POLITECNICO DI MILANO

SCHOOL OF INDUSTRIAL AND
INFORMATION ENGINEERING

BLOCKCHAIN TECHNOLOGY: AN ADOPTION FRAMEWORK FOR FINANCIAL SERVICES

SUPERVISOR:

FILIPPO MARIA RENGA

CO-SUPERVISORS:

VALERIA PORTALE

GIACOMO VELLA

MASTER THESIS OF:

AMOROSO GIADA 872220

REGGIORI EDOARDO 862165

ACADEMIC YEAR 2017/2018

AKNOWLEDGEMENTS

Auctores scientiae move cupiditas quia
vitium grave vitandum incognitis pro cognitis
ne habeant diligentes vel assentiant novi
impetu ruere caeci timoris ad catenam causa.
Animi quae ab optime Renga Filippo donatur,
haec adiuvat libertas modusque nos umquam nullius
in speculando recentes notiones ingenis tactas.
Lumina tres sola aperte remotam inculta de alto
viam ostendunt regione quibus Jacomus nomina
Jacopus sunt perclara Valeria studiose sequimur.
Magnum officium vim da nobis difficile iter
facere et id dignus sit annorum finis cum magno
quinque labore. Corona, viridis laurus, nos caput.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABSTRACT (ITALIAN)

Questa tesi di ricerca è volta a definire le potenziali applicazioni della tecnologia blockchain nel settore finanziario, mappare come i processi as-is si evolverebbero con la sua adozione e individuare quali benefici potrebbe apportare. Tale necessità sorge da un continuo incremento dell'interesse per la tecnologia da parte di enti finanziari e startup fintech, a fronte di una scarsa letteratura scientifica che tratta il tema in modo non strutturato.

Per una maggiore completezza della ricerca, la raccolta dei dati è stata effettuata tramite molteplici metodologie:

1. da un censimento quantitativo sul web sono state costruite due basi di dati strutturate, attinenti ai progetti di startup e di istituti finanziari a livello globale;
2. da tali iniziative è stata scaricata e analizzata la relativa letteratura grigia, ove disponibile;
3. attraverso interviste a esperti del settore, sono stati generati dieci casi di studio riguardanti gli istituti finanziari italiani.

Le metodologie sono state utilizzate in modo complementare per rispondere alla domanda di ricerca. La prima ha consentito di determinare tutti i possibili ambiti applicativi della tecnologia; la seconda di mappare i processi to-be; la terza di approfondire eventuali benefici o limiti nell'adozione, nonché di confrontare la posizione degli istituti italiani rispetto ad essa con un'analisi qualitativa comparativa.

Dalla ricerca è emerso che la tecnologia blockchain è applicabile in numerose aree del settore finanziario, con i principali vantaggi di portare una semplificazione dei processi as-is, una riduzione dei costi e in alcuni casi di consentire l'introduzione di nuovi servizi, non possibili con le soluzioni attuali. Tuttavia, risulta che la tecnologia presenta anche due grandi limiti che rallentano una più vasta diffusione sul mercato: la necessità di essere adottata da una molteplicità di attori uniti in un consorzio per portare i benefici sopracitati (una blockchain non può essere sviluppata ed utilizzata da un singolo istituto); l'assenza di leggi specifiche e la presenza di ostacoli normativi che rendono impossibile l'adozione o quantomeno la ostacolano creando un rischio di compliance.

ABSTRACT (ENGLISH)

The present thesis work aims at defining possible applications for blockchain technology in financial services, mapping changes in existing process in case of adoption and highlighting its potential benefits. Such need arises from the increasing interest for the technology by financial institutions and fintech startups, against the scarce scientific literature which deals with the topic in an unstructured way.

For a better thoroughness in this study, data gathering was carried out following multiple methods:

1. a quantitative internet research gave place to two structured databases, clustering blockchain projects launched by startups and financial institutions worldwide;
2. for these initiatives, related grey literature was downloaded and analyzed, if available;
3. through interviews with industry experts, ten case studies concerning Italian institutions were generated.

The three methods were complimentary to answer the research question. The first allowed to determine all possible areas where blockchain technology can be adopted; the second allowed to map to-be processes; the third shed light on possible benefits and limits to implementation. Additionally, the latter enabled a comparison of Italian institutions' position toward blockchain with a qualitative comparative analysis.

From the research, blockchain turned out to be viable for numerous areas in financial services, with the main advantages being a simplification of current processes, a cost reduction and, in some cases, the possibility to launch new services which other technologies are unable to offer. Nevertheless, a wider diffusion of the technology across the market is highly hampered by two hurdles: the need for a joint development and usage in a consortium of institutions (a blockchain cannot be developed and used by a single entity) to rip off the aforementioned benefits; the gaps in regulatory policies and the presence of restrictive laws which either make its usage unfeasible or generate an off-putting compliance risk.

EXECUTIVE SUMMARY

In the last years, the word 'blockchain' has been ubiquitous in the news. Near the end of 2017, the interest in this technology was particularly high, when the hype on its potential led many to invest in cryptocurrencies. Speculation on cryptocurrencies and their skyrocketing prices echoed across media, making even more people aware of the technology, causing the bubble to grow further in a vicious circle. This phenomenon is particularly evident by looking at Google Trends' reports on blockchain-related searches: by the end of November 2017, the technology popularity began to surge, until reaching its peak around December of the same year[1]. In this context of inflated expectations, we thought that blockchains needed to be studied with a scientific approach.

Definition

The definition we reference to was given by the Digital Finance Observatory (2016) and by Hileman and Rauchs (2017): blockchain is an IT architecture that stores transactional data; it is distributed in a network, so it is composed of several servers (nodes) which store copies of the same data; new data can be added in batches (blocks) only if the majority of the nodes agrees; approved blocks are ordered and linked together to form a unique chain. According to Hileman and Rauchs (2017), blockchain is similar to a distributed ledger technology, the only difference being that validating nodes have to batch transactions in blocks before transmitting them to the rest of the network.

In Chapter 1, a list of the different typologies of blockchain is provided, as well as a description of the mechanism through which they work. Moreover, we will provide an explanation of smart contracts technology and functioning: a smart contract is a computerized transaction protocol that executes the terms of a contract (Szabo, 1994). They were conceived well before the existence of a blockchain but writing them on-chain gives the advantage of immutability and the possibility that they reliably self-execute without the need of control from third parties (Swan, 2015).

[1] https://trends.google.com/trends/explore?date=2017-08-01%202018-11-23&q=blockchain

Literature review

A systematic approach was selected as our method to carry out the literature review on the topic. Indeed, the purpose of the systematic study is to provide an overview of a research area, and to deliver a detailed summary of all the available information already proposed by the scientific researchers related to a topic (Kitchenham, et al., 2009). We chose to use this process as our initial goal was to explore the existing studies regarding the BCT in order to assess whether they neglected some research areas.

The process consists of five phases: the definition of research questions, which in our case was the acquisition of knowledge about the already existing studies with respect to the BCT, the research conducting, the screening of the relevant papers, the theme analysis and the mapping process (Hannay, Sjøberg, & Dybå, 2007).

By selecting papers using the keywords "blockchain", "BCT", "DLT" and "distributed ledger database", we obtained initially 807 results, which were subsequently screened based on their relevance, and sorted by topic, thus we eventually created a final database made of 142 scientific papers, as we can see in the following image.

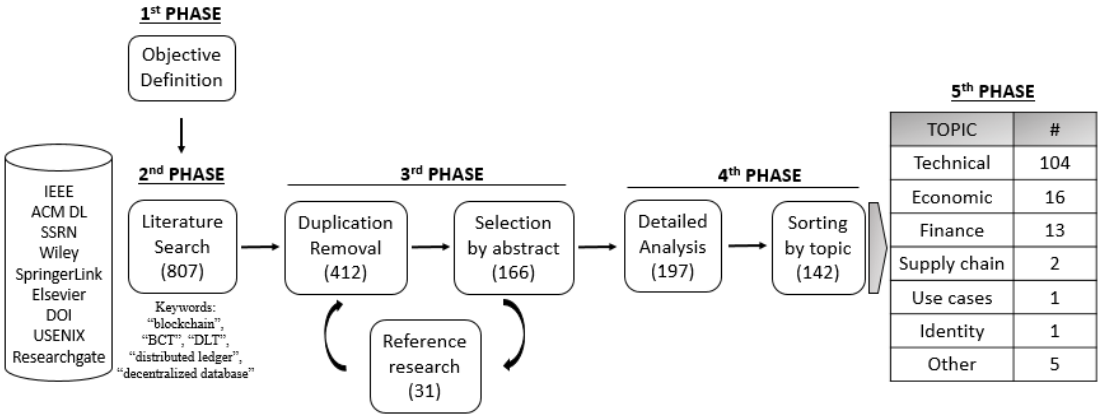


Figure 1, Systematic literature review process

From the literature analysis we could conclude that little attention has been paid to researches which go beyond the technical sphere (Beck & Muller-Bloch, 2017), indeed, the existing works are oriented to either a technical or an economical perspective of the blockchain (de Kruijff & Weigand, 2017; Risius & Spoher, 2017). The scientific literature lacks a comprehensive understanding of the possible various implementations of the technology in the real life. Indeed, the application-oriented studies are mainly traceable in the grey literature, in which different industry reports describe their internal researches on the implementation of blockchain-based solutions for their needs (Hofmann et al., 2018).

Moreover, these studies are usually oriented on a single process, missing a global vision of the worldwide experimentations. This results in disperse information which cannot provide a comprehensive understanding of where and how the blockchain technology might be suitable to be applied (Risius & Spohrer, 2017).

From a preliminary analysis of census literature (Hileman and Rauchs, 2017), we found finance to be the most active area in blockchain projects among companies and startups. Yet, scientific literature contributions in financial application turned out being scarce and disconnected (de Kruijff & Weigand, 2017). Indeed, the financial sector lacks a theoretical background as well as comprehensive observations in the context of blockchain applicability.

Thus, having as a purpose to fill the abovementioned literature gaps, we identified the following research question:

RQ: *In which application areas the BCT might be a beneficial instrument for the financial sector?*

Indeed, we considered that finding real financial applications of the blockchain would have been interesting for us and beneficial for scientific research, given the lack of papers on blockchain applications[5].

To answer the above research question, we structured our research in four different phases, which are presented in as many chapters, as showed by the following image.

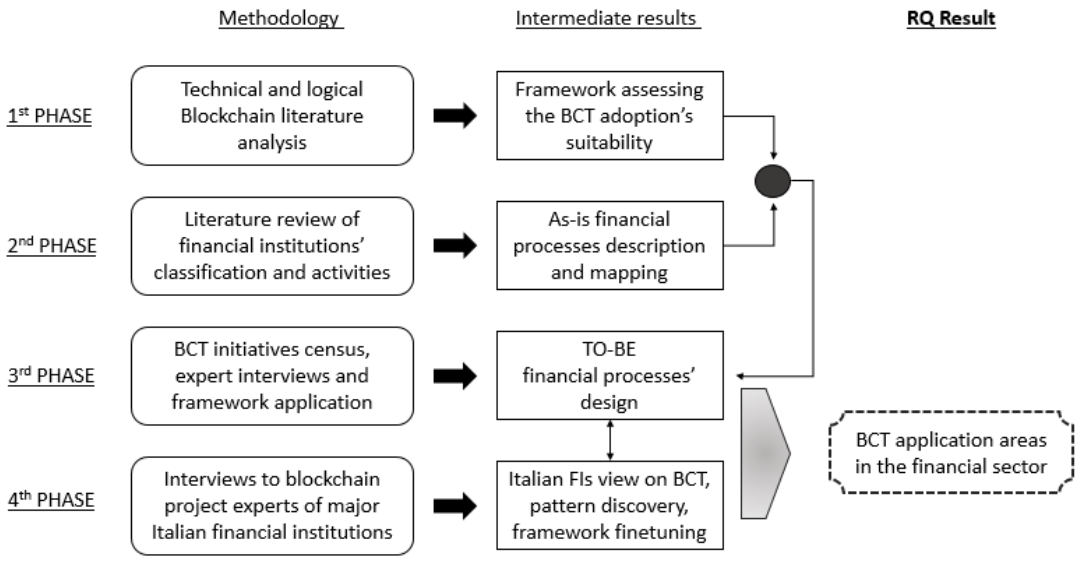


Figure 2, research methodology process

Technology analysis

To give a consistent framework for blockchain adoption in financial services, a thorough understanding of the technology in general was needed. The ability to differentiate various solutions (e.g. private or public blockchains?) as well as their performances was crucial to provide a sensible framework. So, we reviewed both technical literature and strategic literature, which guided the choice of blockchain adoption from a logical perspective (e.g. is it better a centralized database or a blockchain infrastructure?).

This analysis was carried out to define whether, independently from the sector of application, blockchain made sense to be used. It was fundamental to later review the sample database and discard solutions that did not provide a feasible process with respect to open technological issues.

In Chapter 3, a deeper description of blockchain technology with its main limits is proposed with a review of the main papers covering the issues hindering the adoption of the BCT. They were clustered according to the scheme proposed by Swan (2015), which consists of limited network capacity, security, usability, versioning, hard forks, and wasted resources. Besides, a further constrain has been added, the privacy, after the review of the other technical papers (Herrera-Joancomartì, 2015). Describing existing blockchain limits, we shall also present literature concerning proposed solutions. This way, the reader can distinguish between issues which are still hampering BCT usage and solved problems.

In the second part of the chapter, the focus shifts from the technical analysis to the strategical one. Even in this case, a review of the literature addressing strategical constraints is to consider, when evaluating the implementation of blockchain technology versus that of a traditional database. Such considerations allow to distinguish between legitimate and deceptive use cases for BCT, but also, among the legitimate ones, they provide a guideline to choose the most appropriate typology of blockchains. Then, we modelled a general framework putting together the contributions by the different authors and expanding them by introducing the technical constraints previously discussed. In this way, we provide a sensible instrument through which we can identify viable use cases in financial services.

