ETSI GR PDL 034 V1.1.1 (2025-09)

GROUP REPORT

Permissioned Distributed Ledger (PDL); Trustworthy Data Space Infrastructure with PDL

Disclaimer

The present document has been produced and approved by the Permissioned Distributed Ledger (PDL) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/PDL-0034_Trust_Data_Space

Keywords

data interoperability, data management,
data sharing, distributed ledger, PDL,
trustworthy AI

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI Search & Browse Standards application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver repository.

Users should be aware that the present document may be revised or have its status changed,
this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to
the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2025.
All rights reserved.

Contents

List of figures

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI IPR online database.

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Permissioned Distributed Ledger (PDL).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document addresses the design, implementation, and governance of Trustworthy Data Spaces (TDS) underpinned by Permissioned Distributed Ledger (PDL) technology. As data ecosystems grow increasingly complex, the need for secure, interoperable, and regulatory-compliant frameworks becomes critical. TDS provides a decentralized infrastructure that ensures data integrity, sovereignty, and privacy while enabling cross-organizational collaboration.

Key technologies explored include blockchain for immutable audit trails, privacy computing for confidential data processing, and adaptive consensus mechanisms to balance scalability with security. The present document outlines core components of TDS, such as layered architectures for trusted data flow, decentralized identity management, and compliance with regulations like GDPR and MiCA.

Practical use cases, such as Digital Product Passports for circular economies, Supply Chain Data Exchange for real-time transparency, and Life-Cycle Management for sustainability, demonstrate TDS's transformative potential across industries. Challenges such as interoperability gaps, regulatory fragmentation, and legacy system integration are discussed alongside future trends, including AI-blockchain convergence and global standardization efforts.

The present document serves as a foundational guide for enterprises, policymakers, and technologists aiming to build ethical, resilient, and scalable data ecosystems in alignment with emerging Web 3.0 paradigms.

Introduction

The present document focuses on the role of Permissioned Distributed Ledgers (PDL) in realizing TDS. Unlike public blockchains, PDLs provide controlled access, enhanced scalability, and governance tailored to enterprise needs. By integrating advanced cryptographic techniques, decentralized identity systems, and adaptive consensus models, TDS enables secure data transactions, auditable workflows and privacy-preserving analytics across industries.

1 Scope

The present document specifies the architectural framework, technical requirements, and implementation guidelines for establishing Trustworthy Data Space (TDS) infrastructures utilizing Permissioned Distributed Ledger (PDL) technology. It addresses the integration of decentralized systems, data sovereignty, security mechanisms, and privacy-preserving technologies to enable secure, interoperable, and compliant data sharing across organizational and jurisdictional boundaries.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

[i.1] 3GPP 23.501 (V19.3.0) (2025-03): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 19)".

[i.2] 3GPP TS 33.501 (V19.2.0) (2025-03): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G System (Release 19)".

[i.3] 3GPP TR 33.794 (V19.1.0) (2025-03): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on enablers for zero trust security (Release 19)".

[i.4] Data Spaces Business Alliance: "Technical Convergence".

[i.5] European Data: "EU's Digital Product Passport: Advancing transparency and sustainability".

[i.6] Supplychainexchange.

[i.7] Life Cycle Initiative: "Life Cycle Management".

[i.8] Catena-X: "Sustainability with Catena-X".

[i.9] Digitaldefynd: "10 ways JP Morgan is using AI".

[i.10] Accenture: "Building a Responsible Metaverse".

[i.11] The data economy lab: "Cities & Data Sharing — Part 3: Barcelona".

[i.12] The HBS Digital Initiative: "Farm to Data Table: John Deere and Data in Precision Agriculture".

[i.13] Deterministic6G: "5G latency analysis and possible improvements".

[i.14] gridX: "Prosumer".

[i.15] International Data Spaces.

[i.16] ISO/IEC DIS 27090: "Cybersecurity — Artificial Intelligence — Guidance for addressing security threats to artificial intelligence systems".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

data: facts, observations, or values represented in any format

data security: protection of data from unauthorized access, corruption, theft, or misuse

distributed: system or architecture where components are spread across multiple nodes rather than centralized

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
APPID	APPlication IDentity
BCADD	BlockChain ADDress
BDVA	Big Data Value Association
CA	Certificate Authority
CIM	cross cutting Context Information Management
DAGs	Directed Acyclic Graphs
DGA	Data Governance Act
DID	Decentralized IDentifier
DLT	Distributed Ledger Technology
DPP	Digital Product Passport
DSBA	Data Spaces Business Alliance
EBSI	European Blockchain Services Infrastructure
ECC	Elliptic Curve Cryptography
EHDS	European Health Data Space
EPR	Extended Producer Responsibility
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
HE	Homomorphic Encryption
IDSA	International Data Spaces Association
IoT	Internet of Things
IPFS	InterPlanetary File System
JSON-LD	JSON for Linked Data
KYC	Know Your Customer
MAS	Monetary Authority of Singapore
MFA	Multi-Factor Authentication
MiCA	Markets in Crypto-Assets Regulation
ML	Machine Learning
MVF	Minimum Viable Framework
NAT	Network Address Translation
NFT	Non-Fungible Token

NGSI-LD	Next Generation Service Interfaces - Linked Data
NIST	National Institute of Standards and Technology
NIZK	Non-Interactive Zero-Knowledge proof
ODRL	Open Digital Rights Language
PBFT	Practical Byzantine Fault Tolerance
PDP	Policy Decision Points
PEP	Policy Enforcement Points
PoA	Proof of Authority
PoR	Proof of Routing
PoS	Proof of Stake
PoW	Proof of Work
PQC	Post-Quantum Cryptography
RDF	Resource Description Framework
REST	REpresentational State Transfer
SLA	Service Level Agreement
SMPC	Secure Multi-Party Computation
SSI	Self-Sovereign Identity
TDS	Trustworthy Data Space
VC	Verifiable Credentials
ZKPs	Zero-Knowledge Proofs

4 Trustworthy-Data-Space-Related Definitions

4.1 Definition of Data Space

4.1.1 Definition of Data

Data refers to structured or unstructured representations of facts, figures, or information in a form suitable for processing, analysis, or communication. Data can be generated, stored, transmitted, and utilized through digital or analog means, serving as the foundational element for decision-making, automation, and knowledge creation.

4.1.2 Definition of Data Space

A Data Space is a decentralized, interoperable ecosystem where data is shared, governed, and utilized under predefined rules and technical frameworks. It ensures secure, sovereign, and privacy-preserving interactions among participants while enabling seamless data exchange across organizational and technological boundaries.

4.2 Key Technology Concerning Data Space

4.2.1 Distributed Architecture

Distributed Architecture refers to a system design where data and computational resources are decentralized across multiple nodes or entities. This architecture enhances scalability, fault tolerance, and resilience by eliminating single points of failure and enabling peer-to-peer collaboration.

4.2.2 Blockchain

Blockchain is a decentralized database system based on Distributed Ledger Technology (DLT), constructed through a distributed network of nodes, and consensus mechanisms.

4.2.3 Privacy Computing Technology

Privacy Computing Technology is the technology that enables data processing while preserving the privacy and confidentiality of the data. Examples include homomorphic encryption, secure multi-party computation, and zero-knowledge proofs.

4.2.4 Data Sovereignty Management

Data sovereignty management refers to the fact that data collected or stored in a particular country or the European Union is subject to the laws and governance of the country or the European Union of collection.

In Web 3.0, its main features are as follows:

1) Decentralization.

2) Users have their own autonomy and more control over their personal data and privacy.

4.2.5 Data Security Technology

Technologies and practices designed to protect data from unauthorized access, corruption, or theft. This includes encryption, access control, and intrusion detection systems.

4.3 Definitions of Data-Related Processes

4.3.1 Data Management

Data Management involves the systematic organization, storage, and maintenance of data throughout its lifecycle. Key activities include data cataloging, quality assurance, metadata management, and compliance auditing.

4.3.2 Data Flow

The movement of data between different systems or components within a data space. It includes data ingestion, transformation and transmission.

