An HFB interface for the adoption of blockchain in data spaces

Yasiru Witharanage[12], Santiago Figueroa-Lorenzo[123], and Saioa Arrizabalaga[123]

[1] CEIT-Basque Research and Technology Alliance (BRTA), Manuel Lardizabal 15, Donostia / San Sebastian, 20018, Basque Country, Spain.
[2] Universidad de Navarra, Tecnun, Manuel Lardizabal 13, Donostia / San Sebastian, 20018, Basque Country, Spain.
[3] Institute of Data Science and Artificial Intelligence (DATAI), Universidad de Navarra, Edificio Ismael Sánchez Bella, Campus Universitario, 31009-Pamplona, Spain

Abstract. Data is a fundamental asset for organizations. Data spaces emerge as distributed structures that promote secure and reliable data sharing. The International Data Space (IDS) protocol is currently one of the main standards in the data space environment. The growing evolution of data spaces implies the emergence of challenges associated with aspects such as digital sovereignty, decentralization, veracity, security and privacy protection. Distributed Ledger Technologies (DLTs) are emerging as information structures that can provide solutions to these challenges. This paper proposes the migration of trust entities in the IDS architecture, such as the Clearing House, to Hyperledger Fabric Blockchain infrastructure as a solution mechanism to the above challenges. To this end, it presents a Hyperledger Fabric Blockchain interface that guarantees the interaction between an IDS Connector and the blockchain, which is demonstrated in this study with an Eclipse Dataspace Components (EDC) Connector.

Keywords: Blockchain, Data spaces, EDC, HFB

1 Introduction

Data is a fundamental asset for organizations as it generates competitive advantages, both in decision-making and the generation of new services. According to Gartner Research, data sharing provides several benefits to organizations that drive efficiency in supply chains, spur innovation and enable faster product development [1]. Data spaces emerge as decentralized infrastructures with common regulatory and technical standards, where diverse actors can share, access and use data in a secure, reliable and trustworthy way [2]. In addition to being a part of the European strategy for data [2], the growth of data spaces is driven by a focus on the

David C. Wyld et al. (Eds): NLAI, IBCOM, MLDS, GridCom, SCAI, ICCSEA, SPPR – 2024
pp. 75-99, 2024. - CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.142206

non-functional requirements of the industry such as interoperability, auditability, accountability, maintainability, scalability (thus high availability) and sovereignty.

However, such an ambitious strategy involves considerable challenges. For example, Gartner predicts that government organizations will establish formal accountability structures for data sharing in 2024, including standards for data structure, quality and timeliness [1]. In addition, the Big Data Value Association (BDVA) has defined the challenges of data spaces with regard to several categories, in which their technical challenges involve aspects such as digital sovereignty (delegating the control of data to its owner), decentralization, veracity (quality of data), security and privacy protection [3]. In this context, Distributed Ledger Technology (DLT) constitutes an emerging technology in data spaces that can partially address these challenges due to its robust approach to data management, security, immutability, data integrity and provenance [4]. Data spaces literature recognizes the relevance of using blockchain technology as part of data spaces, e.g. for transparency, auditability, confidentiality, interoperability and portability [2]. Consequently, it must be adopted and integrated into the subsequent implementation layers of data spaces such as Eclipse Dataspace Components (EDC). A permissioned blockchain with an open, proven and enterprise-grade framework, such as Hyperledger Fabric Blockchain (HFB), can be considered a viable alternative for such applications in the industrial context.

The main contribution of this article is to ensure the adoption of blockchain technology in data spaces, through a proposal for an interface in IDS Connectors that interacts with Hyperledger Fabric. Consequently, this enables the migration of data space trust entities to HFB, where its underlying blockchain technology enhances the trust of such entities by fulfilling their non-functional requirements such as auditability, sovereignty, transparency and traceability.

The rest of the manuscript is structured as follows: Section 2 introduces concepts such as data spaces, IDS architecture, EDC and blockchain with HFB Framework. Section 3 discusses the existing work on integrating blockchain technology into data spaces as well as a review of how blockchain technology fulfills its non-functional requirements. Section 4 proposes the EDC-HFB interface with regard to the functionality of a Clearing House. Section 5 discusses the presented approach with possible future work and finally the paper presents conclusions.

2 Background

This section provides an overview of data spaces while focusing on the International Data Space Association (IDSA) and its reference architecture promoted by the International Data Space (IDS) protocol. The section also considers Eclipse Dataspace Component (EDC) as a base implementation that follows the IDSA recommendations. Finally, DLT technologies are introduced with a particular focus on HFB, which serves as a permissioned blockchain framework.