Financial sector analysis

In the second part of our literature analysis, we decided to study more in depth the current financial sector with the purpose to understand which actors play a crucial role in it, and subsequently how each of them may use the BCT.

Among the three types of classification proposed by the scientific literature, which are based on the performed functions (De Hann, Oosterloo, & Schoenmaker, 2009; Bhattacharya & Thakor, 1993), on the faced risks (Hess & Laisathit, 1997) or on the governance (Zazzaro, 2001; Gillan & Starks, 2000), we selected the former. It indeed results being more in line with our goal, since the latter is country specific (Italy), thus not aligned with our global perspective, while the risk-based one entails the difficulty of computing the portfolio risk for each institution of interest, thus it is not consistent with the purpose of the thesis. Therefore, the identified players are described in detail in Chapter 4: depository institutions, insurance, investment banks, funds, finance companies and financial markets' intermediaries. In the same chapter we list their activities following the scheme on financial services reported by Saunders and Cornett (2008): payments, deposit and lending, risk management and insurance, supply chain finance and investment products. To these categories, KYC activities and fiduciary services are added, since they represent further sources of competition in the industry; moreover, KYC is required for regulatory compliance, thus in order to perform all the primary processes (Sathye, Nicoll, & Chadderton, 2017; Holsapple & Singh, 2001). Financial institutions are then combined with their performed tasks:

Function / Institution	Payment services	Investment products	Deposit & Lending	Supply chain finance	Insurance products	Fiduciary Services	KYC
Depository Institution	X	X	X	X	X	X	X
Insurance Companies	X	X	X	X	X	X	X
Securities Firm	X	X	X	X	X	X	X
Finance Companies	X	X	X	X	X	X	X
Fund Companies	X	X			X	X	X
Financial Intermediaries	x	X			X	X	X

Figure 3, functions performed by FIs (adapted from Saunders and Cornett, 2008)

We can easily conclude that nowadays financial institutions are no longer specialized in only one function. Indeed, today the universal bank is the most widespread model of banking institution, engaging in the provision of many different financial services and products, combining retail, wholesale and investment ones. Consequently, we will abandon the initial idea of reviewing blockchain application by the type of institution, instead, we shall focus on the *services offered* to propose a relevant classification for financial intermediaries.

Thus, we started reviewing the scientific literature dealing with the description of the aforementioned services. Through the literature surrounding these services, industry reports and interviews with experts of the sector, we drew the as-is processes for each of the classified categories. These descriptions are reported in Chapter 5.

Empirical analysis

The objective of the empirical analysis is to assess where the blockchain can be efficiently applied and how the current financial processes will change with it. To do this, different methods of analysis have been used: a quantitative census of blockchain-based initiatives of startups and existing firms, the reviewing of related grey literature and interviews to sector experts.

The research is carried out analyzing the state of the art of the use cases from a global point of view, by mapping the already existing initiatives of international startups or established firms. Then, using an inductive approach, we define where the BCT might improve existing financial services, and how.

All international blockchain-based startups on CrunchBase and international initiatives on BCT published on specialized websites since 2016 have been listed in two separate databases, with information regarding their sector of application and other relevant data. Among them, we selected the ones related to the functions listed above and fitting the framework developed in Chapter 3. In this way, the area in which the blockchain could be efficiently applied have been highlighted. Then, the correspondent grey literature has been studied with the purpose to design the to-be processes, and to describe in detail the advantages the application of the BCT may bring. All these pieces of information can be found in Chapter 5.

Once we defined a detailed description of the possible and appropriate applicability of the BCT in financial services from a global point of view, our focus narrowed to the Italian market. This step is useful to finetune our framework, checking if it can be considered a reliable instrument of analysis for BCT in a business context and to enrich it with advantages and limits of the scouted projects. We aim to understand whether Italian institutions selected already-known use cases, or if they found new areas still unexplored. Moreover, we would like to determine the Italian financial market position with respect to this technology. Twelve interviews to Italian banks and insurance company have been conducted to gain these data, two of which reported they were not performing any studies about the blockchain. The information is leveraged to highlight the main area in which the blockchain is employed by

Italian financial institutions and to draw their position concerning their level of awareness and of commitment regarding the technology.

From these analyses we can conclude that the blockchain technology can be efficiently applied in different areas of financial sector, and multiple use cases exist that can bring new value to incumbents' business models.

Even if generating economic benefits such as the reduction of the time and costs needed to perform activities, some problems still limits blockchain full exploitation. Mainly, it was reported by the respondents to the interviews that blockchain technology requires a collaborative approach among the parties to gain the maximum benefits from its use, thus financial institutions should start to work together in a cooperative logic on the same platform, which currently is hardly happening. Another issue which has been highlighted several times, and which has been reported by the grey literature too, is the lack of regulations concerning the blockchain. Some financial activities need legal validation, for example securities should be established by a CSD or KYC activities should be aligned with the GDPR. These norms hinder a full implementation in certain use cases or raise serious concerns for compliance risk in others, making them off-putting for incumbents.

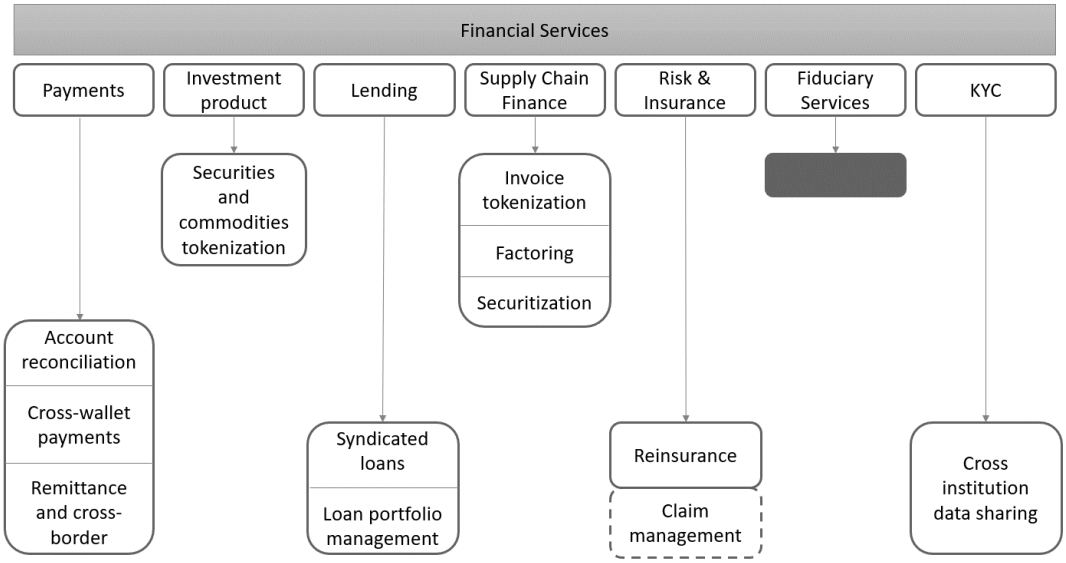


Figure 4, BCT adoption framework in financial services

Thesis structure

The dissertation follows the steps described above.

Chapter 1 aims at aligning the reader with the definitions used throughout the work. So, it will present what blockchain is, its main characteristics and how it works, as well as a separate section dedicated to smart contracts.

Chapter 2 will describe more in detail the methodology used to develop the analysis and the researches used to answer the dissertation's research question.

Chapter 3 deals with the technical and strategic analysis of the blockchain, reviewing the scientific literature which addresses the main technological and architectural constraints to consider when evaluating the use of BCT. It concludes proposing a general adoption framework for blockchain technology which we used to filter startups and companies' projects in the empirical data.

Chapter 4 shifts to financial services, listing the possible classification for financial institutions, describing them in detail, and eventually comparing them against the performed functions.

Chapter 5 combines literature review and part of the empirical research. Indeed, the different activities carried out by the financial institutions are described as they are now, then, leveraging empirical data, how they can be transformed with the adoption of BCT.

Chapter 6 presents the second part of the empirical analysis. First, the way in which the interviews to the Italian financial institutions are conducted is described, then a within-case analysis is performed, followed by a cross-case one. The former has the purpose of extracting precise information from each respondent individually, while the latter compares data among all the participants to find similarities and possible patterns.

Chapter 7 eventually concludes the dissertation, summarizing the main results, highlighting some limitations and criticalities of the findings, and indicating directions for future research on questions that are still open.

CHAPTER 1
INTRODUCTION

In this chapter, we give a brief overview on the reasons that brought us to develop our thesis around blockchain technology, along with some preliminary definitions. In particular, we will present differences and similarities between blockchains and other data storage architectures, briefly describe what blockchain is and how it works, define smart contracts as they are a relevant instrument to drive value in blockchain solutions. A structured introduction to the literature review methodology, literature gaps and research methodology can be found in Chapter 2.

1.1 Why blockchain

We came across the world blockchain while reading some article[2] on *Milano Finanza*, an Italian newspaper reporting financial news. The technology was indicated to be potentially disruptive for the financial sector, yet, contrarily to other technological trends such as machine learning, IoT etc., we never heard of it. Driven by curiosity, we decided to approach the topic, and, from initial researches, we found it to be intriguing. Besides, as we will explain in detail in the methodology section, we found no literature reviewing financial application for blockchain, and very few papers on the usage of blockchain in finance in general.

When we approached the technology, near the end of 2017, it was a particular moment for blockchain: mainstream media were talking more and more about it, while the hype on its potential lead many to invest in cryptocurrencies such as Bitcoin, Ethereum or Litecoin. Besides, many companies were leveraging ICOs as a very successful means of financing, since it provided large capitals at a relatively small cost, thanks to the market enthusiasm.

[2] https://www.milanofinanza.it/news/bitcoin-dalla-bce-solo-questione-di-tempo-201709252019502932

Speculation on cryptocurrencies and their skyrocketing prices infested newspapers articles, making even more people aware of the phenomenon and of the technology, causing the bubble to grow further in a vicious circle. This phenomenon is particularly evident also by looking at Google Trends' reports on blockchain-related searches: by the end of November 2017, the technology popularity began to surge, until reaching its peak around December of the same year[3].

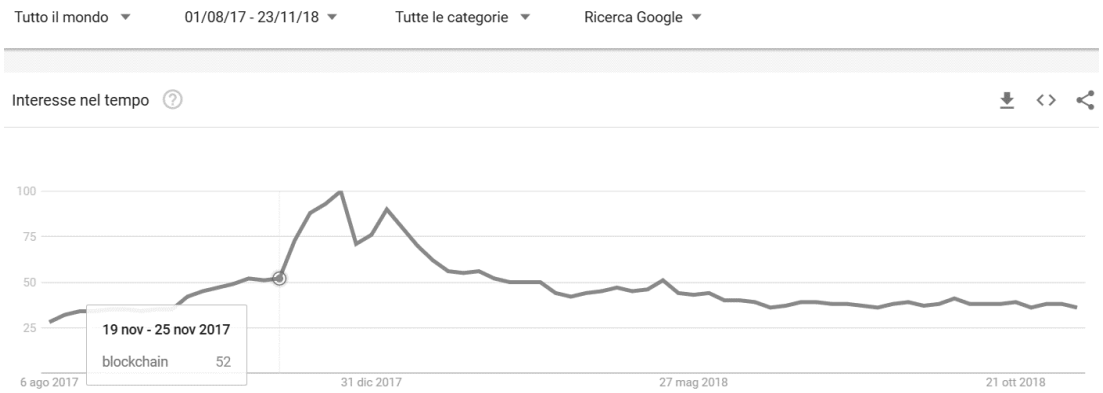


Figure 5, Google Trends report on blockchain-related searches from August 2017 to November 2018.

Anyway, the phenomenon came to a halt on Sunday, December 17th, when Bitcoin reached its peak price of $20.078, and when CME group launched Bitcoin futures[4]. Just a few days later, the price had already plunged to $12.350[5]. The drop of prices was followed by that of search popularity: the speculative bubble had burst. In this context of inflated expectations, we thought that the technology needed to be studied with a scientific approach. Also, finding its real financial applications would have been interesting for us and, hopefully, beneficial for scientific research, given the lack of papers on blockchain applications[6]. Besides, from initial readings we found the technology to be very complex or at least, very hard to explain in simple terms, and we decided that a deepened study was needed.

[3] https://trends.google.com/trends/explore?date=2017-08-01%202018-11-23&q=blockchain

[4] https://www.cnbc.com/2017/12/17/worlds-largest-futures-exchange-set-to-launch-bitcoin-futures-sunday-night.html

[5] https://www.forbes.com/sites/stephenpope/2017/12/22/badly-burnt-by-bitcoins-bursting-bubble/#7d7f9c25207f

[6] A detailed explanation on the way the literature review took place is carried out in Chapter 2.

1.2 What blockchain is

In this section, we give a brief definition of the technology to align the reader with the terminology employed in the rest of the work. The definition we reference to was given by the Digital Finance Observatory (2016) and by Hileman and Rauchs (2017): blockchain is an IT architecture that stores transactional data; it is distributed in a network, so it is composed of several servers (nodes) which store copies of the same data; new data can be added in batches (blocks) only if the majority of the nodes agrees; blocks are ordered and linked together to form a unique chain.

To further understand blockchain, Hileman and Rauchs (2017) show its differences with other technologies that serves to store data. Typically, information is stored in a centralized database, where a master node controls all information present in other units. Databases could then be distributed if no central node manages operations, but data is replicated across servers, so that a consistent view of the database is kept. Yet, the latter solution does not consider the possibility of a malicious node wiling to overtake the system, in fact, it is implemented in highly trusted environments (e.g. within the same company). If trust is no longer an assumption, a DLT is needed. With this solution, a validating node examines new data to check that it is consistent with previously recorded data. Only then, it transmits this data to other nodes to be recorded. A blockchain is very similar to a DLT, the only difference being that validating nodes have to batch transactions in blocks before transmitting them to the rest of the network.

