



Carlos Soeima

**Sistema de Gestão de Reclamações Baseado em
Blockchain**

Blockchain Based Complaint Management System



Universidade de Aveiro
Ano 2021

CARLOS SOEIMA

**Sistema de Gestão de Reclamações Baseado em
Blockchain**

Blockchain Based Complaint Management System

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia de Computadores e Telemática, realizada sob a orientação científica do Professor do Doutor Hélder José Rodrigues Gomes, Professor Adjunto da Escola Superior de Tecnologia e Gestão de Águeda da Universidade de Aveiro.

o júri

presidente

Prof. Doutor Paulo Jorge Salvador Serra Ferreira
professor associado da Universidade de Aveiro

Prof. Doutor Filipe Alexandre Pais de Figueiredo Correia
professor auxiliar da Faculdade de Engenharia da Universidade do Porto

Prof. Doutor Hélder José Rodrigues Gomes
professor adjunto da Universidade de Aveiro

agradecimentos

Aproveito esta oportunidade para expressar o meu agradecimento às pessoas que contribuíram para que este trabalho fosse possível.

Aos meus orientadores por partilharem a sua experiência, conhecimento e disponibilidade para me guiarem no desenvolvimento deste projeto.

À minha família que nunca me deixou sentir a falta de qualquer tipo de apoio ou condições durante o meu percurso académico.

Aos meus amigos com quem cresci e aprendi lado a lado durante estes últimos anos e um especial obrigado àqueles que me acompanharam e incentivaram durante estes tempos de isolamento onde manter o foco se tornou numa das tarefas mais árduas.

palavras-chave

Blockchain, Reclamações, Sistemas Distribuídos, Gestão

resumo

Os sistemas de gestão de reclamações existentes visam estabelecer uma linha de comunicação entre o consumidor e o provedor de serviços para facilitar uma interação saudável entre ambas as entidades de forma a chegarem a uma solução, se for o caso. Estes sistemas apresentam características que podem desmotivar o cliente de submeter uma reclamação, tais como serem administrados pelas entidades cujas reclamações são dirigidas ou não incluírem uma autoridade reguladora no processo de reclamação.

Este estudo pretende apontar essas debilidades e propôr um método alternativo de processar reclamações de forma a que haja um maior envolvimento do cliente, provedor de serviço e da autoridade reguladora e um equilíbrio de poder entre as entidades.

Para esse efeito, a solução proposta é baseada na tecnologia blockchain que alicerça as cryptomoedas e são analisadas as suas mais valias e desvalias no contexto em questão.

keywords

Blockchain, Complaints, Distributed Systems, Management

abstract

The existing complaint management systems aim to establish a line of communication between the consumer and service provider to facilitate a healthy interaction in order for both entities to come to an agreement, if that is the case. These systems present characteristics that may demotivate the customer from submitting a complaint, such as being administered by the very entities that the complaint is aimed at or not including a regulator authority in the complaint process.

This study intends to point out those debilitations and propose an alternative method of processing complaints in a way that the customer, the service provider and the regulatory authority are more involved in the process and a better power balance between these entities.

To that effect, the proposed solution is based on the technology that serves as the foundation for cryptocurrency and evaluate the pros and cons of applying said technology to this use case.

Contents

1. Introduction	5
1.1 Motivation	7
1.2 Objectives	8
1.3 Contributions	8
1.4 Document Structure	9
2. State of the art	11
2.1 Brief History	11
2.2 Complaint Handling	12
2.2.1 Livro de Reclamações (Complaints Book)	13
2.2.2 Livro de Reclamações Online Platform	15
2.2.3 Better Business Bureau	16
2.2.4 Portal da Queixa (Complaint Portal)	18
2.2.5 Deco	20
2.3 Discussion	21
2.3.1 Customer Authentication	21
2.3.2 Registry Integrity	22
2.3.3 Information Visibility	23
3. Blockchain	25
3.1 How does blockchain work	25
3.2 Peer-to-peer (P2P)	28
3.3 Consensus	29
3.4 Types of blockchain	30
3.5 Smart Contracts	31
4. Solution Proposal	33
4.1 Use-case Scenarios	33
4.2.1 Scenario 1	33
4.2.2 Scenario 2	34
4.2.3 Scenario 3	35
4.2.4 Scenario 4	36
4.2 State Diagram	39
4.3 Visibility and Accessibility	42
4.4 Integrity and Transparency	43
4.5 Identity	43
4.6 File Transfer	44
4.7 Comparison with State of the Art	45

5. Implementation	47
5.1 Blockchain selection	47
5.2 Tools	50
5.2.1 Hyperledger	50
5.2.1.1 Hyperledger Fabric	50
5.2.1.2 Hyperledger Composer	51
5.2.2 IPFS	54
5.3 Business Logic	55
5.4 Transactions	59
5.5 Access Rules	60
6. Results	63
6.1 Creating/Adding the Participant	63
6.2 Use-case Test	66
6.3 Ending Notes	73
7. Conclusions	75
7.1 Future Work	76
8. References	79

List of Figures

Figure 2.1 - Livro de Reclamações workflow.....	14
Figure 2.2 - Livro de Reclamações Online.....	15
Figure 2.3 - BBB complaint submission workflow.....	18
Figure 2.4 - Portal da Queixa.....	20
Figure 3.1 - Chain of blocks	30
Figure 3.2 - Tampering a block.....	31
Figure 3.3 - Types of blockchain.....	35
Figure 4.1 - Scenario 1 workflow diagram (No Regulator Intervention)	38
Figure 4.2 - Scenario 2 workflow diagram (Illegitimate complaint, Regulator agrees).....	39
Figure 4.3 - Scenario 3 workflow diagram (Regulator is requested, settles the complaint for the Customer).....	40
Figure 4.4 - Scenario 4 workflow diagram (Complaint gone inactive, Regulator archives the complaint)	41
Figure 4.5 - General scenario workflow diagram.....	42
Figure 4.6 - State transition diagram.....	45
Figure 5.1 - Blockchain flowchart.....	51
Figure 5.2 - Blockchain architecture options.....	53
Figure 5.3 - Typical Hyperledger Composer Solution Architecture.....	56
Figure 5.4 - Web Playground.....	57
Figure 5.5 - IPFS workflow diagram.....	58
Figure 5.6 - Participant classes definition.....	60
Figure 5.7 - Asset class definition.....	60
Figure 5.8 - Enumerate with complaint states.....	61
Figure 5.9 - Class diagram of our business model.....	62
Figure 5.10 - State transitions through transactions.....	63
Figure 5.11 - Transaction function example.....	64
Figure 5.12 - Access rule definition example	66

Figure 6.1 - Creating a Participant in the registry	67
Figure 6.2 - Creating a new Business.....	68
Figure 6.3 - ID Registry.....	69
Figure 6.4 - Business Network Card example.....	69
Figure 6.5 - Complaint submission parameters example.....	70
Figure 6.6 - Complaint asset in the registry.....	71
Figure 6.7 - <i>counterOffer</i> transaction example.....	72
Figure 6.8 - IPFS extension.....	73
Figure 6.9 - IPFS Dashboard.....	73
Figure 6.10 - Complaint transition including IPFS hash.....	74
Figure 6.11 - Example file transferred through IPFS.....	75
Figure 6.12 - Complaint logs example.....	75
Figure 6.13 - Transaction record example.....	76

1. Introduction

Nowadays, almost every product and service can be purchased via the internet and 1.8 billion people are doing just that. 53% of the world's population are connected through the internet and a quarter of them is shopping via world wide web [1]. Consumerism is not just a term for high levels of consumption, referring to the frivolous acquisition of products or economic materialism, it is also a concept that the marketplace itself is responsible for ensuring social justice through fair economic practices, consumer protection policies and laws that compel manufacturers to make products safe [2]. As this marketplace coverage through online shopping grew, so did the consumers' demands for customer service quality standards. Whether it is eating at a restaurant, buying a piece of clothing at a store or ordering something from Amazon, the consumer's rights should always be preserved along with his right to express dissatisfaction towards a provided service and the responsible party, in other words, to complain.

The cost of customer acquisition, the process of bringing new customers or clients to your business, is five times the cost of customer retention [3], meaning, a company loses more if an unhappy client decides to do business with a competitor than it would by attempting to restore his trust. By doing so, the customer would become more faithful and spread his positive experience to potential new customers, in other words, good marketing.

The act of complaining dates back as far as 1750 b.C. where one side of a goods trade, not satisfied with the product received nor the attitude he was given after, decided to relay those feelings onto a clay tablet that can be found in exposition in the British Museum [4].

The way people complain and the way businesses handle those complaints vary with each culture. In the end, each customer uses the means to complain that are available to him and each establishment has its independent way of dealing with complaints. The way customers expose their complaints have since evolved to take various forms such as satisfaction surveys, complaint forms and negative reviews/ratings. Besides the entities

object of a complaint, other entities that may handle complaints can be governmental or nongovernmental organizations that aim to protect consumer's rights and educate businesses and customers on the best practices.

Most complaints can now be submitted online through numerous different platforms that serve similar goals such as creating a bridge between the business and the consumer so that they can sort out a resolution for the complaint (and also pressure the companies to acknowledge the customer), but also divergent features such as statistics gathering and rating profiles.

Every online exchange is dependant on a trusting party to be truthful, Facebook can tell us that our life events and posts are being shared only with our friends, an email service provider telling us that our email has been delivered to the desired destination, a bank could be saying that our money has been received by our dear ones in a remote country. We live our life precariously in the digital world relying on third parties for security and privacy of our digital assets, but alas, forgetful that even they are propitious to hackers, manipulation and compromised information [5].

Blockchain is one of the answers to this trust problem and it accomplishes this without compromising the integrity of the digital assets and privacy of parties involved, revolutionizing the online transaction status quo with a distributed consensus where every event is accounted for and verifiable at any time in the future.

A blockchain is mostly known as the technology that underpins digital currency such as Bitcoin and Ethereum and continues to expand to other applications in non-financial sectors. It is basically a decentralized database in which new additions or changes to it that are recorded are seen as blocks which are linked and secured through the use of cryptographic hashes. Some of the blockchain's properties are the persistence and immutability of the data recorded in it which is supplied by the chain of hashed blocks, once a piece of data changes, the value of the subsequent hashes will also be different, rendering the blockchain invalid. The blockchain would be invalid because it is shared in a

Peer-to-Peer network, each node has a copy of it and, through a consensus protocol, the peers decide as a whole if a block should be accepted or not into the chain, keeping all records synchronized. A successful tampering of a piece of data in a blockchain would require a computation of a new hash for the adulterated block, the computation of new hashes for each block that followed it and the ownership of more than 50% of the network's peers to be able to accept the change into the blockchain, this is called the 51% attack.

As the complaint systems stand, most of them are owned and administered by companies or organizations and that gives them a great deal of power compared to a customer, meaning, they have full control over what goes on inside the system enabling them to manipulate complaints or handle user's private data any way they want. We believe blockchain could mitigate these critical factors and bring more transparency and integrity to a complaint system since it has a P2P architecture, record immutability and traceability, customers will be able to submit their complaint themselves and monitor it, verifying that it was not tampered with.

1.1 Motivation

As said before, consumer's rights should be protected and a complaint management system that provides a better power balance between the customers, businesses and regulators of the marketplace should be created to help the consumer not feel intimidated when submitting a complaint.

A lot of the interest for blockchain technology came from the growth of the cryptocurrency in recent years, this curiosity expanded to what other fields could blockchain also be of use.

Unifying both topics could result in a relevant enough design capable of opening new

avenues for complaint systems in the future and even blockchain technology applications for other sectors.

1.2 Objectives

The main purpose of this study is to design and develop a system stripped of any organization/company total ownership with a defined set of rules to control the participant's access level, where a customer should not depend on a third-party to submit his complaint or tell them how the complaint process is going, while keeping sensitive and proprietary information safe.

In the end this project should allow for an evaluation of how the blockchain technology fared in this context.

1.3 Contributions

The combination of blockchain technology and a new design of a complaint management system allowed for a more proactive participation from the consumer in the complaint procedure while making the latter more transparent and secure. Limiting the users' access just enough for them to ensure that the activity of other peers does not compromise the integrity of the network without jeopardizing their privacy, finding this balance proved to be crucial in our system and in most blockchain based solutions.

1.4 Document Structure

The organization of this document is as follows: In Chapter 2 (State of the art) we introduce the reader to the problem at hand and present the state of the art in complaint's handling; in Chapter 3 (Blockchain), we describe the main concepts of blockchain and how they work; in Chapter 4 (Proposed Solution), we discuss in what ways blockchain would bring benefits to the complaints context and proposes a solution architecture; in Chapter 5 (Implementation), we describe the implementation of the developed system; in Chapter 6 (Results) we follow a scenario while showcasing the final product; and finally in Chapter 7 we reflect on the outcomes of our investigation.

2. State of the art

Organizations that deal with people, sell a product, or provide a service, will likely face complaints in their lifetime [6]. A complaint is usually defined as “an expression of dissatisfaction on a consumer’s behalf to a responsible party” [7]. Generally, it is issued upon a negative transaction experience by a customer.

2.1 Brief History

The first ever recorded complaint dates back to Babylonia, some time around 1750 B.C. In the British Museum lies an emotionally inscribed clay tablet containing a customer service complaint after the author, named Nanni, received a shipment of copper ore of an inferior grade to what was promised to him, after some annoying delay and in a damaged condition. The seller also refused to reimburse the money to several messengers sent by the customer, treating them with contempt [4].

Fast forward a couple of millennia and we’ve transitioned from engraving clay to filling out paper forms and surveys. Typically, consumers have been issuing complaints directly to vendors (aka service providers), or the designated bureaus, by filling out a complaint form or by directly speaking to the vendor [8]. This method is performed in person at the time and place where the offense took place, the complaint is always private and stored in archive, the complaint handling is exclusively controlled by the complained party.

If it were today, Nanni would have the assistance of government and nongovernmental organizations while issuing a complaint. Not only do they enforce good behaviour practices upon businesses towards customers, avoiding a complaint altogether, but in the case of an offense, they are able to provide a platform to assist the customer in resolving the dispute, to publicly (or not) voice the consumer’s experience and back it up using their

standing, conduct investigations and apply sanctions to unregulated establishments, while providing useful information about companies such as ratings, previous incidents and reviews.

Nowadays, in a social media era, consumers share all kinds of experiences, positive or negative, but mostly negative. Everything is rateable, from restaurants, hotel rooms, items for sale to the reviews themselves. With any device that has internet access, a complaint can be issued through an App or website, which is perfect for consumers that do not like to engage in this sort of situation due to inconvenience or embarrassment [8]. Ratings can be beneficial or harmful to a company, since potential customers often make decisions based on those values and would rather avoid a badly critiqued service. Companies are also motivated to provide good services to increase their rating, and resort to damage control if a complaint is received in order to prevent further rating decay. Negative reviews/ratings are seen as complaints and endanger the reputation of a business if not handled promptly and correctly.

2.2 Complaint Handling

To protect consumers, like Nanni, governments and non-profit consumer organizations exist and provide means to inform customers about the products and services of a vendor, reinforce standards for how businesses should treat the public in a fair and honest manner, process the public's complaints and take measures accordingly [8][9].

After a displeased customer issued a complaint to some of these organizations, it is incorporated with other complaints concerning the particular vendor, compiling a profile or report describing its reputation [8], which may be public or not. Having this repository of complaints publicly available also motivates the companies to reach out and restore the customers' trust. If the complaint is resolved, the consumers are likely to come back and

even spread the positive (previously negative) experience to other potential clients through word-of-mouth. On the other hand, if a customer remains unanswered and unhappy, it may signify the loss of its patronage and the gain of a competitor company.

The cost of customer acquisition is five times greater than the cost of customer retention (Lee Resources 2010, [3]), making perfect sense for companies to focus on restoring a consumer's satisfaction.

What follows are some of the methods/organizations that regulate and fiscalize the trade market industry, mostly in Portugal, and some of their main features.

2.2.1 Livro de Reclamações (Complaints Book)

A case implemented in Portugal, named Livro de Reclamações, is a particular one. It exists both in physical and digital forms, which will be addressed further.

What is so special about this method is its enforcement via legislation. The book is purchasable and it is mandatory by law that every official commercial establishment must have it available at all times and be given to a customer upon request. The right to issue a complaint is considered an act of citizen rights' defense. The book is typically used as a last resort if a verbal settlement between both parties is not reached on the spot. Upon the complaint submission, the bureau (the one responsible for the economic sector that the service was provided in) will be notified and proceed with further investigations, applying sanctions if needed. The book's integrity is also part of a properly regulated establishment, it must contain twenty five pages with two duplicates each [10].

Whenever a customer wants to issue a complaint, all it takes is to fill out the form in one of the book's pages with the complainant personal data (name, email, address, postal code, phone number and citizen identification number), information of the service provider

(name, CAE code, which represents a classification of the economic activity the business performs, address and postal code) and the reason for the offense along with the time and date of occurrence [11]. This procedure takes place at the establishment, accompanied by a staff member that is obliged to assist the customer in any piece of information related to the business.

The pages are made from carbonless copy paper, which means that two duplicates of that sheet of paper are created when someone writes on them; the first one should stay with the consumer that issued the complaint, the second should remain in the book belonging to the establishment and the original should be sent, within a defined period of time by the responsible management of the establishment, to the corresponding responsible authority, department or bureau which will take action and manage the procedure from then on.

In Figure 2.1 shows a generic workflow of a complaint issuing through the Complaints Book.

