Sovereign IIoT Data Exchange Using DAG-Based DLT and International Data Spaces Architecture

Anhelina Kovach
Ikerlan Technology Research Centre, Basque Research and Technology Alliance
Mondragón, Spain
akovach@ikerlan.es

Jorge Lanza
Network Planning and Mobile Communications Laboratory, University of Cantabria
Santander, Spain
jlanza@tlmat.unican.es

Leticia Montalvillo
Ikerlan Technology Research Centre, Basque Research and Technology Alliance
Mondragón, Spain
lmontalvillo@ikerlan.es

Aitor Urbieta
Ikerlan Technology Research Centre, Basque Research and Technology Alliance
Mondragón, Spain
aurbieta@ikerlan.es

Abstract

Securing interoperable and sovereign data exchange in the Industrial Internet of Things (IIoT) for machine data exploitation by third parties presents a significant challenge. This work addresses this by integrating IOTA Distributed Ledger Technology (DLT) with the International Data Spaces (IDS) Reference Architecture Model (RAM), creating a decentralized data space optimized for IIoT ecosystems. This research demonstrates the practical implementation of core IDS architectural concepts within the IOTA framework, overcoming theoretical DLT limitations and showcasing IOTA's capability to enhance data sovereignty and interoperability in the IIoT, moving beyond traditional blockchains, which are constrained by scalability and efficiency issues. It sets the stage for future evaluations and broader applicability studies, paving the way for advancements in secure, sovereign, interoperable, and efficient data management.

CCS Concepts

• **Computer systems organization** → **Distributed architectures**; • **Security and privacy** → **Information accountability and usage control**; **Distributed systems security**; *Information flow control.*

Keywords

Data Space, Distributed Ledger Technology, Eclipse Dataspace Components, International Data Spaces, IOTA, Self-Sovereign Identity

ACM Reference Format:
Anhelina Kovach, Jorge Lanza, Leticia Montalvillo, and Aitor Urbieta. 2024. Sovereign IIoT Data Exchange Using DAG-Based DLT and International Data Spaces Architecture. In *4th Eclipse Security, AI, Architecture and Modelling Conference on Data Space (eSAAM 2024), October 22, 2024, Mainz, Germany*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3685651.3686658

eSAAM 2024, October 22, 2024, Mainz, Germany

ACM ISBN 979-8-4007-0984-5/24/10
https://doi.org/10.1145/3685651.3686658

1 Introduction

The emergence of Industry 4.0 and the widespread deployment of Industrial Internet of Things (IIoT) devices have transformed industrial ecosystems, positioning data as the core of this new paradigm. The role of data in optimizing processes, enhancing production efficiency, and enabling precise operational monitoring is increasingly evident [32]. This paradigm underscores the necessity for a systematic design and management approach to the entire data lifecycle. This encompasses the creation and collection of data, ensuring its integrity and provenance, secure storage, and efficient exploitation.

Within the IIoT landscape, decentralized storage mechanisms provided by Distributed Ledger Technology (DLT) present a robust approach to data management, significantly enhancing security and immutability, which are crucial for maintaining data integrity and provenance [22]. Incorporating Self-Sovereign Identity (SSI) facilitates secure identification within the industrial ecosystem, ensuring data storage security and enabling precise traceability and provenance verification, thus substantially improving data management across its entire lifecycle.

Leveraging the capabilities of IOTA's Tangle [25], a DLT utilizing a Directed Acyclic Graph (DAG) structure, this article explores its potential as a robust foundation for IIoT applications [28], [15]. The IOTA architecture provides notable benefits for secure, scalable, and efficient data and value transfer in industrial settings. This research builds on a platform previously detailed in [19], which was developed to support a billing model for the use of rented industrial machinery between clients and suppliers. Transactions are securely recorded in the Tangle, extending the foundational scenario illustrated in Figure 1 as the basis for the current study.

Acknowledging the evolving landscape of IIoT, this work aims to extend the platform's capabilities to enable the sharing and monetization of machine-generated data with third parties. The extension focuses on maintaining data sovereignty and secure usage within a broader ecosystem. This includes (*1*) enabling secure data exchange across multiple entities, (*2*) ensuring data sovereignty by enabling control over data access, usage, and compliance with regulatory requirements, (*3*) identifying and authenticating all ecosystem participants and components, (*4*) providing descriptive features, usage terms, and pricing for offered data assets, and (*5*) recording of all operations within the ecosystem.

This evolution necessitates the adoption of data space technology, an emerging solution that fosters secure data exchange under a common framework of trust and governance, facilitated by initiatives such as the International Data Spaces (IDS). This approach,

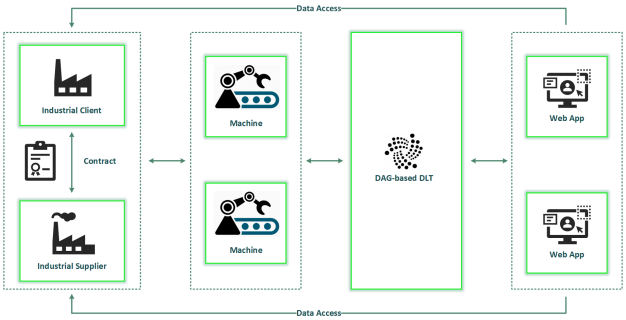

Figure 1: DLT data storage for machine usage billing

which focuses on establishing a shared technical infrastructure, addresses the need for secure, governed, and sovereign data exchange within a unified framework [37], a requirement not fully met by the IOTA framework. While IOTA ensures transaction security and data integrity, it lacks the comprehensive access control, governance, and interoperability across heterogeneous systems needed to establish a common trust framework.

The primary focus of this work is to demonstrate the practical application and benefits of integrating the IDS within the IOTA ecosystem, enabling a use case for data exploitation. By implementing IDS Reference Architecture Model (RAM) [24] architectural concepts into IOTA's DLT and leveraging its frameworks, the integration aims to establish identity management, data cataloging, and logging functionalities, thereby enhancing data sovereignty, sharing, governance, and interoperability. This detailed deployment and operation of the IOTA framework highlight its capacity to meet the demands of the data spaces domain. Furthermore, it illustrates how these advancements pave the way for empirical evaluation and continuous improvement in industrial settings, ultimately facilitating data sharing across IIoT platforms.

This article is structured as follows: Section 2 introduces concepts such as DLT, SSI, and the data space paradigm, mainly focusing on the IDS architecture. Section 3 reviews related work and its limitations. Section 4 elaborates on the processes to be implemented in the data space, while Section 5 introduces the proposed IOTA-enabled data space architecture. Section 6 details the architecture's implementation and participant interactions. Section 7 concludes by outlining future directions for this research in progress.

