INTERNATIONAL DATA SPACES ASSOCIATION

BLOCKCHAIN TECHNOLOGY IN IDS

POSITION PAPER ON THE APPLICATION OF BLOCKCHAIN TECHNOLOGY IN THE CONTEXT OF INTERNATIONAL DATA SPACES

Position Paper | Version 1.0 | March 2019

Position Paper of members of the IDS Association
Position Paper of bodies of the IDS Association
Position Paper of the IDS Association
White Paper of the IDS Association

TNO innovation for life IBM Fraunhofer

Publisher

International Data Spaces Association
Anna-Louisa-Karsch-Str. 2
10178 Berlin
Germany

Editor

Sebastian Steinbuss,
International Data Spaces Association

Contributing Projects

http://amable.eu

https://midih.eu

http://boost40.eu

http://market40.eu/

https://www.fraunhofer.de/en/research/light-house-projects-fraunhofer-initiatives/industrial-data-space.html

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMMEUNDER GRANT AGREEMENT NO 768775, 780732, 822064, 767498

Authors & Contributors: Matthijs Punter, TNO
Fabiana Fournier, IBM
Inna Skarbovski, IBM

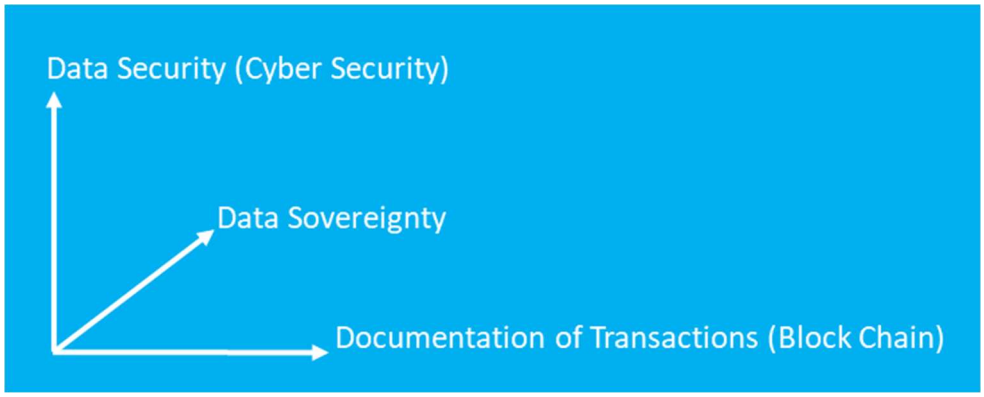
Prof. Dr. Jan Jürjens, Fraunhofer ISST
Dr. Bernhard Holtkamp, Fraunhofer ISST
Sebastian Steinbuss, IDSA

Preamble

The International Data Spaces Association aims at open, federated data ecosystems and marketplaces ensuring data sovereignty for the creator of the data.

Today, there is a common understanding that data is of high value. Leveraging this value and trading data creates huge revenues for the large data platform providers. Rarely, the creators of data are benefitting from this value in an adequate way. Often, only the cost for data creation and management remain with them. Furthermore, many give their data away for free or pay with it for the use of a service. Finally, others keep it for themselves without taking advantage of the value.

There is a need for vendor independent data ecosystems and marketplaces, open to all at low cost and with low entry barriers. This need is addressed by the International Data Spaces (IDS) Association, a nonprofit organization with today about 100 members from various industrial and scientific domains. The IDS Association specified an architecture, interfaces and sample code for an open, secure data ecosystem of trusted partners.



Trust between participants and data-sovereignty are placed at the heart of the IDS: They will be guaranteed to data providers in terms of e. g. who is using their data, for how long, for which application, how many times and under which terms & conditions. However trust can only be established by a common understanding of Data Security and by application of current cyber security measures.

The creation of data-driven business-ecosystems and data marketplaces can only be successful by providing a mechanism for the documentation of transactions for billing, clearing, provenance tracking, and more. Blockchains and Distributed Ledger Technologies are suitable, mature, and accepted technologies for the application in data-driven business ecosystems. This document represents the current state of discussion among the members of the IDSA regarding the use of Blockchain.

