TECHNICAL SPECIFICATION

ISO/TS 23258

First edition
2021-11

Blockchain and distributed ledger technologies — Taxonomy and Ontology

Technologies des chaînes de blocs et technologies de registre distribué — Taxinomie et ontologie

Reference number
ISO/TS 23258:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 307, *Blockchain and distributed ledger technologies*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

A taxonomy is useful for defining information and data classification rules and for identifying classification items and classification criteria. An ontology aims at clearly showing the concepts that make up the conceptual basis and the vocabulary of the technology under consideration and at creating a foundation that is a prerequisite for understanding the concepts through the definition of their mutual relations (synonyms, inclusions, dependencies, etc.).

A consistent taxonomy is a valuable resource in its own right that also supports and helps to understand other relevant standards.

This document includes a taxonomy of concepts, a taxonomy of DLT systems, and a taxonomy of application domains, purposes and economic activity sections for use cases. This document includes an ontology providing classes and attributes as well as relations between concepts.

Figure 1 shows the relationships between this document and other standards developed by ISO/TC 307.

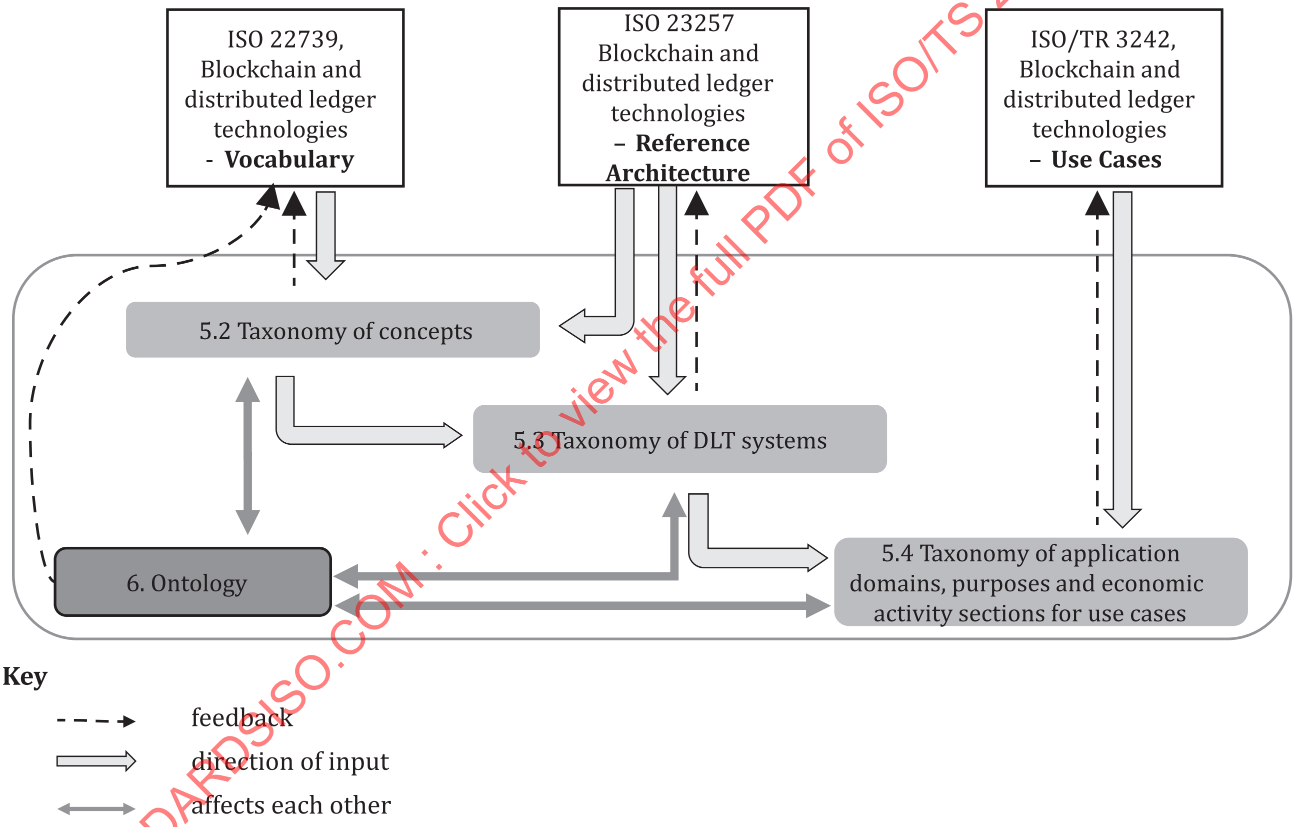
ISO 22739, Blockchain and distributed ledger technologies - **Vocabulary**
ISO 23257 Blockchain and distributed ledger technologies – **Reference Architecture**
ISO/TR 3242, Blockchain and distributed ledger technologies – **Use Cases**
5.2 Taxonomy of concepts
5.3 Taxonomy of DLT systems
5.4 Taxonomy of application domains, purposes and economic activity sections for use cases
6. Ontology
Key
feedback
direction of input
affects each other

Figure 1 — Relationships between this document and other standards developed by ISO/TC 307

Blockchain and distributed ledger technologies — Taxonomy and Ontology

1 Scope

This document specifies a taxonomy and an ontology for blockchain and distributed ledger technologies (DLT). The taxonomy includes a taxonomy of concepts, a taxonomy of DLT systems and a taxonomy of application domains, purposes and economy activity sections for use cases. The ontology includes classes and attributes as well as relations between concepts.

