktion vorgegeben sind.

Diese fachspezifischen Anforderungen sind entscheidend, um Produktqualität, Sicherheit, Umweltverträglichkeit und ethische Standards entlang der Lieferkette zu gewährleisten. Unternehmen müssen diese Anforderungen erfüllen, um gesetzlichen Vorgaben zu entsprechen, das Vertrauen der Kunden zu gewinnen und ihre Marktposition zu stärken.

2.1.9 Technische Anforderungen

Basierend auf den regulatorischen und fachspezifischen Anforderungen lassen sich auch die wesentlichen technischen Anforderungen definieren:

- Zugriffssteuerung auf Daten:
  - Benutzerberechtigungen: Implementierung eines rollenbasierten Zugriffskontrollsystems, bei dem jeder Benutzer oder Benutzergruppe nur auf die für ihre Rolle relevanten Daten und Funktionen Zugriff hat. Dies könnte das Personal in der Logistik, das Management, die IT-Abteilung und externe Partner wie Lieferanten und Distributoren einschließen. Die wirksame technische Prüfung der Autorisierungen wird durch ein Accessmanagement sichergestellt.
  - Identifizierung und Authentisierung: Eindeutige Identifizierung der Beteiligten innerhalb der Lieferkette gem. ETSI TS 119 461 oder vergleichbar, Einsatz wirksamer, Mehrfaktor-Authentifizierungsverfahren. Dies stellt sicher, dass nur autorisierte Benutzer auf sensible Systeme und Daten zugreifen können.
  - Umsetzung von Verschlüsselungsmaßnahmen sowohl bei der Übertragung als auch bei der Speicherung von Daten, um diese vor unbefugtem Zugriff und Leaks zu schützen. Dies schließt die Verschlüsselung von Datenbanken und die sichere Übertragung von Daten über Netzwerke entsprechend ETSI TS 119 312 oder BSI TR-02102 ein.
- Nachweis von Authentizität und Integrität, durch Anwendung (qualifizierter) elektronischer Signaturen, Siegel und Zeitstempel

  - Digitale Nachweise müssen als Qualifizierte Attributsbescheinigungen vorliegen.

- Nachweis der Nachvollziehbarkeit des Prozesses durch wirksames Records Management nach Kap. 1.7

- Langfristige Prüfbarkeit und Lesbarkeit: Endnutzer und Auditoren müssen in der Lage sein, die notwendigen Dokumente und Informationen einzusehen, um ggf. noch Jahre später eine Prüfung durchführen zu können. Gerade bei Produkten, die eine lange Lebenszeit haben, müssen diese Daten während der Lebenszeit und teilweise sogar noch eine gewisse Zeit danach abrufbar sein. Erreicht wird dies durch Bewahrung der Authentizität, Integrität der Aufzeichnungen unter Wahrung von deren Verkehrsfähigkeit gem. BSI TR-03125 resp. ETSI TS 119 511/512 sowie deren Verfügbarkeit durch eine Archivierung nach dem Stand der Technik.

- Vermeidung eines Single Point of Failure:

  - Redundanz: Implementierung redundanter Systemkomponenten, wie doppelte Netzwerkverbindungen, Energieversorgungen und Server. Dies hilft, Ausfallzeiten zu minimieren, falls eine Komponente ausfällt.

  - Verteilte Architektur: Nutzung einer verteilten Infrastruktur, wie Cloud-Computing, die es ermöglicht, Daten und Anwendungen über mehrere Server und Standorte zu verteilen. Dies erhöht die Ausfallsicherheit und Flexibilität.

- Regelmäßige Backups und Disaster Recovery: Einrichtung eines robusten Backup- und Wiederherstellungsplans, der regelmäßige automatische Backups und schnelle Wiederherstellungsmöglichkeiten im Falle eines Datenverlusts umfasst.

- Cybersicherheit:

  - Manipulationssicherheit: Informationen müssen nach dem Stand der Technik gegen Manipulation geschützt werden. Die Berücksichtigung von Empfehlungen wie vom Bundesamt für Sicherheit in der Informationstechnik sind hierbei relevant, besonders bei dem Aspekt der Kryptoagilität.

  - Eindeutige Verantwortlichkeit: Ausgestellte Nachweise müssen im Kontext der Verantwortlichkeit eindeutig zuordenbar sein, damit im Falle einer Untersuchung eine effiziente Bearbeitung durchgeführt werden kann.

  - Verschlüsselung: Kritische Informationen, deren Einsicht beschränkt sein soll, müssen verschlüsselt gespeichert und übertragen werden. Die Anforderung ergibt sich aus Prinzipien wie dem Security by Design sowie den Interessen der Vertraulichkeit der Teilnehmer.

  - Wirksames Informationssicherheitsmanagement: klare Verantwortlichkeiten, Prozesse und Dokumente und Risikomanagement gem. ISO 27001 bzw. 31.000-Standardreihe einschließlich eines mindestens jährlichen internen und zweijährlichen externen Audits

  - Sicherheitskonzepte: Um böswillige Eingriffe von außen abwehren zu können, sind Konzepte sowie Audits notwendig. Sie helfen dabei, das Risiko präventiv zu verringern und im Falle eines Schadens diesen zu minimieren.

  - Wirksames Notfallmanagement: klare Verantwortlichkeiten, Prozesse und Dokumente gem. ISO 22301

- Maschinenlesbare Daten
  - Standardformate: Verwendung von Industriestandards im Bereich des elektronischen Datenaustausches oder GS1-Standards für Produktkennzeichnungen, um die Konsistenz und Kompatibilität der Daten zu gewährleisten.
  - Application Programming Interfaces (APIs): Entwicklung und Implementierung offener APIs, die eine reibungslose Integration mit verschiedenen Software-Systemen ermöglichen, und die Nutzung von RESTful-APIs oder SOAP für Webdienste.
  - Automatisierte Datenerfassung: Einsatz fortschrittlicher Technologien wie RFID-Tags für eine genauere und effizientere Erfassung und Verfolgung von Produkten in der Lieferkette, im Vergleich zu herkömmlichen Barcodes.
- Integration in vorhandene Systeme:
  - Kompatibilität und Interoperabilität: Sicherstellung, dass neue Systeme und Lösungen kompatibel mit vorhandenen ERP-, CRM- und SCM-Systemen sind. Dies beinhaltet die Fähigkeit, Datenformate und Protokolle dieser Systeme zu unterstützen.
  - Anpassbare Schnittstellen: Entwicklung von Benutzerschnittstellen und Dashboards, die an die spezifischen Bedürfnisse und Prozesse der verschiedenen Nutzer angepasst werden können, einschließlich der Anpassung an verschiedene Sprachen und kulturelle Gegebenheiten.
  - Modulare Systeme: Einsatz modularer und skalierbarer Systemarchitekturen, die es ermöglichen, einzelne Komponenten zu aktualisieren oder zu ersetzen, ohne das gesamte System neu gestalten zu müssen. Dies ermöglicht eine kosteneffiziente und flexible Anpassung an sich ändernde Anforderungen.
- Betrieb
  - Vorhaltung eines Beendigungsplans inklusive Migrationsplan
  - Umsetzung eines wirksamen Servicemanagement nach ISO 20.000

Diese detaillierten technischen Anforderungen sind entscheidend für eine zuverlässige, sichere und effiziente Lieferkettenverfolgung. Sie tragen dazu bei, Risiken zu minimieren, die Compliance zu verbessern und eine nahtlose Integration in die bestehende IT-Infrastruktur zu ermöglichen, was für die optimale Funktionsweise moderner Lieferketten unerlässlich ist.

2.1.10 Zusammenfassung

Die Erfüllung der regulatorischen, fachlichen und technischen Anforderungen erfordert das Vorhandensein eines oder mehrerer Betreiber eines Systems zur Lieferkettennachverfolgung. Dies limitiert den Einsatz von DLT de facto auf permissioned DLT. Darüber hinaus wird die Umsetzung durch den neuen QTSP für Ledger nach eIDAS erleichtert, da ein direkter Betreiber mit klarer Haftung und geprüfter Sicherheit (Konformitätsbewertung nach eIDAS) vorliegt.

Der nachfolgende Vergleich von DLT und klassischen Verfahren zur Lieferkettennachverfolgung soll beispielhaft aufzeigen, wie die genannten Anforderungen in beiden Systemen technisch erfüllt werden könnten. Die konkrete Prüfung im Einzelfall anhand der tatsächlichen Anforderungen des Anwendungsfalls wird dadurch nicht ersetzt, vielmehr dient der Vergleich einem groben Überblick und grundlegender Tendenz.

Die Details des Vergleichs enthält Anhang 1. Die wesentlichen Ergebnisse beschreibt das nachfolgende Kapitel.