Dr. Reinhold Achatz
Chairman of the IDSA Board

Blockchain technology

In recent years there has been a significant growth of interest and investment in Blockchain technology with a many companies and government organisations, large and small, proposing applications of this technology across a range of social, financial, industrial, and governmental sectors. Blockchain technology is seen as providing opportunities to disrupt traditional products and services. This is mainly due to features such as the absence of a single trusted third party, the immutability of the blockchain record, the distributed, decentralised nature of blockchains, and the ability to run smart contracts.

The International Data Spaces (IDS) reference architecture focuses on the concept of 'data sovereignty', allowing organizations to share datasets in a secure and controlled way using the International Data Spaces Connector concept. Some of the features of blockchain technology are consistent with features of the International Data Spaces architecture, such as the absence of a single trusted party (e.g. where all data is being stored) and the decentralized nature. Other features are complementary, such as the permanence of the blockchain record. This makes it highly interesting to explore how IDS and blockchain technology fit together and how blockchain technology could be used in future versions of the International Data Spaces reference architecture.

IN THIS DOCUMENT WE WILL HIGHLIGHT:

- The core concepts of blockchain technology
- Potential usage scenarios for blockchain technology in an IDS context
- Possibilities for implementing IDS architectural concepts using blockchain technology
- How several projects currently use IDS in combination with blockchain technology

1 Core Features of Blockchain Technology

BLOCKCHAIN AS A "PEER-TO-PEER BASED DISTRIBUTED DATABASE"

Blockchain technology essentially integrates networks with databases resulting in a peer-to-peer based distributed database spread across multiple entities, with no single owner or single point of failure. This means that for data stored in a blockchain:

- The technology removes the need for trust in individual endpoints because immediate synchronisation ("near real time") across entities participating in the blockchain takes place, meaning no single trusted third party is needed to guarantee that the transaction occurs.
- Blockchain technology also guarantees a permanent record because no data is ever deleted only appended. Blockchain technology makes extensive use of cryptography in order to prove identity and authenticity using digital signatures.

BLOCKCHAIN AS A DISTRIBUTED COMPUTER: 'SMART CONTRACTS'

Blockchain technologies were first developed as part of the Bitcoin cryptocurrency but are now believed to offer many other capabilities. The recent development of Ethereum (and similar initiatives like Hyperledger) envisage the blockchain as a distributed computer capable of running (relatively simple) programs called "smart contracts". Based on changes in the data stored in the blockchain such 'smart contracts' could automatically trigger further actions without the intervention of one of the participants in the blockchain. For example: automatically triggering a payment transaction when goods have been received. Some experts indicate that these two capabilities (distributed database together with smart contracts) provide an opportunity to develop "distributed autonomous organisations" (DAOs), run by software and entirely outside of the control of individual or institution.

PERMISSIONED VS. PERMISSIONLESS BLOCKCHAINS

Early blockchain technologies applied the concept of 'permissionless' blockchains. This meant that anyone being able to physically access the blockchain could read and write data in the blockchain. This is for instance the case in the use of blockchains for cryptocurrencies (e.g. bitcoin): in this case it is needed for anyone to be able to exchange bitcoins – without any restrictions. When using blockchains in a more closed business community it becomes important to be able to govern the roles and rights of the various participants. Some might only read data, whereas others can also add or change data in the blockchain. In this case the term 'permissioned blockchain' is used. This allows for using blockchains in a more closed user group, thus more adequate for business networks. This is important in the context of International Data Spaces, given the principle of data sovereignty.

