Building a Data Space for the Public Security Domain using Smart Contracts

PREPRINT

Roman Karl*, Valentina Mazzonello†, Bernardo Pacheco‡, Joao Silveira‡, Sven Schlarb*, Veronika Siska*, Axel Weissenfeld*
*AIT Austrian Institute of Technology, Vienna , Austria.
Email: firstname.lastname@ait.ac.at
†Engineering Ingegneria Informatica s.p.a., Palermo, Italy
Email: firstname.lastname@eng.it
‡INOV - Instituto de Engenharia de Sistemas e Computadores Inovação, Lisboa, Portugal
Email: firstname.lastname@inov.pt

***Abstract*—The publication focuses on exploring ways of integrating smart contracts within a data space dedicated to the public security domain. This data space shall facilitate involving various stakeholders, such as law enforcement agencies (LEAs), research facilities and universities as well as and research-oriented companies by taking their needs and requirements into account. On the one hand, we discuss the benefits of smart contracts in this context, particularly how blockchain-backed processes can contribute to building a trustworthy data sharing ecosystem. On the other hand, we also investigate challenges and costs associated with this approach.**

***Index Terms*—smart contract, data space, blockchain, data sharing**

I. Introduction

One of the foremost obstacles hindering the training of sophisticated AI models for applications in the area of crime and terrorism is the scarcity and fragmented nature of available data, which has been discussed at multiple fight crime and terrorism (FCT) workshops and EU events[1]. Addressing this challenge, the development of a data space for the public security domain has emerged as a pivotal solution. The data space is crafted to facilitate the seamless exchange of data among law enforcement agencies (LEAs) and research facilities as well as industry stakeholders. However, the success of such an enterprise hinges significantly on the establishment of trust as a foundational prerequisite. Without a robust foundation of trust, active participation and meaningful data exchange among the diverse participants of the data space remain unachievable goals. Leveraging decentralized solutions such as a decentralized license agreement and validation framework seem to be very suitable in achieving this goal. Central to the functionality of this framework is the integration of a blockchain node, serving as a robust notary to validate and authenticate agreements.

This work was funded by the European Commission under contract No. 101073951 LAGO and by the Austrian Gaia-X Hub.

[1]For instance, in the CERIS Community of Users (CoU) Workshop on "Research Data in Fighting Crime and Terrorism" held on Jan. 10, 2021, organized by the EC in Brussels

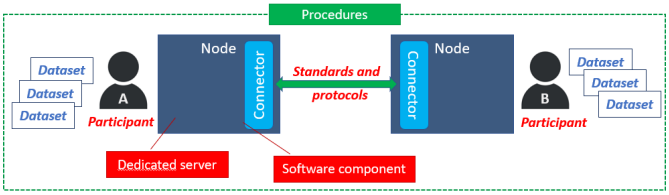

Fig. 1. Building blocks of the developed data space.

Through the immutable ledger of the blockchain, the integrity and authenticity of licenses and data transactions are upheld, providing stakeholders with the confidence that the concluded contracts are protected from tampering or unauthorized access to provided datasets. The building blocks to create this kind of data space for the public security domain are developed within LAGO (*Lessen data Access and Governance Obstacles*), an European Commission funded project in the context of the Horizon Europe programme[2].

The idea of data spaces appeared about 20 years ago, as a solution to shift from centralised databases to storing data at the source [1], to enable data owners to retain control over their data (data sovereignty [2]). Data sovereignty recently gained particular focus on the international scene, largely due to the European data strategy and corresponding regulations, such as the General Data Protection Regulation (GDPR), the Data Governance Act and the Data Act. Many initiatives now support the shift towards a future data economy based on these principles, such as the International Data Spaces Association[3], provider of the first reference architecture (International Data Spaces Reference Architecture Model), or Gaia-X, focusing on establishing trust and supporting interoperability and thus independence from dominant hyperscalers.