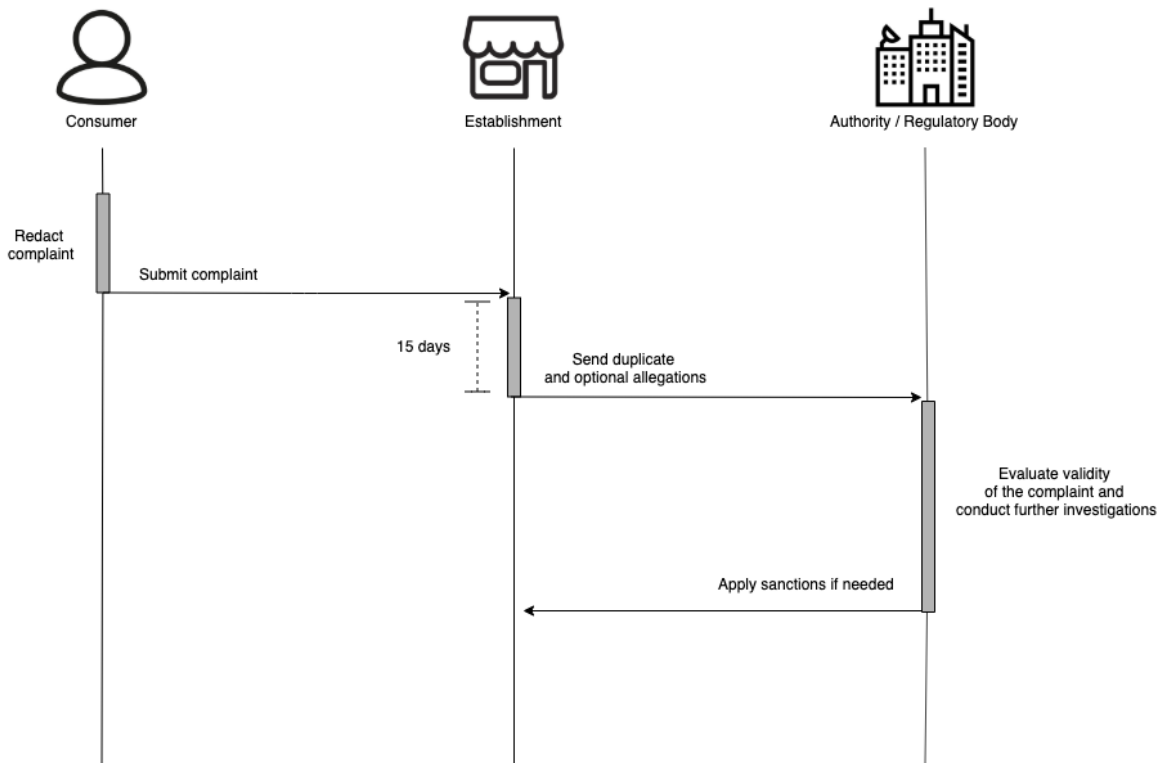


Figure 2.1 - Livro de Reclamações workflow.

2.2.2 Livro de Reclamações Online Platform

The screenshot shows the '1. Identificação do reclamante' (1. Identification of the complainant) step of the online complaint process. The page has a dark red header with the 'LIVRO DE RECLAMAÇÕES' logo and navigation links for 'Ajuda ao utilizador' and 'ajuda'. Below the header, there are buttons for 'Registar Operador' and 'Login'. The main content area is white with a red border. It features a progress indicator with four steps, the first of which is active. A text box explains the use of the 'Cartão de Cidadão / Chave Móvel Digital' for authentication. The form is divided into sections: 'DADOS PESSOAIS' (Personal Data) with fields for Name, Surname, NIF, Document Type, and Document Number; 'RESIDÊNCIA' (Residence) with fields for Country, Municipality, Door, Floor, Postal Code, and Locality; 'MORADA DE FORNECIMENTO DO SERVIÇO' (Service Provider Address) with a checkbox for indicating the address; and 'CONTACTOS' (Contacts) with fields for Fixed and Mobile Phone Numbers. A 'Seguinte' (Next) button is at the bottom right. The footer contains logos for the Portuguese Republic, Consumer, INCM, and SIMPLEX+, along with a 'Política de privacidade' (Privacy Policy) link.

Figure 2.2 - Livro de Reclamações Online.

An online version of Livro de Reclamações is operational in www.livroreclamacoes.pt/inicio/reclamacao, this provides the consumers that do not like confrontation an outlet to issue a complaint in a similar way one would have by using the physical Livro de Reclamações.

A customer begins by inserting his email address and verifying it using the link that is sent to them. This will not create an account, it serves as an email validation step to prevent spamming and an opportunity to send the user some further information about what one is agreeing to when submitting a complaint according to the law, such as data protection

guidelines (e.g. GDPR guidelines), who will receive the complaint along with the user's personal information, what will it be used for and for how long it will be held (usually 3 years, the amount of time the physical Livro de Reclamações has to be archived for). Upon pressing the given link, the user will be redirected to the web page where they will be able to redact the complaint.

The data required is the same as in the original Livro de Reclamações, although the online version has the option to authorize the service provider to access the residence and contact information of the customer. The next step is identifying the establishment, which is done through a search engine in the platform, it should provide every business registered as they are obligated to own both versions of the book (physical and digital), and name the respective regulation authority in charge of handling the complaints in the service provider's business sector. The third step is the issuing of the offense, consumers are able to categorize the complaint and name the specific service at fault (e.g. Internet service, prices and advertising campaign or product quality), redact complaint (with a maximum of 2000 characters) followed by additional information, such as a contract identification number or even a reference to a previously complaint issued on the same subject. Since the ticket is not filled out in loco, consumers also have the option to attach files, usually a proof of the actually provided service or relevant documents/pictures, such as purchase receipts or photos of the scene. The final step is to give a chance to the user to verify all the information before submitting the complaint.

As stated in the email sent by the platform to the user, the complaint will be redirected to the service provider or business and to the authority that represents the respective economic sector, the latter will process it and perform investigations or apply sanctions to the extent of the law.

2.2.3 Better Business Bureau

The BBB is a private, non-profit organization in North America that serves as a brand of trust amongst marketplace entities. They set standards and best practices for trustworthy and healthy interactions between customers and vendors.

Companies that abide by those regulations receive a seal of approval by the BBB that invokes immediate reliability within the consumer base.

Not only do they analyze complaints sent to them, they also provide an online public database where a customer can search any listed establishment and check their profile which contains their reviews, complaints filed, if it is BBB accredited and a rating.

A complaint ticket filing begins with the consumer naming the nature of the complaint, if it is related to a vehicle, cellphone, advertising, policies and practices of a business, etc. Next, through a search engine, the user will have to identify the establishment to which they wish to complain. After selecting the correct facility, the user will be redirected to a domain corresponding to the location of the business, due to different laws applied in different states and countries (i.e. BBB Northwest + Pacific, BBB of Northeast California). If the facility is not registered, the user is able to fill another form with the information for that particular establishment. The next step requires the user's personal information, such as name, residence information, contact information and email address; if the consumer does not have the latter, he will have to file the complaint in writing with the local BBB where the business is located. Then, the user has 2000 characters to type his complaint and another 1000 for the desired outcome. They are allowed to select the type of settlement they wish for, but the bureau will not pursue certain resolutions, which are described in detail within the complaint filing procedure (e.g., perform inspections, filing lawsuits, issue fines, change of store policies, etc). All that is left is to fill out additional optional complaint details, such as contract number, name of the salesperson, date of the purchase/service provided and other. The final step serves to review all the information one last time before submitting it and sign waivers (using check boxes) allowing the user's

personal information to be shared with the BBB and the complaint to be publicly posted on their platform.

After a complaint is received, the BBB processes it, relays it to the business at issue and demands a response within 14 days. If a response is not received within that time period, a follow-up letter is sent. The customer is notified of the response and is asked to respond back. Generally, a complaint will be closed within approximately 30 days after its filing.

Upon closing a complaint, the BBB will assign it one of the following statuses:

- Resolved: The complainant verified that the issue was resolved to their satisfaction.
- Answered: The business addressed the issues within the complaint, but the consumer either (a) did not accept the response, OR (b) did not notify BBB about their satisfaction.
- Unresolved: The business responded to the dispute but failed to make a good effort to solve it.
- Unanswered: The business failed to respond to the dispute.
- Unpursuable: BBB is unable to locate the business.

Depending on the outcome of the complaint, the company's rating on the BBB registry, represented by a letter grade or 0-100 point score, will be affected [12]. In Figure 2.2 we can see a workflow of a complaint issuing through BBB.

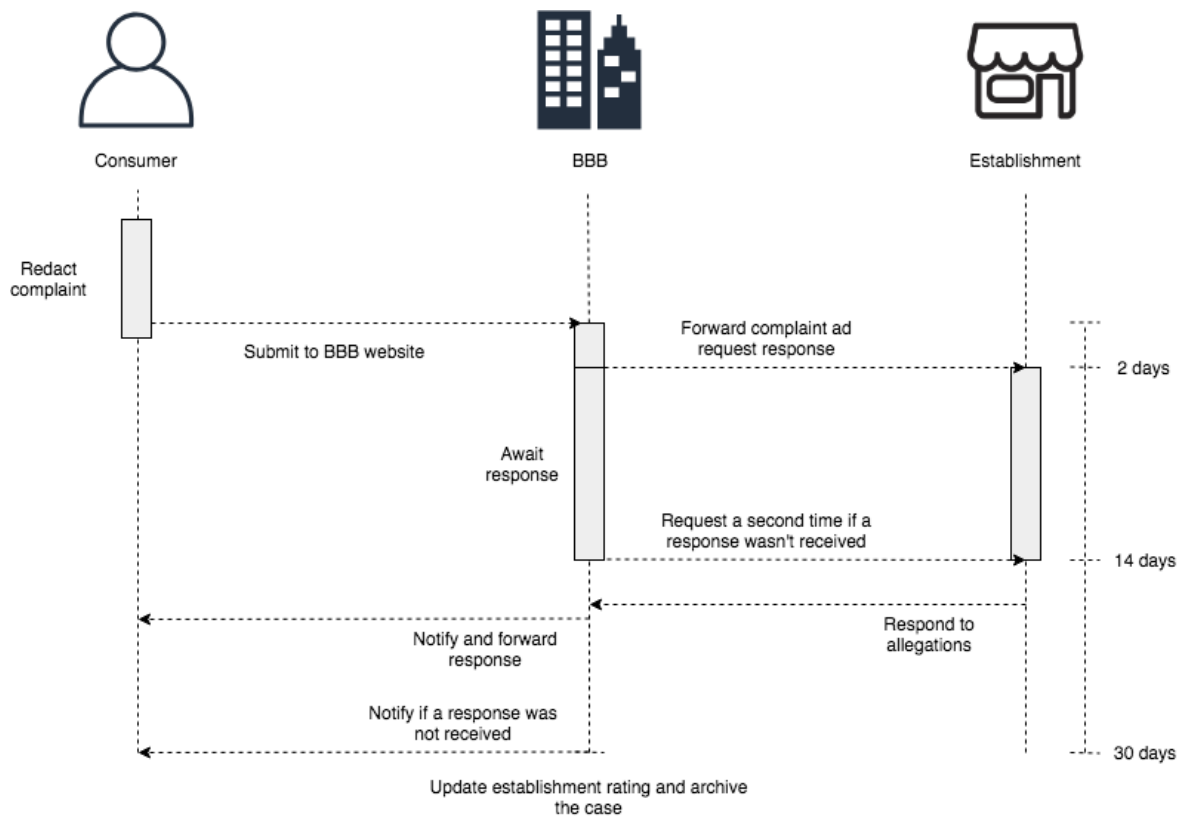


Figure 2.3 - BBB complaint submission workflow.

2.2.4 Portal da Queixa (Complaint Portal)

Portal da Queixa is a social network for online consumers that also originated in Portugal.

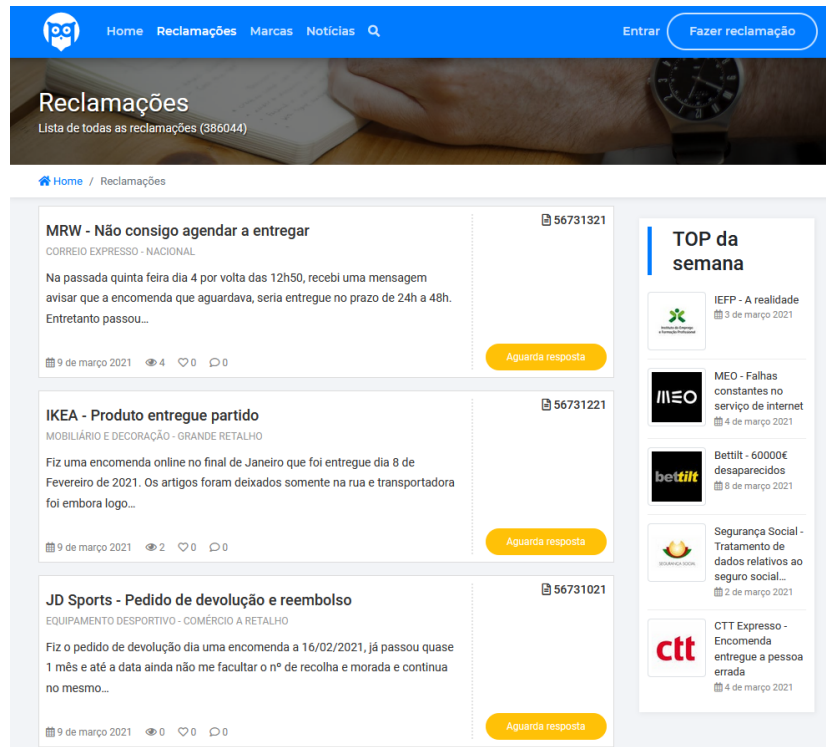


Figure 2.4 - Portal da Queixa.

In this web platform it is possible to follow the complaints issued by a company, fill out our own, follow other complainants' resolution procedure and check the brands' satisfaction index, which represents their performance in interacting with the customer who has already filled the complaint. This index is measured on a 0 to 100 range and is calculated using a public formula, allowing for a quick comparison between brands, which plays an important role in the customer's decision of where to take their business.

The website has five different views: Activity, Complaints, Brands/Businesses, News and Results.

The Activity tab is a feed of complaints or responses to complaints, every action in the

network is registered and publicly visible to any user. Each item in the feed contains the profile of the business that the complaint is addressed to, the name or alias of the user complaining, a preview of the complaint (can be seen in full by clicking on it), the status of the complaint (ranging between “Awaiting Response”, “In Progress”, “Resolved” and “Unsolvable”), a like button, a comment button and a bell icon that allows the user to follow that complaint.

The Complaints tab displays a list of the complaints in chronological order, having the same details as before, only omitting the name/alias of the name from the preview.

The Brands/Businesses tab shows all companies registered in the website, categorized by business sector and ordered by ranking; these can be filtered by category for easier search. This ranking is dictated by a satisfaction index score and the response rate (amount of times they reply given a number of complaints).

The News tab contains articles that could be of interest to consumers.

The Results tab presents the website’s statistics, such as graphs, with the amount of monthly complaints and their respective statuses, values regarding the number of users, complaints, businesses and responses recorded in the system and a top ten of companies with most complaints and best response rate in the last 30 days.

In order to complain, a user has to create an account or log in using Facebook. The filling is divided in three steps: identifying the business, which is done by a search engine with the registered companies; adding personal information, such as full name, email address, NIF, phone number and, optionally, home address (every piece of information in this step is kept private from the feed posts and will only be given to the company subject to the complaint); writing the motive, characterize the state of mind of the user during the filling of the complaint, include a reference (account number or receipt number), describe the offense, supply relevant details to the company, propose a resolution and attach documents (evidence or identification) (with the option of keeping them also private).

During the development of this State of the Art research, the Portal da Queixa platform switched to a blockchain implementation. Taking advantage of BaaS (Blockchain-as-a-Service), the platform administrators allied themselves with a company (www.hash.business) that manages their data and registers it in the Ethereum Blockchain, this way they could guarantee maximum safety and transparency to their users through the immutability of their complaints and ratings.

Although this platform already serves as one proof of concept of blockchain applied to complaint management, it still lacks the involvement of a regulator authority in the complaint process, which is one of the requirements for this study.

2.2.5 Deco

Deco is the oldest and biggest consumer defense association in Portugal, with over 380 thousand members [14]. It began as a paid magazine subscription that provided articles, reviews, evaluations and testing of products and services. Since then, it has gained the approval and financial aid of the government. Now, it has its own website, where they recommend products or services, advertise campaigns with partners and collect complaints from consumers.

In order to complain, a consumer needs to register on the website with an email address (that will receive a verification email) or a social media account. To start the complaining procedure, the user has to identify the business that offended him by introducing its name on a search engine, then provide a complimentary reference to facilitate the identification of the conflict, such as a client number, receipt id, NIF or any other form, and supply a phone number to be used in further communications.

The complaint will require a title and gives the user 6000 characters to describe the motives, the consequences of the offense caused and what has already been done to

remedy the situation. The consumer is able to select one or more desired outcomes and allow the complaint to be made public or not. In the latter case, attached documents and personal information will not be disclosed. The next step allows for document attachments related to the complaint, such as contracts, receipts, letters or proofs of payments. After a final review of the complaint, the user can submit it, leaving it to Deco to notify the company and await further developments.

2.2.6 Other studies

At the time of development of the State of the Art, there were no clear existent studies of blockchain applied to complaint systems to start from. Near the end of this dissertation appeared two new studies which were not taken into account while developing this project, but we figured they could still add value to our own dissertation.

One of the systems manages criminal related complaints that are addressed to the Police [39] and the second one handles the processing of complaints of citizens towards a municipality corporation [40]. Both of them aim to propose a revitalized complaint system, catered to their respective context and requirements, that supports a decentralized network, eliminating central points of vulnerability making the system more secure, transparent and trustworthy.

Both of these works were implemented using Ethereum, a public blockchain, which differs slightly from our approach that will be tackling the problem using a hybrid blockchain with more access conditions that aim to protect the system's users' data.

2.3 Discussion

There are a variety of platforms and systems available to the consumers for their ventings and complaints, each of them with their own independent handling process, some might even be equal, creating redundancy. In this reflection are mentioned some of the core features that the state of the art presents and an analysis of their importance.

