Theoretical Integration of Hyperledger Fabric in Gaia-X: Towards an Approach for Federated Data Access

Liron Ahmeti*, Klara Dolos*, Conrad Meyer*, Andreas Attenberger*, Rudolf Hackenberg†
*Research Unit, Central Office for Information Technology in the Security Sector
Munich, Germany
Email: poststelle@zitis.bund.de
†Dept. Informatics and Mathematics, OTH Regensburg
Regensburg, Germany
Email: rudolf.hackenberg@oth-regensburg.de

***Abstract*—Securing and managing distributed data in federated ecosystems is a key challenge when data protection, sovereignty and interoperability need to be guaranteed at the same time. Previous blockchain-based solutions often reach their limits in terms of integration capability and fine-grained access mechanisms. This theoretical paper presents a multilayered architecture concept that integrates Hyperledger Fabric into the Gaia-X ecosystem. Advanced encryption methods and a smart-contract-based reassembly logic are used to securely distribute fragmented data and make it accessible only to authorized actors. The approach promotes digital sovereignty and scalability within Gaia-X-compliant data spaces and serves as an initial conceptual basis that will be technically validated and further developed in future work.**

***Keywords*-Gaia-X; blockchain; architecture concept; federated data spaces**

I. Introduction

Incorporating blockchain technology into existing and new digital ecosystems can promote a secure and decentralized method for storing and managing data while creating new opportunities for effective data governance and interoperability. Gaia-X, a European initiative, aims to create a secure and federated data ecosystem in Europe, allowing participants to share information interoperably while maintaining their digital sovereignty [1]. In this context, Hyperledger Fabric is presented as a blockchain platform that provides a flexible basis for such integrations through its permission-based architecture and the ability to implement smart contracts. The main goal of this paper is to develop an architecture to merge Hyperledger Fabric and the Gaia-X ecosystem to implement an interoperable private blockchain. These requirements include the ability to store data in an encrypted and partitioned manner and to reassemble and make this data accessible. The research will focus on the following key questions:

i How can blockchain be designed to be compatible with Gaia-X to store and reassemble encrypted, split data?
ii What security measures are necessary to ensure the integrity and confidentiality of the data?
iii What challenges and opportunities arise from integrating blockchain technology into the Gaia-X ecosystem?

By answering these questions, this approach will help promote digital sovereignty and improve interoperability within the Gaia-X ecosystem. The remainder of the paper is organized as follows: Section II analyses the current state of the art and associated challenges. Section III presents the conceptual model, explaining the multi-layered structure of the system. Finally, Section IV discusses the advantages and disadvantages of the proposed approach and provides an outlook on future empirical validations and further developments.

II. Related Work

Secure and decentralized data management is becoming increasingly important, especially in trustworthy data ecosystems. Blockchain technology, particularly Hyperledger Fabric, offers promising approaches for secure data management through decentralization, transparency and tamper-proofing. At the same time, Gaia-X is pursuing the goal of establishing a federated and interoperable European data infrastructure. Integrating blockchain into Gaia-X could create new opportunities for trustworthy and privacy-compliant data spaces. A key aspect is data encryption and sharing to meet data protection requirements while ensuring efficient use and storage of sensitive information. This section provides an overview of the current state of research on blockchain technology, Gaia-X and data encryption and sharing methods in the context of distributed systems.

A. Blockchain

Blockchain technology has emerged as a transformative innovation, initially conceptualized by Nakamoto as the framework for Bitcoin [2]. Since then, it has evolved beyond cryptocurrencies to become a foundation for secure, decentralized, and transparent data exchange [3]. As a distributed ledger technology, blockchain enables immutable, trustless transactions without intermediaries [4]. Its applications span various sectors, including finance, healthcare, supply chain management, and identity verification [5][6]. Blockchains are typically classified into three categories: public, private, and consortium [7]. Public blockchains, like Bitcoin and Ethereum, operate in open, permissionless environments but face challenges, such as high energy consumption and scalability [3]. In contrast, private blockchains restrict access to authorized entities, which enhances efficiency and security [8]. Current research is focused on optimizing consensus mechanisms and improving interoperability with existing digital infrastructures

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

Copyright (c) IARIA, 2025. ISBN: 978-1-68558-258-6

to fully realize the transformative capabilities of blockchain [8]. Current research focuses on optimizing consensus and improving interoperability with established infrastructures, aiming to harness blockchain's transformative potential [8] fully. However, many existing solutions concentrate on single-use cases or rely on built-in cryptocurrencies, reducing flexibility in more complex enterprise scenarios [5].

