DIN/TS 31648:2021-04 (D)

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

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 16

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 19
7.1.7 Monitoring und Evaluation 19
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 20
7.2.3 Identifizierung 20
7.2.4 Rechtemanagement 20
7.2.5 Rechtevergabe 20
7.2.6 Zugangskontrolle 21
7.2.7 Datenschutz und Vertraulichkeit 21
7.2.8 Digitale Langzeitspeicherung 22
7.2.9 Aussonderung und Löschung 22

8 Technische Kriterien für den Einsatz von Blockchain/DLT im Records Management 23
8.1 Informationssicherheit 23
8.1.1 Konsensmechanismus 23
8.1.2 Kryptografische Verfahren 23
8.1.3 Virtuell-Real-Schnittstelle 23
8.1.4 Weitere Angriffsszenarien 24
8.1.5 Allgemeine IT-Sicherheit 24
8.1.6 Zeitstempelerneuerung und Hashbaumerneuerung 24
8.1.7 Sicherstellung Proof of Existence 25
8.2 Interoperabilität 26
8.3 Leistung 26
8.4 Skalierbarkeit 26
8.5 Übertragbarkeit 27

8.6 Wartbarkeit ... 28
8.7 Zuverlässigkeit ... 28
8.7.1 Ausfallsicherheit/Fehlertoleranz ... 28
8.7.2 Shared secrets/Stimmrechte ... 28
8.7.3 Verteilung zur Datensicherheit ... 29
8.7.4 Verteilung zur Ausfallsicherheit ... 29

Anhang A (informativ) Anwendungsbeispiele ... 30

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

Literaturhinweise ... 32

Bilder

Bild 1 — Problematik fehlenden Rehashings und Proof of Existence in Blockchain/DLT ... 17

Bild 2 — Beweiswerterhaltung und langfristige Integritätssicherung in Blockchain/DLT ... 25

Bild 3 — Beschränkungen von verteilten Systemen: „wähle 2 von 3 Eigenschaften“ ... 27

Tabellen

Tabelle 1 — Bewertung Blockchain/DLT hinsichtlich signifikanter Eigenschaften geschäftsrelevanter Aufzeichnungen ... 14

Tabelle B.1 — Erfüllung Anforderungen an Records Management durch geeignete eIDAS-Werkzeuge ... 31