IMPLICATION OF THESE FEATURES

Putting these three characteristics together has made many researchers, entrepreneurs, and pundits predict that the technology will revolutionize a large number of different commercial sectors from finance and insurance, through health records and tax collection, to supply chains, the music industry, as well as the financial industry:

- It enables new solutions for providing visibility in the supply chain, thereby reducing risks for participants in that chain.
- It changes the roles of existing intermediaries as the blockchain facilitates built-in consensus approaches. In new platform business models this strengthens the position of the asset-holder, whereas in more centralized approaches much of the market power and profit margin shifts to the new intermediary.
- It still requires businesses to consider matters such as governance models, semantics of the data being shared and the technologies used: e.g. is a permissionless blockchain an option or is a permissioned approach more feasible? Should all data be put in one blockchain? Or is a set-up needed with multiple blockchains?

2 Potential Use for Blockchains in an international Data Spaces context

SHARED DATA ASSETS

The core feature of IDS is to enable the controlled sharing of data between organizations - regardless of the type of data. In many International Data Spaces use cases this is some form of structured data. For example: measurements, product data, or logistics/procurement data. But also other types of (streaming) data is being supported. The IDS Connector allows for sharing this data with other participants in the IDS ecosystem, whereby the owner of the data can control – through its Connector – with whom this data is being shared.

This data sharing is done for various purposes, but in use cases we often see two different patterns:

- The sharing of data to feed new data driven services: using the data in a new app, smart algorithm or other digital service in which data of different sources/providers is combined.
- The sharing of data for some form of business process synchronization: using the data to commit transactions (e.g. exchanging orders), enable production (e.g. exchanging product data), check quality (e.g. the temperature of perishable goods), or to synchronize processes (e.g. exchanging status data).

In many of these cases the data leads to transactions whereby the data itself becomes what one could call a 'shared data asset' with a liability/responsibility for the participating organizations. The data has become – in a way – a joint or shared asset.

For example:

- Because of a too high temperature of perishable goods the person ordering them might decide to refuse accepting the goods. In this case the temperature has become a shared data asset and their might be a need to store this fact in a shared environment which acts as a trusted record keeper of such quality data.
- Organizations wanting to share their capabilities (e.g. to produce a certain type of goods). In this case, this capability becomes a shared data asset to be stored in a shared 'yellow pages' accessible for all.

From a functional perspective we expect blockchain technology – given the core features we explained before – to play an important role in maintaining these 'shared data assets' in an IDS environment.

This complements the existing capabilities of the IDS architecture to share (potentially large) datasets through its connector architecture. For instance: the shared data asset might encompass a hash code ('fingerprint' of a piece of data) which can be used to verify a larger file (e.g. a complex product design for which an order was sent) being shared through an IDS connector.

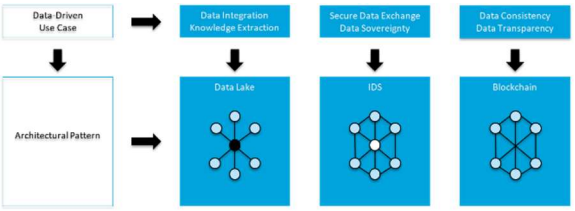


Figure 1 General architectural patterns for data exchange and data sharing

In general, the use of Blockchain technology can ensure data consistency and transparency in a network of organizations. This complements the general general IDS approach for data sovereignty and secure data exchange and sharing. Both can leverage existing data-integration set-ups within organizations (e.g. internal Data Lakes for the purpose of knowledge extraction); see figure 1.

AN IDS BLOCKCHAIN "APP"

There are two options when a business community decides to store shared data assets in a blockchain and make this data accessible to the IDS ecosystem.

- The blockchain acting as a data consumer: in this case certain data from the IDS ecosystem needs to be registered in a blockchain. For instance a measurement which has taken place or certain sensor data.
- The blockchain acting as a data provider: in this case the blockchain contains data which needs to be made accessible to other parties in the IDS ecosystem. For instance, certain transaction data recorded on a blockchain.

The IDS architecture provides a key mechanism to enable such integration, namely the

so-called 'data apps' in a Custom Container (see figure 2) Such apps are linked to an IDS Connector and facilitate the integration of IDS with external systems. Such data apps can be used for instance to link a Connector to a REST-API of an existing ERP system or to an OPC-UA interface of a smart device.