2.3.1 Customer Authentication

This segment is possibly the most sensitive of the entire complaint filing process. The customer's identity is needed for several reasons, the establishment might attempt to reach the consumer after the complaint to try and resolve the dispute (by offering compensation or a refund, for example) and will need his contact information or residence address, a regulatory body might want to proceed with further investigations with a business and needs witnesses. A complaint can not be legitimized without an identity behind it (assuming it is a real one), by signing a name and giving civil identification data is holding responsibility for what is claimed in the complaint, this demotivates complaints with defamation purposes or denigrates a company's reputation. Being able to file a complaint in person is the customer authentication method used in Livro de Reclamações, the staff will allow a consumer to file the complaint freely as long as he is in possession of his civil identification so it can be validated, as of that moment, the consumer was in fact, at the establishment and can exert his right to complain about a poor service or other displeasure. From a customer's point of view, this procedure puts him at a disadvantage since he has to come face to face with a staff member that, most likely, will not appreciate the critique, at an hostile environment (the establishment, "enemy territory") and leave his personal information registered in the book which the business will have unlimited access to. All these factors leave a consumer vulnerable and possibly less willing to file a complaint.

On the other hand we have online authentication implemented in the online version of the

platform. The Livro de Reclamações Online relieves the customer from such pressures by allowing him to file a complaint from anywhere he finds most comfortable, although the identification procedure is not enough to prove that the customer was ever a consumer in the first place. The information provided is not cross checked as it would be with the staff member with a civil identification card in hand, to file a false complaint one would only require a “throw away” email account and use false information, the system does not question it (the only validation performed is the email address). To compensate for this, the online platforms include a common feature such as attachments or optional fields to include references or documents that serve as proof that the customer was at the establishment (e.g. receipts, account numbers, NIF).

2.3.2 Registry Integrity

Another worry from a customer’s point of view is the possibility for adulteration of the complaint since they remain in possession of other parties. In Livro de Reclamações (physical version) usually one would not have a concern about this problem, upon filing an issue (complaint) it creates two duplicates resulting in three pages, one for each participating entity to hold (the customer, the business and the respective authority that handles the sector, the latter receives the original). This method prevents the business from tampering with the complaint, they would only have access to a copy and even if they managed to adulterate the original before shipping it out to the authority, the duplicate that is held by the customer is still intact. They can not get rid of the page because, by legislation enforcement, the book must contain all 25 pages and must be in storage for three years, inspections to these conditions are made and if they are not met the business is subject to heavy fines.

Although the BBB focuses on protecting consumers’ rights and acts as a dispute mediator between marketplace entities, it has been the subject of controversy for allegedly accepting payments for adulterating ratings on their website. Ultimately, this means that any business

score may be untrustworthy [13], jeopardizing the trust from the platform's users.

In regards to online platforms, each of them holds their own database to store complaints with complete control over them. The Portal da Queixa and the BBB platforms allow a consumer to publicly post their complaint, this visibility appeases users as they can check if their issue has been altered or not, they also have rating features that depend on the amount of complaints enabling competitors to submit fake ones to damage their credibility. Systems like Deco's and Livro de Reclamações Online are like a black box to their users, one does not know what becomes of their complaint. Deco is a company that does partnerships with brands to supply better deals to their members which does not inspire a lot of impartiality that is required from a party in this standpoint, a customer submits a compromising complaint against a partner and it could turn out to be a conflict of interests.

2.3.3 Information Visibility

In most of the analysed platforms it is clear that the customer should be able to choose what and what not to disclose while filing a complaint seeing as it contains sensitive personal information.

The Livro de Reclamações Online allows the user to decide whether or not the establishment will have access to his residence and contact information, by not letting the business know how to reach the customer he is actively renouncing a possible resolution, or perhaps, he does not intend to reach one. Systems that incorporate a social media feature, such as BBB and Portal da Queixa, allow the customer to choose if his complaint is posted publicly or not, having it public would benefit the platforms in terms of enriching the profiles of the businesses and by privatizing it the customer would not receive the benefits that complaint visibility brings such as other consumers relating to the issue by "liking" and "sharing" it, not taking advantage of the pressure that businesses would be put under.

As discussed above (in Registry Integrity), the platform's administrators have the ability to

control the information deposited in them but not the ownership of it. Users can never be sure to whom their information might be exposed.

3. Blockchain

Ever since blockchain technology exploded due to Bitcoin and the cryptocurrency fever its potential for both financial and non-financial applications has been truly disruptive, so much so that its been classified as the most important invention since the Internet itself or to be considered as major as the steam or combustion engine, capable of changing the world around us [5][15].

One cannot escape mentioning Bitcoin and cryptocurrency as generic examples since they're intrinsically tied to blockchain.

In 2008, a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System" was published by Satoshi Nakamoto, whose true identity remains a mystery to this day. This paper specified an electronic cash system that allowed online payments from one party directly to the other without the need of it going through a financial institution. Months later, January 2009, the first record (block) in the Bitcoin blockchain was created (mined), also known as Genesis, making public the first ever decentralized cryptocurrency [16]. May 2010 was marked by the first ever purchase with bitcoin amounting in 10,000 BTC in exchange for two pizzas. A wide number of variations of cryptocurrencies started surging given the popularity of Satoshi's vision. Nearly a decade after its release, Bitcoin reached its first highest market capitalization yet of over 850 billion dollars [17][18]. At the date of writing this document, Bitcoin's value doubled and those pizzas would've been worth over 450 million dollars.

3.1 How does blockchain work

A blockchain is a chain of blocks, each of which, containing data, a hash and the hash of the previous block. The data stored in the block depends on the purpose of the blockchain, for example, Bitcoin blocks harness data of transactions such as sender account, receiver

account and amount of currency to be transferred. A hash is used to mask original data with another value, using a hash function is applying a deterministic algorithm that, given an input, always returns the same output, meaning that if the input is changed in any way, the resulting hash will be different every time. This hash can be compared to a fingerprint, it identifies the block and all of its contents and it is always unique, just like a person's fingerprint. The final element of a block is the hash of the previous block, this creates a chain of blocks that gives blockchain one of its most characteristic properties, once a piece of information has been recorded it becomes very difficult to change it.

Giving an example, Block 3 points to Block 2 and Block 2 points to Block 1, Block 1 has no block to point to so, therefore, has no previous block hash, this is commonly referred to as the Genesis block, as illustrated in Figure 3.1.

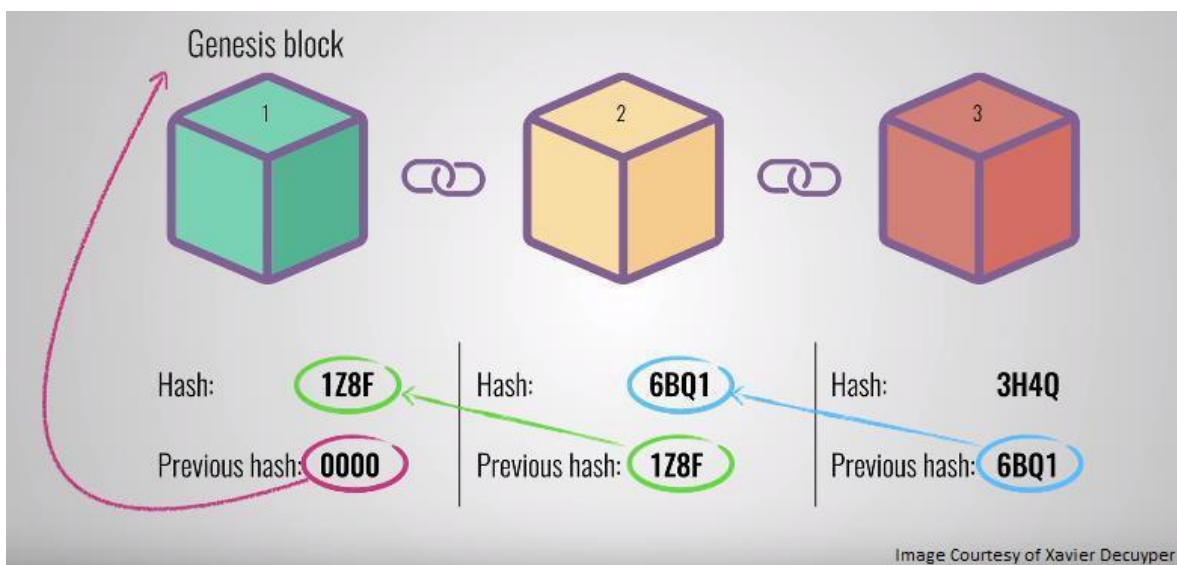


Figure 3.1 - Chain of blocks [26].

If the second block were to be tampered with, the resulting hash would be different and, consequently, make all further blocks invalid because they would point to invalid hashes, as illustrated in Figure 3.2.

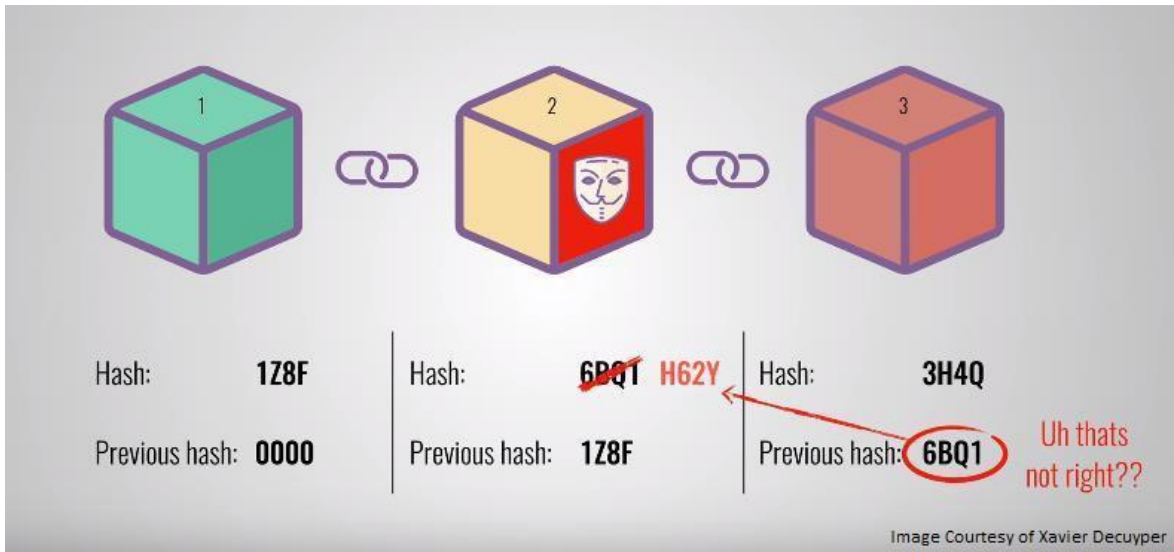


Figure 3.2 - Tampering a block [26].

If one would want to change information already recorded in the blockchain it would need to recalculate the hash for the respective block and the hashes of the following blocks in order to make the blockchain valid again.

Computers nowadays can process hundreds of thousands of hashes in a small period of time, in order to mitigate this and discourage the adultering of the blockchain there are mechanisms that increase the time and resource cost of a block creation, in case of the Bitcoin blockchain, it is used proof-of-work (referred further in the chapter). The security a blockchain provides comes from the use of chained hashed blocks, the proof-of-work required to create a block and the fact that its architecture is peer-to-peer based, distributed.

3.2 Peer-to-peer (P2P)

This technology is peer-to-peer based, a network comprised of several computers and servers that are represented as nodes. Whenever someone joins the network, they get a full copy of the blockchain which can be used to verify if everything is still in order.

This architecture allows for a decentralization of its database, no amount of data is lost if a node exits the network and quick copies are provided to a new node that joins it. The nature of P2P poses synchronization issues, in order for the network to remain consistent, every node must be up to date [19]. For example, picture Alice who makes a transaction of digital currency to Bob, since it consists of a file that can be duplicated or falsified, she can perform another transaction using the same currency for Carl, resulting in two people owning the same coin, this particular problem is called double spending.

Bitcoin, as the first implementation of blockchain, resolved it without the need of a centralized entity to verify attempts at double spending. New entries to the blockchain have to be accredited by a majority of the participants of the network and once inside, the data cannot be altered or erased. Once a new block is generated it is sent to everyone on the network, each node will verify the block to make sure it hasn't been tampered with and add it to their blockchain, this is referred to as consensus, the nodes agree on which blocks are valid or invalid, the latter will be rejected.

In order to tamper with a block, one would have to calculate the proof-of-work for that block, the proof-of-work of the following blocks and take over 50% of the P2P network to make sure the block would be accepted by the rest of the nodes, this whole procedure makes it almost impossible to successfully change any recorded information on the blockchain.

3.3 Consensus

The consensus mechanism is how the blockchain nodes come to an agreement about its

state; it ensures that the latest block is added accurately and consistently. There are numerous different consensus algorithms, the most popular being proof-of-work and proof-of-stake, explored by Bitcoin and Ethereum, the largest blockchains at the moment.

Proof-of-work (PoW): A PoW is a piece of data which is difficult (costly or time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a PoW can be a random process with low probability so that a lot of trial and error is required on average before a valid PoW is generated [20], this process is called “mining”.

Mining requires nodes to verify various transactions and compute a hash value that’s lower than a pre-established “target value”, called Difficulty Target [21]. Upon solving the block, most likely the individual holding the highest level of computing power, he can forward it on to the network’s peers, which will, in turn, verify if the answer is correct and decide if it is added to the chain. Miners are then rewarded with cryptocurrency for participating in the consensus activities.

Proof-of-Stake (PoS): PoW and PoS have common characteristics such as rewarding participants with cryptocurrency upon verifying and storing transactions. However, PoW is too expensive in terms of computing power as it is what dictates who will mine the block. With PoS the one who will mine the block depends on the amount of currency (stake) an individual owns. If a user owns 1% of the total stake of the blockchain, he will mine 1% of the blocks in a PoS consensus. Attempts to attack the network are discouraged because they would take a lot of stake to be held and therefore be mostly self-inflicting damage [20].

3.4 Types of blockchain

Blockchain splits into three different categories: Public blockchain, Private blockchain and Consortium blockchain.

Public (permissionless) blockchain: a blockchain that's completely open and public, any node can read, write, verify and participate in the consensus processes. Bitcoin and Ethereum are both examples of such blockchain which reward nodes with cryptocurrency incentives according to their contribution.

Private (permissioned) blockchain: a blockchain in which the access permissions are managed by the central authority. Often owned and used by a single organization where the writing privileges are centralized and the reading access may be public or private according to the administrators of the chain. Since it's an internal use purposed type of blockchain, the consensus protocol does not work in the same way it would with a public blockchain since it's completely owned by the organization. It is a centralized model using a distributed storage system that could be used for auditings and database management.

Consortium (hybrid) blockchain: a blockchain with both public and private features, only a pre-selected group of nodes is able to participate in the consensus process. This type of blockchain aggregates like-minded institutions such as banks, hospitals and police departments into a partially decentralized blockchain, writing and reading permissions would be managed by the core of the consortium. The Hyperledger project has many instances of blockchain one of which, Fabric, has this type of blockchain [20][22][23].

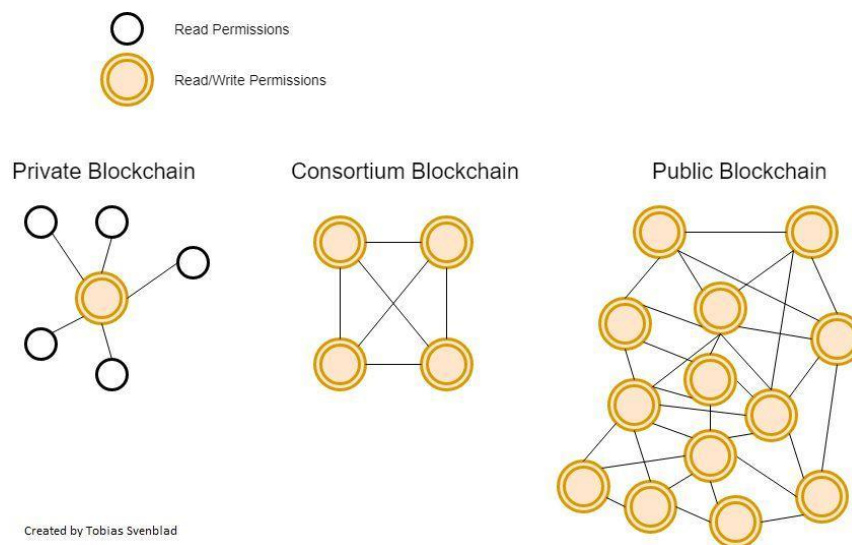


Figure 3.3 - Types of blockchain [23].

There is no one-answer-fits-all in terms of choosing a blockchain for a given context since they're very flexible [23]. In Figure 3.3 we can see an illustration of the architecture of the types of blockchains that exist.

3.5 Smart Contracts

This concept was introduced by Nick Szabo [24], smart contracts are just like real life contracts, except they're digital. They're small applications that run on blockchains which allow users to lock up assets and release them when certain conditions are met [25]. It can be thought of a stored procedure in a relational database, employing if-then type clauses with transactions.

As an example use case, we have Alice and Bob, two friends who trust each other. Alice would like to ship a pallet of goods to Bob, but she doesn't trust trucker Tom, who will carry her pallet. Tom also doesn't trust Alice, maybe she won't pay him. An agreement has to be signed between Alice and Tom so that it ensures that the payment will be done a few days after the shipment is complete. This involves legal papers, contract scans, prints,

signings, most of them performed through third parties.

With the help of smart contracts, this process can be simplified. Alice makes a payment to the smart contract on the day of cargo loading, locking her funds. Once the delivery is finished and confirmed by Bob, those funds are released by the smart contract and automatically transferred to Tom. With a GPS tracker attached to the package, Bob's confirmation wouldn't even be needed if the set rule for the contract were the final destination of the pallet [27].

Since smart contracts reside in blockchains, they inherit its features, such as immutability and distribution. Once a smart contract is submitted to the blockchain, one cannot alter its rules. Each participant holds this script in its node so they can verify if the value of others smart contract's output is valid, so no one can release funds from a contract without the criteria being met.

The main platform that deploys smart contracts is the Ethereum blockchain, and it's written in Solidity, a language exclusive for smart contract coding, similar to Javascript.

4. Solution Proposal

This chapter aims to showcase our proposal for the Complaint Management System. We begin by describing and illustrating a few use-case scenarios that represent typical complaint management flows, then a state transition diagram for the complaint processing. Then we reflect on some characteristics that are relevant to our solution proposal such as visibility, accessibility, integrity, transparency, identity and file management. We conclude this chapter with a comparison between our proposal and our analysis of the state of the art.