Blockchain can be public, if anyone can read data, or private, if data is restricted to only certain users. Another distinction is between permissionless blockchain that allow any user to post transactions that are written in network's database, or permissioned if only certain users are allowed to post such transactions. Typically, permissioned private blockchains are referred to as consortium blockchains, due to their use by consortia of companies. Instead, public permissionless blockchains are the one used by most cryptocurrencies.

1.3 How blockchain works

The functioning of a blockchain depends on the underlying protocol that is implemented in the system, we shall describe the first one, that is, the one by Nakamoto (2008). As we mentioned, blockchain take its name from the fact that transactional data, that it stores, is batched into blocks. The protocol gives specific indication on the format of such data, for instance a transaction is composed by certain elements (such as version, inputs, outputs, lock

time), as well as blocks (such as block header, set of transactions, nonce) that also have a maximum size (in Bitcoin it is 4MB[7]).

Blockchain data is secured by public-key cryptography: a user can ask the blockchain to generate a set of keys at no cost, a public key that corresponds to his address, and a private key that he can use to sign transactions from that address. These keys need to be stored on a device that can either be the user's computer or a centralized service storing keys such as an online wallet. To enter a valid transaction, a user signs it with his private key and broadcasts it to the closest node available. The node propagates the transaction to other nodes, following protocol rules. Some of these nodes are called miner nodes, as they are in charge of validating transactions, i.e. checking that the amount sent is lower than the account's balance. Anyone can become a node by downloading the blockchain on his computer, and a miner node if he wishes to validate transactions. Valid transactions are batched into blocks, that, in case of Bitcoin, are added to the blockchain every 10 minutes. Because the block size is limited, a fee needs to be attached to the transaction to have miners validate it: the more is the fee offered, the more likely it is that the transaction will enter the next block (Antonopoulos, 2014).

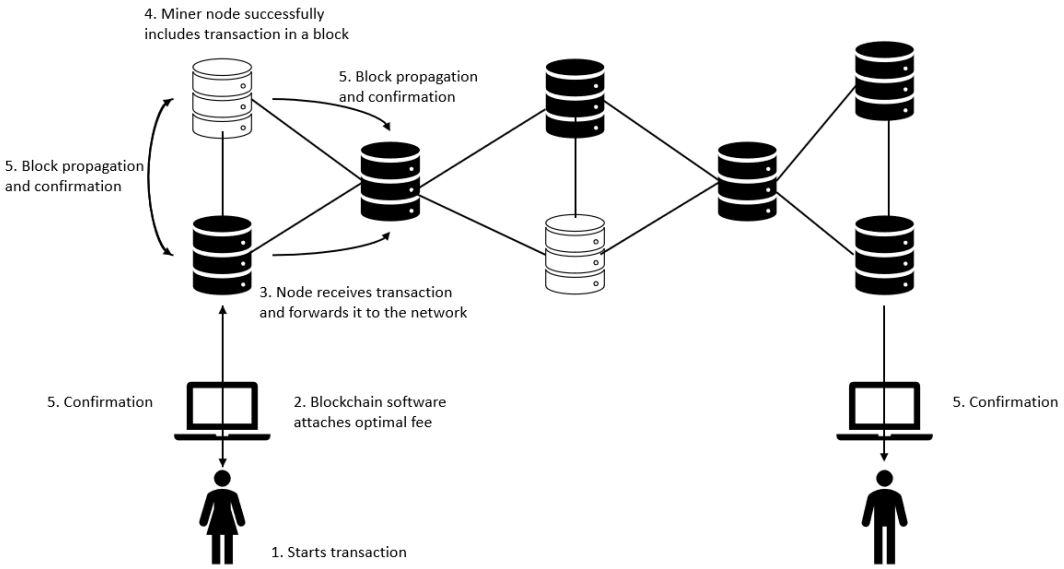


Figure 6, a simplified vision of blockchain transactions between two users. Black database are nodes, white are miner nodes. Any user can choose to become a node or a miner node.

Still, the incentive system is not complete: if anyone can be a miner, and miners get paid to include transactions in new blocks, what stops anyone from becoming a miner? What

[7] Considering the Segwit soft-fork, more on that in Chapter 3.

prevents miners from including invalid transactions into blocks? The solution proposed by Nakamoto (2008) is proof-of-work (PoW). Once a new block is created, all of its content is hashed[8], and the output string is called header. Not any block is good to be attached to the chain: the protocol imposes that headers start with a minimum number of zeros, otherwise they are considered invalid.

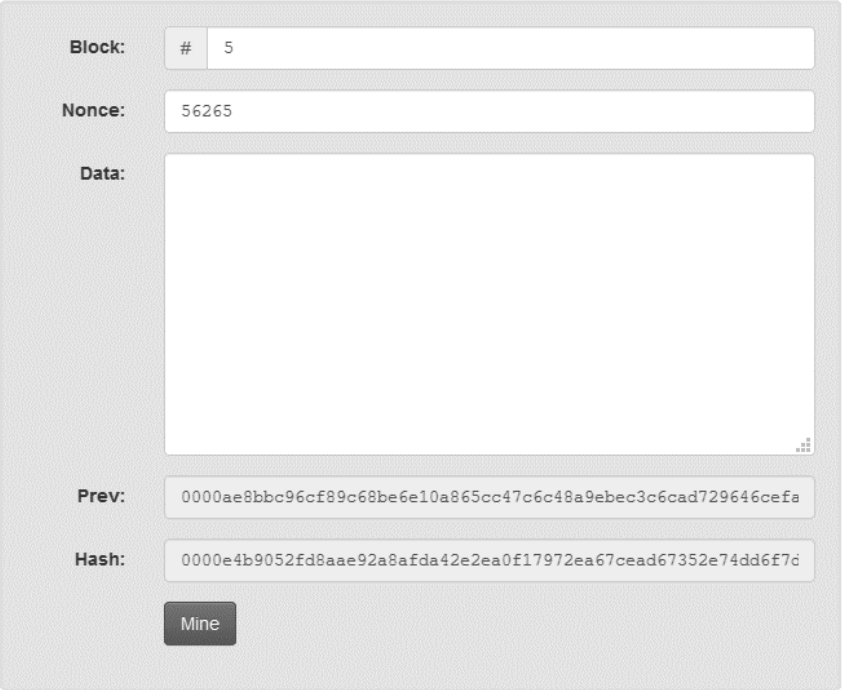


Figure 7, a simplified representation of a block content. The data section is usually filled with transactions (from https://anders.com/blockchain/distributed.html).

Looking at Figure 7, miners have to include in a block: its number, transactions (in the data section), and the header of the previous block. Then, they can compute the current block hash (its header). It is unlikely that the hash computed this way has the minimum number of zeros required by the protocol (4 in the example). To adjust the hash so that it is compliant with protocol requirements, miners also add a nonce, a random number, to the block data. Proof-of-work consists of a CPU randomizing the nonce until the hash of the block has the required number of zeros which is called difficulty. The more zeros, the harder it is to find the right nonce giving the requested hash. So, mining is not free: a CPU needs to be bought and

[8] A hash functions takes as input any arbitrary large amount of data and returns a fixed size alphanumeric string. Changing the original data returns a totally different hash. The hash function has the property of being easy to compute, but very hard to revert: i.e. from the alphanumeric string it is unfeasible to go back to the original data by brute force, that is, by repeated tests.

employed, using electrical energy, to find a solution to the hash problem. The first miner to find a correct hash gets all of the reward (i.e. all of the fees attached to transactions, plus newly minted coins if contemplated by the protocol).

In this sense, blocks are chained together: if someone tries to alter the content in a previous block, its hash will change, so, its nonce has to be computed again[9]. Moreover, all the subsequent blocks' hashes will change, because the previous block hash they reference to is changed, creating a domino effect. An attacker willing to modify the chain has to re-compute all hashes of the blocks following the one he tampers and do it faster than the rest of the network, because the protocol considers the longest chain to be the valid one. To be faster, the attacker would need at least 51% of the computing power of the network. So, a malicious user would have to spend a relevant amount of money on CPUs to mine blocks with invalid transactions faster than the rest of the network, and he is not incentivized to do so. Also, not everyone becomes a miner because an investment is needed (buying a machine with a CPU; Nakamoto, 2008).

Another feature of blockchain is that of programmability. Almost all blockchains are programmable, either with Turing complete or not[10] languages. Bitcoin is non-Turing complete, so new cryptocurrencies were proposed that allow for more computations to happen on the blockchain. The first was Ethereum in 2014 (Wood, 2014). Turing completeness allows the implementation of smart contracts on the blockchain, which we shall discuss in the next section.

1.4 Smart contracts

A smart contract is a computerized transaction protocol that executes the terms of a contract (Szabo, 1994). They were conceived well before the existence of a blockchain but writing them on-chain gives the advantage of immutability and the possibility that they reliably self-execute without the need of control from third party (Swan, 2015).

In Figure 8, we report a simple example of a smart contract that was programmed using solidity, the Ethereum programming language. Contracts can be created by any user, and they receive a public address from the blockchain protocol.

[9] A simple test to see in practice what we explained can be found at: https://anders.com/blockchain/distributed.html. Values can be modified freely, then, by clicking "Mine", the website will seek a new nonce that makes the block valid.

[10] Turing completeness, among other things, allows to run loops in the code, store a state and execute programs in more phases (http://wiki.c2.com/?TuringComplete).

```
pragma solidity ^0.4.23;

contract Split {
    address owner;
    address beneficiario1;
    address beneficiario2;

    function Split(address _beneficiario1, address _beneficiario2) public {
        owner=msg.sender;
        beneficiario1 = _beneficiario1;
        beneficiario2 = _beneficiario2;
    }

    function Paga() public payable {
        uint amount;
        amount = msg.value;
        beneficiario1.send(amount/2);
        beneficiario2.send(amount/3);
    }
}
```

Figure 8, an example of smart contract that splits a payment received among two beneficiaries.

In the example, sending a payment to the contract address, practically splits it in two among the beneficiaries. Smart contracts are a powerful tool that can be employed in many domains and automate current procedures, yet, they need to be carefully implemented as a logical mistake in the code cannot be corrected, once uploaded, due to blockchain immutability (Atzei et al., 2016). For instance, in the proposed example there is a mistake: beneficiary 1 receives half of the sum, beneficiary 2, due to a typo, receives only a third of it. The remaining amount that is not sent to the beneficiaries is lost forever: it stays in the contract address and cannot be redeemed in any way. We shall discuss more on smart contracts issues in Chapter 3.

CHAPTER 2
METHODOLOGY

In this chapter we are going to present the process through which we have developed our dissertation. Firstly, a literature review led us to highlight limitations and gaps regarding the topic of the BCT. The identified lack in the literature was the starting point of our research, as we aimed to fill it and contribute to the theoretical studies with our work. Therefore, based on these initial findings, the research questions we want to address in our thesis have been generated. Subsequently, we will describe the approach chosen to conduct our research, which combines different methodology in order to obtain comprehensive and detailed results.

2.1 Literature review

A systematic approach was selected as our method to carry out the literature review on the topic. Indeed, the purpose of the systematic study is to provide an overview of a research area, and to deliver a detailed summary of all the available information already proposed by the scientific researchers related to a topic (Kitchenham, et al., 2009). We chose to use this process as our initial goal was to explore the existing studies regarding the BCT in order to assess whether they neglected some research areas.

The process consists of five phases: the definition of research questions, the research conducting, the screening of the relevant papers, the theme analysis and the mapping process (Hannay, Sjøberg, & Dybå, 2007).

In this initial phase, our research objective was the acquisition of knowledge about the already existing studies with respect to the BCT, and to highlight possible still unexplored areas, where we could contribute.

The second step of the systematic approach is the search for all relevant papers. We used various databases in order to retrieve a wide range of information. We decided to include both peer-reviewed papers, as well as the grey literature, in order to have a broader view of the topic. Indeed, scientific databases often do not include white papers published by specific firm about their personal researches, thus missing important sources of industry-related information (li-Huumo & Smolander, 2016). In these databases we inserted some keywords, previously and jointly selected by this dissertation's authors: blockchain, BCT, DLT, distributed ledger, decentralized database. In this phase, a multitude of articles and books have been selected, thus we focused mainly on the mostly cited ones.

The third phase of the analysis was the screening of the collected papers. First of all, we excluded all the works dated before 2008, the year in which the Nakamoto's white paper was published. Then, we eliminated the duplicates gathered because of the use of diverse databases. The remaining ones were examined based on their abstracts (Vom Brocke, Simons, Niehaves, Niehaves, & Reimer, 2009). All the studies which did not actually present the above listed keywords, or which were not centered on the BCT were excluded. After selecting the valid papers, we conducted a reference research, also known as backward-forward research, which allows to enlarge the knowledge on the relevant pieces of information (Okoli, 2015). Therefore, we examined the references cited in already gathered papers, or we deepened our understanding of a topic by looking for its subsequent evolution in papers citing the already evaluated one. At this point, we replicated the screening of the papers with the newly collected ones. In this way, we gathered other 31 papers.

Eventually we obtained a list of 142 papers. Each of them was classified based on its main focus in the context of BCT, subdividing them into 7 main topics: technical, economic, finance, identity, supply chain, use case census and other. Technical one groups all the works which give a detailed explanation of what a blockchain is, how it works, its main issues, and possible improvements to solve them. Economic literature studies the impact the blockchain technology may have in the economy or conducts an economic evaluation of cryptocurrencies. Finance and supply chain are two set of papers which focus on the blockchain in these specific processes. On the contrary, the use case census lists all possible application of blockchain technology. The 'other' group instead refers to the social, legal or political impact of this new technology.

Figure 9 shows our literature review process. The numbers in brackets represents the papers collected for each phase.