2 Background

This section provides an overview of distributed ledgers, particularly DAGs and its implementation on IOTA technology. It then introduces SSI concepts and delves into the data spaces paradigm and the initiative of the International Data Spaces Association (IDSA).

2.1 Distributed Ledger Technology

DLT encompasses distributed systems for data management, utilizing a network of nodes for decentralized control, thus enhancing transparency and consensus in data validation to identify malicious activities. In particular, blockchain and DAG-based networks are the two primary forms of DLT. Blockchain operates through a sequential chain of immutable transaction blocks, while DAG-based DLTs utilize directed graph structures to link transactions, enabling mutual validation. This approach improves scalability by facilitating the efficient processing of large volumes of transactions.

While blockchain faces scalability issues, transaction fees, and latency bottlenecks that degrade network performance [18], DAG technology overcomes these challenges. It provides a viable solution for high-throughput environments such as IIoT by eliminating transaction fees, enabling micro-transactions, and improving network agility and scalability through the multiple access points of its graph structure [29]. At a more practical level, IOTA's Tangle, a DAG-based DLT, not only overcomes blockchain's limitations but also provides a comprehensive ecosystem of solutions and frameworks for deploying additional services on its underlying network.

2.2 Self-Sovereign Identity

The SSI technology represents a significant advancement in data sovereignty, giving individuals complete control over their digital identities and challenging traditional intermediary-based identity management systems. This innovation allows users to control the specifics of data sharing, determining what data is shared, the terms of sharing, and the parties involved. At the core of SSI are digital identities and their associated Verifiable Credential (VC).

Digital identities, enabled by Decentralized Identifier (DID) [1], provide a decentralized and verifiable approach to digital identity, eliminating the need for centralized authorities [17]. A DID acts as a unique identifier pointing to a DID document containing verification methods, all stored on a secure ledger.

Complementing digital identities, VCs [2] attach attributes and claims to an identity authenticated by various verification methods. The SSI ecosystem includes key actors integrated into the narrative: (*1*) a Holder who owns VCs and can create a Verifiable Presentation (VP) for identity verification, (*2*) an Issuer who asserts claims on a subject and converts them into VCs for the holder, (*3*) a Verifier responsible for validating VPs against a data registry, and (*4*) a Verifiable Data Registry that maintains and verifies digital identities and their associated public keys, primarily through DLT.

2.3 Data Spaces

Data spaces are a distributed data integration concept where data providers deliver their data to consumers under a common technical and legislative standardized framework. Participants can contribute data while maintaining sovereignty over what data is shared, by whom, and for how long. This model ensures trust in data interactions and fosters an economic environment centered on data sharing while maintaining privacy and security [23].

On a legislative level, the European Union (EU) data spaces concept is driven by policies such as the European Strategy for Data [8], designed to enhance data access, sharing, and governance and aims at integrating sector-specific data spaces into a unified data market for the EU. Together with the General Data Protection Regulation (GDPR) [9], which ensures data protection and privacy, the framework is further strengthened by the Data Governance Act [10] and the Data Act [11]. These legislative components collectively shape

[1] https://www.w3.org/TR/did-core/
[2] https://www.w3.org/TR/vc-data-model-2.0/

a robust legal framework that underpins the European Strategy for Data, guiding the development of sector-specific data spaces and ensuring that data is accessible and governed by clear regulations.

The IDSA is an organization that unites numerous industrial actors [35] to provide a technology-agnostic and standardized description of a data space software architecture. It focuses on facilitating trustworthy data exchange between data providers and consumers, ensuring that all participants adhere to a common trust framework.

The IDS, developed and maintained by the IDSA, and Gaia-X are emerging as major initiatives in advancing data space frameworks rooted in the principles of data sovereignty and trust. The IDSA promotes a secure, decentralized framework for sharing data assets, while Gaia-X focuses on building federated cloud services across multiple providers. Unlike the more centralized, certificate-based X.509 approach described in the IDS RAM [24], Gaia-X implements a decentralized identity management system that leverages self-descriptions and VCs for services and participants [12].

A key enabler for participating in the data space is the connector, which ensures data sovereignty throughout the data lifecycle. Connectors do more than facilitate data transfers; they also provide functionalities for discovery, connection, contract negotiation, policy enforcement, and transaction auditing [14].

The IDS architecture is divided into five layers: business, functional, process, information, and system. Participants are described on the Business Layer and classified into four categories concerning their role in the data space [3], as shown in Figure 2:

(1) **Core Participants**: Entities involved and required every time data is exchanged.
   - Data Owner/Provider: Generates or owns data introduced into the IDS ecosystem. This implies the creation of data, establishing usage contracts, and setting policies to define how data can be accessed and used.
   - Data Consumer/User: Searches for data within the IDS and logs transaction details in the Clearing House.

(2) **Intermediary Participants**: Trusted entities in charge of establishing trust, providing metadata descriptions, and creating business models around offered services.
   - Broker Service Provider: Maintains a repository of data sources within IDS, offering an interface for submitting and retrieving descriptive metadata [2].
   - Clearing House: Manages data transaction services within the IDS, ensuring accurate logging for billing purposes and data transfer validation [1].
   - Identity Provider: Entity responsible for creating, managing, and validating identities within the IDS. This includes a Certification Authority (CA) to issue digital certificates, a Dynamic Attribute Provisioning Service (DAPS) to attach properties, and a Dynamic Trust Monitoring (DTM) for enhanced network security.
   - Vocabulary Provider: Oversees the management of data models and metadata elements for the proper annotation and description of datasets in the IDS.
   - App Store Provider: Distributes Data Apps, providing tools for data processing workflows.

(3) **Service Providers**: IT entities providing Software as a Service (SaaS), encompassing hosting infrastructure and data services for data quality enhancement and supplying software essential for IDS connector functionalities based on agreements between providers and consumers.

(4) **Governance Body**: Entities collaborating on the certification processes of IDS components and participants. It includes the IDSA itself as the main developer of the RAM and coordinator of working groups on specific data space implementation and governance aspects.

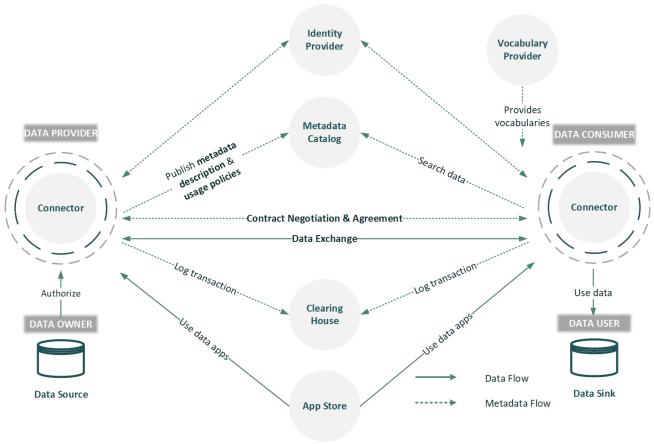

Figure 2: IDS architecture based on IDS RAM [24]

The IDSA is developing the Dataspace Protocol (DSP) [16], which is becoming the basis for the technical development of the Eclipse Dataspace Components (EDC) [3]. The protocol defines component interactions and is the technical specification for the IDS RAM. It is divided into four domains:

(1) Data space model and terminology: Creates the foundation for interoperability among participants through defined ontologies and taxonomies.