[2]https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

[3]https://internationaldataspaces.org

The integration of blockchain-based systems and smart contracts in data spaces can improve transparency while reducing the dependence on central agencies. Furthermore, the blocks that form the blockchain are replicated throughout the system, thereby ensuring that confirmed data will not be lost and is also tamper-proof. By utilizing blockchain, data integrity and authenticity can be guaranteed, reducing the risk of unauthorized access or manipulation. Smart contracts are small programs whose code is put on the blockchain and whose results can be safely reproduced. They are sometimes described as automated contracts, in the sense that they can contain clauses which can describe valid actions while automatically prohibiting forbidden actions. In the rest of the paper, we will always distinguish between smart and legal contract, because even if some clauses can occur in both, there is usually a large gap between legal clauses and rules that can be automatically enforced. Despite this, combining a legal contract with a smart contract still offers some additional potential. For instance, smart contracts can facilitate the exchange of sensitive information between different entities while ensuring compliance with predefined rules and regulations. Additionally, smart contracts can enable secure and transparent transactions, such as the authentication of identities or the issuance of valid contracts, without the need for intermediaries. Providing this functionality, nodes of the blockchain-based system serve as reliable notaries in legal proceedings by securely time-stamping and storing essential information about documents and transactions. Their immutable nature ensures the integrity and authenticity of records, reducing disputes over validity and providing evidence in court.

This work introduces a data space dedicated to the public security domain (Fig. 1), which addresses the so called “data issue” in the FCT research landscape, i.e., the lack of domain-specific data in sufficient quality and quantity to enable appropriate training and testing of research methods, platforms and tools oriented to the FCT domain. The principles and foundation of this approach are explained in Sec. III. The next section provides an overview of the application scenario Sec. IV. The main contribution of our work is the utilization of smart contracts for the introduced data space (Sec. V) as well as an evaluation of the data space implementation (Sec. VI).

II. Related Work

With the emergence of blockchain technology as a means to create distributed data sharing ecosystems, the potential of using the technology to build distributed data market have been suggested by [3] and also by the ”Data Market Austria” project [4]. Both approaches aimed to enhance security, transparency, and trust among participants by decentralizing data management and transaction verification. Blockchain played a crucial role in ensuring the integrity and immutability of data exchanged on the platform. However, in both cases, the application domain was not related specifically to the public security domain.

[5] present an approach using the Hyperledger Blockchain for secure and private government data sharing. The publication explores the implementation of privacy-preserving mechanisms within Hyperledger to ensure confidentiality while facilitating data exchange among governmental entities. The difference of our work is the use of an Ethereum Blockchain instead of Hyperledger and the focus of this work on data sharing in the public security domain.

[6] explore the intersection of data protection laws and multi-party computation, particularly in the context of information exchange between law enforcement agencies. The publication investigates how secure collaboration can be enabled while adhering to data privacy regulations. It shows practical applications and legal implications of employing multi-party computation for sensitive data sharing among multiple parties in law enforcement settings. In this case the requirements concerning data privacy are similar to the ones assumed for data sharing in the approach presented here, with the difference that blockchain technology is used as a technological basis for establishing contracts between law enforcement entities sharing data.

[7] give an overview about approaches in the interplay between cybersecurity, data privacy, and blockchain technology. It examines various aspects such as the role of blockchain in enhancing data security and privacy protection. Our work, however, differs in that it focuses specifically on secure data sharing in the context of machine learning scenarios between LEAs, research facilities and industry.

Another blockchain-based solution, the Pontus-X ecosystem[4], is developed by deltaDAO and used by multiple Gaia-X-related projects. They build on the existing Ocean Protocol for a blockchain-based data marketplace, connected with their own permissioned ledger (GEN-X) operated by a circle of verifiers and using proof-of-authority. They also integrate Gaia-X-compatible verifiable credentials for their participants and offers (both datasets and services), to be compliant with the Gaia-X Trust Framework and rely on blockchain-based decentralised identities (DIDs) as an identity mechanism.

There are also data space implementations that do not rely on a blockchain [8]. For example, the IDS RAM describes a technology-agnostic system, where offers (datasets with a certain policy) are held internally at the connector and contracts are negotiated and signed directly between the connectors (without the use of smart contracts). Transactions, including contracting, may be recorded by a dedicated logging service. However, this service may not necessarily use a blockchain, but could also be a centralised system at a trusted authority or some immutable storage (e.g., immuDB). Transactions in the IDS RAM are based on the dataspace protocol, which describes a technology-agnostic contracting process. Major implementations, such as the Eclipse Dataspace Components, also do not require the use of blockchain. The current Gaia-X software also does not rely on a blockchain: their identities normally use did:web, while their current broadcasting channel for service offerings, the Credential Events Service, uses a Kafka queue internally.