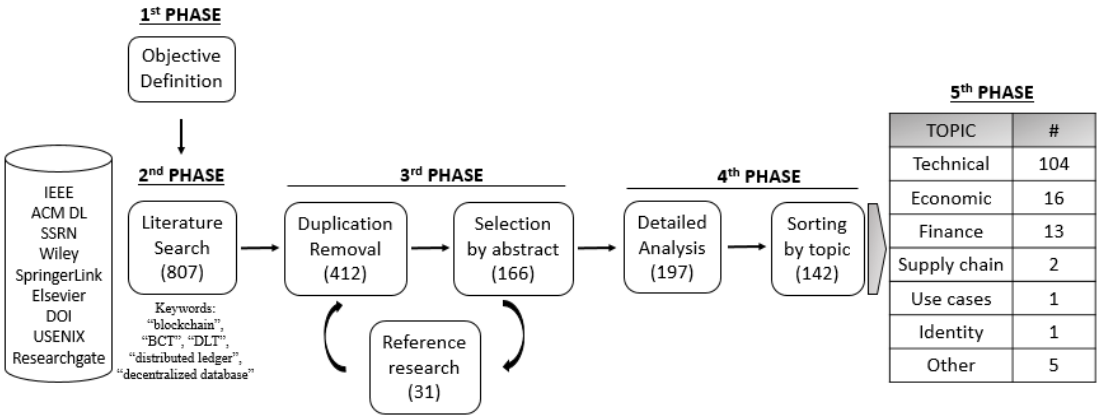


Figure 9, Systematic literature review process

In the end, a database was built, where we reported the author's name, the title, the publication year, the topic we assigned in the previous phase, a subtopic in order to better define the main focus of the paper, the source, the type of publication, distinguished between white paper, report, article, book, and a brief description of the content. This mapping of the data was extremely useful for our purpose of understanding where the literature mainly focused so far and whether any research gaps were present.

As we can see from the results of the literature classification, technical studies have been the one performed the most. Indeed, for many years the blockchain has been considered as strictly related to Bitcoin, thus the interest was mainly focused on these topics. Only in the last five years, the studies turned to the technology behind bitcoin and its possible applicability in other sectors (Crosby, Pattanayak, Varna, & Kalyanaraman, 2016). Yet, little attention has been paid to researches which go beyond the technical sphere (Beck & Muller-Bloch, 2017); indeed, the existing works are oriented to either a technical or a theoretical-economics perspective of blockchain (de Kruijff & Weigand, 2017; Risius & Spoher, 2017). The scientific literature lacks a comprehensive understanding of the possible various implementations of the technology in the real life. In fact, the application-oriented studies are mainly traceable in the grey literature, in which different industry reports describe their personal researches on the implementation of blockchain-based solutions for their needs (Hofmann et al., 2018). Moreover, these studies are usually oriented on a single process, meaning that they try to understand the possible functions of the technology in a specific activity, such as, for example, interbank payments. Glaser (2017) defines the blockchain as an "*innovative technology in search for use cases*", and that is exactly what is happing now. Many different actors, from

startups to already established firms, are putting a great amount of efforts in the discovery of suitable applications for this *innovative technology,* though, usually without a global vision of worldwide experimentations. This results in disperse information which cannot provide a comprehensive understanding of where and how blockchain technology might be suitable to be applied (Risius & Spohrer, 2017). Thus, we can conclude that currently there is a deep understanding of the technological aspects of the blockchain, being the most heavily investigated topic so far, but this knowledge has been little combined in the scientific literature with possible business applications. Further researches are therefore needed to contribute to fill this gap in a structured and impactful way. In this regard, we developed a framework for blockchain applicability, trying to assess under which conditions it is preferable using this new technology instead of traditional ones.

It is a widely shared opinion that blockchain might be particularly suitable for financial purposes, as it also emerged by our review and previous works in similar direction (Deloitte Development LLC, 2018; Hileman & Rauchs, 2017; Ammous, 2016), this sector is the mostly investigated one among the use cases, with many proofs-of-concept (PoC) launched by financial institutions. Because of its primary characteristic of being a decentralized database which does not require any trusted intermediary, blockchain seems to be particularly well-fitting in all that context where a third party is required to perform and verify an activity. Nowadays, this function is carried out by middleman, but besides being time consuming and costly, the financial crisis has also revealed that it bears risks in case of an intermediary's failure (Nofer, Gomber, Hinz, & Schiereck, 2017). Blockchain would be therefore a solution to these inefficiencies, that is the reason why many financial institutions are currently studying it (Glaser, 2017). At this point we carried out a further literature analysis combining the keywork "blockchain" with "financial sector", "finance", "financial intermediaries". Despite the increasing interest in the new technology by the financial sector, we can encounter the same problems assessed above: first, there is a lack of a general and standard overview of the current state of the research, proprietary implementations written on reports or white papers are mainly the only detailed references to BCT applicability in finance, while application-oriented scientific literature contributions come out being scarce and disconnected (de Kruijff & Weigand, 2017); moreover, they are usually mono-disciplinary, limiting the perspective to a single use case (Glaser, 2017). But, a proper diffusion of an innovative technology on a large scale is possible only when the benefits it can bear are widely known and assessed (Everett, 1995). Thus, having a comprehensive understanding of the state of the maturity of current researches' results and, consequently, figuring out when and how the technology should be used are essential elements to drive its adoption and value generation.

After identifying the main limits of the scientific literature, we defined our research objectives. Our aim is the definition of a general and formal framework for the blockchain

adoption. For feasibility reasons, we decided to apply these considerations only on the financial sector, which appears to be the most promising one but still lacks a theoretical background as well as comprehensive observations in the context of applicability. We will evaluate in depth when BCT usage makes sense in the activities performed by financial institutions.

Thus, having as a purpose the filling of the abovementioned literature gaps, we identified the following research question:

RQ: *In which application areas the BCT might be a beneficial instrument for the financial sector?*

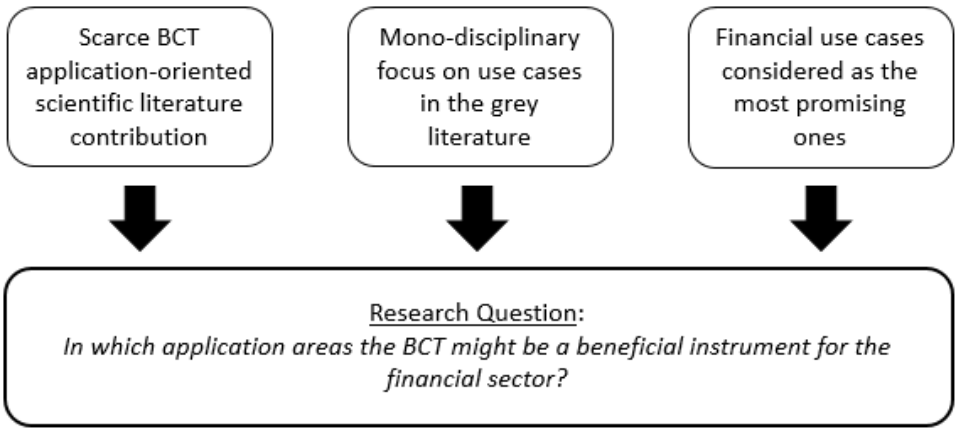


Figure 10, research question generation from scientific literature

To answer the above research question, we structured our research in four different phases:

Firstly, we studied the blockchain from a more technological point of view. We deepened our pre-existing knowledge on the topic through the already gathered scientific papers, to understand the blockchain main characteristics, its benefits, its limits and how it generally works. Moreover, independently from the sector of reference, we developed a framework which could drive in the choice of selecting the blockchain or of another traditional instrument as the technology for a certain process.

During the second step we turned to the financial sector, with the purpose of acquiring a deeper understanding of this field. Through a further scientific literature review, we aimed to identify the main financial institution, and to select an adequate classification of them. Subsequently, we listed the activities they are performing and through reports and expert interviews, we drew the as-is processes of those activities. Moreover, we highlighted current

limits and criticalities that affect these operations, to understand if they might be overcome by the BCT.

These separate studies have been then combined to extract the suitable application of the blockchain in finance. To do this, we relied on empirical researches, by doing a census of the current international startups and existing firms which deal with the blockchain. We selected only the adequate ones according to our adoption framework, we studied them, and we defined how the processes selected in the previous phase could be performed and transformed through the BCT.

The last phase was used to finetune our research and our framework. We narrowed our attention to the Italian financial sector and we conducted interviews to representants of nine Italians banks and one insurance company. The goal of this procedure is to doublecheck blockchain projects with experts' opinions, shedding light on benefits and constraints, but also to understand the Italian financial institutions' position with respect to the BCT.

The following image represents the process we followed to answer our research question:

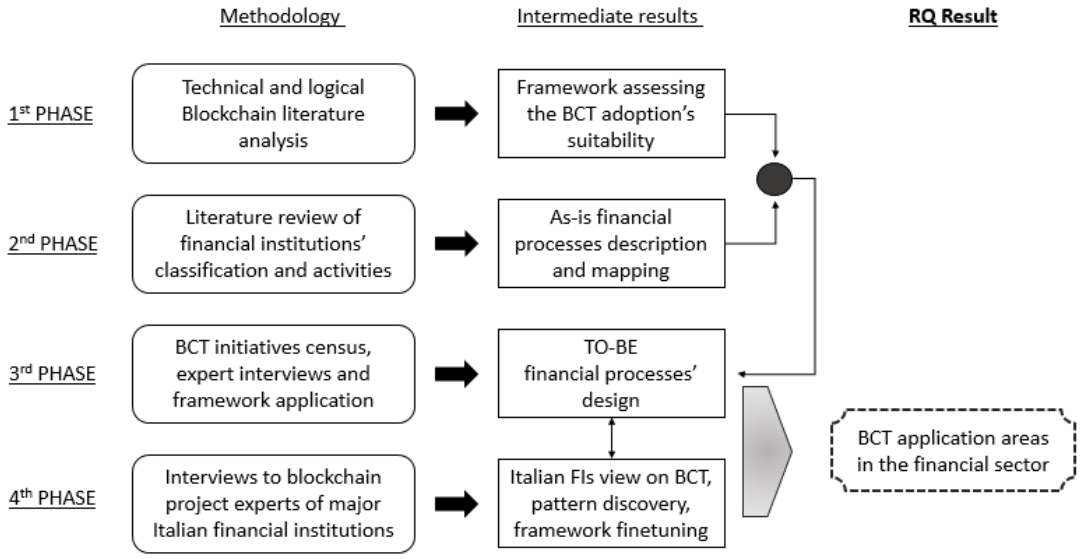


Figure 11, research methodology process

2.2 First phase

Which logical and technical constraints should be considered when evaluating the implementation of a blockchain technology in general?

As we have already mentioned, many studies have been conducted about the technology beyond the blockchain, nevertheless little is known regarding how to assess whether the choice of a blockchain solution might be useful for a certain application or not. The characteristics of

the BCT are indeed not suitable for any purpose, therefore it would be convenient identifying guidelines which can assist us in the decision between the use of a traditional database or any of the different typologies of blockchains (Beck & Muller-Bloch, 2017). In order to derive this framework, we combined both a technical analysis and a strategic one.

In the first case, we studied the issues hindering the adoption of the BCT by reviewing the papers collected in the initial phase of our research. While identifying them, we gathered information in order to understand whether or not these limits have been solved and how. The starting point of this analysis was the classification of the blockchain limitations proposed by Swan (2015), to which we added a further constraint, the privacy, after the review of the other technical papers. In this way, the hurdles which might negatively affect the performance of the technology have been listed, as we can see from the following image.

Publications/constraints	Privacy	Network capacity	Security	Usability	Wasted resources
Androulaki et al. (2013)	X			X	
Andrychowicz et al. (2015)			X		X
Antonopoulos (2014)	X	X		X	
Beikverdi and Song (2015)			X		
Bos et al. (2014)	X		X		
Chuat et al., (2015)		X			X
Cong et al. (2018)			X		X
Croman et al. (2016)	X	X		X	
Decker and Wattenhofer (2013)				X	
Decker and Wattenhofer (2014)			X		
Dimakis et al., (2006)	X	X		X	
Eskandari et al. (2015)			X	X	
Eyal et al. (2015)		X			X
Eyal and Sirer (2014)		X	X		
Garavaglia (2018)	X		X		X
Garay et al. (2015)			X		
Herrera-Joancomartì, (2015)	X			X	
Johansen et al. (2015)		X		X	
King (2013)			X		X
Lin and Marzullo, (1999)		X			
Meiklejohn et al. (2013)	X				X
Moser et al. (2013)	X			X	
Paul et al. (2014)		X			X
Sompolisky and Zohar (2015)		X		X	
Spagnuolo et al. (2014)	X		X		
Swan (2015)		X	X	X	X
Tschorsch and Scheuermann (2016)	X			X	
Vasek et al. (2014)			X		X
Wang and Liu (2015)		X			X
Yli-Huumo et al. (2016)		X	X	X	

Figure 12, theoretical review of BCT issues

The above listed papers are the ones which mainly describe the criticalities of the BCT. Beside these, we reviewed other works proposing solutions to the mentioned problems. In this

way, we assessed whether these limits are still hindering the adoption of the technology or, instead, new findings have been introduced to soften them.

As for any other technology, it is evident that simply checking the performance capabilities of BCT to elect it as the solution for a given use case is not enough: an assessment of the use case is needed to verify that traditional technologies such as centralized database are unfit. Therefore, we reviewed the literature proposing logical constraints to consider when evaluating the implementation of blockchain technology versus that of a traditional database. Moreover, not only do these considerations allow to distinguish between legitimate and deceptive use cases for BCT, but also, among the legitimate ones, they provide a guideline to choose the most appropriate typology of blockchains, between the permissionless versions or the permissioned ones. Then, we modelled a general framework putting together the contributions by the different authors and expanding them by introducing the technical constraints previously discussed. In this way, we provide a sensible instrument through which we can identify viable use cases in the financial industry.

