UNIVERSIDADE FEDERAL DE JUIZ DE FORA
INSTITUTO DE CIÊNCIAS EXATAS
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

Mattheus Soares Santos

Development of a Smart Contract-Based Security Layer for an Industry 4.0 Framework

Juiz de Fora

Setembro, 2021

Mattheus Soares Santos

Development of a Smart Contract-Based Security Layer for an Industry 4.0 Framework

Trabalho de conclusão de curso apresentado ao Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do grau de bacharel em Sistemas de Informação.

Adviser: Professor Dr. Mario Antonio Ribeiro Dantas

Co-Adviser: Professor Dr. José Maria Nazar David

Juiz de Fora

Setembro, 2021

Mattheus Soares Santos

Development of a Smart Contract-Based Security Layer for an Industry 4.0 Framework

Trabalho de conclusão de curso apresentado ao Instituto de Ciências Exatas da Universidade Federal de Juiz de Fora como requisito parcial à obtenção do grau de bacharel em Sistemas de Informação.

EXAMINING BOARD

Professor Dr. Mario Antonio Ribeiro Dantas - Adviser
Universidade Federal de Juiz de Fora

Professor Felipe Schneider Costa
Universidade Federal de Santa Catarina

Professor Marcelo Ferreira Moreno
Universidade Federal de Juiz de Fora

Professor Luciano Jerez Chaves
Universidade Federal de Juiz de Fora

Dedico este trabalho aos meus pais, minha avó, e meus professores, por todo o apoio e orientação.

ACKNOWLEDGEMENTS

Agradeço aos meus pais, Oséas e Silvia, pelo apoio e confiança, que por toda esta jornada da minha vida estiveram ao meu lado. Agradeço também a minha avó Dalva, que sempre me motivou e acreditou que eu seria capaz.

Ao professor Mario Antonio pela orientação, amizade e principalmente, por todas as oportunidades que me foram oferecidas. Agradeço também aos coorientadores, professor José Maria e professora Regina Braga, pela orientação, paciência, auxílio nesta pesquisa. Agradeço ainda o professor Felipe Costa, pela paciência e pelo auxílio no desenvolvimento.

Aos alunos Carlos Magnun e Rômulo Soares pelo desenvolvimento e pesquisa na bolsa de iniciação científica. E à mestranda Raiane Coelho, pelo auxílio na estruturação e desenvolvimento do projeto.

Aos professores do Departamento de Ciência da Computação pelos seus ensinamentos e aos funcionários do curso, que durante esses anos, contribuíram de algum modo para meu enriquecimento pessoal e profissional.

"A journey of a thousand miles begins with a single step."
Lao Tzu (Tao Te Ching)

RESUMO

Com a integração dos dispositivos IoT no ambiente industrial, possibilitou-se o desenvolvimento das chamadas fábricas inteligentes. Entretanto, a segurança nesse novo ambiente industrial é uma preocupação crescente. A comunicação entre esses dispositivos, diferentes usuários e o volume de dados digitais transferidos aumenta a vulnerabilidade dos recursos e dados no ambiente industrial. Visando enfrentar este desafio, desenvolvemos estudos relacionados à aplicação de contratos inteligentes com suporte de blockchain para garantir a autenticidade de identidade dos dados digitais que trafegam no ambiente de IoT Industrial (IIoT). Neste trabalho, apresentamos a proposta do Métis, uma abordagem que utiliza blockchain com contratos inteligentes por meio da plataforma do Hyperledger Fabric para validar a identidade das requisições submetidas para o ambiente do framework FASTEN Manufacturing. A proposta foi testada por meio de simulações de modo a fornecer uma camada de segurança para este framework. A partir destas simulações, foi possível verificar que a integração de contratos inteligentes com blockchain é capaz de prover uma camada de segurança que auxilia na validação de dados dentro do ambiente da Indústria 4.0.

Palavras-chave: Blockchain. Indústria 4.0. Contratos Inteligentes. Internet das Coisas. Segurança da Informação.

ABSTRACT

The integration of IoT devices in the industrial environment made possible the development of so-called smart factories. However, safety in this new industrial environment is a growing concern. The communication between these devices, different users, and the volume of digital data transferred increases the vulnerability of resources and data in the industrial environment. In order to face this challenge, we developed studies related to the application of smart contracts with blockchain support to ensure the identity authenticity of the digital data that travels in the Industrial IoT (IIoT) environment. In this work, we present the Métis proposal, an approach that uses blockchain with smart contracts through the Hyperledger Fabric platform to validate the identity of the requests submitted to the FASTEN Manufacturing framework environment. The proposal was tested through simulations in order to provide a layer of security for this framework. From these simulations, it was possible to verify that the integration of smart contracts with blockchain can provide a security layer that helps in data validation within the Industry 4.0 environment.

Keywords: Blockchain. Industry 4.0. Smart Contracts. Internet of Things. Information Security.

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS AND ACRONYMS

IoT	Internet of Things
IIoT	Industrial Internet of Things
ISO	International Organization for Standardization
CPS	Cyber-Physical Systems
DDoS	Distributed Denial of Service
ROS	Robot Operating System
UUID	Universally Unique Identifier

SUMMARY

1 INTRODUCTION

The fourth industrial revolution is a new paradigm in the industrial environment, defined by the integration of cyber-physical systems (CPS) within the industrial environments. These systems can communicate with each other and make autonomous and decentralized decisions (1). This enabled the development of what are called smart factories, which includes smart networking, mobility, the flexibility of industrial operations and their interoperability, integration of customers, and innovative business models. However, these new integrations in the industrial environment bring new security problems, mainly due to the integration of Industrial IoT (IIoT) devices and the large volume of digital data transmitted within this IIoT environment (2).