2.1 Data spaces overview

Data space is a distributed data integration concept where data providers deliver their data to consumers under a common technical and legislative standardized framework. The data spaces are built based on principles such as data sovereignty, transparency, security, fairness, consumer protection, fundamental rights, citizen centricity, data altruism (sharing data for the benefit of others), inclusion, sustainability, openness, self-determination, trust, fair competition and innovation [1]. On a legislative level, the European Union (EU) data spaces concept is driven by policies such as the European Strategy for Data [5], which is designed to enhance data access, sharing and governance. It further aims to integrate sector-specific data spaces into a unified data market for the EU. IDSA is an organization that brings together numerous industrial actors to provide a technology-agnostic and standardized description of a data space and its distributed software architecture. The International Data Space (IDS) protocol is developed and maintained by IDSA and Gaia-X[4].

2.2 IDS architecture and protocols

As a distributed network, IDS relies on the connection of different participants with IDS Connectors and other core components (Fig. 1). The IDS Connector serves as a gateway component with multiple endpoints to initiate and execute data transfer processes between the participating organizations in a data space. A self-description of a Connector (e.g. technical interface description, authentication mechanism) along with a catalog of data (e.g. associated data usage policies) can be provided to a Metadata Broker such that the Connector becomes discoverable to any interested party. A Connector can enforce restrictions on the exchanged data via usage policies and transfer them to a Clearing House for further trust and transparency. In essence, a Clearing House logs all activities related to a data exchange process which can be used later for billing, clearing and conflict resolution purposes. Semantic interoperability (i.e. interpreting the meaning unambiguously) of the exchanged data is enabled via Vocabulary Hubs, which stores and offers information that describes datasets (e.g. ontologies, reference data models, metadata elements).

The IDS protocol separates the scope of information transfer into two concepts: control plane and data plane. In particular, the control plane comprises a set of reusable components for cataloging data with access and usage policies, negotiating their contracts and managing data transfer processes. The data plane associates with the actual exchange of application data through different protocol implementations such as Hypertext Transfer Protocol (HTTP) and Kafka[5]. In addition to

[4] https://gaia-x.eu/gaia-x-framework

[5] https://kafka.apache.org/documentation

the core functions, complementary services (e.g. adapters for enterprise information systems) and operations (e.g. data transformation) can be executed on data by downloading relevant IDS Apps to a Connector. Alternatively, custom container applications can be implemented and deployed within a Connector as necessary (e.g. an application that forwards data to a blockchain).

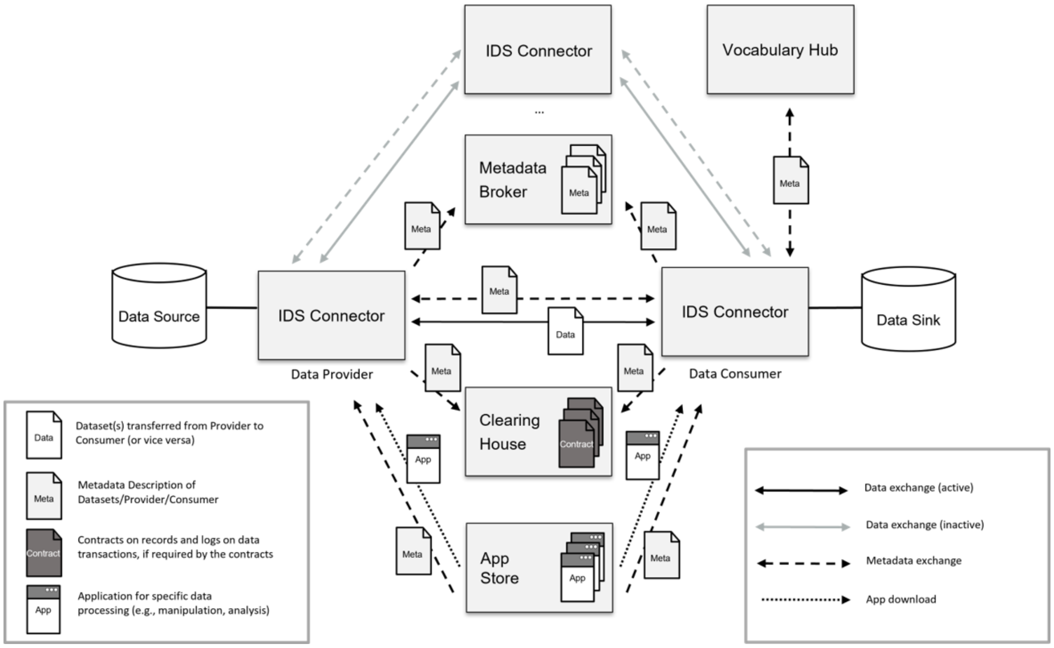
IDS Connector
Vocabulary Hub
...
Metadata Broker
Meta
Data Source
IDS Connector
Data Provider
IDS Connector
Data Consumer
Data Sink
Data
Clearing House
Contract
App
App Store
Dataset(s) transferred from Provider to Consumer (or vice versa)
Metadata Description of Datasets/Provider/Consumer
Contracts on records and logs on data transactions, if required by the contracts
Application for specific data processing (e.g., manipulation, analysis)
Data exchange (active)
Data exchange (inactive)
Metadata exchange
App download

Fig. 1. International Data Space Architecture [6]