3 Vergleich DLT und herkömmliche Verfahren

In dieser Analyse wird beispielhaft dargestellt, wie die regulatorischen Anforderungen an die Lieferkettennachverfolgung sowie die hieraus abgeleiteten, grundlegenden technischen Anforderungen sowohl mit DLT als auch herkömmlichen Verfahren umgesetzt werden könnten.

Die Vergleichstabelle, die als Anhang mit dem vorliegenden Dokument veröffentlicht wird, beschreibt im Detail den konkreten technischen Vergleich beider Lösungswege.

3.1 Vorgehensweise und wesentliche Maßgaben

Vergleichsgegenstand ist die Lieferkettennachverfolgung. Hierfür ist es grundlegend erforderlich, zum einen die verantwortliche juristische Person sowie deren handelnde Personen und ggf. das betroffene Produkt resp. dessen Teile eindeutig zu identifizieren und dem betreffenden produzierenden Unternehmen zuzuordnen (Produktpass) und zum anderen, die eigentliche Lieferkette (Supply Chain), also den Prozess, nachzuweisen und dem Produkt und beteiligten Unternehmen eindeutig zuzuordnen.

Als Verfahren wurden gewählt:

- DLT: Europäische Blockchain Service Infrastructure
  - Für die DLT wurde die EBSI als Beispiel gewählt, da diese als paneuropäische DLT-Infrastruktur der Mitgliedstaaten aufgebaut wird. Zudem wird die Lieferkettennachverfolgung durch verschiedene Projekte aktuell auf der EBSI pilotiert, so z.B. TRACE4EU[29], EBSI ELSA[30]
  - Es gelten damit die organisatorischen (Governance) und technischen Rahmenbedingungen der EBSI[31].
- Herkömmliches Verfahren
  - Für das herkömmliche Verfahren wurde von einem verteilten Datenbanksystem ausgegangen, bei dem für den Prozess der Lieferkette ein Workflowsystem verwendet wird.

Es wurden folgende Anforderungen betrachtet:

Tabelle 13: Überblick Anforderungen zum Vergleich DLT vs. herkömmliche Verfahren

Art der Anforderung	Inhalt
Regulatorisch	eIDAS
	DSGVO
	Lieferkettenspezifische Regelung
Fachlich (abgeleitet aus regulatorischen Vorgaben)	Nachweisfähigkeit (Integrität, Authentizität, Verfügbarkeit etc.)

[29] Vgl. https://trace4eu.eu/ - abgerufen am 23.02.2026

[30] Vgl. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/EBSI-ELSA+EUIPO - abgerufen am 23.02.2026

[31] Vgl. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home bzw. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/What+is+ebsi und https://hub.ebsi.eu/vc-framework - abgerufen am 23.02.2026

Art der Anforderung	Inhalt
	Prozessintegration
Technisch	Identifizierung und Authentisierung
	Langfristige Lesbarkeit und Prüfbarkeit der Nachweisdaten
	Vermeidung Single Point of Failure
	Backup & Recovery
	Cybersicherheitsanforderungen
	Systemintegration
	Datenintegration
	Betrieb

3.2 Ergebnisse

3.2.1 Regulatorische Anforderungen

Hinsichtlich regulatorischer Anforderungen ist festzustellen, dass die Vorgaben der eIDAS hinsichtlich Identifizierung und Nachweisfähigkeit (Vertrauensdienste) sowohl mit DLT (EBSI) als auch herkömmlichen Verfahren umgesetzt werden können. Technisch wäre dies durch Anbindung einer elektronischen Identifizierung bei beiden Verfahren zu lösen. Die mit der neuen eIDAS 2.0 kommende EUDI Wallet kann ebenso in beiden Verfahrensarten verwendet werden, sowohl für die Speicherung als auch Präsentation digitaler Nachweise, wie z.B. einem digitalen Produktpass. Ebenso können qualifizierte elektronische Signaturen und Siegel für den Authentizitätsnachweis von on-chain/off-chain Daten im Falle DLT sowie Daten in herkömmlichen Systemen verwendet werden.

Hinsichtlich der Infrastruktur zum Prozessnachweis der Lieferkette bleibt festzuhalten, dass der Ledger selbst mit Section 11 der neuen eIDAS 2.0 als eigener qualifizierter Vertrauensdienst durch einen entsprechenden QTSP bereitgestellt werden kann. Die hierfür notwendige Konformitätsbewertung weist die Sicherheit der Infrastruktur nach; die Haftungs- und Nachweisregeln der eIDAS 2.0 gewährleisten zudem die notwendige Vertrauenswürdigkeit des Netzwerks für die Anwender der DLT, so dass im Fehlerfall Haftung und Verantwortung eindeutig geregelt sind. Diese Option besteht für herkömmliche Verfahren zur Lieferkettennachverfolgung aktuell nicht, erfordert bei DLT jedoch den zwingenden Einsatz von Public oder Private Permissioned DLT.

Beim Datenschutz ist die Immutabilität der DLT von Nachteil, da keine on-chain Daten gelöscht werden können. Dem kann bspw. durch Vermeidung der Speicherung personenbezogener Daten sowie einem Blacklisting (Sperrung) von on-chain-Daten begegnet werden. Hier sind klassische Verfahren von Vorteil, da diese (sofern nicht sog. WORM Speicher verwendet werden) eine physische Löschung von Daten ermöglichen.

Lieferkettenspezifische Regularien sind durch beide Umsetzungsformen erfüllbar. Dokumentation und Nachweis der Lieferkette werden in DLT durch die Replizierung aller

Transaktionen und Speicherung je Node erreicht; Metadaten können separat gespeichert werden. In herkömmlichen Verfahren kann dies mittels Workflow Engines und Repositories gelöst werden. Die Produktidentifizierung, Zuordnung zum Unternehmen und ähnliche Pflichten können in beiden Verfahrensarten durch QEAA gemäß der eIDAS 2.0 erfüllt werden.

3.2.2 Fachliche Anforderungen

Für den Nachweis von Authentizität, Integrität können bei beiden Verfahren qualifizierte Vertrauensdienste verwendet werden. Der Prozessnachweis kann bei DLT in Form von Smart Contracts sowie durch die Replizierung der on-chain Daten im Ledger, bei herkömmlichen Systemen durch Workflowengines erfolgen.

Hinsichtlich der langfristigen Verfügbarkeit der Nachweisdaten bleibt festzuhalten, dass für DLT aktuell internationale Standards noch in Entwicklung sind[32], während diese für herkömmliche Verfahren z.B. mit ISO 14721:2012[33], ISO 16363:2012[34] etc. bereits vorhanden sind.

3.2.3 Technische Anforderungen

Aus technischer Sicht ist festzuhalten, dass die Vermeidung eines Single Point of Failure, wie er bei rein zentralen Verfahren auftreten kann, bei DLT durch den verteilten Charakter, die Replizierung der on-chain Daten in den einzelnen Nodes sowie den dezentralen Konsensmechanismus verringert wird. Ein Angriff auf eine einzelne Node kann durch den Konsensmechanismus erkannt werden und würde zu einem Fehler im Konsens führen. Ein DLT-System ist durch die Verteilung der Nodes in einem immutablen Netzwerk per definitionem distributed; die Nodes können durch einen oder mehrere Betreiber in n-Jurisdiktionen betrieben werden und leicht ergänzt werden. Insofern ist die Redundanz dem System immanent, gleiches gilt durch die Replizierung der Daten für das Backup und Recovery. Da eine DLT per se jede Transaktion über alle Nodes trackt, ist die Verteilung der Traceability der DLT immanent. Auch ein Workflow in Form eines Smart Contracts wird einmal implementiert. Dabei wird definiert, für welche Nodes er verfügbar sein soll. Im Falle der Hinzufügung einer Node muss diese nur gewählt oder ausgeschlossen werden.

Hinsichtlich der Redundanz und Verteilung sind klassische Verfahren im Nachteil, da die Komplexität auch verteilter Datenbanken exponentiell mit der Anzahl der beteiligten Organisationen und Jurisdiktionen wächst. Der Kern einer DLT, die Verteilung, wird bei klassischen Verfahren eher zum Risiko, da sie für jede Datenbankinstanz aufwändiger zu implementieren ist als das Hinzufügen einer Node. Gleiches gilt für Mechanismen für Backup & Recovery, Workflow, Traceability oder ein Äquivalent zum Konsensmechanismus etc., die jeweils ebenso einzeln je Instanz zu implementieren und zu verteilen sind.