A technology that is growing in terms of development and adoption is the blockchain paradigm. Given the nature of its architecture, the blockchain can provide reliability and security solutions for different domains beyond *e-commerce* and IIoT. Recently, several researchers have explored the implementation of the blockchain in IIoT environments, in order to guarantee the security of the environment's data and resources. One way to implement this security with blockchain is by using smart contracts. Smart contracts are codes that execute the terms of a contract to ensure that certain rules are adhered to. Thus, it is possible to ensure digital data security of IIoT devices within the industrial environment through the use of smart contracts in conjunction with a blockchain network (3).

In this context, the Métis project was conceived and developed as an approach to provide a differentiated identity authenticity for requests in an IIoT environment. The implementation of a blockchain network with smart contracts to perform validation and verification, ensures the integrity and identity authenticity of the trafficked data, thus enabling to aggregate a security approach to an IIoT environment. The blockchain network was implemented using Docker images, which provides a test environment for our experimental results, but our goal is to implement this network with physical peers, so that if one peer disconnects, the rest of the network is still able to operate properly. The smart contracts are implemented to define a layout for a valid request, hence any request that doesn't follow this layout will be considered invalid. However, due to the structure of the blockchain network, these validations are expected to be slower than a traditional approach, such as authenticating identity on a SQL or NoSQL database.

Therefore, the main objective of our proposal is to develop a solution that guarantees digital data protection, bringing a valuable solution that can maintain the identity security of an IIoT environment.

1.1 RESEARCH QUESTION

Based on the elements presented, the question that this work aims to answer is: "How to develop an approach that can provide a differentiated identity authenticity for requests in an IIoT environment?"

1.2 OBJECTIVES

1.2.1 GENERAL OBJECTIVE

The general objective of this work is to provide a security layer in the context of the framework FASTEN, using blockchain and smart contracts, which guarantee the information security paradigms, through the Hyperledger Fabric, which is an enterprise-grade distributed ledger platform (4). This platform is essential for the industrial environment, to maintain a robust system for IIoT, preventing attacks against industrial espionage, information leakage, attacks to disrupt a production network, and other situations that can be fatal for a company. These information security paradigms are defined by ISO 27002 (5).

1.2.2 SPECIFIC OBJECTIVES

The general objective of this research will be reached from the specific objectives, which are:

1. Develop a research about related works, both on security aspects in industry 4.0 and on the application of smart contracts and blockchain in the industrial 4.0 environment.
2. Check the possibility of using the tools available for the development and application of smart contracts to support security. This includes both platforms that integrate blockchain and smart contracts and the option of developing our platform.
3. Develop a proposal for an environment that will be used for the operation of smart contracts as a security tool, which will provide a unique identity authenticity validation.
4. Develop the proposed environment, in which tests will be performed to obtain experimental results to validate our proposal.
5. Analyze the experimental results obtained from the environment and validate if such results are in accordance with the information security paradigms.

1.3 ACCEPTED PAPERS

The research carried out by our group allowed us to publish three articles, which are presented at the end of this document. In (6) it is presented how we can create a custom network in Hyperledger Fabric, and how to use this network to validate data in an IIoT environment. In (7) we present a proposal of an environment to guarantee identity authenticity for a transaction within FASTEN Manufacturing. In (8) we further explore the concepts and the architecture of the proposal presented in the previous paper.

1.4 ORGANIZATION

This document is organized as follows. In Chapter 2 we presented the theoretical concepts and related works needed for a better understanding of our research. We present the concepts of Blockchain, Smart Contracts, Industrial Internet of Things, Information Security, IIoT Security, and the platforms FASTEN, and Hyperledger Fabric. Our proposal and its development are presented in Chapter 3. The experimental results obtained from the tests in our simulated environment are presented in Chapter 4. And finally, in Chapter 5 we presented the conclusions and future work.

2 THEORETICAL CONCEPTS AND RELATED WORKS

2.1 BLOCKCHAIN

Blockchain is a distributed database, which was initially developed to carry out the validations of Bitcoin cryptocurrency transactions, as thought by Satoshi Nakamoto (9). It uses the concepts of **Proof-of-Work** for validation, which is a cryptographic protocol that requires all (or a certain amount of) members of a network to validate any transaction that is issued within the said network, to prove that a certain amount of a specific computational effort has been expended and that a consensus was reached.

Blockchain stores its data in blocks of predetermined storage capacity, and then, when a block is filled, a new one is created and attached to the previous one, so creating a chain of data or a blockchain. This chain is equally distributed to all members within a network, so every entity who is participating in a blockchain network will have a copy of all data.

A blockchain network can be categorized between permissionless and permissioned. A permissionless blockchain requires no authentication for a new user to join the network. This makes it so anyone can join and try to issue a transaction within the network, but the transaction still requires validation from the rest of the network.

On the other hand, in a permissioned blockchain, only those who are allowed within the network can issue and validate the transaction. This type of blockchain is more suited for companies and organizations who want to have full control of the network.

These data decentralization and validation protocols make the blockchain an effective technology against DDoS attacks, with high data integrity and confidentiality, since, in a permissioned blockchain, only members of a network are authorized to carry out transactions, and in a permissionless blockchain, every transaction is anonymous.

2.2 SMART CONTRACTS

Although the concept of smart contracts is very often associated with blockchain, it dates from at least ten years before. The concept of smart contracts was first proposed by Nick Szabo (10). He defined it as

> Smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols.

The main goals of smart contracts are to facilitate all steps of contractual processes between two (or more) parties and reduce mental and computational transaction costs imposed by

such processes.

Even though the concept of smart contracts is older, it did not attract the attention of developers and companies until blockchain networks were proposed. The architecture of a blockchain network enables smart contracts to be developed and applied as automated protocols to ensure that transactions between two or more entities are valid, safe, and performed with less effort. These transactions may vary from electronic commerce, contract laws, business forms, accounting controls, and other business relationships that are, nowadays, paper-based (11).

2.3 INDUSTRIAL INTERNET OF THINGS (IIOT)

Internet of Things, as defined in (12),

> an open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data, and resources, reacting and acting in face of situations and changes in the environment.