B. Hyperledger Fabric

Hyperledger Fabric is an open-source blockchain framework tailored for enterprise use. It processes transactions in three phases: Execution, Ordering, and Validation. Initially, transactions are simulated to assess their impacts, then ordered by a dedicated group of nodes, and validated by peer nodes before updating the ledger. This design reduces bottlenecks typical in 'order-execute' systems, enhancing modularity and scalability. In a Fabric network, nodes called peers carry out various roles. Endorsing peers execute chain code to simulate and sign transactions, which are then sent to the ordering service for final arrangement. After consensus, participants validate endorsements and check for conflicts before adding transactions to the ledger. With verifiable identities issued by the Membership Service Provider (MSP), Hyperledger Fabric operates as a permissioned system. This eliminates the need for an internal cryptocurrency and allows users to choose a suitable consensus mechanism. By isolating chain code in Docker containers, Fabric increases security and supports fine-grained data control, enabling channels to restrict information sharing to specific participants. These features make Hyperledger Fabric a robust option for enterprise applications [9], nonetheless, cross-platform interoperability, off-chain data integration, and performance tuning remain challenges [9].

C. Gaia-X

Gaia-X is an initiative to create a federated, secure data infrastructure that promotes data sovereignty and interoperability. This is done by setting up so-called data spaces, i.e. digital representations of different sectors, such as health, agriculture or mobility, which enable secure and transparent data exchange between multiple stakeholders [10]. The architecture is based on three principles: Federation, decentralization and openness [11]. Federation allows different actors to retain their autonomy and interact in the ecosystem. Decentralization ensures no central body controls all processes, strengthening scalability and flexibility. Openness makes all Gaia-X components visible and accessible. A central element is the federation services, which include identity and trust management and support the federated catalogue to find suitable providers and services [11]. Providers register self-descriptions transferred as linked data into a knowledge graph so that users can query and filter them [11]. The Gaia-X Trust Framework also ensures security and compliance so all participants can operate in a protected environment [11]. A Trust Anchor instance acts as the issuing authority for digital identities [12] and confirms the identity of persons, organizations and devices [13]. These identities are based on the Self-Sovereign Identity (SSI) concept, which allows users to manage their digital credentials without central services [13]. An SSI wallet enables the secure storage of identity data and direct, trustworthy exchange.

D. Data encryption and splitting

Encryption and splitting techniques have long been essential for secure data distribution. Modern approaches, such as threshold cryptography and Content-Defined Chunking(CDC), aim to reduce single points of failure and permit partial reassembly only by authorized users. However, these solutions typically focus on data at rest within specialized storage systems and do not adequately consider interactions with external clouds or global consortia like Gaia-X. Additionally, the complexities of key management and vulnerabilities related to side channels, such as deduplication leaks, further complicate their implementation in real-world scenarios.However, most of these approaches focus solely on data security measures and do not fully address how to integrate external cloud infrastructures or handle large-scale federation requirements (e.g. in Gaia-X scenarios) [1][6]. Many solutions rely on a single blockchain domain, leaving a gap in unified, end-to-end architectures that connect on-chain trust mechanisms with off-chain systems.
Current research highlights the potential of Hyperledger Fabric for secure, tamper-proof data management and the capabilities of Gaia-X for federated trust and service discovery. However, few comprehensive approaches integrate these two technologies to create a unified architecture. Specifically, such an architecture should provide on-chain trust, align with Gaia-X's identity and trust framework, and incorporate strong encryption and data segmentation for sensitive information. Our work addresses this gap by proposing an integrated solution that connects Fabric and Gaia-X while leveraging best practices in data protection for scalable, multi-stakeholder scenarios.

III. Conceptual Model

A. Requirements

Integrating a private Hyperledger blockchain into secure data infrastructures in the context of Gaia-X requires both functional and non-functional requirements, focusing on data security, scalability, data splitting and reunification. Functionally, the system must protect data during storage and transmission using modern encryption methods by splitting it into smaller, encrypted units before distribution to different nodes and securely reuniting it later. Non-functionally, it must be ensured that the system remains performant even with an increasing number of transactions and participants by distributing efficient, decentralized storage across a network and, at the same time, acting interoperably with the Gaia-X Trust Framework, which enables access for all users with a Gaia-X identity.