4.3.3 Data Supervision

The monitoring and oversight of data usage to ensure compliance with policies and regulations. It includes data auditing, data monitoring and data governance.

4.3.4 Data Storage

Data Storage encompasses technologies and methodologies for preserving data in physical or cloud-based repositories. Considerations include redundancy, retrieval speed and energy efficiency.

4.3.5 Data Utilization

Data Utilization involves extracting value from data through analytics, machine learning, or visualization. It transforms raw data into actionable insights for business, research or public services.

4.3.6 Data Transaction

Data Transaction is the exchange of data between parties under contractual or algorithmic agreements. Transactions may involve monetary compensation, barter, or reciprocal data sharing, and its main function is reflected in:

1) Data transactions can ensure accurate transmission of information.

2) Data transactions enable real-time updates of data.

4.3.7 Data Sharing

Data Sharing enables collaborative use of data across organizations or systems while respecting ownership and privacy constraints. It is facilitated by standardized APIs, licensing frameworks and trust mechanisms.

4.3.8 Data Acquisition

Data Acquisition is the process of collecting data from sensors, databases, or external sources. It includes validation, preprocessing, and integration steps to ensure data readiness for downstream applications.

5 Introduction to Trustworthy Data Space Infrastructure

5.1 Trustworthy Data Space

5.1.1 Components of Trustworthy Data Space

5.1.1.1 Data Security Infrastructure

Data security infrastructure is a framework of technologies, policies, and practices. As the foundational layer, data security infrastructure ensures data confidentiality, integrity and availability through:

1) Encryption Mechanisms: End-to-end encryption for data at rest and in transit.
2) Access Control: Role-based and attribute-based policies to regulate data access.
3) Authentication & Authorization: Multi-Factor Authentication (MFA) and dynamic authorization aligned with Zero Trust principles.
4) Audit Trails: Immutable logging of data interactions using PDL for traceability.

5.1.1.2 Trusted Data Flow Layer

5.1.1.2.1 Trusted data flow platform

The Trusted Data Flow Platform is a specialized system within the Trusted Data Flow Layer, designed to manage high-volume, real-time data exchanges. Features include:

1) Interoperability Standards: Adherence to ETSI specifications.
2) Data Provenance: Metadata tagging to track data origin, ownership and lineage.
3) Smart Contracts: Automated enforcement of data-sharing agreements (e.g. compliance with predefined trust thresholds).

5.1.1.2.2 Trusted data platform

Trusted data platform serves as a centralized repository for structured and unstructured data, equipped with governance frameworks to ensure compliance and ethical use. It integrates tools for data cataloging, metadata management, and role-based access control. Features include:

1) Distributed Ledger Integration: PDL-based storage for immutable records of data transactions.
2) Trust Index Management: Aggregation of trust indicators (e.g. security, reliability) to compute dynamic trust scores.
3) Decentralized Governance: Consensus mechanisms for validating data transactions and policy updates.

5.1.1.3 Trusted Data Application Layer

This layer supports trust-aware applications and services through:

1) User-Centric Trust: Integration of Self-Sovereign Identity (SSI) for personalized trust evaluation.
2) Dynamic Trust Evaluation: Real-time assessment of entities using contextual data (location, behaviour).

3) Trust-Enabled Use Cases:

   - Collaborative AI/ML: Secure federated learning with verifiable contributor trust.
   - Decentralized IoT: Device-to-device interactions governed by smart contracts.
   - Regulatory Compliance: Automated adherence to eIDAS and GDPR via PDL-based audit trails.

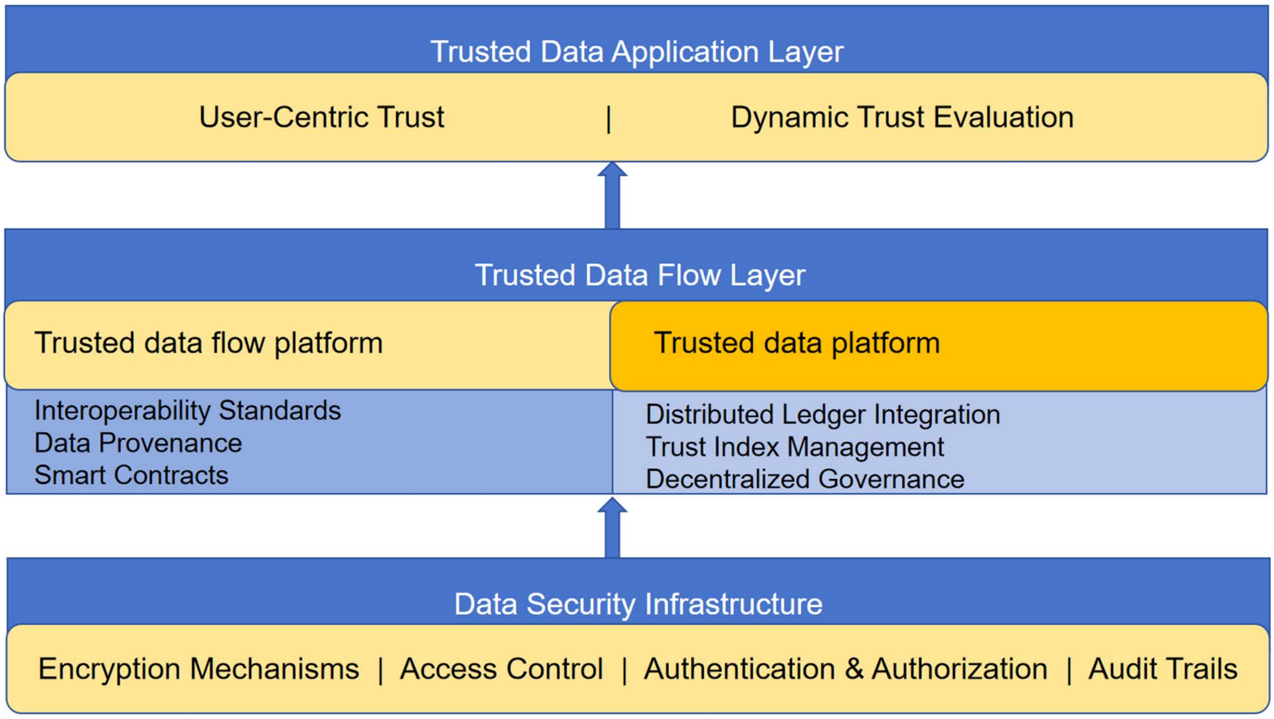

Figure 1: Components of Trustworthy Data Space

5.2 The Functional Architecture of TDS

5.2.1 Client

5.2.1.1 Three Layers of Client

The client serves as the entry point for users to interact with the Trustworthy Data Space (TDS), with its architecture being crucial for user experience and data security. The three-layer structure of the client consists of:

1) User Interface Layer: Responsible for interacting with users, providing a user-friendly interface for data access and management.

2) Application Logic Layer: Manages business rules, workflows, and data processing tasks.

3) Data Access Layer: Communicates with the intermediate service platform to achieve data acquisition, storage, and updates, ensuring data accuracy and timeliness.

5.2.1.2 Functionality

The main functions of the client include:

1) Data Access and Management: Users can query, download, and upload data within the TDS.

2) Data Security Protection: The client encrypts data to ensure its security during transmission and storage.

3) Identity Authentication and Authorization: Manages user authentication and authorization to ensure only legitimate users can access and manipulate data.

4) Data Interaction: Supports data sharing and collaborative work with other clients or servers.

