

# UNIVERSIDAD DE INVESTIGACIÓN DE TECNOLOGÍA EXPERIMENTAL YACHAY

Escuela de Ciencias Matemáticas y Computacionales

**TÍTULO: Blockchain application for the supply chain of  
the ecuadorian oil industry**

Trabajo de integración curricular presentado como requisito para la  
obtención del título de Ingeniero en Tecnologías de la Información

**Autor:**

Villacreses Ponce Ángel Gabriel

**Tutor:**

Ph.D Chang Tortolero Oscar Guillermo

Urcuquí, abril 2020

**SECRETARÍA GENERAL**  
**(Vicerrectorado Académico/Cancillería)**  
**ESCUELA DE CIENCIAS MATEMÁTICAS Y COMPUTACIONALES**  
**CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN**  
**ACTA DE DEFENSA No. UITEY-ITE-2020-00022-AD**

A los 6 días del mes de abril de 2020, a las 12:00 horas, de manera virtual mediante videoconferencia, y ante el Tribunal Calificador, integrado por los docentes:

<b>Presidente Tribunal de Defensa</b>	Dr. ANTON CASTRO , FRANCESC , Ph.D.
<b>Miembro No Tutor</b>	Dr. INFANTE QUIRPA, SABA RAFAEL , Ph.D.
<b>Tutor</b>	Dr. CHANG TORTOLERO, OSCAR GUILLERMO , Ph.D.

El(la) señor(ita) estudiante **VILLACRESES PONCE, ANGEL GABRIEL**, con cédula de identidad No. 1311509796, de la **ESCUELA DE CIENCIAS MATEMÁTICAS Y COMPUTACIONALES**, de la Carrera de **TECNOLOGÍAS DE LA INFORMACIÓN**, aprobada por el Consejo de Educación Superior (CES), mediante Resolución **RPC-SO-43-No.496-2014**, realiza a través de videoconferencia, la sustentación de su trabajo de titulación denominado: **BLOCKCHAIN APPLICATION FOR THE SUPPLY CHAIN OF THE ECUADORIAN OIL INDUSTRY**, previa a la obtención del título de **INGENIERO/A EN TECNOLOGÍAS DE LA INFORMACIÓN**.

El citado trabajo de titulación, fue debidamente aprobado por el(los) docente(s):

<b>Tutor</b>	Dr. CHANG TORTOLERO, OSCAR GUILLERMO , Ph.D.
--------------	--

Y recibió las observaciones de los otros miembros del Tribunal Calificador, las mismas que han sido incorporadas por el(la) estudiante.

Previamente cumplidos los requisitos legales y reglamentarios, el trabajo de titulación fue sustentado por el(la) estudiante y examinado por los miembros del Tribunal Calificador. Escuchada la sustentación del trabajo de titulación a través de videoconferencia, que integró la exposición de el(la) estudiante sobre el contenido de la misma y las preguntas formuladas por los miembros del Tribunal, se califica la sustentación del trabajo de titulación con las siguientes calificaciones:

Tipo	Docente	Calificación
Tutor	Dr. CHANG TORTOLERO, OSCAR GUILLERMO , Ph.D.	10,0
Miembro Tribunal De Defensa	Dr. INFANTE QUIRPA, SABA RAFAEL , Ph.D.	10,0
Presidente Tribunal De Defensa	Dr. ANTON CASTRO , FRANCESC , Ph.D.	9,5

Lo que da un promedio de: **9.8 (Nueve punto Ocho)**, sobre 10 (diez), equivalente a: **APROBADO**

Para constancia de lo actuado, firman los miembros del Tribunal Calificador, el/la estudiante y el/la secretario ad-hoc.

**VILLACRESES PONCE, ANGEL GABRIEL**  
**Estudiante**

**Dr. ANTON CASTRO , FRANCESC , Ph.D.**  
**Presidente Tribunal de Defensa**

**Francesc Anton Castro**

Signé électroniquement par Francesc Anton Castro  
 cni=Francesc Anton Castro, ou=Escuela de Ciencias Matemáticas y Computacionales, email=fcastro@yachaytech.edu.ec  
 Date: 2020.05.29 17:02:13 ECT

**Dr. CHANG TORTOLERO, OSCAR GUILLERMO , Ph.D.**  
**Tutor**



Firmado electrónicamente por:  
**OSCAR GUILLERMO CHANG TORTOLERO**

SABA RAFAEL INFANTE  
QUIRPA

Firmado digitalmente por SABA RAFAEL  
INFANTE QUIRPA  
Fecha: 2020.06.01 19:08:35 -05'00'

**Dr. INFANTE QUIRPA, SABA RAFAEL , Ph.D.**  
**Miembro No Tutor**

DAYSY MARGARITA  
MEDINA BRITO

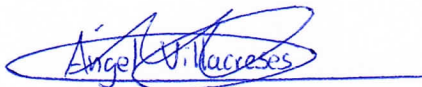
Firmado digitalmente por DAYSY  
MARGARITA MEDINA BRITO  
Fecha: 2020.06.11 20:08:45 -05'00'

**MEDINA BRITO, DAYSY MARGARITA**  
**Secretario Ad-hoc**

## AUTORÍA

Yo, **ÁNGEL GABRIEL VILLACRESES PONCE**, con cédula de identidad 1311509796, declaro que las ideas, juicios, valoraciones, interpretaciones, consultas bibliográficas, definiciones y conceptualizaciones expuestas en el presente trabajo; así cómo, los procedimientos y herramientas utilizadas en la investigación, son de absoluta responsabilidad de el/la autora (a) del trabajo de integración curricular. Así mismo, me acojo a los reglamentos internos de la Universidad de Investigación de Tecnología Experimental Yachay.

Urcuquí, julio 2020.



---

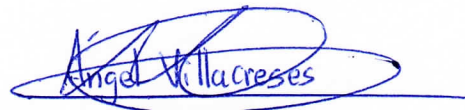
Ángel Gabriel Villacreses Ponce  
CI: 1311509796

## AUTORIZACIÓN DE PUBLICACIÓN

Yo, **ÁNGEL GABRIEL VILLACRESES PONCE**, con cédula de identidad 131150 9796, cedo a la Universidad de Tecnología Experimental Yachay, los derechos de publicación de la presente obra, sin que deba haber un reconocimiento económico por este concepto. Declaro además que el texto del presente trabajo de titulación no podrá ser cedido a ninguna empresa editorial para su publicación u otros fines, sin contar previamente con la autorización escrita de la Universidad.

Asimismo, autorizo a la Universidad que realice la digitalización y publicación de este trabajo de integración curricular en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Urcuquí, julio 2020.



Ángel Gabriel Villacreses Ponce  
CI: 1311509796

# Dedicatoria

A mis amados padres, Holanda y José Luis por todo su amor, apoyo incondicional, creer siempre en mí e inculcarme todos esos valores que me convierten en la persona que soy en la actualidad. A mi hermana Belén, por ser parte de mi vida y para que este trabajo sea una inspiración en su vida y pueda lograr sus sueños académicos. Y por supuesto, a mi amor Jaylenne que entró a mi vida en la recta final de mi carrera y me ayudó e inspiró a culminar con éxito este trabajo.

Ángel Gabriel Villacreses Ponce



# Agradecimiento

Quiero dar un agradecimiento especial a mi padre, por su sacrificio diario que hace por nosotros para que podamos construir un futuro mejor. A mi madre, por sus consejos y enseñanzas de superación, pero especialmente por su amor incondicional que llena de alegría mis días; Los esfuerzos que hacen por mi hermana y por mí, junto con el amor que nos proporcionan para mí son invaluable y detonantes de estas ganas de superación.

Agradezco a todos mis familiares, tanto los de España como los de Ecuador que siempre han estado conmigo animándome a no rendirme y luchar por mis sueños. Pero en particular, agradezco las ayudas de mis tías Margarita y Amanda que desde el principio hasta el día de hoy me han permitido estar donde estoy ahora.

A Jaylenne, quién siempre estuvo conmigo en mis mejores y más difíciles días en estos últimos años. Logrando con paciencia, inteligencia y con mucho amor que siempre siga adelante, incluso cuando ya no tenía esperanzas. Eres lo más preciado que me llevo de esta universidad.

A mis amigos y amigas que se han convertido en mi familia durante estos 6 años de carrera universitaria. Desde la casa 7 de nivelación hasta el H 2-2, sin olvidar a mis amigos de clases, de negocios y de MYT.

Agradezco a mi Tutor y profesor, Ph.D. Oscar Chang quién me mostró el apasionante mundo de la inteligencia artificial, y del Blockchain que inspiraron mis deseos de incursionar en este mundo para realizar mi investigación de tesis. Pero principalmente, por sus enseñanzas y apoyo cuando lo he necesitado.

Finalmente, a la universidad Yachay Tech que fue una de las mejores decisiones que he tomado en mi vida, y estaré siempre agradecido por brindarme todos estos conocimientos. Pero sobre todo, por la oportunidad de vivir experiencias únicas con personas extraordinarias.

Ángel Gabriel Villacreses Ponce



## Resumen

El uso intensivo de la tecnología de datos ha transformado a la mayoría de las industrias modernas, sin embargo, ciertas industrias ecuatorianas como el petróleo y el gas carecen de herramientas administrativas y de gestión efectivas y aún operan de manera tradicional, causando baja productividad y competitividad. Los principales obstáculos que aparecen en la secuencia productiva son la volatilidad en los precios, la cadena de suministro, la seguridad de los datos, la contratación, los procesos de transacción, entre otros. La tecnología blockchain también conocida como cadena de bloques puede ayudar a superar estos problemas, logrando una mayor eficiencia, datos inmutables gracias a la característica ACID de la base de datos Couch DB, transacciones transparentes y auditables a bajo costo, en comparación con las metodologías tradicionales (facturas en papel, contratos notariados, etc.).

Al igual que cualquier otra tecnología de vanguardia, blockchain no se acepta completamente a día de hoy, especialmente en países subdesarrollados, por lo tanto, esta tesis estudiará la logística de la industria petrolera ecuatoriana, elegirá un campo operativo específico (ventas, transporte, mantenimiento, etc.) y propondrá una aplicación basado en la cadena de bloques para mejorar la eficiencia general, la productividad y la transparencia.

**Palabras clave:** Cadena de Bloques, Hyperledger, Aplicación, Industria petrolera, Ecuador, Trazabilidad, Transparencia, Confidencialidad, Interoperabilidad

## Abstract

The intensive use of data technology has transformed most modern industries around the world, however, important Ecuadorian enterprises such as oil and gas lack effective administrative and management up-to-date tools and still operate in a traditional paper-notarized based manner, causing low productivity and weak competitiveness.

The main obstacles that appear in the productive route are high price volatility supply chain failures, data security, contracting, transaction processes, among others. The Blockchain data handling technology can greatly help to overcome these problems by creating a digital, data handling ambient with greater efficiency, immutable data thanks to the ACID feature of the Couch DB database, transparent, and auditable transactions at a low cost, as compared with traditional methodologies (paper invoices, notarized contracts, etc.).

Like any other cutting-edge technology, blockchain is not completely accepted today, specially in under-developed countries, consequently this thesis will study the logistic of the Ecuadorian oil industry, choose a specific operative field (sales, transport, maintenance etc.) and propose an application based on the blockchain to improve efficiency, productivity and transparency.

**Key words:** Blockchain, Hyperledger, Applications, Oil industry, Ecuador, Traceability, Transparency, Confidentiality, Interoperability

# Contents

<b>1</b>	<b>Introduction</b>	<b>6</b>
1.1	Blockchain . . . . .	6
1.1.1	Blockchain 1.0 . . . . .	6
1.1.2	Blockchain 2.0 . . . . .	6
1.1.3	Blockchain 3.0 . . . . .	7
<b>2</b>	<b>Analysis of the problem</b>	<b>9</b>
2.1	Diagnosis of the current situation of the main oil companies in the world	9
2.2	Diagnosis of the current situation of Ecuadorian oil companies . . . . .	10
2.2.1	History of advances in the Ecuadorian oil industry . . . . .	10
2.2.2	Marketing and production . . . . .	10
2.2.3	Transportation and storage of oil . . . . .	11
2.2.4	Main Ecuadorian oil companies . . . . .	11
2.3	Petroamazonas Ep . . . . .	12
2.3.1	Materials Headquarters . . . . .	13
2.3.2	Departments that interrelate with the Purchasing Area . . . . .	14
2.3.3	Purchase Management Time . . . . .	15
2.3.4	Demand Planning . . . . .	16
2.3.5	Provider Development . . . . .	16
2.4	Supply Chain . . . . .	17
2.4.1	How the supply chain works? . . . . .	17
2.4.2	Participants in the supply chain . . . . .	17
2.4.3	Components of a typical supply chain . . . . .	18
2.4.4	Supply Chain Issues . . . . .	19
2.5	Blockchain in the supply chain . . . . .	20
2.5.1	Blockchain for Upstream Operations . . . . .	21
2.5.2	Blockchain for Midstream Operations . . . . .	22
2.5.3	Blockchain for Downstream Operations . . . . .	22
2.5.4	Benefits of Decentralization . . . . .	23
2.6	Oil giants and the blockchain . . . . .	25
2.6.1	Blockchain consortium with oil industries. . . . .	25
2.7	Problem Statement . . . . .	26

<b>3</b>	<b>Hypothesis and Justification</b>	<b>28</b>
3.1	Hypothesis . . . . .	28
3.2	Justification . . . . .	28
<b>4</b>	<b>Objectives</b>	<b>29</b>
4.1	Specific Objectives . . . . .	29
<b>5</b>	<b>Theoretical Framework</b>	<b>30</b>
5.1	Bitcoin . . . . .	30
5.2	Blockchain . . . . .	31
5.2.1	Why is blockchain so safe? . . . . .	32
5.2.2	Main Characteristics of Blockchain . . . . .	33
5.2.3	Types of Blockchain . . . . .	34
5.2.4	Consensus Algorithm . . . . .	34
5.2.5	Security in Blockchain . . . . .	36
5.2.6	A Distributed Ledger . . . . .	36
5.2.7	Blockchain . . . . .	37
5.2.8	Blocks . . . . .	38
5.2.9	Transactions . . . . .	39
5.2.10	Smart Contract . . . . .	40
5.3	Hyperledger . . . . .	40
5.3.1	Hyperledger Fabric . . . . .	41
5.3.2	Hyperledger Fabric model . . . . .	42
5.3.3	Hyperledger Fabric Component Design . . . . .	43
5.3.4	Hyperledger Composer . . . . .	44
<b>6</b>	<b>Related Works</b>	<b>45</b>
6.1	Hongfang Lu et Al. (2019) . . . . .	45
6.2	ECOSC (2019) . . . . .	45
6.3	Enbo Chen (2016) . . . . .	46
<b>7</b>	<b>Methodology</b>	<b>47</b>
7.1	Blockchain Type Choice . . . . .	47
7.2	Supply Chain Model . . . . .	48
7.3	Platforms and Tools . . . . .	50
7.3.1	Prerequisites . . . . .	51
7.3.2	Visual Studio Code (VS Code) . . . . .	51
7.4	Development environment topology . . . . .	51
7.5	Installing the development environment . . . . .	53
7.5.1	Application Modeling . . . . .	54
7.5.2	Create and implement the business network file (BNA) . . . . .	59
7.5.3	Start the RESTful API . . . . .	61
7.5.4	Front End Creation . . . . .	62

<b>8</b>	<b>Results and Discussions</b>	<b>64</b>
8.1	Demo presentation . . . . .	64
8.2	Transparency . . . . .	68
8.3	Traceability . . . . .	71
8.4	Confidentiality . . . . .	73
8.5	Interoperability . . . . .	75
<b>9</b>	<b>Conclusions</b>	<b>76</b>
	<b>References</b>	<b>78</b>
	<b>Appendix</b>	<b>83</b>

# List of Figures

1.1	The value chain of oil and gas industry [1] . . . . .	7
2.1	Main oil companies in Ecuador according to their daily oil production [2]	12
2.2	Organizational Structure Petroamazonas EP - Level 1 [3, p.9] . . . . .	13
2.3	Structural Organization Structure of Materials [4] . . . . .	13
2.4	Shopping area interrelation [4] . . . . .	15
2.5	Purchase management time determination [4] . . . . .	16
2.6	Upstream, midstream and downstream operations in the oil industry [5] .	23
5.1	Centralized vs Decentralized vs Distributed Network [6] . . . . .	32
5.2	Types of blockchain:Consortium, private and public [7] . . . . .	34
5.3	Ledger diagram.The ledger (L) comprises the blockchain (B) and the world state (W), where W is obtained by B [8] . . . . .	37
5.4	Blockchain with four blocks and their parts [8] . . . . .	37
5.5	Block diagram [8] . . . . .	38
5.6	Transactions diagram [8] . . . . .	39
5.7	Smart Contract flow [9]. . . . .	40
5.8	Business Blockchain Frameworks Tools Hosted by Hyperledger [9] . . .	41
5.9	Hyperledger Fabric Flow [9] . . . . .	43
7.1	Do you need a blockchain?. Retrieved from H. Narumanchi (2018) [10] .	47
7.2	Permissioned Blockchain Applications Retrieved from J.Rodriguez (2018) [11] . . . . .	48
7.3	Supply Chain Model in Oil Industry . . . . .	49
7.4	Typical Hyperledger Composer Solution Architecture. Retrieved from Hyperledger Composer [12] . . . . .	50
7.5	Development environment <i>fabric-dev-servers</i> . . . . .	52
7.6	docker-compose.yml file . . . . .	52
7.7	Hyperledger Composer Playground in localhost . . . . .	53
7.8	generate project skeleton . . . . .	54
7.9	Participant in model file . . . . .	55
7.10	Transaction in model file . . . . .	55
7.11	Events in model file . . . . .	56
7.12	Transactions and events of the model are defined . . . . .	57

7.13	Transactions and events of the model are programmed . . . . .	57
7.14	Rules of composer access control . . . . .	58
7.15	business network file (BNA). Retrieved from Hyperledger [12] . . . . .	59
7.16	Create BNA file . . . . .	59
7.17	Install BNA file . . . . .	60
7.18	Implementation of the business network . . . . .	60
7.19	Import the network to a marketable network card . . . . .	60
7.20	Verify the implementation of the network card . . . . .	60
7.21	Flow of information of REST SERVER . . . . .	61
7.22	Configuration of REST SERVER . . . . .	61
7.23	API in the localhost . . . . .	62
7.24	Construction of the frontend . . . . .	62
7.25	Front End Execution . . . . .	63
8.1	BlockOilChain application interface . . . . .	64
8.2	Creation of raw product . . . . .	65
8.3	Raw product created . . . . .	66
8.4	Raw product stored in Manufacturer storage . . . . .	66
8.5	Product stored in Manufacturer storage . . . . .	67
8.6	Product created in the Distributor . . . . .	67
8.7	Product created in the Retailer . . . . .	67
8.8	Product sold to Customer . . . . .	68
8.9	Purchase detail . . . . .	68
8.10	Manufacturer instance confirmation . . . . .	69
8.11	All transaction in the Hyperledger Composer Playground . . . . .	69
8.12	Raw product confirmation . . . . .	70
8.13	Event when the product is created . . . . .	70
8.14	Sale confirmation . . . . .	71
8.15	Distributor rules . . . . .	74
8.16	Raw products registration denied to the distributor . . . . .	74
8.17	REST API methods . . . . .	75



# Chapter 1

## Introduction

### 1.1 Blockchain

”The real progress is the one that puts the technology at the reach of everybody” (Henry Ford)

This phrase, said by a great visionary, implies that depending on the utility that this technology offers, it can be of greater or lesser impact. It is for this reason that many of the innovations go unnoticed and others, on the contrary, achieve a great reach, enabling the development of many applications as the imagination allows them [13].

A high impact case is the birth of a digital tool of great potential that can contribute to the development and certification of billing and distribution systems in the oil and gas industry. This newfangled system is known as Blockchain. In the last 10 years, the development of blockchain can be divided into three eras:

#### 1.1.1 Blockchain 1.0

This era marks the creation of Bitcoin, the revolutionary digital currency that solved the problem of double spending, leaving out an important actor such as the centralized authorities, that is, a Central Bank, managing to provide the necessary confidence to validate a system of these characteristics. This technology was born in 2008 thanks to the anonymous Satoshi Nakamoto, and it is based on two pillars: first, security through cryptographic algorithms to encrypt information and second, the distributed computing that allows the exchange and processing of large amounts of information [14];

#### 1.1.2 Blockchain 2.0

This era was marked by the Ethereum project [15], whose main objective was the construction of decentralized applications. Thus, there was born the concept of smart contracts that are immutable computer programs capable of managing assets that are included in the Ethereum network [16] all possible without the need of a third party or mediator, since the verification of the transactions is carried out between all the nodes

that make up the network, guaranteeing its security by its blockchain structure and its free access for the entire public;

### 1.1.3 Blockchain 3.0

During this era, the applications of the social field begun [15]. Due to its enormous impact on the global economy, hundreds of applications of different kinds emerged.

According to British Petroleum, in June 2018 [17], oil and gas represented 57% of the total energy consumption of the planet. Despite the fact that there is a tendency for the use of renewable energy, oil and natural gas will continue to dominate the energy market for at least 30 more years, according to "BP Energy Outlook 2019 edition" [18]. To stay on top of the energy market, the oil industry is slowly making inroads in the world of digitalization, intellectualization, and automation.

However, its incursion has been deficient and slow, especially in the management of operations, causing high production costs, low efficiency, time delays and high risk [19]. Delays and high risks of non-payments in international transactions are requiring effective and efficient technology to help mitigate these deficiencies [20]. To solve these problems, one must know the logistical parts of the oil, that is in this case, divided into three parts according to market division: upstream, midstream and downstream (see Figure 1.1).

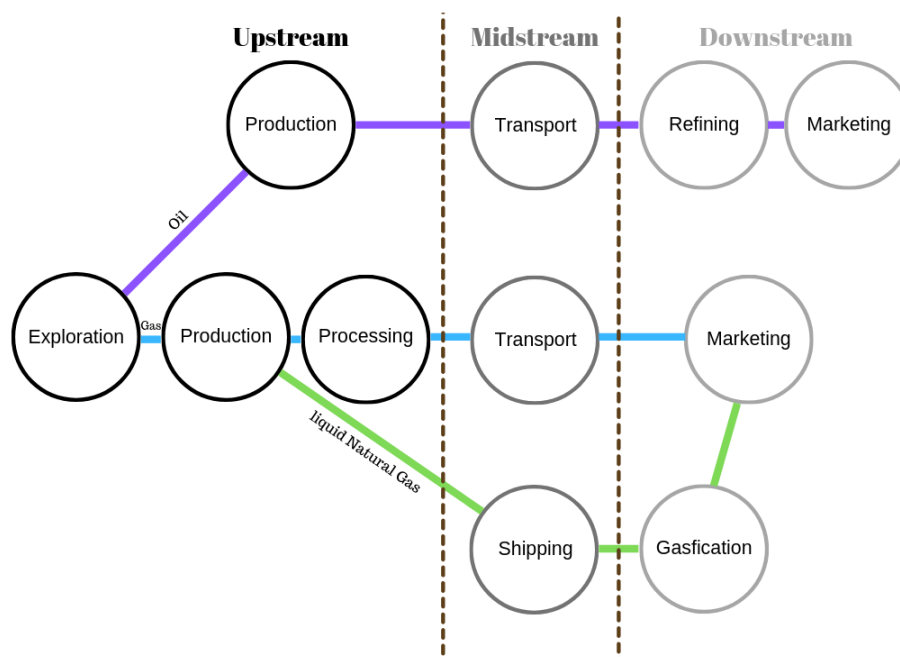


Figure 1.1: The value chain of oil and gas industry [1]

The upstream involves what is the exploration and development of oil and gas, the midstream covers the transportation of oil and gas, and the downstream controls storage and sales [21]. Based on the market division, we get four main problems [1]:

- A large amount of paperwork and verification processes and an increased economic costs and transaction time.
- The risks of fraud, error and inefficiency in transactions are high.
- The work of third parties is very expensive, inefficient and slow
- The important data have a high risk of attack.