The audience includes but is not limited to academics, architects, customers, users, tool developers, regulators, auditors and standards development organizations.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22739 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
taxonomy
scheme of categories and subcategories that can be used to sort and otherwise organize itemized knowledge or information

[SOURCE: ISO 5127:2017, 3.8.6.07]

4 Abbreviated terms

DLT	Distributed Ledger Technology
PoW	Proof-of-Work
PoS	Proof-of-Stake
DPoS	Delegated Proof-of-Stake
BFT	Byzantine Fault Tolerance
PBFT	Practical Byzantine Fault Tolerance
TPS	Transaction Per Second

CA	Certificate Authority
IPFS	InterPlanetary File System
UML	Unified Modeling Language

5 Taxonomy

5.1 Introduction

To better understand DLT systems, it is necessary to classify them into different categories based on their similarities on different aspects. Such classification is also known as the taxonomy of DLT systems. To be able to thoroughly classify and correlate DLT systems, it is imperative to investigate and understand the existing blockchain and distributed ledger technologies as well as the relationships among the DLT system options. This taxonomy helps the potential blockchain users and other stakeholders to compare and choose the right options according to their business needs and applicable legal and regulatory requirements. Furthermore, the ability to classify DLT systems can help with knowledge advancement and can lead to a significant breakthrough in understanding and utilization of DLT systems. Furthermore, the taxonomy informs the scientific research and could support wider understanding and adoption of blockchain and distributed ledger technologies and systems.

5.2 Taxonomy of concepts

Table 1 is based on and refers to the terms and definitions in ISO 22739:2020, ISO 23257:—[1)] and completed with some of the concepts used in Reference [1]. It organizes the concepts into 6-level hierarchical structure with only one entry per concept. Short forms of concepts are given in square brackets and references are provided in parentheses, e.g. "[DLT user (ISO 22739:2020, 3.28)]."

Table 1 — Taxonomy of concepts

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
Asset (ISO 22739:2020, 3.1)	**Digital Asset** (ISO 22739:2020, 3.20)	Cryptographic Asset (**Crypto-asset** [c]) (ISO 22739:2020, 3.13)	**Cryptocurrency** (ISO 22739:2020, 3.14)		
			Token (ISO 22739:2020, 3.76)	(Token) Fungibility (**Fungible** (ISO 23257:—, 3.12)	Fungible Token
					Non-Fungible Token [NFT]
				Token Metadata	Digital Asset Description
					Privilege Description
					Value Description
	(Asset) **Provenance** (ISO 23257:—, 3.11)	Origin of Asset			
		History of Asset			
		History of Custody			

1) Under preparation. Stage at the time of publication: ISO/FDIS 23257:2021.

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
Consensus (ISO 22739:2020, 3.11)	**Consensus Mechanism** (ISO 22739:2020, 3.12)	Fault Tolerance	Byzantine Fault Tolerance [BFT]	Practical Byzantine Fault Tolerance [PBFT]	
			Crash Fault Tolerance		
		Nakamoto Consensus	Proof of Stake [PoS]	Delegated Proof of Stake [DPoS]	
			Proof of Work [PoW]		
	Consensus Security				
Smart Contract (ISO 22739:2020, 3.72)	Legally Binding Smart Contract				
Entity (ISO 22739:2020, 3.34)	Legal Entity	Group [a]			
		Organization	Autonomous Organization	Decentralized Autonomous Organization [DAO]	
	Person	Operator	Distributed Ledger Technology Operator [DLT Operator]		
		User	**Distributed Ledger Technology User** (ISO 22739:2020, 3.31) [**DLT User** (ISO 22739:2020, 3.31)]		
	Process	Action	Confirmation	Block Confirmation	
				Transaction Confirmation	
			Compliance		
			Deletion (**Delete** ISO 23257:—, 3.2)	Transaction Deletion	
			Execution	Execution of Contract	Stateful Execution of Contract
					Stateless Execution of Contract
			Validation (ISO 22739:2020, 3.82)	Block Validation	
				Ledger Record Validation	
				Transaction Validation	

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
		Activity	Archiving (**Archive** ISO 23257:—, 3.3)	**Data Archiving** (ISO 23257:—, 3.4)	
				Resource Archiving	
				Transaction Archiving	
			Hashing		
			Mining (ISO 22739:2020, 3.49)		
			Restoring (**Restore** ISO 23257:—, 3.6)	Data Restoring	
				Resource Restoring	
				Transaction Restoring	
		Event	**Disruption** (ISO 23257:—, 3.10)	Attack	
				Incident (ISO 23257:—, 3.8)	
			Error	Error analytics	
			Failure (ISO 22739:2020, 3.35)		
			Fault	**Fault Tolerance** (ISO 22739:2020, 3.36)	
			Fork (ISO 22739:2020, 3.45)	**Hard Fork** (ISO 22739:2020, 3.38)	
				Soft Fork (ISO 22739:2020, 3.73)	
		Work Process	**Backup** (ISO 23257:—, 3.5)	Data Backup	
				Resource Backup	
				Transaction Backup	
			Transaction (ISO 22739:2020, 3.77)		
	Thing	Object	Device		

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
			Node (ISO 22739:2020, 3.50)	Child Node	
				Distributed Ledger Technology Node [**DLT Node** (ISO 22739:2020, 3.27)] [b]	**Miner** (ISO 22739:2020, 3.48)
					Participant
					Validator (ISO 22739:2020, 3.83)
				Leaf Node (ISO 22739:2020, 3.42)	
				Non-Leaf Node	
				Parent Node	
				Peer	
				Root Node (ISO 22739:2020, 3.69)	(Node) **Merkle Root** (ISO 22739:2020, 3.46)
			Platform	**Distributed Ledger Technology Platform** [**DLT Platform** (ISO 22739:2020, 3.29)]	
Governance	Control	Decentralized Control			
	Governance Rule				
	Incentive	**Incentive Mechanism** (ISO 22739:2020, 3.68)	**Reward System** (ISO 22739:2020, 3.68)	**Block Reward** (ISO 22739:2020, 3.5)	
Interoperability (ISO 22739:2020, 3.41)	Transport Interoperability				
	Syntactic Interoperability				
	Semantic Interoperability				
	Behavioral Interoperability				
	Policy Interoperability				