(2) Catalog protocol: Elaborates on data description, publication, and retrieval mechanisms, adhering to the W3C Data Catalog Vocabulary (DCAT) [4].

(3) Contract negotiation protocol: Delineates the interactions for establishing mutually agreed contracts, ensuring that terms of data access and usage rules are consented, framed by the W3C Open Digital Rights Language (ODRL) [5].

(4) Transfer process protocol: Details the data transfer procedure post-contract agreement, focusing on the transfer states rather than the exchange protocols used.

3 Related Work

Research in the data space domain is actively exploring the integration of Internet of Things (IoT) devices with DLTs to adapt data spaces for IoT environments. This includes leveraging communication protocols for automated data exchange processes [21][27]. Concurrently, the potential of blockchain to enhance the IDS RAM architectural concepts is recognized, with the IDSA investigating

[3] https://github.com/eclipse-edc
[4] https://www.w3.org/TR/vocab-dcat-3/
[5] https://www.w3.org/ns/odrl/2/

its application in data storage and cataloging. The use of blockchain within the IDS framework is discussed in [36] for implementing:

- **Identity Provider**: This role involves integrating the ledger with the IDS connector environment using a consistent certificate schema. Blockchain technology serves as the enabler for decentralized identity management.
- **Broker Service Provider**: The registry of connectors and their available data offerings can be listed on the blockchain. However, due to the immutable nature of DLT, modifying offerings requires uploading new entries for any changes.
- **Clearing House**: Monitoring technologies based on the eXtensible Access Control Markup Language (XACML) [6] architecture generate events indicating data usage and enforce access control policies. These logs can be stored on a blockchain for enhanced security and traceability.

Further extending the potential roles of blockchain in data spaces, Prinz et al. [26] have explored the use of blockchain for executing smart contracts, which can enforce rules within a data space, facilitating authorization and control of access and usage. Additionally, the Data Spaces Support Centre (DSSC) blueprint [7] document highlights the potential of blockchain for decentralized identity management and the storage of participants' identities.

Practical applications of DLT in data spaces have been discussed without detailed technical specifications of their nature or exact implementation. For instance, Meneguzzo et al. [20] [30] describe the use of blockchain to implement a data catalog of energy datasets, while the actual data transfer and control processes are managed via data space connectors. Similarly, Sayad et al. [31] cover the adoption of an unspecified type of DLT for exchanging information regarding threats or cyber-attacks on critical infrastructure.

This work bridges the gap between theoretical blockchain studies and practical applications by focusing on a DAG-based DLT like IOTA's Tangle, which is particularly suited for IIoT environments. Unlike previous research that overlooks the practical implementation and benefits of alternative DLT types, this study integrates specific architectural components within the IOTA framework. These components include an Identity Provider, Broker Service Provider, Clearing House, and a wallet service for secure transactions. Additionally, it addresses practical challenges within data spaces, such as onboarding, data offerings, and exchange procedures, to create a data-sharing ecosystem for the secure exploitation of data.

4 Processes for IIoT Data Exploitation

This work focuses on securely sharing machine-generated data, applying the architecture and protocols outlined by the IDSA to the IOTA ecosystem, adapting the processes described on the Process Layer of the IDS RAM [24]:

- **Onboarding**: Adjusted to encompass the registration, identification, and management of participants within a data space, extending beyond the original scope of connector provision and certification.
- **Data Offering**: This involves describing data assets using the DCAT ontology, outlining usage policies with ODRL, and specifying pricing within the service catalog.
- **Contract Negotiation**: Concentrates on negotiating contract terms between data consumers and providers, highlighting the automation of parameter negotiation and formulating the final contract as critical challenges.
- **Exchanging Data**: This work adopts a decentralized model where each participant maintains their own DLT for data storage. It focuses on ensuring secure access through access control mechanisms and Policy Enforcement Point (PEP)s, with IOTA's DLT employed for storing participant data.
- **Policy Enforcement**: Pertains to the technical enforcement of data usage policies related to data assets, especially concerning the consumer and end-user side, to guarantee correct and compliant data usage.

While the IDS RAM acknowledges the potential development of Data Apps, this initial phase of this work does not include them. However, there is scope for incorporating such functionality through Data Apps in future work.

5 Proposed Architecture

Figure 3 illustrates the proposed architecture, which integrates three core services: an Identity Provider, a Broker Service Provider, and a Clearing House. These services form the control plane of the architecture, which is based on the SSI concept. The control plane implements a decentralized identity management system for participants, components, and services, and is supported by an IOTA Tangle DLT. This shared Tangle network enables the management of identities, ensures traceability, and serves as a verifiable registry of interactions across components.

In the data plane, participants have the flexibility to choose their preferred data storage solutions, which can range from traditional databases to various types of DLTs. However, in this particular implementation, the IOTA Tangle has also been selected for the data plane. This choice ensures that data storage is securely managed, data provenance is maintained, and traceability is upheld. Access to data stored in the Tangle is controlled by access policies and enforcement mechanisms, ensuring compliance and security.

This setup orchestrates a secure data flow, starting from the storage of machine-generated data in the Tangle, cataloging these data assets, negotiating contract terms between data consumers and providers, and culminating in the secure data exchange.

Specifically, the process unfolds as follows: (*1*) Machine-generated datasets are stored on the Tangle, each tagged with a DID linked to the originating machine for data provenance. (*2*) Data owners authorize connectors to publish descriptive metadata for their datasets. This involves interactions with the Identity Provider for registration and DID assignment, followed by VC generation for metadata, policies, and pricing, utilizing the Tangle for identity verification. (*3*) Data owners sign the VC, producing a VP published on the Metadata Catalog as a data offering. (*4*) Publications are logged on the Tangle by the Clearing House for transparency. (*5*) Data users search for datasets via the connector, querying the Metadata Catalog by topics. (*6*) Search operations are audited by the Clearing House, recording all transactions on the Tangle. (*7*) Negotiation of contract terms follows, leading to a Dynamic Attribute Token (DAT) generation upon agreement. (*8*) The DAT enables data retrieval from the Tangle, with access and usage regulated by PEPs.