Our proposal is a Complaint Management System designed to allow the three types of entities (Customer, Business, and Regulator) involved in processing customer complaints, to manage complaints with a healthy power balance between them, covering a wide range of possible use cases.

The main goal is to develop a system where the visibility and management of complaints by certain entities at a given time is controlled by a pre-programmed set of rules, ensuring their integrity and user's privacy.

4.1 Use-case Scenarios

In this section, we will be describing some typical complaint processing scenarios that can happen in real life, followed by their respective activity diagrams to illustrate how they fit in the following presented state diagram.

4.2.1 Scenario 1

In this case we have the optimal scenario where the Customer and Business collaborate with one another to reach a consensus on their own and solve the complaint without needing the intervention of the Regulator (some commercial sectors do not have a

representative regulator authority, in which case, the Regulator should be a consumer protection oriented organization).

The Customer starts by submitting a complaint directed to a Business and a particular Regulator. The Business then receives the complaint and wishes to compensate the Customer, sending a solution proposal for the complaint back to the Customer. The Customer feels satisfied with the offer and accepts the solution for the complaint and later closes the issue as soon as the Business fulfills the agreement. The Regulator can see the outcome of the complaint. This scenario is illustrated in the form of a workflow diagram in Figure 4.1.

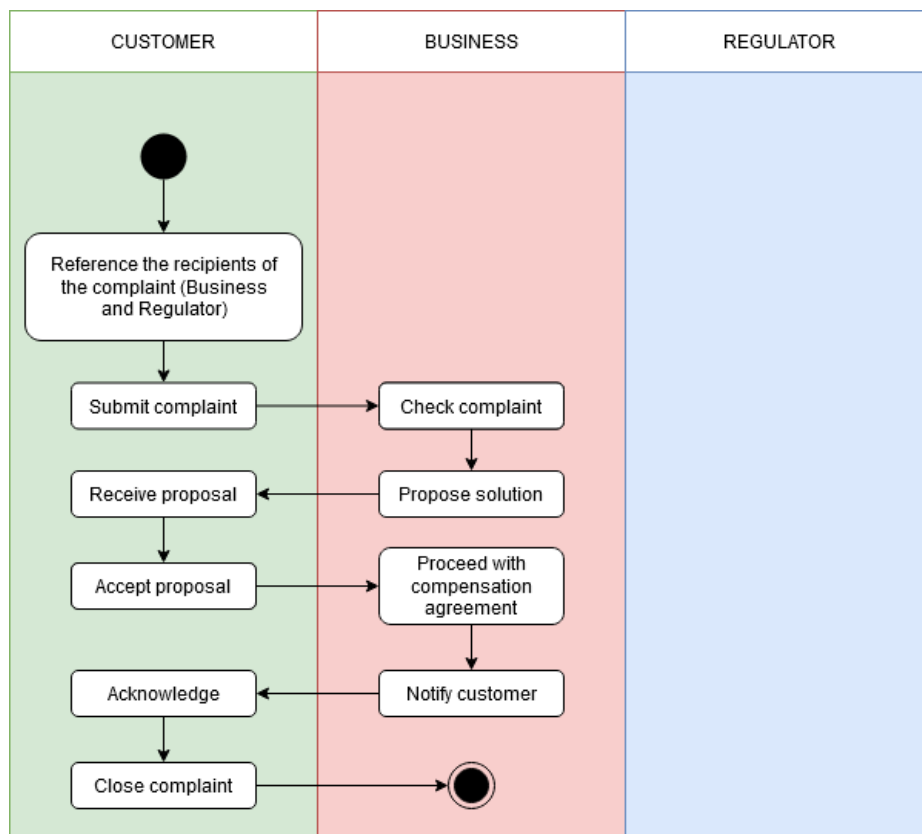


Figure 4.1 - Scenario 1 workflow diagram (No Regulator Intervention)

4.2.2 Scenario 2

In this scenario applies to illegitimate complaints (submitted for defamation for example) or complaints that do not seek compensation (submitted for negative feedback) which are relayed to the Regulator for validation and then archive.

The Customer submits a complaint, the Business receives it and after some analysis it figures that either the complaint doesn't seek compensation or the complaint is unfounded and won't proceed further, sending the complaint to the Regulator for revision. The Regulator conducts a similar analysis and validates the archive of the complaint, allowing every other entity associated with it to see the final outcome. This scenario is illustrated in the form of a workflow diagram in Figure 4.2.

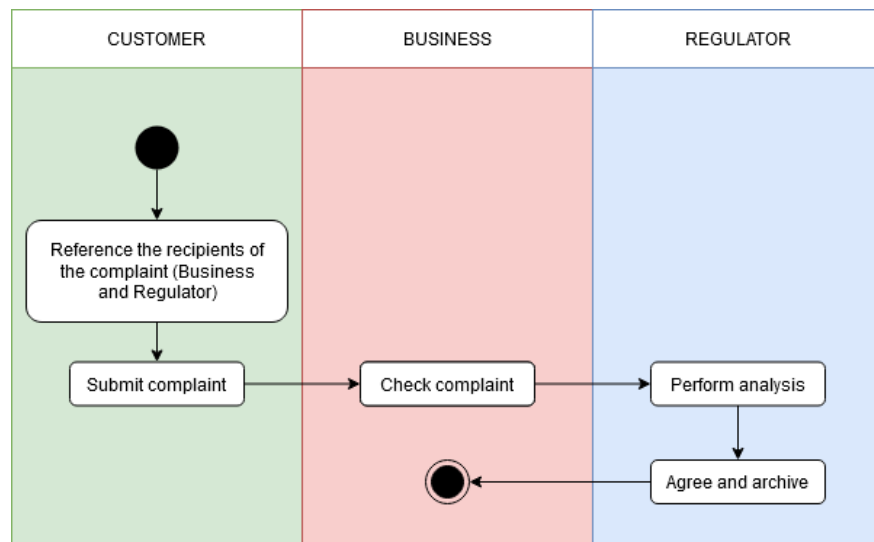


Figure 4.2 - Scenario 2 workflow diagram (Illegitimate complaint, Regulator agrees)

4.2.3 Scenario 3

In this case we mean to illustrate how a Regulator intervenes in a complaint, he could be needed for a comment or to settle the dispute.

The Customer starts once by submitting a complaint and negotiating with the Business, they exchange messages through state change transactions, this process can last indefinitely until one of the parties decides to request the Regulator to settle the matter. In this case, the Customer is the one to ask for the Regulator intervention, which ends up siding with the Customer, and solving the complaint, attaching the indemnity that the Regulator deems fair. The Customer closes the complaint whenever the compensation comes through.

Although the Regulator took the Customer’s side and solved the complaint, the Regulator could also side with the Business and archive the complaint. This scenario is illustrated in the form of a workflow diagram in Figure 4.3.

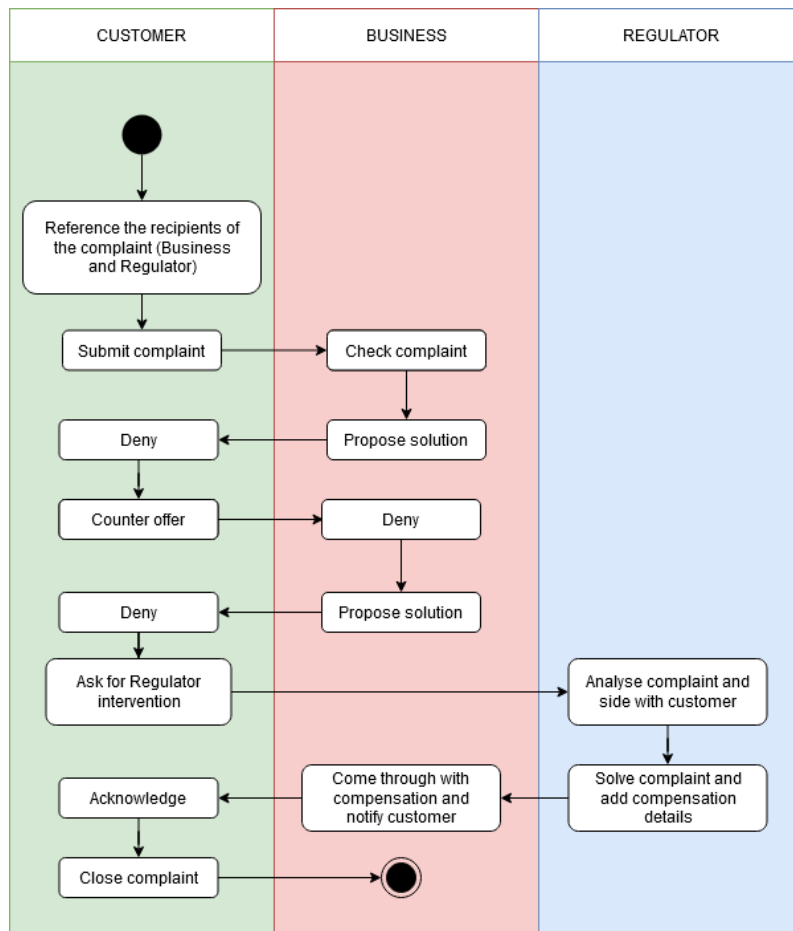


Figure 4.3 - Scenario 3 workflow diagram (Regulator is requested, settles the complaint for the Customer)

4.2.4 Scenario 4

In this case we demonstrate what would happen in our workflow if some entity went inactive in a complaint, stagnating its progression. After a defined period of time without activity, the complaint is relayed to the Regulator to be archived, this way, no complaint is left suspended in a given state other than the final states.

As usual, a complaint is submitted by the Customer and the Business chooses to propose a solution. This time, the Customer goes inactive, suspending the procedure. The same could be done by the Business, there are cases where an entity will purposefully stall the process hoping for it to be given up on. This is avoided by an automated state transition after some time so the Regulator can finalize the complaint, archiving it. This scenario is illustrated in the form of a workflow diagram in Figure 4.5.

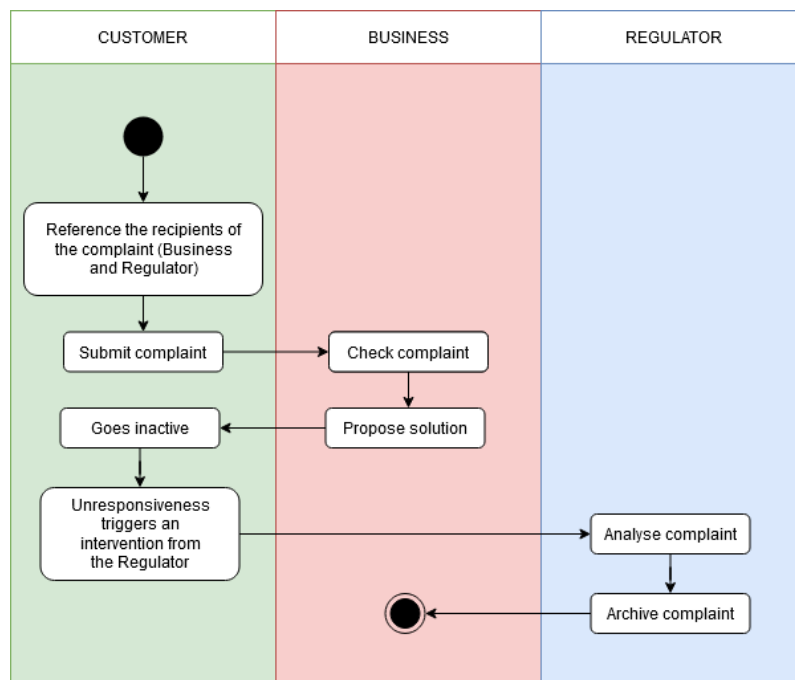


Figure 4.4 - Scenario 4 workflow diagram (Complaint gone inactive, Regulator archives the complaint)

The full picture scenario is shown in Figure 4.5, gathering all different paths possible in our workflow.

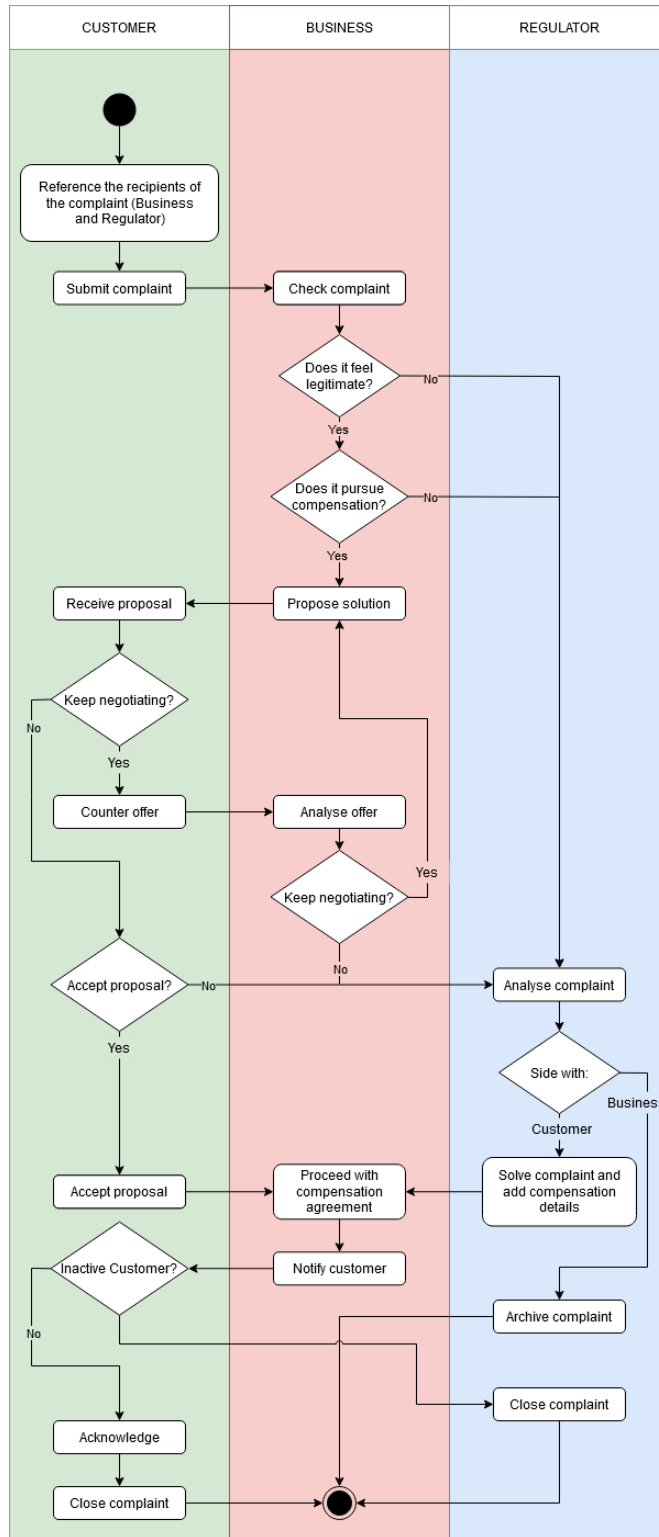


Figure 4.5 - General scenario workflow diagram

4.2 State Diagram

As stated previously, the entities involved in a complaint procedure are a Customer, a Business, and a Regulator . This procedure begins with a displeased Customer that submits a complaint online through our system, naming the Business that wronged him and a Regulator of his choice (usually would be a regulator authority that represents the sector in which the Business provides operates), and a description of the reason for the Customer's displeasure against the service provided to him by the Business. Each entity is represented by their ID, name, email, address and contact info.

In the proposed solution we considered a complaint life-cycle with the following six states, illustrated in Figure 4.1: PENDING, PROPOSED, REVISION, SOLVED, ARCHIVED and CLOSED:

- **PENDING:** The customer has submitted a complaint. The Business must analyse the complaint and decide if it is valid (meaning it has grounds to be considered legitimate) and propose an offer to the Customer for a possible solution/compensation which would progress the complaint to PROPOSED, or not, meaning it would be sent to the Regulator for REVISION;
- **PROPOSED:** The Customer receives an offer to compensate for the complaint. Now, he must decide either to accept the offer, moving to a SOLVED state, or make a counter offer, returning to the PENDING state. This exchange can be considered as a back and forth messaging channel between these two entities while they negotiate and try to form a consensus amongst them;
- **REVISION:** The Regulator has been explicitly requested by the Customer or the Business, or automatically after a long period of inactivity of the previous entities. It is the Regulator's turn to analyse the procedure so far and weigh in on it by adding a comment that can help the progression of the negotiation (reverting the

complaint state back to PENDING or PROPOSED state, depending on who requested the revision, Business or Customer respectively) or progress the complaint himself by deciding the outcome like a jury would, by sending to ARCHIVED which means he sided with the Business, or sending to SOLVED, meaning he sided with the Customer, in each case, adding to the state transition the reason he sided with whoever he chose;

- **SOLVED:** This state is reached when either a Customer has accepted the solution that was discussed or when the Regulator sided with the Customer and enforces a certain solution. Although it is the Business' turn to comply with the agreement/demands, the Customer is the one who decides whether the complaint progresses to the next stage (CLOSED, meaning the compensation from the Business came through) or not (goes to REVISION for the Regulator to intervene);
- **ARCHIVED:** This is one of the potential final states where a complaint can end up. A complaint procedure stamped with the final ARCHIVED state represents an unsuccessful completion of the complaint procedure which can have a variety of motives to end up this way. In the case that the Customer does not agree that the complaint should have been archived, the procedure is still stored and available for him to access the logs and bring it to external judicial authorities;
- **CLOSED:** This final state represents a successful completion and closure of a complaint procedure.

Figure 4.1 presents the state transition diagram representing the complaint life-cycle as explained above.