2.3 Eclipse Dataspace Components (EDC)

EDC is maintained as an open-source project under the governance of the Eclipse Foundation[6]. It provides a framework with components (e.g. Connector, Federated Catalog) to implement a data space in compliance with the IDS Reference Architecture Model (IDS-RAM) and its certification scheme. Particularly, the IDS protocol guarantees technical interoperability among different Connector implementations given that they follow the IDS-RAM standards. The implementation of EDC Connector preserves software modularity such that it allows core modifications and service extensions to the Connector through well-defined interfaces. Due to this loose coupling with the dependencies, different technologies can be implemented and substituted as appropriate (e.g. a Clearing House service based on blockchain technology). The EDC Connector has been listed as a project of the IDS

[6] https://www.eclipse.org

open-source graduation scheme and is further supported by organizations such as Fraunhofer Institute for Software and Systems Engineering ISST, Mercedes-Benz Tech Innovation, BMW Group, Deutsche Telekom, Amadeus, Microsoft, Google, AWS, SAP and ZF Friedrichshafen [7].

2.4 Blockhchain and Hyperledger Fabric Blockchain (HFB)

A blockchain is a shared distributed ledger that records transactions in a network maintained by multiple nodes, where such nodes do not trust each other. In particular, blockchain technologies provide serializability (i.e. a consistent sequence of data), immutability and cryptographic verifiability for data (e.g. authenticating the sender of a transaction) without a single point of trust [8]. Two blockchain categories can be identified as permissionless (e.g. Bitcoin [9], Ethereum [10]) and permissioned (e.g. HFB [11]). In the former, anyone can join the network to perform transactions anonymously whereas the latter requires authentication for its participants, thus making it more suitable for enterprise applications.

As a permissioned blockchain, Hyperledger Fabric allows its organizations to maintain their own network infrastructures and participate in multiple distributed ledgers within the same blockchain network. In the context of HFB, ledgers are maintained as channels that consist of two parts: a database to support efficient queries and a blockchain to record all transactions with immutability and data provenance. It further complements this framework with client applications and chaincodes to enable functionalities that require interactions with the ledger data. For instance, a data space connector may persist data in Hyperledger Fabric by implementing a *set* function in a chaincode and exposing it through a client application to the connector. Consequently, HFB yields the potential to implement external trust services of a data space (e.g. Clearing House) due to its features such as permissioned membership, granular privacy of data, support for rich queries and higher performance compared to other permissioned blockchains [12, 13].

3 Related work

This section analyzes the prior work related to the state of the art for using blockchain technology in the context of data spaces. In addition, this summarizes how non-functional requirements of a data space are covered in other use cases through blockchain technology.

3.1 Blockchain technology uses in data spaces

The potential of blockchain to reinforce IDS-RAM architectural concepts is recognized, with IDSA examining its application in data storage and cataloging.

Blockchain's applicability in IDS is debated on [14] for the implementation of Identity Provider, Broker Service and Clearing House. Extending these roles further, Prinz et. al [15] have proposed blockchain for storing smart contracts, which can dictate actions within a data space according to a set of defined rules to facilitate authorization and access and usage control mechanisms. Moreover, the Data Spaces Support Centre (DSSC) blueprint document [16] emphasizes the use of blockchain for decentralized identity management and storage of participants' identities. Kovach et. al [17] propose an entire data plane modification of the IDS protocol using DLT, which is based on IoTA's Directed Acyclic Graph (DAG) and oriented to support high throughput and low latency. Jürjens et. al discuss the adoption of decentralized Tokenomics to incentivize the participants in a data space for the initial investments of its infrastructure setup [18].

3.2 Shared properties between blockchain and data spaces

The IDS reference architecture primarily focuses on integrating DLT to support storage and catalog functionalities of a data space [14]. In particular, the properties of blockchain technology such as immutability, transparency and provenance of data can be immensely beneficial for data space use cases such as healthcare and supply chain management. An authentication mechanism based on Verifiable Credentials (VCs) with blockchain also realizes the key design principles of a data space, such as sovereignty and trust [19]. However, this section explores the further possibilities that exist in a data space where blockchain can be adopted in other use cases.

Considering the broader context of the vision and key principles for European data sharing, the European Commission has synthesized a set of requirements [2] which have been derived from policy sources such as SWD (Staff Working Document) on data spaces and DIGITAL work programme [20]. Table 1 lists these defined functional and non-functional requirements and further exemplifies them with existing blockchain-based use cases. Consequently, an analysis associated with the Table 1 findings would indicate how blockchain technology can be applicable in the context of data spaces beyond those associated with cataloging and storage functions.

4 Blockchain-based proposal

This section describes the process of integrating blockchain technology into the trust entities of data spaces. As an example, it demonstrates how the functions of a Clearing House can be migrated to Hyperledger Fabric through a set of interfaces implemented in an EDC Connector based on its modularity.

