

ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

SCHOOL OF ECONOMICS AND MANAGEMENT

Second Cycle Degree in Direzione Aziendale – International Management

*A Methodology for Designing and Executing Smart Contracts Using
Business Process Choreography and Private Blockchain:
The Insurtech Case of Shared Technologies*

Defended By

Rocco Goldschmidt
0000918531

Supervisor

Stefano Ferretti

Graduation Session III
Academic Year 20/21

Abstract

The purpose of this thesis is to model blockchain-based smart contracts using collaborative business process solutions such as the Business Process Model and Notation (BPMN). In this thesis, a collaborative business process involving mutually untrusted parties in a decentralized environment is provided. Most specifically, a process choreography for the underwriting of a train delay policy through a parametric insurance to automate claims with smart contracts is illustrated.

Keywords: Parametric Insurance, Decentralized Finance (DeFi), Blockchain, Smart Contracts, Oracles, Business Process Model and Notation (BPMN)

Table of Contents

Introduction.....	7
1 The Future of Insurance	8
1.1 Industry Overview – Insurtech	8
1.2 Trends and Technologies	10
1.3 Parametric Insurance	15
1.4 Benefits of DLTs for the Insurance Sector	17
2 Blockchain and DLT	20
2.1 Decentralized Finance (DeFi)	20
2.2 Blockchain Features	26
2.3 Permissionless vs Permissioned	29
2.4 Consensus Mechanisms	30
3 Smart Contracts	36
3.1 Decentralized Contracting.....	36
3.2 Oracles	39
3.3 APIs.....	42
3.4 Ethereum Solidity	43
3.5 Limits to Existing Smart Contracts.....	45
4 Modelling Business Process Choreographies.....	47
4.1 Business Process Model and Notation (BPMN)	47
4.2 Shared Technologies.....	48

5	Project - Insurtrain	52
5.1	Introduction and Objectives	52
5.2	RACI Model	54
5.3	Process Representation	57
5.4	Data Structure and Codes	61
5.5	Data Interfaces with IT	64
5.6	Results and Limits	65
	Conclusion	69
	Bibliography	70

Table of Figures

Figure 1: Global Insurtech Equity Funding (\$ millions).....	8
Figure 2: VC Global Investment by Industry: 2016 vs 2020.....	9
Figure 3: DeFi Architecture.....	24
Figure 4: Total Value Locked (TVL) in DeFi contracts (USD).....	26
Figure 5: Centralized, Decentralized and Distributed.	28
Figure 6: PoW Mechanism.	32
Figure 7: Approximate Energy Consumption Per Transaction.	34
Figure 8: CryptoKitty Dragon #896775.....	38
Figure 9: Chainlink Nodes Validation.....	40
Figure 10: Logo Shared Technologies.	49
Figure 11: Business Process Development Cycle of Shared Technologies.....	50
Figure 12: Train Insurance Smart Contract Representation.....	52
Figure 13: Orchestica (multi-pool) BPMN Representation.....	58
Figure 14: Harp Client (private) BPMN Representation	59
Figure 15: Harp Insurance (private) BPMN Representation	60

Introduction

For many years, contracts between individuals were conducted on paper and enforced by authorities. This approach needs all participants to believe in a central authority that enforces the contract obligation if required. However, an enforcement process can still take years to settle and can cost a significant amount of money in administration and attorney fees. Recent advancements in blockchain technology have allowed the creation of smart contracts which are specified in software code. They enable secure transactions between parties that do not trust one another. Because of automatic enforcement, no party may refuse to honor its obligations in the contract, and no dispute can emerge. Barriers to trade such as uncertainty about the other party's trustworthiness, lack of reputation, asymmetry of information, or high costs of dispute settlement are reduced (Obyte, 2022). In this thesis, the role of smart contracts for decentralized insurance applications is illustrated. The insurance industry has devolved into an inefficient, expensive, and frustrating industry, making it an impeccable candidate for decentralization. However, the thesis argues that the current modelling language of smart contracts is complex. A solution to design, execute and modify smart contracts in a fast and legible way is needed in order to help this technology to reach its full potential. In this thesis, this issue is addressed by proposing modeling languages, such as the BPMN, that intuitively model the various interactions between stakeholders on blockchain. This approach is demonstrated through a decentralized insurance service, named Insurtrain, which uses oracles and data for the automatic settlement of the claim when a train is delayed. The proposed model-driven methodology supports the automatic generation of smart contracts and the controlled execution of the choreography between the client and the insurer in a transparent method. The thesis is organized as follows. In section 1, an overview of the insurance industry with reference to the most important technologies and trends is discussed. In section 2, the thesis briefly describes the concepts of the blockchain technology and how the problem of trust can be solved. Moreover, in section 3 smart contracts applications and their current modelling problem is addressed. Section 4 introduces the proposed methodology in collaboration with the insurtech start-up Shared Technologies. Finally, section 5 discusses the implementation and evaluation of the Insurtrain project.

1 The Future of Insurance

1.1 Industry Overview – Insurtech

The insurance industry is notoriously conservative and has seen very comparably limited technological improvements over the last years. Among the industries, insurance has one of the lowest customer satisfaction and loyalty ratings, indicating a sense of distrust from individuals. (Dickinson, 2015). Characterized by a fragmented value chain and a scarce digitalisation, the insurance sector is under pressure. Nevertheless, this has opened an enormous market opportunity challenging or augmenting incumbents. A new wave of insurtechs, leveraging on technology and offering more innovative and customer-centric products, are emerging within this traditional industry (Salahshor & Scherrer, 2020). Insurance Technology (insurtech) is a field which has grown out of the Financial Technology (fintech) ecosystem, which can be described as “*any innovative ideas that improve financial service processes by proposing technology solutions according to different business situations, while the ideas could also lead to new business models or even new businesses*” (Leong & Sung, 2018). More specifically, fintech refers to technology-enabled business models that can help disintermediation, reinvent how current firms create and deliver, handle privacy, regulatory and law-enforcement issues, open new doors for entrepreneurship and seed opportunities for inclusive growth (Dhar & Stein, 2017). During the past years, insurtechs have gained traction. In particular, the impact of COVID-19 pushed incumbents to enhance digital capabilities in new ways to become more competitive than ever.

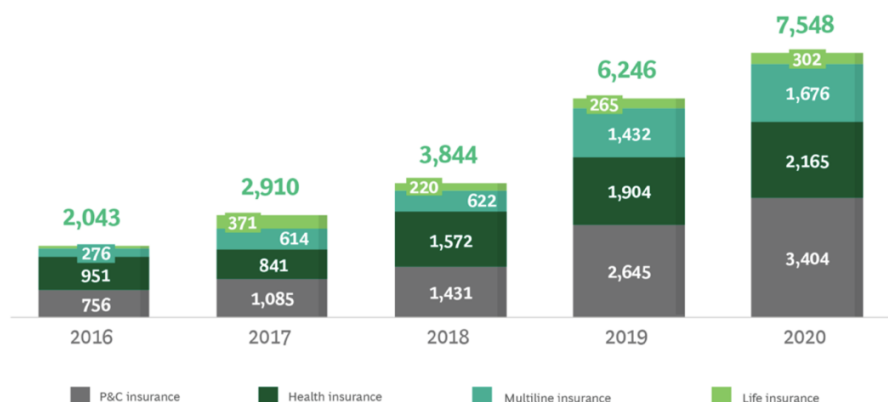


Figure 1: Global Insurtech Equity Funding (\$ millions). Source: (BCG FinTech Control Tower, 2021)

According to the Boston Consulting Group (BCG) FinTech Control Tower (2021), 2020 was a record-breaking year with global funding at \$7.5 billion, up 21% from the previous year. Moreover, already in the first three quarters of 2021 global VC investments reached \$10.5 billion so far (Sifted, 2022). As shown in figure 1, property and casualty (P&C) insurance was the highest funded-cluster (45%), followed by health insurance (29%), multiline insurance (22%) and life insurance (4%) (BCG FinTech Control Tower, 2021).

The insurtech environment is often observed only in the context of startups. However, according to A. Kelley and K. Wang (2021), it is present in a broader “*ecosystem of focused, innovation-based companies*” disrupting the interaction between insurers and their customers, the automation of processes, and the modification of old/creation of new insurance products (Kelley & Wang, 2021). The insurance sector is one of the biggest industries with a \$6 trillion global market. The financial sector excluding insurance represents \$12 trillion, followed by health \$8 trillion and mobility with \$5 trillion. Over the last years, insurtech has been so far underinvested compared to other sectors. However, as can be seen from figure 2, from 2016 it is growing much faster (Dealroom.co, 2021).



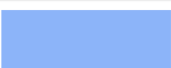
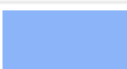
			2016	2020
Insurtech		4.1x	\$1.8B	\$7.3B
Health		2.6x	\$24.2B	\$62.6B
Mobility		1.9x	\$22.2B	\$42.5B
Fintech		1.4x	\$23.9B	\$33.8B

Figure 2: VC Global Investment by Industry: 2016 vs 2020. Source: (Dealroom.co, 2021)

The US is the pioneer market and it has been responsible for 53% of all insurtech investment transactions, followed by the UK (9%), China (7%), Germany (4%), India (4%) and France (3%) (Kelley & Wang, 2021). Within Europe, 85% of the funding since 2016 has centred around the UK (40%), Germany (29%) and France (18%) (Dealroom.co, 2021). Although still in its early adoption (adaptation) phase, insurtech companies are beginning to affect the global insurance

market. According to the Milken Institute (2018), customers are more open to purchase insurance products from tech firms and are more likely to change providers within 12 months (Mueller, 2018). Large technology firms such as Amazon, Ant Financial, Revolut, Google, Flipkart for example are moving into the insurance sector through investments, partnerships and mergers and acquisitions. Moreover, according to Willis Towers Watson (2018), 20% of insurtech funding over the next years will come from tech companies (Willis Towers Watson, 2018). Incumbents should build closer relationships, bridging the contrasting cultures and focusing on joint opportunities in order to digitize faster and augment their value proposition (PwC, 2017). Thus, the entrance of insurtech companies creates a competitive threat, however it also provides potentially valuable opportunities for partnering. Within this context, two key areas of cooperation relate to data and customers. Modern insurtechs can enable incumbents to expand insurance coverage to new market segments, introduce new products and services, simplify activities in the value chain, reduce transaction costs and deliver better risk measurement. At the same time, insurtech companies might take advantage from access to insurer's capital requirement, expertise in risk assessment and underwriting, customer base and compliance with regulation (Koprivica, 2018).

1.2 Trends and Technologies

Creating and delivering value in insurance has significantly changed, and the global COVID-19 pandemic only accelerated this. Insurers need to reimagine their business, both internally and externally, to meet the changing requirements of today's customers who are also facing new risks to their livelihood, health and wellbeing (Accenture, 2021). Climate change, cybercrime, global supply chains, disease, aging populations, technology disruption, and the sharing economy are some of the new factors that are radically changing the current risk landscape. Insurtech developments and potential innovations are expected to impact each of the following activities along the value chain: product development, underwriting and pricing, distribution of platforms and administration and claims processing. By simplifying these activities, insurtechs increase customer centricity in an industry which lags convenience and clarity (Salahshor & Scherrer, 2020). In terms of value drivers, insurtech companies are taking advantage of technology advancements

such as Big Data, Machine Learning (ML) and Artificial Intelligence (AI), Internet of Things (IoT) and Blockchain to lower costs and provide better tailored insurance coverage.

The global blockchain insurance market size is expected to increase with a CAGR of 82% from 2021 to 2028. The use cases of blockchain within the insurance industry are expected to improve existing processes but also introduce new practices (Gromenko, 2021). In today's world, data is becoming an indispensable commodity, leading industries to transform their value chains and processes into data-driven ones. The insurance industry has observed a significant growth of data flow through various sources such as sensors or social media, allowing insurtech companies to gain competitive advantage. Big Data has impacted the insurance industry in these main three areas: IoT, Telematics, Wearable Technology

The future will always be more integrated, and this increase of frequency and specificity of data is transforming how insurers develop predictive insights of policyholders. According to Gartner, the Internet of Things (IoT) is *“the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.”* (Gartner, s.d.). Applications range from telematics, wearables to smart home devices (e.g. smoke alarms, kitchen appliances and security alarms), environmental monitoring (e.g. air and water quality, floods, earthquakes), QR code scanners, infrared sensors and laser scanners for example. In a larger scale, IoT is tapping diverse activities ranging from smart homes, smart cities, smart buildings, connected mobility (rail operations, car, autonomous fleets, etc.). IoT devices helps customers provide a more precise view of their needs and insurers better understand risk, both at time of purchase and an ongoing basis (Krishnakanthan, McElhaney, Milinkovich, & Pradhan, 2021). The emergence of the IoT has provided a tipping point and forecasts suggest that there will be more than 75 billion connected devices in use with a global market value of \$1.6 trillion by 2025 (Statista, 2021). The resulting avalanche of new data created by these devices will allow insurers to understand their clients deeply, resulting in new products, more personalized pricing and real-time service delivery (McKinsey & Company, 2021). The idea of insurers is to put customers at the core of their operations by understanding customer preferences in order to deliver customized advice, right products and tailored pricing models. IoT is expected to disrupt and revolutionize traditional insurers at an unprecedented rate. Nevertheless, IoT is not a plug-and-play technology. Instead, it

has a complex reference multi-level architecture model that hinders its full scalability (Ferretti, 2021).

Telematics refers to the “*use of wireless devices and “black box” technologies to transmit data in real time to an organization*” (Gartner, s.d.). Within the automotive insurance industry, insurers, for a long time, have assessed the risk of making an accident through rating factors such as driver’s age, gender, address, car model and claims experience by trying to predict the likelihood of claim. However, according to D. Cortis, J. Debattista, J. Debono and M. Farrell (2019), there is a problematic mispricing mechanism which leads to an adverse-selection where the low-risk individuals move out of the insured pool. This creates an effect where insurance companies offer coverage at a cost which does not accurately reflect the actual risk exposure, increasing therefore total claims costs. For example, a young driver with a sports car is more likely to be involved in an accident than a middle-aged driver with a sedan, however the driving ability is not objectively taken into consideration. Under these circumstances, telematics in insurance tries to overcome this problem by charging adequate premiums (Cortis, Debattista, Debono, & Farrell, 2019). Through on-board technologies which can measure driving metrics such as location, time of the day, speed, breaking habits, rate of acceleration and distance insurance companies can provide a better objective picture of the driving behaviors and habits. This gathered driving data combined with other factors could validate risk rating models based on behavior measurements. Therefore, a telematic device enables insurance companies to price its products in an objective, fair, accurate and personalized basis.

Similar to telematics, wearables provide the insurer with a system to better determine the true underlying risks of the insured policyholder and therefore improve their pricing models. Data is retrieved from sensors embedded in devices such as smartwatches or fashion items like jewelry, glasses, clothing and shoes. These wearables originate biometric information (e.g. physical activity, sleep data, body temperature, blood sugar, pollution exposure, cardiovascular rates, respiration information, oxygen, muscle activity, etc.) which is meaningful for health care insurers and life insurance companies. Several studies proved a relationship between physical activity and mortality outcomes (Cortis, Debattista, Debono, & Farrell, 2019). According to Deloitte (2021), 39% of individuals in the US personally own a smartwatch or fitness tracker with the majority of users being under 45 years old (Deloitte, 2021). The opportunities for wearables in the insurance industry go beyond current mortality models and could also potentially motivate healthy behavior change

as well as alerting clients to health concerns – reducing moral hazard. Nevertheless, several are the privacy considerations to examine before their use becomes mainstream.

To make sense out of the big raw data and obtain useful insights, insurers are embracing the use of Artificial Intelligence (AI)’s techniques such as Machine Learning (ML), Cognitive Automation (CA), Robotic Process Automation (RPA), computer vision and Natural Language Processing (NLP). AI applications offer insurers the possibility to create personalized experiences based on behaviors and habits in order to meet the high-speed demands of modern consumers. Additionally, insurers can improve claims turnaround cycles and change the whole underwriting process, leading to more accurate and faster analysis. With the new wave of these underlying technologies, insurance is shifting from its present state of “detect and repair” to “predict and prevent” – transforming several aspects of the industry. Instead of compensating losses, AI can be applied to risk reduction and prevention risk management solutions. Moreover, the process of underwriting will be reduced to a few seconds as the majority of the operations will be automated by a combination of machine and deep learning models, requiring very little human engineering. ML is concerned with the building and study of systems that can learn from data and is concerned with predicting the future based on the past (Ferretti, 2021). It is divided between supervised (classification, prediction/regression) and unsupervised learning (clustering). Deep learning is a subset of unsupervised ML which does not include predefined output variables, but its goal is to identify patterns among the input variables independently. Over the last years, deep learning has become increasingly popular since it requires less human effort and it processes data from a broader range of data sources (Eling, Nuesle, & Staubli, 2021). These algorithms are powered by internal data as well as external information retrieved through Application Programming Interfaces (APIs) (McKinsey & Company, 2021). Most AI applications in the insurance sector focus on specific areas of the value chain and are used for customer and operation efficiency. Insurance companies are trying to interact with their customers over the internet and/or via chatbots and robo-advisors, deploying human tasks in a more efficient way. Such technologies can also provide clients with recommendations on what product would best suit their needs. Furthermore, the automation of business processes (processing of contracts, claims reporting) and decisions (underwriting, claim settlement, product offerings) enables the insurer to accelerate tasks and improve customer satisfactions, leading to potential cost savings.

Today's most prominent startup leveraging AI within the insurtech landscape is Oscar Health which uses ML algorithms to analyze patient data and synthesize it into clinical insights. Moreover, another successful example is Lemonade which uses AI and behavioral economics to underwrite risks and manage claims. Other interesting insurtech startups using AI are ZestFinance, Clearcover, Attivio, Kasko, Cocoon and Shift Technologies for example.