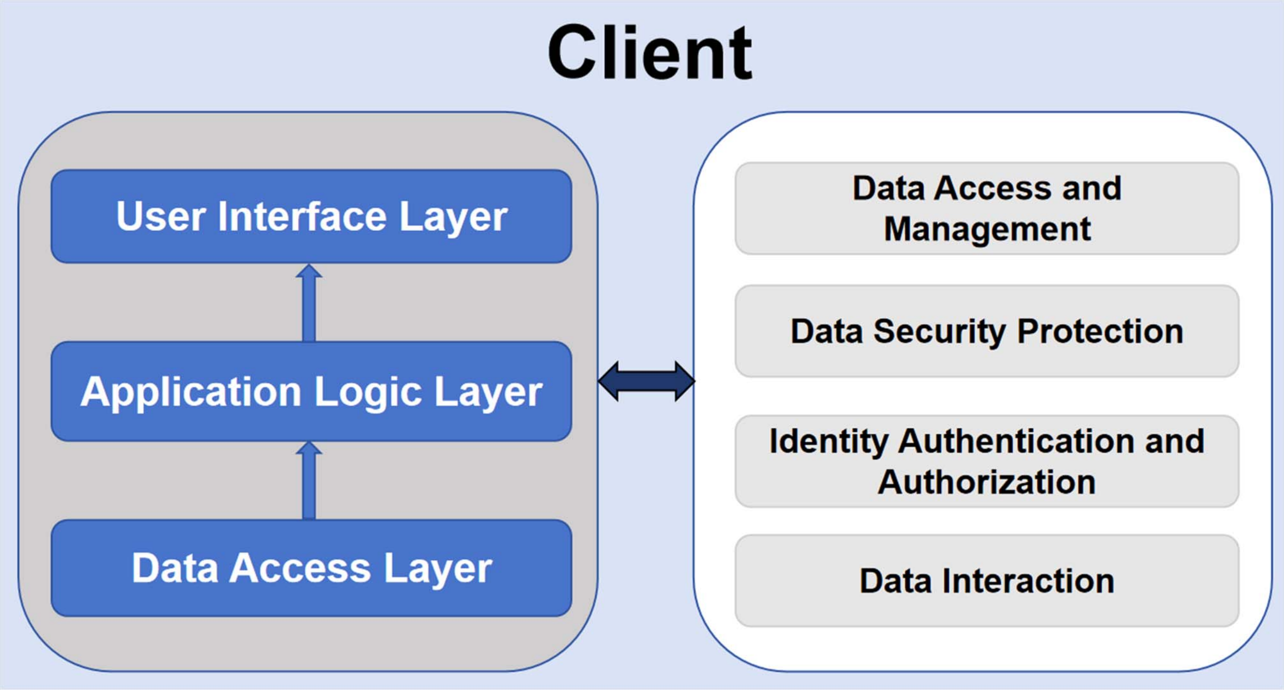

Figure 2: Client

5.2.2 Intermediate Service Platform

5.2.2.1 Three Kinds of Services Available

The intermediate service platform is a core component of the TDS, offering various services to clients and data platforms. The three primary services are:

1) Data Storage Service: Manages data storage and ensures data security and integrity.

2) Data Processing Service: Processes and analyses data, providing functions such as data mining and transformation.

3) Data Transmission Service: Handles data transmission and distribution between components, ensuring efficient and reliable data transfer.

5.2.2.2 Functionality

The main functions of the intermediate service platform include:

1) Service Management: Manages and schedules services on the platform to ensure smooth operation and efficient resource use.

2) Data Routing and Forwarding: Routes and forwards data based on requests and targets for quick delivery.

3) Security Protection: Implements security measures like firewalls and intrusion detection to protect the platform and data.

4) Monitoring and Maintenance: Monitors the platform's operating status in real-time, addressing potential issues promptly to ensure stable operation.

5.3 Emerging Technical Idea Supporting TDS

5.3.1 Identity Management

5.3.1.1 Types of Identity

5.3.1.1.1 User public key identity

In TDS, users use the public key as the identity, and there is no need for the Certificate Authority (CA) to recognize the authenticity of the identity and the ownership of the public key, which has the following characteristics:

1) Decentralization

2) Anonymization

5.3.1.1.2 Network identity

BCADD is the basis of the user's identity at the network layer, which enables the user to:

1) Have more control over personal data and privacy.

2) Have self autonomy to update it.

5.3.1.1.3 Application identity

The user's virtual identity in the application is represented by the APPID, which is generally generated by BCADD for service-specific interactions.

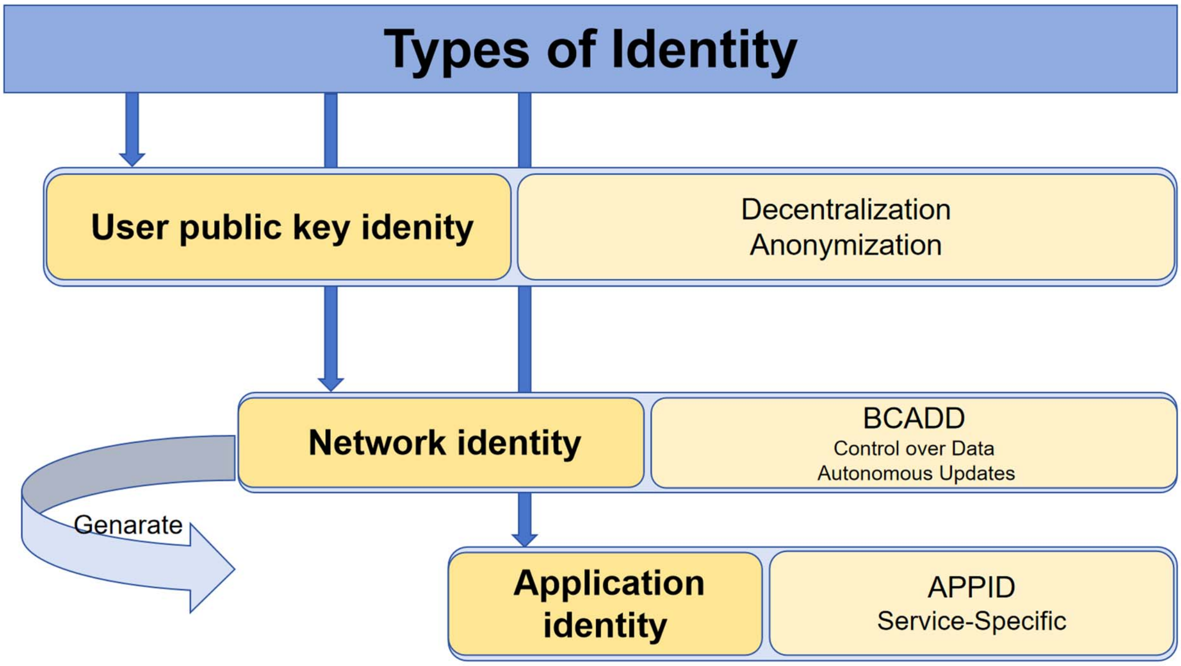

Figure 3: Types of Identity

5.3.1.2 Potential Applications

It is possible to provide users with communication and other related services without a central server.

For example:

1) User-to-user and user-to-application transactions.

2) Use encrypted identities for online gaming, chat interactions, and more.

3) It can be used in World Wide Web (WWW), next-generation mobile communication networks (such as 6G) and new Internet services.

5.3.1.3 Existing Technology

Current technologies underpinning identity management include:

1) Blockchain/DLT: Immutable ledgers for transparent data transactions (e.g. Hyperledger, Ethereum).

2) Zero-Knowledge Proofs (ZKP): Enables privacy-preserving data validation (e.g. zk-SNARKs, Bulletproofs).

3) Distributed Storage: IPFS, Filecoin, and Sia for decentralized data storage.

4) Consensus Mechanisms: Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Proof of Routing (PoR) for network synchronization.

5) Self-Sovereign Identity (SSI): Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) for user-controlled identity management.

5.3.2 Data Storage and Validation

5.3.2.1 Distributed Storage

A distributed data store is a computer network where information is stored on more than one node. It is usually specifically used to refer to either a distributed database where users store information on a number of nodes, or a computer network in which users store information on a number of peer network nodes. User and application data content is stored in distributed memory for the following purposes:

1) It can effectively avoid data loss or corruption.

2) Users have more control over their data and privacy.

5.3.2.2 Consensus Mechanism

A consensus mechanism is a self-regulatory stack of software protocols written into a blockchain's code that synchronizes a network into agreement about the state of a digital ledger. Consensus mechanisms underpinning TDS include:

1) Temporal Consensus: Voting-based hierarchical consensus for synchronization across fractal tiers.

