

DIN/TS 31648



ICS 35.240.99

**Kriterien für vertrauenswürdige Transaktionen –
Records Management und Beweiswerterhaltung in Distributed Ledger
Technologien und Blockchain**

Criteria for Trusted Transactions –
Records Management and Evidence Retention in DLT and Blockchain

Gesamtumfang 33 Seiten

DIN-Normenausschuss Information und Dokumentation (NID)

Inhalt

	Seite
Vorwort	4
Einleitung	5
1 Anwendungsbereich	6
2 Normative Verweisungen	6
3 Begriffe	7
4 Technologischer Überblick Blockchain/DLT	12
5 Vertrauenswürdigkeit digitaler Transaktionen	13
6 Blockchain/DLT in Beweiswerterhaltung und Records Management	15
6.1 Blockchain/DLT und Records Management	15
6.2 Blockchain/DLT und Beweiswerterhalt	15
7 Fachliche Kriterien für den Einsatz von Blockchain/DLT im Records Management	17
7.1 Kriterien hinsichtlich Compliance und Steuerung geschäftsrelevanter Aufzeichnungen	17
7.1.1 Sicherstellung regulatorischer Vorgaben	17
7.1.2 Sicherstellung des Stands der Technik	17
7.1.3 Nachweisfähigkeit digitaler Prozesse	17
7.1.4 Policies und Richtlinien	18
7.1.5 Risikobewertung	18
7.1.6 Rollen und Verantwortlichkeiten	18
7.1.7 Monitoring und Evaluation	18
7.1.8 Zertifizierung und Prüfung	19
7.2 Kriterien im Lebenszyklus geschäftsrelevanter Aufzeichnungen	19
7.2.1 Erzeugung und Speicherung digitaler Aufzeichnungen	19
7.2.2 Klassifizierung und Indexierung	19
7.2.3 Identifizierung	19
7.2.4 Rechtemanagement	20
7.2.5 Rechtevergabe	20
7.2.6 Zugangskontrolle	20
7.2.7 Datenschutz und Vertraulichkeit	21
7.2.8 Digitale Langzeitspeicherung	21
7.2.9 Aussonderung und Löschung	22
8 Technische Kriterien für den Einsatz von Blockchain/DLT im Records Management	22
8.1 Informationssicherheit	22
8.1.1 Konsensmechanismus	22
8.1.2 Kryptografische Verfahren	22
8.1.3 Virtuell-Real-Schnittstelle	23
8.1.4 Weitere Angriffsszenarien	23
8.1.5 Allgemeine IT-Sicherheit	23
8.1.6 Zeitstempelerneuerung und Hashbaumerneuerung	23
8.1.7 Sicherstellung Proof of Existence	25
8.2 Interoperabilität	25
8.3 Leistung	25
8.4 Skalierbarkeit	26
8.5 Übertragbarkeit	27
8.6 Wartbarkeit	27
8.7 Zuverlässigkeit	27
8.7.1 Ausfallsicherheit/Fehlertoleranz	27
8.7.2 Shared secrets/Stimmrechte	27
8.7.3 Verteilung zur Datensicherheit	28
8.7.4 Verteilung zur Ausfallsicherheit	28
Anhang A (informativ) Anwendungsbeispiele	29

Anhang B (normativ) Erfüllung der Anforderungen an ein Records Management in Blockchain/DLT durch geeignete eIDAS-Werkzeuge	30
Literaturhinweise	31

Bilder

Bild 1 — Problematik fehlenden Rehashings und Proof of Existence in Blockchain/DLT	16
Bild 2 — Beweiswerterhaltung und langfristige Integritätssicherung in Blockchain/DLT	24
Bild 3 — Beschränkungen von verteilten Systemen: „wähle 2 von 3 Eigenschaften“	26

Tabellen

Tabelle 1 — Bewertung Blockchain/DLT hinsichtlich signifikanter Eigenschaften geschäftsrelevanter Aufzeichnungen	14
Tabelle B.1 — Erfüllung Anforderungen an Records Management durch geeignete eIDAS-Werkzeuge	30

Vorwort

Dieses Dokument wurde vom Arbeitskreis NA 009-00-15-02 AK „Records Management“ des Arbeitsausschusses NA 009-00-15 AA „Records Management und Langzeitverfügbarkeit von Informationsobjekten“ im DIN-Normenausschuss Information und Dokumentation (NID) erarbeitet.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Technische Spezifikationen sind nicht Bestandteil des Deutschen Normenwerks.