[6] https://www.oasis-open.org/standard/xacmlv3-0/
[7] https://dssc.eu/page/knowledge-base

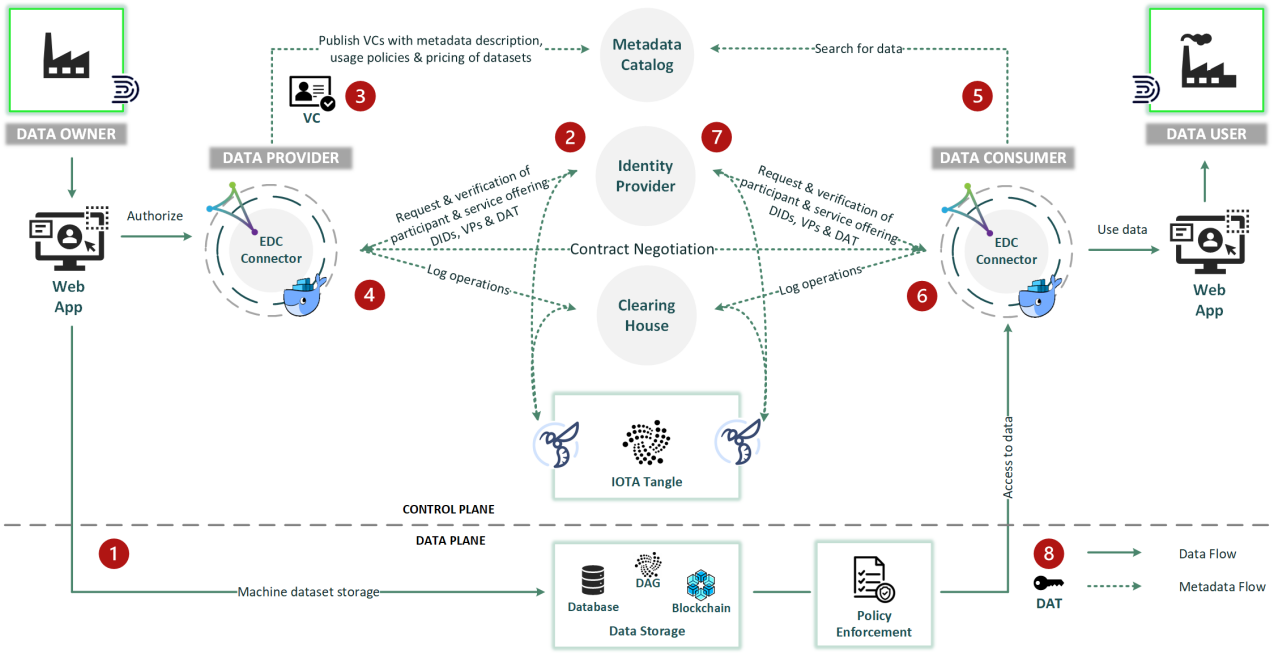

Figure 3: Proposed architecture for the IDS RAM implementation in the IOTA ecosystem

This interaction between the control and data planes ensures that data sharing adheres to the principles of security, transparency, and data sovereignty. Delving into the control plane of the architecture, the following sections detail the core components.

5.1 Identity Provider

This component serves as the identity enabler of the IDSA architecture, representing a shift from the association's standard centralized X.509 certificate-based identity management towards a decentralized model grounded in SSI. This evolution strengthens the fundamental decentralization principles of DLT applications, emphasizing data sovereignty and enhancing participant autonomy in the data space. By adopting a decentralized identity management approach, this architecture aligns with initiatives like Gaia-X [12].

The main functionalities of this component include the following: (*1*) Issuance, management, and validation of DIDs for every data space participant, technical component, and offered datasets or services. (*2*) Issuance, semantic and syntactic validation of VCs, along with the generation and validation of VPs for the description of data offerings. (*3*) Issuance of DATs for data access control.

5.2 Metadata Catalog

The Metadata Catalog, serving as the Broker Service Provider within the IDSA architecture, facilitates the search and querying of data within the data space. It provides access to VPs that include metadata descriptions, usage policies in ODRL format, and pricing details. For example, Figure 4 illustrates the structure of a policy that permits the assigned entity to perform a read action on the target dataset, constrained to a single access instance. Additionally, a duty is imposed, requiring the participant to make a specified payment before the permission is granted.

The structure of VCs positions the data owner as the offer holder and the infrastructure administrator as the credential issuer, serving as the trust anchor in the ecosystem. In this environment, access links to the data are revealed only after the parties reach an agreement. Publishing a data offer triggers the logging of essential details,

```
{
  "<http://exa.eu/policy:0231>": {
    "a": "odrl:Offer",
    "odrl:permission": {
      "a": "odrl:Permission",
      "odrl:target": "<https://exa.eu/dataset/2b3d441b>",
      "odrl:assigned": "<https://exa.eu/org/Participant:Provider01>",
      "odrl:action": "odrl:read",
      "odrl:duty": "_:requirements",
      "odrl:constraint": {
        "a": "odrl:Constraint",
        "odrl:count": 1,
        "odrl:operator": "odrl:lteq"
      }
    }
  },
  "_:requirements": {
    "a": "odrl:Duty",
    "odrl:action": "odrl:pay",
    "odrl:constraint": {
      "a": "odrl:Constraint",
      "odrl:payAmount": 50.00,
      "odrl:operator": "odrl:eq",
      "odrl:unit": "<http://cvx.iptc.org/iso4217a:EUR>"
    }
  }
}
```

Figure 4: Structure of ODRL usage policy definition

such as a hash of the complete dataset and a link to the catalog, stored in the Tangle through the Clearing House.

Each participant must maintain a local VC wallet, ensuring personal control and secure storage of their credentials. In contrast, VPs, which are VCs signed by the holder to describe data offerings, are made publicly available in the Metadata Catalog through the cataloging service. This setup guarantees that while the VC wallet provides secure, localized storage for credentials, VPs enable public access to the descriptions of data offerings.

In the preliminary stages of this research, the Metadata Catalog is configured as a global entity accessible to all participants within the data space, serving as a unified point of interaction. However, a decentralized approach can also be envisioned, where individual providers manage their own metadata catalogs hosting VPs specific to their data offerings. In this decentralized framework, a global Metadata Catalog would aggregate selected VPs from these provider-specific catalogs, selectively making information publicly accessible. This architecture supports a distributed storage model where data is held within provider-controlled zones, augmented by a generalized, aggregated layer to facilitate broader access, aligning with the principles of data sovereignty and controlled data sharing.

To improve descriptive VPs for data offerings based on the DCAT standard, it is crucial for all ecosystem participants to adopt a consistent, standardized data format. Therefore, integrating a Vocabulary Provider in the future would enhance interoperability by supporting various data formats, thus improving communication and data exchange across entities.