Other major disruptive opportunities in the insurance industry are driven by the Distributed Ledger Technology (DLT). In essence, it is considered a database which is distributed across several independent computing devices (nodes) where changes to the data are protected and managed by cryptography and consensus, providing a reliable and transparent single source of truth. In insurance, DLT enables more efficient claims handling by automating business processes through the execution of smart contracts and oracles, arguments that will be discussed later on. Moreover, it limits the scope of disagreement between involved parties. DLT aims to transform the process of verifying transactions but also identities and smart contracts (CRO Forum, 2019). According to M. Mainelli and C. von Guten (2014), DLT impacts insurance in mainly four areas: identity, time, space and mutuality. DLT can improve the underwriting and Know Your Customer (KYC) requirements. Since claim events are recorded multiple incidents can be prevented, fraud minimized and compliance with anti-money laundering facilitated (Mainelli & Von Guten, 2014). Moreover, through DLT the insurer may be able to quote a premium without the need to retrieve data from filled forms. This analysis of transparent data combined with external info enables real-time adjustments to coverage and pricing. DLT's impact on space means that these ledgers are distributed over a network of computers, increasing the scope of application. For example, any microinsurance based on a parametric model such as climate (e.g. weather conditions) can be automated without the need of a physical evaluation. This is possible through the implementation of a smart contract built on external triggers (oracles) providing secure input. Furthermore, DLT results in more Peer-to-Peer (P2P) insurance practices where policyholders own the mutual insurance and can share the risk without even the need of an underlying entity (Mainelli & Von Guten, 2014).

Nevertheless, with great power comes great responsibility. It is precisely in this context that ownership of data generated and elaborated through these technologies becomes a delicate issue

to be taken into consideration. Data nowadays is everywhere, but data availability does not mean that it is legally permissible to process it just because it is accessible. It is acknowledged that there is a general mistrust towards insurers due to their lack of transparency and ethics. This is particularly important as insurers generally lack the skills to process and interpret this type of data efficiently. The precision and accuracy with which algorithms are able to discover patterns and calculate risk should be fairly estimated and unbiased. Hence, this can possibly lead to dangerous social credit systems where there can be some inequity in how the rating risk structure functions, leading to potential discriminations. The result can lead to a sort of commodification of the individual, presenting serious consequences if the consumer cannot obtain insurance as their risk factor is too high (Barsan, 2020). Being conscious of the potential social costs of the IoT and AI and being proactive are key actions that policymakers should make in ensuring that consumers are fairly protected (OECD, 2020). Part of this data is very intimate and data owners (including insurers) should ethically ensure that the customer understands and consents to the way information is gathered and used. Data dependence comes at a price and the emergence of insurtech is making these concerns more prominent. Nevertheless, the impact on underwriting practices of prudential requirements of insurers and the broader issue of social inclusion should be subject to further studies (Lin, 2019). Furthermore, this unbound collection of customer data and its exclusive exploitation can even increase the imbalanced relationship between large insurers and customers. All of this, it might lead to an unfair competitive advantage for large companies which leverage data to offer personalized products. One of the core goals of the project developed in this thesis is to address this issue by increasing transparency in order to reduce information asymmetry.

1.3 Parametric Insurance

In the late 90s, parametric insurance emerged as an objective and data-driven approach to insurance claims. Under this model, claims payments are agreed before and they are based on the occurrence of a triggering, objective and predefined event. Examples of such events can be a train delay (case study of the project developed), temperature, rainfall, wind, speed, sea level, earthquakes, death, etc. Parametric insurance is an attractive model as it avoids any type of biased and subjective assessment of damages. Over the years, this type of insurance did not progress as

rapidly due to the lack of a reliable infrastructure and available data to secure settling. However, with the emergence of the blockchain technology and the possibility to connect real-world data (through oracles) to the execution of smart contracts, parametric insurance contracted a high level of traction (Clyde & Co, 2021). Moreover, if COVID-19 pandemic has taught us anything, it is that the world is unpredictable. This is why a reliable application that can quickly and objectively settle claims is more than needed in such a volatile future. The contingent nature of such an insurance which pays out only when defined parameters are experienced makes the mechanism predictable, simple and rapid. The entire execution from the input data to the pay-out can be automated. Smart contracts, which run on blockchain, are conditional logic (if/then) that execute transactions upon the occurrence of a predetermined event. In order to trigger transactions in response to an event they are connected to entities called oracles which can bridge the blockchain with outside live data, interfacing with Application Programming Interfaces (APIs) and IoT (Zhou, 2021). The technology and methodology are applicable to every independent, trusted and verifiable data. Several industries such as agriculture (crop insurance), mobility (flight and travel delay coverage), logistics and supply chain, life and health insurance for example can be impacted by the potential use of blockchain in the insurance sector. Descartes Underwriting is using ML and real-time monitoring from satellite imagery and IoT, to help businesses against natural catastrophes and emerging risks. While, Parsyl uses IoT to monitor cold chain logistics, from perishable foods to health supplies. Currently, its technology monitors vaccines for over 200M people. Both companies raised \$120M and \$25 respectively during January 2022 (Dealroom.co, 2021). Arbol and Etherisc are other companies using smart contracts to automate parametric insurance through the oracle application Chainlink. Moreover, in 2017 AXA launched “Fizzy” – an automated blockchain-based parametric insurance against flight delays recorded on the Ethereum blockchain and connected to air traffic databases.

Parametric insurance’s solutions for weather risks are expected to increase due to the high levels of uncertainty of weather patterns. Most of the farmers are largely relying all of their production on climate conditions and the problem is expected to get even stronger in the upcoming years. Given the obvious synergy between parametric insurance and smart contracts, incumbents and insurtech startups are launching blockchain-based solutions. By doing so, they have the possibility to remain agile and competitive by developing a new portfolio of products to target customers who are

focused on efficiency and speed (Clyde & Co, 2021). By pairing these technologies, insurers can also rethink the way classes of insurance are supplied.

1.4 Benefits of DLTs for the Insurance Sector

The greater efficiencies across the insurance pipeline obtained through these technologies bring several advantages to insurers. Nevertheless, an important question should be evaluated. Is this greater efficiency also leading to a greater inclusion of individuals? More specifically, are these technological advancements simply altering firm's earnings or are they resulting in better pricing and reduced costs to the end-user? According to a research done by T. Philippon (2020), the unit cost of financial intermediation in the US has remained around 2% over the past 130 years, meaning that "*improvements in information technologies have not been passed through to the end users of financial services.*" (Mueller, 2018). Nevertheless, its provisional conclusion is that the fintech environment has the potential to provide widespread welfare benefits, but this will require modifications in existing regulations to realize its full potential. While allowing data to be transferred in real-time between numerous parties in a trusted and traceable manner, blockchain technology will result in considerable efficiency advantages, cost savings, transparency, speedier payouts, and fraud reduction. New insurance practices may be able to use blockchains to create better products and marketplaces (Consensys, 2022). According to A. Sheth and H. Subramanian (2020), smart contracts improve efficiency by reducing information asymmetry, improving enforcement by lowering transaction costs, and improving shared transaction risks by lowering transaction time, transaction uncertainty, and second-order effects due to extraneous institutional factors like local regulations, commission agents, and so on. All of this is attained by disintermediation using consensus mechanisms working on the blockchain, which drastically reduces the scope of legal institutions and penalties (Sheth & Subramanian, 2020). This technology therefore represents an opportunity for positive transformation and growth in the insurance industry. Currently, the insurance market is characterized by a significant lack of transparency and a complex contract management. This is why the potential benefits of blockchain are essential in order to gain trust from clients and acquire a competitive advantage. Some of the benefits are listed in further detail below.

Cost: more than 30% of small businesses in 2020 were uninsured despite 75% of them reporting having experienced an insurable event that year. Currently, the traditional insurance sector provides high and complicated barriers. Traditionally, the costs of hiring individuals to monitor, qualify and verify an event and authorize the payment were distributed to the policyholders. However, with the development of smart contracts and oracles networks is it possible to make insurance cheaper, faster and more accessible. Insurers can lower auditing and operating costs by not relying anymore on a subjective assessment of damages and losses. Moreover, they can secure the assurance with automatic pre-agreed payouts (Zhou, 2021).

Inclusion: by using datasets which are global and working on the blockchain it is possible to deploy insurance products in regions where several businesses, especially in the agriculture sector, do not have adequate coverage options. Under these circumstances for example, Arbol, through its trusted oracle solution Chainlink, has the possibility to provide insurance solutions to anyone that has an internet connection.

Trust: actors participating to a transaction are able to build trust without a third party. Blockchain-based smart contracts are saved and executed via a computer coding and, unlike a piece of paper, cannot be easily destroyed. Previously entered information is stored in “blocks” into the ledger and it cannot be changed. Cryptography connects each new block of data to the previous one and no one can seize control of the information because each node must verify each transaction. As a result, transactions on the blockchain are more immutable and transparent (CRO Forum, 2019). So, once the network (actors) reaches a consensus that the contract is valid the smart contract is added as a block to the chain which then monitors and verifies the execution, without the need of an intermediary. This results in an objective, independent, transparent and consistent solution for clients. Data cannot be tampered since the system is based on a shared ledger with secure and immutable information. The scope of disagreement between parties and all the handling costs involved will be limited due to the nature of blockchain. The reliability of blockchains and the increase of transparency could also facilitate fraud detection. Insurers have the possibility to eliminate multiple claims, false claims and fake replacement from the same ownership through digital authentic certifications, reducing counterfeiting. This is quite relevant if considering that 5-

10% of all insurance claims are fraudulent (Singer, 2019). Moreover, because regulators will be able to monitor everything on the ledger in real time, auditing will become much easier.

Speed: as previously mentioned most intermediaries, paperwork, claims investigation and human error are all eliminated from the payout process. This results in an obvious decrease of costs through the whole claim procedure thanks to the automation obtained through smart contracts. Parametric insurance can streamline the entire process by lowering the time of payment of the claim from months to two weeks or even less.

2 Blockchain and DLT

2.1 Decentralized Finance (DeFi)

Decentralized Finance (DeFi) is an alternative financial infrastructure built on top of public smart contracts, algorithms built in a secure and deterministic way. It is an open, permissionless and interoperable protocol stack which replicates the existing financial products on a blockchain (Schär, 2021). A decentralized solution for digital currency was a concern that many have tried to confront, however, it was not until 2009 when Satoshi Nakamoto introduced the Bitcoin Protocol (Ion, 2021). The mysterious and still unknown figure(s) behind the white paper *Bitcoin: A Peer-to-Peer Electronic Cash System* provided us a technology whose full potential has yet to be revealed (Nakamoto, 2008). DeFi does not rely on intermediaries and centralized institutions but it is instead based on open protocols and decentralized applications (DApps), most of which are built on Ethereum. It tries to avoid the complex and sophisticated traditional financial system where high costs, lack of transparency and interoperability are some of the major outlets. According to Y. Chen and C. Bellavitis (2019), the main advantages for a DeFi model are:

- **Interoperability:** ability of various blockchains to communicate with each other in the network. This free-flow of information is essential to create an easier, transparent and merit-based ecosystem without the need for an intermediary. The goal of interoperability is to enable the use to move funds and/or assets to another system. While composability is intended when a DApp on one blockchain is able to call a DApp on another one (Boneh, Gervais, Miller, Parlour, & Song, 2021). Public blockchains are open-source digital ledgers that are accessible to everyone. However, while all data on the blockchain is transparent, the infrastructure serves a self-contained ecosystem. This is done so that only miners who rigorously follow the rules of each network are able to validate and write transactions to the blockchain, ensuring the security and authenticity of the shared ledger. This system is highly effective, but the siloed nature of the blockchain is restricting the opportunities of DeFi (MakerDAO, 2021). Within a free ecosystem, users, developers and applications operate in a vast multichain universe, developing

different functionalities by generating economies of scale and stimulating innovation. DeFi is built on public blockchains and open standards with the potential of increasing the flow of financial capital across different services – creating an internet of value (Chen & Bellavitis, 2019). In contrast, Centralized Finance (CeFi) is more inclined to work in pure silos with transaction barriers and private ledgers.

Nevertheless, the limited use or even lack of interoperability is one of the biggest concerns preventing the mass adoption of its different applications. Under these circumstances, operators in the sectors will have to choose between two alternative roads to achieve a total integration. One option is to encourage the dominance of a single platform where all projects can enjoy a high level of interoperability. At the moment, Ethereum is the dominant platform for DeFi and the emergence of its ETH 2.0 project will improve its scalability. In 2019, 87% of the top 800 tokens were built around the Ethereum infrastructure (Consensys, 2018). This larger attention on the on-chain activity carried more expensive fees and an increase in the confirmation time of transactions. Ethereum approaches the limit of ca. 15-20 transactions per seconds (tps) while the visa network can process up to 24,000 tps (Boneh, Gervais, Miller, Parlour, & Song, 2021). As the number of users increases, so does the size of the blockchain, the requirements to run a node and the cost for users increase as well. This is why Ethereum must scale in order to sustain a DeFi ecosystem that can realize its full potential (Interdax, 2020). However, a better option, which avoids the inefficiencies of single monopoly and leads to a faster production of effective scaling solutions, is to increase interconnectivity across different blockchains to achieve full interoperability at the time of need. Projects such as Cosmos, Polkadot, Avalanche, Solana, Polygon and Harmony are working towards this interconnected direction (Meijer, 2016). The traction of these projects shows that the future will be in a multi-chain environment with interconnected federated bridges and pegged coins. The previous attack and exploit to the wormhole bridge between the Solana and Ethereum blockchain show even more the direction of a multi-chain future and not a cross-chain one due to the fundamental limits to security. Interoperability between blockchains, including a main chain and a sidechain, allows users to benefit from both without surrendering the host chain's advantages. This approach encourages innovation in various ecosystems without requiring a winner-take-all mindset (MakerDAO, 2021).

- **Decentralization:** current financial transactions within CeFi are mediated and controlled by financial institutions, acting as intermediaries to help reduce costs by allowing transactions to be carried out efficiently. These organizations such as JP Morgan, PayPal, or Square can however accumulate a disparate market power and leverage it to maximize self-interest, raising concerns over monopoly power (Chen & Bellavitis, 2019). In contrast, in a DeFi system, financial transactions are enabled by decentralized Peer-to-Peer (P2P) networks which can reduce transaction costs and create network effects without incurring in monopoly costs (Catalini & Gans, 2019). Within this scenario, transaction possibilities will be enlarged, and everybody should benefit from the network effects since no single entity can accumulate sufficient monopoly power to control the network and exclude others from participating (Huberman, Leshno, & Moallemi, 2019). Yet, full decentralization in DeFi is still illusory. Almost all of the DeFi solutions have central governance frameworks that define how operational priorities should be determined. The governance tokens are usually at the center of this type of centralization. This aspect of centralization could be used to establish DeFi platforms as legal entities similar to corporations. While legal systems are in the early stages of adapting, Decentralised Autonomous Organisations (DAOs), which manage many DeFi applications, have been allowed to register as limited liability firms in some states of US only since mid-2021. Moreover, the presence of some characteristics of the blockchain such as the proof of stake for example can lead to concentration of large coin-holders (so called whales). The power of these large validators can alter the blockchain, limiting its viability. Hence, some centralization seems unavoidable (Aramonte, Huang, & Schrimpf, 2021).
- **Innovativeness:** DeFi promotes permissionless and combinatorial innovation rather than open innovation and experimentation which are present within centralized platforms. As a result, developers can freely build and experiment new applications without seeking approval from a controlling party. By guaranteeing open access and permissionless innovation to the ecosystem, developers have room for creative exploration and are empowered to evolve DeFi in a fast, organic and unexpected way (Chen & Bellavitis, 2019). Models that embrace ongoing economic and social experimentation, evolution and adaption are likely to unlock opportunities and experience growth in the long-term. According to A. Thierier (2016), permissionless

innovation is “*the creativity of the human mind to run wild in its inherent curiosity and inventiveness, even when it disrupts certain cultural norms or economic business models*” (Thierer, 2016).

Moreover, DeFi can also facilitate combinatorial innovation through open-source licensing, allowing anybody to make use of their core technology stacks, tools, processes, and methods as well as to build new applications on top of them. Eric Schmidt, former Google CEO, defines combinatorial innovation as a way “*of combining and recombining existing technologies to create new inventions*” (Flairbit, 2021). Information and power are distributed systematically, and this could potentially result in an increase of market competition, leading to newer, better and cheaper financial services due to a faster pace of innovation (Chen & Bellavitis, 2019).

- **Borderlessness:** CeFi is tied to a specific geographic location with the consequence of having to adopt certain fiat currency for transactions. As a result, any transfer of value between areas with diverse currencies is subject to transactional exchange costs and deferred delays. Instead, DeFi relies on borderless cryptocurrencies and it is not tied to any specific central bank or government. This system enables a quick transfer of value across the globe with practically negligible costs (Chen & Bellavitis, 2019). Token transfers are much faster. Additionally, this speed combined with the transaction throughput can be further increased with layer 2 scaling solutions such as sidechains or state channels networks. The most promising layer 2 scaling solutions for Ethereum are Plasma, payment channels (such as Raiden Network), sidechains (such as Polygon and xDai Stable Chain), ZK-Rollups, Optimistic Rollups and L1 chains that are Ethereum Virtual Machina (EVM)-compatible (such as Avalanche, Polkadot, Cosmos, etc.) (Interdax, 2020). Additionally, due to the non-stop nature of blockchains, most DeFi markets are open 24/7.
- **Transparency:** centralized institutions secure their ledgers by restricting data access, instead DeFi secures transactions through the Distributed Ledger Technology (DLT) protocol. Each transaction is recorded on public ledgers which can be checked and verified by anyone at any time through keys and cryptographic signatures. This technology is the contractual backbone of the blockchain. With public ledgers, parties can transact with each other without pre-existing relationships or trusted intermediary, expanding the scale and scope of potential transaction (Seidel, 2018). Moreover, a system of public ledgers and open source code expose parties from

all hidden risks and biases and it helps keep record of all historical transactions, helping to explore the origin and potential consequences of any financial accident (Chen & Bellavitis, 2019).