Die Manipulationssicherheit wird in DLT durch die Hashverkettung der Blöcke resp. deren Äquivalente gelöst. Problematisch dabei ist ein DLT unabhängiger Proof of Existence, der nur durch externe (qualifizierte) Zeitstempel, also im Kern durch das gleiche Verfahren wie bei herkömmlicher Lieferkettennachverfolgung, gelöst werden kann. Im Falle EBSI ist hierfür auch bereits eine entsprechende Funktionalität gegeben[35]. Bei klassischen Verfahren wird diese

32 CEN JTC19 entwickelt die technischen Vorgaben derzeit

33 ISO 14721:2012 Space data and information transfer systems — Open archival information system (OAIS) — Reference model

34 ISO 16363:2012

Space data and information transfer systems — Audit and certification of trustworthy digital repositories

35 https://hub.ebsi.eu/vc-framework/e-signing-e-sealing - abgerufen am 23.02.2026

Sicherheit bspw. durch sog. WORM Speicher oder die Verwendung qualifizierter Zeitstempel erreicht. QES etc. können bei beiden Optionen für Authentizität/Integrität eingesetzt werden.

Im Themenkomplex Cybersicherheit sind herkömmliche Verfahren derzeit als vorteilhafter anzusehen als DLT, da die notwendigen Standards zur Implementierung und Prüfung der Sicherheit des Verfahrens bereits vorhanden sind. Hervorzuheben sind hier bspw.:

- Verschlüsselung
  - Umsetzung gem. BSI TR-02102 oder SOGIS
- Kryptosicherheit
  - Umsetzung gem. ETSI TS 119 312
- Kryptostabilität
  - Umsetzung gem. ETSI TS 119 511 bzw. BSI TR-03125
- Informationssicherheitsmanagement
  - ISMS nach ISO 27001 resp. Sicherheitskonzept nach BSI Grundschutz

Im Falle DLT sind die notwendigen Standards aktuell in der Entstehung, so u.a.

- Policy und Security Requirements in CEN JTC 19
- Auditing Guidelines und Sicherheitsanforderungen in ISO Tc 307

Diese Vorgaben werden ca. Ende 2025 vorliegen.

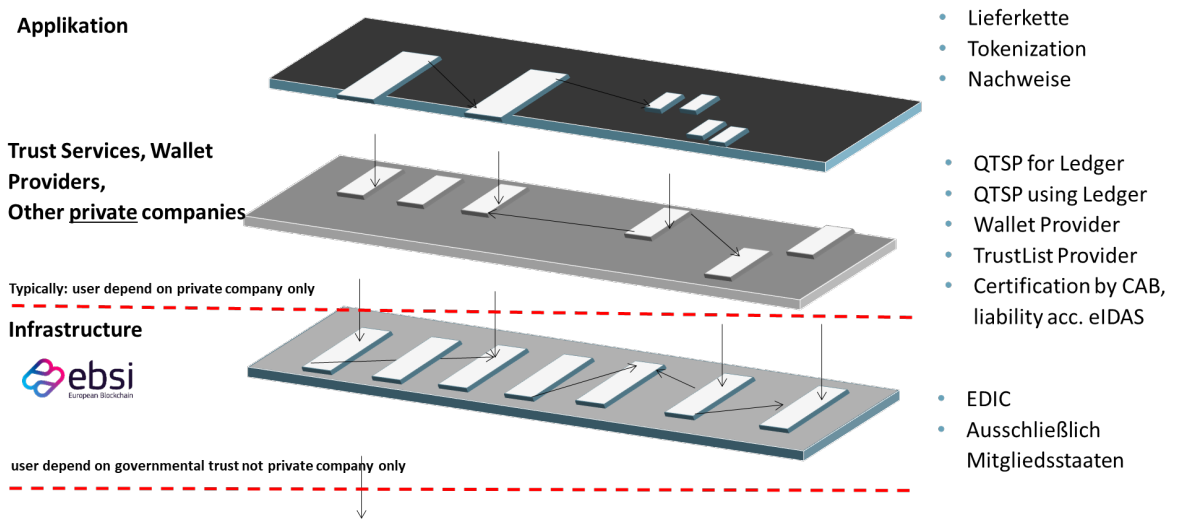
Eine ähnliche Situation liegt hinsichtlich der Datenintegration vor. Im Falle der Systemintegration bestehen mit den EBSI Spezifikationen[36] die notwendigen technischen Rahmenbedingungen bei DLT, die mit denen für herkömmliche Verfahren vergleichbar sind.

Im Falle des Betriebs wurde bei EBSI mit EDIC eine Betriebsorganisation der Mitgliedstaaten gegründet. Diese stellt die Grundinfrastruktur der EBSI bereit. Auf dieser werden die Anwendungen, wie bspw. die Lieferkettennachverfolgung, in Form von Sidechains implementiert. Das bedeutet, im Falle EBSI liegt immer eine de facto permanent vorhandene Grundinfrastruktur der europäischen Mitgliedsaten vor. Die Lieferkettennachverfolgung nutzt diese nur und stellt eine Applikation dar. Das bedeutet für die*den Anwender*in eine zusätzliche Betriebssicherheit und Cybersicherheit, da a) die Grundinfrastruktur auf Dauer angelegt und b) Manipulationen der Applikation in der Grundinfrastruktur erkannt werden können. Der Nachteil von EBSI ist, dass diese aktuell kein Servicemanagement oder wirksame Skalierung für Lieferkettennachverfolgung aufweist.

Die nachstehende Grafik verdeutlicht den Aufbau von EBSI.

36 https://hub.ebsi.eu/apis - abgerufen am 23.02.2026

Abbildung 4: Aufbau EBSI



Quelle: eigene Darstellung, msg systems ag

Herkömmliche Verfahren sind im Betrieb aktuell von Vorteil, da Service Management Prozesse und Service Level sowie entsprechendes Notfallmanagement i.d.R. vorhanden und erprobt ist.

3.3 Zusammenfassung

Zusammenfassend lässt sich festhalten, dass EBSI vor allem hinsichtlich der Datenverteilung, Traceability und Prüfung des Prozesses einer Lieferkette, der Systemredundanz, Backup & Recovery oder Prozessnachweis aufgrund der DLT immanenten Eigenschaften herkömmlichen Verfahren gegenüber von Vorteil ist. Nachteilig bleiben für DLT im Allgemeinen und EBSI im Besonderen die derzeit noch fehlenden Sicherheitsstandards sowie Schwächen bei Servicemanagement und Skalierung. Mit dem QTSP für Ledger schafft die Neufassung der eIDAS klare Regelungen für Haftung, Betrieb und prüfbare Sicherheit in DLT. Sobald die notwendigen technischen Standards vorliegen, dürfen die diesbezüglichen Nachteile behoben und DLT eine tatsächliche Alternative für herkömmliche Verfahren zur Lieferkettennachverfolgung darstellen. Dies gilt umso mehr, als dass die regulatorischen Vorgaben durch beide Verfahrensarten umsetzbar sind. Grundlegend ist jedoch festzustellen, dass DLT nur als Permissioned DLT die Anforderungen an die Lieferkettennachverfolgung erfüllen kann.

Herkömmliche Verfahren sind deutlich im Vorteil bei Fragen des Betriebs sowie der Informationssicherheit und Einsatz kryptographischer Mittel zum Authentizitäts- und Integritätsnachweis gem. eIDAS. Dies liegt vor allem daran, dass diese Methoden für bestehende Verfahren etabliert und erprobt sind sowie umfänglich genutzt werden. Darüber hinaus sind herkömmliche Verfahren vorteilhaft bei weniger komplexen, also weniger verteilten Lieferketten, wo der hohe Aufwand eines umfangreichen verteilten Prozesses weniger zum Tragen kommt. Des Weiteren sind die einfachere Nutzung von Identifizierungs-/ Authentisierungsmechanismen sowie etablierte Methoden für die langfristige Lesbarkeit und Prüfbarkeit zu nennen. Dies ist angesichts teilweise umfangreicher Aufbewahrungsfristen im Falle der Lieferkettennachverfolgung nicht zu unterschätzen.

4 Fazit

Mit dem QTSP für elektronische Ledger etabliert eIDAS einen dedizierten (qualifizierten) Vertrauensdienst für DLT. Durch die Integration von DLT in das eIDAS-Vertrauensrahmenwerk gelten alle Anforderungen an QTSP wie Haftung, Konformitätsbewertung durch unabhängige Konformitätsbewertungsstellen auch für DLT-Systeme, die von QTSP bereitgestellt werden. Dies gewährleistet nachgewiesene Sicherheit und das rechtliche Vertrauen, wie es u.a. für die Lieferkettennachverfolgung essentiell ist. Insofern kann QTSP für Ledger ein entscheidender Faktor für Industrie 4.0 sein, insbesondere in Sektoren wie Energie, Lieferkette und Fertigung.