The blockchain allows us to take market exchange models to digital profitable platforms unimaginable a few years ago. Thanks to the fact that it keeps a single copy of the record of all the transactions made, it is very useful to reduce costs in transaction processes, distribution and coordination among others, favoring efficiency and security in company certifications. [20]

Considering these benefits, this thesis work proposes a model that is based on Blockchain technology, allows the Ecuadorian industry to make use of all the features and capabilities that it offers, making possible in principle the execution of the procedure for registering all types of contracts for the offices of the oil industry as an innovative and immutable registry thanks to an ACID database that provides Couch DB, this contributes to a credible system in terms of document handling and inviolability.

In the world of blockchain, there are several companies that are dedicated to developing such platforms, one of the most important and open source is Hyperledger created by the Linux Foundation, to support distributed ledgers [22].

Development with this platform is very simple since it uses common programming languages such as JavaScript and object-oriented modeling language, which allow it to be much more flexible than competitive products. To ensure the security and inviolability of the data, a physical device can be integrated into the company's computers, called the Hardware Security Module (HSM) that stores and generates the private keys of the nodes for solid authentication, through processing cryptographic [23].

The document records the step-by-step development of a demo of an oil supply chain that uses a blockchain. The process is detailed from the beginning with the selection of the tools until the interaction of the user with the system, which presents the basic characteristics and the behavior closest to a real environment.

# Chapter 2

## Analysis of the problem

As oil prices recover tentatively from the collapse of 2014 and investments in alternative sources of renewable energy gather momentum, oil and gas companies need to innovate to stay competitive and maintain fuel flow [24].

The real task for the oil and gas sector is the speed with which it can move to take advantage of the many opportunities that blockchain will convey.

### 2.1 Diagnosis of the current situation of the main oil companies in the world

The United States is the largest consumer of oil in the world, followed by China. According to the Energy Information Association of the United States (2019), the North American country consumed about 7.5 billion barrels in the year, which is equivalent to 22% of the world oil consumption [25].

Nowadays, there are more than 200 oil and gas companies in the world, which are being seriously attacked by the great growth of the National Oil Companies (NOCs), run by the government of each country itself. The five main oil companies in the world are listed below by their annual revenue: [26]

- Sinopec – USD 420.38 billion in 2018
- Royal Dutch Shell – USD 388.38 billion in 2018
- Saudi Aramco – USD 356.00 billion in 2018
- China National Petroleum – USD 342.21 billion in 2018
- British Petroleum (BP) – USD 298.76 billion in 2018

The world currently has large oil reserves in different countries. The one with the biggest oil reserves is Venezuela, followed by Saudi Arabia, Canada, Iran, Iraq, among others [27].

According to the Colombian Petroleum Association (ACP), for 2019, investments close to 5 billion dollars were made for the sector, 14% more than 2018, thus going from 800,000 barrels per day to 900,000, meaning a growth of 4 %.

The oil company Ecopetrol is following the actions of the world's largest oil companies such as BP and Shell that use blockchain technology to carry out transactions within the industry. This implementation allows them to reduce costs, reduce time and keep a more transparent record of all the processes that are carried out in the supply chain, avoiding the risk of fraud and human mistakes. Ecopetrol's plan to implement this technology requires an investment of USD 120 million for its first phase. However, this investment will allow estimated savings between USD 240 million and USD 360 million by 2023, the oil company estimates [28].

## 2.2 Diagnosis of the current situation of Ecuadorian oil companies

### 2.2.1 History of advances in the Ecuadorian oil industry

In Ecuador, the first oil well was discovered in Ancón, in the peninsula of Santa Elena, by the English company Anglo. However, production at commercial levels did not occur until 1925 and export until 1928, although in marginal quantities. Until 1971, oil exports did not exceed 6% of total Ecuadorian exports, according to data from the Central Bank [29]. Between 1928 and 1957, the country exported 42 million barrels of crude, equal to the volume exported only in 1972, the year in which the era of the oil boom was inaugurated. For nearly forty years, from 1928 to 1959, the exploitation of crude was concentrated in the Santa Elena peninsula. However, in those years, several foreign companies such as Shell, Standard Oil, California Oil, Tennessee, and the Western Geophysical Co, obtained more than 5 million hectares in new concessions to carry out oil exploration on the Ecuadorian coast and in the Amazonian region. This is reported in the book "Milestones of the Petroleum Industry 1829 - 2005", published by Petroecuador in 2006. [30]

On June 23rd, 1972, the Ecuadorian Petroleum State Corporation (CEPE) was created to carry out activities assigned by the Hydrocarbons Law: explore, industrialize and market necessary products of the petroleum and petrochemical activity. When CEPE was created, for the first time, the National Government had an instrument that allowed it to put into practice the national will to administer and control its own account for the benefit of the country. CEPE began its activities in exploration, that is, in the search for new deposits; in commercialization, transportation of hydrocarbons and derivatives, amid the resistance of local and foreign interests [30].

### 2.2.2 Marketing and production

As for its problems of production and commercialization, the national oil is located in Amazonian sections of difficult penetration, so it is necessary to work adapting jungle regions at great costs and complications of transport of the equipment for its extraction.

The oil is transferred to Puerto Balao in Esmeraldas, so the immense transecuadorian pipeline that has to go up and down the mountain ranges was built. Around 340,000 barrels per day are pumped through the pipeline, the remaining 50,000 barrels are transported through the Transandino pipeline of Colombia to the port of Tumaco and from there, by means of Cabotage to Esmeraldas. Petroecuador transports the products of the Refinery from Esmeraldas to Quito and Guayaquil, by means of a pipeline and from there, to the cities by Cabotage. The transport from the plants and deposits to the different places of the country is done by means of auto tanks in charge of private transporters.

For international transport we have an Ecuadorian Oil Fleet (FLOPEC) created with Ecuadorian and Japanese capitals, which in any case is not supplied by having to lease other ships; so its expansion is necessary.

### 2.2.3 Transportation and storage of oil

The pipeline has five pumping stations, four pressure reducing stations, a marine terminal in Balao, a monoboya, a ballast water treatment system, eighteen oil storage tanks, an electronic monitoring and automatic data acquisition system and an integral system of radio and television communications.

The internal transport of crude oil and derivatives is carried out in different ways, with a network of pipelines, pipelines and gas pipelines with a length of 1,600 km, capable of transporting more than half a million barrels a day. The SOTE Transecuadorian Pipeline System transports crude from the eastern region to Balao, near the Esmeraldas State Refinery.

Petroecuador transports the products of the Esmeraldas Refinery to Quito and Guayaquil, by means of a pipeline and from there to the cities by cabotage. The transport from the plants and deposits to the different places of the country, it is done by means of auto tanks in charge of private transporters. In the Eastern region there is a total crude storage capacity of 593,000 barrels, at the head of the pipeline and in the export port, the storage capacity is 5 220 000 barrels distributed in 18 tanks installed, these tanks They are located on 3 km of beach and at a height of 183 meters above sea level, which facilitates loading on ships. [31]

### 2.2.4 Main Ecuadorian oil companies

In Ecuador, there are several private and public oil companies settled throughout the region and regulated by the *Agencia de Regulación y Control Hidrocarburífero* (ARCH). Below is Figure 2.1 showing the daily production of oil barrels of oil companies operating in the country. The table shows that the main Ecuadorian oil production company is Petroamazonas EP with 361,501 barrels of oil per day, contributing with more than 65% of national production, which is why it will be considered for the analysis of the supply chain.

ORD	EMPRESA	BLS DIA
1	Petroamazonas EP	361,501
2	Operaciones Rio Napo Compañía De Economía Mixta	73,056
3	Andes Petroleum Ecuador Ltd	34,024
4	Repsol Ecuador S.A.	25,751
5	Sociedad Internacional Petrolera S.A.	12,714
6	Agip Oil Ecuador B.V.	10,696
7	Petrooriental S.A.	9,959
8	Orionoil Er S.A	4,793
9	Gente Oil Ecuador Pte.Ltd	4,447
10	Consorcio Petrosud Petroriva	3,962
11	Orion Energy Ocanopb S.A.	3,272
12	Petrobell Inc.	2,407
13	Tecpecuador S.A.	2,352
14	Consorcio Petrolero Palanda -Yuca Sur	1,923
15	Pacifpetrol	1,277
16	Consorcio Pegaso (Campo Puma Oriente S.A.)	731

Figure 2.1: Main oil companies in Ecuador according to their daily oil production [2]

## 2.3 Petroamazonas Ep

The Public Petroleum Exploration and Exploitation Company Petroamazonas EP was created by Executive Decree No. 314 of April 6, 2010. Dedicated to the management of activities undertaken by the State in the strategic sector of hydrocarbons and substances that accompany them, in the exploration and exploitation phases; with its own assets and budgetary, financial, economic, administrative and management autonomy [3, p.1].

The oil company with 80% of national oil production, operating in 22 blocks, 19 of which are located in Eastern Ecuador and 3 in Coastal Ecuador. In 2019, Petroamazonas EP met 99.79% of its goal in terms of production requested by the government, reaching a production of 423,970 barrels of oil per day, with a cost of USD 18 each. With a budget of approximately USD 2,855 million, it managed to develop 250 additional wells [32].

The institution is made up of different strategic areas that allow the correct operation of its operations, this organizational structure is detailed in Figure 2.2



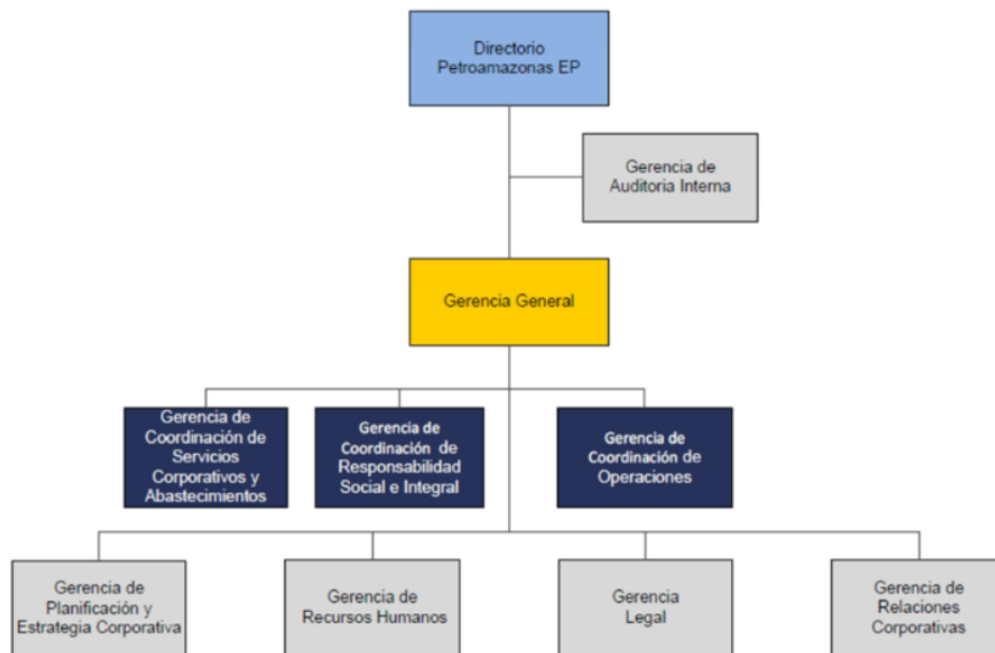


Figure 2.2: Organizational Structure Petroamazonas EP - Level 1 [3, p.9]

For the present research work, the Materials Headquarters will be considered, because the different support processes for the supply chain are controlled.

### 2.3.1 Materials Headquarters



Figure 2.3: Structural Organization Structure of Materials [4]

According to Petroamazonas EP [4, p.58-61], the main contributions are:

- Perform a timely and agile management of the different processes of purchasing equipment and materials, as well as compliance with the delivery times established for these efforts;
- Maintain proper administration of Suppliers;
- Control compliance with the policies and procedures that regulate local and international purchases of the company and administration of warehouses and / or stores;

- Plan the strategy of the Logistics and Materials Chain and supervise its execution;
- Supervise and control the time in the placement of purchase orders to local and foreign suppliers;
- Guarantee stock control levels in warehouses of supplies and materials;
- Ensure a safe air operation for personnel logistics, and;
- Maintain a quality management system.

The products that are delivered by the Headquarters are:

- Purchase Orders;
- List of approved Local Providers;
- List of approved International Suppliers;
- Material Master Catalog;
- Registration of air, land and sea transportation services of Petroamazonas EP personnel;
- Registration of transport and logistics services of materials, and;
- Custody and storage of materials.

### **2.3.2 Departments that interrelate with the Purchasing Area**

Purchasing Area department is part of the support processes, and this is where the main production failures are evidenced. The area works in a transversal way with all of the company, since it provides the necessary materials and supplies for the execution of the processes. Figure 2.4 shows the interrelations that this area has with the main managements that require purchases.



Figure 2.4: Shopping area interrelation [4]

Once the main areas that are interrelated with the purchase area have been identified, we can perform the analysis of the processes and procedures, in order to determine the main distribution failures in the supply chain and issue a recommendation based on blockchain technology to improve procedures.

### 2.3.3 Purchase Management Time

The purchasing department is a strategic area in which a good management model can reduce costs and increase profit margins, because it is the area that most expenses entail within the entire company, becoming a strategic element of the company [33].

According to Ballou, Ronald H. (1991), in most companies, the purchasing department plays a fundamental role within the organization since the materials used represent between 40 and 60% of the value of the final product. Therefore, a reduction in costs, although minimal, may reflect the same or greater impact on the company's benefits compared to other areas with greater reductions [34].

Analyzing each of the following stages of the purchasing process within Petroamazonas EP, the Materials Headquarters can determine the time of purchase management of goods.

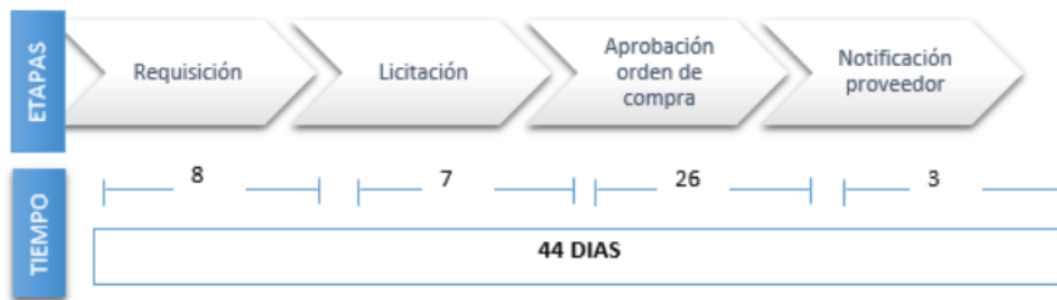


Figure 2.5: Purchase management time determination [4]

As we can see in Figure 2.5, the purchasing management time is quite extensive and tedious, having to go through four stages of 8, 7, 26 and 3 days respectively. Since this process is cumbersome and it is interrelated with other areas, it makes the overall process is time consuming and expensive, due to the time involved in all the procedures.

### 2.3.4 Demand Planning

The optimization of operations through the supply chain, known as demand planning, has become a highly relevant activity within the supply flow between suppliers and customers. The objective is to maintain adequate stock levels to meet the requested demand [35].

Currently, the Materials Headquarters do not have a correct standardization of processes and procedures for demand planning, causing problems with the control of the supply chain and sales, among others [36].

Due to this, we seek to improve information management internally and externally, by integrating a blockchain model for the supply chain, thus achieving an effective and transparent collaboration between the different departments that interrelate with the Materials Headquarters.

### 2.3.5 Provider Development

Nowadays, the Materials Headquarters do not have a methodology for developing the capabilities of their suppliers, causing unstable business relationships, affecting the delivery time of the materials and the price, and causing disagreements by the end users. The aforementioned issues caused by the purchasing management time can not be standardized by the various conflicts that come into existence. To solve these problems, it is intended to implement a blockchain model, in which an optimal and transparent collaboration between the different actors involved is achieved, helping to meet suppliers with the objectives established by Petroamazonas EP, thus achieving stability in their processes and an increase in economic income for the optimization of time and communication in the supply chain.

In order for Petroamazonas EP to continue to be a reference and leader of the Ecuadorian oil industry, in the exploration and exploitation sector, it must constantly maintain evaluations in its different activities and frequently improve its supply chain, and jointly

with the Materials Headquarters, work in creating bonds of trust and improving business relationships with their suppliers, in order to optimize resources and be more effective in the service with the end user, for which it is necessary to establish a new form of purchasing procedures through the use of blockchain.

## 2.4 Supply Chain

In the business world, the supply chain is a network of organizations, people, activities, information and resources involved in moving a product or service from the supplier to the customer. The chain executes processes that involve the transformation of natural resources, raw materials and components into a finished product that is delivered to the final consumer [37].

One of the objectives of the supply chain is to reduce manufacturing costs and be competitive at the same time. In addition, to include functions such as customer service, marketing, development, operations, etc. [38].

### 2.4.1 How the supply chain works?

The entire supply chain of a company originates from suppliers. In the case of hydrocarbons to offer a service, it needs suppliers that will provide the necessary supplies and materials for the Exploration and Production phases, thus obtaining a crude product necessary for the final product. The supplier provides the necessary amount of materials, these are taken to the production line or related processes to make the final product [38].

The final product must pass quality tests in Petroamazonas EP laboratories and then be stored. Once it is stored, it is transported in distribution centers according to its demand, these centers function as an intermediate station between the manufacturer and place of sale. These processes may not be very complex but if any element of this chain fails, then the entire system will collapse.

### 2.4.2 Participants in the supply chain

Each company has a different supply chain. Sometimes, companies are cautious about the operation and management of the supply chain because it becomes a fundamental part of their success and thus preventing their competitors from copying their distribution model. However, all supply chains have in common 5 participants, which are: [38]

- **Suppliers:** Organizations that supply the raw materials or fundamental components for the realization of a product.
- **Producers or Manufacturers:** Organizations that manufacture the product. It includes all the organizations that manufacture the final product. Normally, producers obtain the necessary materials for the manufacturing of the final product from suppliers. Sometimes, manufacturers develop their own components but due

to their high costs and the long process that this entails, they choose to manage several suppliers and a production line to reduce costs.

- **Distributors:** These companies acquire the largest amount of products from producers based on consumer behavior. They need to keep an inventory, transport products and to sell to retailers, and organizations. Distributors can acquire full ownership of the product or simply work as intermediaries between the customer and the producer and request more or less products depending on demand. In addition, they act as a buffer for producers, as they protect them from market fluctuations. The fact of storing a large quantity of products in their inventories protects the producers, since if the demand increases, the distributors will offer stored products, and in case it decreases, the inventory of the producers is simply maintained. Therefore, the producer will not feel the market fluctuations and will not have to reduce its production, thus achieving a constant rhythm in the supply chain.
- **Retailers:** Store the final products and sell on a smaller scale to the individual consumer. They also study the market and customer preferences, attracting customers through advertising and discounts.
- **Clients:** groups of people or organizations that acquire or use any product from a company. In the supply chain, large organizations are also customers, since when producers buy products from suppliers, they become customers, so at each stage, there is a seller and a buyer.

### 2.4.3 Components of a typical supply chain

A supply chain typically is bidirectional, that is, you can go in both directions. Ideally, a supply chain would have an address, but it is possible that a customer is not satisfied with the product due to product failures, or because he did not like the product, for which he can request a refund of the money, return of the product or exchange, which leads to the need to go back in the opposite direction to the chain for this request to be carried out successfully.

In the chain, there are 8 main components: [38]

- **Natural resources:** For the execution of a product you may need natural resources such as light, water, gas, etc.
- **Raw materials:** They are necessary raw materials to produce a certain material to have the final product, these can be alloys, farm products, steel, etc.
- **Components:** These are basic components to build the final product, they can be chemicals or devices that are needed to obtain the final product.
- **Finished products:** Once put together the natural resources, raw materials and components the finished product can be created.

- **E-commerce and the retail sale:** When the product is finished, it is time to announce it to physical and virtual stores for later sale to the final consumer.
- **Recycling and return:** If the customer is not satisfied with the product, it can be returned. In some cases it can be recycled or reused, regardless of the final product, the customer should always get a refund.
- **Distribution:** Occurs at almost all levels of the supply chain. The supplier distributes the products to the producers which distribute it to the distribution center and so on.
- **Transport and storage:** It occurs in several stages of the supply chain, since at each stage, transport is needed. Storage also occurs at each level, except when it reaches the final consumer.

#### 2.4.4 Supply Chain Issues

The supply chain must deal with many problems, which cause large economic losses. The main problems are the following: [38]

- **Globalization:** Globalization allowed the global economy to be brought together. However, chain management remains a very complex challenge and it is profitable, so many companies set up their operations centers in the country where labor can be cheaper. This leads to outsourcing that complicates the entire process, since they must deal with different collaborations in the settled country and coordinate with as many companies to cross the borders. Therefore, the oil industry faces the risk of losing visibility, control and management of its total products.
- **Rapid changes in the market:** Consumer tastes are constantly changing due to fashions, personal aspects, social, cultural and psychological behaviors. Thus, the industry must ensure that these changes are well known. They should also ensure that production costs remain low because no one can know how long products will be in demand.
- **Features and forecasts:** Companies must sometimes add new features to existing ones to stay in the market. They should also predict the demands of their products, because if they are not accurate, they may lose revenue.
- **Compliance and quality:** When you handle thousands of products a day, tracing them becomes a very difficult task. So you must ensure compliance with national and international regulations, from manufacturing until it reaches the final consumer.
- **Lack of transparency:** Generally, the final consumers do not know where their products come from or who makes them, so they do not know the true value of the components.



- **Corruption:** The supply chain is prone to human errors, however many of these errors are intentional, which generates losses in quality and income, without counting the legal problems that could be caused if discovered. Some of the factors that cause corruption are personal relationships, bribery, scams, counterfeit products and data.
- **Quality costs:** To verify that the products meet the quality requirements, it is necessary to hire laboratories and qualified personnel to perform the corresponding quality tests. These analyses involve economic expenses, time, human resources and infrastructure. In addition, any product that does not pass the test will be discarded, causing economic losses.
- **Inventory costs:** It is necessary to preserve the components, raw materials, and final products so it requires large spaces to store preserving their quality.
- **Transportation costs:** Transportation is necessary at all levels of the supply chain, which implies large daily costs. There are cheaper solutions but slow down the process, which eventually causes a loss in income.
- **Acquisition costs:** When components are purchased from other companies in exchange for money, there is a risk that prices will change based on demand and shortages.
- **Relatively slow:** Currency exchange is extremely slow and prone to problems, logistics are inadequate, business is quite regressive due to time difference, and payments last several days or weeks so the materials and components remain locked during that time, causing delays in the production line.
- **Poor customer service:** To have a more efficient service, better customer support is required, as customers play a fundamental role in the outcome of the products.

## 2.5 Blockchain in the supply chain

Currently, the oil and gas supply chain is prone to errors and is not able to effectively keep up with consumer demand. So the blockchain comes into play to solve the main problems of the supply chain with its main properties. [38]

- **Decentralization:** This means that the registry data is not exclusively owned of a person, organization or company. On the contrary, all members of the network will have access to it. So the concept of counterfeiting will disappear since no one can own any kind of information.
- **Immutable database:** Thanks to this property, no one can manipulate information in the registry. However, in the private blockchain, it can be modified, but it must be verified the same as in all cases by the users of the network who have the

exclusive control to modify. The information can be modified but not deleted, so the change history will always remain.

- **Transparency:** In a public blockchain, all people in the network will be responsible for their actions since everything on the network is visible for anyone. While, in a private one, it is partially visible where the authorities have greater power due to it would be difficult to handle it if everything was public.

Thanks to these characteristics, opportunities exist in the industry for transparency, efficiency and optimization [39]. In today's industry, the use of databases and computer programs does not enable the adequate coordination due to the continuous attacks of hackers and the risk of fraud due to the constant manipulation of data by workers in this industry [20]. In addition, these centralized systems are expensive and difficult to maintain, so the performance of these processes is seriously affected [39].

The implementation of blockchain technology in the supply chain has the ability to reduce maintenance, upgrade, security, labor, and runtime costs [20], [39].

The oil industry supply chain is divided into 3 categories [39]. Upstream refers to all operations related to the exploration and extraction of raw materials, in this case, oil and gas. Midstream refers to the transportation and storage part of the resources obtained. Downstream refers to the operations of refining resources in different final products to sell to its customers such as gas stations, domestic users, etc.[20].