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
Ledger (ISO 22739:2020, 3.43)	**Distributed Ledger** (ISO 22739:2020, 3.22)	**Blockchain** (ISO 22739:2020, 3.6)			
		Distributed Ledger Control	Distributed Ledger Control Architecture		
		Distributed Ledger Privilege			
		Distributed Ledger Pruning (**Prune** (ISO 22739:2020, 3.63)			
		Distributed Ledger Storage	Distributed Ledger Storage Architecture		
		Shared Ledger (ISO 22739:2020, 3.70)			
	Ledger Implementation	**Block** (ISO 22739:2020, 3.2)	**Block Data** (ISO 22739:2020, 3.3)		
			Block Header (ISO 22739:2020, 3.4)	(Block) **Hash Value** (ISO 22739:2020, 3.39)	
				(Block) Merkle Root	
				(Block) **Nonce** (ISO 22739:2020, 3.51)	
				Block Number (or Block Height)	**Genesis Block** (ISO 22739:2020, 3.37)
					Previous Block
				(Block) **Timestamp** (ISO 22739:2020, 3.75)	
			Block Status	**Confirmed** (ISO 22739:2020, 3.8) **Block** (ISO 22739:2020, 3.9)	
				Validated (ISO 22739:2020, 3.81) Block	

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
Permission	Ledger Status	Inconsistent Ledger	**Double Spending** (ISO 22739:2020, 3.33)		
		Ledger Split (ISO 22739:2020, 3.45)			
	Ledger Tamper Resistance	Tamper-Resistant			
	Traditional Ledger				
	Hybrid Permission				
	Permissioned (ISO 22739:2020, 3.57)	Permissioned Distributed Ledger	Permissioned Blockchain	Permissioned Private Blockchain	
				Permissioned Public Blockchain	
		Permissioned DLT System (ISO 22739:2020, 3.58)	Permissioned Blockchain System		
	Permissionless (ISO 22739:2020, 3.59)	Permissionless Distributed Ledger	Permissionless Blockchain	Permissionless Private Blockchain	
				Permissionless Public Blockchain	
		Permissionless DLT System (ISO 22739:2020, 3.60)	Permissionless Blockchain System		

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
Record (ISO 22739:2020, 3.67)	**Ledger Record** (ISO 22739:2020, 3.44)	(Ledger Record) **Immutability** (ISO 22739:2020, 3.40)	Immutable		
		Ledger Record Status	**Validated** (ISO 22739:2020, 3.81) Ledger Record		
		Transaction Record (ISO 22739:2020, 3.79)	**Transaction Fee** (ISO 22739:2020, 3.78)		
			(Transaction) **Hash Value** (ISO 22739:2020, 3.39)		
			(Transaction) **Nonce** (ISO 22739:2020, 3.51)		
			(Transaction) **Timestamp** (ISO 22739:2020, 3.75)		
		Transaction Status	**Confirmed** (ISO 22739:2020, 3.8) **Transaction** (ISO 22739:2020, 3.10)		
			Validated (ISO 22739:2020, 3.81) Transaction		

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
Security	Authentication	User Authentication	Password		
	Authorization	User Authorizations			
	Cryptography (ISO 22739:2020, 3.17)	Asymmetric Cryptography	**Public Key Cryptography** (ISO 22739:2020, 3.66)		
		Cryptographic Technique	**Cryptographic Hash Function** (ISO 22739:2020, 3.15)	**Hash Value** (ISO 22739:2020, 3.39)	
			Cryptographic Link (ISO 22739:2020, 3.16)		
			Cryptographic Tree	Tree Data Structure	**Merkle Tree** (ISO 22739:2020, 3.47)
				Digital Signature (ISO 22739:2020, 3.21)	
				Encryption Key	**Private Key** (ISO 22739:2020, 3.62)
					Public Key (ISO 22739:2020, 3.65)
	Decryption				
	Encryption				
	Identifiable Information	**Personally Identifiable Information** [PII (ISO 23257:—, 3.1)]			
	Identity Management	Identity	Self-Sovereign Identity [SSID]		
	Integrity Check	Integrity			
	Privacy Management				

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
Service	Application	**Decentralized Application** [**DApp** (ISO 22739:2020, 3.18)]			
		Wallet (ISO 22739:2020, 3.84)	Account	**Distributed Ledger Technology Account** [**DLT Account** (ISO 22739:2020, 3.24)]	
			Address	**Distributed Ledger Technology Address** [**DLT Address** (ISO 22739:2020, 3.25)]	
			Hardware Wallet		
			Software Wallet		
	Cloud Service	Blockchain as a Service [BaaS]			
	Oracle	**Distributed Ledger Technology Oracle** [**DLT Oracle** (ISO 22739:2020, 3.28)]			
System	**Decentralized System** (ISO 22739:2020, 3.19)				

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
	Distributed System (ISO 22739:2020, 3.32)	**Distributed Ledger System** [**DLT System** (ISO 22739:2020, 3.30)]	**Blockchain System** (ISO 22739:2020, 3.7)	**Off-Chain** (ISO 22739:2020, 3.52)	
				On-Chain (ISO 22739:2020, 3.54)	
				Sidechain (ISO 22739:2020, 3.71)	Associated Blockchain System
					Main chain
				Subchain (ISO 22739:2020, 3.74)	
			Off-Ledger (ISO 22739:2020, 3.53)		
			On-Ledger (ISO 22739:2020, 3.55)		
			Private Distributed Ledger (Technology) System [**Private DLT System** (ISO 22739:2020, 3.61)]		
			Public Distributed Ledger (Technology) System [**Public DLT System** (ISO 22739:2020, 3.64)]		
	Ecosystem	Token Ecosystem			
	Subsystem	Network	**Distributed Ledger Technology Network** [**DLT Network** (ISO 22739:2020, 3.26)]		
			Peer-To-Peer (ISO 22739:2020, 3.56) Network		
	(System) **Resilience** (ISO 23257:—, 3.7)				

Table 1 *(continued)*

Level 1 concepts	Level 2 concepts	Level 3 concepts	Level 4 concepts	Level 5 concepts	Level 6 concepts
Technology	**Information and Communication Technology** [**ICT** (ISO 23257:—, 3.9)]				
	Ledger Technology	**Distributed Ledger Technology** [**DLT** (ISO 22739:2020, 3.23)]	Blockchain Technology		
Trust (ISO 22739:2020, 3.80)	Product Confidence				
	Service Confidence				

[a] Group can be a group of items including legal entity, person, process, thing according to ISO 22739:2020, 3.34.