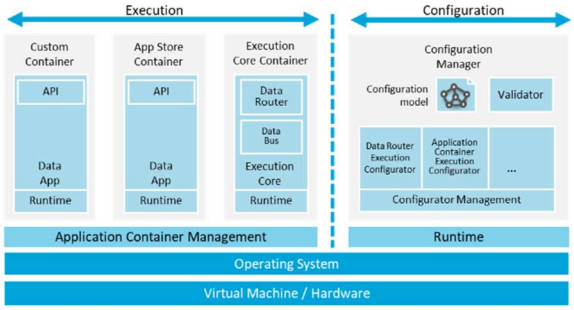


Figure 2 Connector Architecture as in IDS-RAM 3.0

Typical blockchain implementations consist of nodes (which 'synchronize' data amongst each other) which contain or are connected to client applications. Such a client application sometimes contains a user interface, but often also contains an API through which other systems can access data on the blockchain.

An IDS 'data app' connects to this API and exposes its functions in the IDS ecosystem 9see Figure 3). Such data apps have been developed for Hyperledger Fabric in several IDS projects and are under construction for BigChainDB. It should be noted however that such integrations are on both a technical and semantic level.

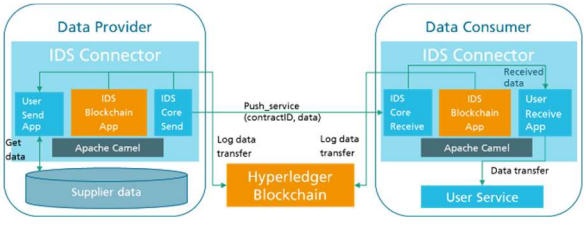


Figure 3 Example for Blockchain App wih Hyperledger in IDS Connector

A key challenge which still needs to be addressed in detail in use cases is the topic of identity management. Preferably such an identity management schema is linked between the distributed ledger and the IDS Connector environment. For instance: the usage of the same certificate scheme in both the blockchain and the IDS Connector environment. The Identity provider as defined in the IDS Reference Architecture can play an important role here.

Using blockchain for Identity management

There are currently several initiatives aiming to adopt blockchain technology for identity management. In these concepts actors can specify their identity in the blockchain (self-sovereign identities) which are then verified by a third party. The result, being stored on the blockchain, is exchangeable with other parties.

An example of this approach are the re:claimID (www.reclaim-identity.io) and Sovrin (www.sovrin.org) initiatives (). They are opportunities for the future how such approaches might be able to implement the identity provider role in the IDS architecture

3 Potential for Implementing IDS Architectural concepts using Blockchain

Apart from using blockchain in specific use cases through an IDS Blockchain app, it is also imaginable to use blockchain technology to implement certain key architectural concepts of the IDS Reference Architecture.

Apart from the aforementioned identity management approach, this mostly relates to the IDS Broker and the IDS Clearing House.

BROKER IN A BLOCKCHAIN

The IDS Broker acts as a 'registry' of connected data sources. It is possible to query the broker to find out which Connectors are available in the ecosystem and what kind of data

they provide. This information (metadata) is expressed using the IDS Information Model. An IDS Connector needs to be registered in a Broker to enable such search-and-find functionality.

The IDS Broker however needs to be hosted by a service provider in the specific ecosystem which it serves. When there is an overlap of ecosystems the broker needs to be synchronized with others, so actors in the (sub-) ecosystem can retrieve data from other ecosystems. This would imply that in the future there should be an ecosystem of brokers.

It would be imaginable to replace this ecosystem in the future through a blockchain based approach. In this case data providers and consumers could declare their Connector on the blockchain – using the very same IDS Information Model to provide the minimum required set of metadata. When the Connector is certified, the certification provider could also add this information. A key challenge here is the immutability of data on the blockchain: actors should again declare when the Connector is no longer available or no longer certified.

BLOCKCHAIN BASED CLEARING HOUSE

Another fundamental concept of the IDS Reference Architecture is that of the Clearing House. The Clearing House keeps track of data transactions between IDS participants and is thus a prerequisite for data-driven business models in which the consumption of data is billed.