Industrielle Anwendungsfälle wie Third-Party Risk Management, Smart Manufacturing, digitale Produktpässe und Lieferkettenoptimierung können von einer qualifizierten DLT-Infrastruktur profitieren. Im Industriebereich können qualifizierte elektronische Ledger die Umsetzung der europäischen Lieferkettenverordnung zum Nachweis der Herkunft von Produkten, aber auch zur Rückverfolgbarkeit von Produkten/Daten und Dokumenten ermöglichen. Vertrauenswürdige digitale Produktpässe können mithilfe qualifizierter Ledger sowie einem EUDI Wallet für juristische Personen ermöglicht werden. Damit könnte DLT in Verbindung mit dem EUDI Wallet, also der Verbindung von Transaktion (DLT) und Identität (EUDI Wallet), weiteren Mehrwert erzeugen. Mit EBSI liegt zudem eine gemeinsame DLT-Infrastruktur der Mitgliedstaaten vor, auf deren Basis Anwendungen, wie z.B. für die Lieferkette durch QTSP, bereitgestellt werden können. Das heißt, der qualifizierte Vertrauensdienst eines privaten Unternehmens würde auf Basis einer Infrastruktur der Mitgliedstaaten – also quasi einem staatlichen Vertrauensanker per default – aufgebaut.

Wesentliche Voraussetzung für eine Anwendung der DLT für die Lieferkette bilden valide europäische Standards, die die eIDAS Verordnung technisch untersetzen und Interoperabilität mit der internationalen Standardisierung aufweisen. Diese sind aktuell in CEN JTC 19 (Europa) und ISO Tc 307 (international) in Entwicklung. Hinzu kommen die laufenden europäischen Projekte, die die Anwendung der DLT für die Lieferkette pilotieren. Diese Erfahrungen müssen in die Entscheidungsfindung zur Nutzung von DLT einfließen.

Zusammenfassend schafft eIDAS die Grundlage für eine sichere Nutzung von DLT u.a. für die Lieferkette. Für die praktische Anwendung über Forschungsprojekte hinaus sollten jedoch die Standardisierung sowie die Durchführungsrechtsakte der eIDAS (EUDI-Wallet und QEAA: November 2024) bzw. QTSP für Ledger (Mai 2025), die auf konkrete technische Standards verweisen werden, sowie die Anwendung von ETSI/CEN Standards als Voraussetzung für EUDI Wallet und qualifizierte Vertrauensdienste abgewartet werden. Ohne diese Vorbedingungen erscheint eine Nutzung von DLT für die Lieferkette aufgrund mangelnder unabhängig geprüfter Sicherheit, fehlender klarer Haftungsregeln für den/die Betreiber des DLT-Systems sowie die mangelnde europäische Rechtsgrundlage, wie sie die eIDAS darstellt, kritisch. Dies bedeutet, dass DLT nur als Permissioned DLT die Anforderungen an die Lieferkettennachverfolgung erfüllen kann.

5 Bibliographie

Alamillo D., I. (2020). SSI eIDAS Legal Report. How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market. Brussels: European Commission. Retrieved April 26, 2021 from https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI_eIDAS_legal_report_final_0.pdf

Alamillo D., I., Schwalm, S. (2021): Self-Sovereign-Identity & eIDAS: a Contradiction? Challenges and Chances of eIDAS 2.0. European Review of Digital Administration & Law – Erdal 2021, Volume 2, Issue 2, pp. 89-100. DOI 9791259947529 10

Alamillo D., I., Schwalm, S., Stocker, C. Thiermann, R. (2024): Qualified Ledgers: Bridging the Gap between DLT Technology and Legal Compliance. 2024 https://medium.com/@schwalm.steffen/qualified-ledgers-bridging-the-gap-between-blockchain-technology-and-legal-compliance-c08d24a68db9

Alamillo D., I., Schwalm, S., Stocker, C. Thiermann, R. (2024): Qualified Ledgers – Breakthrough for proven security and legal trust in DLT through eIDAS2?. Open Identity Summit 2024. Bonn: Gesellschaft für Informatik e.V.. PISSN: 1617-5468. ISBN: 978-3-88579-744-9. pp. 195-200. DOI: 10.18420/OID2024_19.

Allen, C: https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md - abgerufen am 23.02.2026

Anke, J., Ehrlich, T., Richter, D, Meisel, M. (2021): Self-Sovereign Identity as the Basis for Universally Applicable Digital Identities. HMD 58, 247–270 (2021). https://doi.org/10.1365/s40702-021-00711-5

Bernabe, j. (2019): An Overview on ARIES: Reliable European Identity Ecosystem. In: Challenges in Cybersecurity and Privacy - the European Research Landscape. Chapter: 11

EU Blockchain Observatory (2018): Blockchain and the GDPR.. Brussels https://tinyurl.com/mkzkh9s4

Bundesamt für Sicherheit in der Informationstechnik (2024): BSI TR-02102-1. Kryptographische Verfahren: Empfehlungen und Schlüssellängen. https://tinyurl.com/58efntm5.

Bundesamt für Sicherheit in der Informationstechnik (2019): Towards Secure DLTs. Concepts, Requirements, Assessments. 2019. https://tinyurl.com/8tz6tn9j

CFR - Code of Federal Regulations Title 21. ITLE 21--FOOD AND DRUGS CHAPTER I--FOOD AND DRUG ADMINISTRATION DEPARTMENT OF HEALTH AND HUMAN SERVICES SUBCHAPTER A—GENERAL PART 11 ELECTRONIC RECORDS; ELECTRONIC SIGNATURE

COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market

DIN TS 31648:2021 Criteria for Trusted Transactions — Records Management and Preservation of Evidence in DLT/DLT. 2021.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). (2022). Official Journal, L 333, 80-152. ELI: http://data.europa.eu/eli/dir/2022/2555/oj

European Aviation Safety Agency (2023): ANNEX TO ED DECISION 2023/014/R Acceptable Means of Compliance (AMC) and Guidance Material (GM) to Annex I (Part 21) to Commission Regulation (EU) No 748/2012. Issue 2, Amendment 16

https://www.easa.europa.eu/en/document-library/acceptable-means-of-compliance-and-guidance-materials/amc-gm-part-21-issue-2-14

European Union Agency for Cybersecurity 82022): DIGITAL IDENTITY. Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust. https://www.enisa.europa.eu/publications/digital-identity-leveraging-the-ssi-concept-to-build-trust

EBSI, European Blockchain service Infrastructure: https://ec.europa.eu/digital-building-

eIDAS Bridge specification https://joinup.ec.europa.eu/collection/ssi-eidas-bridge/document/ssi-eidas-bridge-use-cases-and-technical-specifications

ESSIF, European Self-Sovereign Identity Framework, https://www.eesc.europa.eu/en/news-media/presentations/european-self-sovereign-identity-framework, accessed: 30/03/2020.

ETSI EN 319 411-1 v1.3.1 (2021): Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.03.01_60/en_31941101v010301p.pdf

ETSI EN 319 421 v1.1.1 (2016): Electronic Signatures and Infrastructures (ESI) Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. Electronic Signatures and Infrastructures (ESI). https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf

ETSI TS 103 732-1 v2.1.1 CYBER (2023): Consumer Mobile Device Protection Profile. https://www.etsi.org/deliver/etsi_ts/103700_103799/10373201/02.01.01_60/ts_10373201v020101p.pdf

ETSI TS 119102-1 v1.2.1 (2018): Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, 2018. https://www.etsi.org/deliver/etsi_ts/119100_119199/11910201/01.02.01_60/ts_11910201v010201p.pdf

ETSI TS 119 312 v1.4.3 (2023): Electronic Signatures and Infrastructures (ESI); Cryptographic Suites. https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.04.03_60/ts_119312v010403p.pdf

ETSI TS 119 612 v2.3.1 (2024): Electronic Signatures and Infrastructures (ESI); Trusted Lists. https://cdn.standards.iteh.ai/samples/69597/fce3734a908c4e18b2b6741164a16594/ETSI-TS-119-612-V2-3-1-2024-11-.pdf

European Parliament: Directorate-General for Parliamentary Research Services and Finck, M., Blockchain and the general data protection regulation – Can distributed ledgers be squared with European data protection law?, Publications Office of the European Union, 2019, https://data.europa.eu/doi/10.2861/535

Hellwig, D., Karlic, G., Huchzermeier, A. (2020). Build Your Own Blockchain: A Practical Guide to Distributed Ledger Technology. Springer, Cham. https://doi.org/10.1007/978-3-030-40142-9.