In other words, the Internet of Things can be described as devices that have the ability to send and receive data over the Internet, or other internal networks, to other devices or computers. These devices may or may not have some processing capacity, but their main characteristic is the collection of data through sensors and sending this data through a network.

From the moment these devices become part of the industrial environment, together with the integration of monitoring, prediction, and analysis tools, the Fourth Industrial Revolution takes place, or as it is also known, IIoT. This new industrial environment is primarily aimed at increasing the efficiency of existing production systems, and through digital transformation, deploying cyber-physical systems to facilitate monitoring, integration, and control between the different components of the production environment.

One of the main factors defining IIoT, in addition to autonomy, flexibility, modularity, and decentralization, are vertical and horizontal integrations. According to (13),

> vertical integration focuses on the internal integration of manufacturing companies and aims to convert data, events, and information from the real world to the digital world and vice versa. Horizontal integration, on the other hand, aims to bring together all the networks of suppliers and customers, thus supporting the management of the supply chain.

2.4 INFORMATION SECURITY

To ensure that our information security approach is effective, we use smart contracts in a blockchain network as a validation tool so that information security paradigms as defined by ISO 27002 (5) are met.

The tool of choice for implementing smart contracts is the Hyperledger Fabric, which is a distributed operating system for blockchains licensees (4).

This tool guarantees the information security paradigms as follows:

1. Data confidentiality through channel architecture and private data capabilities.
2. Availability through the blockchain architecture, which distributes data to all nodes in the system.
3. Integrity through the mechanism of digital signatures of the data that are transferred in the system.

2.5 IIOT SECURITY

With technological advances, especially in the industrial area, issues such as business and industrial data security become a concern. As defined in (2),

> Industry 4.0 is more vulnerable to cyber espionage because of smart and connected business processes. Currently, we have seen the development of well-organized groups of cybercriminals with excellent skills used to target specific industries, to hack confidential information and intellectual property.

Among the security issues are industrial espionage, intellectual property attacks, and DDoS attacks.

2.6 FASTEN

The Fasten Manufacturing Framework (14) was developed based upon pillars from industry 4.0. The Fasten is a middleware with the objective of developing a fully connected and scalable manufacturing system, integrating robotics, automation, simulation, optimization technologies, and prescriptive analysis, to produce projects for unique customers (14).

Due to the way supply chains have changed with the introduction of the internet into the industrial environment, the demand for customized products with shorter life cycles and low volumes per order is growing. The objective of FASTEN is to develop a manufacturing system for tailored-designed products through additive manufacturing to meet this growing demand (15).

The architecture of FASTEN framework is represented as shown in Figure 1. It is composed of three tiers: the Edge Tier, the Platform Tier, and the Enterprise Tier. On the Edge Tier are the IIoT devices, which receive manufacturing requests and return responses such as device temperature and production progress. On the Platform Tier are ROS (Robot Operating System) (16), FIROS, which helps connecting robots to the cloud (17), the Kafka topics, which order the requests and responses inside the platform, and the IoT Data Repository which is composed by a number of databases, like MongoDB, CrateDB, PostgreSQL and InfluxDB. The last one is the Enterprise Tier, which is composed of several types of applications, such as monitoring tools, industrial analytics suite, and management software (Supply Chain Management, Enterprise Resources Planning, and others).

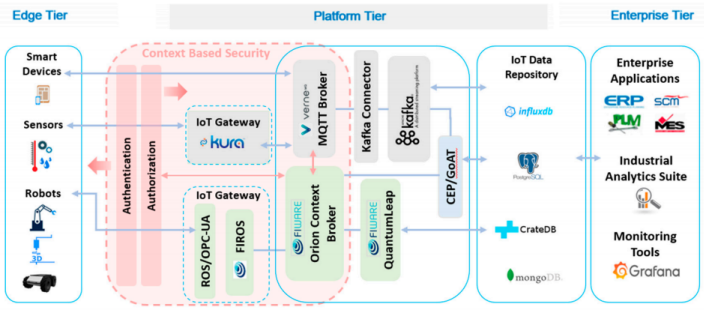


Figure 1 – FASTEN Industrial Internet of Things (IIoT) Platform (14)

The way that a request is treated by the framework can be seen in Figure 2. The requests to manufacture a product made by an operator 4.0 are issued to the framework, and then, through an optimization algorithm, they are forwarded to IIoT devices, so manufacturing may begin.

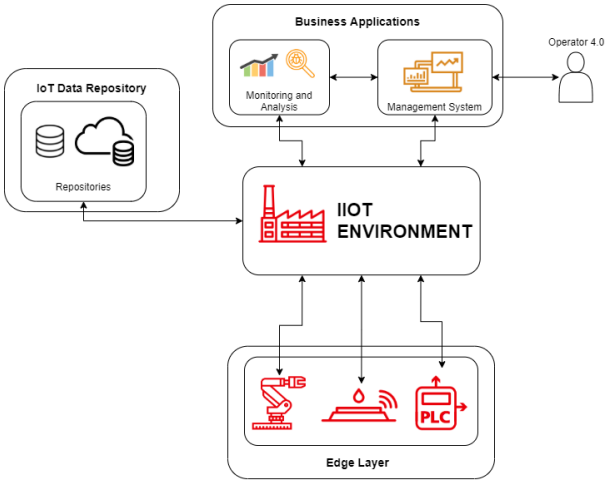


Figure 2 – FASTEN Manufacturing Framework (8)

2.7 HYPERLEDGER FABRIC

Many platforms offer a blockchain network with smart contracts, such as Ethereum (18), Polkadot (19), Iota (20), among many others. We choose Hyperledger Fabric, mainly due to its permissioned blockchain aspect, modular architecture, versatility, scalability, consensus, privacy, and membership services. Another interesting aspect of the Hyperledger Fabric is characterized by an open-source community focused on developing a suite of stable frameworks, tools, and libraries for enterprise-grade blockchain deployments (4).