- 1 - A complaint is submitted by the Customer and received by the Business
- 2 - The Business proposes a solution to the Customer
- 3 - A Customer rejects the proposal and returns to the Business with a counter offer
- 4 - The Regulator is asked to intervene
- 5 - The Regulator returns the complaint to the previous state after contributing
- 6 - The Customer is satisfied by the proposed solution and accepts it.
- 7 - The Regulator archives the complaint, siding with the Business
- 8 - The Regulator solves the complaint, siding with the Customer
- 9 - The Customer closes the complaint when the Business fulfills the agreement
- 10 - Something went wrong with the compensation stage and the Regulator intervenes
- 11 - The Regulator closes the complaint due to Customer inactivity

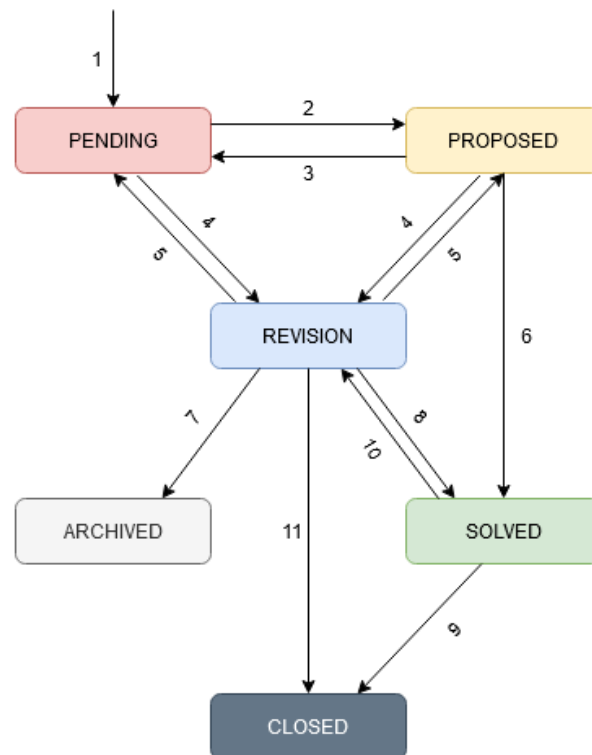


Figure 4.6 - Complaint state transition diagram.

The sequence of state transitions should be preserved and represent the entirety of the complaint procedure for every entity participating in it to be able to follow up the unfolding of the resolution.

4.3 Visibility and Accessibility

In a complaint management system we should have measures in place to protect the customer’s privacy, especially in a shared environment such as this one.

A Customer must always be allowed to see the complaints he has submitted. Also, when creating a complaint, he must be able to see which Businesses and Regulators are available in the system to choose those to associate with the complaint. But Businesses and

Regulators have no need to know of the existence of the Customers using the system.

As an example, consider the following three complaint submissions:

- Customer A submits a complaint to Business A with Regulator A;
- Customer B submits a complaint to Business A with Regulator B;
- Customer C submits a complaint to Business B with Regulator A;

In this example, Business A and Regulator B do not know of the existence of Customer C, until Customer C associated them with a complaint, just like Business B does not need to know Customer A and B, and of the complaints they submitted.

This rule is applied to the complaint and the operations performed on it, the Complaint cannot be visible to other entities not associated with it, and the ones that are associated with it can only operate on the Complaint when it is their turn to do so, in other words, when the correct state allows the respective entity to interact with the complaint, for example, a Complaint in state PENDING can only be operated on by the Business.

4.4 Integrity and Transparency

This solution is meant to be implemented using blockchain, which, as we have explained before, allows us to persist the data recorded on it, rendering the information immutable, and sharing it through a distributed network to numerous peers. Customers can rest assured knowing that their complaints will not take the risk of being adulterated.

The terms of every transaction performed within a blockchain system remain, much like the complaints would, irrevocable. Transactions are open for inspection to everyone or to authorized auditors, making the system that much more transparent.

We also need to discuss the ownership of this blockchain based system, this is important since it can be manipulated if it is owned by a single organization, which would jeopardize

the integrity and transparency of the complaint procedure. The ideal set up would be that the network is managed by several participants with distinct purposes and roles in the system, which would make them suspicious of one another. The ability to verify transactions allows the network users to police each other keeping the system not only integrate relatively to the data but also to the behaviour of the peers.

4.5 Identity

Another aspect that is important to mention is how the users will have access to this system. Some platforms demand some form of document that proves that the person behind the account is real, other platforms make it as easy as registering with an email address. While choosing which method to use, we are making a compromise between accountability and ease of access. Requesting identification as a requirement to access the system will make the user more aware of his behaviour in the network (will avoid making complaints purely out of defamation or spam) since he is staking his identity in a system that permanently records his actions. On the other hand, keeping the access requirements to a minimum such as an email address is less intimidating to a user, as opposed to giving away personal information right at the start.

With our current design, the customer will have more chances to provide further personal information to complement the complaint, with each complaint state transition that is performed by him, he is able to add an observation and attach a file such as receipts, contract numbers or IDs, this will require a form of file transfer.

4.6 File Transfer

At some point during the negotiation stages of the complaint procedure, it may be necessary to provide information in the form of files, by any of the entities involved in a

complaint processing. For example, the Business/Regulator might request some form of proof of transaction or identification from the Customer, to make sure that the complaint is legitimate and to get access to customer profiles in their systems to process the eventual resolution.

File transfer through a blockchain network can hinder its performance by making the blocks heavier and therefore slower to generate. It is important that the system supports a way to transfer files that are private only to the entities that should have them.

For this purpose, we plan on using a protocol which is, much like blockchain, decentralized. This protocol, IPFS that will be elaborated further in the document, along with the visibility rules that will be implemented, will keep sensitive documents private and only accessible by the intended entities. Each file will be represented by a *hash* that will be logged within the complaint, making it available without having to store the documents in the network, but storing a reference to them in an external and also distributed layer of the system.

4.7 Comparison with State of the Art

As opposed to the complaint systems analysed before, in which the Regulator is the owner/provider of the complaint service (and sometimes the Business itself), the entities would all be users of the proposed system, in a way that they participate in the procedure at the same level, each of them have their specific role and set of functions preventing them from stepping over each others' boundaries. This way, the customer should feel safer when using the service knowing that the system itself is impartial to everyone and works based on a previously defined set of rules, balancing the power dynamic between the entities.

A negative component of the researched complaint platforms was also the fact that some were not very transparent, they keep the customer in the dark by not providing a proper follow up of the procedure to the parties involved. With the proposed architecture we avoid

this “black box” effect by representing each complaint procedure stage with a state and allowing everyone associated with the complaint to follow the full development of its resolution.

The visibility rules applied to the entities and complaints in the system also provide a more secure and private experience, customers will no longer have exposed information that they do not wish to provide themselves but will always be able to verify the integrity of the data they submit onto the system and who has access to it.

5. Implementation

In this chapter, we're going to be discussing the technical decisions made before starting the development, describe briefly the tools we used, talk about the business model and functions we created, show the results and comment on them.

5.1 Blockchain selection

Before we could develop the proof of concept, we had to have an understanding of the type of blockchains that were available to us and which one would be the most appropriate for our use-case. Decision flowcharts are pretty popular when it comes to aid in finding the most fitting option for a blockchain:

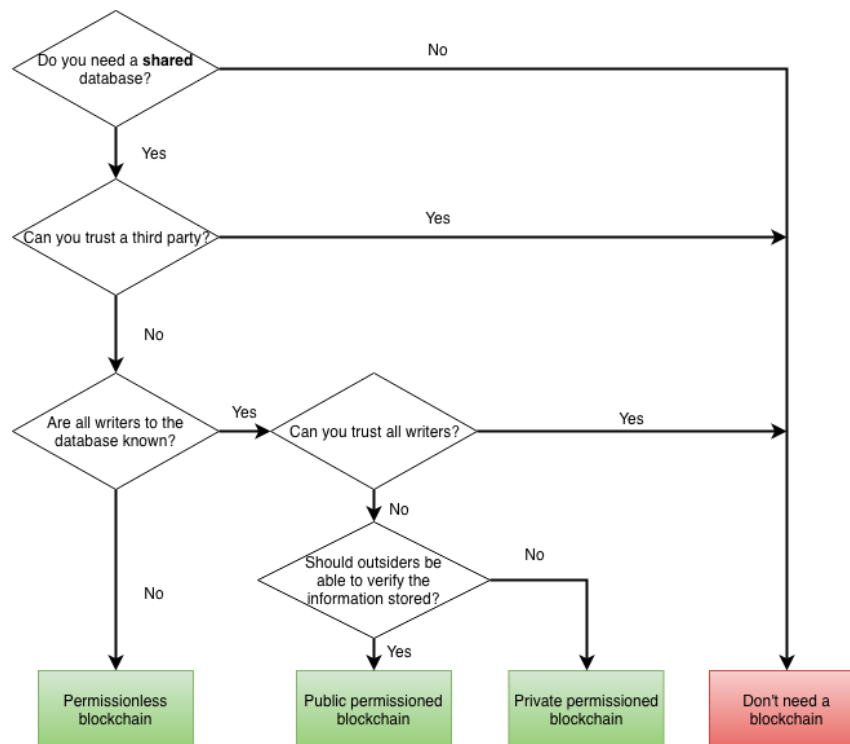


Figure 5.1 - Blockchain flowchart from [28] adapted from [29]

- Do you need a shared database?

The system should minimize unnecessary redundancy meaning that the Customer, the Business and the Regulator should have access to the same complaint that addresses their case. Being a dissertation about blockchain, one of the requirements for the proposed solution would be a distributed database.

- Can you trust a third party?

Intermediaries increase the vulnerability of the data exchanged between entities as well as compromising their privacy and the integrity of the complaints. Many of the eventual users of this system either are direct competitors amongst each other, like businesses, or naturally don't have a very trustful relationship, like customers and businesses. They have opposite ends of a transaction in this complaint system therefore it is safe to assume that they would not trust each other let alone a third party more than they trust themselves as participants.

- Are all writers to the database known?

Yes, the writers should all be known, staking their real life identity should deter malicious behaviour in the network. Although their identity should be supplied to interact with the system, it does not mean that it is completely exposed to everyone, private data should have a strict access control provided by the system or the owner of the data himself.

- Can you trust all writers?

No, the writers should be a group with similar purposes but skeptical between each other, meaning, there has to be a healthy amount of competitiveness in the group so that no alliances are made to control the network and to police one another so no one takes advantage of anyone (i.e. Two competitor businesses will monitor each other; Two

businesses in the same sector will not be allowed to manipulate the network due to the presence of a third entity representing the consumer’s rights). The divergent interests will ironically work towards the goal that is to create the most impartial system possible.

- Should outsiders be able to verify the information stored?

It depends, the information should not be totally public but not so private as to no entity can access it. Reading privileges should be well distributed so that the referenced parties in a complaint can see the required fields and the rest should have limited access to it or none at all. Certain fields referring to the participants and the complaint should be obscured, but the integrity of the transactions should be verifiable by everyone for maximum transparency.

By answering the previous questions we landed on a public permissioned blockchain, which could also be denominated by a Consortium blockchain already described in a previous chapter. Although it is a public blockchain and anyone can become a participant in the network, we can control those interactions through a set of rules and define our workflow scenarios within the system, as seen in the following figure.

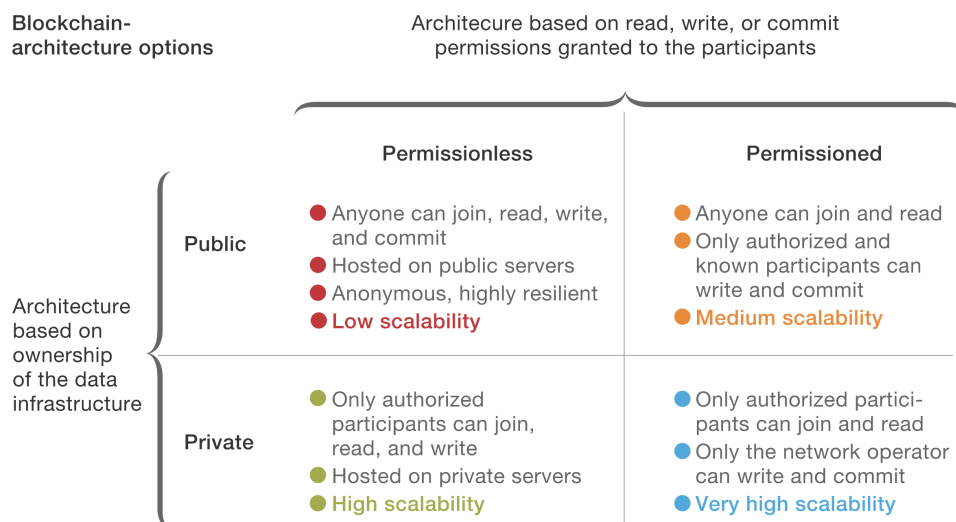


Figure 5.2 - Blockchain architecture options [30]

5.2 Tools

5.2.1 Hyperledger

Hyperledger is a collaborative effort created to advance blockchain technology [31] that consists of several projects ranging from multiple distributed ledgers, libraries and tools for blockchain development that cater to various requirements and use-cases [32]. Within these open-source projects lies Hyperledger Fabric and Hyperledger Composer which we will enter in further detail about next.

5.2.1.1 Hyperledger Fabric

Hyperledger Fabric is a permissioned distributed ledger aimed for enterprise-grade solutions such as banking, finance, insurance, healthcare, human resources, and more [33]. Participants in this network must have their identity known, reducing distrust between them as opposed to what a fully anonymous network would be like. The network can be operated under a governance model that is built off of what trust does exist between participants [33], they could be competitors in the same industry and therefore police each other on their actions within the system. Fabric allows for access control rules, meaning that the permissions of the participants are based on their role in the network, which can be configured to maintain a healthy balance of confidentiality and transparency. Its modular architecture allows for a pluggable consensus protocol, ensuring that the blockchain-related features can be developed independently [34].

5.1.1.2 Hyperledger Composer

Hyperledger Composer is a framework that aims to accelerate time to value by making blockchain solutions development easier. Composer offers abstractions and an environment where we can model our business network using the Hyperledger Fabric runtime.

To build a test network, Hyperledger Composer utilises instances of Fabric components in docker containers named *fabric-peer*, *fabric-ca*, *fabric-orderer*, and *fabric-couchdb*. *Fabric-peer* is the node that handles the transactions, *fabric-orderer* is responsible for validating and creating blocks for the transactions, *fabric-ca* is the Certificate Authority that manages certificates and permissions of each entity, and *fabric-couchdb* supports the world state database for query operations. Figure 5.3 illustrates the Hyperledger Composer architecture:

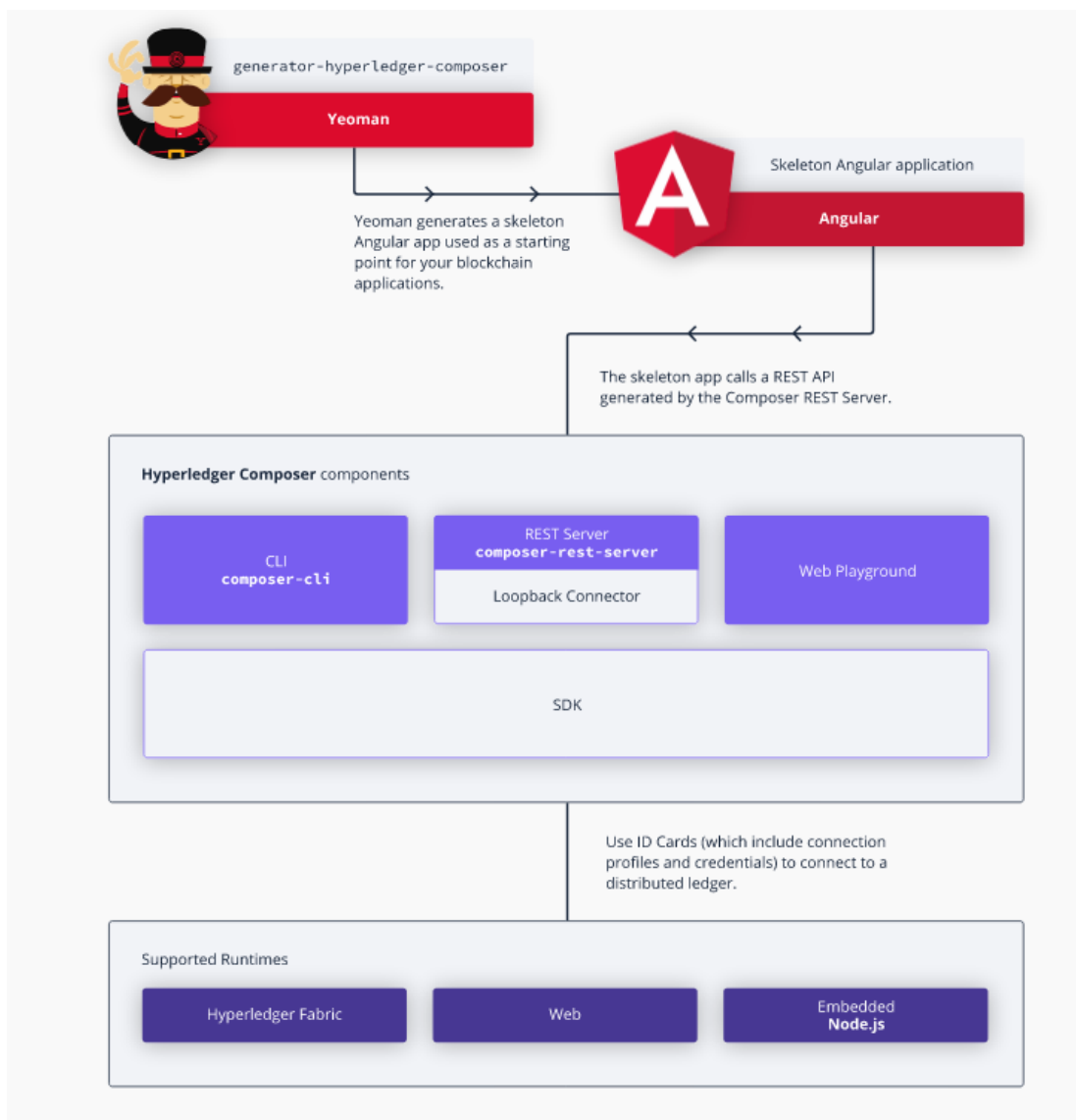


Figure 5.3 - Typical Hyperledger Composer Solution Architecture [35]

After deploying the instance of Hyperledger Fabric, we can launch Hyperledger Composer on top of it enabling us to use the Web Playground where we can define and test our network, which is visible in Figure 5.4.