DeFi is built on a multi-layered architecture composed of 5 specific levels, as shown in figure 1: settlement, asset, protocol, application and aggregation. Each layer is built on each other, creating an open, composable and hierarchical infrastructure. The term composability refers to the interoperability of the components, allowing therefore developers to build on top and use other parts of the stack in limitless combinations.

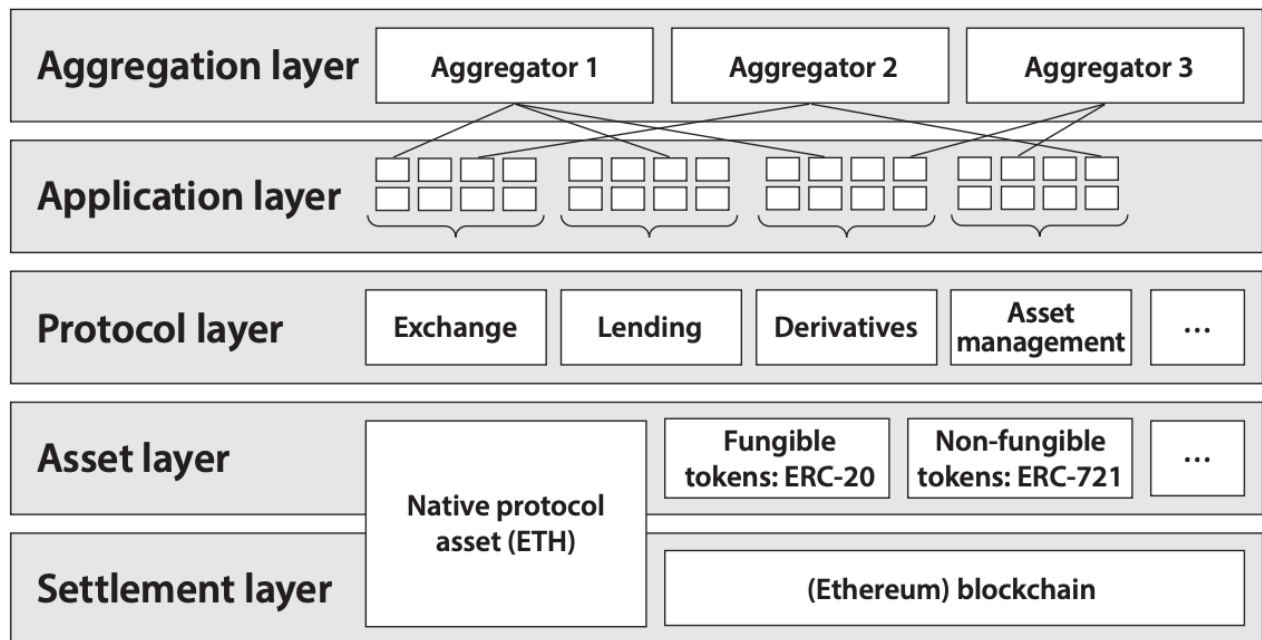


Figure 3: DeFi Architecture. Source: Schär (2021)

- 1 The settlement layer consists of the blockchain and its native protocol asset. Examples of such layers are Bitcoin (BTC) and Ethereum (ETH) blockchain. It serves as a settlement and dispute resolution, providing an incorruptible and secure ecosystem able to process settlements unbiasedly. This layer provides a sort of anchor to the network where any of the state changes should obey to the set of rules (Schär, 2021). The blockchain here acts a guarantor of trust and security. From here on every layer is built on or is compatible with the layers below it.

- 2 The asset layer consists of all tokens issued on top of the settlement layer. It is also referred to as a scalability layer serving for token transactions. The process of adding new assets to a blockchain is called tokenization and it helps transactions to be more accessible and efficient. Layer 2 includes the native protocol asset as well as any additional supported tokens operating for example on ERC-20 or ERC-721. Non-Fungible Tokens (NFTs) are usually built on the ERC-721 token standard. The vast majority of listed tokens, almost 90 %, are issued on the ETH blockchain through a smart contract referred as the ERC-20 standard (Schär, 2021). Example of such a platform operating in this layer is MakerDao (MKR) through its Dai stablecoin.
- 3 The protocol layer provides standards for specific use-cases such as debt markets, decentralized exchanges, derivatives and on-chain asset management. These protocols are highly interoperable and can be accessed by any user or DApps to handle rules and smart contracts. Within this protocol it is possible to build exchange marketplace or any financial products which use tokens from layer 2.
- 4 The application layer creates a user-oriented application connecting individual protocols. The smart contract interaction is represented by a web browser-based front end so that users can easily interact. Example of such frameworks are Liquidity Providers (LPs) and Automated Market Maker (AMM).
- 5 The aggregation layer is an extension where user-centric platforms connects several applications and protocols. Zapper, InstaDapp Zerion, Settle and Argent are the main aggregators operating to make the world of DeFi easy to understand providing a clear and friendly user interface.

DeFi is still a niche market with relatively low volumes, nevertheless these numbers are growing rapidly. The value of funds locked in DeFi-related smart contracts is measured by the Total Value Locked (TVL). This metric shows the total liquidity locked up in a DeFi contract and it measures the health and market share of the different projects (Schär, 2021). As showed in figure 3, TLV recently crossed 10 billion USD according to DeFi Pulse with Maker, Curve Finance, Convex

Finance, Aave, InstaDapp, Compound and Uniswap being the main DApps (DeFi Pulse, 2022). TVL is a significant benchmark to understand the investors' confidence in the DeFi industry. Over the last months, as can be seen from figure 3, substantial investments and capital inflow has been injected, permitting a higher degree of liquidity and stability to the system. The outstanding growth of these assets together with some innovative protocols suggests that DeFi will become relevant in a much greater expression – considering the recent interest among individuals, policymakers, corporations, researchers, investors and financial institutions.

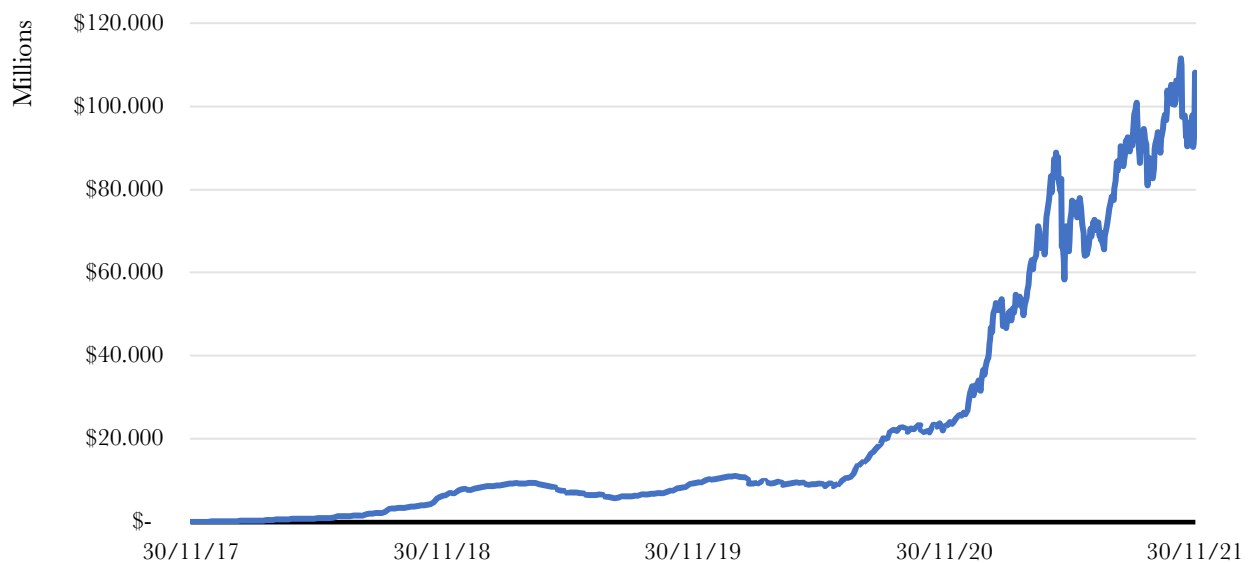


Figure 4: Total Value Locked (TVL) in DeFi contracts (USD). Data retrieved from DeFi Pulse

A new era of fintech is upon us and DeFi is going to reshape the structure of modern finance by creating a new landscape for innovation to expand financial inclusion and facilitate open access.

2.2 Blockchain Features

The term blockchain derives from the technology's structures in which data is collected and separated into chronological interconnected blocks. The sequence of these blocks is then computed in a decentralized database (ledger) on the internet which is shared with every computer, indicating that the blockchain is not merely kept in a single location or on a server with restricted access.

Blockchain is a particular subset of the DLT which records and shares data across multiple ledgers which are maintained and controlled by a distributed network of computer services, called nodes. The mechanism uses cryptography and a set of mathematical algorithms to create and verify these data structures from which information can only be added throughout the form of chain transactions blocks. Once added, data cannot be removed (persistence). Then, these new blocks are diffused to every party in the network in an encrypted way so that the details of the transactions are not public. The validity of the blocks is determined by the actors in the network through a consensus mechanism. On the blockchain, each user has two unique keys. A private key is used to digitally sign the transaction that he/she intends to carry out. Moreover, the public key serves as an address on the network and it is also used to authenticate a digital signature by confirming the sender's identity. These decentralized identities are also called addresses. Cryptography's backbone is comprised of these keys and the hash function (SHA-256). The effect of these characteristics is an open, neutral, secure and affordable system with no need to rely on a central authority. This technology has the potential to replace the old concept of trust, making it one of the most disruptive innovations in recent decades (Civiero, 2019).

Every blockchain tale begins in 2009, when Satoshi Nakamoto, the enigmatic and still unknown creator of Bitcoin, lay the groundwork for the technology (Nakamoto, 2008). Without discounting the author(s)'s contribution to solving the double-spending problem utilizing a peer-to-peer network and the proof-of-work algorithm and more crucially setting the groundwork for decades of research in cryptography, digital cash and distributed systems, to just mention a few. However, these ties can be traced back to other key players as well. The 'cypherpunk movement', with its pioneer David Chaum, aimed for anonymous electronic money and payment systems in the 1980s (Chaum, 1983). Moreover, in parallel S. Haber and W. S. Stornetta (1990) attempted to register time stamped documents using Merkle Trees (Bayer, Haber, & Stornetta, 1993). Additionally, Adam Back, the creator of Hashcash, a proof-of-work algorithm that was subsequently used in the Bitcoin mining process, contributed significantly to the current adoption of the blockchain. (Back, 1997). Nevertheless, it was only in 2009, after the financial crisis, that Bitcoin sparked people's interest in the crypto world (Ion, 2021).

The network allows people to benefit from the blockchain without need of intermediation. The network's individual 'nodes' are groups of machines sharing information and working on the same ledger. When determining the architecture of a network it is important to understand that there are three different models to consider: centralized, decentralized and distributed (Buterin, The Meaning of Decentralization, 2017). Both decentralization and distribution are often used interchangeably, however this is not entirely accurate. A distributed system can nonetheless be described as centralized in the blockchain paradigm.

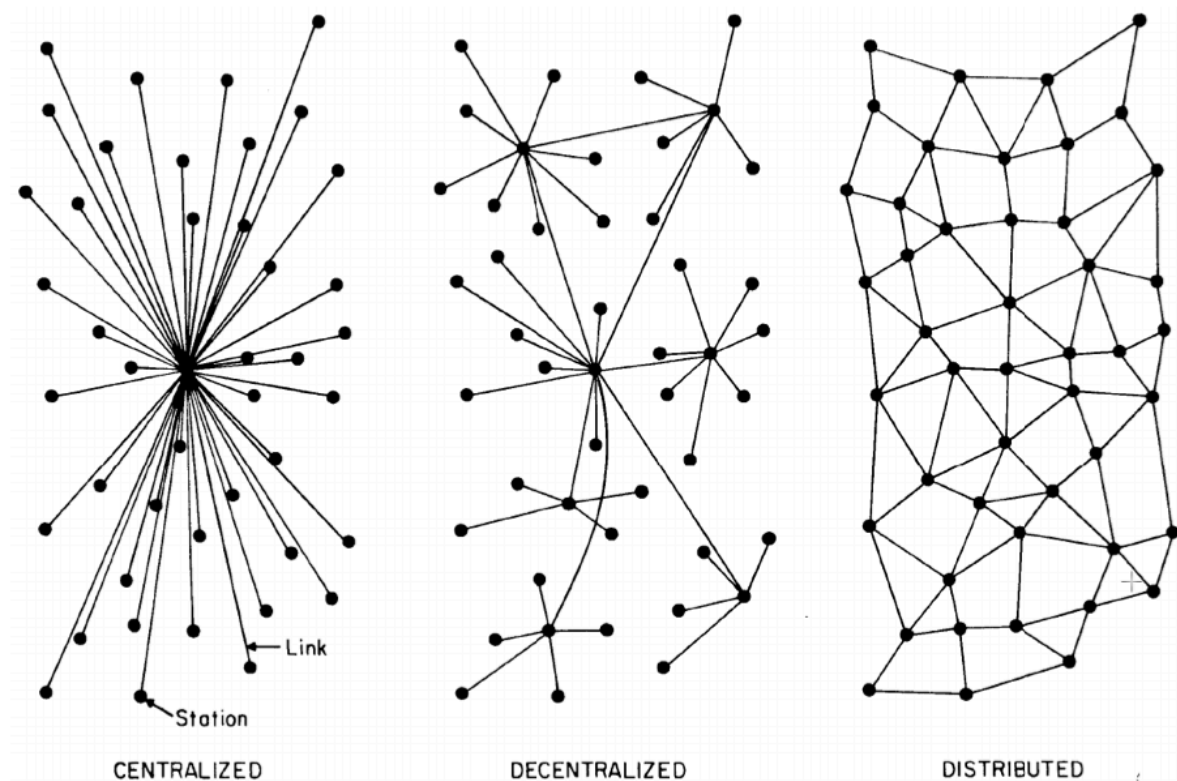


Figure 5: *Centralized, Decentralized and Distributed.* Source: (Buterin, 2017)

- Centralized systems exist when one or more client nodes are directly connected to a central server which is the single point of failure. In the event that this single point fails, the entire system will crash (Civiero, 2019).
- Decentralized systems, on the other hand, exist when information, data and files are spread and duplicated among all network nodes, with no single point of failure. According to the

founder of Ethereum V. Buterin (2017), a system can be (de)centralized in three ways: *architecturally* (depending on how many physical computers a system is made up), *politically* (depending on how many individuals or organizations exert control over the computers) and *logically* (if the system can act independently even if split in half). Traditional corporations are politically (CEO), architecturally (HQ) and logically centralized. While blockchains are politically (no one controls them, they rely on several peers) and architecturally decentralized (no single point of failure), however they are logically centralized (nodes have to agree on a unique state of data structures and the system behaves like a single computer). As a result, depending on the aforementioned dimensions, a system can be more or less (de)centralized (Buterin, The Meaning of Decentralization, 2017).

- Distributed systems are present when a server is submitted to central authority, but data and computations are distributed among different nodes. Google, for example, does not rely on a single database, but rather on a network of data centers located all over the world (Civiero, 2019).

There's a fine line between decentralization and distribution. Decentralization relates to the degree of control. Control is exercised by a single entity in centralized systems, whereas control is shared among independent units in decentralized systems. Instead distribution is more commonly used in the context of system scalability, when different elements of the system are located in separate locations. Nevertheless, decentralized systems are less likely to fail due to their characteristics of relying on separate computers. They are also more expensive to attack because they lack sensitive core points and it is also much harder for participants to collude at the expense of other participants (Buterin, The Meaning of Decentralization, 2017).

2.3 Permissionless vs Permissioned

Permissionless blockchain networks, also called trustless or public, are open to anyone since they are released as open source. There is no central authority to manage the individuals' rights to write to the blockchain, which means that anyone can join the network and access information. Of

course, by being open to anyone, permissionless networks attract malicious users who attempt to craft transactions that will bring them financial gains by taking disproportionate voting power in the system and outvoting the honest majority, jeopardizing the network's integrity and trust guarantees. This is why the blockchain networks use a protection mechanism which assumes the majority of nodes are not malevolent and control more than 51% of the network's computing power. This mechanism is called consensus protocol and will be discussed further below. These blockchains are used by hundreds of different crypto-assets, with Ethereum and Bitcoin being two examples (Ion, 2021). Because of their highly decentralized architecture, these blockchains offer various advantages, including openness to everybody (transparency) and security. However, the majority of the drawbacks of a permissionless blockchain are related to its performance. It takes a lot of energy and computer power to reach agreement, and because it's usually a huge network, it's slower and more difficult to scale (Gola & Sedlmeir, 2022).

Permissioned networks, instead, rely on some type of authority, centralized or decentralized, to decide who has the right to append new blocks. This approach has applications in sectors such as banking and supply chain where the identity of the participants must be confirmed ahead of time. Write access is often restricted to permitted parties, whereas read access may be available to all or restricted to specific parties. Because all participants are known, the consensus mechanism for permissioned blockchains is usually faster than for permissionless networks since any misbehaving node can simply be removed from the network and it is also clear who can vote (Ion, 2021). As a result, there are usually no long wait times to account for network latency or breakdowns. Permissioned blockchains, on the other hand, are not really decentralized, and there is a risk of collusion or consensus overriding. Hyperledger, R3 Corda, Quorum for example are well-known permissioned networks (Cointelegraph, s.d.).