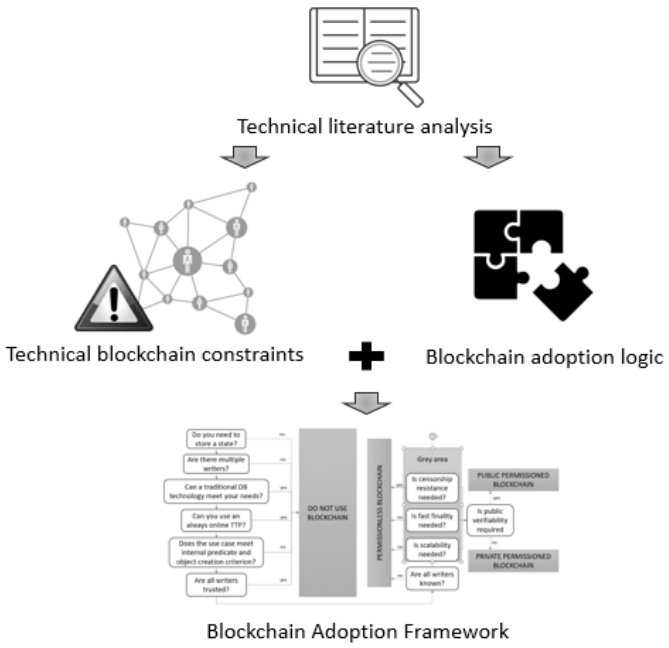


Figure 13, first phase methodological process

2.3 Second phase

Which are the main institutions operating in the financial sector and which functions do they perform? How are these functions processed? Are there inefficiencies?

As we decided to focus our analysis on the financial sector, it is crucial to have a clear image of it. To fulfil this purpose, the starting point of the study was the depiction of the actors operating in the sector, and therefore the players who might be hypothetically interested in turning to the blockchain technology. First of all, we performed a new literature research through the keyworks "financial institutions", "financial institutions classification", "financial actors", "financial intermediaries". Even in this case we followed the same systematic process described at the beginning of this chapter. The collected papers were selected on the bases of their abstract and subsequently on their contents, and eventually we obtained 15 results. The scientific literature focuses on three different types of classification of the financial intermediaries: based on the performed functions (De Hann, Oosterloo, & Schoenmaker, 2009; Bhattacharya & Thakor, 1993), on the faced risks (Hess & Laisathit, 1997) or on the governance (Zazzaro, 2001; Gillan & Starks, 2000). Considering that the goal of our research is the evaluation of the BCT applicability in the financial sectors, we arrived at the conclusion that the classification by functions was the most appropriate for our aim. The differentiation based on the governance indeed is country specific (Italy), thus not aligned with our global perspective, while the risk-based one entails the difficulty of computing the portfolio risk for each institution of interest, thus it is not relevant for us.

Once we have determined the sector's players, we narrowed our analysis to the activities they carry out. It is indeed required to know in detail the characteristics of the functions they perform in order to be able to apply our framework. We found that the most thorough scheme on financial institutions and their functions was reported in Saunders and Cornett (2008). After identifying the main players of the sector, they reported their performed functions subdivided into five main categories: payments, deposit and lending, risk management and insurance, supply chain finance and investment products. To these categories, we added other two, which comprises KYC activity and fiduciary services, since they represent further sources of competitiveness for financial performances; moreover, KYC is required for regulatory compliance, thus in order to perform all the primary processes (Sathye, Nicoll, & Chadderton, 2017; Holsapple & Singh, 2001). Through the literature surrounding these services, industry reports and interviews with experts of the sector, we drew the as-is processes for each of the classified categories. We had face-to-face conversations with employees of Banco BPM and EFG, who solved some of our doubts related to specific procedures in the banking industry, such as the lending process and the many activities surrounding payments. Thanks to their support, we could deepen our understanding of the services, and how they are offered. Moreover, we highlighted the inefficiencies and criticalities affecting these processes, so that we could discuss whether the BCT can eliminate/softened them or not.

The following image sums up the steps of the process we followed to detail the financial sector.

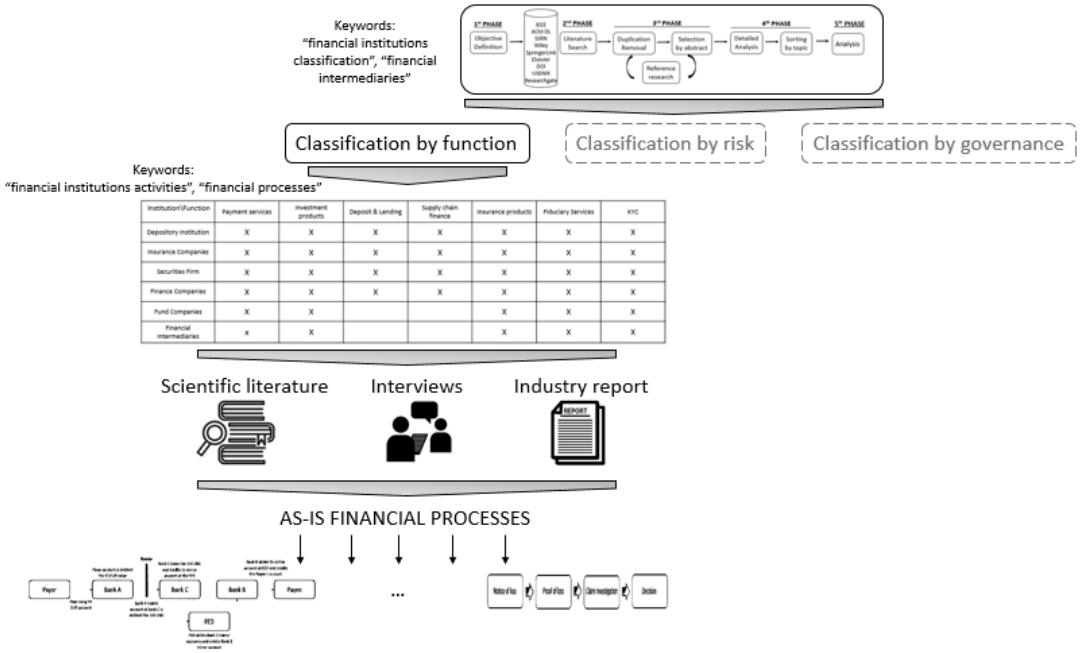


Figure 14, second phase methodological process

2.4 Third phase

Which of the financial processes are suitable for BCT adoption and how would they change?

The goal of our research is to provide a general overview of the appropriate blockchain applications in the financial sector. After defining the criteria of choice about BCT from a general point of view and depicting the financial actors and how their processes are currently carried out, we should combine this knowledge to assess which of the described activities can be efficiently performed by BCT.

The research is carried out analyzing the state of the art of the use cases from a global point of view, by mapping the already existing initiatives of international startups or established firms. Then, using an inductive approach, we define where the BCT might improve existing financial services, and how.

Due to the lack of scientific literature regarding the BCT adoption, this phase of our research was carried out thanks to the use of the grey literature, interviews with experts and through information on use cases world-wide, which we collected in a database. We have registered all the startups and all the initiatives carried out by established firms concerning

BCT since 2009 for the former and 2016 for the latter. This decision was made because startups could be born only after the release of Bitcoin, whereas for news, there were too few mentions of the technology in previous years to constitute a relevant basis for research. We relied on CrunchBase[11] for the startups' census and, for the other one, on the news posted on the main magazines dealing with blockchain news, which are CoinDesk[12], Blochckain4Innovation[13], Bitcoin Magazine[14], Cointelegraph[15], Cryptocoinsnews[16] and ETHnews[17]. Eventually, we obtained 633 startups and 530 news.

For each startup, we inserted in an Excel file information regarding the name, the country of origin, the geographical scope, the foundation year and the amount of received funds, which we could obtain from CrunchBase. In a second phase, we examined in detail each single website to define the sector in which the startup is operating, and, within the sector, the specific process it is specialized on. Thus, we subdivide them between eight groups: finance, logistics, virtual currencies, utility, media and arts, healthcare, market place and general purpose (startups not specialized in a particular sector but offering services to many of them). At this point, we selected only those which were classified as finance, virtual currency or general purpose, thus obtaining a group of 400 startups. These were furtherly analyzed in order to eliminate data which could be considered as a source of noise in our research. The following list are reasons for exclusion from the database:

- Those which likely inserted in CrunchBase the keyword "blockchain" to attract more attention, but which actually were not using it in a deeper analysis of their website,
- 'general purpose' startups which do not address the financial sector,
- Those which changed their names over time and resulted in duplicate entries (different names for the same company), so, we eliminated the old one.

Through this process, we arrived at a database composed of 247 elements. Then, we proceeded with the analysis of the remaining startups through the framework assembled from the literature review: in this way, we were able to identify the ones with a business model that actually requires the usage of BCT, and where technological limits are not hindering the service provision.

Regarding the database about firms' initiatives, we followed a similar path of analysis. Firstly, we classified them using the same scheme, then, we selected only the news concerning

[11] https://www.crunchbase.com/
[12] https://www.coindesk.com/
[13] https://www.blockchain4innovation.it/
[14] https://bitcoinmagazine.com/
[15] https://it.cointelegraph.com/
[16] https://www.ccn.com/
[17] https://www.ethnews.com/

the financial sector and the general-purpose ones. Subsequently, we eliminated the duplicated news due to the fact that we gathered them from various sources. Eventually, we obtained a database made 292 initiatives.

Analyzing the database on a case-by-case basis, we discuss startups and initiatives that are unfit for blockchain adoption according to our framework and why; we study in depth the ones that fit and show how blockchain technology should be implemented and, leveraging information available on the website or in the grey literature published, how to-be processes should be. In addition, we did not consider all the initiatives having the same impact: concerning startups, we gave more relevance to the ones which collected the most funds, signal of a higher level of trust in the initiative, while, in the other case, we have screened them on the basis of their level of development and the already obtained results if tests have been implemented.

The answer to the research question is a theoretical framework describing where and how blockchain technology could impact financial processes.

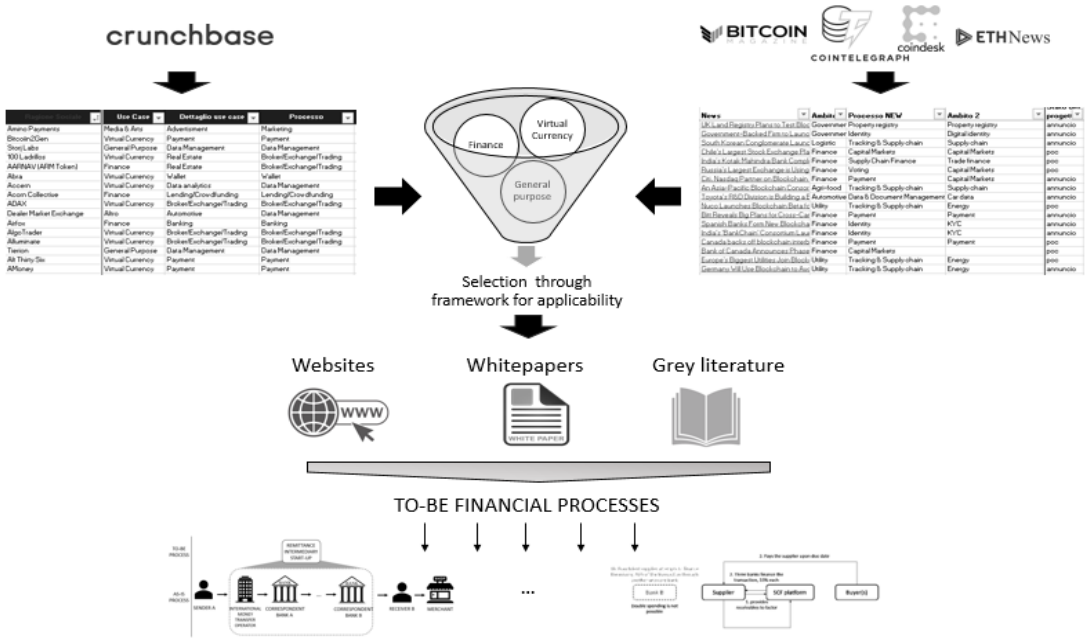


Figure 15, third phase methodological process

2.5 Fourth phase

What is the Italian financial institutions' position regarding BCT? What benefits and limits do they see in the adoption?

Once we defined a detailed description of the possible and appropriate applicability of the BCT in the financial sector from a global point of view, our focus narrowed to the Italian market. We decided to evaluate what Italian banks and insurance companies are doing regarding the blockchain and to compare it with the scheme developed in the previous phases. This step is useful to finetune our framework, checking if it can be considered a reliable instrument of analysis for BCT in a business context, and especially enrich it with experts' opinions on the benefits and limits of the technology. We aim to understand whether they have selected appropriate solutions brought by the BCT, or if they found new areas still unexplored. Moreover, we would like to determine the Italian financial market position with respect to this technology, and whether there are specific factors affecting it.

To gather information on this topic, a primary source was exploited. We have conducted direct interviews with representants of the major Italian financial institutions. Besides their opinion on the technology, which allowed us to define benefits and limits of BCT, they also presented us their projects. In this way we could check if further use cases would have been discovered or if they were aligned with the international ones.

For the selection of the financial intermediaries to be analyzed we considered two conditions: they should be Italian native and listed in the Borsa Italiana. Besides these obtained results, we decided to contact the other Italian banks currently taking part in the ABI Lab BCT project, whose consortium is the one mostly including Italian banks. Though being all contacted by email, we received the answers of nine banks and one insurance company, whose representants regarding the blockchain have been contacted though phone calls. Following the list of the interviewed institutions:

1. Banca Intesa Sanpaolo
2. Banca Unicredit
3. Banca Nazionale del Lavoro
4. Che Banca!, Gruppo Mediobanca
5. Credito Valtellinese
6. Banca Sella
7. BPER Banca
8. UBI Banca
9. Banco BPM
10. Cattolica Assicurazioni

Besides these interviews, we received the answer from two other banks, which stated that they are not currently studying the BCT, which can still be considered an interesting information for our analysis. These banks are Cassa Centrale Banche and Bancoposta.