ISO 14721:2012 Space data and information transfer systems — Open archival information system (OAIS) — Reference model. 2012

ISO 16363:2012 Space data and information transfer systems — Audit and certification of trustworthy digital repositories. 2012

ISO 22739:2024: DLT and distributed ledger technologies - Terminology, 2024.

ISO 23257:2021 DLT and distributed ledger technologies — Reference architecture. 2021

ISO TR 24332:2025. Information and documentation — DLT and DLT in relation to authoritative records, records systems, and records management.

ISO 30301:2019, Information and documentation - Management systems for records - Requirements. 2019

Korte, U., Hühnlein, D, Schwalm, S. (2014): Standards for the preservation of evidence and trust. Proceedings Archiving 2014, Springfield, p. 9-14. DOI:10.2352/issn.2168-3204.2014.11.1.art0000

Kusber, T., Schwalm. S., Korte, U., Berghoff, C (2018): Langfristige Beweiswerterhaltung und Datenschutz in der Blockchain, DACH-Security 2018. p. 177-191 Frechen https://www.syssec.at/en/veranstaltungen/dachsecurity2018/papers/DACH_Security_2018_Paper_21A1.pdf

Kusber, T., Schwalm, S, Korte, U., Shamburger, K, (2021): Records Management and Long-Term Preservation of Evidence in DLT. In: Roßnagel, H., Schunck, C. H. & Mödersheim, S. (Hrsg.), Open Identity Summit 2021. Bonn: Gesellschaft für Informatik e.V.. p 131-142 https://dl.gi.de/server/api/core/bitstreams/0f4107a1-2333-4d3a-a603-18d1ee8cfca7/content

Kubach, M, Schunck, C. Sellung, R., Roßnagel, H. (2020): Self-sovereign and Decentralized identity as the future of identity Management?. In: Roßnagel, H., Schunck, C. H., Mödersheim, S. & Hühnlein, D. (Hrsg.), Open Identity Summit 2020. Bonn: Gesellschaft für Informatik e.V.. p 35-47 DOI: 10.18420/ois2020_03.

Marr, B. (2022): The Important Difference Between Web3 And The Metaverse, Forbes Magazin. 22.02.2022. https://www.forbes.com/sites/bernardmarr/2022/02/22/the-important-difference-between-web3-and-the-metaverse/?sh=3d02677e5af3

Merkle, R. C. (1980): Protocols for Public Key Cryptosystems. In: 1980 IEEE Symposium on Security and Privacy. IEEE, Oakland, CA, 1980. p 122-134.
DOI:10.1109/SP.1980.10006

OECD (2017), OECD Digital Economy Outlook 2017, OECD Publishing, Paris, https://doi.org/10.1787/9789264276284-en

Reddick, C. G.; Cid, G., P.; Ganapati, S.; Bolívar, R. and Scholl, H.J. (2019). Determinants of blockchain adoption in the public sector: An empirical examination. Info. Pol. 24, 4 (2019), 379–396. https://doi.org/10.3233/IP-190150

Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council (Text with EEA relevance). reg/2012/1025/2024-12-13

Regulation (EU) No 910/2014 of the European Parliament and of the Council - of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. eIDAS, 2014. reg/2014/910/2024-10-18

Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). (2016). Official Journal, L 119, 1-88. ELI: http://data.europa.eu/eli/reg/2016/679/oj

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act);

Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937

Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (OJ L, 2024/1183, 30.04.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj)

Sato, M., Matsuo, S.'I (2017): Long-Term Public DLT: Resilience against Compromise of Underlying Cryptography. In ICCCN: 26th International Conference on Computer Communications and Networks (ICCCN) July 31-August 3, 2017, Vancouver, Canada. IEEE, Piscataway, NJ; 2017, pp 1–8. DOI:10.1109/EuroSPW.2017.49

Schwalm, S (2023): eIDAS 2 and the role of identity standards: an outlook of current activities. Conferencia principal: La propuesta de Reglamento eIDAS 2: contexto y visión general. Universidad de Murcia. Murcia 23.11. 2023. https://tinyurl.com/5x5mwmkr
DOI:10.13140/RG.2.2.25074.48321

Sedlmeir, J., Smethurst, R., Rieger, A., Fridgen,G. (2021). Digital Identities and Verifiable Credentials. Bus Inf Syst Eng 63, 603–613 https://doi.org/10.1007/s12599-021-00722-y

Sobolewski, M., & Allessie, D. DLT Applications in the Public Sector: Investigating Seven Real-Life DLT Deployments and Their Benefits. In M. P. and S. H. J. Reddick Christopher G. and Rodríguez-Bolívar (Ed.), DLT and the Public Sector: Theories, Reforms, and Case Studies (pp. 97–126). Springer International Publishing. DOI: 10.1007/978-3-030-55746-1_5

SOG-IS Crypto-Evaluation Scheme. Agreed Cryptographic Mechanisms. Version 1.3. 2023. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf

Strueker J., Urbach, N., Guggenberger, T., Lautenschlager, I., Ruhland, N., Schlatt,V., Sedlmeir, J., Stoetzer, J-C., Voelter, F. (2021): Self-Sovereign Identity - Foundations, applications, and potentials of portable digital identities. Project Group Business & Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT, Bayreuth

UK Government Office for Science (2016): Distributed Ledger Technology: beyond blockchain. https://assets.publishing.service.gov.uk/media/5a818d6fe5274a2e87dbe3dd/gs-16-1-distributed-ledger-technology.pdf

UN United Nations Commission on International Trade (0217): UNCITRAL model law on electronic transferable records. United Nations, New York, 2017.
https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf

W3C Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations. W3C Recommendation 19 July 2022
https://www.w3.org/TR/did-1.0/

Weber, M., Vogt, T., Krogel, W., Schwalm S. (2018): Records Management nach ISO 15489. Einführung und Anleitung, Berlin

Werbach., K. (2018): DLT and the New architecture of Trust. Massachusetts Institute of Technology.

Xu, X.., Weber, I., Staples, M. (2019): Architecture for Blockchain Applications. Cham.

Yaga, D. , Mell, P. , Roby, N. and Scarfone, K. (2018), Blockchain Technology Overview, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.8202

Yildiz,H., Ritter, R., Nguyen, L. T. , Frech, B., Martinez, M. and Küpper, A. (2021): Connecting Self-Sovereign Identity with Federated and User-centric Identities via SAML Integration. IEEE Symposium on Computers and Communications (ISCC), Athens, Greece, 2021, pp. 1-7,
doi: 10.1109/ISCC53001.2021.

A Anhang 1: Fallstudien zur Lieferkettennachverfolgung mit DLT

A.1 Fallstudie 1: Lieferkettennachverfolgung in Übereinstimmung mit der EU-Batterieverordnung

Regulatorische Informationsanforderungen

Die EU-Batterieverordnung (EU 2023/1542) enthält eine Reihe von Informationen, die Wirtschaftsakteure, d. h. die Importeure und Hersteller, die das Endprodukt auf den Markt bringen, über ihre Lieferkette sammeln müssen. Die Hauptkategorien der zu sammelnden Informationen sind:

Der CO_2-Fußabdruck des Produkts

Von Dritten ausgestellte Zertifikate und Lieferanten

Spezifische Mengen an Rohstoffen, die im Endprodukt enthalten sind

Herkunft der Rohstoffe, einschließlich Materialtransaktionen

Die EU-Batterieverordnung ist nicht die einzige Verordnung, die Stakeholder zur Datenerfassung verpflichtet. Weitere EU-Verordnungen enthalten ähnliche Anforderungen, wie der EU Critical Raw Materials Act (EU 2024/1252), der bis 2030 einen Mindestanteil an Rohstoffen aus der EU in Batterien vorsieht, und die EU Conflict Minerals Regulation (EU 2017/821), die den Nachweis einer verantwortungsvollen Beschaffung von Zinn, Tantal, Wolfram und Gold verlangt.

Ähnliche Vorschriften bestehen und entstehen in anderen Teilen der Welt. Der US Inflation Reduction Act ist das prominenteste Beispiel, das unter anderem ein Kreditsystem für Elektrofahrzeuge basierend auf der Herkunft der Rohstoffe einführt.

Technische Anforderungen an ein Lieferkettennachverfolgungssystem

Es ist wichtig zu beachten, dass die oben genannten Informationsanforderungen erfüllt werden können, ohne dass ein digitales System, DLT-basiert oder konventionell, erforderlich ist. So erfüllen Unternehmen derzeit ihre Compliance, indem relevante Dokumente und Daten per E-Mail zwischen den verschiedenen Unternehmen ausgetauscht werden.