A Hyperledger Fabric network is composed of organizations and peers. Organizations are the members of the network, and peers are owned and maintained by members. A peer is an entity that can perform operations to the network. There is also a unique type of organization, which is called Orderer, or Ordering Service. The ordering service is a common binding for the overall network. It contains the cryptographic identity material tied to each member and it exists independent of the peer processes and orders transactions on a first-come-first-serve basis for all channel's on the network (21). An example of the transaction flow can be seen in Figure 3.

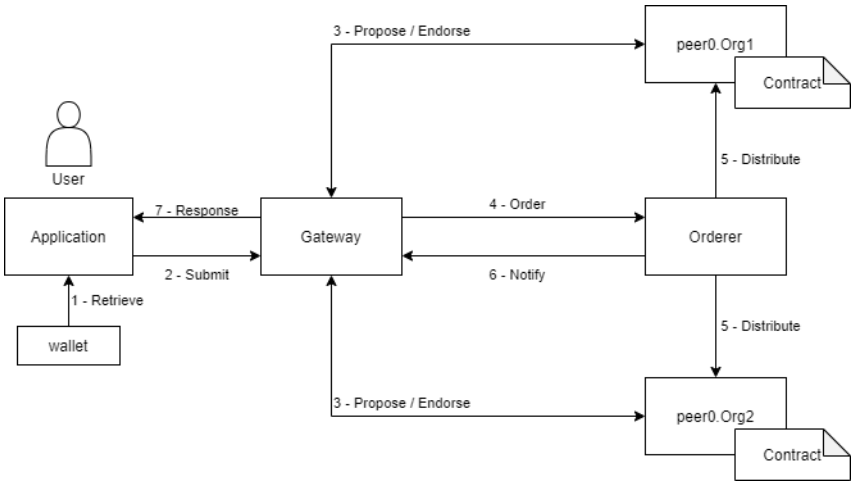


Figure 3 – Hyperledger Fabric Transaction Flow (8)

This transaction flow consists of first retrieving ① the user identity from his wallet, which consists of his access rights within the network. Then, the application submits ② the transaction to the gateway. The gateway sends a proposal ③ of the transaction to all peers of the network. Each peer validates the transaction, and then, if everything checks out, the peers endorse the transaction ③. The gateway submits ④ the transaction to the orderer peer, which orders these transactions into blocks, and distributes ⑤ these transaction blocks to each peer of the network. The orderer peer then notifies ⑥ to the gateway, and the gateway returns the response ⑦ to the application.

All transactions carried out on the network are saved in the ledger, which consists of two distinct, though related, parts – the "blockchain", and the "state database", also

known as “world state”. The blockchain is immutable, and the world state is a database containing the current value of the set of key-value pairs that have been added, modified, or deleted by the set of validated and committed transactions in the blockchain.

A differential element offered by the Hyperledger Fabric platform is the channel concept. A channel is a private blockchain overlay that allows for data isolation and confidentiality. A channel-specific ledger is shared across the peers in the channel, and transacting parties must be properly authenticated to a channel to interact with it. This creates a possibility of privacy between channels, thus members of different channels cannot see each other’s transactions (21).

2.8 RELATED WORKS

Several studies discuss the use of blockchain and smart contracts as a security approach, both for IIoT and for scientific provenance applications (22, 23).

In (24), the authors present a proposal of an integrated IoT platform using blockchain technology, ensuring data integrity of IoT sensors, providing a solution with scalability, high throughput, low data volume, and transparency levels. The work shown in (22) provides similar research, but they developed a system to support process management in the IIoT environment to assess the safety and impact that smart contracts have on communication between IIoT devices. In (25) is presented how smart contracts can also be applied as a solution to automate data packet transactions and data analysis service transactions, bringing confidence and robustness in a decentralized platform.

Another related work is the development of a blockchain-based provenance system for collaborative scientific experiments, with the aim of bringing a reliable environment for scientific experimentation (26).

Our proposal differs from previous works bringing an intelligent security layer to industry 4.0, verifying not only the information of the IIoT devices but also the identity of the person who made the request to authorize the transaction. In this way, we can guarantee that only those who are authorized will be able to participate in the network. This happens both because of the architecture proposed by Métis, and because of the characteristics of the permissioned blockchain.

2.9 FINAL CONSIDERATIONS OF THE CHAPTER

The use of blockchain as a security tool is mainly due to the difficulty of modifying its saved data, and as it keeps a history of all saved operations, even if an improper change occurs in some way, the data is fully auditable. Furthermore, its distributed feature provides high availability of data. These aspects, together with smart contracts, make the blockchain a powerful tool, but its large-scale applicability still requires more research to

find out potential vulnerabilities, as no single solution is a silver bullet for every problem. In this research, The focus of this security tool is to ensure that the IIoT environment is protected against unauthorized access to the supply chain, and integrated systems such as databases, decision support systems, and monitoring systems.

3 MÉTIS PROPOSAL

3.1 PROPOSAL

The FASTEN framework addresses the issue with the demand for personalized products, but it lacks an identity authentication for the requests made in the IIoT platform to manufacture a product. Information security in IIoT is a growing concern, due to both the processes and the technology that composes it. As stated by (2),

> Industry 4.0 is more vulnerable to cyber-espionage because of the smart and connected business processes. Currently, it has been seen the development of well-organized groups of cyber-criminal with excellent skills used to targeting specific industries, towards hacking sensitive information and intellectual property.

To address this issue, we conceived and developed Métis, a platform that integrates blockchain and smart contracts with an IIoT framework. For the smart contracts platform, we chose Hyperledger Fabric, and we used FASTEN as the IIoT framework. Métis acts as a user validation protocol, reassuring that only those who have been previously authorized will be able to request an operation within FASTEN framework. The architecture of our proposal can be seen in Figure 4.