2) Spatial Consensus: Proof of Routing (PoR) optimizes network topology by rewarding nodes with superior routing efficiency.

3) Hybrid Approach: Combines asynchronous timestamping with competitive vertex allocation for resilience.

4) Spatiotemporal Consensus: Combines Proof of Routing (PoR) for topology optimization and PBFT for Byzantine fault tolerance.

5.3.3 Security and Privacy

5.3.3.1 Cryptography Technology

Cryptography is a method of protecting information and communications using codes, so that only those for whom the information is intended can read and process it. In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email. Features include:

1) Confidentiality: Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2) Integrity: Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

3) Non-repudiation: The creator/sender of information cannot deny his intention to send information at a later stage.

4) Authentication: The identities of the sender and receiver are confirmed. As well destination/origin of the information is confirmed.

The cryptography technologies underpinning TDS include:

1) Elliptic Curve Cryptography (ECC): Secures authentication in 5G/6G microservices. The identity authentication mechanism of 5G microservices complies with the security architecture standard of 3GPP TS 33.501 [i.2].

2) Homomorphic Encryption: Enables computation on encrypted data.

3) Non-Interactive ZKP (NIZK): Validates statements without exposing sensitive data.

5.3.3.2 Privacy Protection

1) Data Desensitization: Replaces raw data with ZKP-based proofs.

2) Three-Tier Identity:

   - RealID: Government-issued identity (confidential).

   - BCADD: Blockchain-derived network-layer identity.

   - APPID: Service-specific identity (derived from BCADD).

3) Dynamic Identity Refresh: APPIDs update periodically to prevent tracking.

5.3.4 Legal Compliance

5.3.4.1 Anonymity and Regulatory Balance

KYC/AML Integration: Authorities validate BCADD-to-RealID links without accessing raw data.

Jurisdictional Sharding: Data stored in geo-specific fractal tiers (e.g. EU GDPR-compliant nodes).

5.3.4.2 Data Self-Sovereignty

User-Governed Permissions: Tokenized access rights managed via smart contracts.

5.3.5 Spatial and Time Reference Architecture for Data Space Network

5.3.5.1 Hyperdimensional Simplex Fractal Network

5.3.5.1.1 Introduction

Hyperdimensional Simplex Fractal Network is the basis of a spacetime coordinate system. The novel network entities and functions are defined to make use of hyperdimensional deterministic switching and routing protocols and blockchain-enabled mutual authentication.

5.3.5.1.2 Architecture

5.3.5.1.2.1 Hyperdimensional fractals

Self-Similar Topology: Koch fractal iterations enable tiered growth. The network can grow in terms of tiers, which follows the same pattern of the previous step, and the network can have infinite tiers, allowing infinite connections and infinite shards of the network. The topology is fractal in both dimensional and geometrical.

5.3.5.1.2.2 Design overview

To sculpt the network with fractal shapes abstracted from reality, the computer network is mapped into a new network architecture, named SnowedNet with characteristics from blockchain, fractal shapes, security, routing and switching.

SnowedNet is a Web 3.0 network architecture integrating blockchain, fractal topologies, and secure routing. Key entities and functions include: Blockchain Address (BCADD), SnowedNet Nodes, Data Structures, SnowedNet Address, Routing Path, Hierarchical Design.

SnowedNet combines blockchain's security with fractal topology for scalable, deterministic routing. Upper-tier routers maintain global network views, while shards enable localized consensus and efficient data management.

5.3.5.1.3 Consensus process

1) Proof of Routing (PoR): Mining Priority: Routers with the most active routes gain higher mining chances.

2) Performance Threshold: Nodes are supposed to meet minimum routing/switching speed (via algorithm evaluation) to ensure low latency and deterministic network performance.

3) Competitive Node Re-election: Winning nodes in higher tiers replace underperforming lower-tier nodes. Failed nodes are demoted to higher tiers for revaluation.

4) Heartbeat Packet Workflow:

   - Unicast (1-hop): Neighbour discovery and verification.
   - Multicast (2t-hop): Targets remote routers (t = tier number) to avoid network flooding.
   - Broadcast (1-hop): Updates local entity records.

5) Route Length Calculation: Measured in segment units (shortest path between top-tier nodes = 1 hop). Route efficiency determines consensus rewards and network optimization.

5.3.5.1.4 Routing strategy

1) Routing Mechanism:

   - BCADD-Driven Switching: Uses encrypted Blockchain Addresses (BCADD) as headers to route traffic between network interfaces (e.g. switch ports).
   - Dynamic Binding: Self-claimed identities in blockchain records map entities to their network interfaces for real-time switching.

2) Smart Contract Integration:

   - Service Level Agreements (SLAs): Automatically negotiated via smart contracts, enabling resource reservation (e.g. bandwidth).

   - Transparent Coordination: SLA terms are publicly readable by routers, ensuring accountability and efficient resource allocation.

5.3.5.2 Data Spaces Business Alliance Technical Convergence

5.3.5.2.1 Introduction

The Data Spaces Business Alliance (DSBA), formed by BDVA, FIWARE Foundation, Gaia-X, and IDSA, aims to establish a unified technical framework for interoperable, sovereign, and trustworthy data spaces across Europe. Its goal is to enable secure data sharing and value creation by harmonizing standards, architectures, and governance models. The document outlines a Minimum Viable Framework (MVF) focusing on three pillars: Data Interoperability, Data Sovereignty & Trust, and Data Value Creation, supported by collaborative workstreams to align specifications and implementations [i.4].

5.3.5.2.2 Architecture

5.3.5.2.2.1 Core Components

- Data Space Connectors: Act as gateways for participants to publish or consume data, enforce policies, and negotiate contracts.

- Data Space Registry: Manages participant identities and trust via Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs).

- Federated Services: Global catalog, marketplace, and metadata broker services for discovery and transactions.

5.3.5.2.2.2 Conceptual Model:

Participants (Providers/Consumers), Data Products (combining services/resources), and Self-Descriptions (machine-readable metadata linked to VCs).

5.3.5.2.2.3 Layered Interoperability:

Data Models and APIs for syntactic/semantic interoperability.

Trust Framework: Decentralized identity management and policy enforcement.

5.3.5.2.3 Consensus Process

1) Governance Models:

   - Centralized, Decentralized, or Federated authority models for data space governance, aligned with Gaia-X and IDSA specifications.

2) Trust Anchors:

   - Verification of identities via VCs issued by Trusted Issuers and registered in blockchain-based Trusted Participant Lists.

3) Decentralized Consensus:

   - Uses EBSI-compatible blockchains for maintaining verifiable registries and resolving DIDs via Universal Resolvers.

4) Policy Alignment:

   - Cross-organizational agreement on ODRL profiles and compliance certifications.

5.3.5.2.4 Routing Strategy

1) Data Exchange Control:

- NGSI-LD API: Standard for context-aware data exchange between providers/consumers.
- Dataspace Protocol: Manages contract negotiation, data transfer control, and usage logging.

2) Policy-Driven Routing:

- Policy Enforcement Points (PEP) and Policy Decision Points (PDP): Enforce access/usage policies during data transactions.

3) Service Discovery:

- Metadata Brokers and Federated Catalogs: Enable discovery of data offerings via DCAT standards and TM Forum APIs.

4) Decentralized Workflows:

- Connectors route requests based on Verifiable Credentials and trust anchors, ensuring compliance with negotiated contracts.