The interviews were done through phone calls. Nineteen questions were prepared to make sure of fully covering our research topics. They can be divided into four groups.

The first part of the interview was completely led by the respondents, who described in detail their projects regarding BCT. We deepened our understanding asking whether particular factors have led them to choose a specific use case, therefore we asked the reason behind their decision. Depending on the use case they are applying the BCT, more specific and detailed questions have been asked, especially whether they encountered the same issues we have highlighted during the analysis of the international initiative, and in case how they solve or softened them. Moreover, we asked which kind of blockchain they used for their researched, such as Ethereum, Hyperledger, or other, and which kind of platform they prefer or mostly use between permissionless and permissioned. In the end, we asked about the 2018 budget allocated for blockchain researches.

Then, questions regarding the organization behind their studies on the blockchain were asked. In particular, the interest was on the process which led them to enter in contact with this new technology, which function within the firm firstly moved into this new technology and which one/s currently is/are working on it. Moreover, we asked whether the blockchain is being studying from more a technological or a business point of view, or both.

If not already mentioned, questions regarding the obtained results were proposed. Especially, we were interested in the level of maturity of each project.

The last set of questions are focused on the personal opinion of the respondents regarding the today scenario. We wanted to evaluate their point of view about the BCT's potential based on their knowledge and expertise. Therefore, we asked them whether they consider blockchain as disruptive, which its main limits and benefits are and where they considered it could be applied the most. This way, not only did we gather objective information about what they are doing, but also subjective thoughts.

Although a questionnaire was prepared, we did not strictly follow it. Instead, the interviews were done in a semi-structured way. While speaking with the interviewed, the order of the questions was not kept as it was or other questions were added to have a deeper understanding of their answers. This approach is considered highly appreciable to gather sensible information as it allows the interviewer to clarify doubts generated by unclear answers and to be sure to obtain clear and complete information on the covered topics (Cachia & Millward, 2011; Barriball & While, 1994).

During the interviews, notes have been taken by both the interviewers, which were then unified. In this way we were sure to write down as much information as possible. In case of ambiguity, the written answers were checked though the record of the call.

The data collected was subsequently analyzed. A two-step analysis has been carried out: a within case analysis, with the purpose of extracting precise information from each respondent individually, and a cross-case analysis, to compare these data among all the participants in order to find similarities and possible patterns.

During the first phase, an Excel file has been prepared filled with the relevant material gathered, which was subdivided into sections: number of projects, projects' use cases, starting year, level of development of the projects, leading function, meaning the area within the firm which first moved into the BCT studies, currently active functions, meaning the areas which currently are working on BCT-based initiatives, external support, 2018 allocated budget, consortium participation, name of the consortium BCT preferred platform, and disruptive BCT potentiality. Moreover, other two sections have been added after reviewing the interviews, the need of government support and the need of dedicated regulation. Many respondents indeed shared these last opinions, thus we considered them a relevant information to be highlighted.

Then, the interviews were reported subdividing each into four main categories. After a brief description of the financial institution, we listed the details about its blockchain projects, such us the use case, the possible participation in consortium, the allocated budget and the starting year of the research. Then we provide information about the institution's preference between permissionless and permissionless platform. Subsequently the information about its organization in following the blockchain researches has been proposed. Lastly, the respondent's opinions have been written down.

In this way, we could analyze in detail each single case, evaluating whether they choose efficient use cases, understanding their level of awareness of the technology and their level of maturity in the researches.

Once the database was ready, we started comparing the information to discover both similarities and differences among the considered groups. In this way, we wanted to assess the level of maturity of the Italian financial institutions regarding BCT, and to draw a general picture of the Italian financial sector with respect to this new technology.

Firstly, we created a table in which we combined the respondents and the projects, subdividing the latter by following the classification of the activities we performed in the second phase of our research. In the way, we wanted to highlight where Italian financial institutions are mostly committed to. Then, we evaluated the various projects sorted by activity. Therefore, we analyzed together all BCT application in payments, then in the supply chain finance and so on, with the purpose of comparing them and assessing whether they are efficient or deceptive use cases.

After evaluating the goodness of the financial institutions' undertaken projects though the use of our framework and the obtained results of the previous chapter, we took into consideration the other pieces of information we gathered from the interviews.

We decided to evaluate the level of awareness of each financial institution. In this way, we can have a better understanding of their position concerning the BCT, assessing if they are still in an initial phase of work, or they have already acquired a good level of knowledge regarding the technology. To do so, we decided to define an index ranging from 1 to 5, where 1 refers to a low level of awareness. The index is a weighted average of different information we gathered from the interviews.

- the year in which the FI started studying the technology,
- the number of studied use cases and their level of development,
- the allocated budget for the BCT projects
- the internal organization regarding the BCT.

The starting year of the studies has been considered as a component affecting the awareness as we may assume that the longer an institution has been studying a topic, the more consciousness it has acquired about it. The first one which focused on the blockchain started in 2013, thus we assigned to this year the maximum score of 5, while decreasing values to the subsequent years, as we can see from the following table:

Starting year	2013	2014	2015	2016	2017	2018
Score	5	4	3	2	1	0

Table 1, index scores for projects' starting year

Another critical factor which influences the apprehension on the topic is the number of undertaken use cases and their level of development. If the application of the blockchain by an institution ranges over a high number of different functions, we can presume that the same one has a broader understanding of it. The player may have indeed evaluated more in depth the possibility of the technology, and having acquired more trust in it, as well as greater skills in dealing with it. However, this information alone may be misleading, as an actor might just pick up by chance some projects and test it, without having developed any previous evaluation and considerations. Therefore, we combined this data with the level of development of the correspondent project. We have identified five different possible states:

- not suitable for blockchain, for all those projects which could be better implemented through traditional databases,

- empirical no-result test, for those projects which have been implemented only for studying the underlying technology and acquire familiarity with it, or for those which have been put in hold or abandoned,
- theoretical evaluation of possible use cases, not subsequently implemented,
- proof of concept,
- already or soon operative.

Following the order of the above list, we assigned them scores from 1 to 5.

Each of the project is therefore assigned a score depending on its level of maturity, and then these scores are summed together. Considering that the maximum number of relevant projects developed by an interviewed financial institution is five, we obtained a point range which goes from 1 in the worst case, i.e. in the event an actor is only studying a single use case, which appears not suitable for blockchain, to 25 in the best case, i.e. if a bank is operative (5) with five different blockchain applications.

The third considered factor is the 2018 allocated budget. In this case, we have assumed that the more an institution has invested on blockchain projects, the more it has been dedicated to them, thus the more knowledge about the topic it has gained. The range of financial institutions' investment, which goes from less than €100,000 to more than €1 million, has been divided into five slots, to each of which has been assigned a value, as we can see from the following table (the budget is in euros):

Allocated budget	<150K	150-299K	300-449K	450-600K	>600K
Score	1	2	3	4	5

Table 2, index scores for projects' 2018 allocated budget

The last component of the index is the organization. To have an efficient impact on the firm and on the connected processes, a technological innovation should not only be studied with the focus on the technology, but also from a business point of view (Baden-Fuller & Haefliger, 2013). We considered this notion among the elements impacting the awareness, since only in the event that an institution applies it, it will have the possibility to gain benefits from the blockchain. Therefore, greater advantages can be obtained only if aware of the crucial importance of the business components. In this case, we allocated three different values. A 3 will be assigned when both IT and the business functions are collaborating on the projects, 2 when only the IT people are involved, and 1 when none of them is studying the blockchain, but other functions or no functions at all.

The final values of the index attributed to the banks will range from 1 to 5, thus the second and the last constituents need conversion factors from a scale made respectively of twenty-five

and three elements to the final one, made of five elements. A simple proportion can be performed to translate these values and therefore to obtain the conversion factors:

$x: 5 = y: 25$, where y is the score related to the use cases ranged between 1 and 25, while x is the correspondent score in a range from 1 to 5. Therefore, the conversion factor is 5/25, which is 0,20.

The same calculation can be applied for the conversion of the score regarding to the organization from a three-element scale to a five-element one, thus obtaining a conversion factor equal to 5/3.

After defining the component of the formula, we chose their correspondent weight. Since the second component of the formula, the one relative to the use cases, is made of two different type of the data, i.e. the quantities of projects and their level of development, we considered the index as comprised of five units. Therefore, the budget and the starting year have been assigned 1/5 of the weight, equal to 20%, each. Concerning the organization factor, it has been given a lower weight, since it does not directly refer to the understanding of the blockchain, but instead to a way to fully exploit it. On the other hand, the number of different projects assume a more relevant position for the apprehension process. Therefore, we attributed respectively a weight of 10% and 50% to them (keeping in mind that the latter is a double factor, thus each piece of information is given 25%).

The awareness index can be calculated with the following formula:

$$20\% \times \alpha + 50\% \times \frac{5}{20} \times \beta + 20\% \times \gamma + 10\% \times \frac{5}{3} \times \varepsilon$$

Where

α refers to the score relative to the *projects' starting year,*

β refers to the *use cases* score,

γ refers to the *2018 allocated budget score,*

ε refers to the *organization* score.

The results have been then compared between the various financial institutions.

After having identified the level of awareness about the technology for the interviewed banks, we decided to further analyze how they are approaching it. In this way, we defined the position of the Italian financial institutions with respect to the blockchain. To do this, we combined two gathered pieces of information, the internal organization of the FIs concerning the studies on the blockchain, and the future expectations about it. Two scenarios have been

considered: the blockchain as a disruptive innovation or as an efficiency enabler, which means that it is still considered a potential positive instrument but not able to fully change the current dynamics. For what concern the internal organization, we have defined three possible structure: a team completely dedicated to the blockchain, a non-structured function, which means that the BCT is studied together with other technologies, by people who are therefore not completely focused on it, and absent, for those cases in which the BCT is not studied at all. This information has been combined in a matrix which showed us four different typologies of actors:

The revolutionist, which are the ones mostly convinced of the BCT potentiality and that have therefore a group of people completely dedicated on it.

The experimenters strongly believe the blockchain will be ground-breaking, but they have not fully dived into it yet. They are studying it through usually the innovation function, whose scope is to identify and evaluate new ways to improve the current processes and state of the institutions. They are taking part to many conferences on the topic to enter in contact with many experts and players which are more advanced with their researchers to gain from them useful knowledge.

The cautious expect the blockchain to have a limited impact in the future. They consider it as a useful instrument to be studied and to be used to gain efficiency, but they doubt it will not be able to overcome the current system. For this reason, their IT or innovation functions are partly focusing their attention on the technology and how it can be adapted to the existing ones. They also take part to conferences with the intention of increasing their understanding on the topic and to try to solve their doubts.

The sceptics are currently not studying at all the blockchain. Two may be the reasons behind this choice. On one hand, they might be small financial institutions which do not have sufficient money to be invested in this still early-stage innovation, which is not completely operative yet. On the other hand, they might be uncertain about the blockchain and its real-life applications. They are still not sure it will bring great advantages with respect to the traditional technologies. In both cases, therefore, they are waiting for other to study and test it, and they will approach to the BCT only once it will enter into the market.

In this way, we could highlight the different position of each single institution and determine how many of them are still in an early stage of analysis regarding the topic and how many fully trust the technology and which others do not.

To deepen our understanding of the internal organization choices we have also considered how the institutions, and more precisely their responsible functions, approach the BCT. We have analyzed if they are moved by more technical lenses or by a business vision. For this

research we focused only on the interviewed institutions, as they are the only ones which organizationally arranged for studying the blockchain. This way, we could conclude how the Italian financial institution are viewing the blockchain, if they consider it more from as a more technical instrument or if they see also business potentiality in it. We have indeed said that a new product needs to find its commercial application to fully exploit its potentiality and be considered a real innovation. According to the Schumpeterian business cycle (Kuznets, 1940) indeed an invention can turn into an innovation when it is commercially used.

Finally, we combined all this information regarding the banks in a graph representing on one size their level of awareness, while on the other axe the categories to which they belong, thus depicting their level of maturity with respect to the technology, and therefore showing the Italian financial institutions position and answering our research sub-question.

CHAPTER 3
TECHNICAL ANALYSIS

In this chapter, our purpose is to develop a general adoption framework that can drive us in the selection of blockchain initiatives, as a filter to those that do not employ blockchain in a sensible way, or do not fully consider its technological limits. This is essential to carry out the analysis of empirical data and eliminate the noise of deceptive use cases. We did this by developing a general framework that could be actually employed in any sector, and only in a second moment we applied it to financial services specifically. This general analysis allowed us to understand strength and weaknesses of the technology and have a deeper understanding in the analysis of empirical data.

To review the literature on this topic, we clustered papers according to the classification of blockchain constraints proposed by Swan (2015):

1. privacy,
2. throughput, latency, size and bandwidth,
3. security,
4. usability, versioning and forks;
5. wasted resources.

The same approach is followed by other studies reviewing the technical literature surrounding these technologies, such as Yli-Huumo et al. (2016). To this list, the privacy was added after reviewing several papers highlighting how personal data can be easily identified in public blockchains and other works of literature review (Herrera-Joancomartì, 2015). Open issues are reviewed according to this order, throughout sections 3.1 to 3.5.

In section 3.6, we present innovative proof-of-stake protocols that could allow public blockchains to solve most of these technical limits.

In section 3.7, we review consortium blockchains, if and how technical constraints impact their adoption in business applications.

In section 3.8, we conclude the technical analysis by summarizing the relevant findings and answering the question about the viability of the technology in the financial industry.

Then in section 3.9, we go on with technical literature review, but instead of looking at the hurdles from a performance standpoint, we shall consider the applicability of blockchain technology compared to other solutions, that is, centralized database. Indeed, picking either of the two must be determined by an in-depth analysis of architectural solutions, as an extra cost has to be paid to guarantee decentralization, so the latter should be avoided where possible. We conclude the chapter in section 3.10, with a framework that considers both architectural constraints and technical ones. It will enable us to correctly discriminate between valid blockchain use cases and fallacious ones, as centralized solutions would have been best suited.