B. Proposed Architecture

The proposed architecture is built on a private Hyperledger Fabric blockchain, which is accessible through the Gaia-X Trust Framework for all participants who possess a valid Gaia-X identity. This architecture adopts a multi-layered approach. The following Figure 1 illustrates the architecture.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

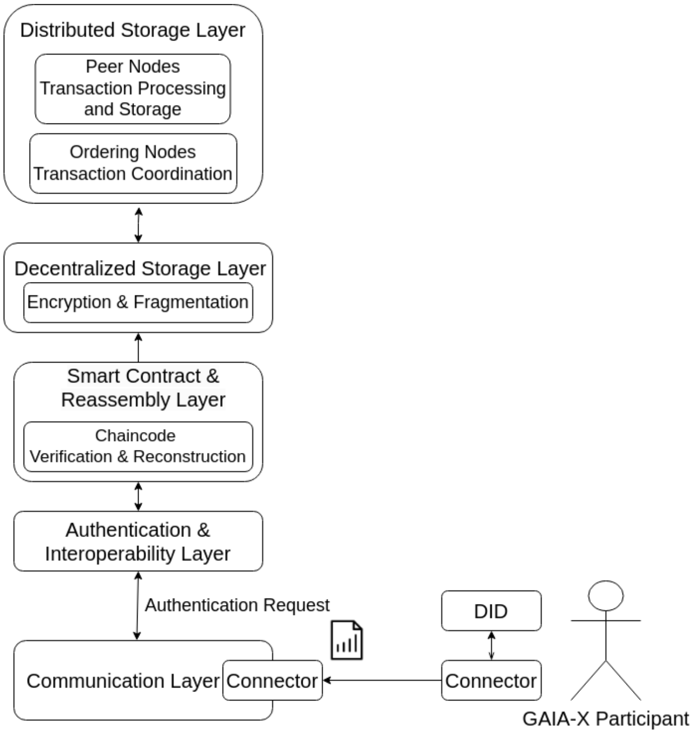
Distributed Storage Layer
Peer Nodes
Transaction Processing and Storage
Ordering Nodes
Transaction Coordination
Decentralized Storage Layer
Encryption & Fragmentation
Smart Contract & Reassembly Layer
Chaincode
Verification & Reconstruction
Authentication & Interoperability Layer
Authentication Request
DID
Communication Layer
Connector
Connector
GAIA-X Participant

Figure 1. Hyperledger-GaiaX-Architecture

1) Decentralized Storage Layer: At the base, raw data is first secured using symmetric encryption. Following encryption, a threshold cryptography approach—employing Shamir's Secret Sharing—is applied to fragment the encrypted data into n pieces, where only a subset (k-out-of-n) is required for complete reassembly [14]. This layer guarantees that even if individual fragments are compromised, they alone reveal no sensitive information.

2) Distributed storage layer: The fragmented data is then distributed across a network of decentralized nodes within the Hyperledger Fabric framework. Each peer stores only a portion of the total data, reducing the risk of a complete data breach. Integrity is maintained by employing cryptographic hash functions (e.g., SHA-256) to monitor that fragments remain unaltered during storage.

3) Smart contract and Reassembly layer: Smart contracts, implemented as chaincode, serve as the control centre for data reassembly. These smart contracts are programmes that automatically check whether all the necessary conditions have been met - similar to an automated system that only acts once all the security checks have been passed [9]. In our approach, they ensure that all necessary data fragments are present and intact and that the requesting user has the necessary authorisations before the reassembly process is started. By automatically initiating and managing the reassembly process, smart contracts ensure that only fully verified and authorised reassembly events occur, thereby tightly coupling the fragmentation and storage layers with the access control mechanism.

4) Authentication and Interoperability layer: This layer collaborates with the Gaia-X connector, the communication layer, to facilitate optimized, standards-based authentication. The connector performs external identity checks using decentralized identifiers (DIDs) and verifiable credentials (VCs) from the Gaia-X ecosystem [1]. Meanwhile, this layer manages internal policy enforcement and session management. Once the connector verifies a Gaia-X identity, the authentication layer can assign it to local roles or authorizations and oversee tasks, such as renewing approvals or reassigning keys. This system ensures that only entities with valid Gaia-X credentials, confirmed by the connector, are granted access to data and the reassembly processes.

5) Communication layer: All layers are interconnected through a secure communication infrastructure that utilizes protocols, such as TLS and VPN. This setup ensures that all data exchanges between processing nodes, storage nodes, smart contracts, and authentication systems occur over encrypted channels, protecting against unauthorized interception or tampering. Additionally, the Gaia-X connector, responsible for processing all incoming and outgoing requests to the Gaia-X ecosystem, is defined within this layer. The connector verifies the identity of external participants to ensure that only authorized data exchanges occur. It also serves as a protocol bridge by adapting internal data formats and processes to maintain interoperability with Gaia-X standards. This layer consolidates all network communication—including secure node-to-node interaction and external Gaia-X requests—to ensure consistent encryption, manage potential VPN segments, and prevent the unauthorized interception or tampering of sensitive data.