In traditional centralized architecture, the role of the Clearing House is taken by a trusted authority that is notified about billable transactions and appends them to an audit log. During the clearing process, transactions from the log are settled in a batch and participants are billed with respect to the recorded events. However, this approach comes with two drawbacks: first, all participants must agree on a single central party that they fully trust and that consequently becomes a single point of failure for the whole system. Second, the clearing process is limited to what the central clearing house supports. As long as billing only refers to the transfer of data from one party to another, the clearing process is easy. However, in the case of complex chains of transaction across several stakeholders, the clearing process quickly becomes complex and must be separated from the maintenance of the actual transaction log.

Consider for example an industrial supply chain where goods are transported from a supplier to a manufacturer. The process involves not only the sender and receiver, but also insurances that will stand in for costs that result from specific events, customs, and export regulation officers who sign for the legality of the transport, and carriers which need to prove that they passed the good to the next hop in the chain in time and intact.

Data Provenance Tracking

Data provenance tracking is closely related, but also complementary to distributed data usage control. It has its origins in the domain of scientific computing, where it was introduced to trace the lineage of data. Data provenance tracking thereby allows finding out when, how, and by whom data was modified, and which other data influenced the process of creating new data items.

This kind of traceability is similar to the data protection requirements a data controller is confronted with, so as to be able to fulfil its data subjects' right to access. It is also closely related to the question of proving compliance with contracts, agreements, or legal regulations. And data provenance tracking can be used to facilitate clearing in decentralized data ecosystems, since it is capable of aggregating information concerning data exchange transactions and data usage.

The operating principle of data provenance tracking is very similar to the operating principle of distributed data usage control. Data provenance tracking relies on passive monitoring technology (e.g., PEPs), which deliver events indicating data usage or data flows for being logged. For this, a PEP needs to convey a semantic description of the data usage or

data flows its events indicate. The data provenance tracking infrastructure provides a data flow tracking component, which understands such semantics specifications. The PEP also needs to forward events together with metadata (including a unique identifier of the data's content), so that logged transactions can be attributed to data content when data provenance is aggregated or queried. The logging of the data can be realized using a centralized approach or using a decentralized approach like Blockchain. In particular, the immutability nature of blockchain can play an important role here.

4 IDS Projects Appling Blockchain Technology

Several IDS-based projects have already started adopting blockchain technology for specific use cases.

AMABLE

The AMAble project aims to provide a data infrastructure for 3D printing. In the ecosystem of 3D printing the secure exchange of digital designs is very important. For instance, the sharing of a design idea to someone making the detailed design. Or the sharing of the design with a manufacturing company which is actually printing the design or parts of it.

In the AMABLE project, IDS Connectors have been set-up to enable the secure sharing of design between two companies. An organization can select with whom the data will be shared with. Connectors then ensure the secure transfer.

However, in this case not only the secure sharing of data is important but also the guarantee that the manufactured product is compliant with the design. To enable this, a hash code (digital fingerprint) of the design file is stored in a blockchain, which is connected through an IDS app.

Additionally, the functionality has been implemented on a Raspberry Pi, providing a simple 'plug-in' for manufacturers to connect to the ecosystem.

More information can be found at http://www.amable.eu/

BOOST 4.0

The BOOST 4.0 project aims to enhance manufacturing through the use of big data. IDS is used as a cornerstone for this to share data in various use cases.

Within a supply chain use case, Hyperledger Fabric is the blockchain technology applied. Two aspects of integration between IDS connectors and Hyperledger Fabric are considered – the conceptual and technical levels.

Conceptually, scenarios/use cases in which applying each technology by itself can fully meet the requirements are investigated, as well as scenarios in which we need a combination of these two technologies. At the technical level, possible integration mechanisms for those scenarios that require a combination of both technologies have been studied.

The selected implementation consists of a blockchain client which is incorporated as a custom container within a regular IDS connector. The logging of the data transfers is not transparent but rather defined as workflow in the core container. In this implementation the data flow is as follows:

- Data consumer and data providers initiate data requests and response between them respectively
- When this happens the workflow manager within the IDS connector based on explicit workflow specification invokes the AppStore/custom blockchain container which, in turn, communicates with the blockchain infrastructure via its API.