Eine Technische Spezifikation ist das Ergebnis einer Normungsarbeit, das wegen bestimmter Vorbehalte zum Inhalt oder wegen des gegenüber einer Norm abweichenden Aufstellungsverfahrens von DIN noch nicht als Norm herausgegeben wird.

Erfahrungen mit dieser Technischen Spezifikation sind erbeten:

- vorzugsweise als Datei per E-Mail an nid@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter <http://www.din.de/stellungnahme> abgerufen werden;
- oder in Papierform an den Normenausschuss Information und Dokumentation (NID) im DIN Deutsches Institut für Normung e. V., 10772 Berlin (Hausanschrift: Burggrafenstraße 6, 10787 Berlin).

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Einleitung

Die Blockchain-Technologie mit ihrem prominentesten Vertreter Bitcoin erlebt seit einiger Zeit einen regelrechten Hype. Ihr wird in verschiedenen Branchen, so z. B. der Finanzindustrie, der Energiewirtschaft oder der öffentlichen Verwaltung, großes Potenzial zugeschrieben. Kerneigenschaften der Blockchain, wie Dezentralität, Diversifizierung der Daten und Knoten zwischen den Nutzern oder eine grundlegende Fälschungssicherheit und Zuverlässigkeit, ermöglichen potenzielle neue Geschäftsmodelle und bieten Chancen für eine effizientere Digitalisierung in Verwaltung und Wirtschaft.

Gleichzeitig unterliegen verschiedene Branchen wie z. B. die öffentliche Verwaltung, Luftfahrt, Energiewirtschaft, Pharmaindustrie, das Gesundheitswesen oder der Finanzsektor umfassenden regulatorischen Vorgaben zur Digitalisierung sowie zur Dokumentation und langfristigen Vorgaben, wie verlustfreien Nachweisen ihrer Prozesse und Aufzeichnungen gegenüber Gerichten, Prüfbehörden und anderen vertrauenswürdigen Dritten.

Im Records Management liegt ein etablierter Standardisierungsrahmen vor, anhand dessen die Rollen, Verantwortlichkeiten, Prozesse sowie fachlich-technischen Maßnahmen für die eingesetzten IT-Verfahren abgeleitet und so eine Dokumentation und Nachweis von Transaktionen anhand der geschäftsrelevanten Aufzeichnungen geführt und somit Vertrauenswürdigkeit der Transaktionen und Aufzeichnungen erreicht werden kann [1].

Diesem Stand der Technik muss auch eine Blockchain/DLT entsprechen sofern diese für vertrauenswürdige digitale Transaktionen genutzt werden soll [1] [2] [3].

Die konkreten fachlichen wie technischen Kriterien der DIN/TS 31648 ermöglichen es Anwendern, Projektleitern, Entscheidern bis hin zu Softwareentwicklern oder Produktanbietern zum einen die notwendigen Anforderungen an Blockchain/DLT für ihren Anwendungsfall zu definieren, zum anderen Blockchain/DLT hinsichtlich ihrer Nutzbarkeit für vertrauenswürdige digitale Transaktionen zu bewerten.

Ziel ist es die Konzeption, Beschaffung und Implementierung oder Integration von Blockchain/DLT auch in hochregulierten Branchen zu erleichtern und neue Geschäftsmodelle zu etablieren — bei gleichzeitiger Erfüllung geltender Dokumentations- und Nachweispflichten auf Basis eines ordnungsgemäßen Records Managements.