2.4 Consensus Mechanisms

In a decentralized system where parties do not trust or even know each other, there is no trusted third-party entity that coordinates and maintains an official version of the ledger. As a result, obtaining the degree of synchronization and security required to establish a trustworthy

infrastructure is more difficult and requires a different strategy. To achieve a strong agreement among all system participants on the valid state of the ledger, a so-called consensus mechanism is used, which employs game theory and/or cryptography principles to ensure the incentive structures and the system's operation even in the presence of failures or malicious agents (Gola & Sedlmeir, 2022). The request to add new data to the ledger is not instantly approved, and the transcription of this information is subject to network consent (Civiero, 2019). Consensus includes people agreeing on values and, these algorithms often make progress when a specific share (51%) of the servers is available and follows the protocol. By doing so, participants are financially incentivized to publish a block since the winner receives transaction fees and/or a block reward. These models are incorporated into the blockchain protocols in order to create a secure, stable and sustainable system by incentivize honest actors and disincentivize malicious ones. Under these circumstances, consensus mechanisms allow distributed systems to interact and remain secure. Furthermore, regardless of the consensus algorithm used, each permissionless blockchain must have a native digital asset (token) that acts as a reward for the participants (nodes) who contribute to its maintenance.

According to D. Mingxiao, M. Xiaofeng, W. Xiangwei and C. Quihun (2017), two main problems have to be solved in blockchain applications: double spending and the Byzantine Generals Problem. Double spending means reusing the currency in two or more transactions at the same time. This creates a disparity between the spending record and the supply of that currency, undermining the trust on which the blockchain is founded. This issue is not present with fiat and traditional currency (Mingxiao, Xiaofeng, Zhang, Xiangwei, & Qijun, 2017). However, in the digital world, where the transfer of value is translated to the transfer of digital objects, an agreed registry that certifies ownership relationships is required (Gola & Sedlmeir, 2022). Protection against this issue is purely a matter of consensus. On the other hand, the Byzantine General Problem (BGP) is a widely known experiment to show the issue of disagreement amongst participants in distributed systems, and it illustrates a situation in which some of the nodes are malicious and provide conflicting information to the other peers (Lamport, Shostak, & Pease, 1982). Only a coordinated attack by all generals each controlling his own army leads to victory. Instead, as soon as one general attacks or deserts another one, the battle is lost. These malicious nodes if attacked may lead to changes of communication content between the network (Mingxiao,

Xiaofeng, Zhang, Xiangwei, & Qijun, 2017). The problem is establishing an algorithm to ensure that the loyal generals achieve an agreement. It is demonstrated that this problem can be solved using solely verbal signals if and only if more than two-thirds of the generals are faithful, so that a single traitor may confuse two loyal generals (Gola & Sedlmeir, 2022). Due to its decentralized characteristics of not having any central authority and that all participants or nodes (generals) are on an equal hierarchical level the problem arises. Under these circumstances, all participating nodes have to agree upon every message that is transmitted in the network. This is why there is a need for the design of corresponding consensus algorithms. There are diverse schemes of distributed consensus that can be used depending on the architecture of the blockchain – permissionless or permissioned. Satoshi Nakamoto introduced his Proof of Work (PoW) solution and since then other mechanism were studied to replace PoW because of its environmental concerns. The Bitcoin network consumes more electricity annually than Austria or Sweden (Gola & Sedlmeir, 2022). Other possible schemes to reach consensus are Proof of Stake (PoS), Delegated PoS, Proof of Authority (PoA), Proof of Space, Proof of Knowledge, Proof of Cooperation, Proof of Elapsed Time, Proof of Importance, Voting, Practical Byzantine Fault Tolerance, etc. (Ferretti, 2021). However, only the most relevant PoW and PoS will be explained further.

- **Proof of Work (PoW):** the core idea behind PoW is to distribute rights and rewards across nodes based on the hashing power competition. It is the consensus algorithm used in Bitcoin, and various nodes determine the answer to a mathematical problem based on the information from the previous block. The first node that solves this will be able to generate the next block and will be rewarded for it. This process of cryptographic solution is known as mining, and it ensures the network's stability (Mingxiao, Xiaofeng, Zhang, Xiangwei, & Qijun, 2017).

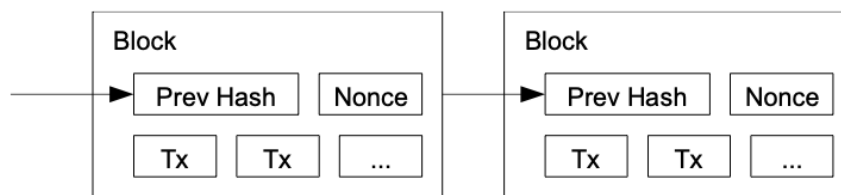


Figure 6: *PoW Mechanism.* Source: (Nakamoto, 2008)

Each block includes some data, the hash and the hash of the previous block. The Secure Hash Algorithm (SHA-256) generates this hash number with some specific properties. A hash

algorithm can be used to identify a block as well as all of its information. It is unique and unidirectional (non-invertible), which means that there is no way to return to the original input. If the input is the same then the hash remains constant, but if it changes even by one character the output hash is entirely different. This is why modifying something within the block will result in a change in the hash. The preceding block's hash is also a key component in forming a chain. Because the initial block cannot reference to earlier ones, it is referred to as the 'genesis block.' Changing a single block will make all subsequent ones invalid. During the hashing power competition, miners attempt to determine the nonce (number used once) by looping through all possible values between 0 and 2^{32} . In Bitcoin, calculating the requisite PoW and adding a new block to the chain takes roughly 10 minutes. Participants with a greater hash rate are more likely to publish the following block. This is why individual nodes attempt to enhance their hash rate in order to maximize their chances of winning and receiving the rewards. This has resulted in increased power use and rising worries about the environmental impact of PoW. However, because block generation is so costly and the length of the chain is proportional to the amount of workload, it works as a defensive for attackers because altering the blockchain history successfully requires the attacker to control more than 50% of the network's hash rate power (Ion, 2021).

- Proof of Stake (PoS): participants must prove ownership of a certain asset in order to become a validator (same as miners in PoS) in the network. Validators pledge their stake of coins to the protocol in return for transaction fees of the new minted coins. Participants are financially incentivized to publish a block and punished for creating any fraudulent activities by losing their collateral (staked coins). When transactions in a new block are discovered to be invalid, the stake is burned by the network, in what is known as a 'slashing event'. The validator is chosen by the network based on the size of their locked stake because they have the most to lose and the length of time they have held it. PoS tries to attempt the inefficiencies of PoW with the idea of increasing speed and efficiency while lowering fees. Within the PoS mechanism, the election process is much faster (smaller block time) and therefore the number of transactions a network can process per second (throughput) is increased, making the whole blockchain faster (Ion, 2021). PoS is a virtual mining and it does not require any hardware equipment and electricity to function, making the whole consensus mechanism more environmentally friendly

(Ferretti, 2021). According to C. Gola and J. Sedlmeir (2022), a PoW DLT consumes approximately a thousand times more energy than a PoS DLT (Gola & Sedlmeir, 2022) as figure 7 shows. Polkadot was selected as the first PoS blockchain with the lowest overall carbon emissions per year by the Crypto Carbon Rating Institute (2022) among the top six PoS blockchains in terms of market capitalization. Moreover, Cardano consumes the least amount of electricity per node, whereas Solana consumes the least amount of electricity per transaction (Crypto Carbon Ratings Institute CCRI, 2022). Another interesting project developed by Dapper Labs, the Canadian company behind CryptoKitties which will be further discussed, is Flow. According to new findings from Deloitte Canada (2022), minting an NFT on Flow takes less energy than a Google search or an Instagram post. In addition to operating on a PoS consensus system, Flow’s unique multi-role node architecture (Specialized Proofs of Confidential Knowledge (SPoCKs) securely divides the job of a validator into four different specialized node roles: collection, consensus, execution, and verification. This vertical pipeline specialization makes the network significantly more efficient than other blockchain architectures (Flow, 2022).

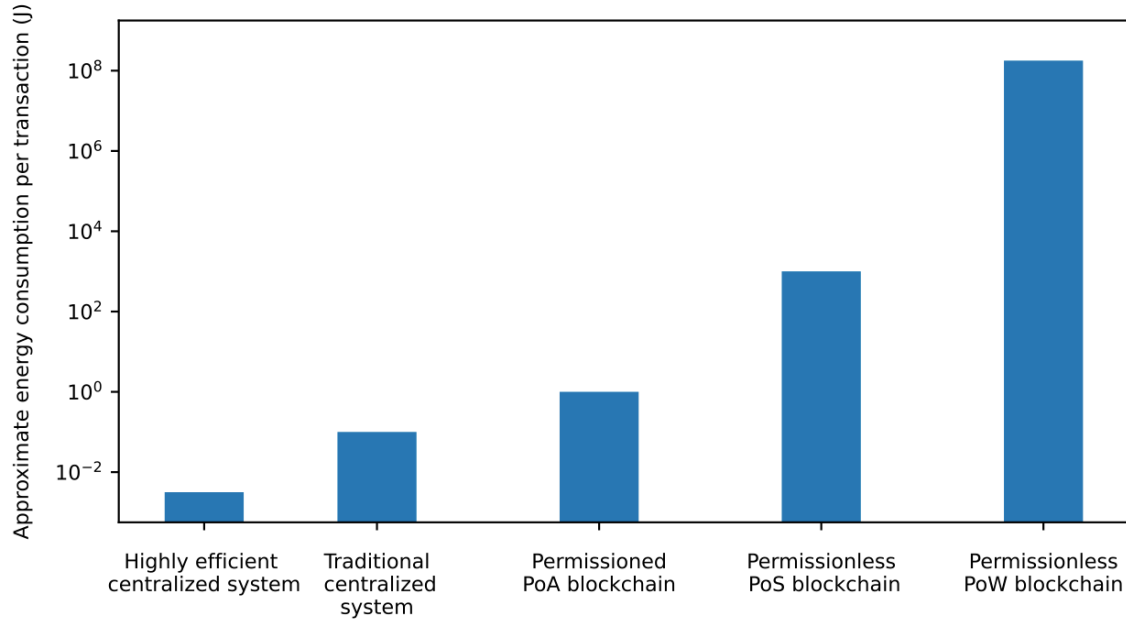


Figure 7: *Approximate Energy Consumption Per Transaction. Source: (Gola & Sedlmeir, 2022)*

PoS protocols are becoming increasingly popular. Ethereum, for example as part of its scalability mission, is in the process of moving to a PoS mechanism. Nevertheless, on the other side speed and flexibility come at a price (trilemma) and moving over to a PoS mechanism could weaken the security strength of the blockchain and present a solution where financial power is more important than computing technological power, favoring wealthy users. Nevertheless, solutions like Cardano have addressed this issue with the inclusion of a randomized selection of block producers. Because not all stakeholders have the expertise to create blocks, stake pools are used to ensure that everyone, regardless of technical experience or availability to maintain a node operating, may participate in the protocol (Cardano, 2022).

3 Smart Contracts

3.1 Decentralized Contracting

Contracts are essential for markets, firms and individuals because they facilitate collaborations and transactions. They formalize voluntary relationships and they are the basis of a market economy. In a world without contracts or currency, society is restricted to bartering, while with contracts, is it possible to trade value or money not simultaneously through the enforcement of obligations (Ferretti, 2021). Contracts, however, may be complicated and expensive due to the costs of negotiating, preparing, enforcing, and renegotiating settlements. Adverse selection and moral hazard can impede financial contracting by rising transaction costs while limiting transaction options. Currently, transacting parties rely on financial intermediaries to create trust and lower transaction costs (Chen & Bellavitis, 2019). Nevertheless, the emergence of blockchain technology over the last years has started to simplify financial contracting by replacing financial intermediaries with smart contracts. Smart contracts are computer program code stored in the blockchain that automatically execute when pre-specified conditions are fulfilled. They act as agreements, enabling transparency, immutability and flexibility (Ferretti, 2021). The term smart contract was first defined by Nick Szabo in 1994 as a “*computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs*” (Szabo, Smart Contracts, 1994). Furthermore, because of the predictable interaction between individuals and machines with no trust among the contractual parties, N. Szabo referred to vending machines as the “*primitive ancestors of smart contract*” in 1997 (Szabo, 1997). Individuals insert coins into the machine, which subsequently provides the goods requested. The machine's technological infrastructure ensures that the contract will be fulfilled as planned (De Filippi, Wray, & Sileno, 2020). However, the concept did not see the light until the emergence of the blockchain technology. V. Buterin (2013) provides another definition of smart contracts as “*systems which automatically move digital assets according to arbitrary pre-specified rules*” (Buterin, Ethereum White Paper, 2013). Under this context, it was exactly Ethereum that brought this great innovation

with its EVM to record transactions and encrypt computer programs such as smart contracts. It uses its own cryptocurrency (ETH) and provides a programming language (Solidity) for the creation of contracts. Thanks to the EVM, smart contracts have become relatively easier to program and more versatile.

By operating on the blockchain, decentralized smart contracts provide an unbiased and honest mediator to conduct actions, allowing participants to be anonymous to each other. They have various advantages, including enhanced speed and real-time updates, higher accuracy, lower execution risk, fewer insurance intermediaries, cheaper costs, and the existence of new business models (Hans, Rizk, Zuber, & Steinmetz, 2017). Smart contracts, due to their flexibility, may be used in a wide range of applications such as certificates, ownership and digital identity, games, contracting and insurance, intellectual property rights, energy grid management, healthcare, and supply chain (Caldarelli, 2020). Moreover, several smart contracting protocol standards such as ERC-20 or ERC-721 for example have been used for various purposes. For instance, the ERC-20 standard contract has been used as a mechanism for startups to raise capital via Initial Coin Offerings (ICOs). The amount of funds raised in 2019 for ICO projects was around \$14.8 billion (Statista, 2019). Another application which sparked a significant amount of interest was the case of CryptoKitties, a blockchain game, based on the ERC-721 (NFTs) protocol, developed by Dapper Labs and deployed in 2017. It is a game where users adopt, breed and trade virtual and unique kittens using smart contracts on Ethereum. The ownership of the kittens is tracked via a smart contract and each of them is represented as an NFT. This game is considered to be one of the first applications of the blockchain technology by integrating the idea of NFTs and using rarity as a factor to make the cats scarce and valuable. The now giant NFT industry reached \$22 billion in trading in 2021 compared with just \$100 million in 2020 (Milmo, 2021). On September 2018, the CryptoKitty #896775 named Dragon, as shown in figure 8, was sold for \$172,000 or 600 ETH (today approx. \$1.86 million) (CryptoKitties, 2022). This trade spread quickly interests on the internet, raising a large amount of attention and attracting new players to the game. As of March 2018, the game had gained more than 1.5 million users who had managed over \$40 million in transactions (Takahashi, 2018).

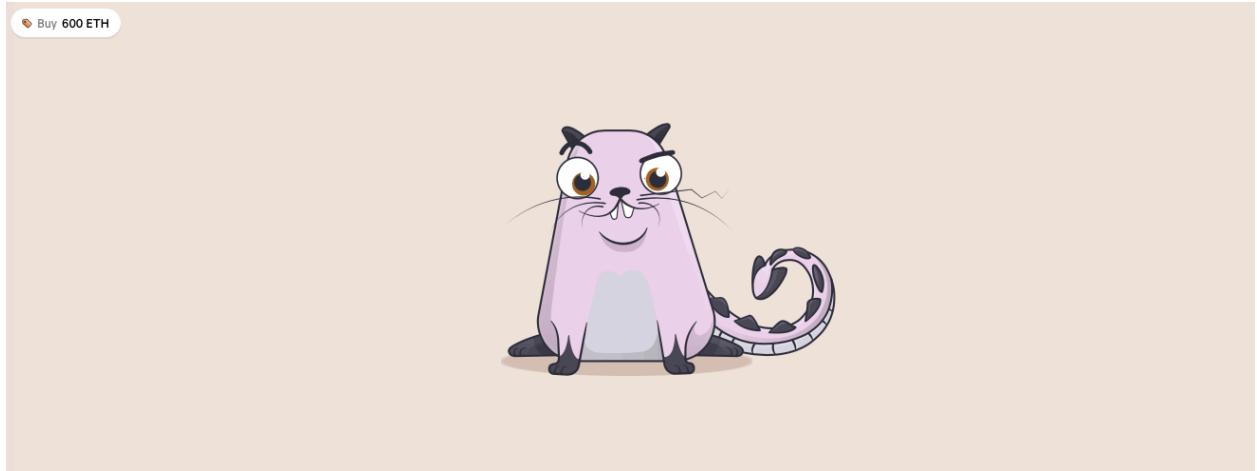


Figure 8: *CryptoKitty Dragon #896775. Source: (CryptoKitties, 2022)*

While this may sound somewhat meaningless, CryptoKitties underscored a fundamental point for the viability of smart contracts and most importantly for the feasibility of Ethereum. The game is completely decentralized, it demonstrates the scalability of Ethereum to everyday micro-transactions and the potential of digital collectibles. This concept of scarcity opened up opportunities for numerous applications that took advantage of the digital signatures. Moreover, the game introduced average users to the possibilities of blockchains and motivated developers to unlock the potential of decentralized solutions (DApps) by combining smart contracts and user interface (Dickson, 2017). The use of smart contracts for financial transactions faces several regulatory risks and scalability constraint, nevertheless the transaction volumes seen in ICOs and/or NFTs for example provide technical evidence of the security and verifiability for practical applications (Sheth & Subramanian, 2020).

Although smart contract codes are deterministic and immutable, they are neither perfect or completely trustworthy since some of its applications rely on oracles in order to communicate with the real world. Blockchain platforms are closed ecosystems and oracles try to bridge the gap between the off-chain world and the smart contract, leading to possible centralized contract execution. Such issue will be outlined in the next paragraph.