[b] DLT Node may be below Device or Process and was set below Object to avoid duplicate.

[c] Non-cryptographic assets are not covered e.g. when token is considered as a subclass of cryptographic asset (or crypto-asset), token refers to cryptographic token (or crypto-token).

5.3 Taxonomy of DLT systems

5.3.1 General

The taxonomy of DLT systems is based on several key aspects including whether it is permissioned or permissionless, the type of consensus mechanism and the existence of incentive mechanisms. Such a classification helps the companies and organizations to understand and differentiate DLT systems.

5.3.2 Major characteristics of DLT systems

5.3.2.1 General

To provide classification for DLT systems, it is required to analyse them into various categories based on their similarities on different aspect through main characteristics. See Annex A for an example for classification of DLT system based on the taxonomy of DLT systems.

5.3.2.2 Purpose of DLT system

DLT systems (including blockchain systems) are designed to implement tamper-resistant distributed ledgers, using consensus for maintaining a ledger in a distributed network of DLT nodes. Incentives in DLT systems can drive the achievement of consensus among decision makers, the resolution of conflicts and the taking of decisions regarding the ongoing governance, design and operation of systems.

Business purpose of DLT systems defines the essential concepts associated with these systems. For example, Bitcoin system is to allow people to store and transfer value securely and anonymously. Therefore, the purpose of the Bitcoin system can be described as a payment.

5.3.2.3 Ledger design

Blockchain is one of the most popular ledger designs in the industry. However another systems might apply a different type of ledger design like DAG (Directed Acyclic Graph) to commit their specific requirements, for example, Internet of Things. In addition, new ledger designs might be continuously inspired by developers of DLT system in the future.

Blockchain is a distributed ledger with confirmed blocks organized in an append-only, sequential chain using cryptographic links. This distributed ledger forms a linear chain of blocks of transactions in an unalterable, chronological order. Transactions are bundled into blocks of transactions to be validated. Validated blocks are added to a chain of previously validated blocks.

By comparison, a DAG is a network of individual transactions linked to multiple other transactions. There are no blocks of transactions in DAG networks. If blockchain is a linked list, a DAG is a tree, branching out from one transaction to another, to another and so on.

Blockchain offers transparency and immutability. It is also relatively well established, being the basis of cryptocurrencies like Bitcoin and of distributed application (Dapp) platforms like Ethereum. Blockchain offers solid guarantees and cost-effectiveness for transactions of medium to high value.

By scaling very efficiently and avoiding or reducing user fees, DAGs are well suited to high volumes of transactions, including micro and nano-transactions. The higher the volume of transactions, the faster a DAG validates them. DAGs also cut out the need for miners and in turn mining equipment — meaning lower energy consumption.

5.3.2.4 DLT system permission

5.3.2.4.1 General

According to whether it is requiring permissions to use or operate the system, the types of DLT systems can be classified as permissionless and permissioned DLT systems.

A permissionless DLT system doesn't require any permission in order to use the system as a DLT user or to participate in operation of the system as a DLT node. By contrast a permissioned DLT system does require some permissions in order to perform a particular activity or activities.

5.3.2.4.2 Permissioned DLT system

In a permissioned DLT system, permissions are required for some capabilities to use the system or permissions are required for some capabilities to operate the system. Therefore, any participant who wants to use the system or join to run the DLT network needs to request and get an approval from the host of the system before they access and use the permissioned DLT system.

In the aspect of operating the system, all DLT nodes of permissioned DLT system are authorized to join the network and participate in the consensus process to build the blockchain or distributed ledger. In such system, there might be a central authority which determines and controls the permission for a DLT node to join the network as well as restricts the DLT nodes on which can participate in the consensus process to validate block transactions and propose blocks.

In the aspect of DLT user, permissioned DLT system can restrict access for DLT users who use services provided by DLT system. In such system, all the users should have a permission to use the DLT system. A permissioned blockchain only allows users who have permissions to read block information and to create smart contracts interacted with the ledger.

5.3.2.4.3 Permissionless DLT system

Permissionless DLT system allow any entity to participate in the system, and there is no authentication or authorization required to access and use the system. Therefore, any participant in the permissionless DLT system is anonymous and there is no way to restrict anyone in such system.

In permissionless DLT system, anyone can download the blockchain base-code and run the base-code on local device which acts as a DLT node to join this DLT system without requiring authentication or providing CA certification. In addition, the nodes are free to validate transactions in the network and also participate in the consensus process that determines which and what block or transactions should be added to the blockchain and on the finalized or canonical chain. It is free to leave the DLT system at any time.

In user perspective for permissionless DLT system, DLT users can read any transaction or any block which were already included in the blockchain because transactions and blocks are transparent and anonymous in the permissionless DLT system.

In terms of building application on top of permissionless DLT systems, it is also open and permissionless for all the users to create smart contracts and use them in a permissionless DLT system.

5.3.2.5 DLT User access

According to whether who can read transaction records on the ledger in user access aspect, the types of DLT systems can be classified by public and private DLT systems.

A public DLT system has transaction records that are readable by anyone (i.e. by the general public). By contrast a private DLT system has transaction records that are readable by not just anyone - read access to the transaction records is deliberately limited - the records are private to the extent that read access is limited to some particular group (see ISO 23257:—, Clause 8)

5.3.2.6 Consensus mechanism

Many different consensus mechanisms can be used to achieve consensus about the inclusion and ordering of transactions and new mechanisms can be developed to overcome the limited performance or functions on current DLT systems. Most popular consensus mechanisms are Proof-of-Work (PoW), Proof-of-Stake (PoS, DPoS) and Byzantine Agreement Methods (PBFT, BFT, Paxos).