Natürlich hat dieser Ansatz seine Grenzen. Die zunehmenden regulatorischen Anforderungen machen es für Unternehmen immer kostspieliger, ihre Sorgfaltspflichten zu erfüllen, und die Notwendigkeit von Software, Standards und Protokollen zur Effizienzsteigerung dieses Prozesses ist offensichtlich. Neben der Anforderung an Effizienz und Automatisierung besteht auch ein Bedarf an einem höheren Maß an Vertrauen in die ausgetauschten Daten, da sonst die immer weitreichenderen Informationsanforderungen nur zu einem verstärkten Greenwashing beitragen.

Zusammenfassend kann gesagt werden, dass Systeme erforderlich sind, die die Sammlung dieser Daten in digitaler Form an dem Punkt erleichtern, an dem sie erzeugt werden. Solche Systeme sollen:

1. den Datenaustausch zwischen den Akteuren in einer stark verteilten und vielfältigen Lieferkette ermöglichen und
2. sicherstellen, dass der Ursprung und die Authentizität der Informationen von jedem autorisierten Akteur verifiziert werden können, unabhängig davon, wo sie am Ende in der Lieferkette landen.

Diese Punkte machen deutlich, dass kein einzelnes System, und noch weniger eine einzelne Software, alle diese Anforderungen erfüllen kann. Daher sind Standards für alle verschiedenen Teile des Systems und Schnittstellen zwischen diesen verschiedenen Modulen erforderlich.

DLT und die breitere Kategorie der Kryptographie-Technologien sind von besonderer Bedeutung und Interesse für die Anforderungen Datensicherheit und Verifizierbarkeit. Wie eine solche Umsetzung mit DLT aussehen kann, wird im folgenden Abschnitt erläutert.

Beispielszenario für ein Rückverfolgbarkeitssystem für die EU-Batterieverordnung

Notwendigkeit dezentraler und privater Datenspeicherung

Die EU-Batterieverordnung betrifft insbesondere Hersteller von Elektroautos. Die Lieferkette in dieser Industrie ist hochkompetitiv, und daher sind die meisten Daten, einschließlich der Identität der Lieferanten, hochvertraulich und können nicht ohne weiteres öffentlich gemacht werden. Um maximale Vertraulichkeit zu gewährleisten, sollten daher immer nur die zwei betroffenen Parteien in den Datenaustausch involviert sein. Die Parteien müssen die volle Kontrolle über ihre Daten behalten und diese nur auf Anfrage über eine direkte Verbindung mit einer anderen Partei teilen können.

Diese Bedingung der maximalen Vertraulichkeit und Datenkontrolle besteht auch in vielen anderen Lieferketten, wie Elektronik, Textilien usw. Sie schließt auch die Nutzung von DLTs jeglicher Art als Datenaustauschsystem aus, ob public, permissioned, oder private-permissioned. Es schließt aber auch die Existenz einer, eventuell von dem Regulator bereitgestellten, zentralen Datenbank aus. Eine solche Datenbank wäre per Definition für mindestens eine zusätzliche Partei zugänglich.

DLT Hashes als Integritätsnachweis

Dies bedeutet jedoch nicht, dass DLTs und ihre zugrunde liegenden kryptographischen Bausteine nutzlos sind. Tatsächlich können wir, anstatt die Daten direkt auf einer DLT zu speichern – was sie für jeden zugänglich machen würde, der Zugriff auf diese DLT hat –, einige ihrer nützlichen Eigenschaften nutzen, indem wir Hashes von Daten auf der DLT speichern.

Ein Hash ist eine Zusammenfassung einer großen Datenmenge in einer kurzen alphanumerischen Zeichenkette. Hashes haben einige vorteilhafte Eigenschaften:

- Man kann die ursprünglichen Daten nicht aus dem Hash ableiten.
- Dieselben Daten resultieren immer in demselben Hash.
- Hashes sind immer gleich lang, egal wie groß die ursprünglichen Daten sind.

Diese Eigenschaften sind hilfreich, um zwei Versionen von Datensätzen zu vergleichen und sich zu versichern, dass sie exakt identisch sind. Anstatt zwei Versionen von einem 900 Seiten Buch Buchstabe um Buchstabe zu vergleichen, genügt es, einfach die Hashes der beiden Versionen zu vergleichen.

Um zu sehen, wie die Hashes und DLT kombiniert werden können, betrachten wir das folgende Beispiel: Eine Zertifizierungsstelle, TUFF, stellt ein Zertifikat Z für nachhaltigen Bergbau für die Bergbaugesellschaft Copper Gold aus. Darüber hinaus generiert TUFF den Hash des Zertifikats (HZ) und speichert ihn auf einer DLT (nehmen wir an, es handelt sich um eine öffentliche DLT wie Ethereum). Dazu verwendet TUFF eine der gängigen Hash Methoden gem. SOGIS[37].

[37] Vgl. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf - abgerufen am 23.02.2026

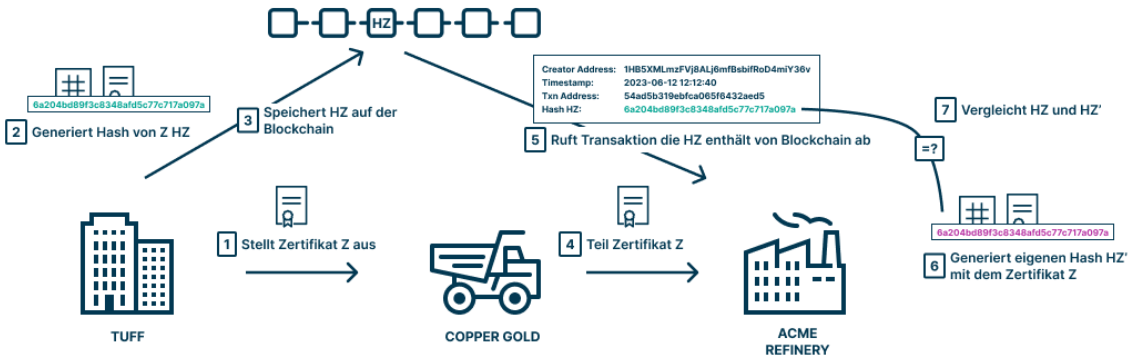
Einer der Kunden von Copper Gold, ACME Refinery, muss Drittzertifikate von seinen Lieferanten sammeln, um die neue EU-Batterieverordnung einzuhalten. Copper Gold teilt das Zertifikat Z mit ACME, einschließlich der Adresse des Hashes auf der DLT.

ACME kann nun in einigen Schritten die Authentizität von Z nachprüfen:

1. Unter Benutzung der DLT-Adresse, ruft ACME HZ von der DLT ab. Im Zuge dessen erhält ACME auch den Zeitstempel T des Blocks, in dem HZ gespeichert ist. T entspricht dem Erstellungsdatum des Blocks. Aufgrund der in Kapitel 1 erläuterten Eigenschaften der DLT lässt sich mit Sicherheit sagen, dass HZ vor dem Zeitpunkt T erstellt wurde, da Daten, die einmal auf der DLT gespeichert wurden, nicht mehr verändert werden können.
2. Als nächstes benutzt ACME jetzt ebenfalls die Hash-Methode MD5, um seinen eigenen Hash von Z zu generieren (HZ'). Ein Vergleich von HZ und HZ' ergibt eine 100% Übereinstimmung.
3. Wir nehmen für den Moment an, dass ACME überprüfen kann, dass TUFF der Ersteller von HZ auf der DLT ist. Diese Annahme ist essentiell, da die Aussagekraft des Hashvergleichs sonst deutlich reduziert ist. Dies ist jedoch derzeit bei weitem noch nicht automatisch der Fall. Diese Annahme erfordert das Vorhandensein eines Vertrauensökosystems. Auf diesen Aspekt wird im nächsten Absatz eingegangen.

Nach Ausführung der Schritte 1-3 kann ACME mit Sicherheit sagen: 1) Der Hash wurde von TUFF auf der DLT abgelegt. 2) TUFF hat den Hash mindestens vor Zeit T erstellt. 3) Der Hash HZ von der DLT entspricht genau dem Hash HZ'. Dementsprechend lässt sich sagen, dass der Inhalt des Dokuments Z seit der Erstellung durch TUFF nicht von Copper Gold Mining oder einer anderen Partei geändert wurde.

Abbildung 5: TUFF DLT



Quelle: eigene Darstellung, msg systems ag

Auch wenn der obige Verifizierungsprozess kompliziert erscheint, wäre er in einer realen Situation vollständig automatisiert und würde nur einen Sekundenbruchteil dauern. Ein hervorzuhebender Vorteil ist außerdem, dass ACME TUFF nicht kontaktieren muss, um die Authentizität des Dokuments zu überprüfen. Dies trägt sowohl zur Effizienz als auch zur Privatsphäre aller Teilnehmer bei.