3.2 Oracles

It is important to differentiate between different smart contracts and/or DApps in order to understand which of them rely on oracles. DeFi applications like token management contracts (e.g. ERC-20), DEXes (e.g. Uniswap), NFT multi-player games where the characters or game pieces take form of NFTs (e.g. CryptoKitties) do not rely on external data (oracles) and can be fully decentralized. In contrast, lending contracts (e.g. MakerDao) which allow users to borrow against cryptocurrencies, insurance contracts (e.g. train delay insurance) where users buy policies and receive compensation in case the pre-defined event happens, and some NFT games (using randomness external info) need external data outside the blockchain in order to function correctly. For instance, parametric train insurance contracts need data from external services in order to track the status of the train. Moreover, MakerDao needs real-time price of assets to define whether loans are under-collateralized and must be liquidated. Oracles, therefore, act as a bridge that can retrieve external and non-deterministic information into a format that a blockchain can understand. They bring real-world data to the ledger, usually by reading publicly accessible API and posting data as a feed transaction on the blockchain. The term oracle comes from the Greek mythology and refers to portals through which the gods were able to communicate directly to people. In ancient stories, people turned to oracles for knowledge which was beyond their understanding in order to see the unknown future (Caldarelli, 2020). In the blockchain environment, oracles are off-chain platforms that connect blockchain with other systems. They act as a gateway by gathering and storing data from the real world with the sole control over input for smart contracts. In other words, it is a connection between real world data and blockchain decentralized systems. Examples of oracles are IoT systems and in general they are fetched through APIs. They increase the scope in which smart contracts can operate because, without oracles, they would have very limited use as they would only have access to data from within their blockchain networks. The data transmitted by oracles comes in many forms such as price information, weather conditions, sporting and political events, geolocation, static and dynamic data (e.g. temperature, time measurements), events in other blockchains, etc. Nevertheless, since oracles are third-party services they are not part of the blockchain consensus mechanism. They have power on the authenticity and accuracy of information required to execute smart contracts, and as a result, the whole trust that is given by the blockchain ecosystem falls apart. So, the blockchain, which should

be based on the premise of consensus in order to have trustless agents, is now forced to rely on oracles. As oracles are not distributed, they reintroduce the single point of failure problem and moreover their reliability needs to be trusted, removing trustless P2P interaction. This causes the ‘oracle paradox’ or ‘oracle problem’ which is seen as a major impediment to the adoption of various smart contracts (Albizri & Appelbaum, 2021). According to D. E. Ion (2021), oracles are still an immature area with ambiguity and no transparency, presenting a high risk for many DeFi protocols (Ion, 2021). To mitigate this risk, many projects are relying on Decentralized Oracle Networks (DONs). Chainlink was created in 2017 to secure smart contracts with off-chain data. The company proposed a system of decentralized oracles, based on reputation, to reproduce the consensus mechanism of a blockchain. By doing so, the company eliminates the reliability issues that might occur if using a single centralized source. As of February 15 2022, Chainlink oracles secured more than \$60 billion deposits into smart contracts and it generated more than 2.5 million verifiably random numbers for NFT distribution and gaming (Canny, 2022). As described in figure 9, the system of decentralized oracles starts when a smart contract puts out a request (request contract) for information. The Chainlink protocol, then, registers this request as an event and it creates a corresponding smart contract (service level agreement contract) on the blockchain to obtain this off-chain data. The latter generates three sub contracts, respectively named reputation, order-matching, and aggregating contract. Each of them has a particular function in order to verify the authenticity and history of the oracle and to validate them.

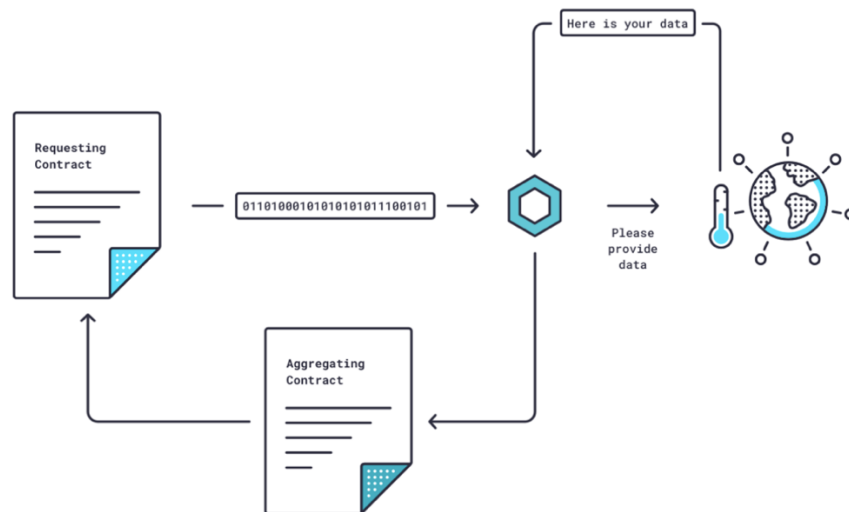


Figure 9: Chainlink Nodes Validation. Source: (Gemini, 2022)

In other words, the Chainlink software manages to translate the request from an on-blockchain to an off-chain programming language through APIs. Moreover, the aggregating contract is able to validate data from single and multiple source so that it can disregard the nodes that are dishonest and provide accurate, reliable and efficient data back to the smart contract. DECO and Town Crier, which will be further explained, are a pair of technologies currently being developed in Chainlink. The LINK token, built with the ERC-20 standard, is used to demonstrate the commitment of the operators to the network in order to incentivize good actions (Gemini, 2022).

Today, most web servers allow users to connect over a secure channel using a protocol named Transport Layer Security (TLS). URLs prefixed with a 'https' denote the use of TLS for security. However, most of these servers do not digitally sign data, and therefore a user (prover) cannot present the data to a third party (verifier), such as an oracle or smart contract, in a way to ensure the authenticity of the data obtained in the website. Under these circumstances, DECO (Decentralized Oracle) and Town Crier (TC) are designed to allow a prover from not making alterations so that the data obtained from a web maintains its integrity and confidentiality (Chainlink Labs, 2021). DECO allows users to prove that a piece of data accessed via TLS came from a particular website and prove statements about such data, keeping the info secret through cryptographic protocols and in compliance with current GDPR. By doing so, a single node can export data from a private session with a web to all nodes in a DON that then can attest the authenticity of it (Zhang, Maram, Malvai, Goldfeder, & Juels, 2020). On the other hand, Town Crier (TC) is a project from Cornell University and IC3, and recently acquired and integrated into the DON of Chainlink. It leverages trusted hardware such as Intel SGX to provide a strong guarantee that data comes from an existing and trustworthy source. Moreover, it also provides confidentiality so that customers' info is not publicly revealed on the blockchain (Zhang, Checchetti, Croman, Juels, & Shi, 2020). Both systems have similar goals but differ in their trust models and cryptographic techniques. Other advanced use cases trying to solve the problem are crypto-economic oracles that use Time-Weighted Average Price (TWAP), Verifiable Random Functions (VRFs) and wrapped currency. These solutions are trying to solve the robustness and privacy challenges of oracles systems in order to unlock the potential for DeFi applications. Nevertheless, when decentralization is insufficient, or data authenticity is not properly validated, companies controlling the service may still engage in data tampering or collusion. As a result,

neglecting to address or underestimating the oracle problem poses a significant risk to the development of real-world blockchain applications (Caldarelli, 2020).

3.3 APIs

APIs are the building blocks of several modern applications and software that are used every day. They simplify software development and innovation by enabling different applications to exchange data and functionality easily and securely. Developers do not need to know how an API is implemented but they can just use the interface to communicate with other services. API use has surged over the past decade, to the degree that many of the most popular web applications today would not be possible without APIs. They allow interoperability, frictionless integration, and delivery of new services at an unprecedented speed. By using APIs companies are reducing time-to-market by leveraging on external functionalities that do not need to be built internally. In order to initiate the process, an API call (request) from the client application is needed. After receiving a valid request, the API makes a call to the external program of web server which then sends a response to the API and finally transfers the data to the initial requesting application. Each API contains and is implemented through function calls (IBM Cloud Education, 2020). One of the most recognised API architectural style is Representational State Transfers (REST) which uses HTTP requests (GET, PUT, POST, DELETE) to access and use data. Web APIs that comply with REST architectural constraints are called RESTful APIs. REST is a prevailing choice for building public APIs because it supports multiple formats (JSON, XML, HTML, etc.), it is easier to code since it makes data available through unique URL, and it uses less bandwidth (Gillis, 2020).

In order to execute the smart contract, it is required to use a third-party API. In generally, a smart contract calls an oracle which then connects with the outside through APIs to retrieve external data. Moreover, the API information is not on-chain, so an oracle will be required to gather that information and provide the outcome so that the smart contract can execute. When bridging the blockchain and the real world, APIs are an important mechanism to query and update variable info into your smart contracts. The blockchain is designed to be entirely deterministic, meaning that the outcome of any transaction must always be the identical, regardless of where, when and

how many times you perform it. Since the internet is non-deterministic and it changes over time, every data input must be initiated through an external transaction with oracles. It is important to distinct between third-party and first-party oracles. The latter is when the API provider itself is the oracle and publishes data directly to the blockchain. Instead, a third-party oracle calls the API from another entity to get data and then publishes it to the blockchain. If the API provider published directly on-chain then the data does not have to pass through an untrusted middleman, leading to several benefits of first-party oracles. However, the current space is dominated by third-party oracles since it is difficult and risky for API providers to run first-party oracles (cryptocurrencies staking, volatility, etc.) (API3, 2022). With the rise of decentralized applications, it is crucial to be able to access web APIs, however these APIs are not yet natively compatible with DeFi. So, the problem is to receive services from traditional API providers in a decentralized way (dAPIs). In this context, API3 is building scalable, efficient, and transparent data feeds based on first-party oracles through Airnode. By doing so, consumers are able to choose their oracles (which is also the data source itself) based on reputation and data performance (Benligiray, Milic, & Vantinen, 2021). So, while Chainlink focuses more on the lack of an interface through third-party providers, API3 instead is focusing more on API connectivity between DApps and web APIs through first-party oracles. Nevertheless, both blockchain data oracles projects are trying to solve the same problem from different perspectives.

3.4 Ethereum Solidity

The concept of writing software on blockchain has only been possible for a few years. There are several platforms that enable the creation of smart contracts in standard programming language. Ethereum is the most popular, and it deals with programming languages that have been adapted to be compiled in bytecode executable from the EVM, such as Solidity and Vyper. The EVM bytecode set is Turing-complete, and users may select amongst various programming languages that miners can execute. The EVM is creating a layer of abstraction between the executing code and the machine in order to improve the software portability by enabling developers to create DApps. So, smart contracts are frequently written in the programming language Solidity, which cannot be directly executed by the EVM. They are instead compiled to low-level machine

instructions known as opcodes (Hollander, 2019). The EVM itself exists simply to ensure the continued, uninterrupted and immutable functioning of this particular state machine. It is the environment in which all Ethereum accounts and smart contracts live (Maffi, 2018). Essentially, the EVM is a worldwide 256-bit computer anybody may utilize for a small fee payable in ETH, in which all transactions are local to each network node and completed in relative synchrony (Wu, Zou, & Song, 2019). Other active and developing smart contract platforms are EOS, Tezos, NEO, Lisk, and RSK Smart Bitcoin (Costantini, 2018).

Solidity is a “*statistically typed, contract-oriented, high-level language for implementing smart contracts*” on the EVM (Wackerow, 2021). It is not the only one, but it is the most widely used and accepted. It is influenced by C++, Python and JavaScript and it cannot be directly performed by the EVM. Currently, the EVM implements 141 opcodes which can be described as low level human readable instructions of the program and all of them are represented with hexadecimal values (0x). The more complicated the smart contract, the more gas must be paid (in ETH) (Peh, 2017). Whenever there is a transfer of tokens, interaction with a contract, or anything else on the blockchain, that computation must be paid for. That payment is calculated in terms of gas, and gas is paid in ETH. A transaction's total cost is the gas limit multiplied by the gas price. The limit is intended to prevent accidental and hostile infinite loops from complicating and breaking the entire system (MyCrypto, 2021). Moreover, ETH must be reserved in advance, and any unused gas is refunded at the end of the contract execution. Each opcode has a gas cost, which can be retrieved from the Ethereum Yellow Paper (Wood, 2022). As a result, a smart contract is a coded scripted agreement between interacting parties that is stored on the Ethereum blockchain and cannot be tampered or removed. This increases the credibility of the legal document. Because the EVM is completely sandboxed and isolated from other networks too, it is impossible for a party to back out of a smart contract. In practice, this is because smart contracts have the ability to store assets (ETH for example) in escrow and move them when the contract's requirements are satisfied (Wu, Zou, & Song, 2019).

3.5 Limits to Existing Smart Contracts

Smart contracts need to be easily understandable by both humans and machines in order to attract public consent and be valued in legal and social contexts. Without that, the value will never be fully grasped. At the end of the day, very few companies fail because their technology doesn't work, but they fail for lack of customers (Anon & Gonzalez de Villaumbrosia, 2017). One obstacle that today exists in fulfilling the vision of trustless smart contracts is the requirement for shared rules that are transparent to all participants. With normal legal contracts the execution rules are written in a natural human language and therefore should be understood by most. Instead, smart contracts' rules are written in bytecode which can only be understood and executed by developers or a very limited part of our society (Lachance, 2017). Therefore, the aim of this thesis is to introduce and combine another approach by ideally enlarging the potentials of smart contracts. The solution, which will be touched in the following sections, is to develop business processes through visual representations on top of the blockchain in order to ensure trusted executions in a more transparent environment. At the moment, there is a problem in creating and modifying smart coded contracts in a fast and legible way. Contracting parties, who are not qualified to or do not have time and effort to fully understand the rules of execution, need to be entitled to a user-friendly way to accurately represent the contract conditions by still exploiting the features of the blockchain. By doing so, it is possible to reach a broader audience. Contract conditions will be graphically represented through the Business Process Model and Notation (BPMN) standard and enforced by the private blockchain of Shared Technologies. By combining low-code development and business processes it is possible to promote a higher level of transparency. What is needed is a user-friendly description where users can accurately and quickly understand the contract rules. Just as source code can be bound to bytecode, so also can a BPMN visual diagram, represented in XML, be bound to the generated source code by including the process engine version (Lachance, 2017). The aim of this solution is to overcome the high technical barriers of Solidity in order to enhance transparency and therefore trust within smart contracts. By combining the advantages of a business process management system with those of blockchain, it is possible to execute collaborative tasks between mutually untrusting parties and still maintain a ledger of transactions. Implementing agreements with graphical abstractions provides quicker process-oriented applications, without requiring low-level or specialized development skills (López-Pintado, García-Bañuelos, Dumas,

Weber, & Ponomarev, 2019). Hence, the objective still remains the same. Smart contracts are intended to simplify the execution and enforcement of legal agreements through the use of programming language (Brown, 2022). Nevertheless, the thesis argues that an evolution from complex low-code rules to a simplified approach is needed to enhance the immense potentials of smart contracts to a larger audience. Contractual rules need to reflect and regulate the complexity of human behaviour. This is why obligations cannot be easily transposed into a technical language such as coding. By drafting contractual terms in a simpler and open-ended manner, smart contracts can be applied to a larger variety of contexts. Furthermore, organizations who seek to create business-to-blockchain solutions to track and coordinate business operations into the blockchain are obstructed by skills requirement. Managers and business analyst should be interfaced using a model-driven approach, which reduces the need to know encoding language details in order to create, manage, and alter smart contracts behind collaborative processes. This degree of abstraction has long been established, in traditional business process management, through notations such as BPMN. Smart contracts should be designed to be understandable, fast, reliable and verifiable (Di Ciccio, et al., 2019)

4 Modelling Business Process Choreographies

4.1 Business Process Model and Notation (BPMN)

The Object Management Group (OMG) has developed the BPMN standard. The goal is to provide a record that is easily understandable by all business users, from the business analysts who create the initial process designs to the developers responsible for implementing the technology that will implement those processes to the business people who will manage and monitor those processes (Hribersek, 2021). As a result, BPMN attempts to graphically construct a systematic perspective of processes that can be simply read and understood by all involved stakeholders, regardless of technical expertise (Markovska, 2019). BPMN bridges the gap between business process design and execution by graphically representing artefacts such as start, end, flow, activity, event, and gateways. Formally, the model represents a graph with nodes and links. In chapter 5, examples of such representations will be shown in further depth. XML is the markup language implemented for the development of this widely used and proven industry standard. The XML schema enables integration with smart contracts and/or APIs on the blockchain (Hribersek, 2021).

BPMN offers a variety of sub-models with varying degrees of complexity. However, only orchestration and choreography will be examined. Orchestration (private) is designed for internal use and shows business processes within an organization. Interactions with other parties are frequently not displayed here, or if they are, the procedures of the external stakeholder are kept blank. Choreography (public), on the other hand, is a high-level perspective of cooperation that is beneficial when more than two organizations are engaging, or internal procedures are not yet well defined. Choreography can be useful for clarifying high-level interaction activities between partners during the early stages of a business collaboration when the detailed process flow has not yet been defined, or when organizations are unwilling to disclose their internal process flows to third parties for reasons of privacy or business secrecy (Markovska, 2019). As a result, an orchestration process describes the flow of activities of a particular participant or organization.

Choreography, instead, formalizes the way stakeholders coordinate their interactions (Polančič, 2014).