Basierend auf grundlegenden Anforderungen an vertrauenswürdige digitale Transaktionen sowie einer Darstellung zur Umsetzung eines ordnungsgemäßen Records Management in Blockchain/DLT gliedert sich die Technische Spezifikation 31648 in zwei Teile:

- Fachliche Kriterien;
- Technische Kriterien.

Die fachlichen Kriterien beschreiben anhand der an der ISO 15489-1:2016 angelehnten Gliederung organisatorisch-prozessuale Anforderungen zur Nutzung von Blockchain/DLT für vertrauenswürdige digitale Transaktionen — Records Management und Beweiswerterhaltung. Die technischen Kriterien untersetzen die Ausführungen hinsichtlich Informationssicherheit, Kryptostabilität und langfristige Nachweisfähigkeit bis hin zu Architektur- und Betriebsfragen.

1 Anwendungsbereich

Dieses Dokument legt fachliche und technische Kriterien zur Anwendung der Blockchain und Distributed Ledger Technologie (DLT) für vertrauenswürdige digitale Transaktionen sowie der notwendigen Berechtigungsmodelle aus Sicht der Nachweisfähigkeit (Records Management) und Beweiswerterhaltung fest.

Dieses Dokument gilt für alle digitalen Transaktionen, die gesetzlichen oder sonstigen Dokumentations-, Aufbewahrungs- und Nachweispflichten unterliegen, für die damit ein ordnungsgemäßes Records Management sowie Beweiswerterhaltung nach dem Stand der Technik erforderlich ist und die mit Blockchain/DLT abgebildet werden sollen.

Anwendungsbeispiele sind in Anhang A enthalten.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

BSI TR-02102, *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*

BSI TR-03125 TR-ESOR, *Beweiswerterhaltung kryptographisch signierter Dokumente*

BSI TR-03147, *Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen*

DIN 31644:2012-04, *Information und Dokumentation — Kriterien für vertrauenswürdige digitale Langzeitarchive*

DIN 31647:2015-05, *Information und Dokumentation — Beweiswerterhaltung kryptographisch signierter Dokumente*

DIN EN 62734:2015-07, *Industrielle Kommunikationsnetze — Drahtlose Kommunikationsnetze und Kommunikationsprofile — ISA 100.11a (IEC 62734:2014); Englische Fassung EN 62734:2015*

ETSI EN 319401, *Electronic Signatures and Infrastructures (ESI) — General Policy Requirements for Trust Service Providers, ETSI V2.2.1*

ETSI EN 319422, *Electronic Signatures and Infrastructures (ESI) Time-stamping protocol and electronic time-stamp token profiles*

ETSI TS 119312, *Electronic Signatures and Infrastructures (ESI) — Cryptographic Suites*

ETSI TS 119511:2019, *Electronic Signatures and Infrastructures (ESI) — Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques*

ETSI TS 119512, *Electronic Signatures and Infrastructures (ESI) — Protocols for trust service providers providing long-term data preservation services*

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

ISO 15489-1:2016, *Information and documentation — Records management — Part 1: Concepts and principles*

ISO 22739, *Blockchain and distributed ledger technologies — Vocabulary*

ISO 30300:2020, *Information and documentation — Records management — Core concepts and vocabulary*

ISO/IEC 25010, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*

SOG-IS Crypto Working Group: *SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.1 June 2018*,
<https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.1.pdf>

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO 30300:2020, nach DIN 31647, nach BSI TR-03125 und die folgenden Begriffe.

DIN und DKE stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— DIN-TERMinologieportal: verfügbar unter <https://www.din.de/go/din-term>

— DKE-IEV: verfügbar unter <http://www.dke.de/DKE-IEV>

3.1

Authentizität

Übereinstimmung mit den Ursprungsdaten (Echtheit der Dokumente) und deren eindeutige Zurechenbarkeit zu einem Aussteller (Verfasser, Ersteller und/oder Absender), im Sinne der Beweiswerterhaltung kryptographisch signierter Dokumente

[QUELLE: DIN 31647:2015-05, 3.5]