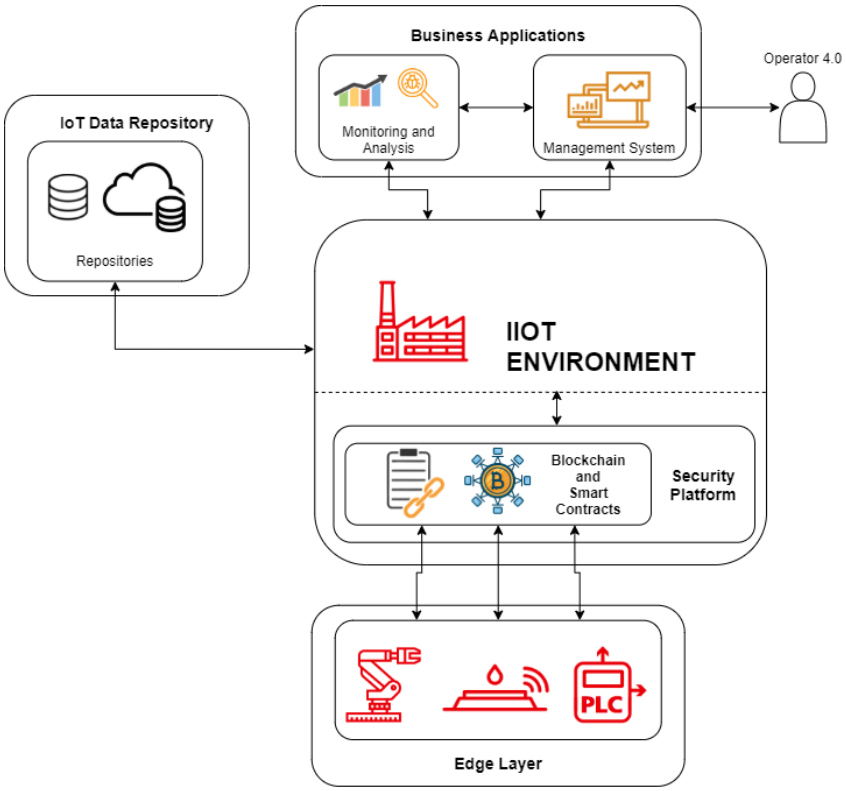


Figure 4 – FASTEN Manufacturing Architecture with proposed blockchain network (8)

We developed the security platform within the framework, acting as a filter to all requests before they are issued to the edge layer. With this blockchain network, we were able to increase the difficulty of the attempts to directly access the edge layer. As a result, hijacking or hacking of these IIoT devices is harder. All transactions issued to the FASTEN framework are redirected to our blockchain network after the optimization process, where Métis can then validate all information, such as who issued the transaction, which is the IIoT device, and which operation is being requested. Then, if the transaction is valid, it will be forwarded to the IIoT device to execute it. We also keep a record of all transactions, whether valid or not, in a database so that we can keep track of all transactions and unauthorized attempts to access the platform. This workflow can be seen in Figure 5.

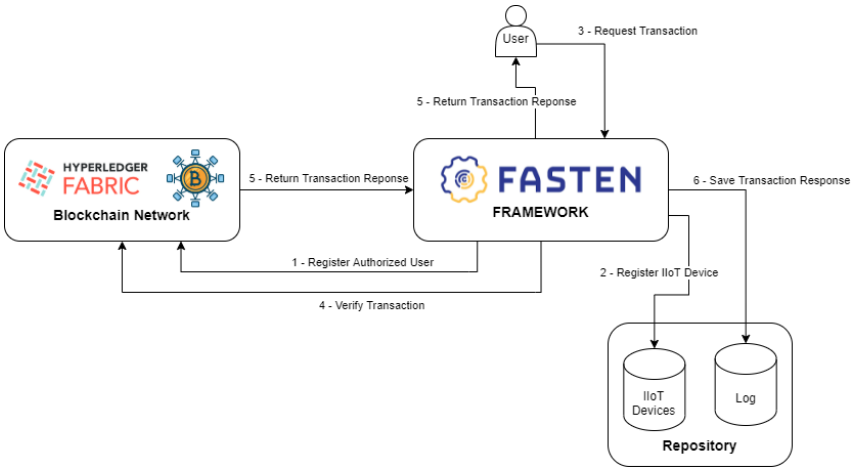


Figure 5 – Workflow of proposed blockchain network integrated with FASTEN framework (8)

First, we register the authorized users ① in the blockchain network, and then we register the IIoT devices ② in our repository. After that, when a user issues a transaction request ③ to the Fasten framework platform, this transaction is redirected to our blockchain network, where the transaction is verified and validated ④. Then, the transaction response is returned ⑤ to the Fasten framework, and the framework returns this response to the user ⑤. This response is also saved in our log repository ⑥, regardless if it was valid or not.

3.2 COMPUTATIONAL ARCHITECTURE AND DEVELOPMENT

To initially test our proposal, a simulated environment was developed, in which the structure of a request received from the FASTEN framework would be replicated and which response would be returned to the framework. We chose to develop a simulated environment to test our proposal because the integration with FASTEN proved a little complicated, more because of code impediments.

The first step in this environment is to start the network. This process was executed automatically by scripts provided by the Hyperledger Fabric, which initialized docker images containing the network components (organizations, peers, orderers, and certificate authority). Then the administrator is enrolled in the network. This step is necessary to ensure that further users can be registered since the administrator is needed for adding new users to the network. After this, we register a new user to the network. Since only one value can be assigned to identify a user, we used a UUID (Universally Unique Identifier) that would identify each user. For testing purposes, this value was filled in manually via a form in the interface, but it is important to note that this would not occur in a production environment.

Subsequently, as can be seen in Figure 5, we registered the information of an IIoT device in our repository, with a UUID for the IIoT device as well, treating it as a resource of the platform. At this point, Métis is ready to handle the requests issued by a user. We receive the information of a transaction and validate its content. We consider a request to be valid if the user is registered in our blockchain network, if the IIoT device request is valid, and if the operation requested to this device is also valid.