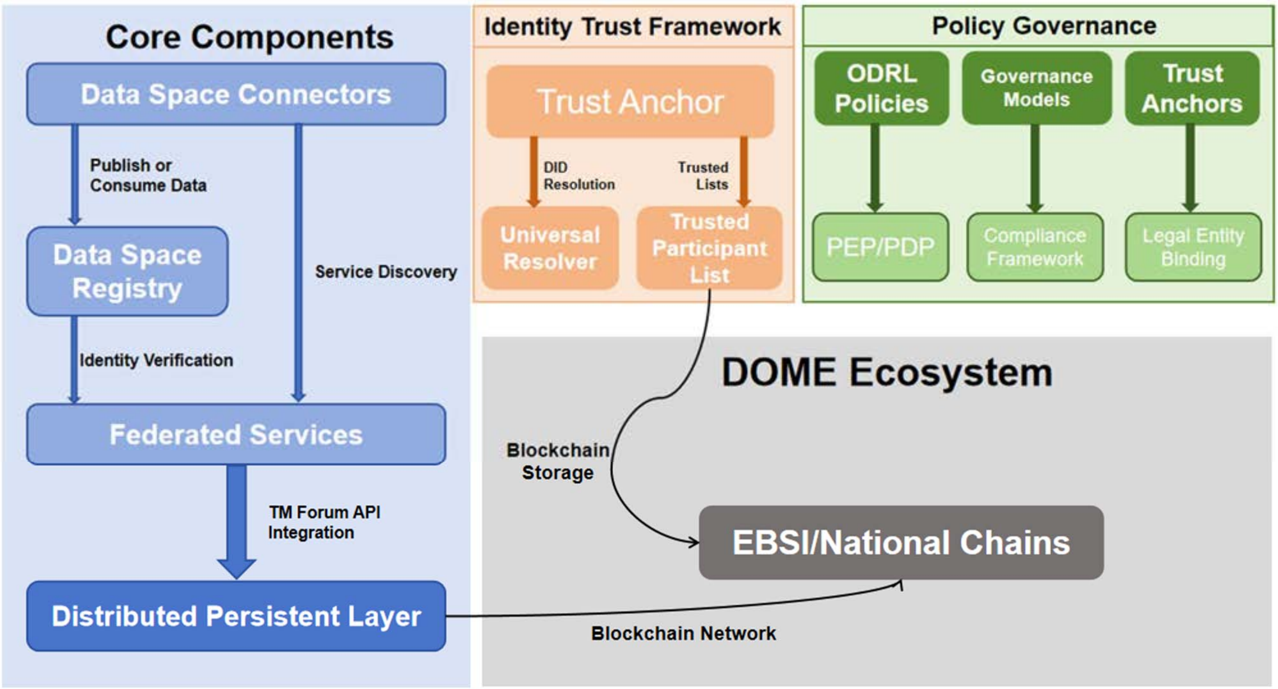

Figure 4: Data Spaces Business Alliance Technical Convergence

5.3.5.3 International Data Space Reference Architecture Model

5.3.5.3.1 Introduction

The International Data Spaces (IDS) is a decentralized framework designed to enable secure, sovereign data exchange across organizations and industries. It emphasizes trust, interoperability, and data sovereignty, allowing data providers to retain control over their data while facilitating collaboration. IDS addresses challenges in data sharing by establishing a standardized ecosystem where participants can exchange information securely under defined policies, fostering innovation and compliance.

5.3.5.3.2 Architecture

The IDS architecture comprises core components that ensure decentralized, secure data interactions:

1) Connector: Facilitates secure data exchange between participants, enforcing usage policies and encryption.
2) Broker: Acts as a registry for discovering data sources and services.
3) Identity Provider: Manages authentication and authorization via certificates.
4) App Store: Offers data-related services and tools.
   - Built on REST APIs, RDF, and JSON-LD standards, the architecture integrates DLT for auditing and emphasizes data usage control to ensure compliance with provider policies.

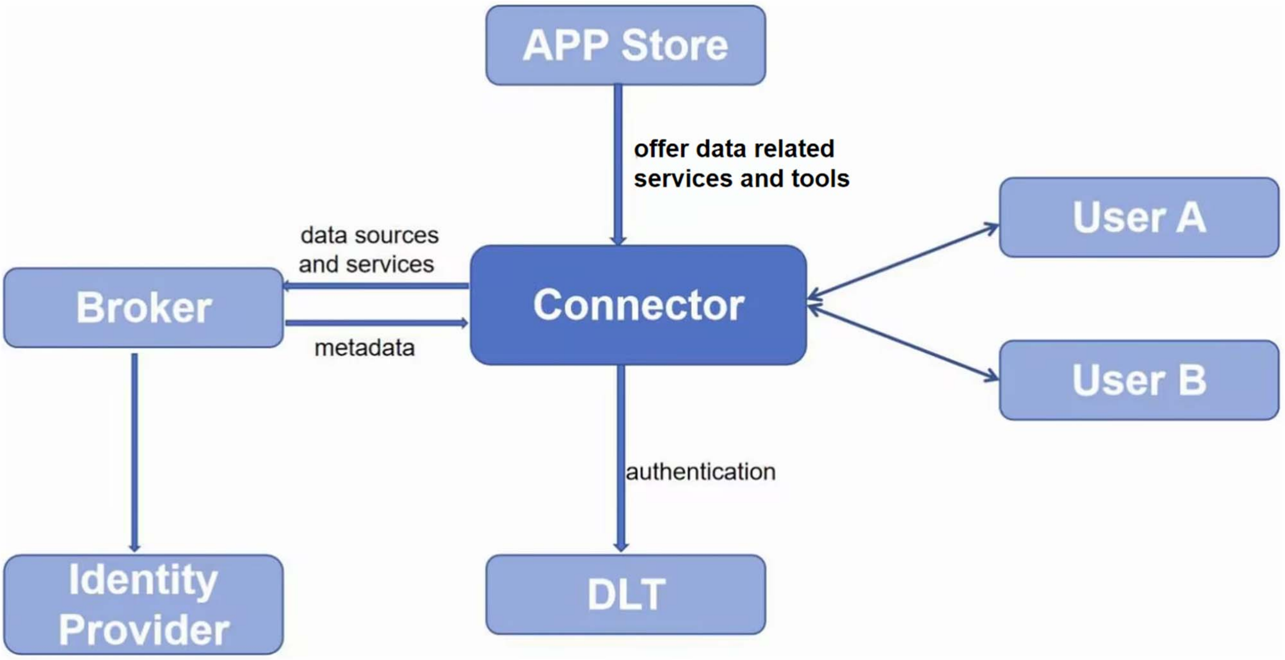

Figure 5: Architecture of IDS

5.3.5.3.3 Consensus Process

IDS relies on a governance model where stakeholders collaboratively define technical standards, business rules, and certification processes. Consensus is achieved through agreements among participants (e.g. enterprises, policymakers) on policies ensuring trust, security, and interoperability. Components and services should undergo certification to comply with IDS criteria, creating a unified ecosystem. This governance framework ensures alignment across diverse industries and regions.

5.3.5.3.4 Routing Strategy

Data routing in IDS combines decentralized discovery and direct peer-to-peer communication. The Broker enables participants to locate data sources via metadata, while Connectors establish secure, policy-compliant connections once a match is found. Routing adheres to data usage controls, ensuring efficient and auditable transfers. This strategy minimizes central points of failure, prioritizing security and sovereignty through encrypted channels and dynamic policy enforcement [i.15].

5.3.6 Web 3.0 Decentralized Controller for TDS

5.3.6.1 Identity and Access

The authentication is one fundamental function for decentralized controllers, including identity and service access:

1) Identity Hierarchy:

   - RealID: Confidential user identity (e.g. government-issued).
   - BCADD: Blockchain-derived network-layer identity for encrypted access.
   - APPID: Service-specific identity derived from BCADD.