6) Interlayer Interactions and Data Flow: The Communication Layer receives an incoming request to store data at the initial stage. This layer verifies the request and forwards it to the Authentication and Interoperability Layer, where the requester's credentials are validated. Upon successful authentication, the request is forwarded to the Smart Contracts and Reassembly Layer, where smart contracts are triggered to initiate the data processing pipeline. The Data Processing and Fragmentation Layer then encrypts the raw data using symmetric encryption techniques and partitions it into secure fragments using Shamir's Secret Sharing. These encrypted and fragmented data pieces are subsequently distributed across the Distributed Storage Layer, ensuring that each storage node holds only a portion of the fragmented data alongside cryptographic hashes for integrity verification. When an access request is made to retrieve stored data, the Communication Layer first receives the request and forwards it to the Authentication and Interoperability Layer for identity verification. The request moves forward if the requester is authorized to access the requested data. The Smart Contracts and Reassembly Layer then autonomously verifies the required fragments' presence and integrity before triggering the reassembly process. The required encrypted data fragments are retrieved from the Distributed Storage Layer and reassembled, ensuring data integrity. The reassembled encrypted data is then securely transmitted to the requester. Throughout these stages, the Secure Communication Infrastructure ensures that all inter-

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

layer data exchanges are protected by protocols, such as TLS, thereby maintaining confidentiality and preventing tampering. This structured approach ensures data storage and retrieval under strictly verified and secure conditions.

IV. Discussion

The proposed model is built on a private Hyperledger Fabric blockchain and utilizes the Gaia-X Trust Framework to facilitate secure, decentralized data storage. While it introduces several approaches, it also brings forth critical issues that warrant discussion in current research. One of the key advantages of this model is its combination of data encryption, secret sharing, and distributed storage. The model achieves robust security by employing AES-256 alongside Shamir's Secret Sharing. This ensures that complete data is not disclosed even if individual nodes are partially compromised, significantly reducing the risk of data leaks and providing mathematically sound security. Additionally, the decentralized storage of data fragments enhances resilience and scalability, as the load is distributed across multiple nodes. The Gaia-X Trust Framework establishes W3C Verifiable Credentials and self-descriptions as essential components for creating interoperable identity and access controls within Gaia-X ecosystems [12]. This ensures that only participants with a validated Gaia-X identity can access the system, promoting security, transparency, and traceability of data access within a federated ecosystem. This model encounters several significant challenges. Lessons learned so far indicate that integrating hybrid encryption and secret-sharing mechanisms is complicated and requires careful coordination to prevent performance bottlenecks or potential security vulnerabilities. In real-time applications, cryptographic operations can drastically impact throughput and scalability as the number of participants increases. Interoperability is also a critical concern; differing implementations and standard versions can result in practical inconsistencies. Furthermore, developing smart contracts for the secure reassembly of fragmented data is a complex task. Recent blockchain research has highlighted considerable security risks associated with insufficiently validated smart contract code, underscoring the importance of thorough testing and formal verification. In terms of future use cases, potential domains include Healthcare, enabling secure patient record exchange and real-time collaboration among hospitals, although large file sizes may require specialized data-splitting and off-chain indexing solutions; Supply Chain, verifying product provenance across multiple organizations, where Gaia-X can standardize participant identity while Fabric ensures transaction immutability and private data channels; and Automotive Mobility Services, supporting distributed sensor data or usage-based insurance under a federated yet privacy-preserving environment. By providing more technical details on these potential domains, we clarify how advanced encryption, threshold cryptography, and trusted identities interact in real multi-stakeholder ecosystems. Ultimately, bridging the gap between blockchain's decentralized trust model and Gaia-X's federated governance will pave the way for scalable and secure data spaces.

V. Conclusion and Future Work

This approach introduces a theoretical concept for integrating a private Hyperledger Fabric blockchain into the Gaia-X ecosystem. The proposed approach employs hybrid encryption, secret sharing, and decentralized storage to guarantee high levels of data security and sovereignty. Throughout the research, the following questions were specifically addressed:

i Compatibility between blockchain and Gaia-X was established through a multi-layered architecture, facilitating the storage and secure reassembly of encrypted, fragmented data using smart contracts.

ii Necessary security measures for ensuring integrity and confidentiality—including AES-256 encryption, Shamir's Secret Sharing, and cryptographic hashes—were defined

iii Opportunities, such as increased digital sovereignty and enhanced interoperability, and challenges, like performance limitations, complex smart contract validations, and interoperability constraints, were identified and discussed.