If the request is valid, the transaction will be issued to the blockchain network, and then the network will validate our request based on our smart contract or are referred in Hyperledger Fabric, chaincode. This chaincode contains the values we want to save in the transaction. We have chosen to save a unique identifier for the transaction, with which we can refer to it, if necessary. Also both user and IIoT identifiers, the operation requested to the device, and the current timestamp to track of all transactions performed.

Regardless of the transaction is valid or not, we save it with its result in our log repository, so we can verify all attempts to access our platform. We assigned the corresponding result to the log entry according to the response received from the blockchain network.

3.3 FINAL CONSIDERATIONS OF THE CHAPTER

In addition to the challenge of integrating our proposal with the framework FASTEN, the Hyperledger Fabric network configuration was another challenge, as it requires a high level of attention in the files, to the point of having problems if there was a difference in uppercase or lowercase characters. Because of this complexity, we also chose to use one of the sample networks that the Hyperledger platform provides.

4 ENVIRONMENT AND EXPERIMENTAL RESULTS

In this section, we will present the simulated environment and the results from the experiments carried out in our simulated environment. We tested possible request attempts that would be issued to the FASTEN framework and the behavior would be expected in each case.

The first simulated environment was developed using a personal computer[1]. This environment provides flexibility to our initial developments. However, for more comprehensive simulations, in terms of data science research, we are developing efforts to execute at the NEC Tsubasa, similarly to a previous research from our group (27). Targeting to develop the simulated environment that would handle both the blockchain network and the request and response of the transactions, we used Node.js integrated with MongoDB. An interface was developed using javascript, in which the request data that would be forwarded to the devices would be filled. In this same interface, users authorized to carry out transactions would be registered, and IIoT devices would also be registered as resources in the MongoDB database. We anticipate four possible cases, depending on what data would be received from a request. The first case is what we consider a success, in which both user and IIoT identifiers are valid, and the operation requested is also valid. In this case, we expect to succeed both in getting the user from the blockchain network and in successfully saving the transaction on the network. In the second case, we treat it as an invalid request if the user identifier cannot be found on the network. This means that the user is not allowed to perform a request on the platform. The third and fourth cases take into account the IIoT device identifier and the operation that this device can perform. If any of these values are incorrect, we treat the request as invalid. The flow of each of these cases is represented in Figure 6.

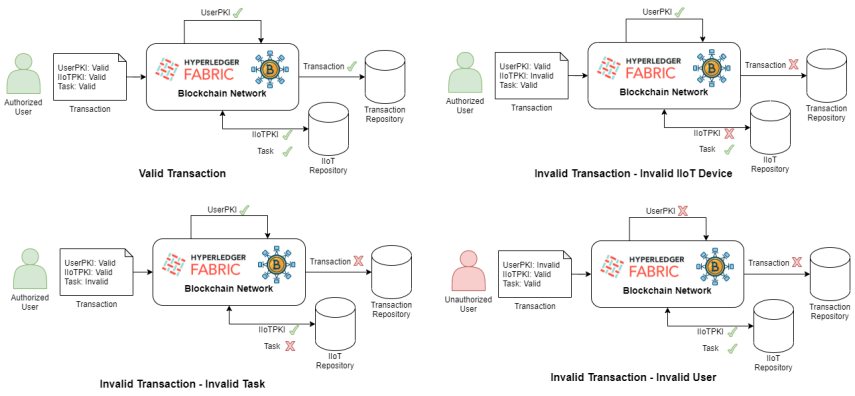


Figure 6 – Transaction flow (8)

[1] DELL Inspiron 14 3442 notebook, 8GB of RAM and a Core i5-4210U 1.7GHz processor, with 1TB hard drive

In Figure 7 we present the simulated interface for the Operator 4.0, in which he will create a new request and issue a transaction for the blockchain network. We simulate some requests, and the behavior of Métis is shown in Figure 8. The valid transactions can be seen in the green rows, and the invalid transactions and respective statuses are represented in the red rows. The third and fourth cases take into account the IIoT device identifier and the operation that this device can perform. If any of these values are incorrect, we also consider the request invalid.

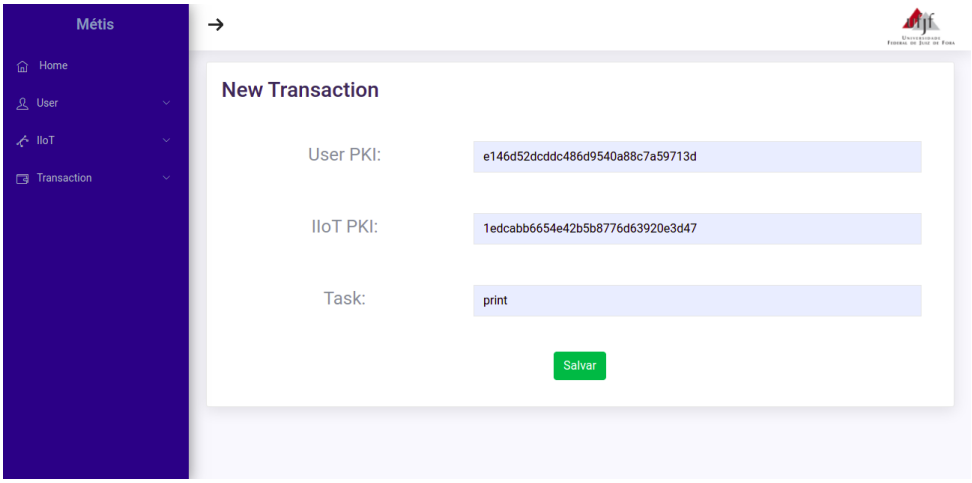
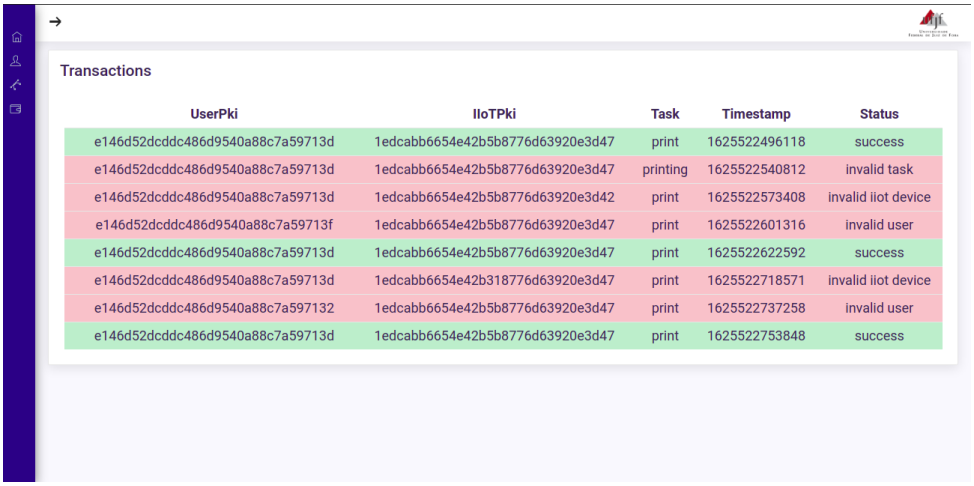