One of the essential features of IDS architecture is the separation of data and control planes, where the data plane functions are associated with the transfer of

Policy provision	Functional requirements	Non-functional requirements	Blockchain use cases
- A secure and privacy-preserving IT infrastructure to pool, access, process, use and share data.	- Data transfer and exchange - Data storage - Data processing and analytics - Data pooling and collaboration	- Security - Confidentiality	[22]
- Data holders will have the possibility, in the data space, to grant access to or share certain personal or non-personal data under their control.	- Identity, authentication and access control - Usage control policies	- Confidentiality - Sovereignty	[23]
- Data holders could use tools to ease the uploading of data into data spaces, to give or revoke their authorisation to data and to change access rights and specify new conditions of how their data can be accessed and reused over time.	- Data transfer and exchange - Identity, authentication and access control - Usage control policies	- Interoperability - Auditability	[24]
- Data that is made available can be reused against compensation, including remuneration, or for free.	- Transaction metering and billing	- Data valuation	[25]
- European rules and values, in particular personal data protection, consumer protection legislation and competition law, are fully respected.	- Compliance monitoring and auditing - Data protection	- Auditability	[26]
- Enhance the development of new data-driven products and services in the EU and thereby create the core tissue of an interconnected and competitive European data economy.	- Data processing and analytics	- Sovereignty - Data level playing field	[27]
- Data spaces middleware: provide data mapping services, data anonymisation and masking services.	- Privacy-preserving mechanisms - Data interoperability features	- Confidentiality - Interoperability	[28]
- Data spaces middleware: provide secure resource efficient data storage services.	- Data storage		[29]
- A common European data space brings together relevant data infrastructures and governance frameworks in order to facilitate data pooling and sharing. - A clear and practical structure for access to and use of data in a fair, transparent, proportionate and/non-discriminatory manner and clear and trustworthy data governance mechanisms.	- Data pooling and collaboration - Usage control policies - Privacy-preserving mechanisms - Data protection - Data governance	- Inclusivity - Fairness - Sustainability - Trustworthiness - Transparency	[30]

Table 1. Relation between blockchain use cases and data space requirements.

application data. The distributed environment of data spaces depends on maintaining Peer-to-Peer (P2P) relationships between connectors, which are established through the control plane. In addition to such P2P relationships, the control plane also interacts with trusted entities (e.g. Clearing House) in the current IDS architecture. These interactions are usually related to functionalities such as data governance, access control, trust management, metadata management, policy enforcement, monitoring and auditing. For this reason, the study considers it relevant that the interactions with blockchain technology are conducted from a control plane perspective.

4.1 HFB interface for Clearing House

An HFB interface is integrated into the IDS Connector as one of its service extensions, while primarily focusing on the control plane (Fig. 2). During a process (e.g. negotiation, data transfer), the relevant activities can be digitally signed (for non-repudiation) and emitted by a connector through this interface to a client application, which then interacts with a smart contract and persists such activities in an HFB network. In particular, it stores these messages in both blockchain and the state database. The former provides immutability and provenance for the logged activities whereas the latter supports efficient message queries whenever required. Consequently, HFB can be considered a potential platform for the application of Clearing House.

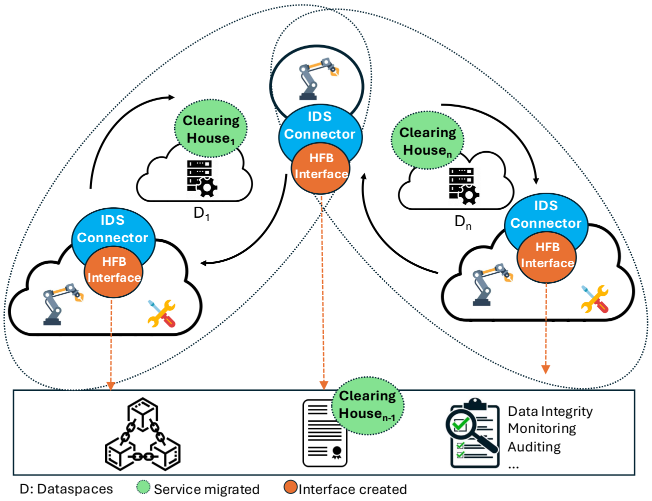

Fig. 2. HFB-based Clearing House and Connector interface

This section only focuses on the Logging service of the Clearing House, which can be feasibly migrated due to its API-oriented functionalities such as creating a process, logging activities and querying messages of a process [21]. Such APIs can be invoked by a Connector at the time when it sends (receives) a message to (from) another Connector [20]. Despite the interface being defined based on the Clearing House use case, it can also be modified as necessary to support the integration of a new trust entity (e.g. Metadata Broker).