1) Proof-of-Work (PoW)

PoW could be simply considered as a proof for the certain amount of work that has been done by resolving a very difficult cryptographic puzzle. One of the core features of this scheme is asymmetry. The process of proving the amount of work is usually extremely inefficient and difficult, but it is very efficient and easy to verify the completion of corresponding workload by verifying the results of Proof-of-Work.

In PoW-based DLT system, any node (miner) needs to solve a difficult cryptographic puzzle to produce a hash value nonce that is smaller than the current difficulty target in order to collect transactions and/or propose a block which will be potentially included in the canonical blockchain. The probability of mining a new block depends on the instantaneous computational power devoted to the task.[2] As a reward for mining a block, the node (miner) will receive a certain amount of cryptocurrency and transaction fees.

In PoW-based DLT system, Proof-of-Work consensus involves three essential key elements, including workload proof function, block and difficulty. The workload proof function is the cryptographic function to calculate the hash value nonce to meet the criteria for a new block. This function takes any length of value as input and output with a fixed length hash value. The block determines the input value for the cryptographic function. A block consists of a block header and a block body which contains a list of transactions. Block header is the input value of Proof-of-Work cryptographic function. Then there is the difficulty, which is an essential parameter of the mining process. It determines the amount of work which is needed for the PoW blockchain to produce a valid block. The difficulty value changes according to the computation power of the entire network, so as to ensure a more constant block time.

2) Proof-of-Stake (PoS)

In PoS-based DLT system, DLT nodes need to provide certain amount of native cryptocurrency as their stake to be able to participate in consensus algorithm. By providing stake in the network, the PoS blockchain gains benefits from different approaches. Such as, the nodes acquire legitimate right to participate in consensus algorithm to validate transactions and propose block. The amount of stake which nodes provided in the system determines the probability of acceptance of its proposed blocks.

Since DLT nodes provides their stakes in the system, they can face the risk of losing their stakes as punishment for not participating or act abnormally in the consensus algorithm.

3) Byzantine Fault Tolerance (BFT)

In DLT system, there may be some nodes that behave abnormally which causes Byzantine Fault to the system. BFT-based consensus algorithm is designed and implemented to solve the Byzantine fault problem, and it ensures the DLT system to function normally even with abnormal nodes involved in the network.

In BFT-based DLT system, all nodes in the network need to participate in the consensus process which performs multiple rounds of voting and communication to reach consensus on a block and the blockchain. So, it is more compatible with small systems with limited nodes. Meanwhile, since BFT requires that all participants agree on the list of participants in the network, the protocol is normally only used in permissioned blockchains.[3] For permissioned blockchains, BFT-based consensus algorithm is deterministic and it is a more conventional approach, compared with the PoW consensus mechanism in permissionless blockchains. So, the BFT-based DLT system can offer better consistency and lower latency.

4) Delegated Proof-of-Stake (DPoS)

DPoS leverages the power of stakeholder’s approval used to resolve consensus issues in a fair and democratic way. In a Delegated PoS-based DLT system, the nodes, which own certain amount of native cryptocurrency as stake, has the ability to vote for delegates.

All the delegates act as a delegation in the system to validate transactions, produce blocks, and maintain the blockchain. As reward for their contribution in the consensus mechanisms, delegates will collect the block rewards and transaction fees. Accordingly, the delegates will be punished or voted out if they act abnormally, such as not producing blocks or signs two blocks with the same timestamp or the same block height.

5) Direct Acyclic Graph (DAG) Consensus

DAG-based DLT system can serve as a feasible alternative to blockchain technology to implement DLT system.

In a blockchain, transactions are collected and validated by the mining node, and then grouped into a block that can potentially be appended to the blockchain. However, DAG-based DLT system works differently than the blockchain because there are no miners, no blocks in a DAG-based DLT system. All the transactions in a DAG-based distributed system are linked from one to another which means the DLT nodes or DLT users confirm each other’s transactions by validating and confirming its previous transactions with a new transaction.

In DAG-based DLT system, to issue a new transaction and reach an agreement for the consensus among nodes, the main procedures are listed as follows. (i) A node creates a storage unit to store the new transaction. (ii) The node selects two previous transactions with no-conflict according to transaction selection algorithm, and adds the hash of the selected transactions into its storage unit. (iii) The node finds a nonce to solve a cryptographic puzzle to meet the difficulty target, which is similar to PoW but with a very low difficulty-of-work for avoiding spamming. (iv) The node uses its private key to sign the new transaction and broadcasts it to others. (v) When the other nodes receive it, they check whether it is legal or not based on the digital signature and nonce.

Comparing with blockchain, the DAG-based DLT system gains the advantage of scalability, meaning more transactions were received by the system, the faster the available transactions will be confirmed which means short confirmation time and higher TPS. DAG is depicted in Figure 2.

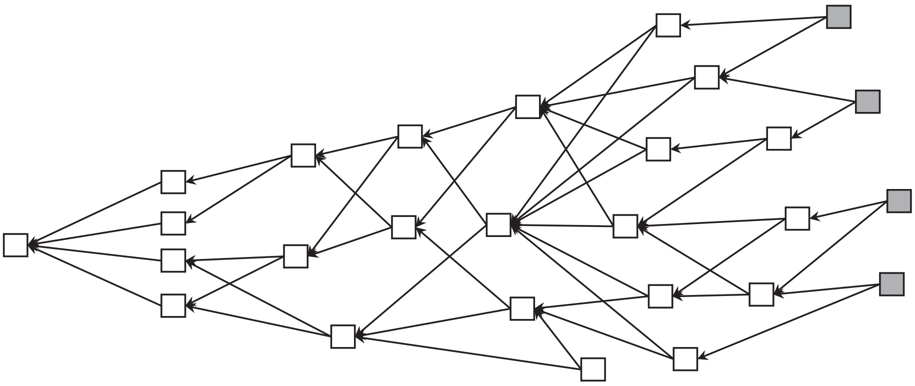

Figure 2 — Direct Acyclic Graph (DAG)

5.3.2.7 Smart contract

Not all DLT systems support a smart contract function. Smart contracts are usually written in high-level computer programming languages in order to represent business logic or pre-determined criteria to trigger transfer of values. They are stored on the ledger on the DLT system and may have variables to store data and functions which access, process, and write data.