[4]https://docs.pontus-x.eu/

III. Principles and Foundations

The developed data space is intended as a set of well-established elements that interact through standardised protocols and procedures to enable access to research data related to FCT domains. The core elements of this particular data space (Fig. 1) are the following:

- **participants**, intended as organisations that share or need access to data.
- **resources**, intended as datasets or any other exchangeable digital content for research (e.g. ML models).
- **procedures**, intended as well-established methods and practices that participants can follow to take part effectively in the data space (from dataset creation to sharing and reuse).
- **standards and protocols**, for the interoperable exchange of resources.
- **technical components**, which implement the data space standards and protocols to allow participants to access resources.

The following foundational principles constitute the guidelines that have been strongly followed for conceptualisation of the data space:

- *security* and *trust*, related to confidence in the identity and capability of participants.
- *data sovereignty*, data owners (controllers) are in control of their own data. In addition, data is subject to the laws of the country in which they are located.
- *decentralisation*, with no unique central repository of data, but data stored at source, and shared via semantic interoperability only when necessary.
- *data quality*, to ensure that research data shared between participants are not corrupted, well-formatted and compliant with agreed formats.
- *proportionality* and *risk*, with regards to measures to assess the risk of sharing data in particular contexts (requesting participants, types of datasets, purpose of use, etc.) and proportionality between the legitimacy of the sharing and the ethics, legal and privacy compliance.
- *openness*, in terms of rules, specification, and protocols to participate in data sharing and exchange.
- *transparency*, related to clarity on what happens to data and interactions among participants exchanging datasets.
- *interoperability* and *portability*, enabling the exchange of data through technical means and standard protocols.
- *ethics*, *legal* and *privacy compliance*, especially focusing on FCT domain, where access to research data needs to consider EU regulations, national frameworks, ethics, privacy and data protection measures.

The developed data space for the public security domain consists of a decentralised data repository, which guarantees full control to data providers in terms of which data to make available, to whom, and under which conditions (i.e. licenses and usage policies). Participants maintain their datasets stored on their premises (on a dedicated server called *node*) and provide access to them through a dedicated software component called *connector*. Connectors implement the standards and protocols defined for the data space to enable access and sharing of research data in fully controlled way.

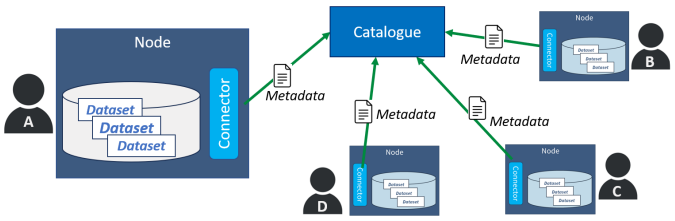

Fig. 2. Interactions between participants and the data catalogue.

An important question is also who is allowed to participate in a data space, which procedures are put in place for onboarding and authorisation, and which entities can be considered to be trusted. These aspects can be addressed with an appropriate governance model. First, participants that provide or consume data must be onboarded to the data space, which involves verifying their identity and issuing a proof of membership in the form of verifiable credentials. During this phase, participants' identities may be validated, potentially by connecting to external trust anchors, such as governmental systems like EU Trusted Service Providers, or dedicated data space trust services like the Gaia-X Trust Services. Other sector-specific rules may also be applied to grant a membership that supports proper authentication and authorisation. Before each transaction, such credentials may be verified to check their validity. To this end, LAGO foresees an onboarding procedure where a *trusted authority* is responsible for granting access only to verified participants (more information in section IV). The governance model of LAGO and of data spaces in general is not described in detail as this is not the primary focus of this paper.