Figure 7 – Métis 4.0 Operator Interface (8)

As stated before, all transactions presented in Figure 8 were saved in our log database, but only the successful ones were stored in our blockchain network. This ensures that we have a history of attempted transactions performed and that only transactions with valid parameters were performed.



UserPki	IIoTPki	Task	Timestamp	Status
e146d52dcddc486d9540a88c7a59713d	1edcabb6654e42b5b8776d63920e3d47	print	1625522496118	success
e146d52dcddc486d9540a88c7a59713d	1edcabb6654e42b5b8776d63920e3d47	printing	1625522540812	invalid task
e146d52dcddc486d9540a88c7a59713d	1edcabb6654e42b5b8776d63920e3d42	print	1625522573408	invalid iiot device
e146d52dcddc486d9540a88c7a59713f	1edcabb6654e42b5b8776d63920e3d47	print	1625522601316	invalid user
e146d52dcddc486d9540a88c7a59713d	1edcabb6654e42b5b8776d63920e3d47	print	1625522622592	success
e146d52dcddc486d9540a88c7a59713d	1edcabb6654e42b318776d63920e3d47	print	1625522718571	invalid iiot device
e146d52dcddc486d9540a88c7a597132	1edcabb6654e42b5b8776d63920e3d47	print	1625522737258	invalid user
e146d52dcddc486d9540a88c7a59713d	1edcabb6654e42b5b8776d63920e3d47	print	1625522753848	success

Figure 8 – Simulated Transaction Results (8)

4.1 FINAL CONSIDERATIONS OF THE CHAPTER

The test cases presented take into account only the most important data that are part of a request in the FASTEN environment, but improvements can be made if necessary, and new fields can be added. The proposal is strongly based on the smart contracts aspect and on the architecture that the blockchain network itself provides. Still, the Hyperledger Fabric structure has a high degree of customization, so future changes to suit a more robust solution are feasible.

5 CONCLUSIONS AND FUTURE WORK

This research presented a differentiated identity authenticity for requests in the industrial environment, called Métis. There is evidence that blockchain technology with smart contracts has several facilities to offer to the industrial environment, acting as a layer of security to protect resources, in this case, IIoT devices, from unauthorized access.

One difficulty faced during the development of this research was configuring and using a Hyperledger Fabric network. Due to its complexity, we chose to use one of the standard network examples offered by Hyperledger Fabric. Another difficulty faced was integrating Métis platform with FASTEN framework. This is because FASTEN uses Kafka topics, and this would increase the complexity of the development of our platform, mainly in communication with FASTEN. For this reason, we chose to develop a simulated environment to perform transaction testing.

As future work, our group intends to improve the validations and processing of request data, to ensure a viable security solution for the IIoT environment. We also aim to integrate our platform with the FASTEN framework, to carry out more elaborate tests and develop a more robust solution. With this integration, we intend to develop the blockchain network with physical peers and test the possibility of using the edge devices as peers for the network.

REFERENCES

1 Boyes, H., Hallaq, B., Cunningham, J., and Watson, T. (2018). The industrial internet of things (IIoT): An analysis framework. Computers in Industry, 101:1–12.

2 Pereira, T., Barreto, L., and Amaral, A. M. (2017). Network and information security challenges within Industry 4.0 paradigm.

3 Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4:2292–2303.

4 Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., Enyeart,D., Ferris, C., Laventman, G., Manevich, Y., Muralidharan, S., Murthy, C., Nguyen, B.,Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolic, M., Cocco,S. W., and Yellick, J. (2018). Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. CoRR, abs/1801.10228.

5 ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ISO/IEC 27002: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. 2013

6 Pinto, C. M.; Santos, M. S.; Soares, R. L. A. S.; David, J. M. N.; Villela, R. M. M. B. ; Dantas, M. A. R. (2021) Uso de blockchain na indústria 4.0: Uso do hyperledger fabric no projeto fasten. In: Anais da VII Escola Regional de Sistemas de Informação do Rio de Janeiro, p. 56–63, Porto Alegre, RS, Brasil, 2021. SBC

7 Santos, M. S.; Dantas, M. A. R.; David, J. M. N.; Villela, R. M. M. B. ; Costa, F. S. (2021) Métis - Uma Abordagem de Autenticidade Diferenciada para Ambientes IIoT. Accepted Paper. In: Anais do IV Workshop em Blockchain: Teoria, Tecnologias e Aplicações, p. 74–79, Porto Alegre, RS, Brasil, 2021.SBC.

8 Costa, F. S.; Dantas, M. A. R.; David, J. M. N.; Villela, R. M. M. B. ; Santos, M. S. (2021) Métis - an approach utilized as differentiated authenticity tool in an iiot infrastructure. Accepted Paper. 3PGCIC - IoT Computing Systems Track.