According to an investigation carried out in 2017 by a company recognized worldwide in the field of business intelligence, called IBISWorld, revenues for this industry for the Upstream sector were around USD 2 billion, contributing approximately between 2-3% of the world GDP. This number can reach up to 8% of world GDP if we consider the other two sectors that entered USD 3 billion in 2017 [40].

### 2.5.1 Blockchain for Upstream Operations

This sector involves several stakeholders that cooperate with each other for the exploration and extraction of resources. This group is made up of companies that conduct surveys to decide where to drill, companies that conduct exploratory drilling, companies that supply oil platforms or skilled labor, and many more [39].

The upstream segment is controlled by four relevant stakeholders: majors who are the big international oil companies that control a large part of the oil wells, usually these companies are involved in the 3 sectors, among the best known we have BP, Chevron, ExxonMobil and Royal Dutch Shell. The national oil companies known as NOCs, are oil companies run by the government of the country to which they belong, in the case of Ecuador, they are Petroecuador and Petroamazonas EP. The independents are companies that offer specific services for a specific segment, in this case, they provide jobs in exploration and production for oil and gas fields. Last but not least, the oilfield services that are companies that provide specialized machinery, labor, and support so that all processes in this sector are carried out [41].

Therefore, data transmission and security in this sector are very important for success and profitability. The use of blockchain technology in conjunction with the use of smart contracts can end the inability to effectively coordinate between hundreds of departments that interact with each other, eliminating physical paperwork and wasting time on paperwork which imply economic losses [20],[39]. The goal of any oil company is to maximize oil extraction, but this process requires the participation of many parties that must demonstrate that their work has been done correctly. Currently, the process is very long and tedious as many companies outsource to other companies to obtain items they need to offer their services. These processes that are carried out within the entire supply chain can take up to 100 days, where only the purchase process as we saw in chapter 2.3.4 takes up to 44 days. With blockchain technology, it can easily demonstrate who performs their work correctly, granting faster and more secure certifications and payment mechanisms in a matter of a few days [40].

### 2.5.2 Blockchain for Midstream Operations

In this process, crude and refined oil are transported from the platforms and extraction fields to the refineries, where they are also stored. Different means of transportation such as ships, trucks, trains, pipes and even airplanes come into play in this procedure. So that coordination between the companies providing these services is as big and complicated as in Upstream [39].

Despite the need for multiple interconnections between companies, the capital risk is lower than the Upstream. This is because everything is regulated, from transport, storage to environmental implications, since the product must pass through international, national, local and municipal borders. However, this highly regulated process with precarious environmental implications can be improved thanks to the transparency offered by the use of the blockchain, optimizing time and money in these procedures [42].

An application for this sector is the inspection of pipes that can be hundreds of kilometers long with dozens of bifurcations that must be inspected manually. Currently, this process is very long and expensive for a single company but with the application of blockchain technology, local companies can be hired to inspect the section of the pipeline in their area. In this way, each local company attests to its work done in exchange for economic rewards and at the same time, it gains reputation and credibility when it fulfills a correct job. With responsibilities endorsed by the company and with transparency this process becomes more efficient in terms of energy used and money invested [39].

### 2.5.3 Blockchain for Downstream Operations

Here, the final process is carried out where the raw material reaches the consumer in different ways after going through the processing, refining, and purification of crude oil and natural gas. The main products are gasoline, jet fuel, diesel, asphalt, kerosene, plastic, and more [39].

There are two great participants that play an important role in this sector. Global Integrated Refiners (GIR) is the major we saw in Upstream which participate in all 3 sectors. And the independents, in this case, are companies that are dedicated to refining and selling the final products to consumers [43].

In this sector, the implementation of the blockchain would have a very important role in the petrol stations with the final consumers, such as granting them certain benefits for their loyalty and thus, improving the user experience, achieving greater loyalty, reducing administration and costs [39].

Since there are companies dedicated to the consumer, their success can be altered by global geopolitical trends that affect the price of crude oil and any optimization in these processes are very beneficial for GIRs as well as for independent ones, so the use of the blockchain offers opportunities with immediate benefit [43].

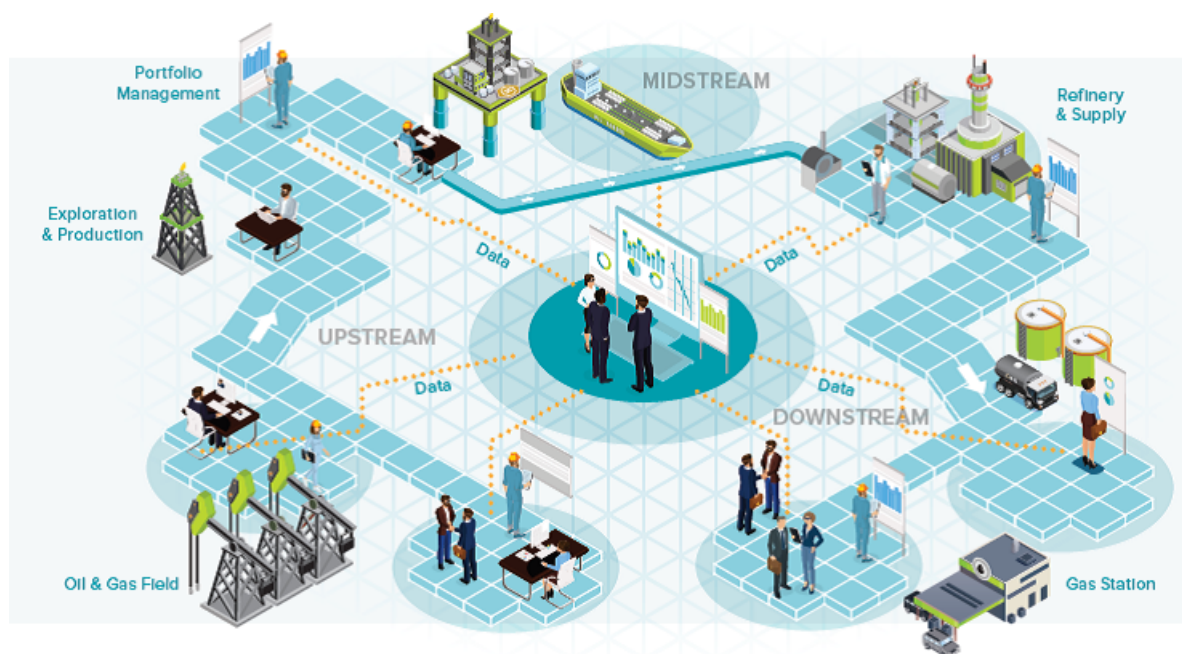


Figure 2.6: Upstream, midstream and downstream operations in the oil industry [5]

#### 2.5.4 Benefits of Decentralization

The implementation of the blockchain in the supply chain enable considerable improvements in the 3 sectors of the industry as we see in Figure 2.6, where it is possible to interconnect all the departments of the 3 sectors in a single platform, preventing fakes and thus, increasing customer satisfaction. In addition, it makes it possible to eliminate bureaucracy and unnecessary resources. Being more specific, it offers systems of transparent records, real-time monitoring of products, faster and more efficient services, a chain without trust where it is no longer necessary to blindly trust elsewhere, product certifications, greater safety, pollution reduction, and costs reduction [38].

In the **Upstream sector**, they manage performance-based contracts that they reward based on the quality of their work. This method causes economic losses as inefficiencies arise in the procedures and a lack of security, which leads to fraud. Its main causes are: how complicated it is to demonstrate whether your work has been done correctly because of the amount of paperwork you must perform; and how difficult it is to align the objectives of all the companies that work for oil exploration and extraction [41].

The use of the blockchain achieves to end with the chain without trust since it will not be necessary to blindly trust a company and expect it to do its job well. With the certificate, you can grant benefits to the company for performing correctly its job and making payments in a few days instead of months. In the event that another company finds errors or fraud in the process, it would take its place and the first company would have legal problems and lose all types of contracts with the industry. In this way, it is possible to find errors in real-time and propose solutions immediately to optimize the processes of oil extraction and exploration [41].

Other cases of immediate improvement with the implementation of the blockchain in performance-based contracts are: the identification and maintenance of wells and equipment, thanks to the constant updating of information on well records and equipment maintenance history; and waste and recycling management that due to performance control can be economically incentivized to those companies that promote recycling [41].

A big problem in this sector is that before digging it must be determined who the lands are from. This tedious process can be greatly optimized thanks to the benefits that the blockchain offers. The main problem is that each town, city, province, and states have different ways of registering and managing the properties. These differences cause duplicate, lost and fraudulent registrations that require long legal processes to solve them. However, with the blockchain all these records can be collected by obtaining a single, clear and immutable record of the landowners, thus avoiding long legal processes.[41].

In the **Midstream sector**, the blockchain plays a fundamental role in multiple transportation thanks to the real-time tracking of products, avoiding long manual efforts that end in confusing information. With the blockchain it is possible to share the database to all interested parties from different sectors, giving the possibility to see in real time the status and location of the assets. It is also crucial for the maintenance and regulation of the transport network and all the infrastructure that this entails [42].

A very important and life-saving application is to have quick responses and mitigate environmental disasters. This is possible thanks to the records obtained in real-time processes equipment maintenance because with this you can support the efforts of planning, response, and recovery. Being able to implement intelligent alerts in the event of a disaster or a certain event that requires the intervention of other parties. In addition, it is possible to know exactly where the fault was caused, which equipment failed, who was responsible for examining this equipment, what is the real amount of economic losses as well as the product, and more. Recovery can be a long and legally complex process but with the blockchain, it can be quickly and more accurately identified thus avoiding environmental disasters [42].

As a result of the strong regulations and the number of assets that are managed per



day, it is necessary for companies to work together to mitigate risks, and thus be able to benefit from sharing information.

The main problem of the **downstream sector** is that the companies that handle the products change the records and sell lower quality products, harming the industry and company that runs everything. If blockchain is implemented in a mandatory manner throughout the supply chain, companies would find it almost impossible to falsify documents or hide quality records [43].

The smart contracts make it possible to pay immediately according to the quality and the moment in which it is performed, allowing more efficient and frequent flows between the different parties, reducing delays and responsibilities [43].

## 2.6 Oil giants and the blockchain

In the last two years many oil companies, banks and development companies are working together to develop this new technology. Finboot is the startup that collaborates with the oil giant Repsol. Together they created the BlockLabs application. This, based on blockchain, enables the digitalization of refining and petrochemical products to simplify expensive verification processes. Verifying refining and petrochemical products is not an easy task. Many samples are handled: some mislabeled, others with confusing information, plus those that get lost along the way. The oil companies, specifically Repsol, these problems bring losses of up to 400,000 euros.[44]

Repsol's research laboratory, Tech Lab, has been working with Finboot for some time. This startup is teaching you how to use the blockchain in the oil industry. For what Repsol intends, the blockchain involved has to share the products with the verifying agents. A flow of information, which, thanks to this solution, can be done digitally and not on paper, as it was done until now [44].

Create digital equivalents: BlockLabs, the application developed by Finboot and Tech Lab, creates a digital equivalent of a physical product. Then it grants a token (digital right) that will always be associated with an article. "This code is created only once and is unalterable," says Repsol. With this code is how Repsol digitalizes processes, simplifies them, and estimates to save 400,000 euros. In the summer they made the first laboratory tests, and they trust that since April 2019 the application is working in Tech Lab, where a year they handle up to 60,000 samples of these product [44].

Tomas Malango, manager of experimentation at the Repsol laboratory, says on the oil company's website that the application "could be interesting" for clients such as the Barajas airport. "For example, if you want to know at all times the quality of our aviation kerosene".

### 2.6.1 Blockchain consortium with oil industries.

According to a press release on February 26, 2019, seven global oil and gas companies, including the giants of the US industry ExxonMobil and Chevron, have partnered to form a Blockchain consortium, with the aim of overcoming limits they have in common. The

so-called Consortium of Oil and Gas Blockchain, which resides in the Offshore Operators Committee (OOC), intends to carry out Proof of Concept tests (PoC) to explore and apply the Blockchain benefits, as well as contribute to the adoption as a global technology. The founding members include Chevron and ExxonMobil, two of the 10 largest oil and gas companies in the world, based on 2017 revenues of \$ 237 billion and \$ 134 billion, respectively. The OOC board also includes ConocoPhillips, Pioneer Natural Resources, Hess, Norwegian Equinor and Spanish Repsol, based in the United States. Rebecca Hofmann, chairwoman of the OOC board of directors, said the creation of the consortium is an important step towards establishing a basis for blockchain-oriented standards, frameworks and capabilities for the oil and gas industry [45].

**Costs and times:** It is well known that international exchanges of hydrocarbons are made daily in large amounts of volume and therefore, of great monetary value. When making use of a blockchain regulated by a trustworthy entity for international transactions, it would reduce the shipments of documents, purchase of invoices, transfers of bank funds, reducing costs and times [46].

**Transparency:** Companies invest a large amount of time and effort to ensure that all interested parties have access to all these documents in time and form. Having this information in a blockchain would save time and reduce the risk of fraud [46].

**Supply chain management:** Globally, the supply chains of the oil and gas industry manage a large network of suppliers, transporters and buyers, which requires a great administrative effort, opening the possibility that mistakes are made, through a blockchain. A record of all these movements could be kept, which would significantly reduce the risk of making an error [46].

## 2.7 Problem Statement

For oil and gas business, data have gone from an asset to a burden. Companies are drowning in data and urgently need a way to control and authenticate information. Blockchain has an enormous potential to reduce the risk of fraud, error, and invalid transactions in energy trading, make financial transactions more efficient, facilitate regulatory reporting requirements, and enable interoperability. Blockchain will have huge benefits both upstream and downstream. From scheduling equipment maintenance to managing exploration acreage records, blockchain offers a single, unalterable record of transactions and documentation between numerous parties. Distributed ledgers also create more efficient and transparent downstream activities, such as exchanging products, secondary distribution delivery documentation, demurrage, and claims management. Mid-stream, it will revolutionize joint ventures, risk management, contracting, and regulatory compliance [24].

The oil industry is a highly complex business that has different processes such as production, refining and delivery of fuel products.

The main problems facing this industry are:

- Find new ways to locate oil and gas deposits.

- Transport of volatile fuel components safely and efficiently.
- Management of complex supply chains.
- Ensure trade and settlement of energy raw materials.
- Ensure and simplify billing and payments.
- Maintain an arduous and always changing regulatory compliance.

These problems, together with the producers, transporters and distributors can be solved or reduced to a great extent with the use of blockchain technology [47].



# Chapter 3

## Hypothesis and Justification

### 3.1 Hypothesis

Can blockchain technology optimize the supply chain process in the Ecuadorian oil and gas industry, reducing the risk of fraud and errors?

### 3.2 Justification

In the industrial sector specifically in oil, they have a big problem with the amount of paperwork that must be carried out at the time of exchanging goods. This event is because they use traditional and inefficient digital systems that do not allow having all the necessary information available, avoiding taking advantage of the information properly.

Large oil companies in the world such as Total, Chevron, Shell, BP, Equinor, Mercuria, and Gunvor joined together to invest in the development of a platform based on blockchain technology in this sector. With the aim of boosting efficiency and savings of commercial financing up to 30-40%. Since a basic process can rely on up to 36 original documents and more than 240 copies [48].

This event led to the question of whether is it possible to apply this technology in the Ecuadorian oil industry, specifically in the Petroamazonas EP oil company. After a short investigation of this technology and the most frequent problems in the supply chain, it was possible to conclude that the blockchain is capable of transforming this industry through the implementation of this platform in the supply chain. Thanks to its transparency, traceability, confidentiality and interoperability properties.

# Chapter 4

## Objectives

General Objective Develop an application based on blockchain technology for the supply chain of the Ecuadorian oil company PetroAmazonas EP, to show the benefits related to time, security and money.

### 4.1 Specific Objectives

- Analysis and study of Blockchain technology. Know what are the fundamental bases for its operation. Know the current state of technology and its different tools.
- Deployment of a distributed network based on Hyperledger Fabric and Composer. Being able to implement a blockchain in the supply chain of the oil industry, defining the nodes, assets, chaincode and transactions that are carried out during the logistics process.
- Install all the requirements and environments to run the network.
- Development of a real demonstration of the operation of hyperledger technology in the oil supply chain. A use case is implemented in which the study is applied.
- Design and configuration of the front-end and the back-end for the demonstration.
- Transparency: Propose a distributed network, with immutable database and with verification of all participants in real time.
- Traceability: View in real time the history of the records of the transactions made and the status of the assets.
- Confidentiality: Network administrators can restrict information that the participants may or may not display.
- Interoperability: Integration with current platforms and systems.

# Chapter 5

## Theoretical Framework

Since its birth, blockchain had promoted big changes in industries, a clear example is the Bit-coin, the digital currency based entirely on blockchain, enabling interaction peer-to-peer (P2P) capable of managing transactions currency without the need to resort to an intermediary agent [14]. This success gave rise to hundreds of companies and organizations that developed their own cryptocurrencies and purses where to store this currency, managing to expand the concept of Blockchain.

In spite of blockchain's success in recent times, there have been security failures in cryptocurrencies and smart contracts that use this technology [49]. According to the magazine TENDENCIA 2019, in 2018 there were several cases of attacks on different cryptocurrencies through illegal mining [50].

An example of this case is the attack called number 51 that occurred in January 2019 against Ethereum Classic, in which cybercriminals stole a million dollars [49]. This attack requires a lot of computing power so most attacks are aimed at low-value cryptocurrencies that demand less computing power; reaching to steal about 120 million dollars in total. Despite the vulnerabilities found, blockchain continues to be a safe tool for which new challenges arise due to the natural development of the technological ecosystem, which includes cybercrime. These problems have not prevented its evolution and improvement, since the blockchain not only allows simple transactions but also allows to make safe contracts, labor contracts, mortgages and other types of documents with legal bases, preserving its structure and original content, eliminating intermediaries to guarantee its validity [13].

### 5.1 Bitcoin

In August 2008 the domain [www.bitcoin.org](http://www.bitcoin.org) was registered and in October an individual or group under the name of Satoshi Nakamoto publishes the first Bit-coin document, entitled "Bitcoin: A Peer-to-Peer Electronic Cash System" [51]. Many communities praise for the awarding of the Nobel Prize for Economics to Satoshi, however, their identity remains an unknown until today [52]. The document describes a program capable of making online payments from one party to another without going through a financial

institution [51]. In January 2009, the bitcoin network was born with the publication of its open source. This is the moment when, Satoshi mined the first block bitcoins, called Block Genesis, for which he received a 50 bitcoins reward. The first shipment of digital money was made when Satoshi transferred a quantity of bitcoins to Hal Finney. In October 2009, the first change from bitcoins to dollars was carried out. His last contribution to bitcoin was in 2010 and at that time, he named Garvin Andersen as the visible leader of the foundation and development of bitcoin [52]. Thanks to Satoshi, cryptocurrencies emerged that are used to describe all the networks and means of exchange using cryptography to carry out transactions, unlike those transactions that we all know that are verified through a centralized entity [51].

Bitcoin is both a currency and a digital system. As a currency, it can be used in the same way as any currency such as the dollar, the euro, the pound, etc. Since its operation and use are totally the same, but instead of being managed by a central entity that issues it and it supports it, it is completely based on the digital system. One of the most distinguishing characteristics is that the bitcoin system does not belong to anyone, and those who keep it in constant operation are the users themselves. Bitcoin is a digital currency that only supports itself and it can be verified by blockchain technology, it does not allow double spending. Where each bitcoin or part of it is unique, because each transfer process is unique and publicly recorded in a digital accounting book, supported by complex cryptographic structures, called blockchain. It is the main reason why bitcoin is known as "cryptocurrency" and it is the first of its kind, which explains its great value as a digital system. Its distributed accounting technology is an encrypted database where you can store all kinds of information, from digital currencies to smart contracts. So its acquired value is thanks to its power to encrypt all types of information and register it with a unique Urcuquí, abril 2020tprint that makes it unrepeatabe and immutable [53].

The bitcoin protocol is not just a way to transfer "money" from one person to another. It has many more functions and opens a world of possibilities that the global community is analyzing through its blockchain technology.

## 5.2 Blockchain

The blockchain is a single register, consensual and distributed in several nodes of a network. In the case of cryptocurrencies, we can associate it with the accounting book where each of the transactions is recorded. Blockchain is a technology that allows the transfer of digital data with a very sophisticated coding and in a completely secure way [54].

According to the I'MNOVATION article [55], the blockchain contributes with a tremendous novelty: any transfer does not require a centralized intermediary that identifies and certifies the information, but is distributed in multiple independent nodes that register and validate it without the need for let there be trust between them. Once entered, the information can not be deleted, only new records can be added, and will not be legitimized unless most of them agree to do so.

Along with the level of security that this system provides against hacking, we find

another enormous advantage: even if the network were to fall, with only one of those computers or nodes not doing so, the information would never be lost or the service, depending on the case that we speak, it would continue working. An example that illustrates the importance of the distributed network is in social networks. With this system, blockchain would eliminate the centralization imposed by applications such as Facebook or Twitter when identifying or validating the origin of our messages, and the integrity of them would be guaranteed by the network of nodes [56].

### 5.2.1 Why is blockchain so safe?

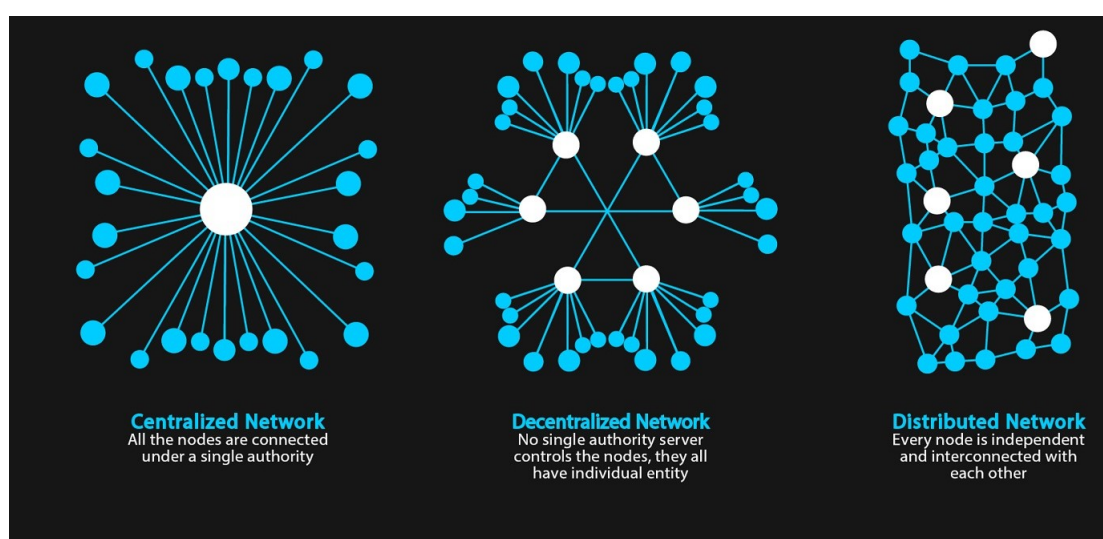


Figure 5.1: Centralized vs Decentralized vs Distributed Network [6]

Being a distributed technology (see Figure 5.1), where each node of the network stores an exact copy of the chain, the availability of the information is guaranteed at all times. In case an attacker wants to cause a denial of service, he should make inoperative all the nodes of the network, since it is enough that at least one is operative for the information to be available. On the other hand, being a consensual record, where all the nodes contain the same information, it is almost impossible to alter it, ensuring its integrity. If an attacker wants to modify the information in the blockchain, he should modify the entire chain in at least 51 percent of the nodes. Since each block is mathematically linked to the next block, once a new block is added to the chain, it becomes unchangeable. If a block is modified its relationship with the chain is broken. That is to say, that all the information registered in the blocks is immutable and perpetual. In this way, the blockchain technology allows us to store information that can never be lost, modified or eliminated. In addition, each node of the network uses certificates and digital signatures to verify the information and validate the transactions and data stored in the blockchain, which ensures the authenticity of said information. In this way, we can think of blockchain as a scribe. A means to certify and validate any type of information. A reliable, decentralized

registry, resistant to data manipulation, and where everything is registered. Currently, we are used to centralized models. We give all our information to companies such as Google or Facebook to administer it, send all our messages through the Telegram or WhatsApp servers so that they can send them or spend fortunes on notaries and institutions to certify and keep our writings or important documents. In blockchain, the data is distributed in all the nodes of the network. As there is no central node, everyone participates equally, storing and validating all the information. It is a very powerful tool to communicate and store information reliably; a decentralized model where information is ours, since we do not depend on a company that provides the service [54].