5.3 Clearing House

The Clearing House component in the proposed architecture is integral to recording and monitoring operations throughout the data space. It directly interfaces with the underlying Tangle network nodes to securely store logs. This component systematically tracks all activities within the data space, including: (*1*) participant registration, (*2*) data offering publications, (*3*) data asset searches, (*4*) contract negotiations, and (*5*) data access and usage control. These records are fundamental for ensuring transparency, enabling the monitoring of policy compliance, and managing data exchange billing through the platform's payment system.

The architecture ensures that all recorded transactions are both verifiable and traceable across the entire ecosystem. While this information is accessible to the entire data space, access to the stored data is nonetheless strictly controlled and limited to authorized services or specific operational needs. This approach maintains a critical balance between transparency and data privacy, enhancing the integrity and accountability of the data space while effectively safeguarding sensitive information from unauthorized access.

6 Implementation

This section demonstrates the implementation of various processes and interactions among components and participant roles within the proposed architecture for the defined IIoT scenario. A sequence diagram in Figure 5 illustrates the overall flow of interactions within the data space, highlighting how components and participants interact to achieve seamless data exchange and management.

Table 1: Implementation details and involved processes of the proposed architecture's control plane

Component	Implementation	Processes
Identity Provider	IOTA Identity	Onboarding, Data Offering
Metadata Catalog	MongoDB	Data Offering
Clearing House	IOTA Client, IOTA Wallet	Policy Enforcement
Connector	EDC Connector, Minimum Viable Dataspace[1]	All
DLT	Private IOTA Tangle, Stardust version[2], Alias Outputs[3], Basic Outputs[4]	Onboarding, Data Offering, Contract Negotiation

(1) https://github.com/eclipse-edc/MinimumViableDataspace
(2) https://github.com/iotaledger/hornet/tree/develop/private_tangle
(3) https://wiki.iota.org/tips/tips/TIP-0018/#alias-output
(4) https://wiki.iota.org/tips/tips/TIP-0018/#basic-output

Table 1 further details the components described for the control plane of the proposed architecture. It outlines the various IOTA frameworks, deployment solutions, and the main processes they support, providing a comprehensive view of how each component contributes to the functionality and efficiency of the data space.

The control plane is anchored on a private IOTA Tangle network consisting of multiple Hornet nodes. In this configuration, the DID documents associated with participant identities are stored as Alias Outputs, while records from the Clearing House are stored as Basic Outputs, encapsulating data within their metadata field. Additionally, a separate IOTA network is utilized for data storage within the data provider's data plane, where machine-generated data is also stored in transactions categorized as Basic Outputs.

To implement the data space, the architecture relies on EDC connectors, chosen for their modular design and compatibility with the IDSA's DSP [4]. These connectors are implemented within the Minimum Viable Dataspace (MVD) scenario, ensuring seamless integration and efficient data exchange across the data space.

Regarding processes, the onboarding process is successfully implemented through a decentralized identity management system based on SSI, which identifies all participants in the data space using their DID. This system allows for the assignment of properties or attributes in the form of VCs, facilitated by the IOTA Identity framework. For policy enforcement, the system ensures traceability by relying on logs from the Clearing House, securely stored on the IOTA network using the IOTA Client and IOTA Wallet frameworks, encapsulating data within transactions.

The data offering process, which includes describing data and publishing it in the catalog, is managed using MongoDB to store the data offerings. The data transfer process then enables controlled access to data stored on the Tangle, which is granted after an agreement is reached and the corresponding access token is verified.

That said, this research work is still under development, and ongoing efforts are focused on improving contract terms negotiation and the technical enforcement of usage policies.

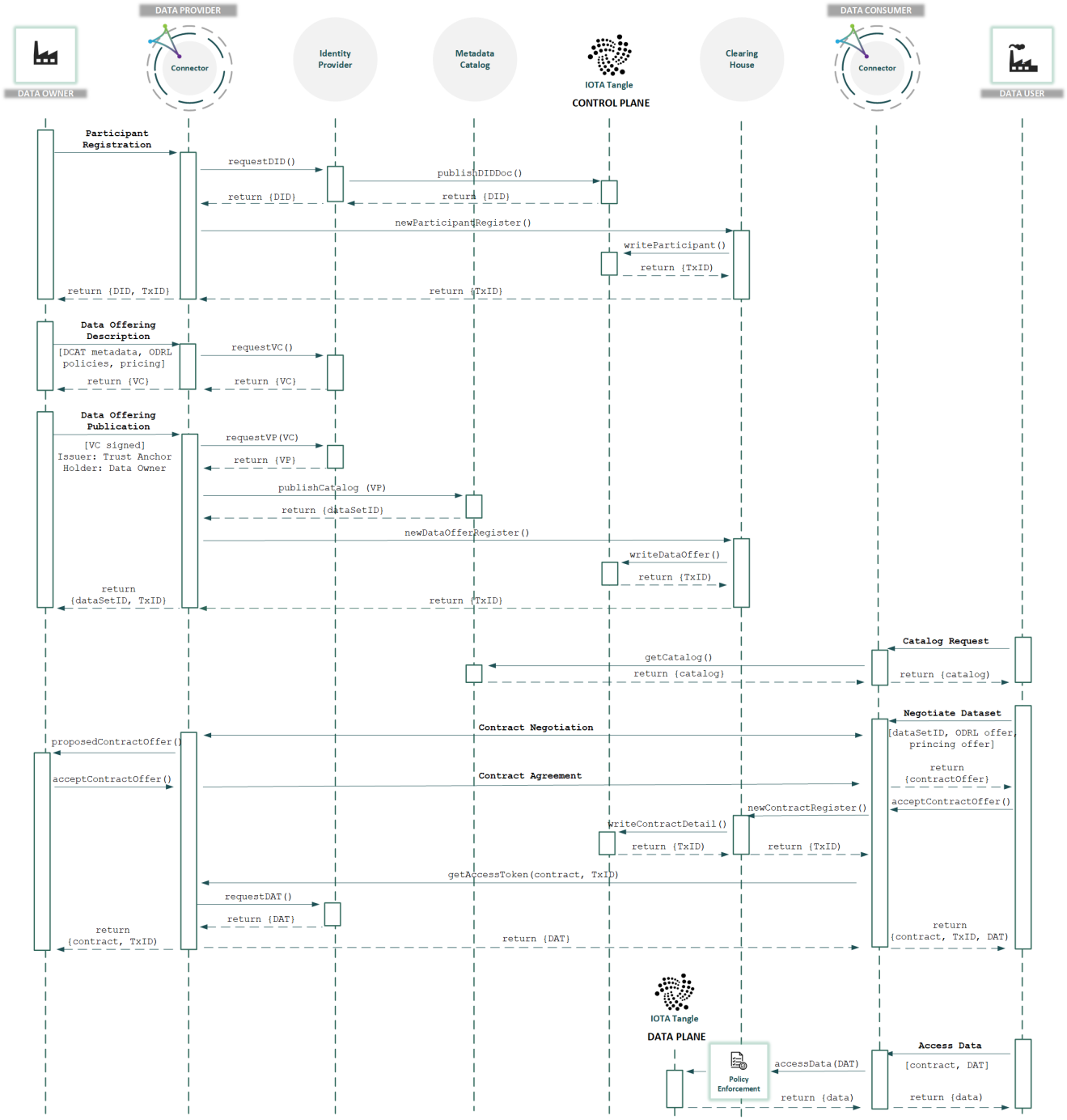

Figure 5: Participant onboarding, data offering, contract negotiation and data exchange processes in the IOTA-based data space