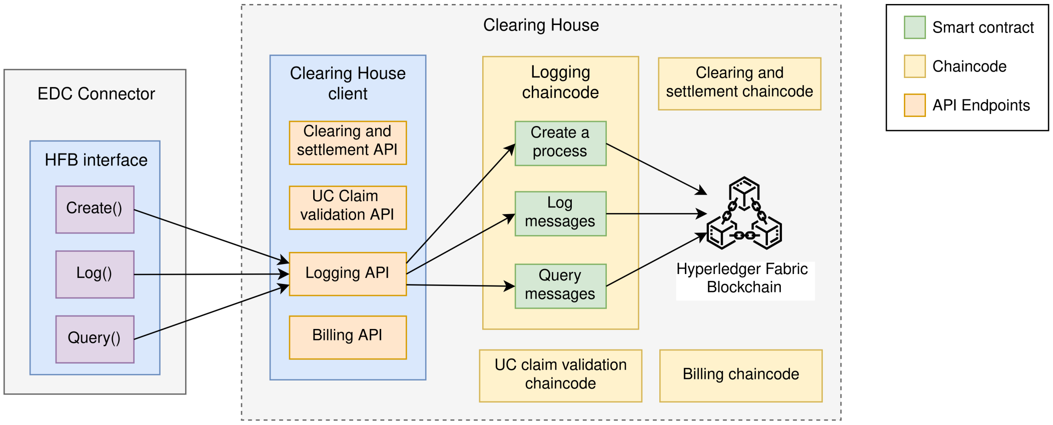

Fig. 3. Software design of components and their interactions

The software design of the proposed Clearing House (Fig. 3) shows how its services can be migrated to HFB along with the invocation flow from an EDC Connector. Each API endpoint of the Clearing House can be implemented in a distinctive smart contract with the core functions and essential features (e.g. validating if a Connector has *write* permissions before logging an activity in a process). These smart contracts combine into a chaincode to form an individual service of the Clearing House (e.g. create, log and query smart contracts form the Logging service chaincode). Such chaincodes will be exposed to external IDS Connectors via client applications with relevant API endpoints. Any additional feature to the primary flow of a particular service (e.g. middleware) can be included in the client application. HFB interface, client application and chaincodes construct the logical Clearing House despite that they can be located separately in different networks based on the use case.

The following subsections describe the message flows of each function of a Logging service and how they can be migrated with the proposed HFB interface.

Creating a process: A process in the Clearing House represents an instance of data exchange along with its contract agreement and other relevant messages. Consequently, a process with a unique ID and a list of owners should be created in the Clearing House, under which all the subsequent activities of its data exchange will be logged. In this proposal, an IDS Connector (exemplified with an EDC Connector) uses an HFB interface to create a process in the Clearing House, by invoking the corresponding chaincode through a client application as shown in Figure 4.

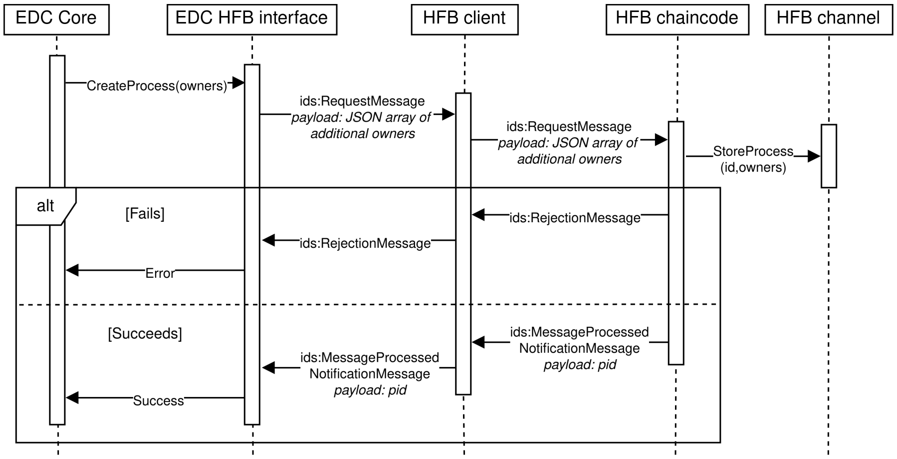

Fig. 4. Creating a process with HFB interface

Logging messages: The information that should be logged in the Clearing House is sent in the payload of a Log Message. This information can either be hashed or in plain depending on the use case, whereas the former ensures data sovereignty since the Clearing House will not be able to decrypt the message [20]. The log entry stored in the Clearing House consists of the payload and metadata from the Log Message, given that it is sent by an owner of the process with *write* permissions. Messages can either be sent to an existing process or a non-existing process, in which case the Clearing House will create a new process.

This entire functionality can be transformed into blockchain technology with the proposed HFB interface, specifically by sending requests to the client application for logging activities. These requests will be redirected to the corresponding smart contract and persisted in the distributed ledger. Fig. 5 shows this message flow between the HFB interface and the Clearing House chaincode.

Querying messages: Given the proper authentication, an IDS Connector can retrieve the log entries for a specific process. When queried with a process ID, the Clearing House responds with a Result Message that contains all the log entries of the process. If the request corresponds to a particular log ID, it will respond only with the relevant log entry. In the case of multiple log entries, the payload of the Result message will contain a JSON array of Log Messages, and if otherwise, it will only return a single Log Message. Fig. 6 and 7 show the sequences of messages in both these query functions with the corresponding data types.