### 5.2.2 Main Characteristics of Blockchain

The blockchain stands out for having 6 characteristics.

- **Decentralization:** It is the main characteristic of the blockchain since it allows the information in the registry not to have exclusive ownership, that is, it does not depend on a central node, but everyone on the network will have access to it. The system is maintained by the set of nodes which contain the same information, where it does not matter if one fails since the other nodes maintain them. Thanks to this characteristic, it is almost impossible to falsify data so the concept of counterfeit or scam will disappear.
- **Controlled Mutability:** It means that no one manipulates information in the blockchain registry. However, in the private blockchain the data can be modified, but it must be verified as in all cases, by network users who have exclusive control over it. The administrator and users with permissions can edit but never delete the history of the records.
- **Transparency:** In a public blockchain, all the people in the network will be responsible for their actions, since all the data and updates of the nodes that are in the network are visible for anyone. In a private network it is partially visible since the authorities have greater power, because it would be difficult to handle it if everything were public.
- **Efficiency:** It is more efficient in terms of risk and costs since the blockchain makes the database distribution network more transparent.
- **Security:** When a centralized network is attacked, the entire network fails causing large economic losses. However, the blockchain being a decentralized network, if a node is attacked, the system does not fail since all the others contain the same information. For a system to be affected, it must be attacked in 51% of its nodes, this attack is very cost, so it is considered almost impassable. In addition, blockchain have public keys to prevent data from being changed, thus providing better security.

- **Anonymity:** Transactions that are made within the blockchain can be anonymous since the same program is able to automatically determine if the exchange process between nodes is valid.

### 5.2.3 Types of Blockchain



Figure 5.2: Types of blockchain: Consortium, private and public [7]

- **Public Blockchain:** In this case, anyone has full access to read and write in such a way that they can carry out transactions, as well as validate their consensus processes.
- **Private Blockchain:** Its use is limited for companies, individuals or organizations that need privacy in their data. This does not completely solve the trust problem, but it greatly improves the auditability processes, since the writing permits are controlled by the agency that manages it, and the reading permission can be open to anyone.
- **Consortium Blockchain:** It is a combination of a public and private blockchain, where access is restricted by the consortium. In this network, the rules are set by the consortium, and therefore, read and write depend on the agreements. The data they generate can only be seen by authorized people who belong to this network and those who have the corresponding permissions by the consortium, so each participant does not have to worry about where their data are. In this way, it is possible to solve the security and privacy problems and to decentralize them

### 5.2.4 Consensus Algorithm

Consensus algorithms are decision-making procedures for a group, where participants must support the majority decisions. The goal is to create a decentralized system where everyone has the same opportunities to get the reward. To achieve the objective, an agreement must be reached, collaborate among the members of the group, possess the same rights, participate actively in the processes and have the same responsibilities [57]. Next, we detail the main most used granting algorithm.

- **Proof of Work (PoW):** The proof of work comes from the idea of solving the problem with spam. This algorithm is used by bitcoin and lite-coin, among others. The goal is to limit denial of service attacks to Internet resources [19]. Validators, also known as miners, compete with each other to add a new block in the blockchain, after solving a complex cryptography problem, which must start with some consecutive zeros, increasing its complexity [58]. The miners do not know the result and cannot predict it, so it is an act of trial and error that leads to a considerable expense of energy and time, wasting many computer resources but with the advantage of considerably increasing the security of the system, thus avoiding the attacks, and abuses to the system [59].
- **Proof of Stake (PoS):** It is a consensus algorithm developed by critics of the PoW that deals with its main problems. This algorithm changes the computational work by a random selection that depends on the amount of currency the miner owns [60]. With the PoS method, each participant has the same possibility to undermine and even add new blocks to the network based on the amount of currency they own. Therefore, the more coins you have, the greater your chances of winning. In addition, it allows you to join swimming pools or groups to obtain shared benefits, in case you do not have enough coins to participate, dividing the profits in proportion to what you invested [57].

Its advantages over PoW have led it to become a strong competition as it allows blockchains to be faster, consume little energy and virtually eliminate the 51% attack [19]. Its main use is in public blockchains, where validators are unknown and unreliable, or in private business blockchains, where validators come from trusted networks. [48 ieee]

- **Delegated Proof of Stake (DPoS):** It is a variation between the PoS and PoW algorithms [19]. The algorithm is robust and more flexible since it is faster, more efficient and decentralized. Since the mathematical problems are solved democratically, where each member of the network can become a witness and delegate (nodes), and voting only occurs when the system is secure, it is fully decentralized. The code was designed to avoid regulatory problems and manages to make transactions in a second [57].
- **Practical Byzantine Fault Tolerance (PBFT):** The algorithm designed by Miguel Castro and Barbara Liskov in 1999 solves the inefficiency problems of the original algorithm, guaranteeing the security of the system for all its nodes. The consensus is determined by every three votes between nodes [19]. In this case, transactions do not need confirmations, since all nodes communicate with each other at the same time and comprehend the specified block [57]. The protocol does not allow more than  $3n + 1$  failed nodes of the total, thus increasing the security of the system. However, as the number of nodes increases, the system has difficulty tracking the nodes, losing communication between them [57].



- **Proof of Elapsed Time (PoET):** it is a protocol designed by Intel, which creates a certification to use a particular trust code and generates random delays in the CPU to enter the system and keep it safe [57]. Its objective is to generate blocks in a fair and random way without spending valuable resources, such as currencies, energy, or computing power [58]. The user with the shortest waiting time is the one who creates the new block and the system is responsible for verifying that the entry is legitimate. It is mainly used for private networks, where the user must obtain permission to access the network and obtain short wait times to create blocks [57].

### 5.2.5 Security in Blockchain

- **Hash Algorithm:** It is a cryptographic algorithm mainly used in the blockchain. It is mainly used for data integrities, encrypts information, performs proof of work, and joins blocks. Its function is to compress the information in a binary string with a certain length and time, having as output some values called hash. The transformation of information to a hash is a simple process, however, the reverse process is complex. So, the hash algorithm is unidirectional and collision-resistant. Among the most used algorithms are SHA256, SHA1, MD5 and SM3, the first and the last being the safest [19].
- **Asymmetric Encryption Algorithm** Refers to the use of private and public keys for encryption and decryption of information [61]. The public key is accessible to all users who use it to encrypt information addressed to a specific person. The private key is used to decrypt the message and is only known by the user who will receive and see the information. The most commonly used algorithms are Rivest-Shamir-Adleman (RSA), SM2 and elliptic curve cryptography (ECC) [19].

### 5.2.6 A Distributed Ledger

Ledger is the main part of a blockchain network because it records all the transactions that take place on the network, which has a decentralized system. Its function is to add information using encryption techniques such as SHA256, so that once it has been added, its content cannot be deleted or modified [9].

The system that allows us to work with an accounting book is Hyperledger Fabric. The ledger consists of two parts that are related to each other, the world state and the blockchain.

The first is a database that contains the information of the transactions with the current updated values. The database it uses is called Couch DB which allows transactions to be made thanks to its ACID features. The global state allows a program to directly access the information without the need to be making complex calculations throughout the transaction log to obtain the current value. This status is subject to constant changes since it can be created, updated and deleted at any time.

The second, the blockchain: records all the changes that have occurred over time resulting in the current world state. The transactions come from the blocks that are added

in the blockchain, which enables visualizing any change as if it was a browser history. Unlike the world state, the blockchain data structure cannot be modified, so the world state records still exist despite having been modified or deleted. [8]

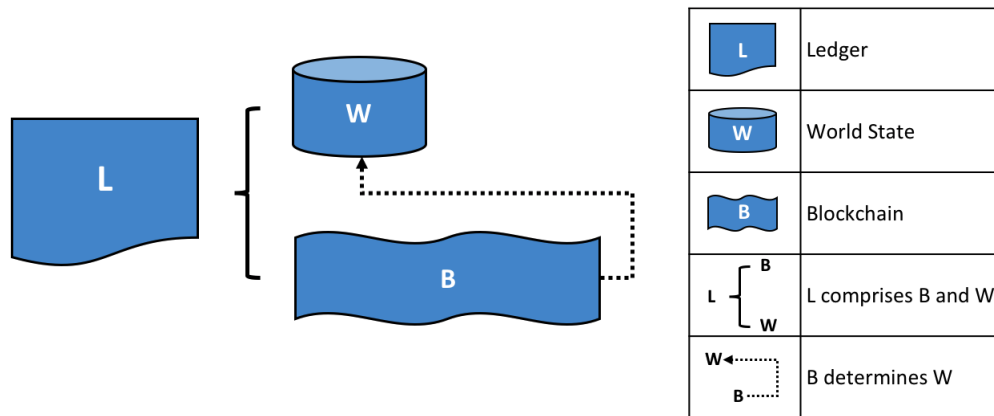


Figure 5.3: Ledger diagram. The ledger (L) comprises the blockchain (B) and the world state (W), where W is obtained by B [8]

### 5.2.7 Blockchain

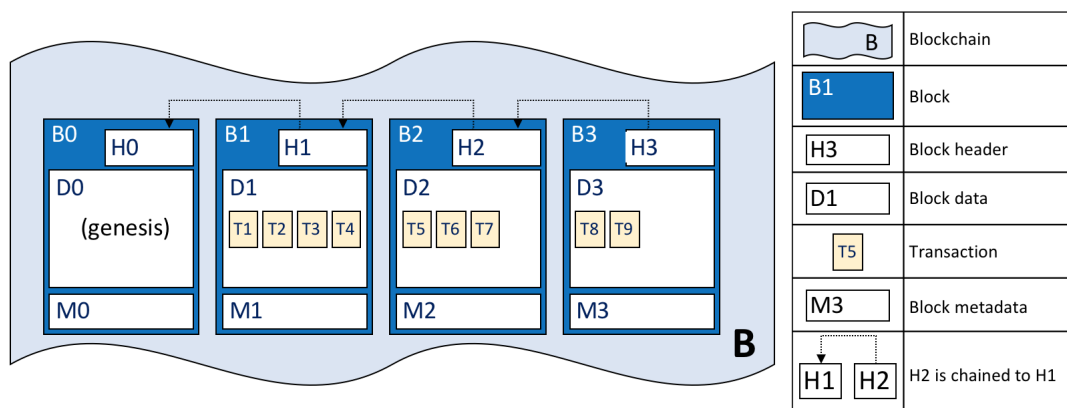


Figure 5.4: Blockchain with four blocks and their parts [8]

The blockchain is structured as a sequence of records that interconnect blocks, which contain a series of transactions each, and where each transaction represents a query or an update of the world state.

As we can see in Figure 5.4, the blockchain is divided into blocks (B0, B1 ...) and in turn, in other parts that make transactions possible. Each block has a header (H0, H1 ...) that includes a hash of the transactions in the block, as well as the header of the previous block. In this way, a link is generated between blocks that link their information through a cryptographic method called Merkle Tree. The Merkle tree has a tree structure where each leaf node has a calculated hash of its data and where the non-leaf node has a hash of all its underlying child elements [23]. This method provides privacy and data integrity. Because a private sheet can be removed but the hash is intact, preserving its integrity [23].

Figure 5.4 shows a blockchain composed of 4 blocks, where the first block called Genesis, is the starting point of the ledger because it has the initial configuration of the network and does not contain transactions. The subsequent blocks contain blocks of data (D1, D2 ...) that have all the transactions made (B1, T2 ...), a section with the metadata of the file and the hash. All this combination makes possible the most notable feature of the blockchain, immutability [8].

### 5.2.8 Blocks

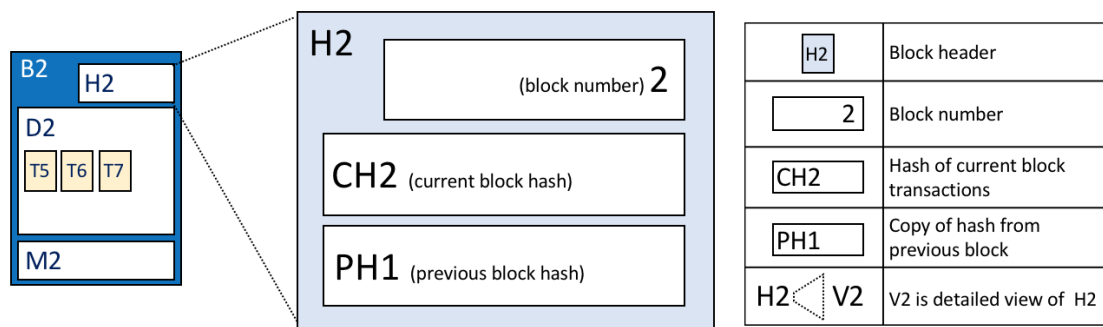


Figure 5.5: Block diagram [8]

Next, we will see in more detail the structure of the block found in Figure 5.5, which is divided into three sections [8].

- Block Header:** Contains 3 important fields that are written when the block is created. In Figure 5.5, it is represented in blue and named as B2.
  - Block number:** Start from 0 (Genesis block), and increase one by one as blocks are added. It is located within the H2 field, in the first box.
  - Hash of the current block:** Contains the hash of all transactions made within the current block. It is located within the H2 field, in the second box.

**Hash of the previous block:** Contains the hash of the previous block. This field allows you to link the neighboring blocks. It is located within the H2 field, in the third box.

- **Block Data:** This section saves all transactions made within the block in an orderly manner. The transaction is created when a change is made or new movements are added to the document.
- **Block Metadata:** This section stores the certificate and signature of the user who created the block, so that the block can be verified on any node in the network. The current field is not used to calculate the hash of the block.

### 5.2.9 Transactions

Transactions capture the changes that occur in the world state. In Figure 5.6, we see in more detail how transactions are structured, specifically transaction T4 [8].

T4 is divided into 5 subsections, where H4 is the header that captures some relevant transaction metadata. S4 is the cryptographic signature of the transaction, created by the application. In this way, it is verified that the transaction has not been altered since the private key is needed for the application to generate this signature. P4 encodes the input parameters by the application to the smart contract created by the proposed ledger, in this way, the combination of the contract with the current world state is able to determine the new world state. R4 captures the previous and subsequent values of the world state so that if it is validated successfully it is attached to the ledger to update the world state. E4 is an endorsement that contains a list of responses of the transactions signed by the required organizations, for approval validity.

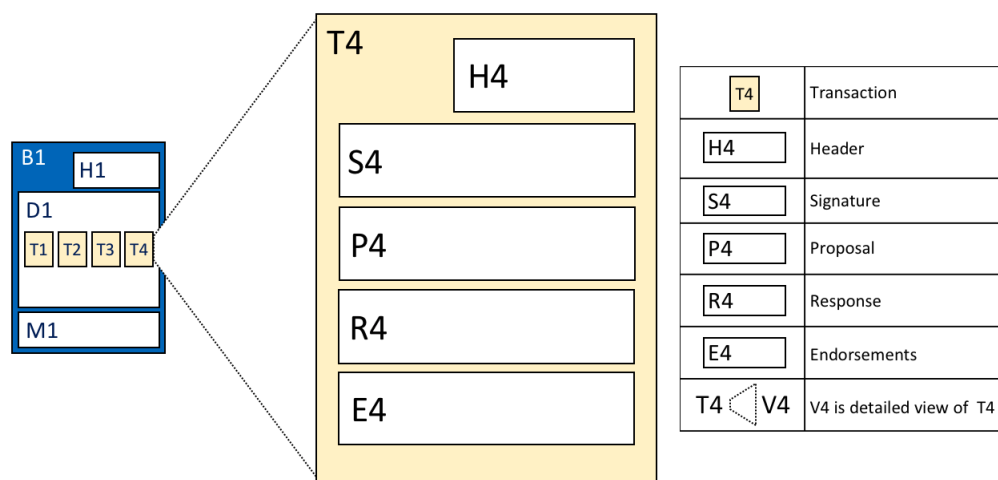


Figure 5.6: Transactions diagram [8]

### 5.2.10 Smart Contract

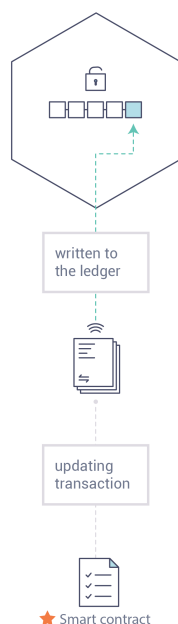


Figure 5.7: Smart Contract flow [9]

By not allowing modifications to the ledger, smart contracts are used to enable updates to the information content (see Figure 5.7), enabling various functions of the ledger such as transactions, queries, etc. In this way, it is possible to have a complete record of the modifications made, since although the information is updated, the traces of the alteration of the document are still present and they can be visualized. Smart contracts not only save all network information but are also capable of executing specific functions automatically when a certain event occurs during the transaction [9].

## 5.3 Hyperledger

In this thesis, Hyperledger is the blockchain platform used for the realization of the supply chain of the oil industry with the objective of optimizing processes related to the oil industry's headquarters. In this way, it is able to track the origin of the products and their materials, guaranteeing the authenticity of the final product, eliminating the falsifications and reducing data conflicts that arise when there are inconsistencies in the data.

Hyperledger is a platform launched in 2016 by The Linux Foundation, an open source created to advance blockchain technologies between industries [9].

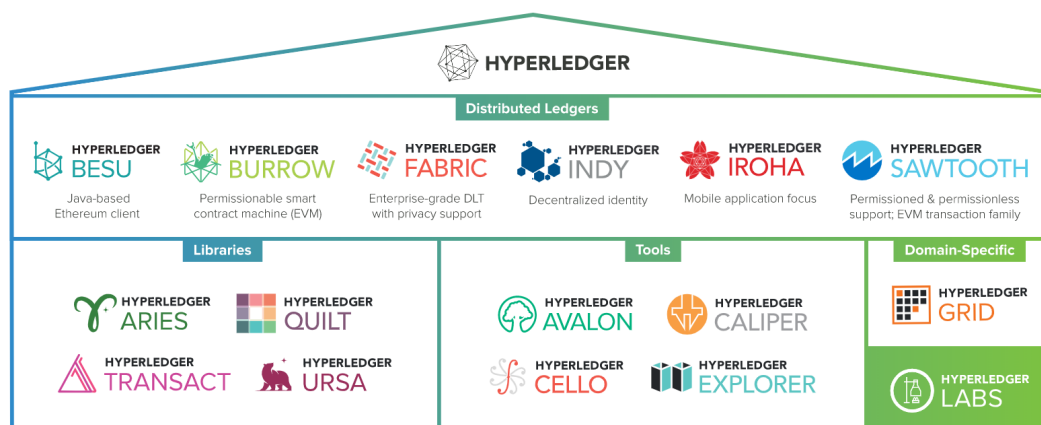


Figure 5.8: Business Blockchain Frameworks Tools Hosted by Hyperledger [9]

Hyperledger has a diverse range of distributed ledgers, tools, libraries, and domain specific tools that fit the needs of the company. The most important of Figure 5.8, are Hyperledger Fabric and Composer.

### 5.3.1 Hyperledger Fabric

The framework used to carry out this project is Hyperledger Fabric for its modular and configurable architecture. This tool is used by companies that require privacy in their business network.

Hyperledger Fabric is an authorized distributed accounting (DTL) platform specially designed for business networks that require privacy and confidentiality. This network is authorized so that to enter it, it requires permits from the network administrators, who also restrict what they may or may not do, and unlike public networks, participants know each other. This means that the network can operate under a governance model based on the trust that exists between the participants. With this feature, the platform manages to establish trust, transparency, and responsibility among the different actors in the network.

One of the problems that the public blockchain has without permission is the lack of confidentiality that exists within the network, where all participants have access to the same information, something that can be very problematic for companies and businesses since they need to perform different business strategies for each participant within the network. And if one participant is given more benefits than another, the latter will cause trouble to obtain the same advantages. This problem is solved by Hyperledger thanks to its architecture of channels, where the participants, in turn, establish a sub-net with restrictions between the different actors, in this way it is possible to restrict the distribution of information to authorized nodes. Therefore, only authorized nodes participating in this channel have access to the smart contract information and its transactions.

One of the most important points of the platform is its support for connectable consensus protocols since it makes it possible to configure which type of consensus algorithm will be used depending on the connectivity of the organization. This modular feature

enables increasing the performance in the systems since if Hyperledger Fabric is implemented within a single company, the Byzantine fault (BFT) algorithm can become inefficient, while for multiparty cases, it may be the most appropriate. So, Hyperledger allows network administrators to choose the consensus mechanism that best represents the relationships that exist between their participants.

Its modular and configurable architecture allows companies to innovate, be more versatile, and optimize their processes as the supply chain. In addition, it is the first DTL that supports smart contracts that can be programmed in common languages such as JavaScript, Java, Go and Node.js.[9]

The identity of the members of the Hyperledger network is registered through a reliable service provider (MSP) and managed by X509 certificates, which contains the private keys that the other members verify, using the associated public key, each time they make a transaction [62].

### 5.3.2 Hyperledger Fabric model

**Assets:** represent a value type that can be from something tangible to the intangible, but with the ability to exchange in the system, i.e., that can be represented digitally and can be modified. This asset representation can be in binary format or in JSON [63].

**Chaincode:** it is a software that defines the states of the assets and their transactions, that is, all the logic of the business network. Conceptually, the chaincode is known in other ledgers distributed as smart contracts [63]. Thanks to the chaincode, companies can automate business processes, giving greater efficiency to the network [62].

**Membership Service Provider (MSP):** It is a component that allows validating and authenticating a participant's access to the network, using an Authority (CA) certificate.

**Ledger:**All transactions are recorded in an encrypted and distributed ledger, where you can track and change the status of the assets[62]. The ledger consists of a blockchain that only has the option to insert data. In such a way that it stores all the transactions sequentially, allowing to consult and write data in the distributed accounting books. Immutability occurs because the data cannot be altered, however, the world state can be updated, which is registered in the Couch DB database. This update is carried out when another valid transaction modifies the previous information. All these transactions are recorded in the history for their immutability [23]. In Hyperledger each channel has a ledger and each participant has a copy of the record of the channel to which it belongs [63].

**Nodes:** Nodes are the communication entities of the blockchain that form a network when connected to each other. This connection is possible thanks to the peer-to-peer protocol that allows them to keep the distributed ledger synchronized at the same time throughout the network [62]. Nodes need valid certificates to communicate with the network, that is, they use it to check if the node is secure or not. In this way, if a participant's certificate is valid but the node certificate is not, the transaction is transmitted on the network but will be rejected because the node is not valid. In hyperledger, unlike other

public blockchain technologies, it has different types of nodes, which are [11]:

- **Client:** This node uses applications to invoke transactions to endorsers and disseminates it to order services.
- **Peers:** Help keep the ledger synchronized throughout the network. Since it confirms the transactions and maintains a copy of the ledger and its current status. There are two types of peers:

**Endorsers:** simulate and certify proposed transactions.

**Committers:** verify transaction proposals and validate the result of transactions before implementing them in the blockchain.

- **Orderers:** They are responsible for the distribution of transactions

**Channels:** Channels allow you to restrict the information that is distributed among organizations. A chaincode created within a channel, only has visibility within that channel. Members can create and participate in multiple channels by deciding who can validate them and what type of policies they can use for validation.

In conclusion, members can participate in multiple networks, peer nodes connect to channels and receive transactions, and channels have their own ledger that allows them to transmit information privately [62].