In the execution perspective, in some systems, smart contracts may be executed on every node, and in others they may be executed on only some limited set of pre-specified nodes.

5.3.2.8 Crypto-asset and cryptocurrency

Many crypto-assets including cryptocurrencies rely on decentralized networks based on Distributed Ledger Technology—a distributed ledger enforced by a disparate network of computers. This decentralized structure allows them to exist outside the control of governments and central authorities.

The first blockchain-based cryptocurrency was Bitcoin, which still remains the most popular one, and there are thousands of alternate cryptocurrencies with various functions and specifications.

5.3.2.9 Reward system

5.3.2.9.1 General

In the DLT design process, the rewarding mechanism plays a crucial role for the stability of the system. For most cases, rewarding is granted to the miner or validating node for doing the transaction checking process. Tokens that exist as a piece in the project ecosystem, usually serve as the main reward, which helps in maintaining the health of the entire system. Based on this feature, current DLT systems can be divided into two types: systems with reward or systems without reward.

5.3.2.9.2 Incentive DLT system

Bitcoin is the ideal example for the blockchain with the rewarding system, where each miner that successfully mined a block will be rewarded with set number of bitcoins. Doing this will keep the distributed network stable, govern and maintain the integrity and data accuracy. Rewarding makes mining profitable and encourages the miners to follow the rules. In the absence of rewards, there is no incentive for the nodes in the public permissionless system to engage in the validation process and/or behave properly. Insufficient number of validating nodes and their wilful behaviour could impact the system's security and integrity. The purpose of providing the reward in the public blockchain is to encourage all the free node miners to follow the rules. This is an indirect way of solving the nodes trust issue in a P2P network.

5.3.2.9.3 Non-incentive DLT system

Blockchain, like Hyperledger, does not have the rewarding mechanism but still can handle the consensus issue. The reason is that each node inside the Hyperledger network will have to gain the permission to join as the validator and this process normally will also require to register the identity of the attendee. This ensures that a traceable result could be found even under some malicious conditions. In this case, node trust issue is resolved directly outside the chain. All the nodes included inside the Hyperledger network will trust each other, so validation becomes a mandatory work or the promises for the node even there is no reward for the computation power spent.

5.3.2.10 DLT oracle

DLT systems and smart contracts cannot access data from outside of their network. Regarding to this issue, DLT oracles are useful for smart contracts that cannot access sources of data external to the DLT system.

DLT oracles represent trusted systems designed to supply external data to a DLT system or to respond to events from DLT systems. Transformation logic and services can be used to perform the translation needed to communicate data to and from DLT systems. DLT oracles can enable smart contracts to ingest real world data during code execution (see ISO 23257:—, 10.3.2).

5.4 Taxonomy of application domains, purposes and economic activity sections for use cases

5.4.1 General

Blockchain use cases are described by several standardization bodies, manufacturers, solution providers, consulting companies, economic organizations and researchers, leading to diverse and non-harmonized documentation.[4] See Annex B for a context from use-case classification.

This subclause generalizes specific use cases so that they apply to more than one activity sector, by distinguishing cross-sector application domains (see 5.4.1), cross-sector use case purposes (see 5.4.2) and economic activity sections (see 5.4.3).

5.4.2 Cross-sector application domains

5.4.2.1 General

Application domains are defined as areas of interest where DLT applies. Cross-sector application domains bring a first abstraction layer for any DLT service or solution deploying any use case in any activity sector.

This subclause proposes 6 cross-sector application domains.

5.4.2.2 Collaboration, decision making, structuration

(Horizontal Category: Governance)

Collaboration relates to creative collaboration and productive collaboration, but not restrictively.

In creative collaboration, the creation process is split into creative tasks (e.g. artistic task) shaping the creative work (e.g. musical work).

Similarly in productive collaboration, the production process is split into productive tasks (e.g. artistic, technical, administrative and legal tasks) shaping the product (e.g. sound recording leading to the music track) or generating the resource (e.g. excess energy from households).

Decision making relies on some decision elements, which are collected to make a relevant decision (e.g. a task is validated and a collaborator can receive a remuneration).

Structuration refers to the decentralized way some processes are orchestrated within, e.g. an application (e.g. a decentralized application), an organization (e.g. a decentralized autonomous organization) or a project (e.g. a collaborative project).

Within this application domain, DLT can record the execution of each task, a decision element, as well as the transaction associated to the remuneration of each collaborator.

5.4.2.3 Intellectual property protection, certification

(Horizontal Category: Process Optimization)

Intellectual property covers copyright and related rights and industrial property as defined by the World Intellectual Property Organization (WIPO)[5].

Certification applies to a creative work, a product, a resource, a service or a system.

Within this application domain, DLT can record and timestamp various types of proofs that can be legally binding (e.g. proof of deposit) but not necessarily.

5.4.2.4 Disintermediation in distribution, actions traceability

(Horizontal Category: Data Provenance)

Disintermediation refers to the removal of some intermediary actors in the value chain.

Actions traceability refers to the supply chain, between the producer and the distributor, and to the logistics chain, inside the distributor processes and between the distributor and the consumer.

Within this application domain, DLT can record transactions related to any action (e.g. delivery, sale) but cannot store higher volume of data (e.g. metadata, media data, meteorology data). For this purpose, a blockchain system may be associated with a distributed storage system (e.g. IPFS) and / or a cloud storage platform.