IV. Data Exchange Framework - Application Scenario

To make participants aware of a dataset available for sharing, a data provider can register the dataset on the *catalogue* (Fig. 2). To ensure data sovereignty, only metadata about datasets are published on the catalogue, while data remains safely stored on participant premises. Metadata (also named *self-descriptors*) include information about not only the nature of the datasets (size, types of data, etc.), but also its intended use, license, provenance information (like methodologies used for the collection, generation, and annotation of the data), presence of personal data, and related legal, ethical, security and privacy concerns.

Any participant can query metadata stored on the catalogue to find datasets of interest. When a participant wants to get access to a specific dataset, it can request access to the data provider. We identified three use cases for the exchange of data related to public security, which require different legal approaches. If a license was already specified for the requested dataset, the data consumer has to accept the license terms

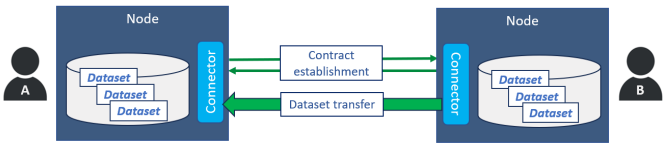

Fig. 3. Contract establishment and dataset transfer.

to request that dataset. On the contrary, other types of data may require the establishment of a contract between the data provider and the data consumer. Firstly, compliance with the General Data Protection Regulation (GDPR) is imperative when personal data is involved, necessitating the agreement on an individual Data Processing Agreement (DPA) to safeguard privacy rights, and complying to GDPR rules [9]. Secondly, in cases where data lacks personal information but raises security concerns, the data space must facilitate the creation of individual contracts for each request from an entity interested in accessing this particular dataset, thereby fortifying data integrity, and minimizing potential risks. Once the license terms are accepted or the contract is established, the dataset exchange can actually take place (Fig. 3).
Agreed usage policies could be enforced through technical means (e.g. duration, number of downloads, etc.), or controlled at organisational level (e.g. legal obligations). Connectors are responsible for monitoring the validity of usage policies that can be technically controlled, contributing to maintaining the process respectful of the contractualized clauses.

Operating in the data space requires a high level of trust between participants, especially because of the nature of the data shared (related to FCT domain). Indeed, potential stakeholders of this kind of data space are not only researchers, but also law enforcement agencies, governmental organisations, policy makers, etc.

To increase trust between the different stakeholders involved in research and lower concerns regarding the potential risks involved with data sharing (e.g. data security, safe use, legal and ethical compliance, etc.), an organisation can become a participant of the data space only after an accreditation procedure (called *onboarding*), performed by a *trusted authority*. During the onboarding, a trusted authority is responsible of verifying the trustworthiness of the organisation and providing it with credentials that certify it has been verified as *trusted* participant and thus can take part. Once obtained, those credentials can be exchanged between participants, to enable mutual verification and prove trust.

In keeping with the data sovereignty philosophy, these credentials use the Verifiable Credential Data Model [10]. Besides from proving participant membership, they can be used to prove other claims about participants. A relevant example would be for a participant to prove they have a certain certification, where such a credential would be issued by a different trusted entity with the specific authority to prove that claim (a certification body, per the example). This allows data providers to describe further usage policies, which are easy to technically verify.

Transparency is another key factor in establishing trust between participants involved in data sharing. When organizations are transparent about how they collect, use, and share data, it helps build trust with stakeholders. Transparency in data practices demonstrates accountability and integrity, which are essential components of trust. In the developed data space, transparency is ensured through the involvement of an Ethereum-based *ledger* component, on which every connector can log data space-related activities, such as participant accreditation, metadata publication on the data catalogue, contract agreements, data exchanges, and violation of usage policies of shared data. The ledger serves as comprehensive audit trail that records the entire history of data-related transactions and exchanges. This auditability is invaluable for compliance monitoring and regulatory reporting. By maintaining a transparent and immutable record of data activities, the ledger enables organizations to demonstrate compliance with legal and regulatory requirements.

V. Utilization of Smart Contracts for Public Security Domain

In the developed data space there are several different smart contracts which undergird the existing procedures in the ecosystem. In general, their role is to create a trustworthy protocol of some relevant events in the implemented data space. Some of the smart contracts additionally offer control mechanisms which can prohibit participants to perform actions that would violate certain rules. In this section we will describe the smart contract involved in creating data offers, concluding contracts, and exchanging data.