Hier wird deutlich, dass die DLT-Technologie in Kombination mit anderen kryptographischen Bausteinen einen erheblichen Beitrag zu mehr Datenauthentizität und damit auch Vertrauen in Daten beitragen kann. Damit werden direkt ACMES Compliance-Risiko und Kosten reduziert. Letztendlich kommt die bessere Datenqualität auch den Regulierungsbehörden, Verbrauchern und dem Planeten zugute.

Dieses Beispiel beleuchtet nicht, über welchen Mechanismus die Informationen zwischen zwei Parteien ausgetauscht werden, ausschließlich wie eine Verifizierung der Daten ablaufen könnte.

Verbleibende Herausforderungen und fehlende Elemente

Wenn wir die aktuelle Entwicklung der Landschaft von Standards und Systemen betrachten, um die Anforderungen aus Kapitel 1.2 zu erfüllen, haben Verifizierbarkeit und Authentizität derzeit nicht die höchste Priorität. Hierfür sind unter anderem folgende Gründe anzuführen:

- **Datenaustauschprotokolle**

Zuerst muss ein Mechanismus für Datenaustausch festgelegt werden und entsprechende Software entwickelt werden. Wie bereits erwähnt, erfolgt der Austausch derzeit hauptsächlich per E-Mail und stellt einen erheblichen Kostenpunkt für alle Beteiligten dar. Außerdem gibt es dadurch kein einheitliches Format für wichtige Informationen wie Materialtransaktionen oder CO2-Fußabdruck. Data Space Technologien wie Catena-X bieten hier Lösungen an. Der Datenaustausch hat für alle Akteure höchste Priorität. Sobald diese Datenaustauschtechnologien weit verbreitet sind, kann das Problem der Datenverifizierbarkeit angegangen werden.

- **Vertrauensökosysteme**

Ein zweiter wichtiger Grund, warum Datenverifizierungsmechanismen wie (qualifizierte) Attributsbescheinigungen noch nicht weit verbreitet sind, liegt an dem Fehlen von Vertrauensökosystemen. Im Wesentlichen muss ACME die reale Entität hinter der DLT-Adresse identifizieren, die den Hash eingereicht hat. Ansonsten lässt sich zwar sagen, dass sich Z seit T nicht verändert hat. Jedoch lässt sich nicht mehr sagen, dass TUFF der Urheber der Originalversion ist. Jede andere Entität hätte HZ erstellen können und damit auch die Möglichkeit, Z vor der Erstellung des Hashes zu manipulieren. Die Lösung dieser Lücke ist Teil mehrerer Arbeitsgruppen, darunter das Trace4EU-Projekt. Der wichtigste Baustein für die Erfüllung dieser Anforderungen ist die öffentliche digitale Infrastruktur der EU wie die European DLT Services Infrastructure (EBSI) und die European Digital Identity (EUDI).

So wird TUFF in einem zukünftigen EUDI-Wallet ein Identitätszertifikat erhalten, das alle relevanten Details der Unternehmensidentität von TUFF enthält. Die ideale Stelle zur Ausstellung dieses Zertifikats wäre das Handelsregister des Landes, in dem TUFF ansässig ist. Zudem würde die TUFF die DLT-Adresse, die es für das Ablegen von Hashes verwendet, an das EUDI-Wallet binden.

Dies wird folgenden Verifizierungsprozess ermöglichen:

- ACME überprüft die kryptographische Bindung der DLT-Adresse an die EUDI-Wallet.
- ACME ruft TUFFs Identitätszertifikat ab und überprüft die digitale Signatur.
- ACME prüft, ob die digitale Signatur des Identitätszertifikats zu dem Handelsregister des Landes gehört. Dafür wird es entsprechende Services auf Landes- und EU Ebene geben.

- **Garbage-in-Garbage-out**

Es ist ein gängiges Missverständnis, dass der Einsatz von DLT-Technologien die Qualität der zugrundeliegenden Daten verbessert. Dies ist ausdrücklich nicht der Fall. Die Technologie kann helfen, zuverlässig die*den Urheber*in der Daten zu identifizieren und sicherzustellen, dass Daten nicht verändert wurden. Dies kann allerdings einen sekundären positiven Effekt auf die Datenqualität haben. Insbesondere werden Systeme zum Datenmanagement häufig von Drittparteien zertifiziert. Mit Hilfe der oben beschriebenen Technologie können diese Parteien

Zertifikate ausstellen, die von jeder anderen Partei verifiziert werden können und so einen Rückschluss auf die Qualität der Daten ermöglichen.

Fazit

Die DLT-Technologie bietet durch die Möglichkeit, Hashes von Daten abzulegen und auf diese Weise einen „Zeitstempel" zu erstellen, Potential für eine bessere Verifizierbarkeit von Daten in der Lieferkettennachverfolgung. Hierbei kann verifiziert werden, ob ein Datensatz seit der Erstellung des Hashes verändert wurde. Eine genauere Betrachtung zeigt jedoch, dass dieser Aspekt nur einen von mehreren Verifizierungsschritten in der Lieferkettennachverfolgung darstellt. Insbesondere ist ein Vertrauensökosystem notwendig, das es erlaubt, die Identität der Ersteller*in der Hashes zu verifizieren. Außerdem benötigen die Parteien in der Lieferkette effiziente Protokolle zum sicheren Datenaustausch.

A.2 Fallstudie 2: FSC DLT

Das FSC-Label

Der Forest Stewardship Council (FSC) ist eine internationale gemeinnützige Organisation, die eine verantwortungsvolle Bewirtschaftung der Wälder weltweit fördert. Gegründet im Jahr 1993, setzt der FSC Standards für Waldprodukte und zertifiziert sie als nachhaltig produziert, wenn sie bestimmte Umwelt-, Sozial- und Wirtschaftskriterien erfüllen. Das FSC-Label stellt sicher, dass Produkte aus verantwortungsvoll bewirtschafteten Wäldern stammen, die ökologische, soziale und wirtschaftliche Vorteile bieten. Damit zielt der FSC darauf ab, Entwaldung zu bekämpfen, die Biodiversität zu schützen und die Rechte indigener Völker und Arbeiter zu gewährleisten.

Die spezifische Art des FSC-Labels hängt vom Detaillierungsgrad der Rückverfolgbarkeit der Rohstoffe und dem Anteil des zertifizierten Holzes im Endprodukt ab. Daher muss der FSC spezifische Massenbilanzmengen entlang der Lieferkette verfolgen.

Darüber hinaus ist der Holzsektor auch von einer bedeutenden neuen Verordnung, der EU-Entwaldungsverordnung (EUDR) betroffen, die insbesondere Anforderungen an die Rückverfolgbarkeit stellt. Der FSC besitzt bereits die entsprechenden Daten, um seinen Mitgliedern bei der Erfüllung dieser Anforderungen der EUDR zu helfen, da er bereits von allen zertifizierten Einheiten die Sammlung der notwendigen Massenbilanz-Rückverfolgbarkeitsdaten verlangt. Die FSC-DLT fügt lediglich die Erfassung von Geolokationen und des rechtlichen Eigentumsübergangs hinzu.