9 Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

10 Szabo, N. (1997). Smart Contracts: Formalizing and Securing Relationships on Public Networks. Available at https://journals.uic.edu/ojs/index.php/fm/article/view/548/469.

11 Alharby, M.; Moorsel, A. v. (2017). Blockchain based smart contracts: A systematic mappingstudy. Computer Science & Information Technology (CS & IT), Aug 2017.

12 Somayya Madakam, R. Ramaswamy, S. T. (2015). Internet of Things (IoT): A Literature Review.

13 Csalódi, R., Süle, Z., Jaskó, S., Holczinger, T., and Abonyi, J. (2021). Industry 4.0 - Driven Development of Optimization Algorithms: A Systematic Overview.

14 Costa, F. S., Nassar, S. M., Gusmeroli, S., Schultz, R., Conceição, A. G. S., Xavier, M.,Hessel, F., and Dantas, M. A. R. (2020). FASTEN IIoT: An Open Real-Time Platform for Vertical, Horizontal and End-To-End Integration. Sensors, 20(19).

15 Pereira, A. R., Dalmarco, G., and Alcalá, S. G. S. (2018). FASTEN - Flexible and Autonomous Manufacturing Systems for Custom - Designed Products.

16 Quigley, M. (2009). ROS: an open-source Robot Operating System. In ICRA 2009.

17 Herranz, F., Jaime, J., González, I.Hernández, Á. (2015).Cloud Robotics in FIWARE: A Proof of Concept. In Hybrid Artificial Intelligent Systems, pages 580–591. Springer International Publishing

18 Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger.

19 Wood, G. (2016). Polkadot: Vision for a heterogeneous multi-chain framework.

20 Popov, S. (2016).The Tangle.

21 Fabric (2021).Hyperledger Fabric Glossary. Available at https://hyperledger-fabric.readthedocs.io/en/release-1.2/glossary.html.

22 Garrocho, C., Ferreira, C. M. S., Junior, A., Cavalcanti, C. F., and Oliveira, R. R. (2019). Industry 4.0: Smart Contract-based Industrial Internet of Things Process Management.In Anais Estendidos do IX Simpósio Brasileiro de Engenharia de Sistemas Computacionais, pages 137–142. SBC, Porto Alegre, RS, Brasil.

23 Coelho, R.; Braga, R.; David, J. M.; Campos, F.; Ströele, V. Blockflow: Trust in scientific provenance data. In: Anais do XIII Brazilian e-Science Workshop, 2019.

24 Hang, L. and Kim, D.-H. (2019). Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity.

25 Jiang, Y., Zhong, Y., and Ge, X. (2019). Smart Contract-Based Data Commodity Transactions for Industrial Internet of Things. volume 7.

26 Coelho, R.; Braga, R.; David, J. M.; Dantas, M.; Ströele, V.; Campos, F. Integrating blockchain for data sharing and collaboration support in scientific ecosystem platform. 2019.

27 do Nascimento, M. G., Braga, R. M. M., David, J. M. N., Dantas, M. A. R., and Colugnati,F. A. B. (2021). Towards an IoT Architecture to Pervasive Environments Through Design Science. In Barolli, L., Woungang, I., and Enokido, T., editors, Advanced Information Networking and Applications - Proceedings of the 35th International Conference on Advanced Information Networking and Applications (AINA-2021), Toronto, ON, Canada, 12-14 May, 2021, Volume 2, volume 226 of Lecture Notes in Networks and Systems, pages 28–39. Springer.

APPENDIX A – ACCEPTED PAPERS

.1 Uso de Blockchain na Indústria 4.0: Uso do Hyperledger Fabric no projeto Fasten - ERSI-RJ

Na Indústria 4.0, a segurança da informação, principalmente na comunicação entre máquinas do meio de produção necessita ser explorada. A comunicação entre dispositivos IIoT (Industrial Internet of Things), tem um alto índice de vulnerabilidade. Neste contexto, o projeto FASTEN apresenta uma solução de comunicação entre dispositivos. Porém, a falta de segurança dos dados ainda é um desafio. Este artigo apresenta uma solução, considerando os preceitos da tecnologia de blockchain, para tratar a segurança da informação no ambiente industrial, considerando o projeto FASTEN melhorando a segurança na comunicação entre os dispositivos IIoT.

.2 Métis - Uma Abordagem de Autenticidade Diferenciada para Ambientes IIoT - SBRC 2021 - WBlockchain

A segurança no ambiente industrial é uma preocupação crescente desde a integração dos dispositivos IoT Industriais (IIoT). A comunicação entre esses dispositivos, diferentes usuários e o volume de dados digitais transferidos aumenta a vulnerabilidade. Visando enfrentar este desafio, desenvolvemos estudos relacionados à aplicação de contratos inteligentes com suporte de blockchain para garantir a integridade da autenticidade de identidade dos dados digitais que trafegam no ambiente IoT Industrial (IIoT). Portanto, neste artigo, apresentamos a proposta do Métis, que representa uma abordagem de autenticidade diferenciada e que foi testada por meio de simulações para fornecer um cenário de segurança para um projeto real da Indústria 4.0.

.3 Métis - An Approach Utilized as Differentiated Authenticity Tool in an IIoT Infrastructure - 3PGCIC 2021 - IoT Computing Systems

The security in industrial environments is a growing concern with the integration of Industrial IoT (IIoT). The communication between devices, diverse users and the volume of digital data transferred increase the vulnerability. Aiming to tackle this challenge, we developed studies related to the application of smart contracts with blockchain support to guarantee the integrity of identity authenticity of the digital data that travels within the Industrial IoT (IIoT) environment. Therefore, in this paper, we present the Métis proposal, which represents a differentiated authenticity approach and which was tested through simulations to provide a security landscape to a real industrial 4.0 project.