

ISO/TR 24332:2025-01 (E)

Information and documentation - Blockchain and distributed ledger technology (DLT) in relation to authoritative records, records systems and records management

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Overview of records management and distributed ledger technology (DLT)	1
4.1	General	1
4.2	Overview of records management concepts and principles	2
4.2.1	Concepts	2
4.2.2	Principles for managing records	2
4.3	Overview of distributed ledger technology (DLT) and blockchain	3
4.3.1	General	3
4.3.2	Overview of the distributed ledger technology (DLT) reference architecture	3
4.3.3	Different types of distributed ledger technology (DLT) systems	4
4.3.4	Distributed ledger technology (DLT) use cases	5
5	Distributed ledger technology (DLT) and authoritative records	5
5.1	General	5
5.2	On-ledger records	6
5.3	Off-ledger records	6
5.4	Metadata for records	6
5.5	Relationship between distributed ledger technology (DLT) and characteristics of authoritative records	7
5.5.1	General	7
5.5.2	Authenticity	7
5.5.3	Reliability	8
5.5.4	Integrity	8
5.5.5	Useability	9
6	Distributed ledger technology (DLT) and records processes	9
6.1	Creating records	9
6.2	Capturing records	9
6.3	Records classification	9
6.4	Access control	10
6.5	Storing records	10
6.6	Use and reuse	11
6.7	Migrating and converting records	12
6.8	Disposition	12
7	Relationship between distributed ledger technology (DLT) systems and records systems	13
7.1	Characteristics of records systems	13
7.2	Design considerations for records systems	14
8	Distributed ledger technology (DLT) systems and records management	15
8.1	Policies and responsibilities	15

8.2	Records controls	15
8.2.1	General	15
8.2.2	Metadata schemas	15
8.2.3	Business classification schemes	16
8.2.4	Access and permissions rules	17
8.2.5	Disposition authorities	17
9	Challenges, considerations and potential benefits	17
9.1	Distributed ledger technology (DLT) and management of retention and disposition of records	17
9.2	Legal issues	18
9.2.1	General	18
9.2.2	eDiscovery	19
9.2.3	Custody and ownership	19
9.2.4	Geolocation restrictions on data storage and transfer	20
9.2.5	Jurisdictional restrictions on the operation of distributed ledger technology (DLTs)	20
9.3	Personally identifiable information (PII) protection	20
9.4	Access control mechanisms	22
9.4.1	General	22
9.4.2	Read access	23
9.4.3	Write access	23
9.5	Identification, authentication, and authoritative records	24
9.6	Addressing the business need to modify records	24
9.7	Distributed ledger technology (DLT) and records destruction	24
9.8	Longevity of distributed ledger technology (DLT) systems	25
9.8.1	General	25
9.8.2	Longevity of cryptographic algorithms	26
9.8.3	Long-term preservation of authoritative records	26
9.9	Timestamping and ordering in DLT	27
9.10	Key management	27
9.11	Distributed ledger technology (DLT) security	28
9.11.1	General	28
9.11.2	Malicious participants	28
9.11.3	Consensus hijacking	28
9.11.4	Vulnerability of distributed ledger technology (DLT) software	29
9.11.5	Vulnerability of smart contracts related to external data	29
9.12	Smart contracts	29
9.13	Auditing, monitoring and evaluation	30
9.14	Tokenization	31
	Bibliography	33