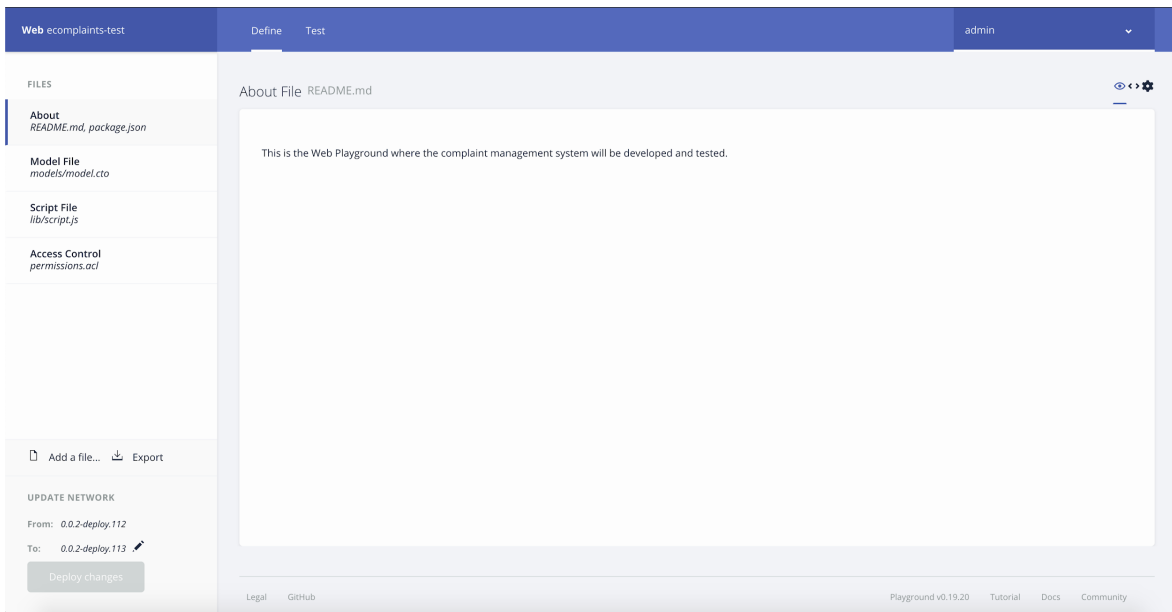


Figure 5.4 - Web Playground

Essentially, to build our use-case, Composer only requires at least three types of files:

- Model file: contains the definition of the objects within the network such as participants, assets and transactions;
- Script file: a set of functions that define the behaviour of the transactions, in essence, the smart contracts/chaincode is placed here;
- Access Control file: where the permissions for Creating, Reading, Updating and Deleting other objects within the namespace are defined for every entity.

Describing further other key concepts, assets are the tangible or intangible goods, services or property, transactions describe the actions done with those assets and the participants are the entities that use transactions to manage the assets within the network [36].

5.2.2 IPFS

In a complaint management system, one might want to upload files to serve as proof of purchase transactions or poorly given services. In a blockchain system that might not be too efficient since transaction speeds are already affected by consensus protocols, big enough files might slow down the block creation process even further, clogging up the network.

IPFS stands for Interplanetary File System and it is a peer-to-peer protocol where each node stores a collection of hashed files. A client who wishes to retrieve any of those files enjoys a nice abstraction layer where it simply needs to call the hash of the file it wants, IPFS will search for it through the nodes and supplies the client with the file [37].

We can think of it as a decentralized way of storing and referring to files. The Figure 5.5 is a simple diagram that illustrates how the IPFS works:

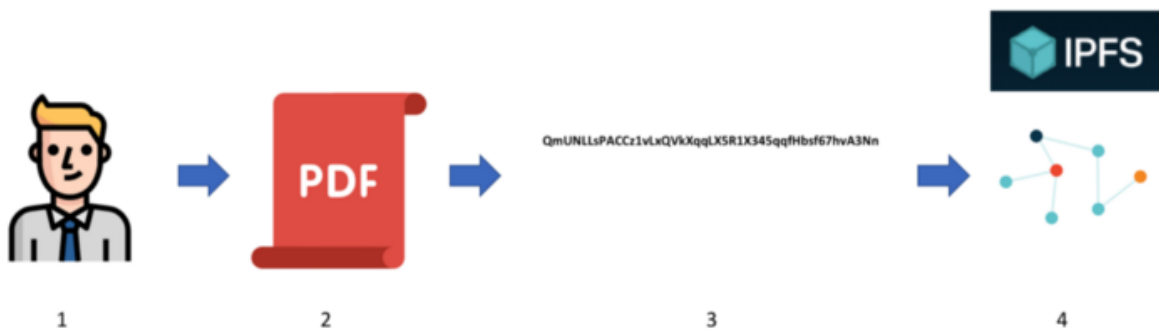


Figure 5.5 - IPFS workflow diagram [38]

1. John wants to upload a PDF file to IPFS;
2. He puts his PDF file in his working directory;
3. He tells IPFS he wants to add this file, which generates a hash of the file;
4. His file is available on the IPFS network;

Suppose we have other entities that require access to John's file, just like our complaint use case. John reveals the hash to those entities and they just need to reverse the process, ask IPFS to retrieve the file that corresponds to the hash and the protocol will provide them with a copy of John's PDF.

This poses a security problem, since anyone who has the hash will have access to those documents, therefore, sensitive data is not well suited to IPFS in their native state. Another security layer could be added by using asymmetric encryption to encrypt the files before uploading them to IPFS.

The way this tool will be used in our implementation is, whenever an entity wants to transfer a file to another, all he needs to do is upload the file manually to his IPFS and obtain the respective hash. Then, paste the hash into the *observation* parameter when submitting a transaction to transition the complaint's state, meaning, the hash will accompany the comment the user will add to the complaint log, which will be accessible by both the other receivers associated in the complaint.

5.3 Business Logic

Our model contains four participants, the Customer, Business, Regulator, and a Timeout Manager. Aside from the Timeout Manager, all of them have similar properties such as a name, email, address, contact information, and an ID, as shown in Figure 5.6. The Timeout Manager takes the system role of ensuring that a complaint does not remain suspended in the same state for a long period of time, he is the one in charge of sending the complaint to the Revision state in case the Customer or Business are inactive.

```

participant Customer identified by customerId {
  o String customerId
  o String name
  o String email optional
  o String address optional
  o String contact optional
}

participant Business identified by businessId {
  o String businessId
  o String name
  o String email optional
  o String address optional
  o String contact optional
}

participant Regulator identified by regulatorId {
  o String regulatorId
  o String name
  o String email optional
  o String address optional
  o String contact optional
}

```

Figure 5.6 - Participant classes definition

Our asset will be the Complaint which has one Customer, one Business, and one Regulator associated with it, the issue (where the Customer describes what he is complaining about), a State, a previousState, an array of logs and a timestamp, as seen in Figure 5.7.

```

asset Complaint identified by complaintId {
  o String complaintId
  --> Customer customer
  --> Business business
  --> Regulator regulator
  o String issue
  o ComplaintState state
  o ComplaintState previousState
  o DateTime timestamp
  o String[] logs optional
}

```

Figure 5.7 - Asset class definition

The entities (Customer, Business and Regulator) are needed to establish a relationship between them and the complaint, otherwise, they will not be able to access it and interact with it. The state and previousState are required for when the Regulator has to revert the

state to whoever requested the revision. Finally, the timestamp is necessary for the Timeout Manager to control when the latest state transition occurred in each complaint, meaning, he will force the state transition to REVISION if the time difference between the latest timestamp and the current time is bigger than a determined threshold.

An enumerate is in order to define the different states the Complaint could be in, as shown in Figure 5.8.

```
enum ComplaintState{  
    ○ NONE  
    ○ PENDING  
    ○ PROPOSED  
    ○ REVISION  
    ○ SOLVED  
    ○ ARCHIVED  
    ○ CLOSED  
}
```

Figure 5.8 - Enumerate with complaint states

Our transactions will be the operations each participant can use to interact with the Complaint in order to fulfill the workflow described before. They shall be:

- Submit complaint;
- Propose solution;
- Counter Offer;
- Accept Solution;
- Revision;
- Revert;
- Archive;
- Solve Complaint;
- Close Complaint;

- Timeout;

Each participant is allowed to have N number of complaints to its name, but a complaint can only have one participant of each type associated and one state at a time. Each participant has its own set of transactions according to the role it will have in the network, as illustrated in the Figure 5.9 class diagram:

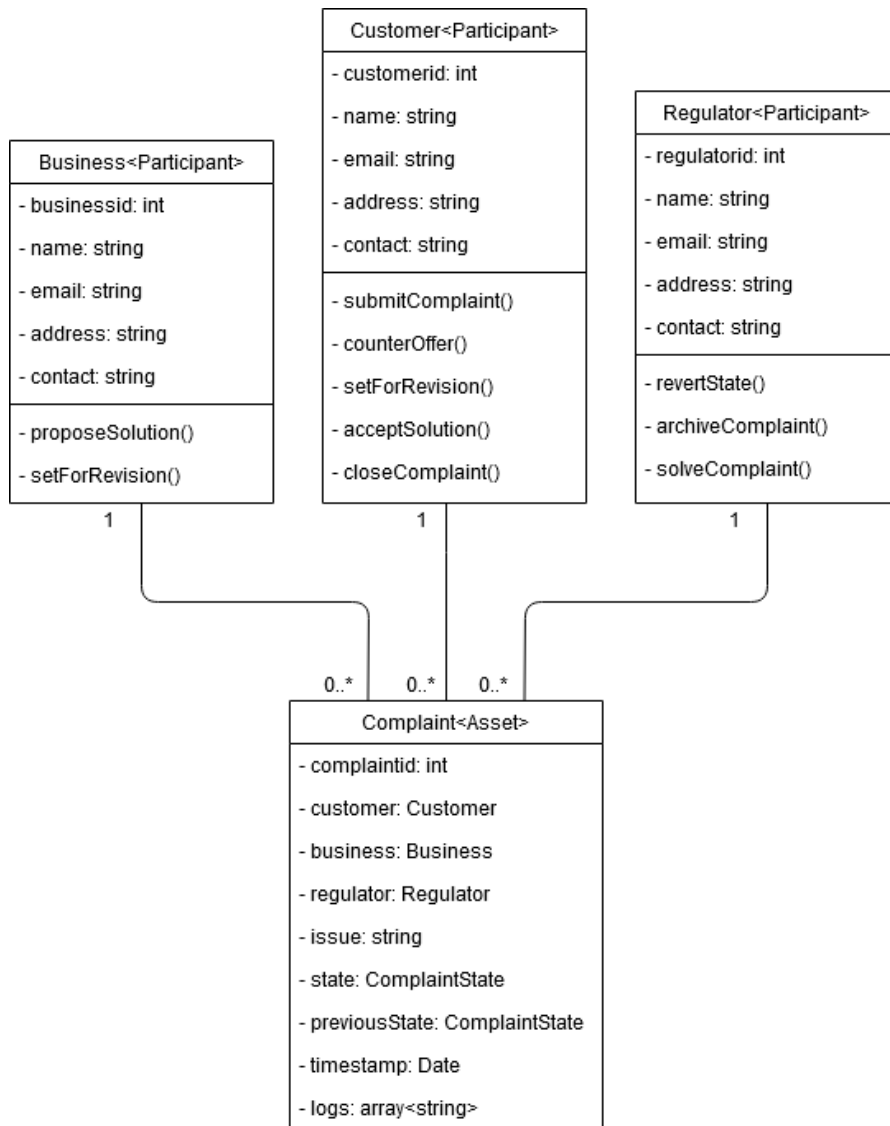


Figure 5.9 - Class diagram of our business model

5.4 Transactions

As illustrated in Figure 5.9, each type of participant has its own set of transactions available to interact with the complaints and progress in the workflow as shown in the Figure 5.10 diagram.

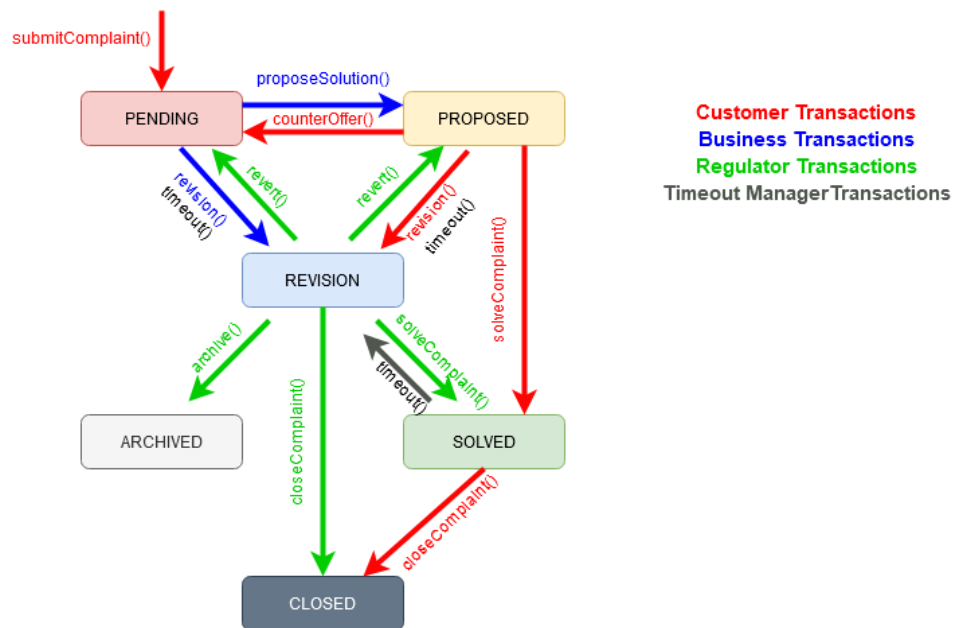


Figure 5.10 - State transitions through transactions

Aside from the *submitComplaint* transaction, which needs to create the asset, every other transaction functions in a similar way, checks if the complaint is at the correct state to allow the transaction to take place following the workflow, updates the complaint's state, storing the previous one in case the following transaction is a *revert*, adds the observation (which comes as a parameter for each transaction) submitted by the entity in the logs and updates the timestamp, enabling the Timeout Manager to check when the last change occurred. The Figure 5.11 is a transaction function implementation example.

```

/**
 * Propose a solution to the Customer
 * @param {org.ecomplaints.proposeSolution} complaint
 * @transaction
 */
async function proposeSolution(tmp) {

  const namespace = 'org.ecomplaints';
  const complaint = tmp.complaint;

  if(complaint.state != 'PENDING'){

    throw new Error("You can't propose a solution at this stage!")

  }

  var transition = complaint.state;
  complaint.previousState = complaint.state;
  complaint.state = 'PROPOSED';
  complaint.timestamp = tmp.timestamp;

  transition = transition + " -> " + complaint.state;

  var log = transition + ": " + tmp.observation;

  if (typeof complaint.logs == 'undefined') {
    complaint.logs = new Array();
    complaint.logs[0] = log;
  }
  else {
    complaint.logs.push(log);
  }

  const assetRegistry = await getAssetRegistry(complaint.getFullyQualifiedType());
  await assetRegistry.update(complaint);

}

```

Figure 5.11 - Transaction function example (*proposeSolution*)

5.5 Access Rules

The Access Control Language (ACL) file contains the description of the rules that dictate which operations (create, update, read and delete) are permitted or not within the network. The following list presents the rules implemented in the system.

Rules applied to Businesses:

- Businesses are allowed to see themselves in the network;
- Businesses are allowed to see complaints associated with themselves;
- Businesses are allowed to use *proposeSolution* transaction;
- Businesses are allowed to use *revision* transaction.

Rules applied to Regulators:

- Regulators are allowed to see themselves in the network;
- Regulators are allowed to see complaints associated with themselves;
- Regulators are allowed to use *revert* transaction;
- Regulators are allowed to use *archive* transaction;
- Regulators are allowed to use *solveComplaint* transaction;
- Regulators are allowed to use *closeComplaint* transaction.

Rules applied to Customers:

- Customers are allowed to see themselves in the network;
- Customers are allowed to see Businesses in the network;
- Customers are allowed to see Regulators in the network;
- Customers are allowed to see their submitted complaints;
- Customers are allowed to use *submitComplaint* transaction;
- Customers are allowed to use *acceptSolution* transaction;
- Customers are allowed to use *revision* transaction;
- Customers are allowed to use *closeComplaint* transaction.

Rules applied to Timeout Manager:

- Timeout Manager is allowed to see all complaints in the network;
- Timeout Manager is allowed to use *timeout* transaction.