3.2

Bewahrungsdienst

bezeichnet einen Vertrauensdienst zur Bewahrung elektronischer Signaturen, Siegel und Zeitstempel

[QUELLE: eIDAS-VO, Art. 3 Nr. 16c]

3.3

Beweisdaten, technische

(en: evidence records)

Informationen zum Nachweis der Unversehrtheit der Integrität und Authentizität der Archiwpakete

[QUELLE: DIN 31647:2015-05, 3.6]

3.4

beweisrelevante Daten

alle Daten, die für eine Beweisführung notwendig und gegenüber den Inhaltsdaten sowie den Metadaten abgegrenzt sind, sowie die Sperrdaten für Signaturen, Zeitstempel und alte Beweisdaten

[QUELLE: DIN 31647:2015-05, 3.7]

3.5

Beweiswerterhaltung

Maßnahmen, die geeignet sind, den Beweiswert elektronischer Dokumente mindestens für die Dauer der vorgeschriebenen Aufbewahrungszeiträume sicherzustellen

[QUELLE: DIN 31647:2015-05, 3.9]

3.6

Blockchain

Distributed Ledger mit per Konsensmechanismus bestätigten Blöcken, die unter Verwendung kryptografischer Verknüpfungen in einer sequentiellen Kette angeordnet sind

[QUELLE: ISO 22739:2020, 3.6, modifiziert – ergänzt: per Konsensmechanismus]

3.7

Blockbeschreibung

SB, en: serialized block

beinhaltet den Blockheader sowie Verweise auf alle zugehörigen Transaktionen

3.8

Distributed Ledger Technology

DLT

Technologie, die den Betrieb und die Nutzung eines Distributed Ledgers ermöglicht, der von einer Gruppe von Netzwerkknoten gemeinsam genutzt und mittels eines Konsensmechanismus synchronisiert wird

[QUELLE: ISO 22739:2020, 3.23, modifiziert – Nebensatz ergänzt: , der von einer Gruppe von Netzwerkknoten gemeinsam genutzt und mittels eines Konsensmechanismus synchronisiert wird]

3.9

Hashwert

eindeutiger durch eine kryptographische Hashfunktion erzeugter „Fingerabdruck“ elektronischer Daten, der auch als Message Digest der Daten bezeichnet wird

[QUELLE: DIN 31647:2015-05, 3.17]

3.10

Hashfunktion

kryptographischer Algorithmus, bei dem (elektronische) Nachrichten beliebiger Länge auf einen Hashwert fester Länge abgebildet werden

[QUELLE: DIN 31647:2015-05, 3.18]

3.11

Hashbaum

(en: Hashtree)

Verfahren, in dem gleichzeitig mehrere Hashwerte mit Hilfe einer Baumstruktur durch eine einzige, an der Wurzel dieses Baums getätigte Signatur signiert werden

[QUELLE: DIN 31647:2015-05, 3.19]

3.12

Identität, digitale

kennzeichnende Eigenschaft oder Persönlichkeit einer Person oder Instanz

[QUELLE: DIN EN 62734:2015-07, 3.1.2.58]

3.13

Identifizierungsmittel, elektronisches

ist eine materielle und/oder immaterielle Einheit, die Personenidentifizierungsdaten enthält und zur Authentifizierung bei Online-Diensten verwendet wird

[QUELLE: eIDAS-VO Art. 3 Nr. 2]

3.14**Integrität**

elektronische Daten sind integer, wenn sie vollständig sind und nachweislich keine Veränderungen oder Manipulationen an den Daten festgestellt werden können

[QUELLE: BSI TR-03125 v1.2.2]

3.15**Interoperabilität**

Interoperabilität bezeichnet im weiteren Sinne die Fähigkeit verschiedener Geräte- oder Softwarekomponenten, direkt miteinander kommunizieren, d. h. insbesondere Daten austauschen zu können. Im engeren Sinne ist Interoperabilität die Fähigkeit von IT-Systemen, direkt mit anderen Systemen zu kommunizieren, wenn sie über ein Netz verbunden sind