5.4.2.5 Rights and identifier management, identification

(Horizontal Category: Identity Management)

In this context, management relates more generally to:

- Rights Management: rights (e.g. copyright and related rights, access right to a resource or a service) can be granted and negotiated based on a contract;
- Identifier Management: identifiers can be allocated to a product, a resource, a service, an event but also to a legal entity or a natural person (in that case, identifiers depict the identity) based on an identifier owner declaration;
- Data Management: data can refer to a natural person (e.g. personal data), a product or a service (e.g. behavioural data, usage data), a resource (e.g. land registry) or an event (e.g. audience, participants);
- Security Management (including the identification process): the identification process verifies the existence of the identifier, the authentication process verifies the password associated with the identifier, whereas the authorization process verifies that the identified and authenticated entity has granted sufficient rights for accessing a product, a resource, a service or a venue. The integrity protection process verifies that data has not been modified, that a product has not been counterfeited or that a natural person is really the person he / she pretends to be (e.g. by means of fingerprint or eye scan).

Within this application domain, DLT can record several types of small data (e.g. rights, identifiers, signatures) in order to facilitate previous management processes.

5.4.2.6 Contract management, automation

(Horizontal Category: Automation)

Contract management addresses multiple contracts combinations especially within the supply chain and the logistics chain (e.g. content distribution chain, energy delivery chain).

The legacy contract is still in force and may be reinforced by the smart contract which adapts some contractual clauses of the legacy contract through a programming language (based on script operators).

Automation applies to the execution of some contractual clauses of the legacy contract.

Within this application domain, DLT can record a legacy contract hash, i.e. the timestamp of a unique fingerprint of the legacy contract (as for Bitcoin through the free information field of a transaction) in relation with certification. It can also automate the execution of some contractual clauses of the legacy contract through the smart contract, i.e. automate the execution of a task and the payment of interested parties (as for Ethereum) in relation with electronic payment.

5.4.2.7 Electronic payment, cryptocurrency and token exchange

(Horizontal Category: Cryptocurrency and Asset Exchange)

Electronic payment is used for paying products and services without using cash or bank cheque. It is based on a currency (e.g. euro, dollar) and an electronic payment system that proceeds the transaction and the payment.

Micropayment allows buying and paying a unit of product, resource or service below a unit of currency (e.g. below 1 dollar).

A cryptocurrency, also called coin, allows paying below fiat currency cent (i.e. below 0,01 dollar) thanks to low transaction amounts supported by DLT systems.A token relies on an external DLT system (e.g. tether token relies on Omni blockchain system). Tokens can be defined and exchanged on a DLT system. Within this application domain, which is at the essence of Bitcoin system, DLT can offer new instant payment methods based on micropayment (e.g. per download or stream, page view, unit of data, minute of call, unit of energy).

5.4.3 Cross-sector use cases purposes

Cross-sector use case purposes bring a second abstraction layer as they are associated with each cross-sector application domain.

For harmonization reasons, a cross-sector use case purpose is expressed as a list of present participle forms of action verbs (e.g. certifying, creating, remunerating, rewarding), sometimes completed by objects (e.g. data, product, resource, service).

Table 2 shows cross-sector use case purposes, associated to the six cross-sector application domains.

Table 2 — Cross-sector use case purpose for each cross-sector applications domain

Cross-sector applications domain	Cross-sector use case purpose
Collaboration, Decision Making, Structuration	Administrating, Governing, Organising and Structuring
	Branding, Creating Work, Designing and Patenting
	Collaborating, Hiring, Including, Partnering, Relating, Remunerating, Tasking and Trusting
	Creating Digital Asset, Financing and Funding
	Creating Event, Product or Service, Issuing, Producing, Publishing and Serving
	Creating and Generating Resource

Table 2 *(continued)*

Cross-sector applications domain	Cross-sector use case purpose
	Deciding and Voting
	Donating, Giving and Lending
	Operating, Proceeding and Processing
	Rewarding
	Saving Costs and Resource
	Sharing Data, Human Resource and Revenue
Intellectual Property Protection, Certification	Authenticating, Certifying and Notarising
	Authoring and Protecting Authorship
	Complying to Law, Regulation or Conforming to Standard
	Labelling
	Owning Cryptocurrency, Token, Data, Product, Resource or Rights and Protecting Ownership
	Proofing
	Recording, Registrating and Timestamping
Disintermediation in Distribution, Actions Traceability	Bearing, Sourcing, Supplying and Supporting
	Commercialising, Delivering, Distributing, Exchanging Product, Material Resource or Service, Marketing, Monetising, Promoting, Purchasing and Selling
	Communicating and Messaging
	Connecting and Interconnecting
	Controlling, Monitoring, Tracing and Tracking
	Consuming and Entertaining
	Discovering, Endorsing and Recommending
	Sharing Product, Material Resource or Service
Rights and Identifier Management, Identification	Accessing Data, Product, Resource, Service or Venue
	Allocating, Assigning, Credentialing, Crediting and Granting
	Archiving, Conserving, Managing Data, Preserving and Storing
	Auditing, Qualifying, Rating, Quoting and Reporting
	Authorising and Licensing
	Checking, Validating and Verifying
	Claiming and Reconciliating
	Encrypting, Hashing, Protecting, Securing and Signing Data (including Content)
	Fighting and Preventing against Counterfeiting, Fraud, Laundering, Piracy or Theft
	Identifying Creative Work, Event, Organization, Person, Product, Resource or Service
	Managing Rights and Royalties
Contract Management, Automation	Accounting, Billing and Charging
	Agreeing, Committing, Consenting, Contracting and Engaging
	Automating Process or Task
	Guaranteeing, Insuring and Responsibilizing
	Interoperating and Porting

Table 2 *(continued)*

Cross-sector applications domain	Cross-sector use case purpose
	Regulating and Taxing
	Ticketing
Electronic Payment, Cryptocurrency and Token Exchange	Exchanging Cryptocurrency or Token, Gambling, Ordering, Paying, Settling, Trading and Transacting
	Managing Wallet

5.4.4 Economic activity sections

Economic activities, also referred to as activity sectors, business activities or industrial activities, have been classified and standardized in Reference [6].