This integrated approach provides a strong foundation for building high-assurance federated ecosystems. However, the lessons learned emphasize the importance of thorough testing, rigorous performance optimization, and formal verification of chain code to address the complexities identified during the initial theoretical analysis. Future expansions of this research will include extended pilot projects involving various domain partners, deeper evaluations based on metrics, such as latency with large participant pools, targeted performance enhancements, rigorous validation of smart contracts, and ongoing standardization of cryptographic operations within the Gaia-X environment. Practical validation and empirical studies will be essential to confirm whether current security, performance, and interoperability expectations are fully met or require adjustments.

Acknowledgements

This paper was written as part of the project GAIA-X 4 Advanced Mobility Services in the project family Future Mobility funded by the Federal Ministry of Economics and Climate Protection (BMWK).

References

[1] G.-X. H. Austria, *Building a dataspace: Technical overview*, Available from https://www.gaia-x.at/wp-content/uploads/2023/04/WhitepaperGaiaX.pdf, 2023. (retrieved: 2025-03-04).

[2] F. Salzano, L. Marchesi, R. Pareschi, and R. Tonelli, "Integrating blockchain technology within an information ecosystem," *Blockchain: Research and Applications*, vol. 5, no. 4, p. 100 225, 2024, Available from https://www.sciencedirect.com/science/article/pii/S2096720924000381, ISSN: 2096-7209. DOI: https://doi.org/10.1016/j.bcra.2024.100225.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

[3] N.Arunkumar and P.Sivaprakasam, "Blockchain technology in data management," in *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)*, 2020, pp. 199–206. DOI: 10.1109/ICCMC48092.2020.ICCMC-00039.

[4] D. V. Dimitrov, "Blockchain applications for healthcare data management," *Healthcare Informatics Research*, vol. 25, pp. 51–56, 2019, Available from https://api.semanticscholar.org/CorpusID:67771752. (retrieved: 2025-03-04).

[5] M. Hasnain, F. R. Albogamy, S. S. Alamri, I. Ghani, and B. Mehboob, "The hyperledger fabric as a blockchain framework preserves the security of electronic health records," *Frontiers in Public Health*, vol. 11, 2023, Available from https://api.semanticscholar.org/CorpusID:265576007. (retrieved: 2025-03-04).

[6] S. Wong, J.-K.-W. Yeung, Y.-y. Lau, T. Kawasaki, and R. Kwong, "A critical literature review on blockchain technology adoption in supply chains," *Sustainability*, 2024, Available from https://api.semanticscholar.org/CorpusID:270607203. (retrieved: 2025-03-04).

[7] W. Gao, X. Hei, and Y. Wang, "The data privacy protection method for hyperledger fabric based on trustzone," *Mathematics*, vol. 11, no. 6, 2023, Available from https://www.mdpi.com/2227-7390/11/6/1357, ISSN: 2227-7390. (retrieved: 2025-03-04).

[8] A. Shukla, P. Jirli, A. Mishra, and A. K. Singh, "An overview of blockchain research and future agenda: Insights from structural topic modeling," *Journal of Innovation Knowledge*, vol. 9, no. 4, p. 100 605, 2024, Available from https://www.sciencedirect.com/science/article/pii/S2444569X24001446, ISSN: 2444-569X. DOI: https://doi.org/10.1016/j.jik.2024.100605. (retrieved: 2025-03-04).

[9] E. A. et al., "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, ser. EuroSys '18, Porto, Portugal: Association for Computing Machinery, 2018, pp. 1–15, ISBN: 9781450355841. DOI: 10.1145/3190508.3190538.

[10] T. Coenen et al., "Gaia-X and European Smart Cities and Communities," Gaia-X, White Paper, Oct. 2021, Version 21.09.

[11] "Gaia-x Architecture Document - 22.04 Release," Gaia-X, Architecture Documentation, version 22.04, Apr. 2022.

[12] "Gaia-X Trust Framework - main version (fb420580)," Gaia-X, 2022, Available from https://gaia-x.gitlab.io/policy-rules-committee/trust-framework/trust%5Fanchors/. (retrieved: 2025-03-04).

[13] B. Maier and N. Pohlmann, "Gaia-X Secure and Trustworthy Ecosystems with Self Sovereign Identity," Gaia-X European Association for Data and Cloud AISBL, White Paper, 2022.

[14] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org