6.1 Contract Negotiation

According to the DSP specification, the current negotiation process within the data space is facilitated through human-mediated solutions. These are suitable for handling personal data where terms are set by the end-user. However, in industrial settings, there is a significant opportunity to transition to a more automated system. Instead of relying on simple comparisons, the focus shifts to aligning offer and demand through policy matching, based on initial descriptions using ODRL policies. This move towards automation is particularly beneficial in environments dominated by non-personal, machine-generated data, where policy-driven negotiations can substantially enhance the efficiency and precision of stakeholder agreements.

This approach sets the stage for a dynamic negotiation setup, allowing for iterative terms adjustments within preset policies until a mutual agreement is reached. By embedding the negotiation phase within smart contracts on a DLT, this method can ensure that agreements are both automated and enforceable, closely aligning with stakeholder needs. This strategy adheres to initial policy mapping, making the negotiation process a central element in achieving consensus between providers and consumers.

Building on the manual comparison of ODRL policies as outlined in [7], incorporating the more automated compliance checking methods described in [5] and the methodology proposed by Gaia-X on their Policy Reasoning Engine [8], this work aims to advance the automation of the negotiation process. The goal is to enable more dynamic and efficient negotiation of contract terms.

At this initial stage, the proposed process flow is illustrated in Figure 6, based on the state diagram from the contract negotiation process outlined in the DSP specification. This diagram simplifies the case by assuming that the consumer initiates the negotiation and excludes the *Terminated* state for clarity. The process involves establishing the main terms of the contract as well as threshold values for each term to ensure flexibility and mutual agreement.

Once the data provider defines its metadata description of the data following the DCAT standard and attaches the corresponding usage policies specified in ODRL, additional contract terms can be added to the offer. Moreover, the contract terms can be dynamically modified even after they have been initially defined in the data offer published in the Metadata Catalog. On the other hand, the provider can also define different thresholds for each specified term. These additional thresholds and details are not publicly available in the Metadata Catalog but are used internally by the process to determine if an offer is compliant.

When the data consumer selects the desired data offer, the contract negotiation process begins with the consumer sending a Contract Request Message, transitioning the state to *Requested*. The system then performs a policy check to verify if the policy meets the predefined conditions. If the policy does not match initially, the process moves to the *Within Threshold* check, facilitated by predefined threshold values for each term in the data usage contract. These thresholds ensure that the proposed terms are within the acceptable limits set by both parties. If the terms are within these thresholds, the provider sends a Contract Agreement Message, changing the state to *Agreed*. The contract then proceeds to the verification stage by the consumer, resulting in the state *Verified*. Once verified, the Contract Negotiation Event Message is dispatched, terminating the contract in the state of *Finalized*.

If the policy does not match or if the terms exceed the defined thresholds, the process allows for generating counteroffers. The provider can send a Contract Offer Message if the initial terms are not agreeable, followed by an evaluation by the consumer to accept a counteroffer. If accepted, the state advances to *Accepted*, leading to the final agreement and verification stages. Even if this solution remains conceptual, introducing threshold values into the contract negotiation process aims to automate it, thereby enhancing the efficiency of reaching mutual agreements.

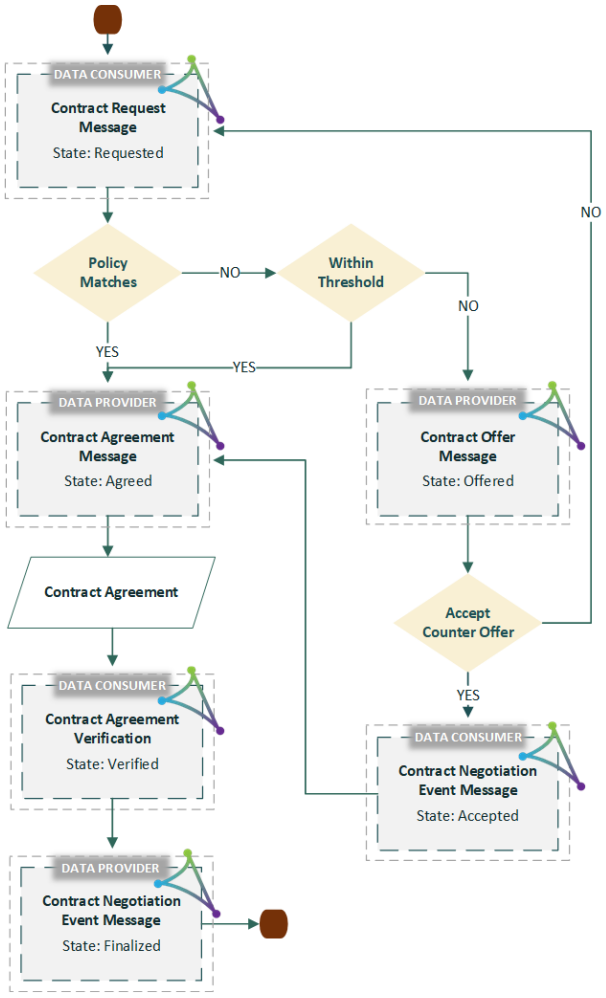

Figure 6: Proposed flow diagram for contract negotiation

6.2 Policy Enforcement

The concept of policy enforcement in the IDS RAM underlines the need for mechanisms to ensure that data remains under the owner's control, facilitating sovereignty and compliance during user access. This approach is central to monitoring data use, ensuring compliance with agreed terms, and managing non-compliance. The IDSA tackles this challenge, as detailed in [34], by advocating for the use of technical enforcement mechanisms. Notably, MYDATA [9] enables defining policies that restrict data access frequencies, specify allowable access time frames, and delineate access based on geographical location, thus providing the technical enforcement of such policies. Moreover, IDSA also promotes using LUCON policies [33] to manage data flows by dictating the routing of messages across services. LUCON policies enhance usage control by preventing information leaks, binding data usage to obligations, and enforcing data flows across services through dynamic analysis at runtime and verification of message routes against policies.