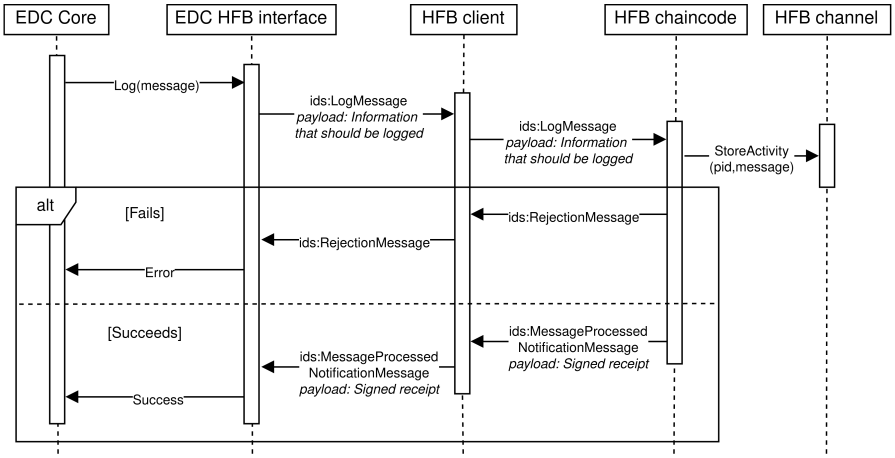

Fig. 5. Logging messages with HFB interface

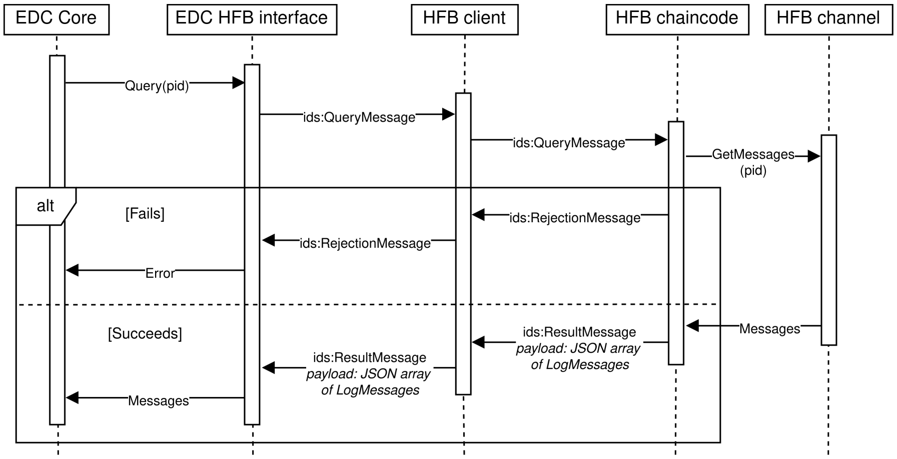

Fig. 6. Querying all logs with HFB interface

5 Discussion and future work

In addition to the technical feasibility of implementing a Clearing House (as described in section 4.1), HFB further complies with its non-functional requirements. As a blockchain technology, it provides data immutability and provenance to support the primary operations of a Clearing House such as clearing, billing, auditing and conflict resolution. It further enforces privacy on data via distinctive channels, permissioned memberships, chaincode access control and private data collections. Endorsement policies when combined with participants' signatures deliver integrity and non-repudiation for the log messages. Due to the elimination of external parties, it also minimizes the possibility of exploiting the logged information for financial

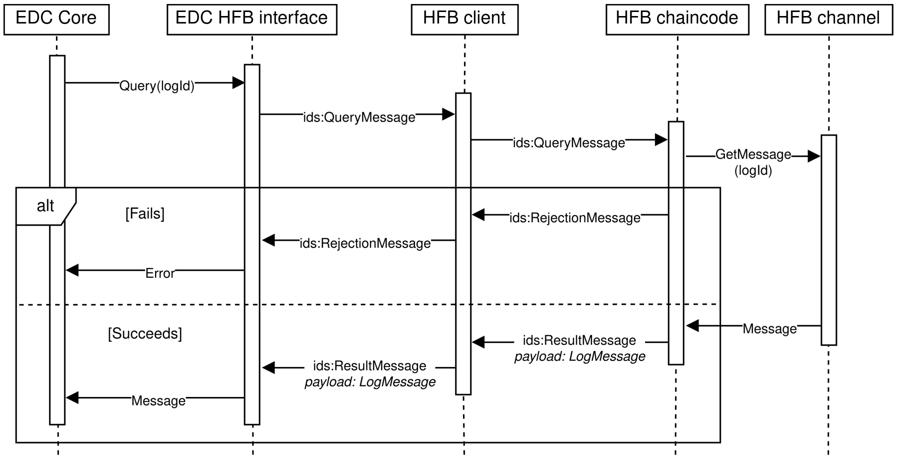

Fig. 7. Querying a single message with HFB interface

gains. Nevertheless, access can be granted explicitly to messages upon request (e.g. for auditors), thus preserving sovereignty and providing cryptographic verifiability.