3.1 Privacy

Contrarily to common knowledge and despite their usage in black markets on the dark web, cryptocurrencies are far from ensuring users privacy, especially for firms and institutions planning to use them. The main issues that can lead to the exposure of users' identities are the possibility to analyze the blockchain public ledger with data analytics techniques to extract knowledge about users' accounts and transactions, and the analysis of packets sent between nodes using the internet TCP/IP protocol.

3.1.1 Blockchain Analysis

The first issue we tackle is present in all public blockchains, and it is blockchain analysis: the full list of transactions is available to any node in the system and is updated in real time as the blockchain expands. Furthermore, many websites allow a real time visibility of transactions and block mining[18]. This leaves open space for data analytics techniques to extract relevant information from the ledger, exposing users' data.

If address information is hashed and anonymous, transactions, and thus the flow of money, is visible globally. This property of public blockchains is defined and leveraged by Meiklejohn et al. (2013) to map Bitcoin transactions using data analytics techniques. After downloading the blockchain from Bitcoind public client, they tagged addresses by actively

[18] Such as: https://etherscan.io/

sending transactions to notorious Bitcoin operators of the time and tracing the address they transacted to in the Blockchain to discover its whole transaction history. For instance, they deposited and withdrew money from the exchange Mt. Gox to see the address it used, and then tagged all transactions in the blockchain using that same address as belonging to Mt. Gox. This approach allowed the authors to map transactions of merchants, exchanges, wallets, mining pools and investment schemes, plus a set of unidentified addresses transacting with them. The conclusion is that Bitcoin economy can be easily exposed with a heuristic clustering analysis, highlighting transactions (and thus costs and revenues) between companies using Bitcoins. A possible solution would be to constantly update the address used, with the purpose of hindering such kinds of data analysis, yet this would require a constant effort and a significant loss of usability. Despite the study is focused on Bitcoin, similar results can be achieved on most public blockchain[19].

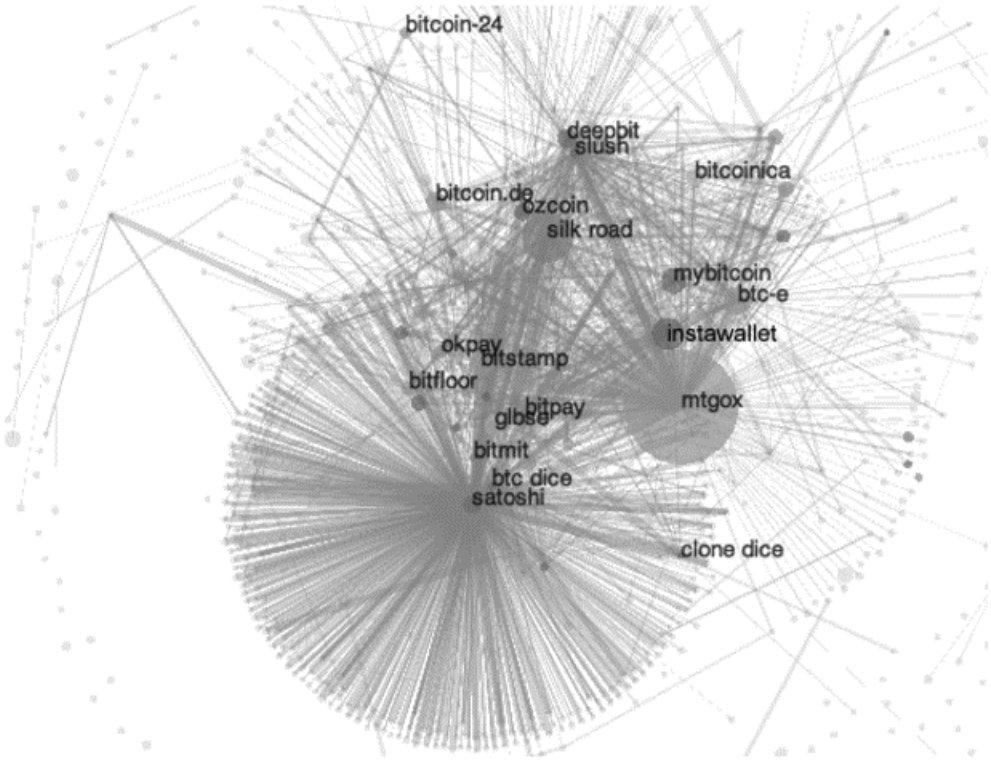


Figure 16, visualization of Bitcoin user network (from Meiklejohn et al., 2013); the area of each cluster represents the value of transactions.

Reid and Harrigan further researches in this direction by constructing similar representations of Bitcoin transactions, but instead of actively sending transactions to identify addresses, they only leverage search engines and publicly available address to tag transactions.

[19] In later paragraphs, we will discuss blockchain protocols enhancing users' privacy.

In fact, many websites and users make their Bitcoin address public to receive payments or donations, consequently jeopardizing their financial privacy. The authors also highlight that transactions moving Bitcoins from two or more different addresses are most likely linked to the same owner, thus easing the tagging process. In conclusion, even with a passive analysis (i.e. not actively sending "marked" Bitcoins), the authors managed to obtain relevant information on specific individuals and organizations using Bitcoins, mapping a detailed view of their activities. In addition, entities such as exchanges can have a far deeper insight on users' activity as not only do they know the blockchain addresses they have, but also real bank account address or credit card numbers which are needed to complete cryptocurrency purchases, together with a set of other information (name, home address, nationality etc.).

A general suggestion to increase anonymity is to ask users to use always new addresses when receiving/sending transactions, so that their activity is harder to cluster[20]. However, Androulaki et al. (2013) find that even this measure is not sufficient. In their study, a simulation software is employed to replicate a university campus conducting transactions with Bitcoins. Even if plain clustering techniques are not applicable to users that are aware of privacy issues and keep changing their address, the authors apply behavioral economics techniques for the clustering, and manage to identify 40% of such privacy-aware students, compromising their anonymity. Therefore, not even constant address change can be considered a solution.

On the bright side, the little privacy available in Bitcoin allows easy forensic analysis and a fast identification of criminal flows, thefts and similar activities. To this purpose, Spagnuolo et al. (2014) engineered a forensic software, BitIodine, which is able to automatically trace address, cluster and tag them leveraging web and exchange queries. With manual input, it allows the identification of specific transactions, and the amounts they contain (for instance, they found the exact value of Ransomware transactions corresponded by the victims).

Concluding this section, we note that the literature is unanimous: blockchain analysis can easily reveal relevant information on users' transactions and their identity; public blockchains using protocols like Bitcoin's and standard encryption of addresses are far from guaranteeing anonymity.

3.1.2 Network TCP/IP analysis

Koshy et al. try to leverage network analysis to obtain relevant information on Bitcoin addresses. In fact, when a user performs a transaction, all relevant information is communicated to peer nodes nearby, and then gossiped (transmitted) across the network. The

[20] https://bitcoin.org/it/

authors develop CoinSeer, a Bitcoin client able to gather gossiped data which is then linked with IP addresses, where possible. The authors managed to associate between 252 and 1,162 Bitcoin addresses to the IP address of their owner, thus compromising his privacy. Nevertheless, a significant amount of anomalous transaction traffic, caused by either a frequent change of address by the same user, the invalid methodology of referring the owner of the transaction to its first transmitter: in fact, in case of slow connections between some of the peers, it could be possible to receive the transaction from the peers first, rather than from the actual owner of the Bitcoins. Also, the authors note that the usage of safer protocol such as Tor or I2P can render they exercise impossible, as the transmitter would never be the owner, who will have his IP address always covered behind a proxy. To conclude, it is possible to identify IP addresses belonging to specific subsets of users and compromise they anonymity, but the instrument is not generally reliable as, with simple measures, users can protect their IP address and make it non-linkable to the transaction they carry out.

3.1.3 Anonymity enhancing practices

To overcome these difficulties in public blockchain protocols, many solutions have been proposed. As we have seen, the most common and simple is the creation of new addresses every time a transaction is carried out, but this practice is useless when using behavioral clustering techniques and if the amount contained in the address is not immediately cashed out: indeed, using it for other transactions or moving it to newly created address just makes the identification process easier.

Mixing

A more elaborated and effective solution is the usage of mixing services. A mixing service is a centralized service grouping incoming transactions and then moving them to the beneficiaries, mixing original senders while making sure transactions amount are the same as specified. For instance, consider Figure 17 representing three users transacting among themselves: in a standard blockchain transaction, the address of the sender and the receiver would be linked and the amount plainly visible; via the mixing service, amounts are still visible, but the receiver and the sender are linked randomly by the mixing service which is only guaranteeing that the amount sent corresponds to the amount received (Moser et al., 2013).

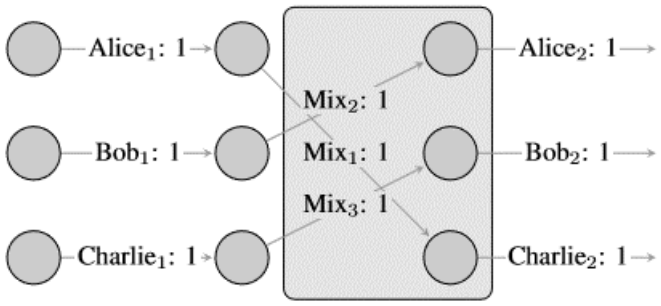


Figure 17, a representation of a mixing service: 3 users are moving 1 Bitcoin to another address they own (from Moser et al.).

The incentive for the mixing service is a fee, which is held from the amounts transacted. In addition, important advantages of the blockchain are cut out: trust is lost as users have to trust the correct and honest functioning of the mixing service; decentralization is lost as the service is fully centralized. Even anonymity itself is not guaranteed: the service has full visibility on the transactions and the users' addresses, which are stored on its database. The service could gain incentives by secretly disclosing data to a paying source or could be hacked and all the centralized data can be exposed (Meiklejohn and Orlandi, 2015).

Moser et al. (2013) also study the legal implication of such services: they are de facto money laundering tools, and their names can make this quite evident (considering for instance "BitLaundry"). The authors also compare different mixing services: Bitcoin Fog, BitLaundry, Blockchain.info with its Bitshared functionality. The authors tried to graph transactions after using such services. As a result, they found that Bitcoin Fog and Bitshared are reliable, as the transaction graph could not highlight relevant links between receiving and sending addresses (despite a clear pattern allowed them to understand how the Bitcoin Fog protocol worked which, according to them, could increase the chance of identifying links for attackers). Conversely, the BitLaundry tool was found to be unreliable due to clear connections in 2 out of 3 tests. Finally, they note that a certain latency in the money transfer, i.e. the mixing service holds coins for a certain period of time before corresponding the payment, can increases its effectiveness.

Nevertheless, new protocols have been proposed which render mixing services trustless, such as CoinJoin (Maxwell, 2013a) or CoinWitness (Maxwell, 2013b) which allows user to agree among them the creation of a multiple input and output transaction leveraging a partial cryptographic signature; on this system is based Dash, an altcoin 13th in terms of market cap[21]. Alternatively, new mixing services were designed giving better guarantees to users, such as

[21] From here on, when we refer to market caps of coins, we intend that data was consulted on https://coinmarketcap.com/ at the moment of writing.

MixCoin, where users receive a signed warranty able to prove that the mixing service has misbehaved (Bonneau et al., 2014).

If several problems hindered the usage and widespread adoption of mixing services, research developments solved many of them, allowing users to retain privacy in their transactions. However, Meiklejohn and Orlandi (2015) still highlight open issues that these enhanced privacy service can trigger, such as relevant trade-offs with the scalability, an increasing complexity in the user interface, since these services requires extra step to carry out transactions and need to be understood by the users. Especially, CoinJoin and similar protocols are exposed to DDoS attacks by the users who could stall joint transactions, and of further data leaks or privacy infringement by collecting all signature data into a single server.

Improvements to the Bitcoin protocol

Other researches propose improvements to the Bitcoin protocol which could increase users' financial privacy. Saxena et al. (2014) propose a system using *composite signatures*. Using this cryptographic tool, the authors implement a better Bitcoin protocol that, instead of including each signed transaction into the blockchain and thus make it visible to anyone, the composite signatures have the property of being aggregate into one signature, such that, once aggregated, individual signatures cannot be recovered. Thus, it is impossible to link input and output address of a transaction, as the sender can sign transactions with no explicit references to the receiver address. In fact, input and output address do not have to be known in advance, and as the composite signature is passed around it is also DDoS resistant, and a better alternative over CoinJoin. However, a modification of the Bitcoin protocol which at the moment of writing has not happened yet, is required to implement this composite signature scheme.

New cryptocurrencies

Many researchers preferred the proposal of new protocols to implement in altcoins, rather than confronting with the task of modifying existing protocols. The main protocols we identified in the literature are of two kind. The first kind leverages non-interactive zero-knowledge proof, and it was proposed for the first time in ZeroCoin by Miers et al. (2013), and ring signatures

Zero-knowledge proofs allow a prover to demonstrate some information to a verifier, without disclosing it; as a naïve example, the verifier has two identical pens of different colors, but he is color blind; the prover can demonstrate he is not colorblind by having the verifier mix or not the pens behind his back and then tell if the mixing has happened, without

disclosing the information of the pens' color[22]. In ZeroCoin, the same happens, instead of attaching the addresses and the amounts transacted to verify that users are not double-spending their coins, a zero-knowledge proof is attached so that no one can see amounts and addresses involved but can verify that the operation can happen; also it is non-interactive, meaning that the verifier does not have to exchange messages with the prover to obtain the proof, thus reducing computational effort. ZeroCoin was a proposal to improve the Bitcoin protocol originally having many issues, such as low scalability and high computational time to achieve the proofs. Lately, most of these problems have been reduced thanks by developing it in the altcoin Zcash[23], 19th most capitalized cryptocurrency. The protocol used by Zcash is zkSNARK (zero-knowledge Succinct Non-interactive ARgument of Knowledge), which effectively implement zero-knowledge proof, and was also adopted by JPMorgan on its Quorum private blockchain[24].