To be able to run smart contracts there needs to be a blockchain network in place. In the developed data space, each connector contains software components

- to participate in a an Ethereum network, called Ethereum nodes, and
- to provide access to the functionalities of the smart contracts.

The Ethereum nodes run go-ethereum as client software and form a private network that uses proof-of-authority as consensus mechanism for the prototype implementation. As the support for proof-of-authority is gradually diminishing in the Ethereum ecosystem at the time of writing, it is planned to set up the Ethereum network with proof-of-stake when it is run in a productive environment after the end of the LAGO project.

On top of the Ethereum node, a web server provides a REST-API for accessing the functionalities of the smart contracts. The web server does not store any information regarding the state on its own. Its only task is to process requests and translate them to requests to the Ethereum node.

In addition to the Ethereum node that is exclusively run by a participant, every participant controls one principal Ethereum account. There are mechanisms provided so that in the simplest case, node and account can be set up almost automatically. Optionally, additional security measures for individual nodes

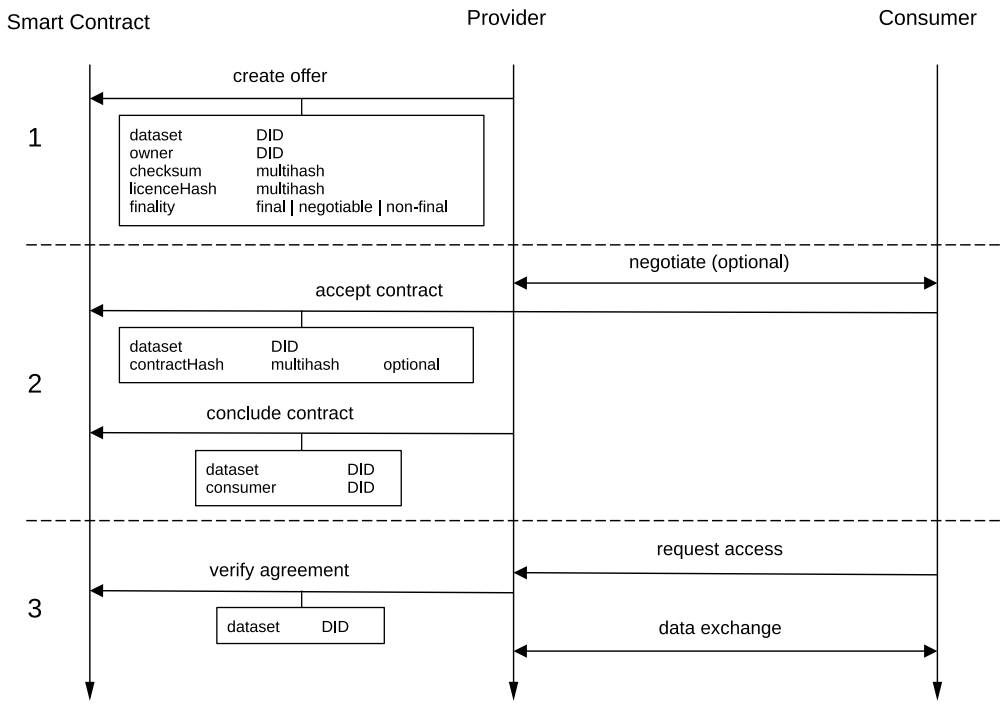

Fig. 4. Required steps for exchanging data. (1) A data provider creates a data offer. (2) Data provider and data consumer conclude a contract. (3) Data provider and data consumer exchange the data.

or the network could be introduced, reducing the ease of use by some degrees.