However, there are several considerations that should be addressed when adopting the proposed approach. Since the external service is based on a decentralized architecture, it involves initialization and maintenance cost of a blockchain network with multiple nodes (e.g. peers, orderers). Moreover, it executes the Clearing House functions through a chaincode and therefore, the integrity and security of such chaincodes should be investigated thoroughly. It also introduces the cost of a transaction flow with ordering and validation phases to each single message, as opposed to a centralized Clearing House architecture.

Despite the approach being presented with an EDC Connector, its abstract interface can generally be applied to all the IDS Connectors that support modularity for integrating service components. Similarly, it can be adopted across multiple data space use cases in addition to the Logging Service of a Clearing House. A potential future work can examine how separate channels with private data collections in HFB can be used to enforce granular privacy for trust entities. This study can also be extended to investigate using data space components such as Identity Providers, DAPS (Dynamic Attribute Provisioning Service) and DTM (Dynamic Trust Monitoring) to provide authentication and authorization in HFB-based data space services.

6 Conclusion

This paper analyses the applicability of blockchain technology in data spaces and indicates how the requirements of a data space have already been fulfilled by the existing blockchain use cases. It then proposes an interface to IDS-compliant Connectors that enables the migration of trust entities to a blockchain. This is demonstrated with a Clearing House use case and an EDC Connector, where its standard messages traverse through the proposed HFB interface, a client application and the corresponding HFB chaincode. These relationships belong to the control plane such that the data plane continues to maintain its distributed P2P approach focused solely on the data exchange process. Through the adoption of blockchain, the proposal ensures the non-functional requirements of the Clearing House such as auditability, sovereignty, transparency and traceability of information.

Acknowledgment

The authors would like to acknowledge the support of the ”PLIADES: AI-Enabled Data Lifecycles Optimization and Data Spaces Integration for Increased Efficiency and Interoperability” project. This project has received funding from the European Union’s Horizon Europe research and innovation programme under grant agreement No. 101135988.

References

1. B. Kaner, A. Mickoleit, Top Trends in Government: Data Sharing as a Program, 2023, https://www.gartner.com/en/doc/785079-top-trends-in-government-data-sharing-as-a-program.
2. European Commission, Joint Research Centre, Farrell, E., Minghini, M., Kotsev, A. et al., European data spaces – Scientific insights into data sharing and utilisation at scale, 2023.
3. Scerri, S., Tuikka, T., de Vallejo, I.L., Curry, E., Common European Data Spaces: Challenges and Opportunities, 2022, In: Curry, E., Scerri, S., Tuikka, T. (eds) Data Spaces. Springer.
4. L. D. Nguyen, A. Br¨oring, M. Pizzol, and P. Popovski, “Analysis of distributed ledger technologies for industrial manufacturing,” Scientific Reports 2022 12:1, vol. 12, pp. 1–11, 10 2022.
5. European Commission, “A European Strategy for Data.” [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/strategy-data.
6. O. Boris, M. Hompel, and S. Wrobel. ”International Data Spaces: Reference architecture for the digitization of industries.” Digital transformation (2019): 109-128.
7. M. Spiekermann, S. Steinbuss, “Eclipse Dataspace Components and IDSA: Let’s build our data-driven future together!.” [Online]. Available: https://internationaldataspaces.org/eclipse-dataspace-components-and-idsa-lets-build-our-data-driven-future-together/
8. P. Thakkar, S. Nathan, and B. Viswanathan, “Performance benchmarking and optimizing hyperledger fabric blockchain platform,” in Proc. IEEE 26th Int. Symp. Model., Anal., Simul. Comput. Telecommun. Syst. (MASCOTS), Milwaukee, Wisconsin, Sep. 2018, pp. 264–276.
9. S. Nakamoto. (2008). A Peer-To-Peer Electronic Cash System. Accessed: Feb. 1, 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf
10. G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, pp. 1–32, Apr. 2017.
11. Open Source Blockchain Technologies. Accessed: Feb. 1, 2023. [Online]. Available: https://www.hyperledger.org/
12. J. Polge, J. Robert, and Y. Le Traon. (2020). Permissioned blockchain frameworks in the industry: A comparison. ICT Express. 7. 10.1016/j.icte.2020.09.002.