[QUELLE: BSI TR-03125 v1.2.2]

3.16**Leistungseffizienz**

eines Computersystems ist die Fähigkeit vorgegebene Leistungsanforderungen, die in der Regel in Service-Level-Vereinbarungen festgeschrieben werden, bereitzustellen

[QUELLE: DIN 66273-2]

3.17**off-chain**

mit Bezug zu einer Blockchain/DLT, aber außerhalb der Blockchain befindlich oder ausgeführt. Beschreibt den eigentlichen Ort der Datenhaltung

[QUELLE: ISO 22739:2020, 3.52, modifiziert – ergänzt: Beschreibt den eigentlichen Ort der Datenhaltung.]

3.18**on-chain**

auf einer Blockchain/DLT befindlich oder ausgeführt. Beschreibt den eigentlichen Ort der Datenhaltung

[QUELLE: ISO 22739:2020, 3.54, modifiziert – ergänzt: Beschreibt den eigentlichen Ort der Datenhaltung.]

3.19**permissioned DLT**

Blockchain/DLT, in der Berechtigungen erforderlich sind, um eine bestimmte Aktivität oder Aktivitäten durchzuführen

[QUELLE: ISO 22739:2020, 3.58, modifiziert – ergänzt: , um eine bestimmte Aktivität oder Aktivitäten durchzuführen]

3.20**permissionless DLT**

Blockchain/DLT, in der keine Berechtigungen erforderlich sind, um eine bestimmte Aktivität durchzuführen

[QUELLE: ISO 22739:2020, 3.60, modifiziert – ergänzt: um eine bestimmte Aktivität oder Aktivitäten durchzuführen]

3.21**private DLT**

Blockchain/DLT, die nur für eine begrenzte Gruppe an Nutzern zugänglich ist

[QUELLE: ISO 22739:2020, 3.61]

3.22

proof of existence

bezeichnet den Nachweis der Existenz von Daten in integrem wie authentischen Zustand zu einem bestimmten Zeitpunkt

[QUELLE: BSI TR-03125 v1.2.2]

3.23

public DLT

Blockchain/DLT, die öffentlich zugänglich ist

[QUELLE: ISO 22739:2020, 3.64]

3.24

rehashing

bezeichnet die Neuverhashung aller nicht mehr sicherheitsgeeigneten technischen Beweisdaten und sonstigen mit dem Hashbaum gesicherten Daten mit einem neuen sicherheitsgeeignetem Hashalgorithmus, bevor die Sicherheitseignung des bestehenden Hashalgorithmus abläuft

Anmerkung 1 zum Begriff: Anzuwenden ist hier das RFC 4998 (Hashtree-renewal) oder ein gleichwertiger Evidence Record Syntax-Standard

3.25

resigning

Anbringung einer neuen elektronischen Signatur/Siegel/Zeitstempel vor Ende der Sicherheitseignung der ihr zugrundeliegenden Algorithmen und Parameter, um den Beweiswert kryptographisch signierter Dokumente zu erhalten

[QUELLE: DIN 31647:2015-05, 3.30]

3.26

Siegel, elektronisches

sind Daten in elektronischer Form, die anderen Daten in elektronischer Form beigelegt oder logisch mit ihnen verbunden werden, um deren Ursprung und Unversehrtheit sicherzustellen

[QUELLE: eIDAS-VO Art. 3 NR. 25]

3.27

Signatur, elektronische

sind Daten in elektronischer Form, die anderen elektronischen Daten beigelegt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet

[QUELLE: eIDAS-VO Art. 3 NR. 10]

3.28

Skalierbarkeit

beschreibt die Fähigkeit, die Menge der eingesetzten Ressourcen zu verändern bzw. dem Bedarf der Anwendung anzupassen

3.29

Transaktion

bezeichnet die kleinste Einheit einer Aktivität, bestehend auf dem Austausch von Informationen und Interaktion zwischen zwei oder mehr Teilnehmern oder Systemen

[QUELLE: ISO 30300:2020, 3.1.29]