[8] https://gaia-x.eu/news-press/gaia-x-and-the-policy-reasoning-engine/

[9] https://www.mydata-control.de/

Gil et al. [13] propose a methodology for determining the most suitable solution for implementing Distributed Usage Control (DUC). Options for deploying a policy control system include integrating it within the connector, as initially proposed by IDS RAM, using an external system, or integrating it directly with the IOTA network, as Denis et al. suggest in [6]. This ensures the integrity of data usage over time. In addition, smart contracts can be used in conjunction with these solutions to track data lifecycle events back to the point of acquisition by the user, addressing the challenges of policy compliance and unauthorized data sharing after acquisition.

7 Conclusion and Future Lines

This work demonstrates the practical integration of the IDS RAM conceptual architecture with the IOTA framework, moving beyond theoretical discussions to implement a DLT solution specifically tailored for the IIoT data space ecosystem. Unlike traditional blockchain-focused studies, this research leverages IOTA's DAG structure to implement core IDS components, including an Identity Provider, a Metadata Catalog, and a Clearing House. This significantly enhances the security and utility of the ecosystem for third-party data use and value exploitation. Grounded in the roles and concepts of IDS and adopting a decentralized interconnection approach inspired by initiatives such as Gaia-X, this work advances sovereign, secure, scalable, interoperable, and efficient data management within the IIoT domain, demonstrating the benefits of integrating IDS with the capabilities of the IOTA framework.

As outlined in Table 2, several processes of the proposed architecture, such as onboarding, data offering, and data exchange, are already complete. Future work will focus on implementing and automating contract terms negotiation. A key element of this will be the application of the conceptual solution presented in this article, which involves setting different threshold values on data offer conditions as part of the usage policies attached to data. In addition, efforts will be directed toward automating technical policy enforcement mechanisms, addressing the adherence to both data usage and legislative policies.

Beyond that, integrating a Vocabulary Provider will improve interoperability, enhancing the platform's ability to facilitate common understanding across systems and stakeholders. Moreover, introducing a Data App Provider will add flexibility to the system by incorporating advanced data handling capabilities tailored to specific needs. These Data Apps can be deployed on connectors within the data space, enabling specialized data processing and management. For instance, Privacy Enhancing Technologies (PET) functionalities could be offered as Data Apps, supporting privacy-preserving data analysis and sharing, making the system more adaptable and capable of securely managing data.

Although this article focuses specifically on the IDS architecture, the same approach could be adapted for the Gaia-X framework as a future line of research, emphasizing the potential for broader application and integration with other emerging data space initiatives. Furthermore, the IDSA is currently developing a new version of the IDS RAM (v5.0), which will align with the protocols defined in the DSP. This new version will see the functions of the Metadata Broker and Clearing House being handled by the connector itself, implementing the protocol. As this new RAM version emerges, it will be needed to evaluate its impact on the proposed architecture.

While the solution proposed in this article is still under development, future evaluations will determine its practical applicability in real-world scenarios. Therefore, continuous assessment and adaptation will be essential to ensure the robustness and reliability of the system in the evolving IIoT domain.

Table 2: Implementation status of proposed IDS solution

Process	Description	Proposed Solution	State
Onboarding	Grant access to IDS as data consumer or provider	Decentralized identity management through SSI	Complete
Data Offering	Description of data assets and usage policies	VCs for asset description, published via VPs	Complete
Contract Negotiation	Negotiation of data usage contract terms	Automated tools for contract terms negotiation	Ongoing Work
Exchanging Data	Provide access to data stored in the Tangle	Using DAT-based control access	Complete
Policy Enforcement	Technical enforcement of usage policies	PEP integration, leveraging smart contracts	Ongoing Work

Acknowledgments

This work has been financed by the European Commission through the Horizon Europe program under the HAVEN project (grant agreement number 101137636). It was also partially supported by MCIN/ AEI /10.13039/501100011033/ FEDER "Una manera de hacer Europa" under the grant PID2021-124502OB-C44 (PRESECREL).

References

[1] Sebastian Bader, Georg Bramm, and Juan Ceballos. 2020. IDSA White Paper Specification IDS Clearing House. *International Data Spaces Association* (2020). https://doi.org/10.5281/zenodo.5675765

[2] Sebastian Bader, Fabian Bruckner, Gernot Böge, Dennis Oliver Kubitza, Jörg Langkau, and Ralf Nagel. 2020. IDSA White Paper Specification IDS Meta Data Broker. *International Data Spaces Association* (2020). https://doi.org/10.5281/zenodo.5675076

[3] Sebastian Bader, Jaroslav Pullmann, and Christian Mader. 2020. The International Data Spaces Information Model – An Ontology for Sovereign Exchange of Digital Content. *Lecture Notes in Computer Science* (2020), 176–192. https://doi.org/10.1007/978-3-030-62466-8_12/FIGURES/5

[4] Tobias Dam, Lukas Daniel Klausner, Sebastian Neumaier, and Torsten Priebe. 2023. A Survey of Dataspace Connector Implementations. *ITADAT2023: Italian Conference on Big Data and Data Science* (2023).

[5] Marina De Vos, Sabrina Kirrane, Julian Padget, and Ken Satoh. 2019. ODRL Policy Modelling and Compliance Checking. In *Rules and Reasoning*, Paul Fodor, Marco Montali, Diego Calvanese, and Dumitru Roman (Eds.). Springer International Publishing, Cham, 36–51.

[6] Nathanael Denis, Maryline Laurent, and Sophie Chabridon. 2023. Integrating Usage Control Into Distributed Ledger Technology for Internet of Things Privacy. *IEEE Internet of Things Journal* 10 (11 2023), 20120–20133. Issue 22. https://doi.org/10.1109/JIOT.2023.3283300

[7] Beatriz Esteves, Víctor Rodríguez-Doncel, and Harshvardhan J. Pandit. 2022. Using the ODRL Profile for Access Control for Solid Pod Resource Governance.

Lecture Notes in Computer Science 13384 LNCS (2022), 16–20. https://doi.org/10.1007/978-3-031-11609-4_3/FIGURES/1

[8] European Commission. 2020. A European Strategy for Data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

[9] European Parliament and Council of the European Union. 2016. Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). , 88 pages.

[10] European Parliament and Council of the European Union. 2022. Regulation (EU) 2022/868 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Official Journal of the European Union, no. L 152. , 44 pages.

[11] European Parliament and Council of the European Union. 2023. Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). Official Journal of the European Union.

[12] Gaia-X European Association for Data and Cloud (AISBL). 2021. Gaia-X Architecture Document - 22.04 Release. (2021).