MARKET 4.0

The MARKET 4.0 project aims to develop a marketplace for equipment manufacturers. The key objective is to build a marketplace which puts equipment manufacturers in the driver's seat. This implies that new business models need to be applied, other than the typical 'winner-takes-all' model.

IDS plays a very important role in the project as it is the technology foreseen to provide Connectors to all actors involved, providing them with a tool to share data with other partners in the ecosystem in a secure and controlled way. Also the project aims to have Apps for connecting with simulation tools and other applications.

Blockchain will also be a core part of the architecture of this future marketplace. It will contain a record of transactions between parties. The detailed set-up of this blockchain is currently being investigated at the time of writing (the project started at the end of 2018).

TrackChain

To overcome the drawbacks mentioned in the subsection on the Blockchain based Clearing House, the IDS features a blockchain-based clearing house named TrackChain that keeps track of billable transactions in a blockchain and creates a non-dispudiatable audit log. Further, to solve the notorious privacy problem that occurs when data is written to a public blockchain, the TrackChain system includes a technology called Attribute-Based-Encryption that implements data access control at a cryptographic level. That is, data is encrypted for certain roles before it is stored in the blockchain. Only users who are assigned the respective role are able to read evens from the audit log so that the audit log itself does not contain any confidential data and can be made public.

TrackChain is integrated into the IDS in the form of a data app that can be downloaded from the IDS app store and installed in the Connector. Any event that shall be logged by the TrackChain system can then simply be routed into this app and will be forwarded to the blockchain-backed TrackChain system.

Orbiter

The Orbiter use-case is an automated payment solution based on blockchain technology and secure data sharing for smart mobility and IoT applications.

The identity of the car and its legal owner are verified and stored on the blockchain. An embedded low-energy Bluetooth unit transmits this data to 3rd-party service providers (parking, toll-collect, charging stations etc.). An additional chip verifies the information and authorizes an automated payment transaction.

Thyssenkrupp and IBM

Industrial Additive Manufacturing technology provides numerous benefits to companies if applied in the right way. This requires dedicated engineering expertise that in many cases is not accessible to SMEs without high investment in knowledge and equipment. The platform developed in this common project aims to bring together all participants in the industrial Additive Manufacturing process chain and provides easy access to engineering expertise as well as AM equipment to any customer. Utilizing IDS Connectors and Blockchain Technology this platform creates a scalable trustworthy ecosystem in various industries and beyond Additive Manufacturing where Big Data can be exchanged amongst multiple parties and provenance and immutability assure product quality and intellectual property.

MIDIH

The MIDIH project (Digital Innovation Hub for the Manufacturing Industry) experiments with FiWare and Apache based open source industrial data platforms in the domains of Smart Factory, Smart Product and Smart Supply Chains. In several smart supply chain scenarios distributed ledgers are used to track transactions between the different stakeholders of a dynamic agile value chain.

5 Conclusions and Recommendations

Blockchain technology is a promising and mature technology which is a basis for an increasing number of use cases. In several projects IDS is used in conjunction with blockchain technology.

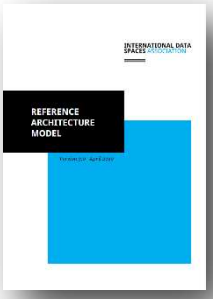
- There are several blockchain technologies available. There is not a 'one-size-fits-all' approach. In addition, other governance aspects continue to play a role: the semantics of data exchange, the rules to be applied, etc.
- Blockchains play an important role when data is considered a 'shared asset', which need to be stored in an immutable way between partners in the ecosystem.
- Within the IDS architecture a 'Blockchain app' can be considered which connect an IDS Connector with the API/SDK of a blockchain client, which in turn is connected to a node in the blockchain. Through this API, data can be shared with the blockchain, either acting as a data provider or data consumer.
- The IDS architecture contains the concepts of a Broker and Clearing house. Both concepts can be potentially implemented using blockchain technology. Implementing the Clearing house using blockchain technology potentially requires an adaptation of the core Connector.
- Identity management remains crucially important, both in IDS and blockchain. When both are used in conjunction, it is important to ensure interoperability between both environments in this regard.
- Several projects are currently exploring the usage of blockchain technology in the context of IDS. It is recommended to follow these developments and adapt the reference architecture when needed.