**Status Database:** Fabric stores the current status in a database that can be recreated at any time from the chain of transactions stored in the blockchain. It is an efficient way to access the state of the registry (world state) through CouchDB that stores JSON objects and presents a very powerful interface. CouchDB provides a semantics of atomicity, consistency, isolation and durability.[23]

### 5.3.3 Hyperledger Fabric Component Design

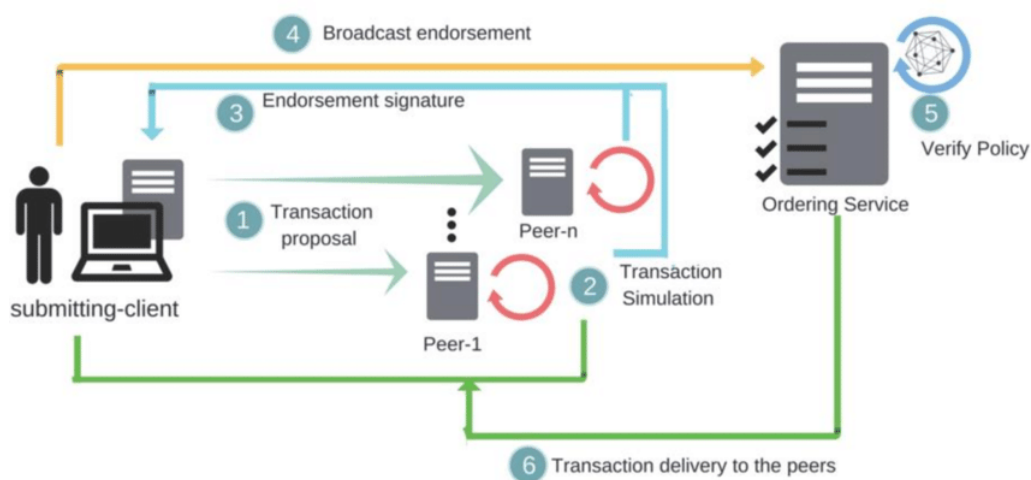


Figure 5.9: Hyperledger Fabric Flow [9]



As we can see in the figure 5.9, the transaction begins with a Client application that sends a transaction proposal to a series of peers called Endorsers.

Once the transaction proposal has been received in each of the endorsers, they simulate the transaction with the current status of the registry without making any changes to it. A package called RW set is generated and returned to the customer after being signed by the endorser.

The client application sends the signed transaction and the package to the Ordering Service that all the participants in the network have. It blocks all transactions in an orderly manner and then be sent to all Committers.

The Committers check whether the RW validity of the package to change the status of the record. Regardless of whether it is valid or not, it is included in the block. But if it is valid, it will be marked as valid and will modify the status of the record, otherwise, it will be marked as invalid and does not modify the record.

Finally, the Committers inform the client application of whether the transaction has been executed successfully or not. [9]

### 5.3.4 Hyperledger Composer

Hyperledger Composer is an open-source tool whose objective is to simplify the development of Hyperledger blockchain applications with existing commercial systems [12].

Its system enables the reduction of the complexity of putting together an underlying structure, so it is possible to quickly develop use cases in just a few weeks, unlike the months it may take to implement a system on another platform. Composer supports the infrastructure and runtime of the Hyperledger Fabric blockchain. Therefore, it is used to quickly model a commercial network, which contains its participants, assets, and transactions related to the network [12].

This tool is made up of a modeling language called CTO, a command-line interface (CLI), and a user interface called Hyperledger Composer Playground, which allows you to model and test the network in an online or local environment.[12]

# Chapter 6

## Related Works

In this section, 3 papers on the subject of this research are analyzed. They are implementing blockchain technology in the oil industry and in other industries. It is advisable to review these articles in more depth to understand their purpose since many of the terms used below have not been explained in the previous sections, so we will try to summarize them.

### 6.1 Hongfang Lu et Al. (2019)

This article is one of the first to deepen the review of the blockchain system in the oil and gas industry [19]. Its objective is that the people of this industry understand what the blockchain is, so that they can undertake new projects applied to the oil industry. The document first presents the basic concepts of the blockchain, its main characteristics, the types of systems, the consensus algorithms that exist, and the security and encryption technologies that they have. He then describes how this system is applied to the oil industry from four aspects: trading, management and decision making, supervision, and cybersecurity. Here, we talk about smart contracts, transactions, how the industry is divided into sectors, and how the business part is structured. Finally, the status of the application is mentioned, the levels of understanding of what the blockchain is in the industry, the opportunities, challenges, risks, and development trends that exist. With this brief study, they conclude that the main developers of this technology are in Europe and Asia, however, due to the little compression that exists on this technology, it is still experimental and with little investment.

### 6.2 ECOSC (2019)

The delay times and the risks of not paying in the oil industry have led to the need to create efficient systems capable of managing supplies and demand in the oil industry, one of them is the company ECOSC [20]. This article describes a system developed by ECOSC that aims to improve the efficiency of the supply chain in the oil industry. With the aim of having a supply chain in which the order data can be viewed in real

time and connected to the different departments, managed by engineers, analysts, and laboratories. In this way, they are able to improve the commercial transaction system by allowing small and large companies within the industry to communicate, without the need for intermediaries or unnecessary and delaying procedures. In turn, it provides fully verifiable and audited assets in real time to ensure stability, value, and security. The document begins by talking about the 3 sectors of the industry: upstream, midstream and downstream. It continues with the problems that the industry covers, the challenges and the improvements that the implementation of the ECOSC system will bring. In another section, they go into more detail with the market analysis of the supply chain and then comment on the problems solved by the ECOSC system, such as data accessibility and transparency to reduce time and avoid the risk of default. Also, the technical part of the web platform is reviewed, where you can find certifications, orders, and management processes, share and upload documents, inspect documents, help communication between companies in the same and different sectors, and more. The structure of the blockchain software is detailed and an example of the part of a smart contract and its architecture is given. Finally, we analyze a business model applicable to the industry with the blockchain with its strategies, competitors, and risk factors.

### **6.3 Enbo Chen (2016)**

The problems of security and reliability caused in the supply chain of the industries led Enbo Chen [64] to prepare a study based on blockchain technology that allows to improve transparency and traceability in a safe and profitable way. To achieve this objective, a study was carried out on the operation of blockchain technology, the network topology, its implementation, and the tools that allow the blockchain to be implemented in the supply chain, in such a way that it is able to synchronize and verify Real-time transactions. With the elaboration of a model of the supply chain and another of the blockchain, it is possible to implement a concrete solution to shape a supply chain in the telephone industry. This solution elaborated with the Hyperledger open-source platform manages to track the origin of the assets in real-time through a complex supply chain.

# Chapter 7

## Methodology

In this section, the reader is given a clear idea about the procedures to follow in order to obtain the application objectives set out in section 3. It will explain the hardware and software features that a computer must have in order for the program to function properly, Similarly, the tools used to code the blockchain system will be detailed.

Finally, the theoretical architecture of the blockchain and Hyperledger will be analyzed explaining the selected parameters.

### 7.1 Blockchain Type Choice

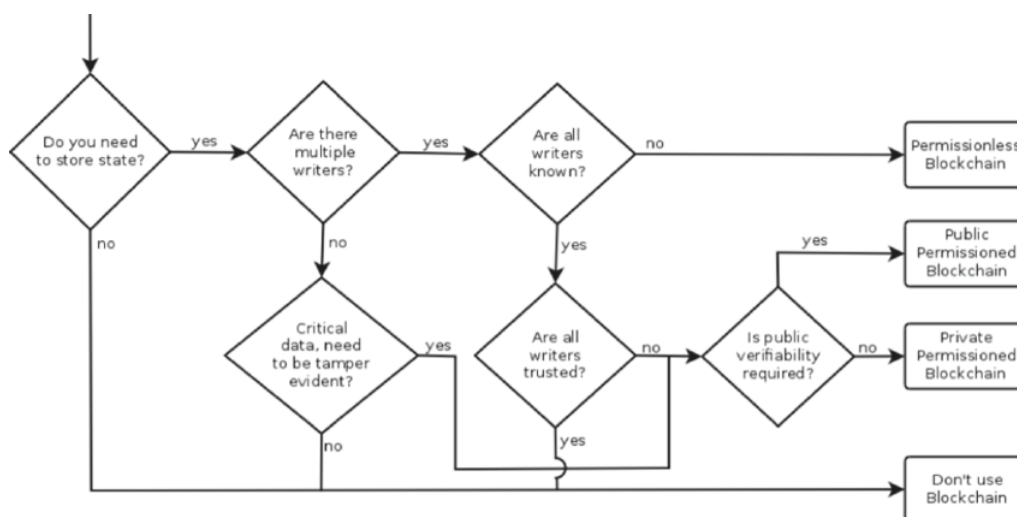


Figure 7.1: Do you need a blockchain?. Retrieved from H. Narumanchi (2018) [10]

Section 5.2.1 showed the 3 different options we have to implement a blockchain depending on the type of network that is needed. With the help of Figure 7.1, we will obtain the most appropriate network for the realization of this project, answering a few simple questions.

Considering the requirements of the supply chain in the oil industry, it was obtained that the one that best suits the problems is the private network. Because a database

is needed to know the real state of the information, several companies require to write permissions to modify, it must be verified so that third parties are trusted, and it does not require a public verification.

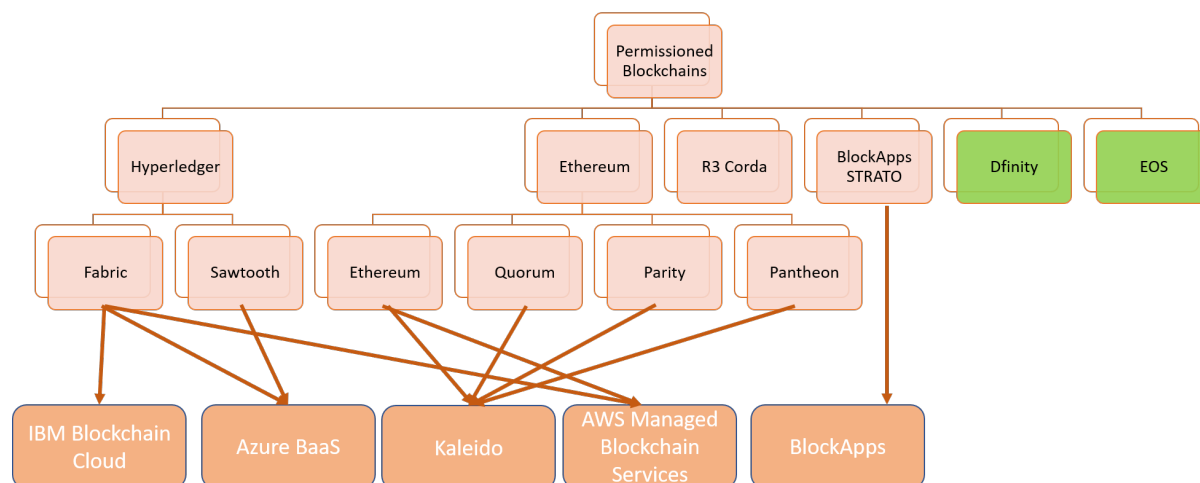


Figure 7.2: Permissioned Blockchain Applications Retrieved from J.Rodriguez (2018) [11]

Once the type of network to be used is obtained, it is necessary to look for the platform with which it will work (see Figure 7.2). In this case, there are multiple open and private open-source platforms such as Hyperledger, Ethereum, Corda, Strato, Dfinity, EOS, Multichain, Openchain, among others. With the chosen platform, the runtime to be used must be selected, that is, the central infrastructure that the platform will use, the best known are Fabric, Sawtooth, Ethereum, Quorum, Parity, and pantheon. Finally, a development tool such as IBM Blockchain Cloud, Azure BaaS, Kaleido, AWS Managed Blockchain Services for network administration and BlockApps is chosen to create DApps, decentralized applications [11].

## 7.2 Supply Chain Model

The current process of the supply chain of the oil company Petroamazonas EP. It is very complex and departments of various sectors of the industry are interconnected, which makes it a very long and tedious model. However, the objective of this project is to demonstrate how the blockchain generally applied to a part of the supply chain works, specifically for the supply of gasoline.

Figure 7.3 shows a simple and illustrative model to understand how the blockchain works in the gasoline supply chain. This model has a horizontal and vertical structure,

which can have several tiers. The horizontal layer refers to the different processes that occur in the supply chain. The vertical layer refers to the different entities that can participate in each process of the horizontal layer [64].

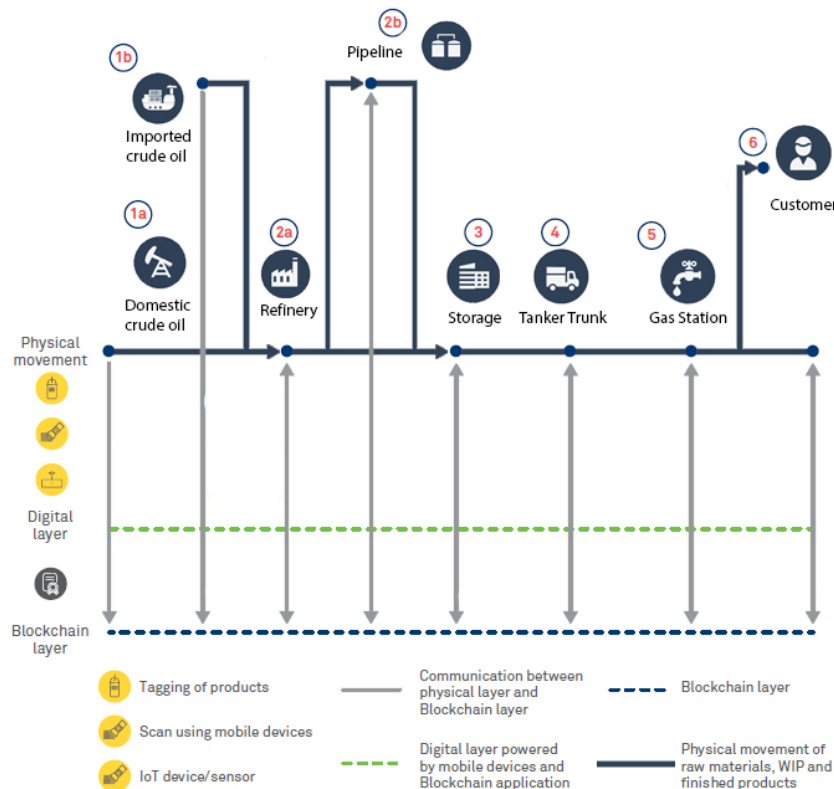


Figure 7.3: Supply Chain Model in Oil Industry

The designated roles in the horizontal layers are 6, where the first and the second are divided into two vertical levels. The first process we find refers to obtaining crude oil, which can be imported (1b) or extracted from its platforms (1a). The second process is the refinement (2a) of crude oil and the distribution of the product through pipelines (2b) or directly to the warehouse, which is the third step. Once stored (3), gasoline (4) is transported to gas stations (5) for later sale to consumers (6). All these processes are physical movements that are carried out in the supply chain, however, within each of these processes other parallel processes must be carried out for the digitalization of the information within the system's blockchain. To keep the system with accurate information, it is required that the products in each of the processes, be labeled and scanned by mobile devices and preferably that have smart devices to control the merchandise. In this way, all the digitalized information is obtained (Digital layer) and finally, it is integrated into the blockchain, having an immutable and transparent record in the whole process of the supply chain.

### 7.3 Platforms and Tools

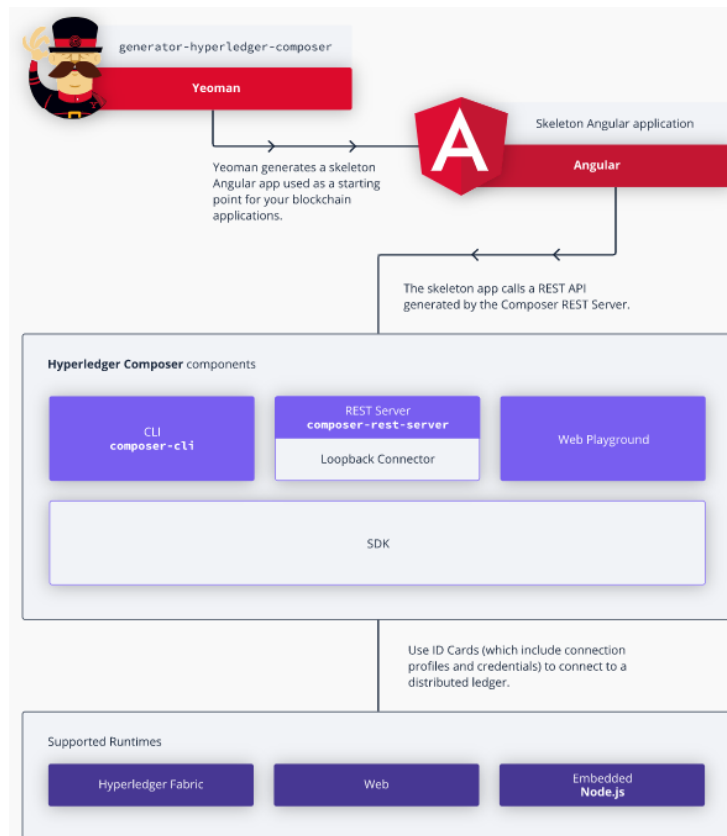


Figure 7.4: Typical Hyperledger Composer Solution Architecture. Retrieved from Hyperledger Composer [12]

Currently, there are several platforms and development tools for creating applications that implement the blockchain. In view of the model to be developed and the options outlined in the previous section, it is recommended to work with IBM Blockchain for its capacity for business-level growth. However, for the present investigation, it was decided to work with open source tools that allow developing any type of project that requires privacy and offers the characteristics of blockchain technology, see Figure 7.4. The framework that contains the blockchain is Hyperledger Fabric, which allows one to configure different data security and visibility options between different companies within the supply chain, and to obtain the confirmation of up to 100,000 transactions per second. The development tool that creates business networks is Hyperledger Composer, which allows us to connect the back-end with the front-end via REST API. Once the communication between both parties is established, thanks to the information sent by the API, applications of any business nature can be developed, in our case, a web application is developed with the Angular programming language with the help of Yeoman that generates the skeleton of the application.

### 7.3.1 Prerequisites

When opting for the tools offered by Hyperledger for the implementation of the blockchain in the supply chain of the oil industry, we need to meet certain hardware and software requirements in order to execute our project locally on our computer. [12]

- RAM memory: 4 Gb
- Operating Systems: Ubuntu Linux 18.04 LTS (64-bit), or Mac OS 10.12
- Docker Engine: Version 17.03 or higher
- Docker-Compose: Version 1.8 or higher
- Node: 8.9.0
- npm: v5.0
- git: 2.9.x or higher
- Python: 2.7.x
- A code editor such as Visual Studio Code

### 7.3.2 Visual Studio Code (VS Code)

Visual Studio Code is a free and open-source software that enables editing and executing code. It includes tools to debug, personalize and install extensions to expand its functionalities. It was created by Microsoft for various operating systems such as Windows, Linux, and Mac OS [65].

According to IBM (2019), with Blockchain, VSCode extension helps developers create, test, and debug smart contracts, connect to Hyperledger Fabric environments, and build applications that transact on your blockchain network.” [66]

## 7.4 Development environment topology

The development environment is divided into 4 fundamental parts, managed by a container called Docker. The first part is the certification authority, that is responsible for providing the credentials to the participants and nodes of the network. The second one is the orderer, that is responsible for distributing itself. The third one is the peer that confirms the transactions. And finally, Couch DB is used for status data.



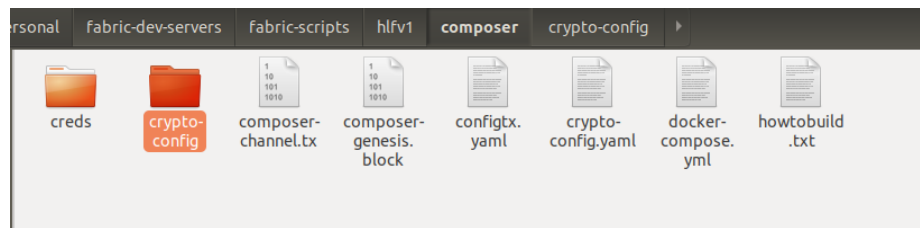


Figure 7.5: Development environment *fabric-dev-servers*

This configuration is managed within the “*fabric-dev-servers*” folder which is created once Hyperledger Fabric is installed (see the next section). In the *composer* folder of the created network is contained the material that has the configuration files of the network, the channel, and the genesis block (see Figure 7.5). The cryptographic material to grant the certificates is located in the *cryptp-config* folder.

```

docker-compose.yml x
home > angel > fabric-dev-servers > fabric-scripts > hlfv1 > composer > docker-compose.yml
 1  version: '2'
 2
 3  services:
 4    ca.org1.example.com:
 5      image: hyperledger/fabric-ca:$ARCH-1.0.4
 6      environment: --
 9      # - FABRIC_CA_SERVER_CA_CERTFILE=/etc/hyperledger/fabric-ca-server-config/org1.example
10      # - FABRIC_CA_SERVER_CA_KEYFILE=/etc/hyperledger/fabric-ca-server-config/a22daf356b2aa
11
12     ports: --
14     command: sh -c 'fabric-ca-server start --ca.certfile /etc/hyperledger/fabric-ca-server-
15     volumes: --
17     container_name: ca.org1.example.com
18
19     orderer.example.com:
20     container_name: orderer.example.com
21     image: hyperledger/fabric-orderer:$ARCH-1.0.4
22     environment: --
29     working_dir: /opt/gopath/src/github.com/hyperledger/fabric
30     command: orderer
31     ports: --
33     volumes: --
36
37     peer0.org1.example.com:
38     container_name: peer0.org1.example.com
39     image: hyperledger/fabric-peer:$ARCH-1.0.4
40     environment: --
51     working_dir: /opt/gopath/src/github.com/hyperledger/fabric
52     command: peer node start --peer-defaultchain=false
53     ports: --
56     volumes: --
61     depends_on: --
64
65     couchdb:
66     container_name: couchdb
67     image: hyperledger/fabric-couchdb:$ARCH-1.0.4
68     ports: --
70     environment: --
72
73

```

Figure 7.6: docker-compose.yml file

Within the file “*docker-compose.yml*” on lines 4, 19, 37 and 65 of the figure 7.6 are defined: the certificate of authority, the orderer, the peer and the Couch DB, which take place within the network called *hlfv1*.

## 7.5 Installing the development environment

The gasoline supply chain demo can be developed and implemented online in hyperledger Composer Online Playground in <http://composer-playground.mybluemix.net>. However, the demo of this thesis is going to be done locally to be able to build a web application made in Angular.

To install the Hyperledger Composer development environment, we must install its components: `composer-cli`, `generator-hyperledger-composer`, `composer-rest-server`, and Yeoman. Hyperledger Fabric and Playground must also be installed. The commands to install these programs can be found on the Hyperledger Composer page.

Once the prerequisites and the development environment with Hyperledger and its components are installed, we begin with the execution of the Docker with the following commands `./startFabric.sh`, `./createPeerAdminCard.sh` and `composer-playground`, which will automatically open in the browser the address `http://localhost: 8080/` that we see in Figure 7.7, where Hyperledger Composer Playground is hosted.