In every decentralised data exchange there are two participants: a data provider who can offer data and a data consumer for whom this data is relevant. Furthermore, provider and consumer will have to agree on legal terms for the data exchange, either a general license or an individual contract. The data exchange including a previous agreement consists of three phases, which are also illustrated in Figure 4:

1) *A data provider creates a data offer.* The data offer is published in the catalogue, which consists of metadata describing the data and a general license. Additionally, the data offer is written to the smart contract, this time only consisting of an identifier of the data and a hash value of the license. Depending on the offer, the license might be final, or it might be possible or even necessary to negotiate an individual contract. The data itself is kept by the provider until the exchange.
2) *Data provider and data consumer conclude a contract.* When a consumer is interested in purchasing a data set, he might start a negotiation with the provider. This negotiation phase is done via traditional means and it is not required if the consumer accepts the general license. The consumer can then confirm via the smart contract that he accepts the conditions, optionally providing the hash value of the contract document that was agreed upon. As a second step, the provider will also confirm his agreement to the data contract, thus concluding the contract. Under the assumption that contract documents are kept by both parties, any party can prove the validity of the agreement at any time after the conclusion just by referring to the corresponding entries on the blockchain.
3) *Data provider and data consumer exchange the data.* The consumer can request the access to a given data set. The connector of the provider will perform a query to the smart contract to verify if there exists a valid agreement. This query can be performed also by the consumer and, without knowing contractual details, by third parties. If a valid agreement exists, the access to the data set by the consumer will be permitted. It will be recorded via the smart contract that a successful data exchange has taken place. Note, that it is not possible to automatically check most of the legal clauses. Also payments are not controlled via the blockchain-based system.

In the developed data space we have adopted the concept of Decentralized Identifiers (DIDs) [11], more specifically DIDs based on Ethereum accounts. This brings the advantage that identifiers can be created locally while no participant can illegitimately claim the ownership of an identifier that does not belong to him. We use DIDs for participants but also for identifying data sets.

We use hash values for referencing to license or contract

documents. While we deal with simple text documents in this data space, the smart contract is agnostic of the employed format. The use of hash values as identifiers offers several advantages. Like DIDs, they can be created locally, but furthermore it is possible to directly prove the relationship between document and identifier without consulting any registry or extra data. On the other hand, hash algorithms also come with risks, as weaknesses in different cryptographic algorithms are regularly discovered. If a hash algorithm is not considered as secure anymore it might be possible to forge proofs of a contract conclusion with wrong documents. As a first measure, the information about the employed algorithm is always added to the hash value so that the hash algorithm can be exchanged quickly if the need arises. This might affect proofs for older entries, but as these proofs are usually needed for a small to medium time period only, and as in problematic cases it will most often still be possible to construct some proof manually, this is not considered to be critical in the context of the targeted application domain.

Smart contracts also play an essential role in supporting the credential issuance and verification operations, and thus the trustworthiness of the entire system. In addition to DIDs, we make use of Verifiable Credentials (VCs). These two concepts combined are one possibility for offering self-sovereign identities, which means that information, attributes, and certificates of one's identity can be kept by each participant. Only the issuance of VCs depends on certain authorities, whereas all the other steps involved in the authentication process are decentralized.

Firstly, the blockchain provides a DID registry used for DID resolution – given a DID, it returns the corresponding DID document, which contains the cryptographic information necessary to authenticate the DID holder. Secondly, it implements the credential registry, where the up-to-date status (*valid*/*revoked*/*deprecated*) of a VC is kept, enforcing the rule that only the issuer of that VC can update it. Finally, it keeps a list of all currently valid issuers of VCs, adding an important layer of trustworthiness and resistance to fake credentials.

VI. Evaluation of the Data Space Implementation

In the chosen approach, the blockchain serves as a protocol for events in the system that are considered to be potentially relevant for later inspections by different actors. But more than just being a place for logging, some processes and automatic checks also rely on the blockchain. Through providing this functionality in a transparent way, the trust of participants into the system should increase. The amount of information written to the blockchain is limited, because first of all, from a technical point, in order to achieve a consensus and because of high replication factors, blockchain-based systems are often designed as a storage of small to medium size with a rather limited throughput. But more relevantly, participants should not be forced to reveal information when it would be against their interest, and thereby be disincentivised to participate in the data space.