The rules are evaluated from top to bottom of the file, as soon as a match is found for a rule the subsequent rules are not evaluated, therefore, they should be written from the most specific to the least specific. This decision table is faster to scan for both humans and computers because of this ordering, if no rule is triggered, the access control is denied by default. This explains why some rules are not implemented such as “Customers are not allowed to see other Customers in the network” or “Customers, Businesses and Regulators are not allowed to see complaints where they are not referenced”. In Figure 5.12 we have a rule definition example:

```
rule businessVisibility2{
  description: "Business is allowed to see his complaints"
  participant(c): "org.ecomplaints.Business"
  operation: READ, UPDATE
  resource(r): "org.ecomplaints.Complaint"
  condition:(c.getIdentifier() == r.business.getIdentifier())
  action: ALLOW
}
```

Figure 5.12 - Access rule definition example

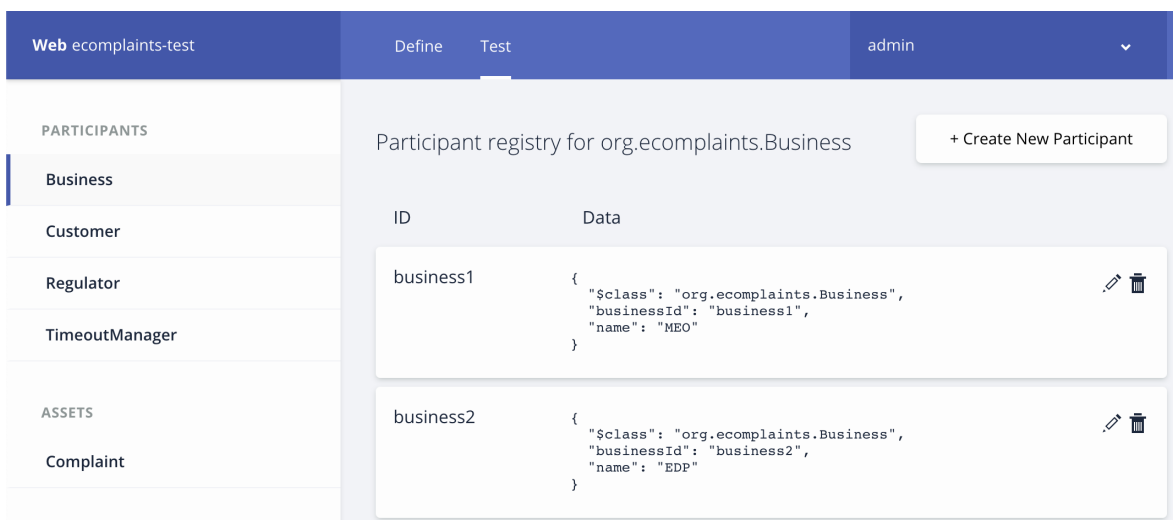
As we can see, the rules are managed by referring to a type of participant, the operations that we want to control in this rule, the resource that the rule is applied to and we could also add a condition to specify the logic of the rule. In this example, we want to limit the access of the Business type participants to only their complaints.

6. Results

In this chapter we will be showing the results of our implementation by simulating a use-case scenario. We will be seeing how one creates a participant and uses it to test the network, run through a scenario to observe the flow of the transitions and the transactions being recorded.

6.1 Creating/Adding the Participant

In order for us to test the network we needed a Business Network Card which is like an identity card that represents a single participant that allows them to connect to the blockchain. In order to create one, we need to use the administrator card, which is provided by default for the network development, to instantiate the participants and then issue their respective Business Network Card.



The screenshot shows a web application interface for managing participants. The top navigation bar includes 'Web ecomplaints-test', 'Define', 'Test', and 'admin'. The left sidebar lists 'PARTICIPANTS' (Business, Customer, Regulator, TimeoutManager) and 'ASSETS' (Complaint). The main content area is titled 'Participant registry for org.ecomplaints.Business' and features a '+ Create New Participant' button. Below this is a table with two entries:

ID	Data
business1	<pre>{ "\$class": "org.ecomplaints.Business", "businessId": "business1", "name": "HEO" }</pre>
business2	<pre>{ "\$class": "org.ecomplaints.Business", "businessId": "business2", "name": "EDP" }</pre>

Figure 6.1 - Creating a Participant in the registry

In Figure 6.1 we have the registry for the existing Businesses and to add a new Participant of this type we must select the top right hand corner option “+ Create New Participant” (with the current applied rules, only the admin has the permission to add new participants to the network).

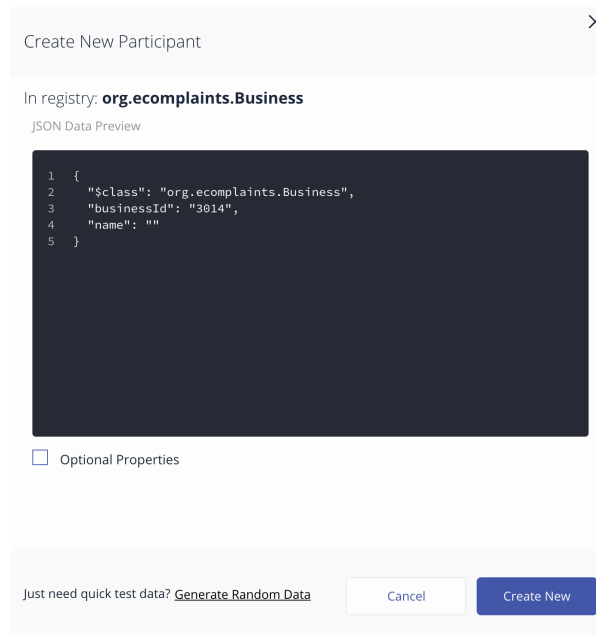


Figure 6.2 - Creating a new Business

We fill the required parameters for the Business, the ID and a name, both can be generated randomly or arbitrary, as seen in Figure 6.2. The rest of the parameters such as email, address and contact are set as optional but can be added at any time by the admin or the Business itself.

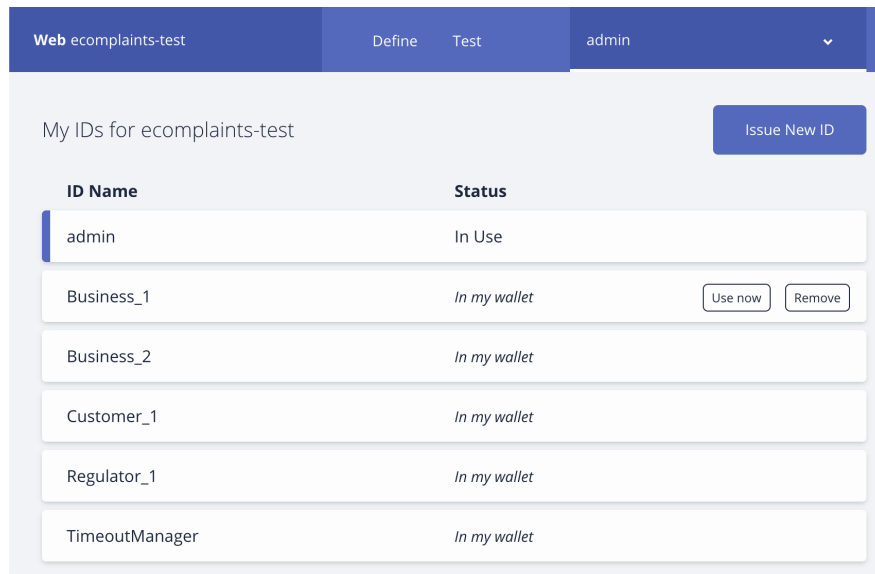


Figure 6.3 - ID Registry

In Figure 6.3 we can see the ID registry menu where the admin manages the list of IDs issued in the network. Once again, in the top right hand corner we can see the “Issue New ID” option where we can generate the Business Network Card for the Participant we want to add to the network, resulting in what can be seen in Figure 6.4.

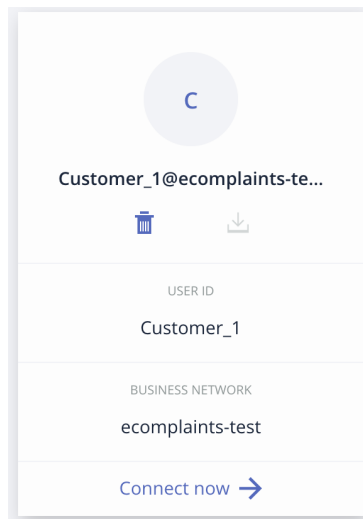
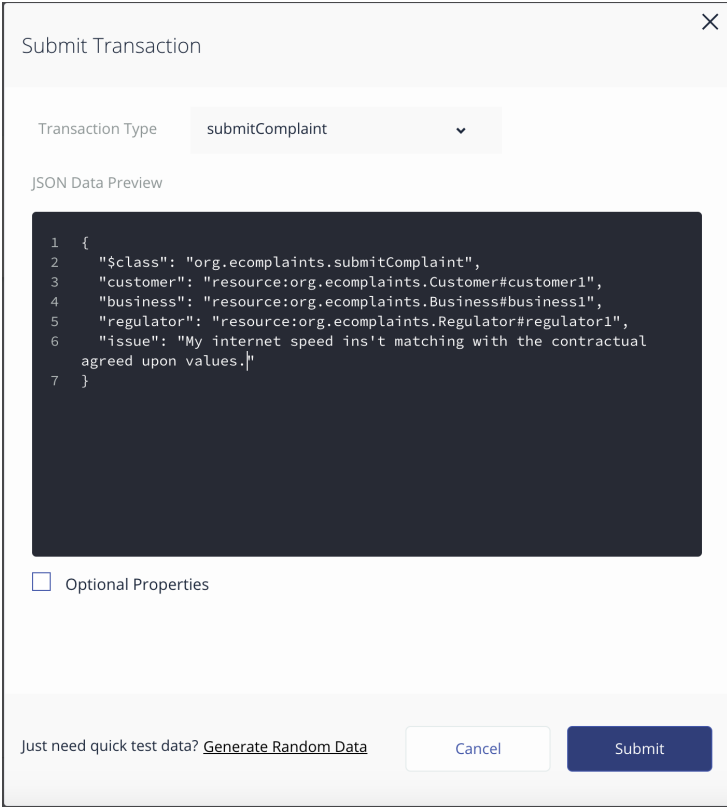


Figure 6.4 - Business Network Card example

With the list of cards, we will take the role of the respective type of participant and test the scenarios presented before, making sure that the visibility constraints are well implemented and, most important of all, the code is fully functional and is able to follow the designed complaint workflow.

6.2 Use-case Test

A Customer would connect to the system and submit a complaint, which is equivalent to executing a *submitComplaint* transaction with the required parameters (CustomerID, BusinessID, RegulatorID and issue), as shown in Figure 6.5.



The screenshot shows a dialog box titled "Submit Transaction" with a close button (X) in the top right corner. Below the title bar, there is a "Transaction Type" dropdown menu currently set to "submitComplaint". Underneath, a "JSON Data Preview" section displays a code editor with the following JSON structure:

```
1 {
2   "$class": "org.ecomplaints.submitComplaint",
3   "customer": "resource:org.ecomplaints.Customer#customer1",
4   "business": "resource:org.ecomplaints.Business#business1",
5   "regulator": "resource:org.ecomplaints.Regulator#regulator1",
6   "issue": "My internet speed ins't matching with the contractual
7   agreed upon values."
8 }
```

Below the JSON preview, there is an unchecked checkbox labeled "Optional Properties". At the bottom of the dialog, there is a link "Just need quick test data? [Generate Random Data](#)", a "Cancel" button, and a "Submit" button.

Figure 6.5 - Complaint submission parameters example

As the Customer_1, we can now see our own complaint in the system as pictured in Figure 6.6, all future complaints submitted by this user will be added and listed to this registry.

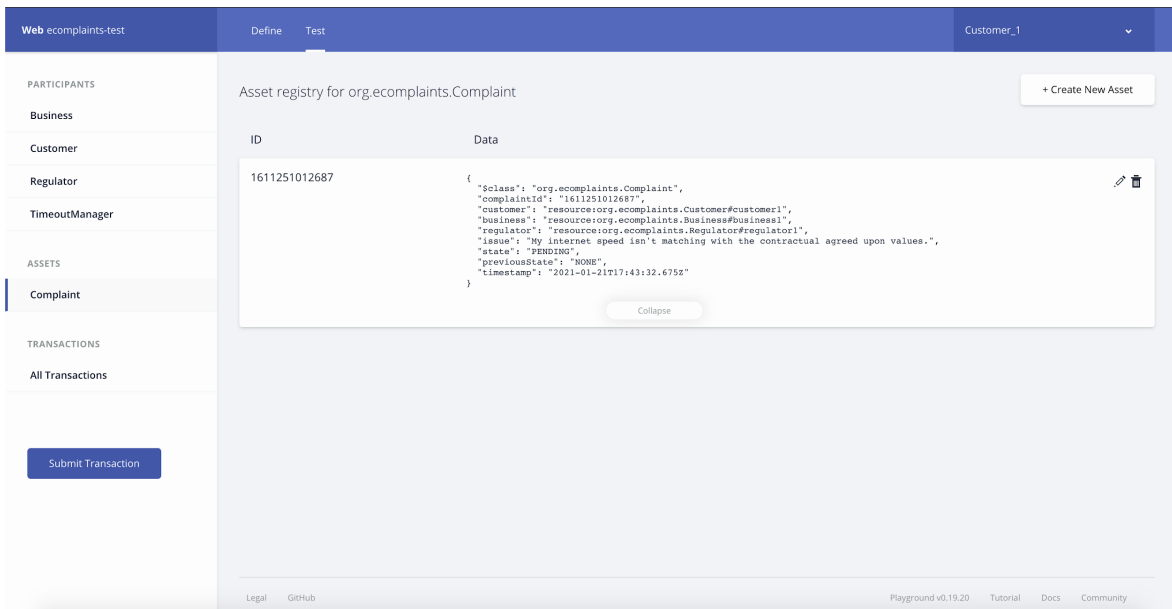


Figure 6.6 - Complaint asset in the registry

Having created the complaint, illustrated in Figure 6.6, the respective Business and Regulator will have access to it and be able to interact with it using the remaining of the transactions available until it reaches the final state of the complaint process. We can see the currently operating identity on the top right corner of Figure 6.6, which in this case was the Customer who just submitted the complaint.

The scenario we are recreating is the simplest one where the Business and Customer arrive to a consensus on their own without the intervention of the Regulator. The next few transitions are a back and forth between them, alternating the state of the complaint between PENDING and PROPOSED while they exchange further information, using the *proposeSolution* and *counterOffer* transactions, Figure 6.7 is an example of the *proposedSolution* where one has to input the complaintID and the comment the user wishes to add.

Submit Transaction

Transaction Type: counterOffer

JSON Data Preview

```
1 {
2   "$class": "org.ecomplaints.counterOffer",
3   "complaint": "resource:org.ecomplaints.Complaint#1611251012687",
4   "observation": ""
5 }
```

Optional Properties

Just need quick test data? [Generate Random Data](#)

Figure 6.7 - *counterOffer* transaction example.

During the negotiation stages, where the Customer and Business throw messages back and forth, they are all registered in the *logs* so that each participant (the ones associated with the complaint) has access to the conversation that took place and is aware of the behaviour of the other parties. In a lot of cases, physical evidence might be required to validate an allegation or an identity, for that purpose, we resorted to the IPFS protocol.

So for the sake of the scenario, let's assume that the customer wanted to provide the Business with a file that gives further input on the state of quality of service of his internet, to do this, the Customer will start by uploading the file to the IPFS network first.

IPFS features both an application and browser extension, we went with the latter which can be seen in Figure 6.8.

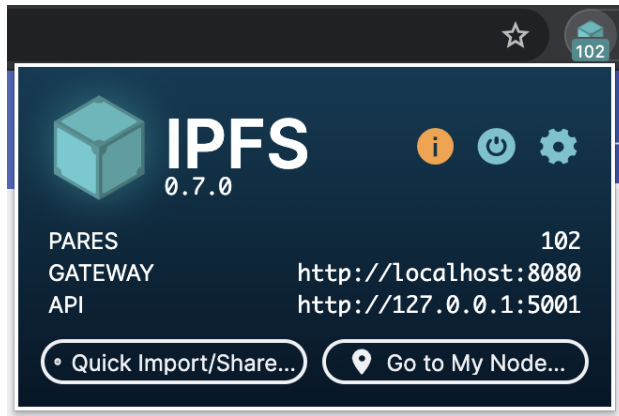


Figure 6.8 - IPFS extension

By selecting the *Quick Import/Share* button we will be redirected to the main dashboard where we can control the files we share in our IPFS node as demonstrated in Figure 6.9. Each file will have a corresponding hash that can be copied and shared to whoever we want.

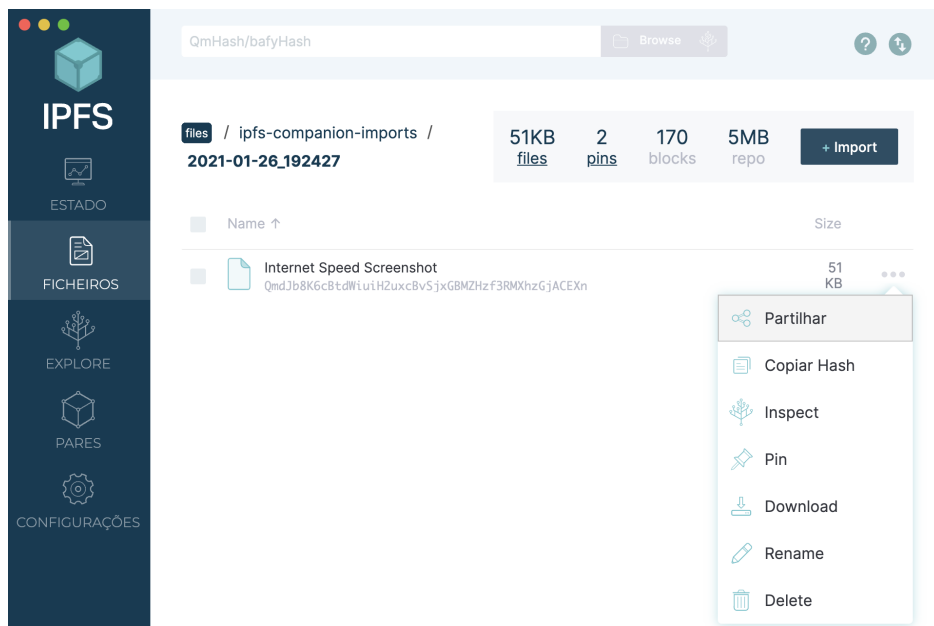


Figure 6.9 - IPFS Dashboard

All the Customer must do is copy the corresponding hash, visible under the file in Figure 6.9, and paste it alongside his next state transition for the Business or Regulator to see.

Figure 6.10 shows an example of how the Customer would do this.

Submit Transaction

Transaction Type: counterOffer

JSON Data Preview

```
1 {
2   "$class": "org.ecomplaints.counterOffer",
3   "complaint": "resource:org.ecomplaints.Complaint#1611251012687",
4   "observation": "The technician claimed that everything was fine
5   with the router but here goes my current internet speeds that prove
   it: QmdJb8K6cBtdWiuIH2uxcBvSjxGBMZhZf3RMXhzGjACEXn"
6 }
```

Optional Properties

Just need quick test data? [Generate Random Data](#)

Figure 6.10 - Complaint transition including IPFS hash

To access the file, all the Business must do is attach the given hash to the protocol public gateway which would be *ipfs.io/ipfs/*, redirecting us to a copy of the file we were given. Figure 6.11 is a picture of the example we used, but it could be a more formal document, receipt or any other type of file that the Business could find relevant.