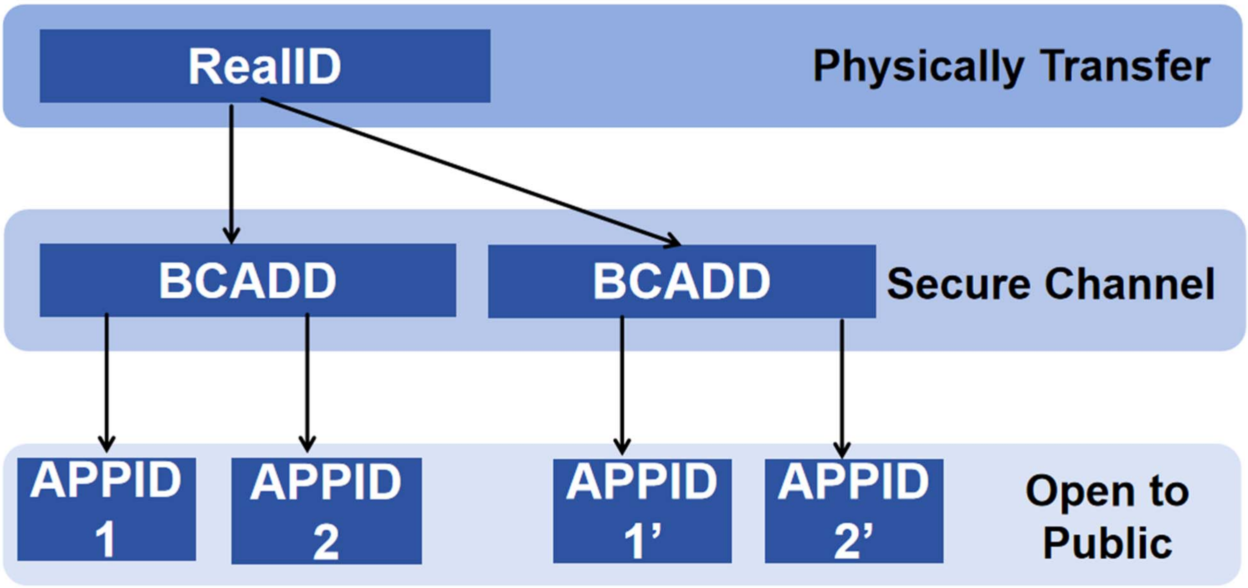

Figure 6: Identity Hierarchy

2) Blockchain Integration:

   - Smart Contracts: Manage identity associations and minor status updates (e.g. mobility, access rights).
   - Efficient Data Handling: Focuses on small, critical data (e.g. topology changes, identity mappings) to reduce blockchain bloat.

3) Security and Scalability:

   - Encrypted Tunnels: The Decentralized Controller acts as an intermediary, enabling secure communication between entities without direct blockchain access.
   - Decentralized Infrastructure: Enhances integrity and scalability while preserving user sovereignty over data.

5.3.6.2 Network and Application Integration

Another key function that the Decentralized Controller should perform is the network segment routing for data delivery:

1) Core Function:

   - Decentralized Routing: Replaces traditional central controllers with blockchain-enabled Decentralized Controllers, eliminating reliance on conventional network addresses.

2) Key Mechanisms:

   - BCADD/APPID Identifiers: Nodes are identified by Blockchain-Derived Addresses (BCADD) or Application-specific IDs (APPID), linked to network topology.

   - Blockchain-Optimized Pathfinding: Routing paths between users are determined by mapping connections between their associated blockchain nodes.

3) Security and Efficiency:

   - Encrypted Logical Tunnels: Paths are secured via keys exchanged between blockchain access points, leveraging blockchain's cryptographic trust.

   - Segmented Network: Blockchain is divided into localized segments (overlay access points), enabling efficient local routing while maintaining global coordination.

4) Global Scalability:

   - Aggregated Topology: Global routing paths are dynamically constructed by aggregating data from all blockchain nodes, ensuring resilience and adaptability.

5.3.6.3 Identity Association with Encrypted Address Translation

The Decentralized Controller architecture leverages ledger records to manage routing, switching, and identity associations in a decentralized network. Key components include:

1) Ledger Records: Store self-claimed identities, address bindings, and routing data.
   Form the backbone of the identity registry, linking entities to their Blockchain Addresses (BCADD) and network interfaces.

2) NEAT Protocol: A lookup protocol using hash tables and bloom filters to efficiently map BCADDs to network interfaces. Directs traffic between entities based on BCADD tags, enabling precise traffic steering without centralized control.

3) Switching Mechanism: Uses BCADD-bound network interfaces to guide traffic, ensuring secure and decentralized communication.

4) Decentralized Controller Functions:

   - Identity Management: Maps Application-specific IDs (APPIDs) to network identifiers and updates BCADD associations.

   - Routing Optimization: Resolves optimal paths via overlay/underlay routing and updates topology dynamically.

5) Security and Authentication: Integrates with blockchain for user authentication, service identity updates, and encrypted tunnelling.

6) Integration with Blockchain: Facilitates aliveness checks, NAT routing, and real-time updates through smart contracts. Ensures transparency and integrity in decentralized service sessions.

5.3.6.4 Decentralized Services Sessions

Key components include:

1) Session-Specific Routing: Each service session is uniquely routed using BCADD (blockchain-derived identity) to steer traffic between encrypted entities.

2) Mutual Authentication:

   - SSL/TLS Handshakes: Every session initiation requires mutual authentication between BCADD identities to ensure secure communication.

3) Dynamic Service Management:

   - Identity Manager: Continuously monitors and updates.
   - Service Quality: Metrics like latency, uptime.
   - Aliveness: Verifies node activity.
   - Service Identity Integrity: Ensures legitimacy and prevents tampering.

5.3.7 Trusted Timestamping Mechanism

5.3.7.1 Principles

1) Immutability and Ordering:

   Timestamps cryptographically bind data/events to a specific point in time, creating an immutable sequence for auditing and event ordering.

   Ensures transactions and blocks are processed chronologically to prevent double-spending and maintain ledger integrity.

2) Decentralized Consensus:

   Timestamps are proposed by network participants and validated via consensus algorithms, eliminating reliance on centralized time authorities.

3) Verifiable Proof:

   Embedded in block headers and linked to cryptographic hashes, enabling independent verification of data existence and integrity at a specific time.

5.3.7.2 Technical Implementation

1) Fractal Network Topology:

   Hierarchical node tiers synchronize time locally while cross-validating globally via multi-path verification.

2) Hash-Chain Anchoring:

   Timestamps embedded in Merkle tree roots, chained to previous blocks for tamper resistance.

3) Dynamic Optimization:

   Machine learning adjusts for network latency, reducing synchronization errors by 30 % in edge environments.

5.4 Core Features of TDS

5.4.1 Decentralization

TDS leverages Distributed Ledger Technology (DLT) and decentralized architectures to eliminate single points of failure and enhance system resilience. Key aspects include:

1) Peer-to-Peer Networks: Data and computational resources are distributed across multiple nodes, ensuring no central authority controls the entire system.

2) Autonomy: Participants retain control over their data and interactions, aligning with Web 3.0 principles of user sovereignty.

3) Fault Tolerance: The decentralized design ensures continuous operation even if individual nodes fail.

5.4.2 Data Integrity

TDS ensures data remains accurate, consistent, and tamper-proof throughout its lifecycle. This is achieved through:

1) Immutable Records: Blockchain technology provides an unalterable audit trail for all data transactions.

2) Consensus Mechanisms: Protocols like Proof of Work (PoW) or Proof of Stake (PoS) validate transactions and maintain ledger consistency.

3) Cryptographic Hashing: Data is secured using cryptographic techniques to detect unauthorized modifications.

5.4.3 Privacy Compliance

TDS adheres to global privacy regulations (e.g. GDPR) and implements advanced privacy-preserving technologies:

1) Zero-Knowledge Proofs (ZKPs): Enables verification of data without revealing the underlying information.

2) Homomorphic Encryption: Allows computation on encrypted data without decryption.

3) Anonymization Techniques: Balances regulatory requirements with user anonymity.

5.4.4 Scalability

TDS supports growing data volumes and user demands without compromising performance:

1) Modular Design: Components can be independently scaled (e.g. storage, computation).

2) Efficient Consensus: Lightweight algorithms (e.g. Practical Byzantine Fault Tolerance) reduce overhead.

3) Interoperability: Standardized APIs and protocols enable seamless integration with existing systems.

6 Use Cases For Trustworthy Data Space Infrastructure

6.1 Use Case 1 - Digital Product Passport

A product passport means that each product has a unique identity that can be linked to one or more data sources with information about that particular product. The product passport enables businesses and consumers access to product information directly from the supplier or other data sources chosen by the supplier. The information may cover the product's sustainability performance, origin, warranty, recycling and instructions for installation or repair.

The Digital Product Passport (DPP) is a set of sustainability data that enables circular products and business models. A consistent digital representation of a physical product creates an improved information exchange along the supply chain, enabling the verification and management of product sustainability [i.5].