Participants investigate into concluded agreements of other participants. The relevant information is not expected to be extracted and presented in an easily understandable manner for everyone, but participants can make requests on information on the blockchain or do simple analyses for themselves. The connection between a participant and its principal account address is a priori not known by other participants, but is not considered to be secret either and it will be feasible for curious parties to make this connection. General license documents are visible for all participants while individual contract documents can be kept secret by provider and consumer. Datasets are referenced with their identifier both in agreements on the blockchain and in the catalogue, allowing curious parties also an insight in the data involved in exchanges by the provided metadata. In the context of other data spaces, these connections between exchanged data and involved parties might already be considered to be critical if participants might have no interest in disclosing what kind of data they are working with. There are ways to address this privacy concern, but they come at the cost of increasing the complexity of the implementation or losing functionality. Furthermore, by increasing privacy one decreases transparency and thus, potentially, trust in the correct working of the system or the behaviour of other participants. These findings have broader implications for data space implementations, emphasizing the delicate balance between privacy and transparency to ensure trust and facilitate data exchanges effectively.

VII. Conclusions

In this work we presented the principles and foundations as well as application scenario of a data space dedicated to the public security domain. Our work focuses on a data space for decentralized data exchange, illustrating the role of smart contracts, blockchain-based systems, and DIDs. Smart contracts are instrumental in establishing trustworthy protocols and enforcing compliance. Through a careful process encompassing data offer creation, contract conclusion, and data exchange, participants engage in transparent and tamper-proof transactions, underpinned by recording interactions of the participants on the blockchain. The adoption of DIDs based on Ethereum accounts enhances participant identification and data set referencing, improving the integrity and authenticity of documents in the data space. The utilization of hash values for document referencing ensures resilience against potential vulnerabilities. Furthermore, the introduction of a blockchain-based system in the general architecture as a means to establish trust is described, with the conception of transparent processes and the verification of certain conditions. Accessibility of information on the blockchain allows participants to review agreements and access relevant data, promoting transparency. However, privacy concerns regarding the connection between exchanged data and involved parties pose challenges, with potential solutions necessitating careful consideration of trade-offs between privacy, complexity, and functionality.

ACKNOWLEDGMENT

This research was supported by the European Commission under contract No. 101073951 LAGO and by the Austrian Gaia-X Hub.

REFERENCES

[1] M. Franklin, A. Halevy, and D. Maier, "From databases to dataspaces: a new abstraction for information management," *ACM Sigmod Record*, vol. 34, no. 4, pp. 27–33, 2005.

[2] B. Otto, M. ten Hompel, and S. Wrobel, *Designing Data Spaces: The Ecosystem Approach to Competitive Advantage*. Springer Nature, 2022.

[3] T. N. Dinh and M. T. Thai, "Ai and blockchain: A disruptive integration," *Computer*, vol. 51, no. 9, pp. 48–53, 2018.

[4] B.-P. Ivanschitz, T. Lampoltshammer, V. Mireles, A. Revenko, S. Schlarb, and L. Thurnay, "A semantic catalogue for the data market austria," 01 2018.

[5] Y. Hao, C. Piao, Y. Zhao, and X. Jiang, "Privacy preserving government data sharing based on hyperledger blockchain," in *Advances in E-Business Engineering for Ubiquitous Computing*, K.-M. Chao, L. Jiang, O. K. Hussain, S.-P. Ma, and X. Fei, Eds. Cham: Springer International Publishing, 2020, pp. 373–388.

[6] A. Treiber, D. Müllmann, T. Schneider, and I. Spiecker genannt Döhmann, "Data protection law and multi-party computation: Applications to information exchange between law enforcement agencies," in *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, ser. WPES'22. New York, NY, USA: Association for Computing Machinery, 2022, p. 69–82. [Online]. Available: https://doi.org/10.1145/3559613.3563192

[7] V. Wylde, N. Rawindaran, J. Lawrence, R. Balasubramanian, E. Prakash, A. Jayal, I. Khan, C. Hewage, and J. Platts, "Cybersecurity, data privacy and blockchain: A review," *SN Computer Science*, vol. 3, p. 127, 2022. [Online]. Available: https://doi.org/10.1007/s42979-022-01020-4

[8] V. Siska, V. Karagiannis, and M. Drobics, "Building a dataspace: Technical overview." [Online]. Available: https://zenodo.org/records/7907563

[9] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[10] "Verifiable credentials data model v1.1," World Wide Web Consortium. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[11] "Decentralized identifiers (dids) v1.0," World Wide Web Consortium. [Online]. Available: https://www.w3.org/TR/did-core/