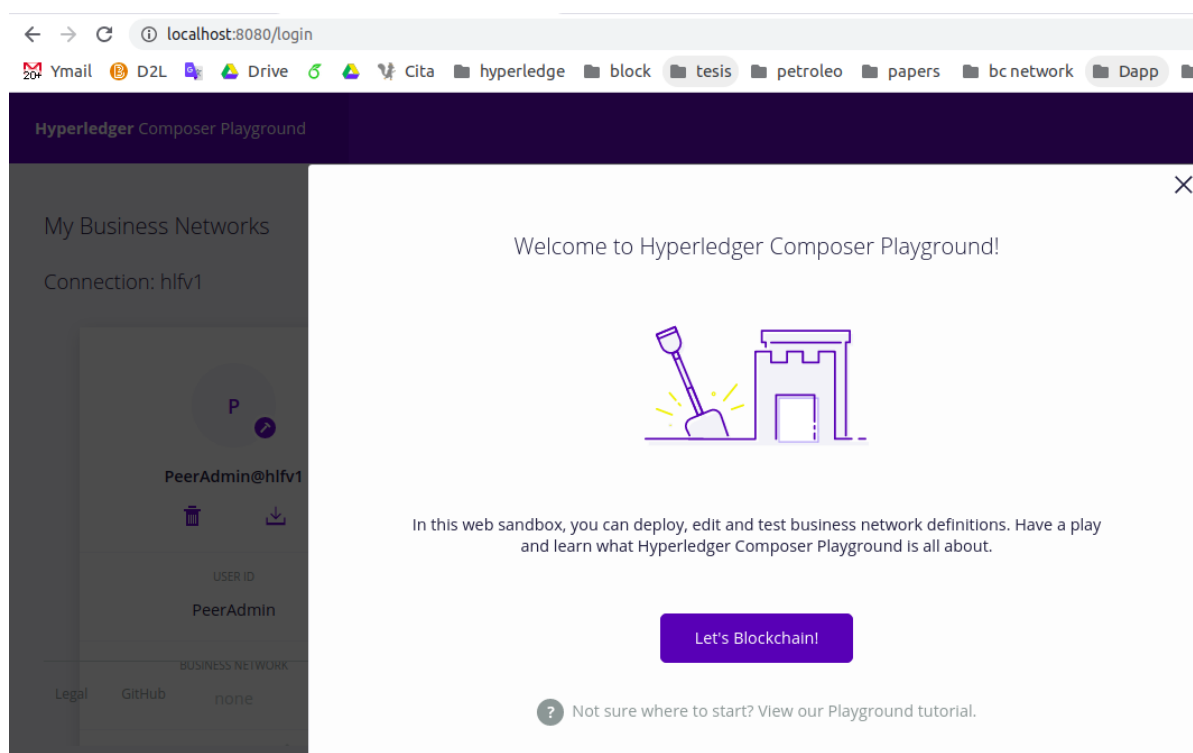


Figure 7.7: Hyperledger Composer Playground in localhost

Once the Hyperledger platform is executed, the next step is to create the document

structure of what will be the web application with Yeoman, from the terminal with the following command: “*yo hyperledger-composer*”.

This command generates a series of questions that must be answered to generate the skeleton. The questions in Figure 7.8 allow you to name the network that is being created and enter the author’s data, and generate the necessary documents to configure the network.

```
angel@angel-HP-Pavilion-g6-Notebook-PC:~$ yo hyperledger-composer
Welcome to the Hyperledger Composer project generator
? Please select the type of project: Business Network
You can run this generator using: 'yo hyperledger-composer:businessnetwork'
Welcome to the business network generator
? Business network name: blockoilchain
? Description: Blockchain application for the supply chain of the ecuadorian oil
  industry
? Author name: Ángel Villacreses
? Author email: angel.villacreses@yachaytech.edu.ec
? License: Apache-2.0
? Namespace: model
? Do you want to generate an empty template network? No: generate a populated sa
mple network
  create package.json
  create README.md
  create models/model.cto
  create permissions.acl
  create .eslintrc.yml
  create features/sample.feature
  create features/support/index.js
  create test/logic.js
  create lib/logic.js
angel@angel-HP-Pavilion-g6-Notebook-PC:~$
```

Figure 7.8: generate project skeleton

### 7.5.1 Application Modeling

At this point, the domain model in the business network must be defined through a very simple object-oriented language, where participants, assets, transactions, and events that will take place within the network are defined. Models are defined in files with a *.cto* extension. Figure 7.9 first shows the declaration of the *namespace*, by which the network is recognized. In this example, it is a simple model to test the operation of the blockchain in the supply chain, the network is defined in a single model. The model defines 5 participants that make up the network.

```

23 }
24 abstract participant SPParticipant identified by id {
25   o String id
26   o String name
27   o Address address
28 }
29
30 participant Supplier extends SPParticipant {
31   o SupplierType supplierType
32 }
33
34 participant Manufacturer extends SPParticipant {
35   o ProductTypeEnum productType
36   --> ProductRaw[] rawStorage
37   --> Product[] productStorage
38 }
39
40 participant Distributor extends SPParticipant {
41   o ProductTypeEnum[] productType
42   --> Product[] productStorage
43 }
44
45 participant Retailer extends SPParticipant{
46   o ProductTypeEnum[] productType
47   --> Product[] productStorage
48 }
49 }
50
51 participant Customer extends SPParticipant{
52   o ProductTypeEnum[] productType
53   --> Product[] productStorage
54 }
55 }

```

Figure 7.9: Participant in model file

```

98 transaction CreateRawTransaction {
99   o ProductRawType rawType
100   -->Supplier atStage
101 }
102 transaction TransferRawTransaction {
103   --> ProductRaw productRaw
104   --> Supplier supplier
105   --> Manufacturer manufacturer
106 }
107 transaction CreateProductTransaction {
108   --> Manufacturer manufacturer
109 }
110 transaction TransferProductTransactionMD {
111   --> Product product
112   --> Manufacturer manufacturer
113   --> Distributor distributor
114 }
115 transaction TransferProductTransactionDR {
116   --> Product product
117   --> Distributor distributor
118   --> Retailer retailer
119 }
120 transaction SellProductTransactionRC {
121   --> Product product
122   --> Retailer retailer
123   --> Customer customer
124 }
125 }

```

Figure 7.10: Transaction in model file

The first is the Supplier, who is able to provide two types of *assets* (*oil and crude gas*). The second participant is the *manufacturer*, who is responsible for converting the crude product into a final product, in this case, *gasoline, diesel, and gas*. The third participant

is the *distributor*, who is responsible for selling in order to distribute the product. In Figure ??, the asset of the *raw product* and the final *product* is created.

The operations that can be performed to change the status of the assets are shown in Figure 7.10. The supplier with the “*CreateRawTransaction*” function can incorporate the raw materials it has into the system, and then transfer them to the manufacturer with the “*TransferRawTransaction*” function. At this time, the manufacturer is able to convert the raw material into a product with the “*CreateProductTransaction*” function and then transfer to the distributor with the “*TransferProductTransaction*” function so that it can sell it with “*SellProductTransaction*”. These transactions generate an ID and a timestamp each time they are executed, incorporating them into the ledger so that any movement in the network is recorded. With the events in Figure 7.11, we can see if the transactions were carried out successfully, since they notify us when the aforementioned transactions have been made correctly, in addition, that a timestamp is inserted at the time it occurs.

```

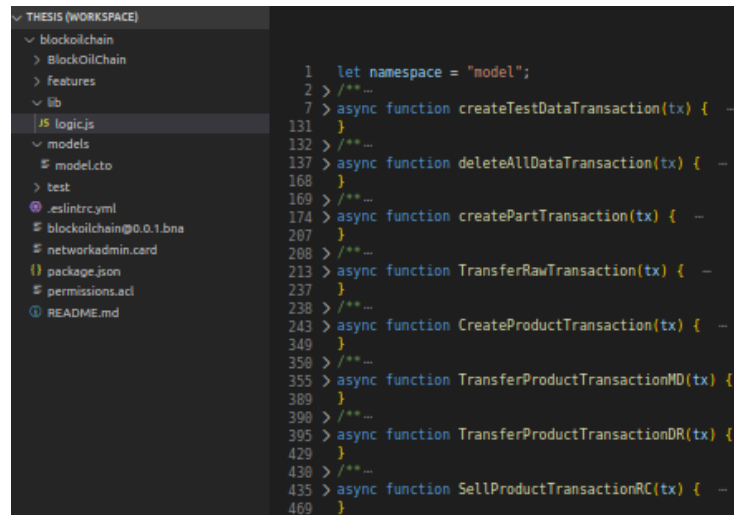
130
131 event ProductRawCreated {
132   --> ProductRaw productRaw
133   --> Supplier supplier
134   o DateTime date
135 }
136 event ProductRawTransferred {
137   --> ProductRaw productRaw
138   --> Supplier from
139   --> Manufacturer to
140   o DateTime date
141 }
142 event ProductCreated {
143   --> Product product
144   --> Manufacturer at
145   o DateTime date
146 }
147 event ProductTransportedMD {
148   --> Product product
149   --> Manufacturer from
150   --> Distributor to
151   o DateTime date
152 }
153 event ProductTransportedDR {
154   --> Product product
155   --> Distributor from
156   --> Retailer to
157   o DateTime date
158 }
159 event ProductSoldRC {
160   --> Product product
161   --> Retailer retailer
162   o DateTime date
163 }
164
165

```

Figure 7.11: Events in model file

For the modeling to be successful, a file in javascript format must be included, which is located in the lib folder of the project, in the file in Figure 7.12, all transactions and events of the model are defined. Within each function, the operations between the participants will be carried out so that the asset changes status depending on the transaction to be carried out. Figure 7.13 shows the programming of the sales function, which is divided into three operations. The first one updates the status of the product that the distributor has to “*sold*” The second removes the product stored from the distributor. And the third

party issues the event that the product has been successfully sold by assigning an *Idevent* and a *timestamp*.

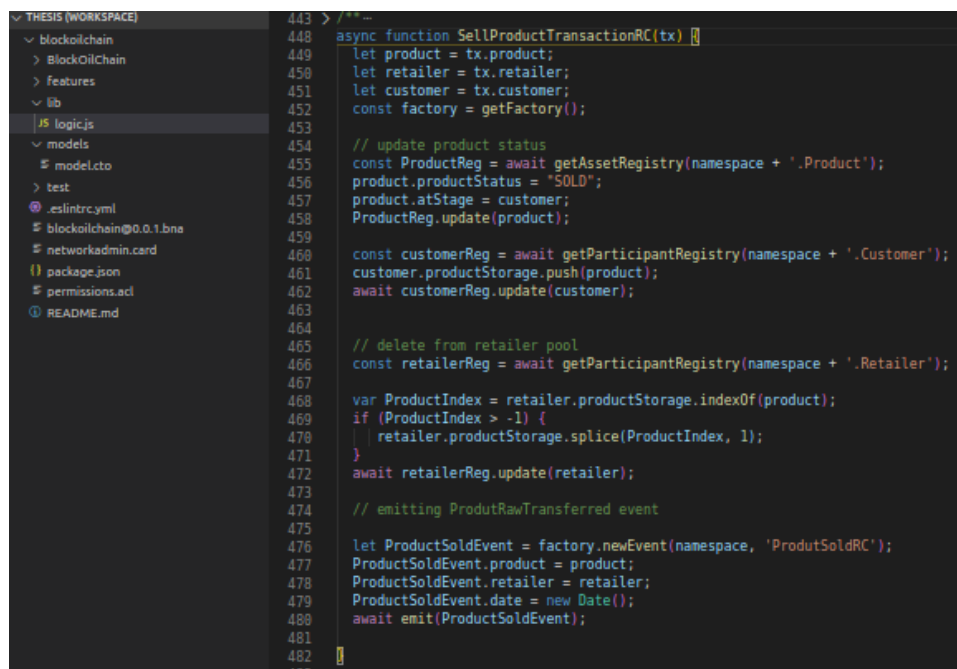


```

1 let namespace = "model";
2 > /**--
7 > async function createTestDataTransaction(tx) { --
131 }
132 > /**--
137 > async function deleteAllDataTransaction(tx) { --
168 }
169 > /**--
174 > async function createPartTransaction(tx) { --
207 }
208 > /**--
213 > async function TransferRawTransaction(tx) { --
237 }
238 > /**--
243 > async function CreateProductTransaction(tx) { --
349 }
350 > /**--
355 > async function TransferProductTransactionMD(tx) {
389 }
390 > /**--
395 > async function TransferProductTransactionDR(tx) {
429 }
430 > /**--
435 > async function SellProductTransactionRC(tx) { --
469 }

```

Figure 7.12: Transactions and events of the model are defined



```

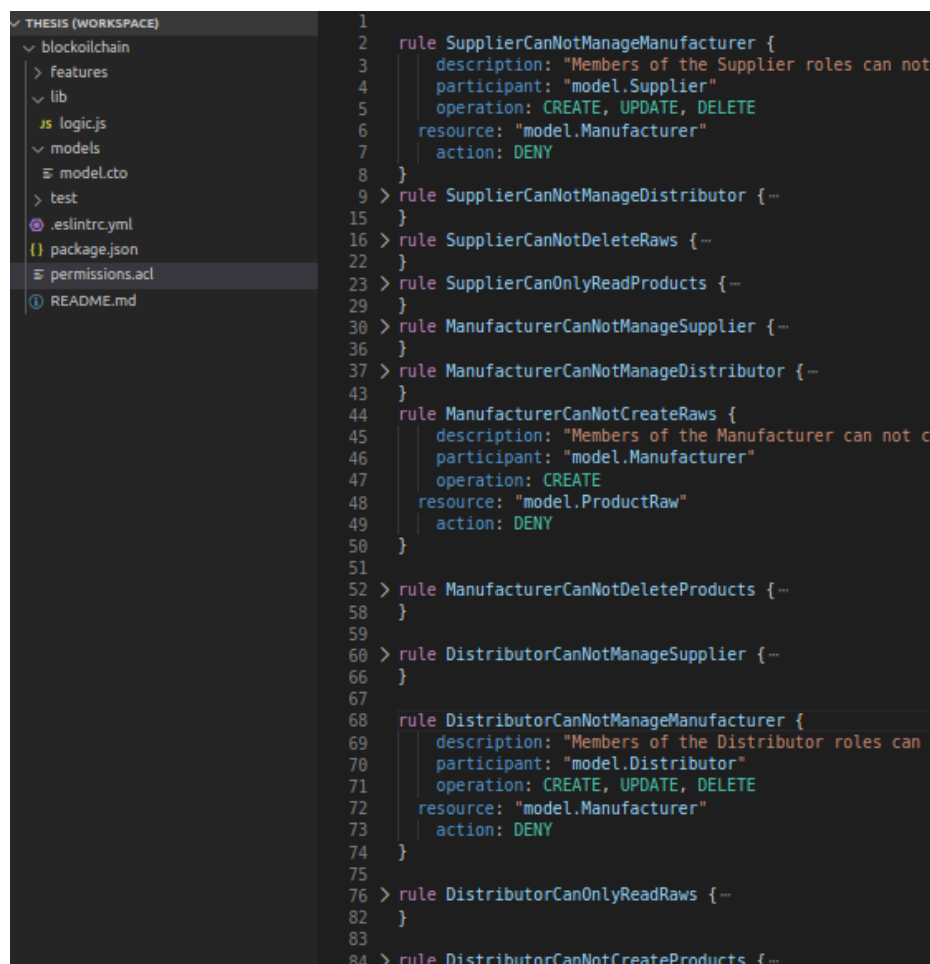
443 > /**--
448 async function SellProductTransactionRC(tx) {
449   let product = tx.product;
450   let retailer = tx.retailer;
451   let customer = tx.customer;
452   const factory = getFactory();
453
454   // update product status
455   const ProductReg = await getAssetRegistry(namespace + '.Product');
456   product.productStatus = "SOLD";
457   product.atStage = customer;
458   ProductReg.update(product);
459
460   const customerReg = await getParticipantRegistry(namespace + '.Customer');
461   customer.productStorage.push(product);
462   await customerReg.update(customer);
463
464
465   // delete from retailer pool
466   const retailerReg = await getParticipantRegistry(namespace + '.Retailer');
467
468   var ProductIndex = retailer.productStorage.indexOf(product);
469   if (ProductIndex > -1) {
470     retailer.productStorage.splice(ProductIndex, 1);
471   }
472   await retailerReg.update(retailer);
473
474   // emitting ProductRawTransferred event
475
476   let ProductSoldEvent = factory.newEvent(namespace, 'ProductSoldRC');
477   ProductSoldEvent.product = product;
478   ProductSoldEvent.retailer = retailer;
479   ProductSoldEvent.date = new Date();
480   await emit(ProductSoldEvent);
481
482 }

```

Figure 7.13: Transactions and events of the model are programmed

Another very important part of this model is the administration of identities. Where the validity of the certificate is checked with the validation authority. In the file *permissions.acl*, some rules of composer access control are established that each participant has within the network. In our case, 4 rules were created for each participant where,

depending on the situation, they are limited to making one transaction or another. In Figure 7.14, the first and second rules do not allow the supplier to manage participants from the manufacturer or the distributor. The third does not allow one to eliminate raw products and the fourth allows one to see the products that are available. These same procedures apply to the rest of the participants.



```

1
2 rule SupplierCanNotManageManufacturer {
3 | description: "Members of the Supplier roles can not
4 | participant: "model.Supplier"
5 | operation: CREATE, UPDATE, DELETE
6 | resource: "model.Manufacturer"
7 | action: DENY
8 }
9 > rule SupplierCanNotManageDistributor {--
15 }
16 > rule SupplierCanNotDeleteRaws {--
22 }
23 > rule SupplierCanOnlyReadProducts {--
29 }
30 > rule ManufacturerCanNotManageSupplier {--
36 }
37 > rule ManufacturerCanNotManageDistributor {--
43 }
44 rule ManufacturerCanNotCreateRaws {
45 | description: "Members of the Manufacturer can not c
46 | participant: "model.Manufacturer"
47 | operation: CREATE
48 | resource: "model.ProductRaw"
49 | action: DENY
50 }
51
52 > rule ManufacturerCanNotDeleteProducts {--
58 }
59
60 > rule DistributorCanNotManageSupplier {--
66 }
67
68 rule DistributorCanNotManageManufacturer {
69 | description: "Members of the Distributor roles can
70 | participant: "model.Distributor"
71 | operation: CREATE, UPDATE, DELETE
72 | resource: "model.Manufacturer"
73 | action: DENY
74 }
75
76 > rule DistributorCanOnlyReadRaws {--
82 }
83
84 > rule DistributorCanNotCreateProducts {--

```

Figure 7.14: Rules of composer access control

## 7.5.2 Create and implement the business network file (BNA)

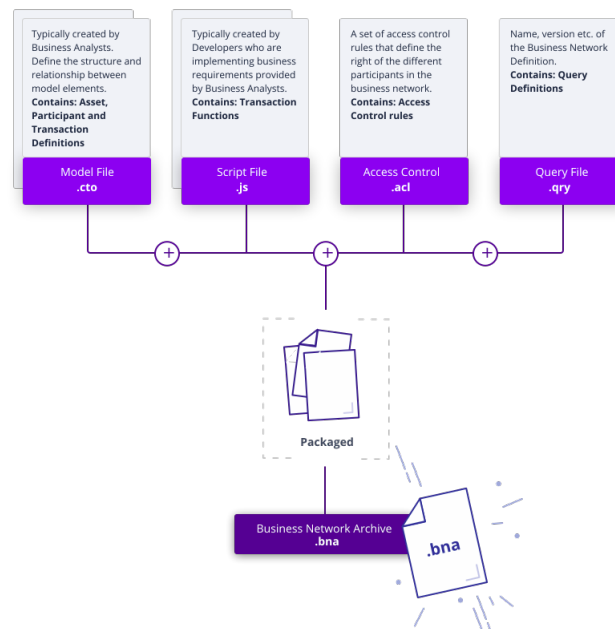


Figure 7.15: business network file (BNA). Retrieved from Hyperledger [12]

The business network file is a package (see Figure 7.15), that contains all the network model files, that is, it contains the model file, the script and the access control file. To create this file, we must open the terminal in the project location and write the following command in Figure 7.16, “*composer archive create -t dir -n .*” The result is the creation of a file called *blockoilchain@0.0.1.bna* located in the directory of the business network.

```
angel@angel-HP-Pavilion-g6-Notebook-PC:~/blockoilchain$ composer archive create
-t dir -n .
Creating Business Network Archive

Looking for package.json of Business Network Definition
Input directory: /home/angel/blockoilchain

Found:
  Description: Blockchain application for the supply chain of the ecuadori
an oil industry
  Name: blockoilchain
  Identifier: blockoilchain@0.0.1

Written Business Network Definition Archive file to
Output file: blockoilchain@0.0.1.bna

Command succeeded
```

Figure 7.16: Create BNA file

The next step is to install the Hyperledger Fabric network BNA file, where the network



must be installed in the peers. This procedure is performed with the following command “*composer network install --card PeerAdmin@hlfv1 --archiveFile blockoilchain@0.0.1.bna*” (see Figure 7.17).

```
angel@angel-HP-Pavilion-g6-Notebook-PC:~/blockoilchain$ composer network install
--card PeerAdmin@hlfv1 --archiveFile blockoilchain@0.0.1.bna
✓ Installing business network. This may take a minute...
Successfully installed business network blockoilchain, version 0.0.1
Command succeeded
```

Figure 7.17: Install BNA file

The following command is used to implement the business network: “*composer network start --networkName blockoilchain --networkVersion 0.0.1 --networkAdmin admin --networkAdminEnrollSecret adminpw --card PeerAdmin@hlfv1 --file networkadmin.card*”. The result should be similar to the one depicted in Figure 7.18. The next step (Figure 7.19) is to import the network to a marketable network card: “*composer card import --file networkadmin.card*” and verify if it was correctly implemented with the bellow command: “*composer network ping --card admin@blockoilchain*” (see, Figure 7.20).

```
angel@angel-HP-Pavilion-g6-Notebook-PC:~/blockoilchain$ composer network start --
--networkName blockoilchain --networkVersion 0.0.1 --networkAdmin admin --network
AdminEnrollSecret adminpw --card PeerAdmin@hlfv1 --file networkadmin.card
Starting business network blockoilchain at version 0.0.1

Processing these Network Admins:
  userName: admin

✓ Starting business network definition. This may take a minute...
Successfully created business network card:
  filename: networkadmin.card

Command succeeded
```

Figure 7.18: Implementation of the business network

```
angel@angel-HP-Pavilion-g6-Notebook-PC:~/blockoilchain$ composer card import --f
ile networkadmin.card

Successfully imported business network card
  Card file: networkadmin.card
  Card name: admin@blockoilchain

Command succeeded
```

Figure 7.19: Import the network to a marketable network card

```
angel@angel-HP-Pavilion-g6-Notebook-PC:~/blockoilchain$ composer network ping --
card admin@blockoilchain
The connection to the network was successfully tested: blockoilchain
  Business network version: 0.0.1
  Composer runtime version: 0.20.9
  participant: org.hyperledger.composer.system.NetworkAdmin#admin
  identity: org.hyperledger.composer.system.Identity#61b428e3280268898eb4e
a6bb7ae686610a475f4b19201eb5db0d5476c9013df

Command succeeded
```

Figure 7.20: Verify the implementation of the network card

### 7.5.3 Start the RESTful API

Once all the classes have been deployed in our local composer, it is time to obtain the REST SERVER, which allows one to communicate the Angular interface with the Hyperledger Fabric platform, in other words, connect the front-end with the back-end. Figure 7.21 shows the flow of information, where the changes made in the Angular App are reflected in the Hyperledger Fabric and vice versa.