To learn more, please check out the website for additional information and our reference architecture model (www.internationaldataspaces.org).

Our Members

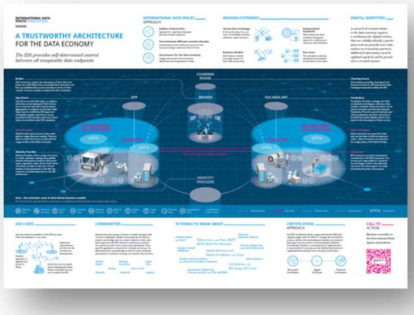

Aalto University
ADVANEO
agmadata
Allianz
Atos
Audi
BAYER
BetterSolutions
bill-X
Boehringer Ingelheim
BOSCH
Brainport Industries
CAICT
CDQ
Cefriel
CERTH
CHALMERS
Cybus
Czech Technical University in Prague
DATAHEAD
DATATRONIQ
DB SCHENKER
Deloitte.
denodo
DGZfP
DR. SCHNEIDER
DHBW
eccenca
EcoDataCenter
ENGINEERING
8760 Fastems
FIWARE
Fraunhofer
GateHouse
HUAWEI
iav
IBM
IK4 TEKNIKER
ILVO
Imperial College London
Institut Mines-Télécom
INDUSTRIE 2025
inmation
innovalia ASSOCIATION
Insight
Irish Manufacturing Research
ITI
i2cat
komsa
koppermann
Leibniz Universität Hannover
Lobster
Logata Digital Solutions
LOGENIOS
LSEC
minnosphere
msg
mtc
nicos AG
orbiter
UNIVERSITY OF PATRAS
POLITECNICO MILANO 1863
pwc
QuinScape
REWE
RITTAL
SALZGITTER AG
SAP
SCHAEFFLER
SETLOG
SICK Sensor Intelligence.
SIEMENS Ingenuity for life
Signal Cruncher
Signal Solutions
SINTEF
SMEV AG
TATA
T
tecnalia
thyssenkrupp
TNO innovation for life
TÜV NORD GROUP
TÜV SÜD
UNIKLINIK RWTH AACHEN
UNISCON Sealed Cloud Technologies
UNITY
universität Witten/Herdecke
VDMA
VOLKSWAGEN
VTT
WELOTEC
ZVEI
Die Elektroindustrie

Overview Publications



Reference Architecture Model

White Paper Certification

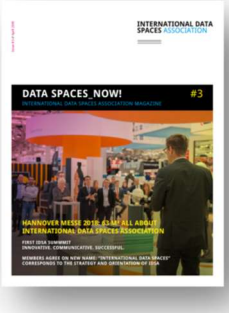


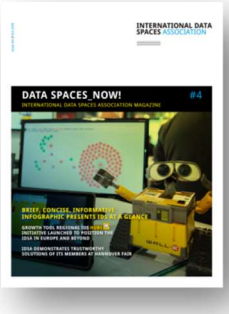
Infographic IDS Ecosystem

Use Case Overview

Study on Data Exchange

Study on Open Data Spaces





International Data Spaces Association Magazine – Data Spaces_now!

Downloads available at **www.internationaldataspaces.org/en/ressource-hub/publications-ids/**

Code available at **https://github.com/industrial-data-space**

CONTACT

Head Office

INTERNATIONAL DATA SPACES ASSOCIATION

Joseph-von-Fraunhofer-Str. 2–4
44227 Dortmund | Germany

phone: +49 231 9743 619
mail: info@internationaldataspaces.org

WWW.INTERNATIONALDATASPACES.ORG

@ids_association