Within this context, blockchain technology allows to ensure that the parties involved in the collaboration comply with an agreed model. In a collaborative supply chain process including a purchasing business, a supplier, and a carrier, for example, blockchain allows the carrier to verify that the invoice is not sent to the supplier until the delivery has been recognized by the purchasing company. All of this may be published on BPMN, where each party registers their transactions on the blockchain and each stakeholder can then verify that the process was carried out as planned. In these settings, blockchain is used as an immutable data storage system to share process status and provide an audit trail. Related actions can be done for parametric insurances. Smart contracts check to see if the interactions are in accordance with the rules of the model. Furthermore, a BPMN choreography is employed to manage automatic payments with microservices and graphically depict the interactions between the parties (Weber, et al., 2016). With the workflow engine it is possible to automate parts of the process by informing human of tasks that they need to do and communicating results with internal and external IT systems via APIs (orchestration). The workflow engine decides which tasks or service calls take place or not.

4.2 Shared Technologies

Shared Holding is a group composed of 3 underneath pillars: a technology firm (Shared Technologies), a life insurance company (Shared Insurance), and an insurance broker (Shared Underwriters). Shared Technologies is based in Bologna (Italy) and it focuses on the development of software and hardware for blockchain-based services. Founded in 2016, Shared is an Italian company spun off by the same team and company that has already produced other successful businesses such as the accelerator Mindseeds Laboratories. The accelerator invests in specific innovation areas, such as blockchain and IoT. So far it owns 25+ patents and was involved in 2 successful exits: 1 in MedTech (Silicon Biosystems - Exit with Menarini) and 1 in Biometric Scanners (UPEK - Exit with Apple with the fingerprint scanner technology integrated on iPhones) (Shared, s.d.).

The company wants to combine blockchain technology, secure hardware and smart sensors to connect real world events to financial transactions. The vision is to “*be the best marketplace for parametric risk*” and the mission is to “*improve efficiency and transparency in insurance business processes, through the use of technology and automation*” (Shared, s.d.).



Figure 10: Logo Shared Technologies. Source: (Shared, s.d.)

Shared uses the Low Code Application Platform (LCAP) for modelling smart contracts through executable business processes. The company adopts Camunda which is an open source workflow and decision automation platform that is compliant with the BPMN standard. The platform LCAP has the following structure and is divided into Orchestica and Harp. Orchestica represents multi-process definitions and is an example of choreography. Instead, Harp represents a single process definition and is an example of private orchestration. Choreography processes, deployed on Orchestica, are used only to orchestrate the smart contracts between two or more actors, and therefore two or more pools. Choreography processes may contain only user tasks and message tasks/events. Therefore, they cannot contain any business logic. The business logic of external actors remains obscured to Shared, however, external organizations have access to APIs in order to control their part of process choreographies. For instance, they are able to initiate process choreography instances, complete tasks, set variables, set, send and receive messages to and from actors of the choreography. These controls are also executable by a Harp process through service tasks, acting as a workflow engine. In Shared, the preferred way to design a business process and the business logic is through executable Harp processes. So, Orchestica presents only the dashboard while on Harp it is possible to deploy process, build forms, check process instances history on Camunda Tasklist and Cockpit. Camunda is a simple web interface and it can be used to monitor and pilot a process instance. Camunda Modeler is used to design the process representation. Camunda Tasklist allows to start and pilot Harp process instances. A process definition represents the local process deployed on the engine and it is identified by an automatic ID and a manual key and version. Instead, a process instance is an individual execution of a process

definition. From a process definition one or more process instances can be executed. Camunda Cockpit allows to monitor the execution of Harp processes instances in real time. Moreover, it is possible to check and modify process variables by simply clicking on the value of the JSON or XML.

In Shared, the following approach is taken for smart contract creation:

1. Define business requirements
2. Design descriptive process diagram
3. Define interfaces
4. Design analytical process diagram (draft smart contract)
5. Test business logic
6. Define IT intervention
7. Design and test smart contract
8. Approve and release smart contract

A simpler version of this approach is represented in the following figure.

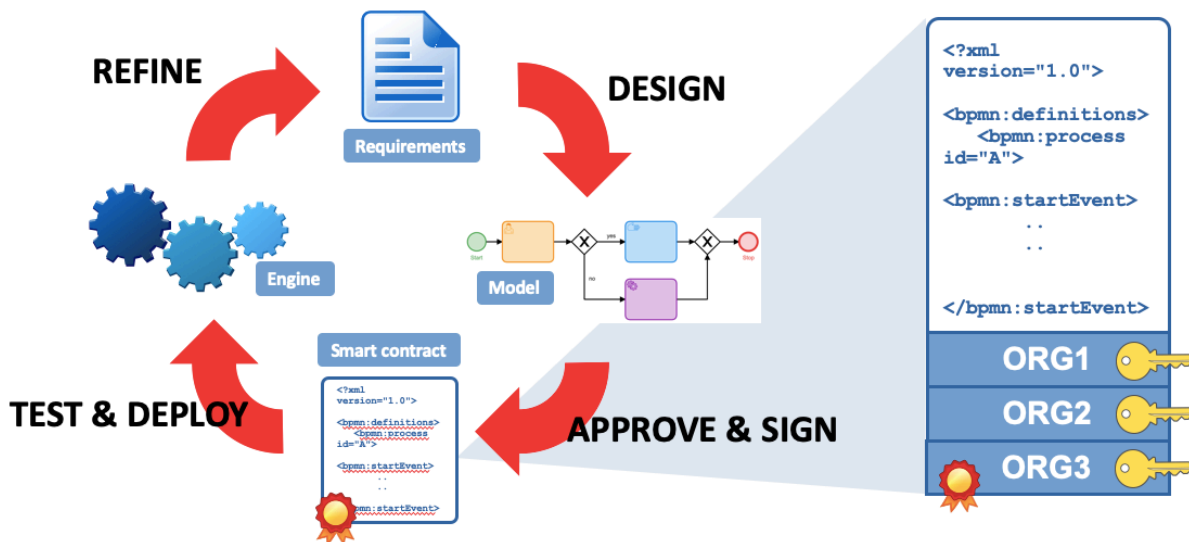


Figure 11: Business Process Development Cycle of Shared Technologies

The business analyst should define the requirements behind a business process and then graphically display these decisions and the interactions between different actors via the BPMN standard. APIs and TLS notarization are implemented. After, all the data in the messages between the interactions is encrypted and digitally signed thanks to the blockchain internally developed by Shared. The processes then are tested and deployed via the LCAP engine.

Shared Technologies supports the whole life-cycle of choreographies, from their design to their execution in blockchain. In particular, the company supports the automatic generation of smart contracts which are completely transparent to the final users. The company is still in its early-stage phase and it is trying to clearly narrow down its business model. Nevertheless, the insurtech from Bologna is trying to develop decentralized parametric insurance applications by using smart contracts. As a business analyst within the company, part of my experience was learning basic programming skills of Python and Groovy and familiarize with the BPMN standard. Moreover, data structures such as JSON and XML have been reviewed. After this learning period, I developed two main projects: - execution of a BPMN workflow for the placement of government securities (treasury bills) through an automated and competitive auction stored in blockchain; - development of a process choreography on BPMN for the underwriting of a train delay policy through a parametric insurance connected with APIs to automate claims with smart contracts. The latter will be further analysed in the next chapter.

5 Project - Insurtrain

5.1 Introduction and Objectives

The project, named Insurtrain, is a representation of a train delay parametric insurance that runs on blockchain. It enables customers to get compensated as soon as they arrive to their destination. The process is completely automated, with a smart contract determining whether or not customers are qualified for indemnification if the train is late. The figure below depicts the procedure in a simplified manner. The user selects a policy and pays the premium to the insurance smart contract. Following the customer's successful payment, the new insurance policy is created and written on the blockchain using the smart contract. When the train reaches at its destination, the smart contract uses oracles (APIs) to retrieve the timetable information from the train website. Consequently, the smart contract computes and transfers the payout (indemnity) in case the train is late according to pre-defined parameters (10 minutes delay). This method requires no human participation, and the smart contract ensures that the open-source code on which the agreement is built is unmodifiable and that the data created is certified and encrypted (Gaggioli, Eskandari, Cipresso, & Lozza, 2019).

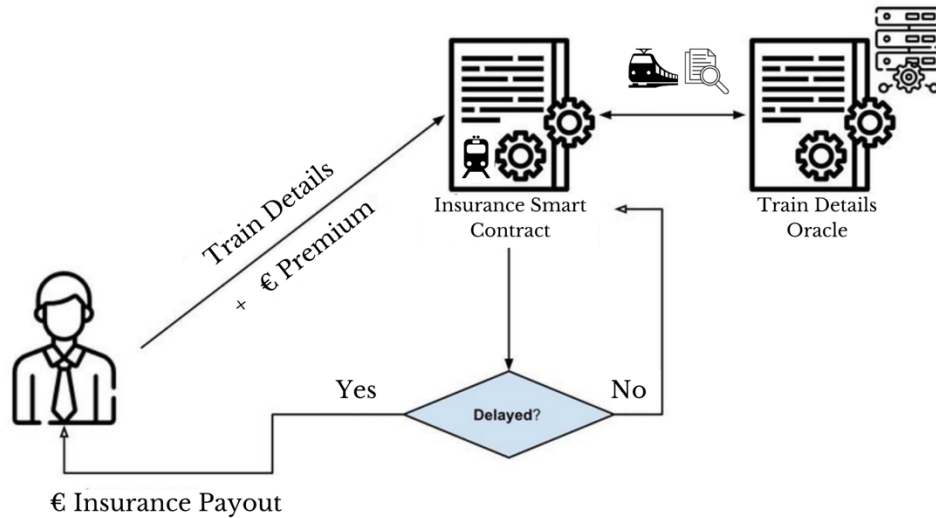


Figure 12: Train Insurance Smart Contract Representation. Adapted from (Gaggioli, Eskandari, Cipresso, & Lozza, 2019)

This insurance solution is transparent and simple. The amount of the compensation is revealed to the user in advance, and terms cannot be changed due to the immutability of the blockchain. The user does not need to request compensation. Instead, it will be automatically triggered by a public database of train status information as soon as he/she arrives to the final destination. A successful and similar experiment with flight delays insurance has been executed by Etherisc in 2016 on Ethereum and it has proven that the concept works.

This parametric solution attempts to address several customer challenges. Currently, train delay insurances are not efficient. Customers are unsure when they will be reimbursed and what are the calculations underpinning the premium and/or the indemnity, creating confusion and uncertainty about whether they are protected or not. Customers must also provide proof of delay. This is a time-consuming process that requires contacting the train company to provide proof and then sending it over to the insurer. All of this leads to an inefficient, stressful, and cumbersome process. Instead, Insurtrain's value proposition, developed in collaboration with Shared, is to rebuild trust and efficiency in the insurance sector. This solution aims to provide as much as clarity and customer-centricity as possible – whatever is promised will be delivered. The goal is to provide travelers with an automated train delay product that relies on reliable data and immediately proceeds with compensation. Characteristics of Insurtrain are respectively described.

- Automation: compensation is automatic and immediate. The user does not have to report the claim. The smart contract is connected to oracles and as soon as a delay of more than 10 minutes is observed (delay: yes/no), compensation is triggered automatically to the customer's Bitcoin wallet in this case. The compensation is certain because the contract has blocked the corresponding amount on the accounts of both the insurer and the insured. The notification of loss is automated by the smart contract since now the damage of loss is not checked by the company but is triggered by data.
- Transparency: the coverage is completely transparent, meaning that the customer knows in advance how much he/she will be reimbursed in case the train is delayed.

- **Trust:** by ensuring transparency and using blockchain this solution aims to enforce trust in an environment where asymmetries of information are typically enforced. The smart contract on the blockchain decides whether the policyholder is eligible for indemnification. In this way, the insurer has delegated the decision to an independent and reliable network, strengthening the trust and confidence that customers can have with the underwriter.
- **Secure:** by using DLT technology, the integrity of the data is recorded and encrypted in a way that no personal data is stored in blockchain (GDPR compliance) but only process metadata and the hash of the dataset.

The development of the project started by a business document (RACI model) in order to define the activities and responsibilities of the actors. This model has been then translated into a BPMN in order to visually describe the process. Then, data structures, simple coding executions, and integrations for complex micro-services with the IT department have been managed.

5.2 RACI Model

The development of the project started from a RACI (Responsible, Accountable, Consulted, and Informed) model. The two following guidelines, from Shared Technologies, were expressed: - the smart contracts, both procedural and local, must be designed in BPMN 2.0; - and, if there's a need to create IT micro-services, its data interfaces (name and type of both input and output variables) must be specified. The RACI model is used for clarifying and defining roles and responsibilities in cross-functional or departmental projects and processes. By doing so, it is possible to understand whether the actor involved in a project activity will be responsible, accountable, consulted, or informed for the corresponding task or decision (Harned, 2021).

- **Responsible:** those that complete the task and there should be at least one with this assignment for each activity.
- **Accountable:** those who assist in the completion of the task and usually is the last one to review it before it is deemed complete.

- Consulted: those with whom there is a two-way communication and it provides input on the deliverable itself.
- Informed: those who are kept up-to-date on the progress and with whom there is a one-way communication.

The RACI model of the policy life cycle process is described in the following table.

Client	Insurance	Smart contract (local – client)	Activity description
R	I	I	<p>The client fills all the necessary details for a policy quotation, that is:</p> <ul style="list-style-type: none"> • Name • Last name • Date of birth • Place of birth • Fiscal code • Place of residency • Train number of the travel • Departure date and time • Departure station • Arrival date and time • Arrival date and time • Arrival station • Ticket price • Bitcoin address
I	I	R	<p>A local smart contract calculates the quotation (premium and indemnity amount) based on the kilometres travelled.</p>

			<ul style="list-style-type: none"> • If travel distance < 100 km: <ul style="list-style-type: none"> ◦ Premium = ticket price * 5% ◦ Indemnity = ticket price * 50% • If travel distance < 200 km: <ul style="list-style-type: none"> ◦ Premium = ticket price * 6% ◦ Indemnity = ticket price * 80% • If travel distance > 201 km: <ul style="list-style-type: none"> ◦ Premium = ticket price * 7% ◦ Indemnity = ticket price * (100 + km/100) %
R	I	-	The client accepts or refuses the quotation.
R	I	-	The client sends the premium amount in Bitcoins to the Insurance address. [Bitcoin Testnet]
I	R	-	1 hour after receiving the transaction in Bitcoin, the policy is considered effective. The insurance company sends the notification to the client.
I	R	-	At the designated time (arrival time + 10 mins), a service verifies that the train has arrived at the destination.
I	R	-	If the train is delayed, the indemnity amount is automatically paid to the client's address via a Bitcoin transaction. A notification of the transaction is sent to the client. If the train is on time, no transaction is made, and the client is notified. The policy is terminated.

5.3 Process Representation

The choreographic BPMN can itself be a smart contract thanks to Shared Technologies since every organization can drive the process through APIs and digital signatures. The simulation of the project involves the insurance, the client, and the smart contract which can be connected to the train provider (Trenitalia). The process is choreographically represented in Orchestica and each actor can pilot its workflow through Harp. The following BPMN representations are displayed. Figure 13 presents the choreography process, deployed on Orchestica, between the client and the insurance. Only user tasks and message tasks/events are implemented. Instead, figure 14 and 15 contain the business logic of external actors (client and insurance) which is obscured to Shared. These organizations have access to APIs and can control their part of the process choreography through Harp.