Figure 7.21: Flow of information of REST SERVER

To obtain the REST SERVER, one must execute the “*composer-rest-server*” command and follow the steps in Figure 7.22. When the process is finished, one must open <http://localhost:3000/explorer> in the browser to be able to interact with the API. If the procedure was successful, a screen like the one in Figure 7.23 will appear. Despite being a more friendly interface, it is still somewhat complicated for a user who is not a developer, so we will not go into detail about its operation.

```

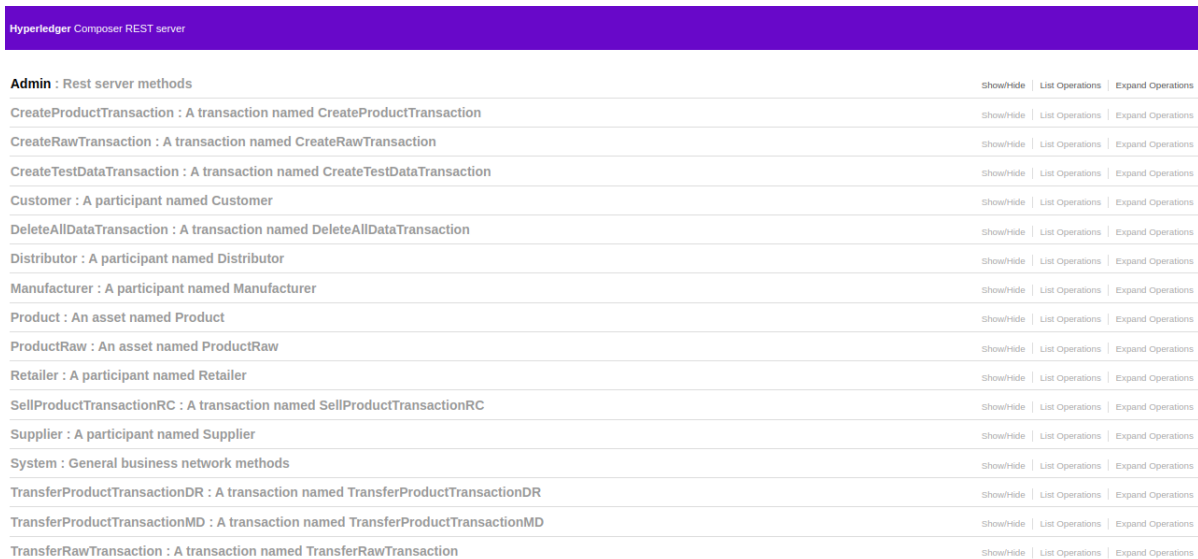
angel@angel-HP-Pavilion-g6-Notebook-PC:~/blockoilchain$ composer-rest-server
? Enter the name of the business network card to use: admin@blockoilchain
? Specify if you want namespaces in the generated REST API: never use namespaces

? Specify if you want to use an API key to secure the REST API: No
? Specify if you want to enable authentication for the REST API using Passport:
No
? Specify if you want to enable the explorer test interface: Yes
? Specify a key if you want to enable dynamic logging: l
? Specify if you want to enable event publication over WebSockets: Yes
? Specify if you want to enable TLS security for the REST API: No

To restart the REST server using the same options, issue the following command:
  composer-rest-server -c admin@blockoilchain -n never -u true -d l -w true

Discovering types from business network definition ...
Discovering the Returning Transactions..
Discovered types from business network definition
Generating schemas for all types in business network definition ...
Generated schemas for all types in business network definition
Adding schemas for all types to Loopback ...
Added schemas for all types to Loopback
Web server listening at: http://localhost:3000
  
```

Figure 7.22: Configuration of REST SERVER



Hyperledger Composer REST server			
<b>Admin</b> : Rest server methods	Show/Hide	List Operations	Expand Operations
CreateProductTransaction : A transaction named CreateProductTransaction	Show/Hide	List Operations	Expand Operations
CreateRawTransaction : A transaction named CreateRawTransaction	Show/Hide	List Operations	Expand Operations
CreateTestDataTransaction : A transaction named CreateTestDataTransaction	Show/Hide	List Operations	Expand Operations
Customer : A participant named Customer	Show/Hide	List Operations	Expand Operations
DeleteAllDataTransaction : A transaction named DeleteAllDataTransaction	Show/Hide	List Operations	Expand Operations
Distributor : A participant named Distributor	Show/Hide	List Operations	Expand Operations
Manufacturer : A participant named Manufacturer	Show/Hide	List Operations	Expand Operations
Product : An asset named Product	Show/Hide	List Operations	Expand Operations
ProductRaw : An asset named ProductRaw	Show/Hide	List Operations	Expand Operations
Retailer : A participant named Retailer	Show/Hide	List Operations	Expand Operations
SellProductTransactionRC : A transaction named SellProductTransactionRC	Show/Hide	List Operations	Expand Operations
Supplier : A participant named Supplier	Show/Hide	List Operations	Expand Operations
System : General business network methods	Show/Hide	List Operations	Expand Operations
TransferProductTransactionDR : A transaction named TransferProductTransactionDR	Show/Hide	List Operations	Expand Operations
TransferProductTransactionMD : A transaction named TransferProductTransactionMD	Show/Hide	List Operations	Expand Operations
TransferRawTransaction : A transaction named TransferRawTransaction	Show/Hide	List Operations	Expand Operations

Figure 7.23: API in the localhost

## 7.5.4 Front End Creation

```

angel@angel-HP-Pavilion-g6-Notebook-PC:~/blockoilchain$ yo
? 'Allo Angel! What would you like to do? Hyperledger Composer

Make sure you are in the directory you want to scaffold into.
This generator can also be run with: yo hyperledger-composer

Welcome to the Hyperledger Composer project generator
? Please select the type of project: Angular
You can run this generator using: 'yo hyperledger-composer:angular'
Welcome to the Hyperledger Composer Angular project generator
? Do you want to connect to a running Business Network? Yes
? Project name: BlockOilChain
? Description: Blockchain Application in the oil supply chain
? Author name: Angel Villacreses
? Author email: angel.villacreses@outlook.es
? License: Apache-2.0
? Name of the Business Network card: admin@blockoilchain
? Do you want to generate a new REST API or connect to an existing REST API? Co
nnect to an existing REST API
? REST server address: http://localhost
? REST server port: 3000
? Should namespaces be used in the generated REST API? Namespaces are not used
Created application!
Completed generation process

```

Figure 7.24: Construction of the frontend

The last step is the construction of the frontend using only one command. For that, one must open a new terminal within the same project location and execute the “*yo*” command, follow the options shown in Figure 7.24, this will create a folder called *BlockOilChain* where one must execute the “*npm start*” command in the terminal to start the application. The result of this procedure should be as in Figure 7.25.

Finally, one must open in the browser <http://localhost:4200> to be able to interact with the blockchain model applied to the oil supply chain.

```
Hash: 06d2c97cc5dcad11c2e4
Time: 41910ms
chunk {0} polyfills.bundle.js, polyfills.bundle.js.map (polyfills) 297 kB {5} [initial] [rendered]
chunk {1} main.bundle.js, main.bundle.js.map (main) 339 kB {4} [initial] [rendered]
chunk {2} styles.bundle.js, styles.bundle.js.map (styles) 184 kB {5} [initial] [rendered]
chunk {3} scripts.bundle.js, scripts.bundle.js.map (scripts) 455 kB {5} [initial] [rendered]
chunk {4} vendor.bundle.js, vendor.bundle.js.map (vendor) 4.16 MB [initial] [rendered]
chunk {5} inline.bundle.js, inline.bundle.js.map (inline) 0 bytes [entry] [rendered]
webpack: Compiled successfully.
```

Figure 7.25: Front End Execution

# Chapter 8

## Results and Discussions

As introduced in section 7.2, the application developed in this thesis emphasizes an use-case for the oil industry, focused on a global model of the gasoline supply chain. With this simple application, the main characteristics of the blockchain are shown that allow improving data transparency, product traceability, data confidentiality and interoperability between different systems.

### 8.1 Demo presentation

To analyze the objectives set out in this thesis, we will first make the case of using the supply chain for gasoline in the web application created. The main interface in Figure 8.1 shows five tabs that have sub-tabs to interact with the system.

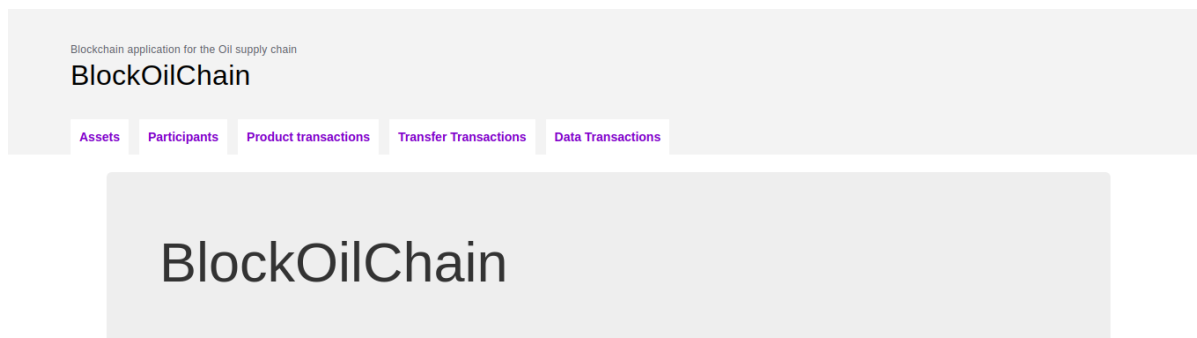


Figure 8.1: BlockOilChain application interface

The *Assets* tab contains the *Raw product* and *Product*, each one allows one to view,

create, edit and delete chain assets. The Participant tab is divided into *Supplier*, *Manufacturer*, *Distributor*, *Retailer*, and *Customer*, here one can create the different companies that participate in each of these sectors. *ProductTransactions* has the *CreateRawTransaction* and *CreateproductTransaction* functions that allow one to create assets for the *Supplier* and the *Manufacturer*. *TransferTransactions* contains the transfer functions: *TransferRawTransaction* allows one to transfer the raw product from the *Supplier* to the *Manufacturer*, *TransferProductTransactionMD* transfers the gasoline from the *Manufacturer* to the *Distributor*, *TransferProductTransactionDR* transfers the product from the *Distributor* to the *Retail*, and with the function, *SellProductTransactionRC* sells the gasoline to the *Customer*. Finally, *DataTransactions* has two functions that are used to create participants automatically, and to erase all system information but not from history.

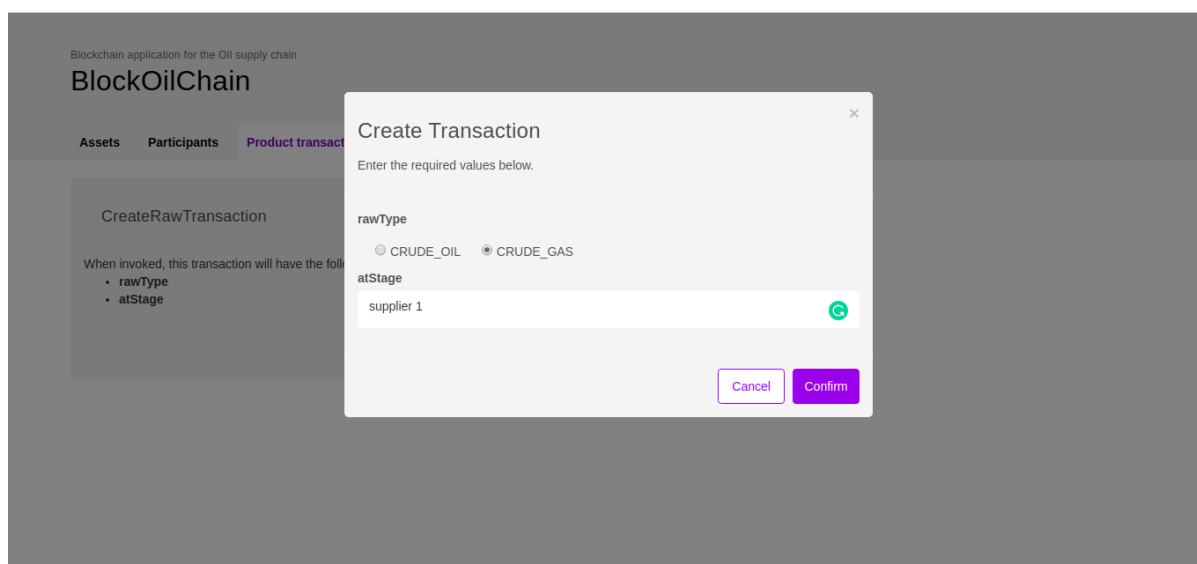


Figure 8.2: Creation of raw product

To speed up the process, we will use the *CreateTestDataTransaction* function, which creates the information of the five participants. Once the participants have been created, the asset that will be part of the final product must be created, for this purpose in *CreateRawTransaction*, the function is invoked. All functions have a pop-up box to create transactions. In Figure 8.2, we can see how the software asks to select the type of crude oil to be processed and the *Supplier* that will generate it.

When the transaction confirmation is sent, the raw products information is automatically incorporated into its corresponding tab, as seen in Figure 8.3.

Blockchain application for the Oil supply chain

## BlockOilChain

Assets Participants Product transactions Transfer Transactions Data Transactions

ProductRaw + | Create Asset





amount	rawType	productRawStatus	id	atStage	Actions
1	CRUDE_OIL	CREATED	1	supplier 1	 
1	CRUDE_GAS	CREATED	2	supplier 1	 

Figure 8.3: Raw product created

In order for the *Manufacturer* (refinery) to create the gasoline, it first needs to obtain the raw products (crude oil and crude gas) from the *Supplier*, for this purpose, the *TransferRawTransaction* function is invoked and the IDs of the products to be transferred are entered, with the IDs of the *Supplier* and *Manufacturer* that will perform this operation. If it was successful, the raw products will appear in *rawStorage* of the *Manufacturer* section, as shown in Figure 8.4.

Manufacturer + | Create Participant



productType	rawStorage	productStorage	id	name	address	Actions
GASOLINE	resource:model/ProductRaw#1,resource:model.Pro...		manufacturer 1	Refinery	[object Object]	 

Figure 8.4: Raw product stored in Manufacturer storage

Once the refinery has crude oil, it can be transformed into a product (gasoline). To convert the raw asset to a product, the *CreateProductTransaction* function is used. In this way, it can be seen in Figure 8.5, that raw products are no longer stored, because they were converted into a product, into gasoline.

Manufacturer + | Create Participant

productType	rawStorage	productStorage	id	name	address	Actions
GASOLINE		resource:model.Product#1	manufacturer 1	Refinery	[object Object]	 

Figure 8.5: Product stored in Manufacturer storage

Once the gasoline is created, it must be sent to the *Distributor* (Tunker Trunk) and then to the *Retailer* (Gasoline Station) in order to sell it to the final consumer. Therefore, the *TransferProductMD* and *TransferProductDR* function must be invoked. In that way, it is seen that the product in Figure 8.6 passes through the *Distributor* and then through the *Retailer*, see Figure 8.7.

Product



productType	productStatus	id	atStage	Actions
GASOLINE	CREATED	1	distributor 1	 

Figure 8.6: Product created in the Distributor

Product



productType	productStatus	id	atStage	Actions
GASOLINE	CREATED	1	retailer 1	 

Figure 8.7: Product created in the Retailer

At this point, the gas station is able to sell gasoline to a *Customer*. For this, the *SellProductTransactionRC* function is used. When the operation is successful, in Figure 8.8, it can be seen that the product has been sold to *Customer* of Figure 8.9, called Ángel Villacreses.



### Product

productType	productStatus	id	atStage
GASOLINE	SOLD	1	Customer 1

Figure 8.8: Product sold to Customer

### Customer

productType	productStorage	id	name	address
Gasoline	Product 1	customer 1	Ángel Villacreses	Ecuador

Figure 8.9: Purchase detail

With the finished recreation of the gasoline supply chain, objectives can be analyzed and discussed from different perspectives using the Hyperledger Composer Playground and API REST platforms.

## 8.2 Transparency

The first parameter to discuss is the transparency of the network, which allows working together between different companies. This transparency allows one to register products and data and see in real-time ones location and all its corresponding information. The information is immutable, so the records cannot be altered, so the origin of the data will always be known. Any member in the chain can access these resources, as long as they have access and are authorized to see such information. For an authorized blockchain, the information that each participant can view depends on the restrictions placed by the network administrator to preserve their business. In this project, you can analyze the transparency of the participants, assets, and transactions.

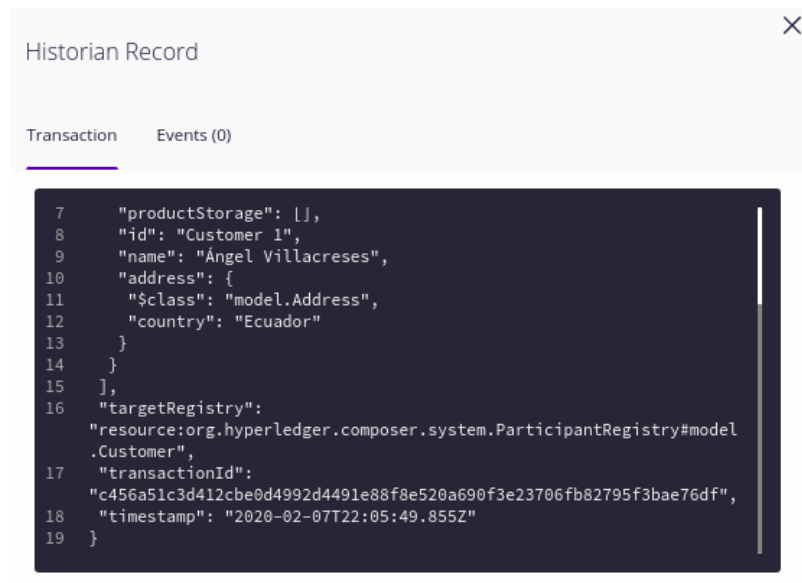


Figure 8.10: Manufacturer instance confirmation

Figure 8.10, shows the creation of the Customer instance, which contains the participant’s ID, the name to which it belongs, the address, and most importantly, the registration of the transaction data. This data is produced after the participant has been successfully created, the resource information, the transaction ID and the timestamp are recorded. This process occurs with all participants when they register for the first time or when they are edited. Each time participants are registered, they are recorded in the All transaction section of the Playground (see Figure 8.11), where time, type of operation, the executor of the operation and an option to see the details of the figure are shown previously.

Date, Time	Entry Type	Participant	
2020-02-07, 17:05:49	AddParticipant	admin (NetworkAdmin)	<a href="#">view record</a>
2020-02-07, 17:05:30	AddParticipant	admin (NetworkAdmin)	<a href="#">view record</a>
2020-02-07, 17:05:06	AddParticipant	admin (NetworkAdmin)	<a href="#">view record</a>
2020-02-07, 17:04:32	AddParticipant	admin (NetworkAdmin)	<a href="#">view record</a>

Figure 8.11: All transaction in the Hyperledger Composer Playground

In this way, there is a record of all the participant incorporations, which cannot be manipulated without a trace. With the registration of the participants, the system is able to interact with each other to carry out the transactions defined for each one. However, the design of this network was done in such a way that they cannot carry out transactions until the supplier has its assets.

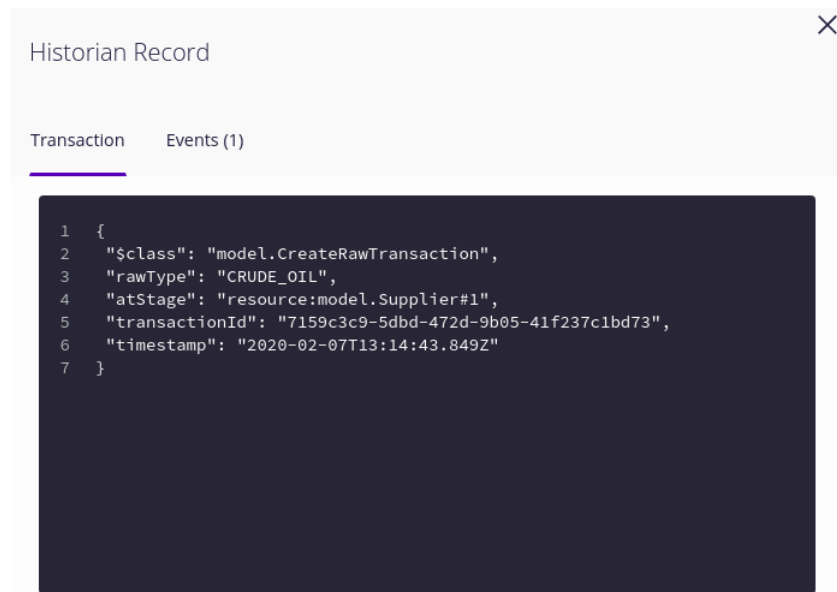


Figure 8.12: Raw product confirmation

The two types of assets also register their products on the blockchain. In Figure 8.12, the creation of the raw product records the type of crude oil one is creating, to whom it belongs, and the transaction ID and timestamp assigned to it, after creating the asset. In the case of creating the product (Figure 8.13), one first need the manufacturer to have the raw product in stock to be able to transform it into gasoline. The registration is the same as the previous one, but these actions also contain events that happen when a certain action is performed. In this case, it generates an event when the product is created by the Manufacturer. The record contains the product and manufacturer's route, with the creation date and the event ID and the timestamp.

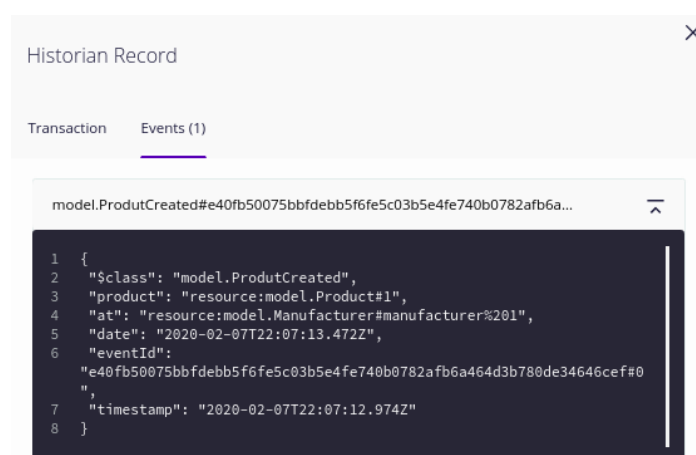


Figure 8.13: Event when the product is created

For the transactions, the process is the same, in Figure 8.14, it is shown how the op-

eration of selling the Retailer product to the Consumer is recorded, just like the previous processes, with the name of the product, the participants of the transaction and the ID and time stamp of the confirmation.

```

1 {
2   "$class": "model.SellProductTransactionRC",
3   "product": "resource:model.Product#1",
4   "retailer": "resource:model.Retailer#retailer%201",
5   "customer": "resource:model.Customer#Customer%201",
6   "transactionId":
7     "2957b8fb747385e552daa6f05e7dfddb14b4e78ae630efa02390cf5cfa4274c8",
8   "timestamp": "2020-02-07T22:09:10.316Z"
9 }

```

Figure 8.14: Sale confirmation

### 8.3 Traceability

One of the most important characteristics of the blockchain is to have a system that is able to do a backward search of a product, that is, that is able to see the traceability of a product or its source information, within Supply Chain. Thanks to the transparency that the products have in the blockchain, it is possible to use the system to track assets and transactions from the beginning, thanks to their identifiers. The program has not implemented the option to quickly search the history of a product. However, a file can be implemented to make inquiries and be able to integrate it into the program, in this way, the user can quickly and efficiently consult the route of an asset. But thanks to the playground, you can consult manually in the history, thus obtaining the traceability of an asset or transaction.

In the following program, the traceability of the product is shown, since it is a crude product (Crude Oil) until it is sold as gasoline to the Customer.

```

1 {
2   "$class": "model.CreateRawTransaction",
3   "rawType": "CRUDE_OIL",
4   "atStage": "resource:model.Supplier#supplier 1",
5   "transactionId": "191424ecfe54ef42463233c299cb8...",
6   "timestamp": "2020-02-07T22:02:21.982Z"
7 }
8 {
9   "$class": "model.ProdutRawCreated",
10  "productRaw": "resource:model.ProductRaw#1",
11  "supplier": "resource:model.Supplier#supplier 1",
12  "date": "2020-02-07T22:02:22.245Z",
13  "eventId": "191424ecfe54ef42463233c299cb87eeef6de...",
14  "timestamp": "2020-02-07T22:02:21.982Z"
15 }
16 {

```

```
17  "$class": "model.TransferRawTransaction",
18  "productRaw": "resource:model.ProductRaw#1",
19  "supplier": "resource:model.Supplier#supplier 1",
20  "manufacturer": "resource:model.Manufacturer#manufacturer 1",
21  "transactionId": "991c41d4f7f5d76397eb2d30e6abcc...",
22  "timestamp": "2020-02-07T22:06:21.013Z"
23 }
24 {
25  "$class": "model.ProdutCreated",
26  "product": "resource:model.Product#1",
27  "at": "resource:model.Manufacturer#manufacturer 1",
28  "date": "2020-02-07T22:07:13.472Z",
29  "eventId": "e40fb50075bbfdebb5f6fe5c03b5e4fe740...",
30  "timestamp": "2020-02-07T22:07:12.974Z"
31 }
32 {
33  "$class": "model.TransferProductTransactionMD",
34  "product": "resource:model.Product#1",
35  "manufacturer": "resource:model.Manufacturer#manufacturer 1",
36  "distributor": "resource:model.Distributor#distributor 1",
37  "transactionId": "cb8c5800b6457b0504172c140d686b3600d25...",
38  "timestamp": "2020-02-07T22:07:55.810Z"
39 }
40
41 {
42  "$class": "model.TransferProductTransactionDR",
43  "product": "resource:model.Product#1",
44  "distributor": "resource:model.Distributor#distributor 1",
45  "retailer": "resource:model.Retailer#retailer 1",
46  "transactionId": "f3c77c7a040e49c2c169b49146b8baf5050c...",
47  "timestamp": "2020-02-07T22:08:18.283Z"
48 }
49 {
50  "$class": "model.SellProductTransactionRC",
51  "product": "resource:model.Product#1",
52  "retailer": "resource:model.Retailer#retailer 1",
53  "customer": "resource:model.Customer#Customer 1",
54  "transactionId": "2957b8fb747385e552daa6f05e7dfddb14b4e...",
55  "timestamp": "2020-02-07T22:09:10.316Z"
56 }
```

Product information is listed chronologically, divided into 7 parts, where all have the *transaction ID* and the *timestamp*. The first is the creation of Crude Oil by *supplier 1*. The second is the confirmation of the creation of the raw product in the *supplier 1*. The

third is the transfer of the raw product from the *supplier 1* to the manufacturer 1. The fourth creates *product 1* in the *manufacturer 1*. Sections 5 and 6 are the transfer of the product from the *manufacturer 1* to the *distributor 1* and from the *distributor 1* to the *retailer 1*. Finally, *product 1* is sold to *customer 1*.