[13] Gonzalo Gil, Aitor Arnaiz, Francisco Javier Diez, and Maria Victoria Higuero. 2020. Evaluation Methodology for Distributed Data Usage Control Solutions. *GIoTS 2020 - Global Internet of Things Summit, Proceedings* (2020). https://doi.org/10.1109/GIOTS49054.2020.9119565

[14] Giulia Giussani, Sebastian Steinbuss, Mario Holesch, and Nora Gras. 2024. Data Connector Report. *International Data Spaces Association* (2024). https://doi.org/records/10710081

[15] Nenad Gligoric, David Escuín, and Lorena Polo. 2024. IOTA-Based Distributed Ledger in the Mining Industry: Efficiency, Sustainability and Transparency. *Sensors 2024, Vol. 24, Page 923* 24 (1 2024), 923. Issue 3. https://doi.org/10.3390/S24030923

[16] International Data Space Association. 2024. Dataspace Protocol 2024-1. https://docs.internationaldataspaces.org/ids-knowledgebase/v/dataspace-protocol/overview/readme

[17] ITU-T. 2020. *Security Guidelines for Using Distributed Ledger Technology for Decentralized Identity Management.* ITU-T Recommendation X.1403. International Telecommunication Union. https://www.itu.int/rec/T-REC-X.1403-202009-I/es

[18] Laith T. Khrais. 2020. Comparison study of blockchain technology and IOTA technology. *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020* (10 2020), 42–47. https://doi.org/10.1109/I-SMAC49090.2020.9243366

[19] Anhelina Kovach. 2023. Sistema descentralizado de gestión de identidades digitales y pagos seguros en entornos IIoT. (2023). Master Thesis, University of Cantabria, Santander, Spain.

[20] Silvio Meneguzzo, Alfredo Favenza, Valentina Gatteschi, and Claudio Schifanella. 2023. Integrating a DLT-Based Data Marketplace with IDSA for a Unified Energy Dataspace: Towards Silo-Free Energy Data Exchange within GAIA-X. *5th Conference on Blockchain Research and Applications for Innovative Networks and Services, BRAINS 2023* (2023). https://doi.org/10.1109/BRAINS59668.2023.10316796

[21] Michael Nast, Benjamin Rother, Frank Golatowski, DIrk Timmermann, Jens Leveling, Christian Olms, and Christian Nissen. 2020. Work-in-Progress: Towards an International Data Spaces Connector for the Internet of Things. *IEEE International Workshop on Factory Communication Systems, WFCS* (2020). https://doi.org/10.1109/WFCS47810.2020.9114503

[22] Lam Duc Nguyen, Arne Bröring, Massimo Pizzol, and Petar Popovski. 2022. Analysis of distributed ledger technologies for industrial manufacturing. *Scientific Reports 2022 12:1* 12 (10 2022), 1–11. Issue 1. https://doi.org/10.1038/s41598-022-22612-3

[23] Boris Otto and Matthias Jarke. 2019. Designing a multi-sided data platform: findings from the International Data Spaces case. *Electronic Markets* 29 (12 2019), 561–580. Issue 4. https://doi.org/10.1007/S12525-019-00362-X/TABLES/14

[24] Boris Otto, Sebastian Steinbuss, Andreas Teuscher, and Sebastian Bader. 2022. IDS RAM 4. *International Data Spaces Association* (2022). https://docs.internationaldataspaces.org/ids-knowledgebase/v/ids-ram-4/

[25] Serguei Yu. Popov. 2015. The Tangle. https://api.semanticscholar.org/CorpusID:4958428

[26] Wolfgang Prinz, Thomas Rose, and Nils Urbach. 2022. Blockchain Technology and International Data Spaces. In *Designing Data Spaces*, B. Otto, M. ten Hompel, and S. Wrobel (Eds.). Springer, Cham, 165–180. https://doi.org/10.1007/978-3-030-93975-5_10

[27] Haydar Qarawlus, Malte Hellmeier, and Johannes Pieperbeck. 2021. Sovereign Data Exchange in Cloud-Connected IoT using International Data Spaces. *2021 IEEE Cloud Summit, Cloud Summit 2021* (2021), 13–18. https://doi.org/10.1109/IEEECLOUDSUMMIT52029.2021.00010

[28] Alexander Raschendorfer, Benjamin Mörzinger, Eric Steinberger, Patrick Pelzmann, and Ralf Oswald. 2019. On IOTA as a potential enabler for an M2M economy in manufacturing. *Procedia CIRP* 79 (1 2019), 379–384. https://doi.org/10.1016/J.PROCIR.2019.02.096

[29] Julia Rosenberger, Felix Rauterberg, and Dieter Schramm. 2021. Performance study on IOTA Chrysalis and Coordicide in the Industrial Internet of Things. *2021 IEEE Global Conference on Artificial Intelligence and Internet of Things, GCAIoT 2021* (2021), 88–93. https://doi.org/10.1109/GCAIOT53516.2021.9692985

[30] S. Meneguzzo, A. Favenza, V. Gatteschi and C. Schifanella. 2023. Exploring the Potential of Energy Data Marketplaces: An Approach based on the Ocean Protocol. *Proceedings - International Computer Software and Applications Conference* 2023-June (2023), 1488–1494. https://doi.org/10.1109/COMPSAC57700.2023.00229

[31] Khaled Sayad and Benoit Lemoine. 2023. Towards Cross-domain Resilience in SDN-enabled Smart Power Grids: Enabling Information Sharing through Dataspaces. *IEEE International Conference on Omni-Layer Intelligent Systems, COINS 2023* (2023). https://doi.org/{10.1109/COINS57856.2023.10189319}

[32] Nicole Schmidt and Arndt Lueder. 2018. The Flow and Reuse of Data: Capabilities of AutomationML in the Production System Life Cycle. *IEEE Industrial Electronics Magazine* 12 (6 2018), 59–63. Issue 2. https://doi.org/10.1109/MIE.2018.2818748

[33] Julian Schuette and Gerd Stefan Brost. 2018. LUCON: Data Flow Control for Message-Based IoT Systems. *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, Trustcom/BigDataSE 2018* (2018), 289–299. https://doi.org/10.1109/TRUSTCOM/BIGDATASE.2018.00052

[34] Sebastian Steinbuss. 2019. Usage Control in the International Data Spaces. *International Data Spaces Association* (2019). https://doi.org/10.5281/zenodo.5675884

[35] Sebastian Steinbuss. 2023. IDSA Rulebook. *International Data Spaces Association* (2023). https://docs.internationaldataspaces.org/ids-knowledgebase/v/idsa-rulebook/front-matter/readme

[36] Sebastian Steinbuss, Matthijs Punter, Fabiana Fournier, and Inna Skarbovski. 2019. Blockchain Technology in IDS. *International Data Spaces Association* (2019). https://doi.org/10.5281/zenodo.5675962

[37] Thomas Uslaender and Simon Dalmolen. 2022. IDSA Position Paper Data Sovereignty - Requirements Analyis of Manufacturing Use Cases. *International Data Spaces Association* (2022). https://doi.org/10.5281/zenodo.6668994