A Trustworthy data spaces enable cross-organizational sharing of this data while ensuring integrity, privacy, and compliance.

1) Key Ponents:

    - Data Collection: IoT sensors, blockchain for immutable provenance, and AI for automated data aggregation.

    - Secure Storage: Federated or decentralized storage (e.g. IPFS) to prevent single points of failure.

    - Access Control: Zero-trust architectures with role-based permissions (e.g. consumers see recyclability data; regulators access compliance metrics).

2) Business Value:

   - Sustainability Compliance: Aligns with EU regulations (e.g. Ecodesign for Sustainable Products Regulation).

   - Circular Economy: Enables resale/refurbishment markets by proving product authenticity and history.

   - Consumer Trust: QR codes on products let buyers scan and verify ethical sourcing or carbon impact [i.6].

3) Example:

   - Electric Vehicle Batteries: Automakers, recyclers, and regulators share DPP data to optimize battery reuse, reduce mining of raw materials, and comply with EU Battery Regulation [i.8].

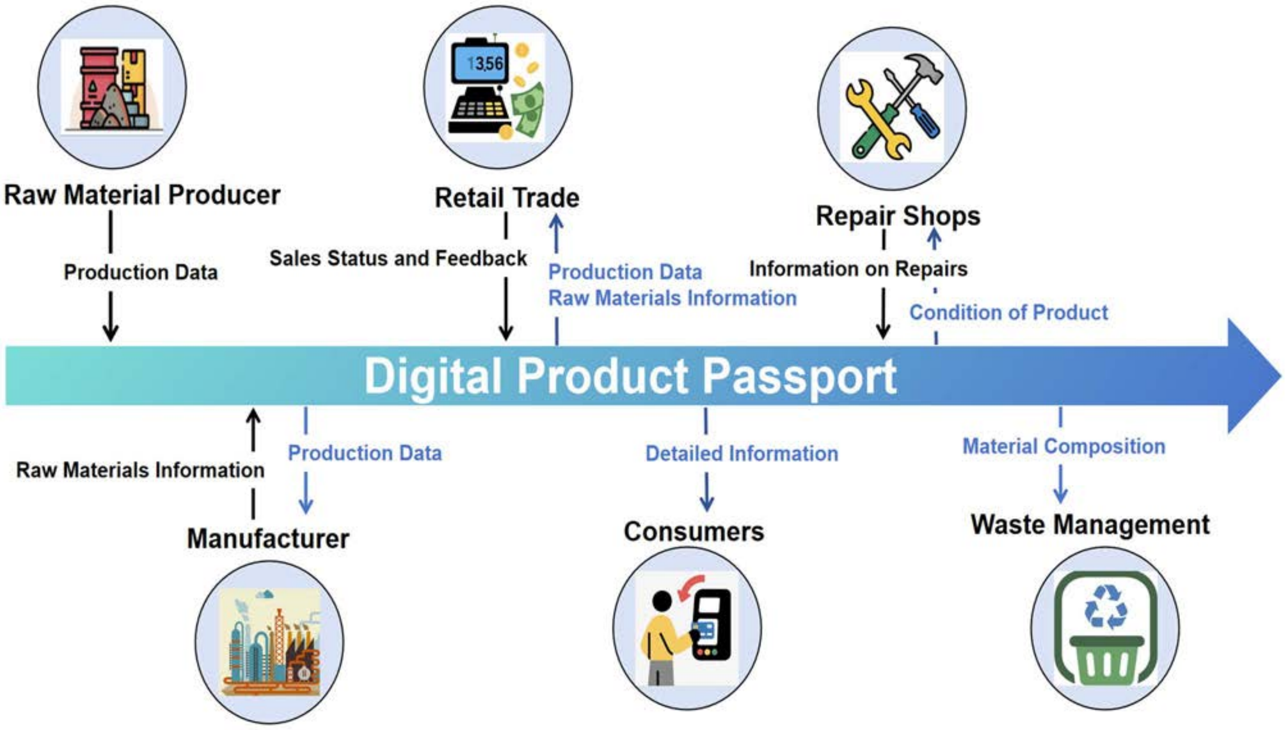

Figure 7: Digital Product Passport

6.2 Use Case 2 - Supply Chain Data Exchange

Secure, real-time data sharing between supply chain partners (suppliers, manufacturers, logistics) to improve transparency, mitigate risks, and streamline operations [i.6].

1) Challenges Addressed:

   - Fragmented Data: Legacy systems create silos; data spaces unify access via APIs and semantic interoperability.

   - Privacy: Confidential business data (e.g. pricing, inventory) is shared selectively using homomorphic encryption or secure multiparty computation.

2) Technical Implementation:

   - Blockchain/DLT: Tamper-proof audit trails for critical events (e.g. customs clearance, quality checks).

   - Predictive Analytics: AI models trained on shared data predict delays (e.g. port congestion) or shortages.

3) Business Value:

   - Resilience: Detect disruptions faster (e.g. geopolitical risks, natural disasters).

- Efficiency: Reduce overstocking via demand forecasting with shared retailer data.

4) Example:

Food Supply Chains: Farmers, transporters, and retailers exchange IoT sensor data (temperature, humidity) to ensure food safety. Smart contracts trigger automatic payments upon delivery confirmation.

6.3 Use Case 3 - Life-Cycle Management

End-to-end data integration across a product's life-cycle (design, production, usage, disposal) to optimize sustainability and operational efficiency [i.7].

1) Key Features:
   - Design Phase: Collaborative engineering data sharing (e.g. 3D models, material specs) with version control.
   - Usage Phase: Predictive maintenance using IoT and AI to analyse equipment performance data.
   - End-of-Life: Track recycling/disposal processes to meet Extended Producer Responsibility (EPR) laws.
2) Technical Enablers:
   - Digital Twins: Virtual replicas of physical assets updated in real time for simulation and decision-making.
   - Data Sovereignty: Tools like Gaia-X ensure companies retain control over shared lifecycle data.
3) Business Value:
   - Cost Reduction: Predictive maintenance cuts downtime by 30 % (McKinsey).
   - Sustainability Metrics: Report Scope 3 emissions using verified supplier data.
4) Example:
   - Wind Turbine Life-cycle: Manufacturers share fatigue sensor data with operators to extend turbine lifespan. At end-of-life, recyclers access material composition data to recover rare earth metals.

7 Development and Application of TDS

7.1 Development Status

7.1.1 Key Milestones in TDS Development

Technical & Regulatory Evolution:

- Phase 1 (2016 - 2018): Foundations:
  1) Emergence of International Data Spaces Association (IDSA) reference architecture.
  2) Early blockchain pilots (Hyperledger Fabric for enterprise data sharing).
- Phase 2 (2019 - 2021): Standardization:
  1) GAIA-X launched as EU's federated data infrastructure.
  2) European Data Governance Act (DGA) proposal (2020).
- Phase 3 (2022 - Present): Industrial Adoption:
  1) Catena-X (automotive) and EHDS (healthcare) operationalize TDS.

2) NIST Post-Quantum Cryptography (PQC) standards integrated into TDS protocols.

7.1.2 Challenges and Limitations

1) Technical Barriers:

- Scalability: Blockchain-based TDS struggle with throughput (e.g. 100 TPS versus IoT's demand for 10 000 + TPS). Solutions like sharding (e.g. Ethereum 2.0) are experimental.

- Interoperability: Competing standards (GAIA-X versus IDSA) create vendor lock-in risks.

2) Regulatory Fragmentation:

- GDPR's "right to erasure" conflicts with blockchain immutability. Hybrid approaches (e.g. off-chain consent logs) are nascent.

3) Adoption Hurdles:

- Legacy systems in manufacturing/healthcare resist TDS integration due to API incompatibility.

7.2 Future Trends

7.2.1 Technological Innovation-Driven

7.2.1.1 Efficient Consensus Mechanism

1) Shift from PoW/PoS to Hybrid Models:

- Proof of Authority (PoA): Used in Catena-X for enterprise scalability (e.g. 1 000 TPS with known validators).

- Directed Acyclic Graphs (DAGs): Projects like IOTA enable feeless micropayments for IoT devices.