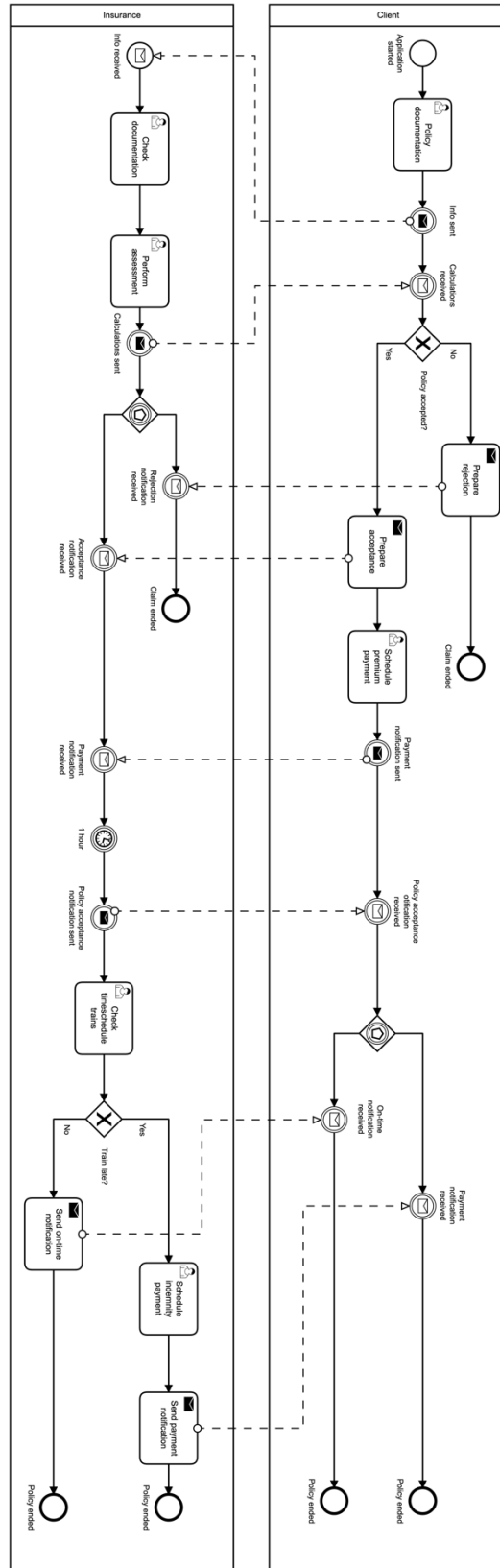


Figure 13: Orchestica (multi-pool) BPMN Representation

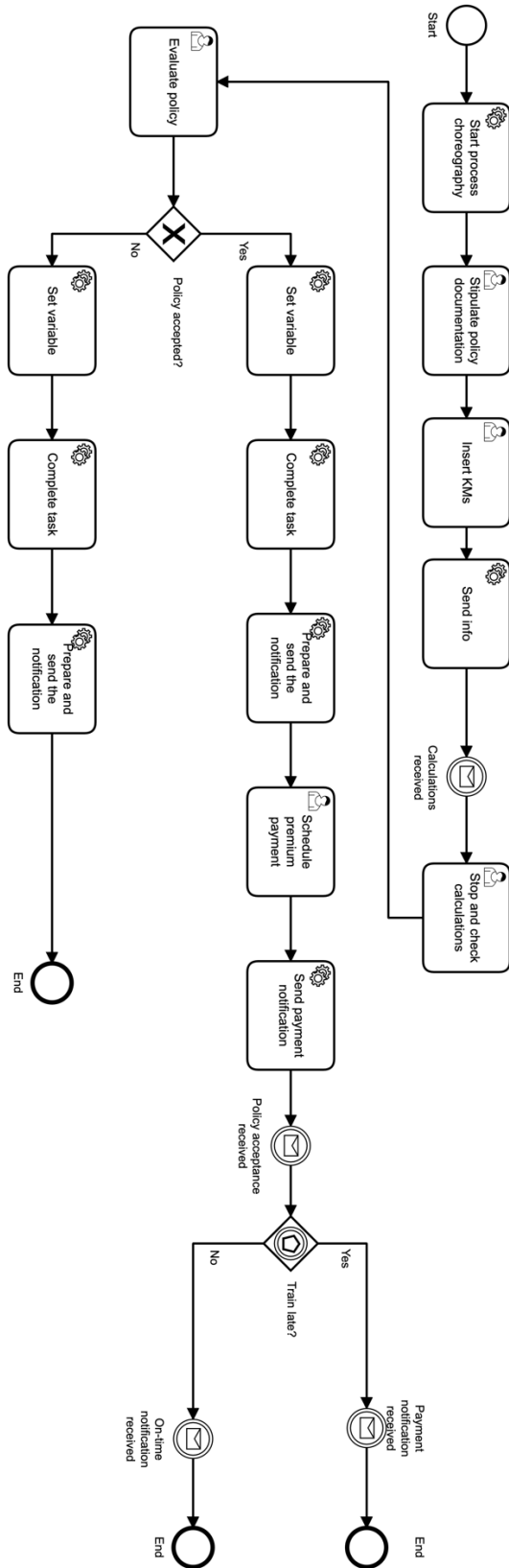


Figure 14: Harp Client (private) BPMN Representation

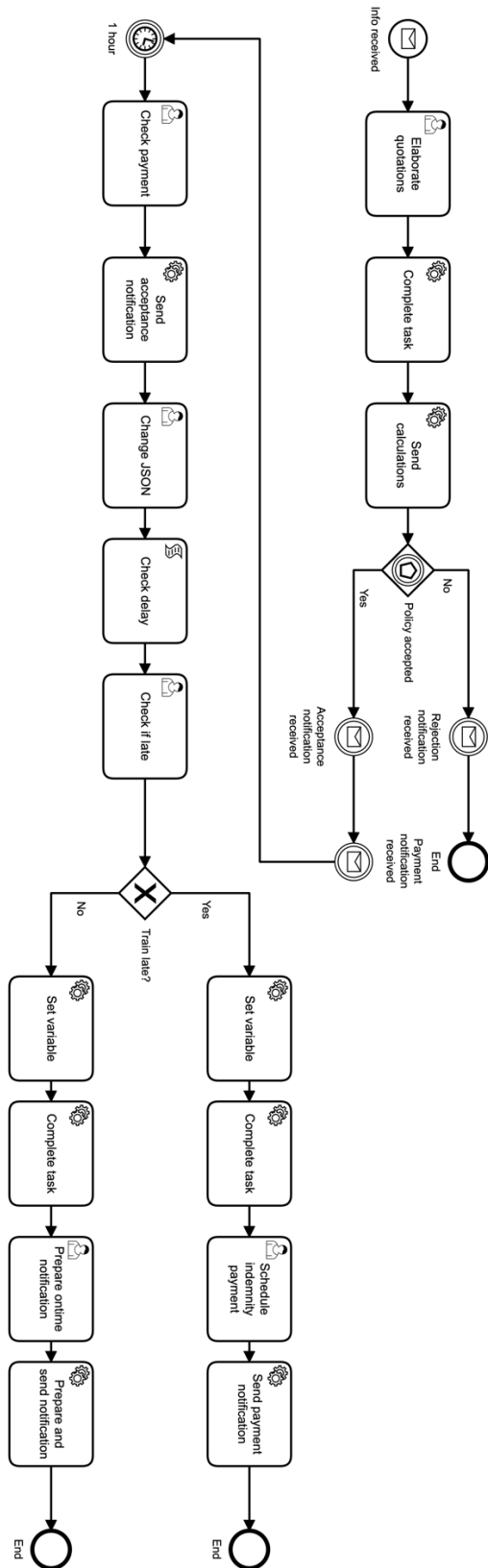


Figure 15: Harp Insurance (private) BPMN Representation

5.4 Data Structure and Codes

In this chapter the most important steps and calculations of the project are showed, however not all variables or messages are displayed. The client at the *stipulate policy documentation* user task receives an embedded *policy documentation* form built in HTML. This form is created with a drag-and-drop builder instrument to create HTML formats. Here, the client needs to insert the details of the policy in order to elaborate the quotations and to check if the train is late or not. Under this scenario, a client named Travis Scott is departing from Milano Centrale to Roma Termini the 28 May 2021 at 15:00:00 and arriving at 16:23:20. The price of the ticket is 30€.

Please, insert your required details in order to elaborate the policy quotation.

Name*	Travis
Surname	
* Scott	
Date birth	
* 30-04-1992	
Place of birth	
* Houston	
Fiscal code	
* SCTRVS92H30G892M	
Place of residency	
* San Francisco	
Train number	
* GTX563B	
Departure date and time (YYYY-MM-DD HH-MM-ss)*	2021-05-28 15:00:00
Departure date and time (unix)*	1622214000
Departure station	
* Milano Centrale	
Arrival date and time (YYYY-MM-DD HH-MM-ss)*	2021-05-28 16:23:20
Arrival date and time (unix)*	1622219000
Arrival station	
* Roma Termini	
BTC address	
* 3FZbgi29cpjq2GjdwV8eyH	
Ticket price*	30

Each of the form elements can be set to a variable usable in the process instance. Name and type must be specified. Moreover, it is possible to generate a JSON with the data filled in the created form, by declaring its name in *JSONVarName*. For each dragged element that needs to be included in the JSON, a *JSONPath* needs to be specified.

The output of the task (back-end) results in the JSON, described below, called *clientInfo* and is then send it through a message sender directly to the insurance company which then performs the calculation of the premium and the indemnity.

```
{
  "name":"Travis",
  "surname":"Scott",
  "dateBirth":"30-04-1992",
  "placeBirth":"Houston",
  "code":"SCTRV592H30G892M",
  "residency":"San Francisco",
  "number":"GTX563B",
  "departure":"2021-05-28 15:00:00",
  "departureUnix":1622214000,
  "stationDeparture":"Milano Centrale",
  "arrival":"2021-05-28 16:23:20",
  "arrivalUnix":1622219000,
  "stationArrival":"Roma Termini",
  "btcaddressClient":"3FZbgi29cpjq2GjdwV8eyHuJJnkLtkZc5",
  "price":30
}
```

After receiving this JSON, the local smart contract calculates the premium that the client needs to pay and the indemnity in case of damage. These calculations are based on travel distance and ticket price. Travel distance in this demo is asked to the client as a user task with a form field inserted directly in Camunda. In this instance, the client answered 150. The variable *travelDistance* is of type integer. Nevertheless, this task should be automated through a microservice executed with an API and this will be further discussed in the next chapter. Calculations are executed, according to the parameters in the RACI model, in the language groovy as an inline script in the properties panel of Camunda. The following libraries are imported:

```
import org.camunda.spin.json.SpinJsonNode;
import org.camunda.spin.SpinList;
import static org.camunda.spin.Spin.*;
```

The *indemnity* variable is 24€ ($= 30€ * 0,8$) and it has been calculated like this:

```
if (infoPolicy_travelDistance < 100) {
    indemnity = infoPolicy_price*0.5;
}
if (infoPolicy_travelDistance < 200) {
    indemnity = infoPolicy_price*0.8;
}
if (infoPolicy_travelDistance > 201) {
    indemnity = infoPolicy_price*((100+infoPolicy_travelDistance/100)/100);
}
intIndemnity = indemnity.intValue();

return intIndemnity;
```

And the *premium* variable is 1,8€ ($= 30€ * 0,06$) accordingly:

```
if (infoPolicy_travelDistance < 100) {
    premium = infoPolicy_price*0.05;
}
if (infoPolicy_travelDistance < 200) {
    premium = infoPolicy_price*0.06;
}
if (infoPolicy_travelDistance > 201) {
    premium = infoPolicy_price*0.07;
}
intPremium = premium.intValue();

return intPremium;
```

So, if Travis Scott wants to be insured he needs to pay 1,8€ and in case of damage (delay of 10 mins) he will get the indemnity of 24€. These quotations are sent to the client who then needs to accept or refuse them. If he refuses the amount, then the process is over. However, if he accepts then he needs to pay the premium in BTC to the insurance's address (*btcaddressInsurance*). 1 hour (PT30S = 30 seconds in the instance process for a matter of efficiency when running and debugging) after receiving the payment, the policy is effective, and the insurance sends a notification to the client. Moreover, to check if the train is late or not, simplifications are made due to technical knowledge. APIs connecting to Trenitalia's database should have been implemented, however this will be further discussed in the next chapter. In order to simplify and automate the workflow, the real arrival time (*arrivalUnix_API*) is asked directly to the insurance in an embedded form field. Time, here, is expressed in unix time stamp since it is easier for computers to store and

manipulate it rather than conventional date systems. Under this scenario, the integer value of the real arrival time is 1622219800 (Friday 28 May 2021, 16:36:40). To check if the condition (variable *late*) of the policy is triggered (parametric) the following inline script in groovy is implemented:

```
delay = (infoPolicy_arrivalUnix_API - infoPolicy_arrivalUnix);

if (delay > 600) {
    late = true;
}

else {
    late = false;
}

return late;
```

600 unix time stamp is the parameter (10 minutes) that triggers the execution of the smart contract. In this case, delay is 800 ($= 1622219800 - 1622219000$) so the train is later than 10 minutes and the indemnity amount is automatically paid to the client's BTC address with a notification of the transaction. The *if else* statement depicts the underlying concept of smart contracts which execute only if a condition is true. This, in the BPMN is translated to exclusive gateways based on boolean expressions.

5.5 Data Interfaces with IT

Moreover, in order to further implement this demo other interfaces of microservices should be implemented by the IT. Usually, requests to developers are implemented through user stories which are part of an agile approach where requirements are defined in a short and simple description. The descriptions of the user stories are the following

- **KMs finder:** as a support user I want that the kilometers of the journey are automatically calculated by fetching the variable *stationDeparture* and *stationArrival* as inputs. Both input variables are type string and through an APIs (see e.g.

<https://it.distance.to/Milano,ITA/Roma> = 476 km) the result is a variable called *travelDistance* of type integer.

- EUR to BTC converter: as a support user I want to convert the premium and indemnity from EUR to BTC so that I can send the exact amount converted in real time. The inputs of this microservice are the *premium* and *indemnity* (integers). While the output variables (type integer) are *premiumBtc* and *indemnityBtc* and can be fetched with APIs (e.g. <https://www.unitconverters.net/currency/eur-to-btc.htm>).
- BTC payment: as a support user I want to be able to integrate in the service a payment infrastructure to pay the premium and indemnity in BTC to the address. Through the Bitcoin Testnet function (<https://coinfaucet.eu/en/btc-testnet/>) it is possible to test without having to use real BTC. Moreover, an implementation with MetaMask (<https://metamask.io>) would be ideal for the final service. The inputs of the premium payment to the insurance are *btcaddressInsurance* (string) and *premiumBtc* (integer). While, the inputs of the indemnity payment to the client if train is late are *btcaddressClient* and *indemnityBtc* (integer). The output of this microservice should result in the execution of the payment.
- Train delay check: as a support user I want to be able to automatically compare the expected arrival time and the real-time arrival of the train so that the damage of the policy is automated. With APIs fetched from third-party providers (e.g. Trenitalia's database) it is possible to check if the train arrived later than 10 minutes. By inserting the number of the train, it is possible to fetch the expected arrival and then compare it with the real arrival of the train. A unix time stamp converter (<https://www.epochconverter.com>) probably is also needed to match both variables.

5.6 Results and Limits

The Insurtrain project started from a BPMN that encodes the collaboration between a client and the insurance company. The aim of the project is to depict the interactions of the two stakeholders

in order to simplify, automate and introduce trust in the whole process, without exposing the internal behavior of the participants. An initial version of a micro-insurance policy has been performed. Every instance represents a smart contract. In this section, the thesis evaluates how this approach can try to solve the problem of the need for a trusted third-party within collaborative process execution. The usage of blockchain technology empowers business partners to facilitate collaboration within choreography processes. The project attempts to lay down the foundation of a parametric insurance based on occurrence of a widely known event (train delay) which makes oracle's activity easily auditable. Moreover, by leveraging on blockchain it is possible to establish integrity and immutability of data shared between participants. As a result, blockchain enables the construction of new types of distributed systems in which all participants have a transparent overview of the ongoing system execution and can have a concrete proof of the counterpart's actions. In particular, in this choreography setting, blockchain technology is used to enable participants to build trust without a central authority, by providing non-repudiable audits (assurance that someone cannot deny the validity of something). In this way it is possible to verify that a certain participant sent/received a given message as specified (Corradini, et al., 2020). This methodology is supported by Shared Technologies, which provides a framework to foster cooperation among unrelated parties by integrating mechanisms for the management of the whole choreography life-cycle, from modelling to execution via smart contracts. Moreover, by applying such a choreographic BPMN, actors can better understand the underlying obligations of the smart contract which are not expressed in a high-level programming language. Notifications of actions performed are visible in order to automate the whole process, from requesting the policy to the payment in case the event is triggered.

According to CRM data provided by Trenitalia (2018), between 30-40% of the causes of customer complaints are related to train delays. Moreover, the average response time is around 13 days (Trenitalia, 2018). By enabling such a solution, it is possible to improve the internal efficiency of the company by reducing claim time and overall administrative costs. Moreover, the company, by relying on this implementation, can improve the omnichannel experience of the customer. This embedded insurance if integrated with the business process of a train operator such as Trenitalia can make the client's experience intuitive and quick. Customers don't want to fill up insurance forms, but they rather rely on an automated, decentralized and trustless service. Transport Focus

(2020) estimates that tens of millions of pounds go unclaimed every year in the UK. Clients are unaware or not bothered to make the claim due to the current time-consuming procedure (Transport Focus, 2020). Instead, by enabling the service developed in this project it is possible to make the railway industry more efficient for travelers and providers. If this service would be expanded to a large amount of commercial trains, a significant amount of data could be leveraged. This would allow customers to pay lower premiums for trains that are more frequently on time and clients would therefore be encouraged to select the most reliable train company, improving the whole customer experience of the industry.

The present work is considered to be a first step to provide a blockchain-based execution framework for Shared Technologies and other insurance companies. The case study intends to display the benefits of a parametric insurance via smart contract. The project's intention is to envision and show to the general public how blockchain-based solutions can be used to solve problems in day-to-day life. Nevertheless, albeit the advantages, the solution proposed seems not suitable for all processes and introduces limitations as well. Key aspects of the blockchain were not touched or implemented due to the limited technical knowledge of the author. Under this circumstance, the treatment of sensitive data about the user has not been discussed. Nevertheless, the idea of Shared Technologies is to contain on the blockchain only process metadata (train number and encrypted personal id) and the hash of the dataset. Whereas, customer information is stored encrypted in external storage only for the time needed to consume the message. Moreover, the implementation of oracles in order to fetch train data has not been executed. At the moment, there is no open and structured documentation to access train time database in Italy. Trenitalia does not offer a fully disclosed and clear API system to fetch its schedules. Moreover, attempts to digitally notarize their webpage through TLSNotary PageSigner have been tried in order to prove that data was received from a trustworthy server. All of this leads to open issues with the reliability and most importantly independency of the source of information triggering the execution of the contract. In order to address this problem, the project should cooperate with an oracle network solution so that the smart contract can access reliable and independent train data feeds from various providers. However, at the moment there are no train database alternatives providing such independent oracles. Moreover, no quantitative performance analysis has been assessed in order to measure projected revenues and cost efficiencies for the involved actors. Nevertheless, these

projections would be difficult to estimate and most likely inaccurate since the project is under an initial phase test. Probabilities of delays are not taken into consideration, so current payouts are set as a constant amount. Furthermore, some terms of contracts which are more complex still needs human decision-making to manage the claim process. In this scenario, parametric insurance will not be valid for contracts involving discretion clauses. However, the approach evaluated may still be used to make processes more efficient, transparent, and flexible.

Conclusion

Blockchain technology and smart contracts are still in an early stage of adoption. Nevertheless, these technologies undergo a disruptive economic impact to unlock value across a diverse range of sectors, providing more efficiency and transparency. The opportunities presented can enhance the traditional insurance industry, which is known for its information asymmetry, overreliance on trust, time-consuming processes, and opaque practices. Insurers have every interest to experiment blockchain-related solutions to define application that will correspond to the uses of the upcoming years. Motivated by these possibilities, the thesis wanted to show to the general public how blockchain technology can be used to solve day-to-day problems in order to increase its adoption. It presented the design and implementation of a blockchain-based train insurance product to autonomously issue policies and execute payouts for travelers who experience delays. The result is an automated insurance solution which is quicker to settle, cheaper to provision, easier to understand and more transparent given its decrease in human overhead and the blockchain infrastructure around it. Moreover, the proposal included a method to model and verify collaborative interactions between actors in an easier language. By doing so, this policy can save travelers (and train operators) time, money, and frustration.