Abbildung 6: FSC Supply Chain



Quelle: eigene Darstellung, msg systems ag

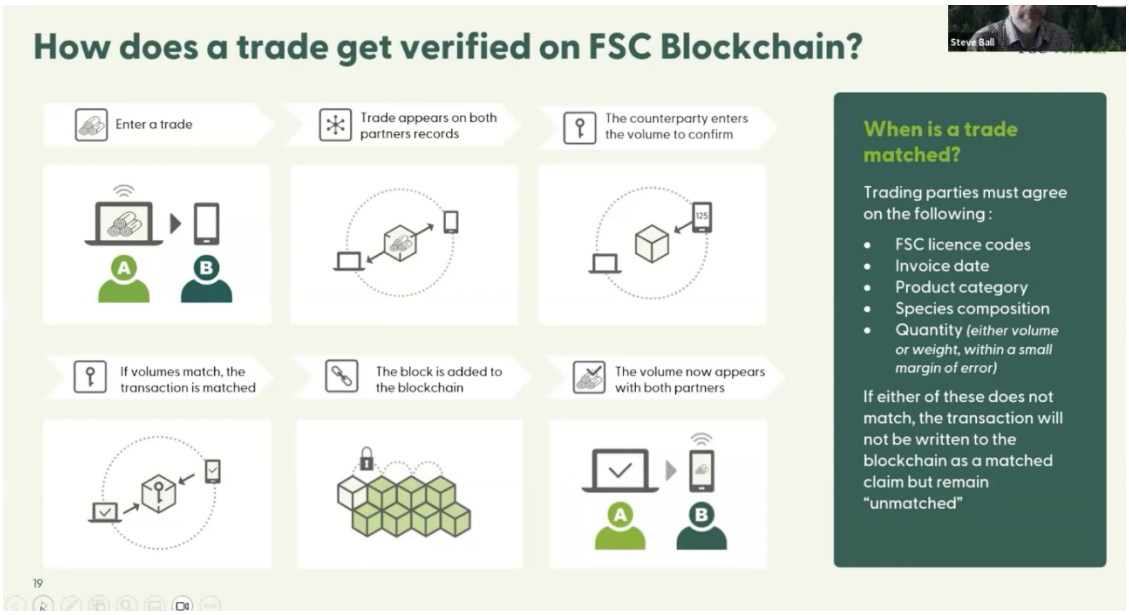
FSC DLT Features

Für den FSC besteht das Ziel der Einführung der DLT darin, alle von den verschiedenen Parteien eingereichten Daten zu verknüpfen, um das Reporting für alle zu vereinfachen. Anstatt dass jeder Stakeholder nur seine eigenen Daten erstellt und E-Mails und PDFs versenden muss, um die Daten seiner Lieferanten zu sammeln, bietet der FSC die DLT-Lösung als Datenaustauschplattform an. Datenaustausch ist also hier auch das Hauptanliegen, obwohl der Begriff DLT etwas anderes suggeriert.

Wie oben erwähnt, sind öffentliche und permissioned DLTs aufgrund der Größenbeschränkungen und unbeschränkten Zugangskontrollen weniger ideal für die Datenspeicherung. Deshalb hat sich der FSC für eine permissioned-private DLT entschieden, die im Wesentlichen eine Datenbank ist, die unter einer kleinen Anzahl vertrauenswürdiger Organisationen synchronisiert wird.

Zwei Parteien, die eine Transaktion von Holzprodukten abwickeln, z.B. Sawmill und Factory, geben die Transaktionsdaten in das interne System des FSC ein. Bevor diese in die DLT übermittelt werden, vergleicht das System die Informationen und markiert sie entsprechend als übereinstimmend oder nicht übereinstimmend. Anschließend werden die Transaktionsinformationen auf der DLT gespeichert. Hier wird dementsprechend auch, wie im vorherigen Beispiel, eine gewisse Unveränderbarkeit der Daten ab dem Zeitpunkt der Speicherung auf der DLT garantiert. Allerdings ist diese Garantie schwer nachweisbar, ohne zu wissen, wie die interne private DLT genau funktioniert.

Abbildung 7: FSC DLT



Quelle: eigene Darstellung, msg systems ag

Laut FSC bleibt die Datenkontrolle vollständig bei den verschiedenen Stakeholdern, da alle eingereichten Daten verschlüsselt sind. Es ist jedoch unklar, wie genau dies möglich ist.

Fazit

Das System scheint seine primäre Anforderung zu erfüllen, Stakeholdern in der Forstlieferkette zu helfen, Daten zu teilen, auf Daten anderer Stakeholder zuzugreifen und in effizienter Art und Weise die erheblichen Informationsanforderungen der EUDR zu erfüllen. Nach allen verfügbaren Informationen ähnelt dieses System jedoch eher einem zentralen Datenbankdienst. Der Einsatz von DLT-Technologie in einem solchen System dürfte einen geringen Mehrwert bieten.

Die Analyse dieses Abschnitts beruht auf den vom FSC geteilten Information in einem Webinar vom 21. Juni 2024.

A.3 Zusammenfassung der Fallstudien

Fazit

1. DLT ist keine All-or-Nothing Lösung. Bestimmte Charakteristiken von DLTs, insbesondere die Unveränderlichkeit und universelle Überprüfbarkeit der Zeitstempel eines Blocks können verwendet werden, wo es nötig ist, ohne sich komplett in ein DLT-System einzuschließen.

2. DLTs eignen sich nicht als Datenspeicher. Public DLTs haben nicht genug Speicherkapazität und sind außerdem öffentlich, was dem vorherrschenden Prinzip der Datenvertraulichkeit in der Lieferkette widerspricht. Private DLTs können zwar mehr Kapazität aufbieten, verlieren jedoch die wesentlichen Nachprüfbarkeitsmechanismen und bieten kaum Vorzüge zu zentralen Datenspeichern.

3. Zentrale Datenspeicher sind auch keine Lösung in kompetitiven Lieferketten wie der Batterielieferkette. Die Daten in der Lieferkette sind vertraulich. Das heißt,

jeder Teilnehmende muss zwingend weiterhin ihre*seine eigenen Daten speichern und nur bei Bedarf mit einer spezifischen Partei teilen.

4. DLT-Lösungen haben den größten Nutzen in einem verteilten dezentralen System, in dem die Daten dezentral gespeichert sind, und in Verbindung mit einem Vertrauensökosystem das es erlaubt, DLT-Signaturen mit echten Unternehmen zu verbinden.

Kurzversion: Rückverfolgbarkeitssystem für die EU-Batterieverordnung

Die EU-Batterieverordnung stellt Hersteller von Elektroautos vor die Herausforderung, vertrauliche Lieferkettendaten sicher zu speichern und auszutauschen. Ein dezentraler Ansatz mit DLT-Hashes bietet hierfür eine Lösung, ohne dass sensible Daten direkt auf der DLT liegen. Stattdessen werden nur Hashes – eine kryptografisch erzeugte Kurzversion der Daten – auf öffentlichen DLTs wie Ethereum gespeichert, um Authentizität und Integrität zu gewährleisten.

Beispiel: TUFF, eine Zertifizierungsstelle, stellt ein Nachhaltigkeitszertifikat für Copper Gold aus und speichert dessen Hash (HZ) auf der DLT. Ein Kunde wie ACME Refinery kann durch den Hash und dessen Zeitstempel sicherstellen, dass das Zertifikat echt ist und nicht verändert wurde.

Herausforderungen: Es fehlen derzeit standardisierte Austauschprotokolle, und die Verifikationsprozesse sind noch nicht weit verbreitet. Data Space-Technologien wie Catena-X könnten diese Lücke schließen, sobald sie implementiert sind. Neben standardisierten Austauschprotokollen fehlen noch umfassende Vertrauensnetzwerke, um sicherzustellen, dass die Urheber der Daten zuverlässig identifiziert werden können. In Zukunft könnte eine Zertifizierungsstelle wie TUFF ein Identitätszertifikat in einem EUDI-Wallet erhalten, das die DLT-Adresse mit ihrer verifizierten Identität verknüpft. Dieser Schritt würde es Handelspartnern wie ACME ermöglichen, die Authentizität und Quelle von Daten durch Verknüpfung mit offiziellen Handelsregistern nachzuvollziehen. Zusätzlich ist die Annahme „Garbage-in-Garbage-out“ zu beachten – die DLT garantiert keine Datenqualität, sondern lediglich unveränderte Daten.

Fazit: DLT-basierte Hashes ermöglichen eine zuverlässige Verifizierbarkeit von Daten, wenn auch nur als ein Baustein. Für eine funktionierende Rückverfolgbarkeit braucht es außerdem Vertrauensnetzwerke und sichere, effiziente Datenprotokolle, die langfristig die Compliance und Datenqualität verbessern können.

Kurzversion: FSC DLT

Der Forest Stewardship Council (FSC) fördert nachhaltige Waldwirtschaft und zertifiziert Produkte, die strenge Umwelt-, Sozial- und Wirtschaftskriterien erfüllen. Das FSC-Label gewährleistet, dass Produkte aus verantwortungsvoll bewirtschafteten Wäldern stammen, was zur Erfüllung der EU-Entwaldungsverordnung (EUDR) beiträgt. Um die Rückverfolgbarkeit der Holzlieferketten zu verbessern, hat der FSC eine permissioned-private DLT eingeführt, die Daten zur Geolokation und Eigentumsübertragung erfasst.

Statt dass Stakeholder Daten per E-Mail oder PDF austauschen, bietet die FSC-DLT eine Plattform für den Datenabgleich und -austausch. Transaktionsdaten werden zwischen Handelspartnern synchronisiert und auf ihre Übereinstimmung geprüft, bevor sie in die DLT geschrieben werden. Obwohl die DLT unveränderliche Daten garantieren soll, ist die genaue Umsetzung aufgrund der privaten Natur des Systems schwer überprüfbar.

Fazit: Die FSC-DLT erfüllt die Anforderung an effizienten Datenaustausch in der Forstwirtschaft, scheint jedoch eher wie eine zentrale Datenbank zu agieren. Der Nutzen der DLT-Technologie bleibt hier fraglich.