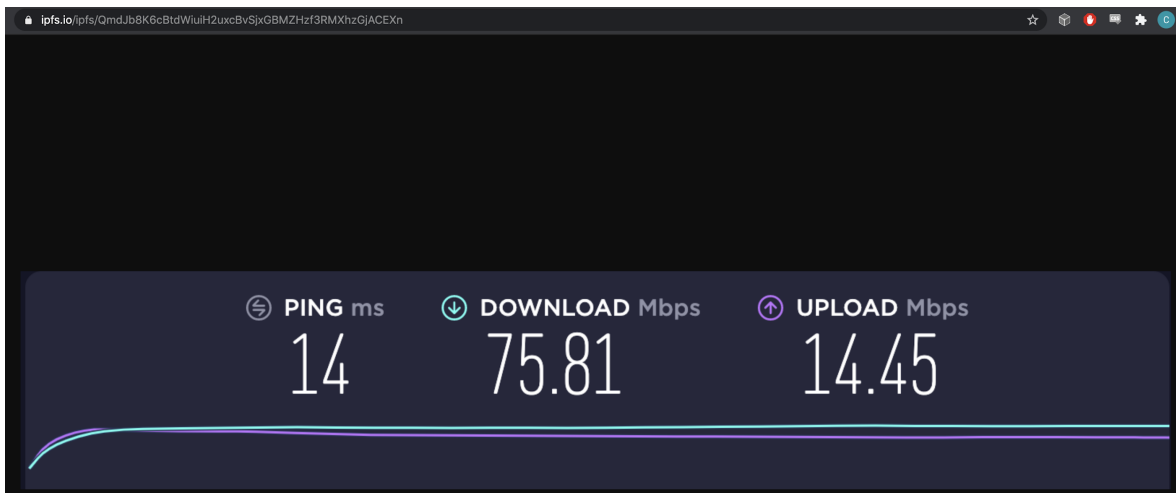


Figure 6.11 - Example file transferred through IPFS

Following the optimal scenario (where there would not be Regulator intervention), the *logs* in the complaint would look like a list of state transitions along with the comments added by both the Customer and Business as shown in Figure 6.12, showing a trace of interactions throughout the complaint's lifecycle.

In registry: **org.ecomplaints.Complaint**

JSON Data Preview

```

11   "logs": [
12     "PENDING -> PROPOSED: We're sorry for the inconvenience! Feel
      free to contact us to set up a technician appointment to fix the
      issue.",
13     "PROPOSED -> PENDING: The technician claimed that everything
      was fine with the router but here goes my current internet speeds
      that prove it: QmdJb8K6cBtdWiuiH2uxcBvSjxGBMZHf3RMXhzGjACEXn",
14     "PENDING -> PROPOSED: We apologize again for the
      inconvenience! We seem to have a hardware malfunction in your
      area, we offer to refund a percentage of this months payment
      equivalent to the time frame you're experiencing the shortage of
      bandwidth.",
15     "PROPOSED -> SOLVED: I accept those terms.",
16     "SOLVED -> CLOSED: My internet speeds are back to normal after
      one week and the corresponding payment has been deducted from the
      final bill."
  ]

```

Figure 6.12 - Complaint logs example

Although the visibility between participants and assets is limited, participants are allowed to see who made what transactions and at what time, the contents of those transactions are hidden however, as demonstrated in Figure 6.13.

Web ecomplaints-test		Define	Test	Customer_1
PARTICIPANTS				
Business				
Customer				
Regulator				
TimeoutManager				
ASSETS				
Complaint				
TRANSACTIONS				
All Transactions				
	2021-01-26, 20:50:18	closeComplaint	customer1 (Customer)	view record
	2021-01-26, 20:44:20	acceptSolution	customer1 (Customer)	view record
	2021-01-26, 20:43:11	proposeSolution	business1 (Business)	view record
	2021-01-26, 20:27:16	RemoveAsset	admin (NetworkAdmin)	view record
	2021-01-26, 20:26:49	proposeSolution	business1 (Business)	view record
	2021-01-26, 20:23:17	submitComplaint	customer1 (Customer)	view record

Figure 6.13 - Transaction record example.

Aside from the *submitComplaint* transaction, every other transaction functions in a similar fashion where the respective participant only adds a comment to the state transition already defined by the transaction that will be used. For example, in order for a Regulator to transition a complaint that is currently in the REVISION state to an ARCHIVED state, he would use the *archive* transaction for this effect. Any other transaction that is not allowed for the Regulator would be met with an error. Another occasion that would throw an error would be the use of a transaction to a given state if the *previousState* is not adjacent to the state we want to go to, for example, a Customer can not use the transaction *closeComplaint* if the current state of the complaint is PROPOSED, it would have to transition to SOLVED first, through *solveComplaint*.

6.3 Ending Notes

The requirements we set out to accomplish were to design and develop a new form of complaint management system using blockchain technology. Having blockchain as a foundation for the system made us aware of how much more exposure and vulnerability we would inflict on the users if their data was not properly handled, since the network can be accessed by anyone and the information is permanently recorded and immutable. That is why the controlled permissions and limited visibility of the participants are some of the most important requirements we set out to implement on our network.

We can say that the proposed requirements were met successfully resulting in a complaint management system that is capable of evening out the playing field for the consumer and while keeping them more up to date regarding their complaint.

7. Conclusions

This chapter contains some final thoughts about the development of this study as a whole, commenting on some conclusions and choices made along the way, and finishing up with a couple suggestions on how to give further depth to this work.

Throughout this thesis, the project went through a couple of variations until we settled on this final form. Much of the initial uncertainty of what the focus of this thesis would be stemmed from the vague meaning of the term “complaint management”. By investigating the topic, at first, we would find that it applies to internal protocols of a business and the handling of customer criticism in a human resource’s perspective, rather than the complaint procedure itself, which caused a bit of confusion.

Not only was the complaint management aspect of this investigation complex, the technical part was also tricky due to the wide variety of blockchains at our disposal. There is no “blockchain-fits-all” solution, a lot of time was allocated to researching which possibility fitted best to the use-case we were going for. And even then, we only scratched the surface of what blockchain technology could accomplish and ended up limiting ourselves by our own choices. In the end, there was a lot of research that ended up not being reflected in this thesis.

The fact of having a limited time frame to accomplish this project led to picking up Hyperledger Composer, a deprecated framework since August 2019, to rapidly develop a use-case and deploy a blockchain solution in weeks rather than months, abstracting the deep level of understanding required to build a full fledged application. Although, for the purpose of presenting a proof-of-concept that is satisfactory for the vision, it was the almost perfect tool for it.

A great deal of time was spent discussing the validity of the blockchain in this complaint management context. The benefits of using blockchain were as expected, the system based

on it is intrinsically more credible and transparent, traceability and immutability create a more solid and trustworthy network for the user, guaranteeing the integrity of its data. On the other hand, handling users' private data can be quite sensitive when using blockchain, since everything is stored permanently, a great deal of care has to go into the design and planning of the blockchain architecture to ensure the users' privacy.

On a final note, we ended up learning a lot about blockchain technology and, compared to the potential for growth the technology has, we could have dove even deeper into it. Designing a complaint system from scratch was also a great learning experience, as someone who has had the luck of never having to formally complain about a service. It was very enlightening to simulate every possible interaction one could experience in a situation like this, ranging from a positive dramaless experience to a very sour unclosed complaint procedure. We believe this project shed some light to some features worth applying in a complaint management system, such as the involvement of regulators in the procedure, a more proactive participation stance for the customer, as opposed to the submission of his complaint and waiting for it to be resolved, and an overall increased accountability to every entity, provided by the fact that anyone can check what the other party is doing, this way evening the ground between them and creating a less intimidating environment for a customer to exercise their right to complain as a consumer.

7.1 Future Work

This project should be a good starting point for a full fledged application that could very well revolutionize the State of the Art, however, some added discussions would have to be made.

This system was built on top of sample nodes provided by the Hyperledger framework. In a production stage, those nodes would have to be owned by the participants using the network and a discussion should be made on who should own nodes and which types of

roles (orderer or peer) and how would that affect the overall picture. Also, this proof of concept would have to be developed using native Hyperledger Fabric (or other blockchain that seems fit) in order to take full advantage of its potential.

The message exchange between the entities should be more fluid, a worthy feature would be an instant messaging option, where the Business and Customer could talk in almost real time. The concept would remain the same, the logs would be stored and the files would be stored in a separate layer protocol, such as IPFS, in order not to overload the network. Along with this, a front-end could prove useful to have a more finalized product that brings to light the full picture of how the complaint management system could improve the consumers' experience.

8. References

- [1] Um Dasch Group Ventures, “The New Era of Shopping - How Megatrends transform Retail”, 23 July 2018,
<<https://www.umdachgroup-ventures.com/en/magazine/the-new-era-of-retail-about-the-transformation-of-shopping>>, (Last accessed 13-12-2020).
- [2] *Wikipedia*, “Consumerism”, 9 November 2020,
<<https://en.m.wikipedia.org/wiki/Consumerism>>, (Last accessed 13-12-2020).
- [3] Graham Charlton, ”Companies more focused on acquisition than retention:stats” [blog post], 30 August 2013,
<<https://econsultancy.com/companies-more-focused-on-acquisition-than-retention-stats>> ,
(Last accessed 13-12-2020).
- [4] Josh Jones, “The First Customer Service Complaint in Recorded History (1750 B.C.)“, 7 March 2015,
<<https://www.openculture.com/2015/03/the-first-recorded-customer-service-complaint-from-1750-b-c.html>>, (Last accessed 13-12-2020).
- [5] Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, “Blockchain Technology: Beyond Bitcoin”, June 2016,
<<https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf>>, (Last accessed 13-12-2020).
- [6] Heather Lancaster, ”What is Complaint Management and Why Do You Need It?” [blog post], 7 June 2016,
<<https://www.issuetrak.com/blog/what-is-complaint-management-and-why-do-you-need-it>> , (Last accessed 13-12-2020).
- [7] E. Laird Landon Jr., ”The Direction of Consumer Complaint Research”, *Advances in Consumer Research*, Volume 7, Issue 1, 1980, Pages 335–338.
- [8] Marshall Allan Sloo, “Method and apparatus for handling a complaint”, 16 September 1997, <<https://patents.google.com/patent/US5668953A/en>>, (Last accessed 13-12-2020).

- [9] Better Business Bureau, “Frequently Asked Questions about the Better Business Bureau (BBB)”, <<https://www.bbb.org/frequently-asked-questions>>, (Last accessed 13-12-2020).
- [10] Rede Telemática de Informação Comum (RTIC), Direção Geral do Consumidor (DGC), Imprensa Nacional - Casa da Moeda (INCM), “O Livro de Reclamações”, 2005, <<https://rtic.consumidor.pt/rtic/brochura.pdf>>, (Last accessed 13-12-2020).
- [11] Diário da República, “Decreto Lei n.º 74/2017”, <<https://dre.pt/application/file/a/107542707>>, (Last accessed 13-12-2020).
- [12] Better Business Bureau, “Process of Complaints and Reviews”, <<https://www.bbb.org/process-of-complaints-and-reviews>>, (Last accessed 13-12-2020).
- [13] Joseph Rhee and Brian Ross, “Terror Group Gets 'A' Rating From Better Business Bureau?”, 11 November 2010, <<https://abcnews.go.com/Blotter/business-bureau-best-ratings-money-buy/story?id=12123843>>, (Last accessed 13-12-2020).
- [14] *Wikipedia*, “Associação Portuguesa para a Defesa do Consumidor”, 11 January 2020, <https://pt.wikipedia.org/wiki/Associa%C3%A7%C3%A3o_Portuguesa_para_a_Defesa_do_Consumidor>, (Last accessed 14-12-2020).
- [15] Joram Borenstein, “A Risk-Based View of Why Banks are Experimenting with Bitcoin and the Blockchain”, 18 September 2015, <<https://www.risktech-forum.com/opinion/a-risk-based-view-of-why-banks-are-experimenting-with-bitcoin-and-the-block>>, (Last accessed 14-12-2020).
- [16] Thomson Reuters, “Bitcoin 101 How to get started with the new trend in virtual currencies” (White Paper), 2016, <https://web.archive.org/web/20161005044141/http://www.trssl.com/wp-content/uploads/2013/05/White_Paper_Bitcoin_101.pdf>, (Last accessed 14-12-2020).
- [17] CoinMarketCap, Today’s Cryptocurrency Prices, <<https://coinmarketcap.com>>, (Last accessed 09-02-2021).
- [18] Ledger, “A brief history on Bitcoin & Cryptocurrencies”, 23 October 2019, <<https://www.ledger.com/academy/crypto/a-brief-history-on-bitcoin-cryptocurrencies>>, (Last accessed 14-12-2020).

- [19] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, 2008, <<https://bitcoin.org/bitcoin.pdf>>, (Last accessed 14-12-2020).
- [20] Lin, I., & Liao, T. (2017). A Survey of Blockchain Security Issues and Challenges. *Int. J. Netw. Secur.*, 19, 653-659, <<https://www.semanticscholar.org/paper/A-Survey-of-Blockchain-Security-Issues-and-Lin-Liao/f61edb500c023c4c4ef665bd7ed2423170773340?p2df>>, (Last accessed 14-12-2020).
- [21] Philemon Viennas, “Ethereum Consensus and Scalability (Blockchain series — Part III)“, 26 October 2018, Medium, <<https://medium.com/bethereum/ethereum-consensus-and-scalability-blockchain-series-part-iii-4acd78d0eb41>>, (Last accessed 14-12-2020).
- [22] Lu Yang, “The blockchain: State-of-the-art and research challenges”, September 2019, Journal of Industrial Information Integration, Volume 15, 2019, Pages 80-90, ISSN 2452-414X, <<https://www.sciencedirect.com/science/article/abs/pii/S2452414X19300019#bib0034>>, (Last accessed 14-12-2020).
- [23] Tobias Svenblad, “An Analysis of Using Blockchains for Processing and Storing Digital Evidence”, Bachelor’s Degree Project, May 29th 2018, Dalarna University, <<http://www.diva-portal.org/smash/get/diva2:1218121/FULLTEXT01.pdf>>, (Last accessed 14-12-2020).
- [24] Nick Szabo, “Smart Contracts“, 1996, <<https://web.archive.org/web/20160323035617/http://szabo.best.vwh.net/smart.contracts.html>>, (Last accessed 14-12-2020).
- [25] Xavier Decuyper, “Smart Contracts (Simply Explained)”, 2017, <<https://www.savjee.be/videos/simply-explained/smart-contracts/>>, (Last accessed 14-12-2020).
- [26] Xavier Decuyper, “How does a blockchain work”, 2017, <<https://www.savjee.be/videos/simply-explained/how-does-a-blockchain-work/>>, (Last accessed 29-01-2021).
- [27] Lukas K., “What is Blockchain and Smart Contracts? Brief introduction”, 1 June 2017, Medium, <<https://medium.com/startup-grind/gentle-intro-to-blockchain-and-smart-contracts-part-1-3328afca62ab>>, (Last accessed 14-12-2020).

- [28] Sebastian Kovats, “Do you need a blockchain?”, <<http://kovats.at/index.html>>, (Last accessed 29-01-2021)
- [29] Karl Wüst, Arthur Gervais , “Do you need a blockchain?”, In 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), pp. 45-54. IEEE, 2018, <<https://eprint.iacr.org/2017/375.pdf>>, (Last accessed 29-01-2021)
- [30] Brant Carson, “Blockchain beyond the hype: What is the strategic business value?”, June 2018, Mckinsey Digital, <<https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value>>, (Last accessed 29-01-2021)
- [31] Tracy Kurt, “Welcome to Hyperledger Fabric”, November 2018, <<https://wiki.hyperledger.org/display/fabric/Welcome+to+Hyperledger+Fabric>>, (Last accessed 29-01-2021)
- [32] The Linux Foundation, ”Hyperledger projects”, <<https://www.hyperledger.org/use>>, (Last accessed 29-01-2021)
- [33] “Hyperledger Fabric”, <<https://hyperledger-fabric.readthedocs.io/en/latest/whatis.html#hyperledger-fabric>>, (Last accessed 29-01-2021)
- [34] Christian Cachin, “Architecture of the Hyperledger Blockchain Fabric”, July 2016, IBM Research - Zurich, <<http://bytacoin.io/main/Hyperledger.pdf>>, (Last accessed 29-01-2021)
- [35] Hyperledger, “Typical Hyperledger Composer Solution Architecture”, <<https://hyperledger.github.io/composer/latest/introduction/solution-architecture>>, (Last accessed 29-01-2021)
- [36] Hyperledger, “Welcome to Hyperledger Composer”, <<https://hyperledger.github.io/composer/latest/introduction/introduction.html>>, (Last accessed 29-01-2021)
- [37] Protocol Labs, “IPFS”, <<https://ipfs.io/>>, (Last accessed 29-01-2021)
- [38] Coral Health, “Learn to securely share files on the blockchain with IPFS”, February 20 2018, Medium, <<https://mycoralhealth.medium.com/learn-to-securely-share-files-on-the-blockchain-with-ipfs-219ee47df54c>>, (Last accessed 29-01-2021)

- [39] I. Hingorani, R. Khara, D. Pomendkar and N. Raul, "Police Complaint Management System using Blockchain Technology," *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, Thoothukudi, India, 2020, pp. 1214-1219, doi: 10.1109/ICISS49785.2020.9315884, <<https://ieeexplore.ieee.org/document/9315884>>, (Last accessed 11-03-2021).
- [40] S. Jattan, V. Kumar, A. R, R. R. Naik and S. N S, "Smart Complaint Redressal System Using Ethereum Blockchain," *2020 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*, Udupi, India, 2020, pp. 224-229, doi: 10.1109/DISCOVER50404.2020.9278122, <<https://ieeexplore.ieee.org/document/9278122>>, (Last accessed 11-03-2021).