Compared to traditional databases, the blockchain allows one to access the traceability of a product more quickly and clearly. This feature enables to find a problem much faster since the information is immutable, therefore, it is reliable.

## 8.4 Confidentiality

From the beginning, the blockchain stood out for its transparency and traceability in its public networks. However, this system where all participants can see all the movements within the network is not beneficial for an enterprise network. Companies or businesses must safeguard their strategic movements they make to obtain contracts, such as offering benefits that others do not receive. Or simply to prevent competitors from knowing the logistics of the business that allow them to stand out in their sector.

For this reason, we opted for the implementation of a permissioned blockchain, through the Hyperledger platform that allows one to configure the scope of the participants and the visibility of the assets. This configuration is possible thanks to the system membership services, it is responsible for granting and validating certificates and user authentication. In order to identify the client and allow her or him to connect securely to the system. In addition, restrictions are placed on the access control file, and the `logic.js` file through programming.

To model the business network, it is necessary to have a network access control that is defined in the access control file in the `.acl` format. This file contains the rules established by the network administrator, who grants or denies participants permissions to perform certain operations within the network. This file contains the rules established by the network administrator, who grants or denies participant's permissions to perform certain operations within the network. In Figure 8.15, 3 rules that restrict the participation of the Distributor are shown. The rules do not allow to manage the roles of the supplier, the manufacturer, or the retailer, since the actions of `CREATE`, `UPDATE` and `DELETE` are with the `DENY` action.

```
ACL File permissions.ad
84 }
85 rule DistributorCanNotManageSupplier {
86   description: "Members of the Delaer roles can not manage Supplier participants"
87   participant: "model.Distributor"
88   operation: CREATE, UPDATE, DELETE
89   resource: "model.Supplier"
90   action: DENY
91 }
92 rule DistributorCanNotManageManufacturer {
93   description: "Members of the Distributor roles can not manage Manufacturer participants"
94   participant: "model.Distributor"
95   operation: CREATE, UPDATE, DELETE
96   resource: "model.Manufacturer"
97   action: DENY
98 }
99 rule DistributorCanNotManageRetailer {
100  description: "Members of the Distributor roles can not manage Retailer participants"
101  participant: "model.Distributor"
102  operation: CREATE, UPDATE, DELETE
103  resource: "model.Retailer"
104  action: DENY
105 }
```

Figure 8.15: Distributor rules

To demonstrate that the Distributor can not access the roles of the Supplier, the user was changed from administrator to participant Distributor 1. In this way, an attempt was made to create a raw product for Supplier 1. However, the results were negative because the user Distributor 1 does not have permission to CREATE, a role that belongs to the Supplier, as seen in the warning in Figure 8.16.



The screenshot shows a 'JSON Data Preview' window with a dark background. The JSON content is as follows:

```
1 {
2   "$class": "model.CreateRawTransaction",
3   "rawType": "CRUDE_OIL",
4   "atStage": "resource:model.Supplier#supplier 1"
5 }
```

Below the JSON, there is a checkbox labeled 'Optional Properties' which is currently unchecked. A red error message is displayed below the checkbox:

```
t: Participant 'model.Distributor#1' does not have 'CREATE' access to resource 'model.ProductRaw#3'
```

On the right side of the interface, there is a vertical sidebar with a dark purple header labeled 'trunk'.

Figure 8.16: Raw products registration denied to the distributor

## 8.5 Interoperability

The current systems used by oil companies have compatibility problems when they interconnect different organizations, becoming a big problem for the transparency and traceability of products. Causing supply chains to be very inefficient as there is no effective communication between different participants from the different companies.

This problem is solved thanks to the ease provided by the Hyperledger Composer REST Server platform to integrate one's system to any existing mobile or web client application of companies that do not use blockchain. Thanks to the use of the REST API, the blockchain network can extract data from existing systems to convert them into assets or participants and integrate them into the Hyperledger composer network.

As seen in Figure 8.17, the interface is quite intuitive, just select an asset, product or function to display the REST methods. Assets and participants have the GET, POST, HEAD, PUT, and DELETE methods, and the transactions have the GET and POST methods. These methods allow the server to indicate how a request should be treated.

The GET method allows one to query information, POST creates a new record, PUT can update a record, DELETE deletes the record, and HEAD obtains information about a particular resource. That way, the system is able to send the information from the blockchain network to other systems that the oil companies have. It is even able to incorporate the information of these decentralized systems into the blockchain network and grant their respective credentials to become participants or assets within the centralized network.

The screenshot displays the Hyperledger Composer REST server interface. It is titled "Hyperledger Composer REST server" and shows three sections of REST API methods:

- ProductRaw**: An asset named ProductRaw. Methods include GET /ProductRaw (Find all instances of the model matched by filter from the data source.), POST /ProductRaw (Create a new instance of the model and persist it into the data source.), GET /ProductRaw/{id} (Find a model instance by {id} from the data source.), HEAD /ProductRaw/{id} (Check whether a model instance exists in the data source.), PUT /ProductRaw/{id} (Replace attributes for a model instance and persist it into the data source.), and DELETE /ProductRaw/{id} (Delete a model instance by {id} from the data source.).
- Retailer**: A participant named Retailer. Methods include GET /Retailer (Find all instances of the model matched by filter from the data source.), POST /Retailer (Create a new instance of the model and persist it into the data source.), GET /Retailer/{id} (Find a model instance by {id} from the data source.), HEAD /Retailer/{id} (Check whether a model instance exists in the data source.), PUT /Retailer/{id} (Replace attributes for a model instance and persist it into the data source.), and DELETE /Retailer/{id} (Delete a model instance by {id} from the data source.).
- SellProductTransactionRC**: A transaction named SellProductTransactionRC. Methods include GET /SellProductTransactionRC (Find all instances of the model matched by filter from the data source.), POST /SellProductTransactionRC (Create a new instance of the model and persist it into the data source.), and GET /SellProductTransactionRC/{id} (Find a model instance by {id} from the data source.).

Figure 8.17: REST API methods



# Chapter 9

## Conclusions

This research collects the most relevant and current blockchain information in the oil industry with the objective of expanding the use of this technology, particularly in Ecuador. We focus specifically in the supply chain, so an exhaustive study of its main structures and problems was carried out. The study case was made with the Petroamazonas EP oil company, with public information found on its official website and research papers.

Once the problems and structures present in the supply chain in the oil industry were defined, a study began on the different tools that allow applying blockchain to Petroamazonas EP with the aim of optimizing the time required to complete transactions and the reliability and immutability of the data. Different platforms such as IBM Blockchain Platform, Multichain, Openchain, and Ethereum were tested. In particular, the IBM platform was difficult to operate because of its timing, limited to one month trial offer and its no download code policy.

As a successful alternative, we used the Hyperledger platform, since it is an open-source tool that allows developers, included IBM itself, to create networks with known programming languages such as Java Script, Node.js, Java etc. It also has multiple tools that facilitate the development of advanced practical systems.

After a detailed study of the *Hyperledger Fabric* and *Composer* platform, testing of the resources code offered by the platform to learn how to develop a network, was completed. Once a basic programming knowledge was acquired, the code was written to implement a demo of the operation of the oil supply chain, in order to demonstrate its benefits and operative potentials. After some errors at the beginning of the system implementation, a stable solution was found. This demonstrated how a transaction in a demo supply chain can remain immutable in time, granting the potential to change and optimize the industry. It also offers the possibility to incorporate this technology to existing, daily used software, including growth capacity and scalability to professional blockchains platforms.

In conclusion, platforms such as Hyperledger based on blockchain technology can provide new opportunities in the oil field, greatly reducing transaction and management processes, saving time and reducing operative costs. This thesis shows that blockchain accomplished the requirements that enable optimizing a supply chain with transparency, traceability, confidentiality and interoperability properties.

Thanks to open-source tools such as Hyperledger, Visual Studio Code, Docker, and Yeoman, it is relatively easy to write applications implementing blockchain, incorporating services that interconnect with each other and are able to create a decentralized network with all the characteristics of a distributed ledger, and with the possibility of scaling and applying it to problems at an industrial scale, such as the oil industry.

# Bibliography

- [1] S. Dutta S. Banerjee, “Blockchain adoption in oil gas: A framework to assess your company’s readiness,” *Tata Consultancy services*, 2018.
- [2] Agencia de Regulación y Control Hidrocarburífero, “Producción mensual nacional de petróleo fiscalizado,” Dec. 2016.
- [3] Petroamazonas EP, “Estatuto orgánico de gestión organizacional por procesos,” Jul. 2017.
- [4] —, “Manual orgánico de gestión organizacional por procesos de petroamazonas ep.” Dec. 2015.
- [5] Editor, “Blockchain es un registro electrónico de contabilidad,” Feb. 2018. [Online]. Available: <https://www.latarde.com.ec/2018/02/08/tecnologia-blockchain-nuevas-aplicaciones-e-innovaciones-de-forma-energetica/>
- [6] H. Anwar, “The ultimate blockchain technology guide: A revolution to change the world,” Oct. 2018. [Online]. Available: <https://101blockchains.com/ultimate-blockchain-technology-guide/>
- [7] Sphinx solutions, “types of blockchain and why businesses need them,” 2018. [Online]. Available: [www.sphinx-solution.com](http://www.sphinx-solution.com)
- [8] Hyperledger, “Ledger,” s.g. [Online]. Available: <https://hyperledger-fabric.readthedocs.io/en/latest/ledger/ledger.html>
- [9] —, “Introduction,” s.g. [Online]. Available: <https://hyperledger-fabric.readthedocs.io/en/latest/blockchain.html>
- [10] H. Narumanchi N. Emmadi , “Practical deployability of permissioned blockchains,” *Springer Nature*, pp. 229–243, Jan. 2019. [Online]. Available: [https://doi.org/10.1007/978-3-030-04849-5\\_21](https://doi.org/10.1007/978-3-030-04849-5_21)
- [11] B. Pran, “Architecting a hyperledger solution — things to keep in mind,” Sep. 2018. [Online]. Available: <https://hackernoon.com/architecting-a-hyperledger-solution-things-to-keep-in-mind-78033e6fee75>

- [12] Hyperledger, “Introduction,” s.g. [Online]. Available: <https://hyperledger.github.io/composer/latest/introduction/introduction.html>
- [13] S. C. Gómez et Al., “Blockchain: mirando más allá del bitcoin,” Apr. 2017. [Online]. Available: <http://marketing.asobancaria.com/hubfs/AsobancariaEventos/Asobancaria-Semanas-Economicas/1084.pdf>
- [14] A. M. Antonopoulos, *Mastering Bitcoin*. O’Reilly Media, Inc., 2014.
- [15] A. H. Mohsin et Al., “Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions,” *Comput. Standards Interfaces*, vol. 64, pp. 41–60, May 2019. [Online]. Available: <https://doi.org/10.1016/j.csi.2018.12.002>
- [16] A. M. Antonopoulos G. Wood, *Mastering Ethereum*. O’Reilly Media, Inc., 2018.
- [17] BP, “BP Statistical Review of World Energy,” *Brit. Petroleum*, Jun. 2018.
- [18] —, “BP Energy Outlook,” *Brit. Petroleum*, Feb. 2019.
- [19] H. Lu et Al., “Blockchain technology in the oil and gas industry: A review of applications, opportunities, challenges, and risks,” *IEEE Access*, vol. 7, pp. 41 426 – 41 444, Mar. 2019.
- [20] ECOSC, “Decentralized supply management system,” *ECOSC*, Mar. 2019.
- [21] Infosys, “Oil and gas industry -blockchain, the disruptive force of the 21st century,” 2018.
- [22] F. Ehsani, “Blockchain in finance: From buzzword to watchword in 2016,” Dec. 2016. [Online]. Available: <https://www.coindesk.com/blockchain-finance-buzzword-watchword-2016>
- [23] N. Gaur et Al., *Building decentralized applications with Hyperledger Fabric and Composer*. Packt Publishing, 2018.
- [24] T. Huseini, “The future of oil and gas: Eight bold industry predictions,” Aug. 2018. [Online]. Available: <https://www.offshore-technology.com/digital-disruption/blockchain/the-future-of-oil-and-gas-predictions/>
- [25] A. McFarland, “In 2018, the united states consumed more energy than ever before,” Apr. 2019. [Online]. Available: <https://www.eia.gov/todayinenergy/detail.php?id=39092>
- [26] K. Buchholz, “The biggest oil and gas companies in the world,” Jan. 2020. [Online]. Available: <https://www.statista.com/chart/17930/the-biggest-oil-and-gas-companies-in-the-world/>

- [27] EnRes Resources LLC, “Titans of the oil industry: The 10 top oil companies of 2019,” Apr. 2019. [Online]. Available: <https://enresllc.com/top-oil-companies/>
- [28] G. González, “Petrolera colombiana incluye una blockchain en su proceso de transformación digital,” Nov. 2019. [Online]. Available: <https://www.criptonoticias.com/comunidad/adopcion/petrolera-colombiana-incluye-blockchain-transformacion-digital/>
- [29] B.C.E, “Reporte del sector petrolero,” Dic. 2017. [Online]. Available: <https://contenido.bce.fin.ec/documentos/Estadisticas/Hidrocarburos/ASP201712.pdf>
- [30] V. Saltos, *Ecuador y su Realidad, de páginas 183 - 196*. Ediciones Peralta, 2018.
- [31] Expansion, “Repsol prevé ahorrar 400.000 euros al año aplicando la tecnología ‘blockchain’ a sus certificaciones,” Jan. 2019. [Online]. Available: <http://www.expansion.com/empresas/energia/2019/01/13/5c3b1acc22601dab018b45d2.html>
- [32] Petroamazonas EP, “Petroamazonas ep incrementó en un 4% su producción petrolera, en 2019,” Jan. 2019. [Online]. Available: <https://www.petroamazonas.gob.ec/?p=11408>
- [33] J. B. Morales, “La gestión de compras,” Jul. 2008. [Online]. Available: <https://www.gestiopolis.com/la-gestion-de-compras/>
- [34] R. H. Ballou, *Logística Administración de la cadena de suministro*. Pearson, 2004.
- [35] MeetLogistics, “Planificación de la demanda: Fundamentos.” Jul. 2015. [Online]. Available: <https://meetlogistics.com/demand-planning/planificacion-de-la-demanda-fundamentos/>
- [36] Lantares Solution, “Planificación dinámica de la demanda,” s.f. [Online]. Available: <http://www.lantares.com/planificacion-dinamica-de-la-demanda>
- [37] I. Kozlenkova et Al. , “The role of marketing channels in supply chain management,” *Journal of Retailing*, vol. 91, pp. 586–609, Dec. 2015. [Online]. Available: <https://doi.org/10.1016/j.jretai.2015.03.003>
- [38] N. Rodriguez, “Blockchain para la cadena de suministro: El cambio en el juego,” Jun. 2019. [Online]. Available: <https://101blockchains.com/es/blockchain-para-la-cadena-de-suministro>
- [39] R. Basu, “Blockchain technology and the oil gas industry,” Aug. 2018. [Online]. Available: <https://media.consensys.net/blockchain-technology-and-the-oil-gas-industry-c8dd946d54b3>
- [40] L. Klancir, “Applications of blockchain technology in the oil and gas industry,” s.f. [Online]. Available: <https://www.asyncclabs.co/blog/blockchain-technology-oil-gas-industry/>

- [41] R. Basu, “Blockchain use cases and benefits for upstream oil gas,” Sep. 2018. [Online]. Available: <https://media.consensys.net/blockchain-use-cases-for-upstream-oil-gas-bd6affd887e5>
- [42] —, “Blockchain use cases for midstream oil gas,” Sep. 2018. [Online]. Available: <https://media.consensys.net/blockchain-use-cases-for-midstream-oil-gas-609033457e33>
- [43] —, “Blockchain use cases for downstream oil gas,” Sep. 2018. [Online]. Available: <https://media.consensys.net/blockchain-use-cases-and-benefits-for-downstream-oil-gas-ac8de9da6dca>
- [44] Computerworld, “Repsol y finboot aprovechan la tecnología 'blockchain' para mejorar sus procesos,” Jan. 2019. [Online]. Available: <https://www.computerworld.es/tecnologia/repsol-y-finboot-aprovechan-la-tecnologia-blockchain-para-mejorar-sus-procesos>
- [45] J. Maldonado, “Repsol prevé ahorrar 400.000 euros al año aplicando la tecnología 'blockchain' a sus certificaciones,” Mar. 2019. [Online]. Available: <https://bit.ly/2WP1K4b>
- [46] Maldonado, *El Petróleo en Ecuador: su historia y su importancia en la economía nacional*. Petroecuador, 2002.
- [47] D. Malets, “13 benefits blockchain offers the oil and gas industry,” Apr 2019. [Online]. Available: <https://technorely.com/blog/blockchain-oil-and-gas-industry/>
- [48] W. E. Trade, “Cómo blockchain está cambiando la cara del comercio del petróleo,” Feb. 2019. [Online]. Available: <https://www.worldenergytrade.com/index.php/m-news-oil-gas/84-news-oil-gas-i-d-i/2032-como-blockchain-esta-cambiando-la-cara-del-comercio-del-petroleo>
- [49] J. M. Harán, “Blockchain: problemas de seguridad que giran alrededor de esta tecnología,” Apr 2019. [Online]. Available: <https://www.welivesecurity.com/la-es/2019/04/02/blockchain-problemas-seguridad-alrededor-tecnologia/>
- [50] W. live security, “Tendencias 2019: Privacidad e intrusión en la aldea global,” 2019. [Online]. Available: <https://www.welivesecurity.com/wp-content/uploads/2018/12/Tendencias-Ciberseguridad-2019-ESET.pdf>
- [51] M. Crosby et Al., “Blockchain technology: Beyond bitcoin,” *Berkeley*, Jun. 2016.
- [52] A. Schuschny, “La blockchain y sus posibles aplicaciones en el Ámbito de la energía,” *ENERLAC*, no. 2, Dec. 2017.
- [53] Criptonoticias, “Qué es bitcoin (btc),” 2019. [Online]. Available: <https://www.criptonoticias.com/criptopedia/que-es-bitcoin-btc/>

- [54] C. Pastorino, “Blockchain: qué es, cómo funciona y cómo se está usando en el mercado,” Sep. 2018. [Online]. Available: <https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/>
- [55] I'MNOVATION, “Qué es el blockchain y cómo funciona,” s.g. [Online]. Available: <https://www.imnovation-hub.com/es/transformacion-digital/que-es-blockchain-y-como-funciona-esta-tecnologia/>
- [56] J. M. Lacarte, *Dinero, Bitcoin, Criptomonedas y la Blockchain: ¿Qué está sucediendo?* CreateSpace Independent Publishing Platform, 2018.
- [57] N. Rodriguez, “Algoritmos de consenso: la raíz de la tecnología blockchain,” Sep. 2018. [Online]. Available: <https://101blockchains.com/es/algoritmos-de-consenso-blockchain/>
- [58] M. Andoni et Al., “Blockchain technology in the energy sector: A systematic review of challenges and opportunities,” *ELSEVIER*, vol. 100, pp. 143–174, Feb. 2019. [Online]. Available: <https://doi.org/10.1016/j.rser.2018.10.014>
- [59] W. Diffie M. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. 22, pp. 644–654, Nov. 1976. [Online]. Available: <https://doi.org/10.1109/TIT.1976.1055638>
- [60] A. Castor, “A (short) guide to blockchain consensus protocols,” May 2017. [Online]. Available: <https://www.coindesk.com/short-guide-blockchain-consensus-protocols/>
- [61] K. L. Brousmiche, A. Durand, T. Heno, C. Poulain, A. Dalmieres, E. B. Hamida, , “Hybrid cryptographic protocol for secure vehicle data sharing over a consortium blockchain,” . *IEEE Conf. Internet Things*, pp. 1281–1286, Aug. 2018. [Online]. Available: [https://doi.org/10.1109/Cybermatics\\_2018.2018.00223](https://doi.org/10.1109/Cybermatics_2018.2018.00223)
- [62] M. Sebastián, “Desarrollo de una aplicación con hyperledger y composer,” Jun. 2017.
- [63] Hyperledger, “Introduction,” s.g. [Online]. Available: [https://hyperledger-fabric.readthedocs.io/en/latest/fabric\\_model.html](https://hyperledger-fabric.readthedocs.io/en/latest/fabric_model.html)
- [64] E. Chen, “An approach for improving transparency and traceability of industrial supply chain with blockchain technology,” Oct. 2016. [Online]. Available: [trepo.tuni.fi/handle/123456789/25401](https://trepo.tuni.fi/handle/123456789/25401)
- [65] F. Lardinois, “Microsoft launches visual studio code, a free cross-platform code editor for os x, linux and windows,” Apr. 2019. [Online]. Available: <https://tcn.ch/2xpqjdm>
- [66] L. Frantzell, “Best practices: Creating a successful blockchain application,” Dec. 2019. [Online]. Available: <https://developer.ibm.com/technologies/blockchain/articles/from-vision-to-reality-creating-a-successful-blockchain-application>

## Appendix 1.

- **API Application:** Acronym Programming Interface, is a set of protocols, routines, functions and / or commands that programmers use to develop software or facilitate the interaction between different systems.
- **Bitcoin:** Digital currency created for use in peer to-peer online transactions, created in 2008 by Satoshi Nakamoto.
- **Blockchain:** Digital database containing encrypted information that can be used and shared simultaneously in a large decentralized public access network.
- **Cryptocurrency:** Any form of currency that exists only digitally, without a central issuing or regulatory authority, since it uses a decentralized system to record transactions and manage the issuance of new units. It is based on cryptography for fakes and fraudulent transactions.
- **Encryption:** Process of using an algorithm to transform information and make it illegible for unauthorized users. This encrypted data can only be decrypted or made readable with a key.
- **Mining:** It is an integral part of the cryptocurrency ed that performs two important functions: first, it is used to generate and release new cryptocurrency tokens for circulation, and secondly it is used to verify, authenticate and then add network transactions in progress to a public ledger.
- **Node:** A node is an intersection / connection point within a network.
- **Assets:** What you put and search for on the blockchain, using smart contracts.
- **Shared ledger:** The ledger records the state and ownership of an asset.
- **Smart contract (or chaincode):** Hyperledger Fabric smart contracts are called chaincode. Chaincode is software that defines assets and related transactions; in other words, it contains the business logic of the system. Chaincode is invoked when an application needs to interact with the ledger. Chaincode can be written in Golang or Node.js.
- **Ordering service:** The ordering service packages transactions into blocks and guarantees the transaction delivery in the network. Key ordering services are Raft and Kafka.
- **Peer node:** Peers are a fundamental element of the network because they host ledgers and smart contracts. A peer executes chaincode, accesses ledger data, endorses transactions, and interfaces with applications. Some peers can be endorsing peers, or endorsers. Every chaincode may specify an endorsement policy, which defines the necessary and sufficient conditions for a valid transaction endorsement.



- **Channel:** Channels are a logical structure formed by a collection of peers. This capability allows a group of peers to create a separate ledger of transactions.
- **Cluster:** A set of machines, called nodes, that run containerized applications managed by Kubernetes. A cluster has several worker nodes and at least one master node.
- **Container:** A lightweight and portable executable image that contains software and all of its dependencies. Containers decouple applications from underlying host infrastructure to make deployment easier in different cloud or OS environments, and for easier scaling.