Due to their immutable nature and decentralized security, distributed ledgers can transform the insurance industry by bringing transparency, trust, and making the barriers to entry low. Given, the automatically executed if/then conditions of smart contracts, insurers can automate a large portion of the claim process in a way that promotes trust and fairness while drastically reducing costs.

While the proposed approach has been designed with the goal of supporting collaborative process execution on blockchain for train delay coverage, its field of possible applications is wider. Climate and weather-related events and supply chain risks are two main applications for future parametric insurances.

Bibliography

- Accenture. (2021). *Technology Vision for Insurance 2021*.
- Albizri, A., & Appelbaum, D. (2021). Trust but Verify: The Oracle Paradox of Blockchain Smart Contracts. *Journal of Information Systems*.
- Anon, J., & Gonzalez de Villaumbrosia, C. (2017). *The Product Book*. Product School.
- API3. (2022). *The Rising Importance of First-Party Oracles*. Retrieved from <https://hackernoon.com/the-rising-importance-of-first-party-oracles>
- Aramonte, S., Huang, W., & Schrimpf, A. (2021). *DeFi Risks and the Decentralisation Illusion*. BIS Quarterly Review.
- Back, A. (1997). *Hashcash. 1997*. Retrieved from <http://www.cypherspace.org/hashcash/>
- Barsan, I. M. (2020). InsurTech – Opportunities and Legal Challenges for the Insurance Industry.
- Bayer, D., Haber, S., & Stornetta, S. W. (1993). Improving the efficiency and reliability of digital timestamping. *Springer*.
- BCG FinTech Control Tower. (2021). *The Pandemic Pushed Insurtech Funding to an All-Time High*. Retrieved from <https://www.bcg.com/industries/insurance/the-strategic-role-of-insurtechs-post-covid-19>
- Benligiray, B., Milic, S., & Vanttinen, H. (2021). *API3 White Paper: Decentralized APIs for Web 3.0*. Retrieved from <https://drive.google.com/file/d/1GzkLKc6DYxImgeDhoKLA4wHGIE0eGGgo/view>
- Boneh, D., Gervais, A., Miller, A., Parlour, C., & Song, D. (2021). *Decentralized Finance: Introduction to Blockchain technology*. Retrieved from Berkeley DeFi: <https://berkeley-defi.github.io/assets/material/lec2-dan-tech-intro.pdf>
- Brown, W. (2022). Limitations of code in contracts: what we can learn from the plain english movement. *Victoria University Law and Justice Journal*.
- Buterin, V. (2013). *Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform*.
- Buterin, V. (2017). *The Meaning of Decentralization*. Retrieved from <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>
- Caldarelli, G. (2020). Understanding the Blockchain Oracle Problem: A Call for Action.

- Canny, W. (2022). *BoFA Says Chainlink Likely Driver for DeFi's TLV Growth to \$203B*. Retrieved from CoinDesk.
- Cardano. (2022). *Proof of stake*. Retrieved from Cardano Docs: <https://docs.cardano.org/new-to-cardano/proof-of-stake>
- Catalini, C., & Gans, J. S. (2019). Some Simple Economics of the Blockchain. *Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16*.
- Chainlink Labs. (2021). *Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks*. Retrieved from https://research.chain.link/whitepaper-v2.pdf?_ga=2.36637032.974642780.1644663461-2032012339.1644663461
- Chaum, D. (1983). Blind signatures for untraceable payments. *Advances in cryptology, Springer*.
- Chen, Y., & Bellavitis, C. (2019). Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models. *Journal of Business Venturing Insights*.
- Civiero, M. (2019). Crypto-Assets and Decentralized Finance. *Università degli Studi di Padova*.
- Clyde & Co. (2021). *Blockchain Technology and the Future of the Global Insurance Industry*.
- Cointelegraph. (n.d.). *Permissioned Blockchain vs. Permissionless Blockchain: Key Differences*. Retrieved from <https://cointelegraph.com/blockchain-for-beginners/permissioned-blockchain-vs-permissionless-blockchain-key-differences>
- Consensys. (2018). *The State of the Ethereum Network – 2018*. Retrieved from Consensys: <https://consensys.net/blog/news/the-state-of-the-ethereum-network-2018/>
- Consensys. (2022). *What are the Benefits of Blockchain in Insurance?* . Retrieved from <https://consensys.net/blockchain-use-cases/finance/insurance/>
- Corradini, F., Marcelletti, A., Morichetta, A., Polini, A., Re, B., & Tiezzi, F. (2020). Engineering Trustable Choreography-based Systems using Blockchain. *The 35th ACM/SIGAPP Symposium on Applied Computing (SAC '20)*.
- Cortis, D., Debattista, J., Debono, J., & Farrell, M. (2019). InsurTech. In *Disrupting Finance: FinTech and Strategy in the 21st Century*. Palgrave Macmillan.
- Costantini, M. (2018). Performance, ottimizzazioni e best-practice nei contratti Solididy di Ethereum. *Università di Bologna (UNIBO)*.
- CRO Forum. (2019). *Insurance and Distributed Ledger Technology*.
- Crypto Carbon Ratings Institute CCRI. (2022). *Energy Efficiency and Carbon Footprint of PoS Blockchain Protocols*.

- CryptoKitties. (2022). *Dragon*. Retrieved from <https://www.cryptokitties.co/kitty/896775>
- De Filippi, P., Wray, C., & Sileno, G. (2020). *Smart contracts*. Retrieved from Internet Policy Review: Journal of Internet Regulation: <https://policyreview.info/open-abstracts/smart-contracts>
- Dealroom.co. (2021). *The State of European Insurtech*. Mundi Ventures, Dealroom.co.
- DeFi Pulse. (2022). Retrieved from DeFi Pulse: <https://defipulse.com/>
- Deloitte. (2021). *How the pandemic has stress-tested the crowded digital home*. Deloitte Center for Technology.
- Dhar, V., & Stein, R. M. (2017). *Fintech Platforms and Strategy*. Retrieved from Communications of the ACM: <https://cacm.acm.org/magazines/2017/10/221331-fintech-platforms-and-strategy/fulltext>
- Di Ciccio, C., Cecconi, A., Dumas, M., Garcia-Banuelos, L., Lopez-Pintado, O., Li, Q., . . . Tran, A. B. (2019). Blockchain Support for Collaborative Business Process. *Informatik Spektrum* 42 3 .
- Dickinson, B. (2015). *Insurance Is The Next Frontier For Fintech*. Retrieved from TechCrunch: <https://techcrunch.com/2015/08/05/insurance-is-the-next-frontier-for-fintech/>
- Dickson, B. (2017). *Can CryptoKitties Teach the World About Blockchain?* Retrieved from <https://uk.pcmag.com/personal-finance/92564/can-digital-kitties-teach-the-world-about-blockchain>
- Eling, M., Nuessle, D., & Staubli, J. (2021). The impact of artificial intelligence along the insurance value chain and on the insurability of risks. *The Geneva Papers on Risk and Insurance - Issues and Practice*.
- Ferretti, S. (2021). Slides: Blockchain - Distributed System, Consensus PoS. Università di Bologna (UNIBO).
- Flairbit. (2021). *What combinatorial innovation is, and how to bring it into digital transformation*. Retrieved from Flairbit: <https://flairbit.com/en/what-combinatorial-innovation-is-and-how-to-bring-it-into-digital-transformation/>
- Flow. (2022). *New findings from Deloitte Canada reveal minting an NFT on Flow takes less energy than a Google search or Instagram post* . Retrieved from <https://www.onflow.org/post/flow-blockchain-sustainability-energy-deloitte-report-nft>

- Gaggioli, A., Eskandari, S., Cipresso, P., & Lozza, E. (2019). The Middleman Is Dead, Long Live the Middleman: The “Trust Factor” and the Psycho-Social Implications of Blockchain. *Frontiers in Blockchain*.
- Gartner. (n.d.). *Gartner Glossary - Information Technology*. Retrieved from <https://www.gartner.com/en/information-technology/glossary/telematics>
- Gartner. (n.d.). *Gartner Glossary - Information Technology*. Retrieved from <https://www.gartner.com/en/information-technology/glossary/internet-of-things>
- Gemini. (2022). *What is Chainlink in 5 Minutes*. Retrieved from <https://www.gemini.com/cryptopedia/what-is-chainlink-and-how-does-it-work>
- Gillis, A. S. (2020). *REST API (RESTful API)*. Retrieved from <https://www.techtarget.com/searchapparchitecture/definition/RESTful-API>
- Gola, C., & Sedlmeir, J. (2022). Addressing the Sustainability of Distributed Ledger Technology. *Banca D'Italia, N. 670 - Questioni di Economia e Finanza*.
- Gromenko, A. (2021). *Benefits of Blockchain in Insurance: Use Cases and Main Features*. Retrieved from <https://code-care.com/blog/benefits-of-blockchain-in-insurance/>
- Hans, R., Rizk, A., Zuber, H., & Steinmetz, R. (2017). Blockchain and Smart Contracts: Disruptive Technologies for the Insurance Market. *Americas Conference on Information Systems (AMCIS)*.
- Harned, B. (2021). *RACI Charts Explained: Definitions, Example, & Template*. Retrieved from Team Gantt: <https://www.teamgantt.com/blog/raci-chart-definition-tips-and-example>
- Hollander, L. (2019). *The Ethereum Virtual Machine — How does it work?* Retrieved from <https://medium.com/mycrypto/the-ethereum-virtual-machine-how-does-it-work-9abac2b7c9e>
- Hribersek, J. (2021). Transformation of the BPMN Business Process Model Into Smart Contracts For the Hyperledger Fabric Environment. *34th Bled EConference*.
- Huberman, G., Leshno, J. D., & Moallemi, C. (2019). An Economist's Perspective on the Bitcoin Payment System. *American Economic Association Vol. 109*.
- IBM Cloud Education. (2020). *Application Programming Interface (API)*. Retrieved from <https://www.ibm.com/cloud/learn/api#toc-apis-and-c-Cp1-KCD->
- Interdax. (2020). *Scaling Ethereum on L2: Optimistic Rollups and ZK-Rollups*.
- Ion, D. E. (2021). *Decentralized Finance Analysis*. Vienna: University of Twente.

- Kelley, C., & Wang, K. (2021). *InsurTech: A Guide for the Actuarial Community*. Society of Actuaries (SOA), Willis Tower Watson.
- Koprivica, M. (2018). Insurtech: Challenges and Opportunities for the Insurance Sector. *Conference Proceedings: 2nd International Scientific Conference ITEMA 2018*.
- Krishnakanthan, K., McElhaney, D., Milinkovich, N., & Pradhan, A. (2021). *How top tech trends will transform insurance*. Accenture.
- Lachance, P. (2017). *How BPMN Could Boost The Transparency & Trust of Smart Contracts*. Retrieved from How BPMN Could Boo...
- Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, *ol. 4, No. 3*.
- Leong, K., & Sung, A. (2018). FinTech (Financial Technology): What is It and How to Use Technologies to Create Business Value in Fintech Way? *International Journal of Innovation, Management and Technology*, *Vol. 9, No. 2*.
- Lin, L. (2019). The Promise and Perils of InsurTech. *Singapore Journal of Legal Studies*.
- López-Pintado, O., García-Bañuelos, L., Dumas, M., Weber, I., & Ponomarev, A. (2019). *Caterpillar: A Business Process Execution Engine on the Ethereum Blockchain*. Retrieved from Institute of Computer Science, University of Tartu, Juhan Liivi 2, 50409 Tartu, Estonia: <https://arxiv.org/pdf/1808.03517.pdf>
- Maffi, A. (2018). Blockchain and Beyond: Proactive Logic Smart Contracts. *Università di Bologna (UNIBO)*.
- Mainelli, M., & Von Guten, C. (2014). Chain of a lifetime: How blockchain technology might transform personal insurance. *How Blockchain Technology Might Transform Personal Insurance - Long Finance, 2014*.
- MakerDAO. (2021). *What Are Blockchain Bridges, and Why are they Important for DeFi?* Retrieved from <https://blog.makerdao.com/what-are-blockchain-bridges-and-why-are-they-important-for-defi/>
- Markovska, M. (2019). Modelling Business Processes on a Blockchain Eco-System (BPMN). *University of Tartu*.
- McKinsey & Company. (2017). *Insurtech - the threat that inspires*.
- McKinsey & Company. (2021). *Insurance 2030 - The impact of AI on the future of insurance*.
- Meijer, C. R. (2016). Blockchain and Interoperability: key to mass adoption. *Finextra*.

- Milmo, D. (2021). NFTs market hits \$22bn as craze turns digital images into assets. *The Guardian*.
- Mingxiao, D., Xiaofeng, M., Zhang, Z., Xiangwei, W., & Qijun, C. (2017). A Review on Consensus Algorithm of Blockchain. *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*.
- Mueller, J. (2018). *InsurTech Rising: A Profile of the InsurTech Landscape*. Milken Institute.
- MyCrypto. (2021). *What is Gas?* Retrieved from <https://support.mycrypto.com/general-knowledge/ethereum-blockchain/what-is-gas/>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
- Obyte. (2022). *Smart Contracts*. Retrieved from <https://obyte.org/platform/smart-contracts>
- OECD. (2020). *The Impact of Big Data and Artificial Intelligence (AI) in the Insurance Sector*.
- Peh, B. (2017). *Solidity Bytecode and Opcode Basics*. Retrieved from <https://medium.com/@blockchain101/solidity-bytecode-and-opcode-basics-672e9b1a88c2>
- Polančič, G. (2014). *Conversation vs. Collaboration vs. Choreography*. Retrieved from <https://blog.goodelearning.com/subject-areas/bpmn/conversation-vs-collaboration-vs-choreography/>
- PwC. (2017). *Insurtech: the new normal for the insurance industry?*
- Salahshor, A., & Scherrer, J. (2020). Smart Contracts, Insurtechs and the Future of Insurance. *Division of Innovation Engineering, Lund University*.
- Schär, F. (2021). *Decentralized Finance: On Blockchain and Smart Contract-Based Financial Markets*. Federal Reserve Bank of St. Louis Review.
- Seidel, M.-D. L. (2018). Questioning Centralized Organizations in a Time of Distributed Trust. *Journal of Management Inquiry* 27.
- Shared. (n.d.). *Shared Website and LinkedIn*. Retrieved from <https://www.sharedchains.com>
- Sheth, A., & Subramanian, H. (2020). Blockchain and contract theory: modeling smart contracts using insurance markets. *Managerial Finance; Patrington Vol. 46, Iss. 6*.
- Sifted. (2022). *Sifted*. Retrieved from Insurtech had a record year - what's next for 2022?: <https://sifted.eu/articles/insurtech-whats-next-for-2022/>
- Singer, A. W. (2019). *Can Blockchain Improve Insurance?* Risk Management, 66(1), 20-22,24-25.
- Statista. (2019). *Amount of funds raised for cryptocurrency initial coin offering (ICO) projects worldwide as of November 2019, by leading industry*. Retrieved from Statista:

- <https://www.statista.com/statistics/802925/worldwide-amount-cryptocurrency-ico-projects-by-industry/>
- Statista. (2021). *Internet of Things (IoT) - statistics & facts*. Retrieved from Statista - Technology & Telecommunications: <https://www.statista.com/topics/2637/internet-of-things/>
- Szabo, N. (1994). *Smart Contracts*. Retrieved from <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- Szabo, N. (1997). *The Idea of Smart Contracts*. Retrieved from <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>
- Szabo, N. (1997). *The Idea of Smart Contracts*. Retrieved from <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>
- Takahashi, D. (2018). *Warriors' Steph Curry will auction off celebrity CryptoKitties (updated)*. Retrieved from Venture Beat: <https://venturebeat.com/2018/05/07/warriors-steph-curry-will-auction-off-celebrity-cryptokitties/>
- Thierer, A. (2016). *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Mercatus Center at George Mason University.
- Transport Focus. (2020). *Millions unclaimed in rail compensation watchdog claims*. Retrieved from BBC News: <https://www.bbc.com/news/uk-51401855>
- Trenitalia. (2018). *Relazione Qualità dei Servizi 2018*. Retrieved from https://www.trenitalia.com/content/dam/tcom/allegati/trenitalia_2014/informazioni/Relazione_Qualità_dei_servizi_Trenitalia_2018.pdf#page=5
- Wackerow, P. (2021). *Smart Contract Languages*. Retrieved from Ethereum: <https://ethereum.org/en/developers/docs/smart-contracts/languages/>
- Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted Business Process Monitoring and Execution Using Blockchain. *Part of the Lecture Notes in Computer Science book series (LNCS, volume 9850)*.
- Willis Towers Watson. (2018). *Quarterly InsurTech Briefing Q1 2018*.
- Wood, G. (2022). *Ethereum: A Secure Decentralised Generalised Transaction Ledger*. Retrieved from Berlin Version 630ed56 – 2022-02-13: <https://ethereum.github.io/yellowpaper/paper.pdf>

Wu, X., Zou, Z., & Song, D. (2019). *Learn Ethereum*. Packt Publishing.

Zhang, F., Checchetti, E., Croman, K., Juels, A., & Shi, E. (2020). Town Crier: An Authenticated Data Feed for Smart Contracts.

Zhang, F., Maram, D., Malvai, H., Goldfeder, S., & Juels, A. (2020). DECO: Liberating Web Data Using Decentralized Oracles for TLS.

Zhou, A. (2021). *4 Ways Blockchain Can Transform Insurance*. Retrieved from Entrepreneur: <https://www.entrepreneur.com/article/397515>