13. P. Ruan, T. Tuan Anh Dinh, D. Loghin, M. Zhang, G. Chen, Q. Lin, and Beng Chin Ooi. 2021. Blockchains vs. Distributed Databases: Dichotomy and Fusion. In Proceedings of the 2021 International Conference on Management of Data (SIGMOD '21). Association for Computing Machinery, New York, NY, USA, 1504–1517. https://doi.org/10.1145/3448016.3452789
14. S. Steinbuss, M. Punter, F. Fournier, and I. Skarbovski, "Blockchain Technology in IDS," International Data Spaces Association, 2019.
15. W. Prinz, T. Rose, and N. Urbach, "Blockchain Technology and International Data Spaces," in Designing Data Spaces, B. Otto, M. ten Hompel, and S. Wrobel, Eds. Springer, Cham, 2022, pp. 165–180.
16. Data Spaces Support Centre, "Data Spaces Blueprint v.0.5," 2023.
17. A. Kovach, L. Montalvillo, A. Urbieta and J. Lanza, "IOTA-Enabled Decentralized Data Space for IIoT Ecosystems," 2024.
18. Jürjens, J., Scheider, S., Yildirim, F., Henke, M. (2022). Tokenomics: Decentralized Incentivization in the Context of Data Spaces. In: Otto, B., ten Hompel, M., Wrobel, S. (eds) Designing Data Spaces . Springer, Cham. https://doi.org/10.1007/978-3-030-93975-5_6
19. Nagel L., Lycklama D. (2021): Design Principles for Data Spaces. Position Paper. Version 1.0. http://doi.org/10.5281/zenodo.5105744
20. "Staff working document on data spaces," Shaping Europe's Digital Future, Feb. 14, 2022. https://digital-strategy.ec.europa.eu/en/library/staff-working-document-data-spaces
21. S. Steinbuss, S. Bader. (2020). Specification: IDS Clearing House (Version 1.0). International Data Spaces Association. https://doi.org/10.5281/zenodo.5675765
22. L. Zhu, S. Song, S. Peng, W. Wang, S. Hu and W. Lan, "The Blockchain and Homomorphic Encryption Data Sharing Method in Privacy-Preserving Computing," 2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science (BCD), Danang, Vietnam, 2022, pp. 84-87, doi: 10.1109/BCD54882.2022.9900530.
23. V. Aanandaram and P. Deepalakshmi, "Blockchain-based Digital Identity for Secure Authentication of IoT Devices In 5G Networks," 2024 Third INCOS conference.
24. Y. Wang et al., "SPDS: A Secure and Auditable Private Data Sharing Scheme for Smart Grid Based on Blockchain," in IEEE Transactions on Industrial Informatics, vol. 17, no. 11, pp. 7688-7699, Nov. 2021, doi: 10.1109/TII.2020.3040171.
25. S. Jeong, N. -N. Dao, Y. Lee, C. Lee and S. Cho, "Blockchain Based Billing System for Electric Vehicle and Charging Station," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), Prague, 2018.
26. C. Ju, W. Tang, C. Chenli, G. Lee, J. H. Seo and T. Jung, "Monitoring Provenance of Delegated Personal Data with Blockchain," 2022 IEEE International Conference on Blockchain (Blockchain), Espoo.
27. G. Bigini, M. Zichichi, E. Lattanzi, S. Ferretti and G. D'Angelo, "Decentralized Health Data Distribution: A DLT-based Architecture for Data Protection," 2022 IEEE International Conference on Blockchain (Blockchain), Espoo, 2022.
28. H. C. Chong and K. L. Eddie Law, "Multi-Blockchain Model for Data Sharing with Bell-LaPadula Access Control," 2023 IEEE International Conference on Blockchain (Blockchain), Danzhou, China.
29. X. Wang et al., "Application of data storage management system in blockchain-based technology," 2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA).
30. A. Sasikumar, L. Ravi, K. Kotecha, A. Abraham, M. Devarajan and S. Vairavasundaram, "A Secure Big Data Storage Framework Based on Blockchain Consensus Mechanism With Flexible Finality," in IEEE Access, vol. 11, pp. 56712-56725, 2023.

Authors

Yasiru Witharanage received his BSc (Hons) in Computer Science & Engineering from University of Moratuwa, Sri Lanka and MSc in Computer Science from The Arctic University of Norway. He has also worked in the industry for several years as a software engineer related to distributed systems. He is currently pursuing his PhD in Computer Science in CEIT Research Center, Spain focusing mainly on data spaces and distributed ledger technologies.

Santiago Figueroa Lorenzo is a researcher at CEIT, collaborating professor at TECNUN (University of Navarra) and associate director of the Data Analysis and Information Management group (DAIM). He obtained the Master in Telecommunication and Telematics Systems by the Faculty of Engineering of Havana (University of Havana) in 2012 and the PhD in Applied Engineering by TECNUN (University of Navarra) in 2021 with specialization in the line of cybersecurity in identity and access management issues in Industrial Internet of Things environments. His current research areas are Security in ICS and IoT systems, Identity and Access Management of systems, Privacy Protection and automation of the Secure Software Development Life Cycle.

Saioa Arrizabalaga received the M.Sc. degree in telecommunication engineering from the University of the Basque Country, in 2003, and the Ph.D. degree from the University of Navarra, Spain, in 2009. She has been a Research Staff Member with CEIT, San Sebastian, Spain, since 2003, and an Associate Professor with the University of Navarra, since 2009. She is currently the Director of the Data Analysis and Information Management Research Group, CEIT. She has been involved in more than 45 national and international projects and is the coauthor of more than 70 scientific contributions in congresses and journals. Her current research interests include data analytics and cybersecurity.