2) Energy Efficiency:

- Emerging Proof of Stake (PoS) variants reduce TDS carbon footprint by 99 % versus Bitcoin.

7.2.1.2 Privacy Computing Fusion

1) Homomorphic Encryption (HE):

- Allows analytics on encrypted EHR data (e.g. IBM's HElib). Latency remains high (~10 times slower than plaintext processing).

2) Secure Multi-Party Computation (SMPC):

- Used in financial TDS for collaborative fraud detection without exposing raw transaction data.

3) Federated Learning:

- Hospitals train AI models on local data, sharing only gradients (e.g. NVIDIA Clara™).

7.2.1.3 Collaboration Between Blockchain and AI

1) Smart Contracts + AI Oracles.

EXAMPLE: Dynamic GDPR compliance checks via Chainlink oracles verifying consent revocation on-chain.

2) AI-Driven Wealth Management Personalization:

- JPMorgan Chase is advancing the frontier of personalized financial services by implementing AI-driven solutions in wealth management [i.9].

7.2.2 Deep Integration of Law and Compliance

7.2.2.1 Dynamic Compliance Framework

1) Machine-Readable Policies:
    - RegTech tools auto-validate smart contracts against MiCA/GDPR.
2) Tokenized Legal Contracts:
    - Accenture's TDS prototypes use NFTs to represent data usage rights [i.10].

7.2.2.2 Global Legal Alliance

1) UN/ITU Data Sovereignty Group:
    - Drafting cross-border TDS governance principles (expected 2025).
2) EU-US Data Privacy Framework:
    - Aligns TDS with Schrems II rulings.

7.2.3 Multi-Field Application Expansion

1) Smart Cities:
    - Barcelona's DATAUNION TDS monetizes traffic/air quality data [i.11].
2) Agriculture:
    - John Deere's FarmSight shares equipment data with agritech startups via TDS [i.12].

7.2.4 Infrastructure Optimization

1) Edge Computing:
    - Siemens MindSphere processes factory data locally before TDS upload.
2) 5G/6G Integration:
    - Ericsson's TDS trials achieve < 1 ms latency for industrial IoT [i.13].

7.2.5 Standardization

7.2.5.1 Current Efforts

1) ETSI ISG CIM:
    - Focuses on interoperability APIs and audit logging.
2) ISO/IEC DIS 27090:
    - Security guidelines for TDS authentication [i.16].

7.2.5.2 Gaps and Roadmap

1) Missing Metadata Standards:
    - Hinders cross-sector searches (e.g. a "temperature" field in healthcare versus manufacturing).
2) 2026 Goal: ETSI-led unified semantic layer for TDS.

7.3 Applications in Different Industries

7.3.1 Communication Field

- Use Case:

  Telecoms share anonymized 5G network data via TDS to optimize coverage. Telecom operators utilize TDS to share anonymized 5G network data (such as coverage analysis) in compliance with the interoperability specifications of 3GPP TS 23.501 [i.1].

- Tech:

  Zero-Knowledge Proofs (ZKPs) verify data quality without revealing user locations.

7.3.2 Financial Field

- Use Case:

  MAS's Project Guardian, in combination with the zero-trust model [i.3], achieves a balance between privacy protection and regulatory compliance.

- Regulation:

  MiCA mandates TDS for crypto asset reporting.

7.3.3 Industrial Field

- Use Case:

  Siemens' TDS enables predictive maintenance via shared machine data (vibration, temperature).

- Challenge:

  Legacy OPC-UA systems require middleware for TDS compatibility.

7.3.4 Energy Field

- Use Case:

  Energy Web's TDS lets prosumers sell solar data to grid operators [i.14].

- Tech:

  DID-based identity for meters + smart contracts for settlements.

7.3.5 Data Element Domain

- Use Case:

  IOTA-based data marketplaces enable sovereign data trading (e.g. weather data for insurers).

- Innovation:

  Tokenized data licenses as NFTs (e.g. Ocean Protocol®).

8 Conclusions and Recommendations

8.1 Summary

Trustworthy Data Spaces (TDS) represent a paradigm shift in secure, ethical, and decentralized data ecosystems. By integrating Permissioned Distributed Ledger (PDL) technology, TDS addresses critical challenges in modern data governance, enabling the following innovations:

1) Core Concepts of Data Spaces:

   - Decentralization: Eliminates reliance on centralized authorities, distributing data control across nodes to enhance resilience and sovereignty.
   - Interoperability: Enables seamless data exchange across heterogeneous systems via standardized APIs and semantic models.
   - Data Sovereignty: Ensures compliance with jurisdictional regulations through geo-specific governance and user-controlled permissions.
   - Trustworthy AI: Supports federated learning and privacy-preserving analytics to derive insights without compromising confidentiality.

2) Blockchain-DLT Synergy:

   - Immutable Auditability: Blockchain's tamper-proof ledger ensures traceability of data transactions.
   - Smart Contracts: Automate compliance and enforce dynamic data-sharing agreements.
   - Decentralized Identity: Self-Sovereign Identity (SSI) frameworks replace centralized credential systems, enhancing privacy and user control.
   - Scalable Consensus: Hybrid mechanisms balance throughput with energy efficiency.

Use cases such as Digital Product Passports and Supply Chain Data Exchange demonstrate how TDS bridges technological innovation with real-world applications, fostering transparency, sustainability and regulatory alignment.

8.2 Recommendations

To accelerate the adoption of TDS and maximize the potential of blockchain-DLT integration, stakeholders should prioritize:

1) Technical Advancements:

   - Hybrid Consensus Models: Combine PoA with sharding or DAGs to balance scalability and energy efficiency.
   - Post-Quantum Cryptography (PQC): Proactively address quantum computing threats to cryptographic systems.
   - Federated Learning and SMPC: Enable privacy-preserving analytics across distributed data silos.

2) Regulatory and Governance Alignment:

   - Dynamic Compliance Frameworks: Develop machine-readable policies to reconcile blockchain immutability with GDPR's "right to erasure".
   - Global Standards: Collaborate with bodies like UN/ITU to harmonize cross-border data governance and certification processes.
   - MiCA Compliance Integration: MiCA regulations into TDS frameworks to standardize crypto asset reporting, ensure legal clarity for tokenized data transactions, and align with EU's crypto governance norms.

3) Cross-Industry Collaboration:

   - Consortia-Driven Pilots: Expand initiatives like Catena-X (automotive) and EHDS (healthcare) to validate TDS architectures in diverse sectors.

   - Legacy System Integration: Invest in middleware for API compatibility.

4) Standardization and Interoperability:

   - Unified Metadata Schemas: ETSI and ISO/IEC should lead efforts to standardize semantic layers.

   - Open-Source Toolkits: Promote adoption of PDL frameworks with prebuilt connectors for IDSA and GAIA-X.

By embracing these strategies, TDS will evolve into a cornerstone of ethical, resilient, and scalable data economies, driving innovation while safeguarding user rights in the Web 3.0 era.

Annex A: Bibliography

- Hao Xu, Yunqing Sun, Zihao Li,Yao Sun, Lei Zhang, and Xiaoshuai Zhang: "deController: A Web3 Native Cyberspace Infrastructure Perspective". August 2023, IEEE Communications Magazine.

- Hao Xu, Yunqing Sun, Xiaoshuai Zhang, Erwu Liu and Chih-Lin I Fellow, IEEE™: "When Web 3.0 Meets Reality: A Hyperdimensional Fractal Polytope P2P Ecosystems". August 2023, arXiv:2308.06829.

- Satoshi NakamotoBitcoin: "A Peer-to-Peer Electronic Cash System". 2008, www.bitcoin.org.

- Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, Srinivasan Muralidharan, Chet Murthy, Binh Nguyen, Manish Sethi, Gari Singh, Keith Smith, Alessandro Sorniotti, Chrysoula Stathakopoulou, Marko Vukolić, Sharon Weed Cocco, Jason Yellick: "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains". April 2017, arxiv.org:1801.10228.

- Protokol: "Digital Product Passport (DPP): The Complete Guide".

History

Document history		
V1.1.1	September 2025	Publication