Economic activity sections bring a third abstraction layer and are a prerequisite for addressing activity sector specificities.

20 Economic activity sections are provided in Table 3, using a voluntarily simplified wording, and aligned with UN / ISIC[6].

Table 3 — UN / ISIC economic activity for each economic activity

Economic Activity Section	UN / ISIC Economic Activity Section
Accommodation and Food	I – Accommodation and food service activities
Agriculture, Forestry and Fishing	A – Agriculture, forestry and fishing
Bank, Finance and Insurance	K – Financial and insurance activities
Construction	F - Construction
Distribution, Retail and Wholesale	G – Wholesale and retail trade; repair of motor vehicles and motorcycles
Education	P - Education
Energy, Environment and Utilities	D – Electricity, gas, steam and air conditioning supply
	E – Water supply; sewerage, waste management and remediation activities
Extraterritorial Organization	U – Activities of extraterritorial organizations and bodies
Government and Public Administration	O – Public administration and defence; compulsory social security
Healthcare and Life Sciences	Q – Human health and social work activities
Households	T – Activities of households as employers; Undifferentiated goods- and services-producing activities of households for own use
Industries and Manufacturing	C - Manufacturing
Information and Communication	J – Information and communication
Media and Entertainment	R – Arts, entertainment and recreation
Mining and Quarrying	B - Mining and quarrying
Private Administration and Support	N – Administrative and support service activities
Professional, Scientific and Technical	M – Professional, scientific and technical activities
Real Estate	L – Real estate activities
Transportation and Travel	H – Transportation and storage
Other Service	S – Other service activities

6 Ontology

6.1 Introduction

An ontology is a formal description of knowledge as a set of concepts within a domain and the relationships that hold between them. For making this description, it is required to define components such as individuals, classes, attributes and relations as well as restrictions, rules and axioms.

This subclause defines the ontology for the most basic foundational concept of DLT based on 5.2. For graphical representation of an ontology, this document uses the Unified Modeling Language (UML), which is a general-purpose, developmental, modeling language in the field of software engineering that is intended to provide a standard way to visualize the design of a system. This document only uses a very simple form of UML class diagrams that are expected to be easily understandable by readers familiar with the basic concepts of object-oriented systems.

Figure 3 shows overall graphical representation of DLT Ontology and explanations for each component of this ontology are covered by other subclause.

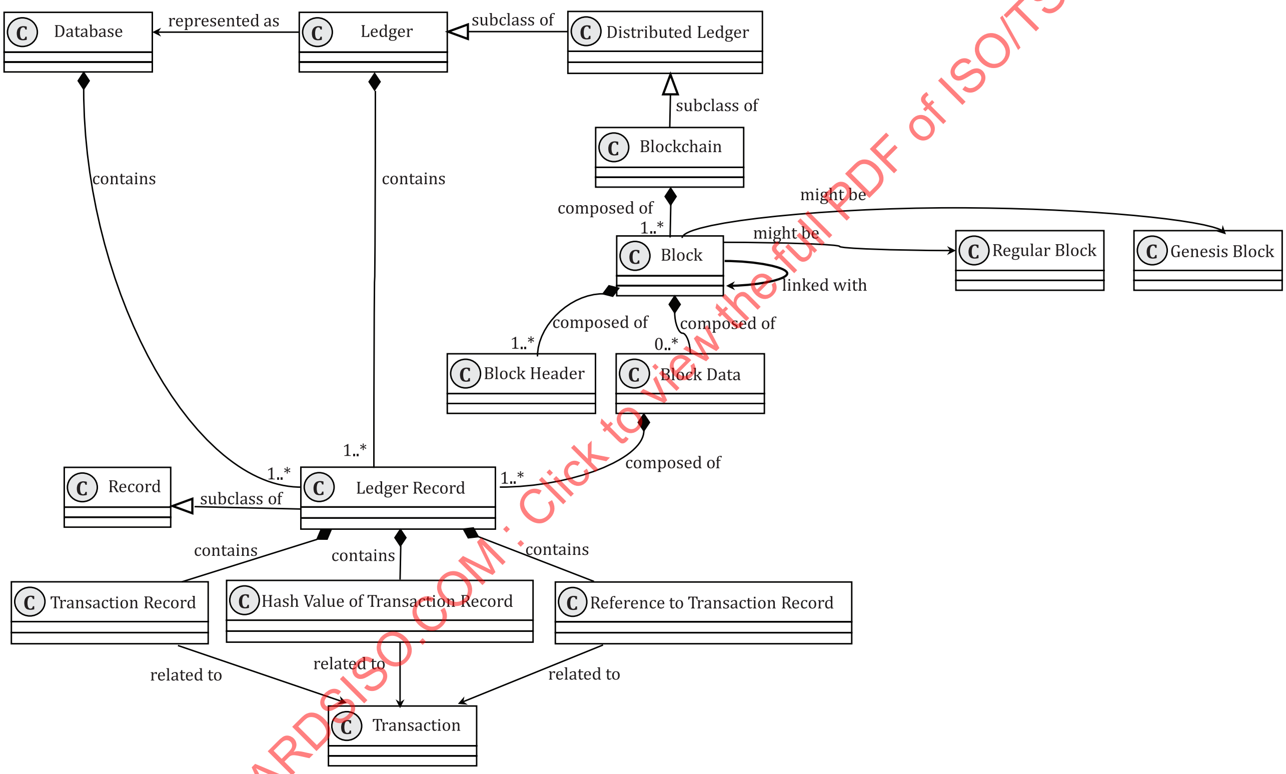

Figure 3 — DLT ontology diagram – Graphical overview

6.2 Ledger Class

A ledger, which is recognized as a type of database, would contain one or more records for related transactions. The concept of ledger is represented as Figure 4.