The other effective tool to render transactions private is ring signature. Ring signatures can hash a message giving a guarantee that: the member of a certain group has signed the message; the member who signed is undistinguishable among his peers in the group. Every member can compute a ring signature on a message using their own private key and the group's public keys, thus verifying for instance that transactions are not in conflict or have been double-spent. For instance, a president of the G20 releases a message using the ring signature of G20 presidents: every verifier can use the public key of G20 presidents to have a prove that the message is actually coming from a president, but the ring signature will not allow him to decrypt which of the 20 presidents actually wrote the message (Rivest et al., 2001; Tschorsch and Scheuermann, 2016). Monero is likely the most famous altcoin leveraging ring signatures to enhance its privacy: it's the 10th most capitalized cryptocurrency.

The general risk with these new cryptocurrencies is that they offer such a high level of privacy that their adoption is far riskier in terms of compliance: regulators are very unlikely to approve such a high level of anonymity on financial transactions and might deem these altcoins as money laundering tools.

Wallets

At last, wallets are one more way to increase anonymity indicated by the literature. Herrera-Joancomartì (2015) defines wallets as centralized services that operate as a bank: instead of having users download Bitcoin (or other) clients to interact with the blockchain, they provide a cryptocurrency account. Users do not have an address themselves, instead, they

[22] https://www.youtube.com/watch?v=HUs1bH85X9I
[23] https://z.cash/
[24] https://www.coindesk.com/jpmorgan-integrates-zcash-privacy-tech-enterprise-blockchain/

leverage the wallet address to carry out payments or receive money, so that their identity cannot be unveiled from a blockchain analysis. Again, the problem with such services is that they are centralized and by using them users have to put a lot of trust in their well-functioning: first, if privacy is guaranteed towards anyone trying to inspect the blockchain, a lot of information is disclosed toward the wallets which have full visibility on account movements, users' identity and any other kind of operation; secondly, wallets store data such as the keys to access users' accounts on centralized servers, posing a cyber risk in case of cyber-attacks as we will see in the security section.

3.1.4 Lack of data

As explained Hoskinson (2017), the apparent lack of privacy in blockchains is still far from the needs requested by institutions, such as financial ones. Blockchain transactions are public, but the only data attached concerns the amount of the transaction and the two public addresses of the sender and the recipient. In a banking transaction, this level of anonymity is unacceptable, despite the techniques explained to unveil identities: banks' transactions also are endowed with metadata, that is, extra data about the transaction, like what is the money being spent on; and attribution, i.e. the entities involved are clearly and unambiguously identifiable. This information is used to comply with authorities' regulations, mainly concerning AML and CFT. This causes many problems to cryptocurrencies users, for instance, a company carrying out an ICO could not be able to cash out the money in a traditional bank without providing extra data about the source of the money and the identity of the investors, which have to be assessed in traditional ways and cannot be embedded in the blockchain. To counter such issues, research is under way to allow payors to include extra encrypted data in transactions which can be read only by authorized institutions. Consequently, a good level of privacy is ensured, while relevant information for institutional use are included, making the transaction usable in a traditional banking environment.

Ateniese et al. (2014) focus their research on this problem, in particular the data required for attribution: as of now, it is impossible to authenticate with certainty the entities connected to public Bitcoin addresses. This problem is the inverse to the lack of privacy issue described: even if an authority can be identified by a blockchain analysis, the authors propose that it be identified by a certified address, so that an active analysis is not needed, and regulators can easily determine which firms or authorities are involved in payments. To do so, an extension of the Bitcoin protocol is developed which introduces a further verification on institution address to determine that it was the one officially released by a regulating authority. In fact, a firm seeking certification can request to a regulator the issuing of a certified Bitcoin address which can later be effortlessly checked upon completing transactions.

In conclusion, there are evident anonymity issues with public blockchains not taking measures to increase users' privacy in their protocol. Several solutions have been proposed, some are centralized such as mixing services and wallets, thus requiring trust in a central player, some are decentralized, such as new cryptocurrencies with privacy-enhancing protocols, but pose a serious compliance risk if adopted at industry level, due to adverse regulation, and have a high computational cost. Indeed, a lot of data surrounds regulated banking transactions, to prevent misusage of funds or the financing of criminal activities which cannot be included in blockchains without further exposing users' privacy. Research is currently in place to solve this latter issue, but functioning solutions have not been released yet in public systems.

3.2 Throughput, latency, size and bandwidth

The second issue, or rather set of issues, we shall deal with is that of network capacity. Important factors related to network capacity are: throughput, generally measured as the amount of transactions that can be processed by the blockchain network in a given time (typically transactions per second, TPS); latency is the time passing between the broadcast of a message to a peer and its response; size and bandwidth have to deal with block size and the time needed to gossip it to peer nodes which depends on the bandwidth of the network; size also refers to the dimension of the blockchain in terms of bytes (Swan, 2015).

From the literature emerged that all these parameters are in a strict tradeoff with one another. In fact, let us consider how the throughput of a blockchain is computed: all blockchains have a block size limit embedded in their protocol, a fixed block production time, telling how often a new block should be created, and an average transaction size, which depends on the information the protocol requires users to include in a transaction. The throughput is then the maximum block size divided by its production frequency and the average transaction size, for instance in Bitcoin where a block can be at most 4MB big, a new block is added every 10 minutes and transactions have an average dimension of 544 bytes[25]:

$$(3.2)\ Throughput = \frac{4{,}000{,}000\ Bytes/block}{600\ \mathrm{sec}/block\ \times\ 544\ Bytes/transaction} = 12.24\ TPS$$

The throughput amounts to 12.24 TPS. This number is often compared with centralized payment processing systems such as that of Visa which can reach peaks of 10,000 TPS, 1000x away from current blockchain capabilities (Swan, 2015). Scaling blockchain throughput is not as easy as increasing block size nor reducing the inter-block time, as the equation above might

[25] https://tradeblock.com/blog/analysis-of-bitcoin-transaction-size-trends

suggest. Indeed, twisting these numbers increases the time needed to propagate information across the network: every node has to receive updated information on the blockchain status, so that e.g. miners can move on mining a new block if the current has already been mined by someone else. The bigger blocks are, the more time it takes to upload information across the network due to bandwidth constraint, which are depending on the internet network used to communicate, and the lower the fees miner can ask. Instead, the smaller the block time, the larger is the probability of forks and their length, which, as we will describe in section 3.4, reduces the reliability of the blockchain and heavily jeopardizes transactions' finality. These implications are discussed in the literature which proposes improvements based on the following factors: block size and block time, general protocol, sharding protocol, sidechains, off-chain solutions.

3.2.1 Block size and block time

A first set of papers tackles the issue of block size and time. A first proposed improvement comes from Johansen et al. (2015) who propose Fireflies, an overlay that is potentially applicable to any network and is useful to give visibility of each network participant to the sender of a communication. In Bitcoin and similar blockchains, communication happens through a gossip protocol, that is, a communication protocol where all nodes have bilateral interactions with one another, routing information to connected peers only; then, the latter further communicate this information to other connected peers and so on, until all the network is reached. This protocol is considered quite inefficient, and the implementation of Fireflies would allow a complete vision of network participants to each node, so that, instead of gossiping information from peer to peer, the sender can communicate straight with the receiver node, significantly increasing efficiency. There are many other studies (Dimakis et al., 2006; Dimakis et al., 2008; Chuat et al., 2015; Lin and Marzullo, 1999) dealing with the efficiency of gossip protocols, anyway, we will not provide further insights in this direction as it is generally related with communication protocols in networks and not a strictly blockchain-related problem, even if, like we noted, development in this research area can strongly benefit blockchain innovation.

Other studies take care of the measurement of information propagation in the Bitcoin network, reaching relevant findings on the block size and time which we anticipated above, as well as how these dimensions are related to the mining fees. Decker and Wattenhofer (2013) analyzed the time needed for blocks to propagate in the Bitcoin network. They found that block size increases significantly the time needed to propagate information across the network, in particular, time increases linearly with the size of the block above 20KB, whereas below this threshold, block propagation is extremely inefficient: as size decreases, transmission delay

increases exponentially. This is not a big issue as blocks typically exceed this size. The problem is more relevant for transactions which have an average dimension of 544B, like we wrote earlier, and 96% of them has a size inferior to 1KB. The reason is that blockchain protocols require a roundtrip for messages before they are actually transmitted: indeed, a node does not communicate a transaction or a block directly, it first sends an *inv* message to check if the receiving node already has the piece of data that should be sent. The receiving node answers the *inv* message and, only in case the data is missing, it is finally propagated. The authors suggest that this roundtrip be implemented for blocks only, whereas transactions be transmitted directly, since they are smaller in size. This way, delays in information propagation would be reduced significantly, as well as the number of forks.

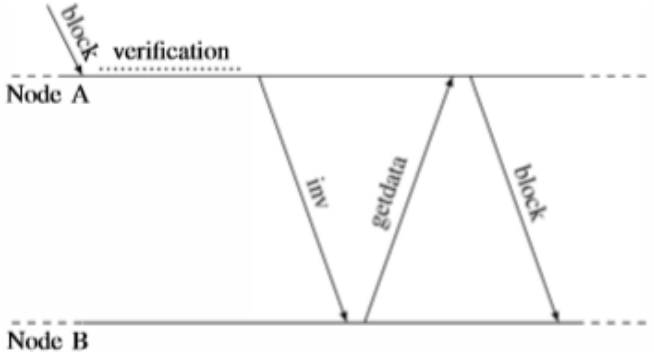


Figure 18, the message exchanged by two nodes to propagate information across the Bitcoin network (from Decker and Wattenhofer, 2013).

Croman et al. (2016) deepen the study on decentralized blockchain scalability by tweaking Bitcoin protocol's parameter, such as block size and its time. From their findings, they establish an upper limit in the block dimension to 4MB[26] (given 10 min block time) or a lower limit to block time to 12 seconds. With these parameters, Bitcoin could be processing at most 27 TPS. This number is conservative, actually the potential throughput of the network is much higher according to the author's measurement, and the limiting factor is the protocol: e.g. transactions are transmitted twice, first to gossip it, then again as part of the block; or due to the lack of pipelining, delays increases as multiple hops are needed for longer paths. The successful implementation of SegWit confirmed the authors' findings.

Another central aspect in the block size and time fine-tuning is constituted by miners' fees. Specifically, Houy (2014b) demonstrates that from an economics theoretical standpoint, setting a block limit while leaving an open market for block space is equivalent to setting a fixed fee for each transaction. In general, fees can be attached to transactions at users'

[26] Ed. at the moment of writing, block size in Bitcoin was still of 1MB, only after the implementation of Segwit it did reach 4MB.

discretion: the reason to attach fee is to give miners an incentive to include one's transaction in a block. If this incentive is not high enough, transaction will remain orphan and not included in any block, i.e. it will not take place. Transaction fees are largely out of users' control and mainly depend on the size of the transaction itself: bigger transactions require bigger fees as they take up more room in the block. An increase in the block size would reduce competition (i.e. fees) to include transactions in a block, thus reducing miners' incentive to mine new blocks: this is the main reason why miners generally oppose block size increases. At the moment of writing, average transaction fees hover around 0,5$ but can increase dramatically as the posted transactions increase and block space becomes a scarce resource, for instance in December 2017 transaction fees reached an average of 55$ per transaction[27]. On the other hand, Croman et al. (2016) found that blocks with empty space increase transaction costs, whereas blocks mined at maximum throughput decrease costs, highlighting an economy of scale factor.

In conclusion, tweaking protocol parameters to optimize throughput is possible but results have low impact because other factors come in tradeoff: miners' fees (and their incentive) decrease, bandwidth usage increases (causing delays), communication protocols, and probability of forks.

3.2.2 General protocol improvements

More radical suggestions propose new protocols to work around the constraints limiting blockchains throughput. Sompolisky and Zohar (2015) again give evidence on the difficulties in Bitcoin throughput, shedding light also on the fact that at high throughputs there are even implications for security. They criticize the tweak of parameters as a solution, since accelerated block creation for instance causes an increasing number of forks and thus a loss of efficiency in the chain creation; on the other hand, an attacker would be able to create blocks faster without any efficiency loss. As a solution, they propose the GHOST protocol, adopted by Ethereum in a modified version, to improve throughput without jeopardizing security against attacks.

The GHOST protocol is an acronym for greedy heaviest-observed sub-tree which is a new protocol to select the "right" chain to work on in case of forks. Bitcoin protocols ensures that new blocks select a parent block considering which is the longest available chain; in the GHOST protocol instead, it is not the length of the chain that counts but the weight of all the blocks forked: this weight is computed based on the largest proof-of-work effort embedded in the blocks. For the sake of simplicity, in Figure 19, it can be seen how the GHOST protocols

[27] https://bitinfocharts.com/comparison/bitcoin-transactionfees.html

selects the parent of new blocks: instead of selecting the longest chain, the chain with the most blocks (the most proof-of-work) is selected, that is the one with 12 blocks appended to it (all the ones branching from block 1B). Conversely, the Bitcoin protocol would only consider the chain following block 2D, constituted by 5 blocks and that can be easily attacked by a hypothetical attacker trying to attach blocks 1A and following. This attack is largely negated by the GHOST protocol. This way, blockchains with a much smaller block time and bigger block size are possible, such as Ethereum adding a new block every 12 seconds on average, allowing for 15-25TPS processing (Buterin, 2013). The GHOST protocol has however been criticized by the literature in terms of security and communication problems when transmitting information to compute the heaviest subtree, which miner should consider, to add further blocks (Kiayas and Panagiotakos, 2015).

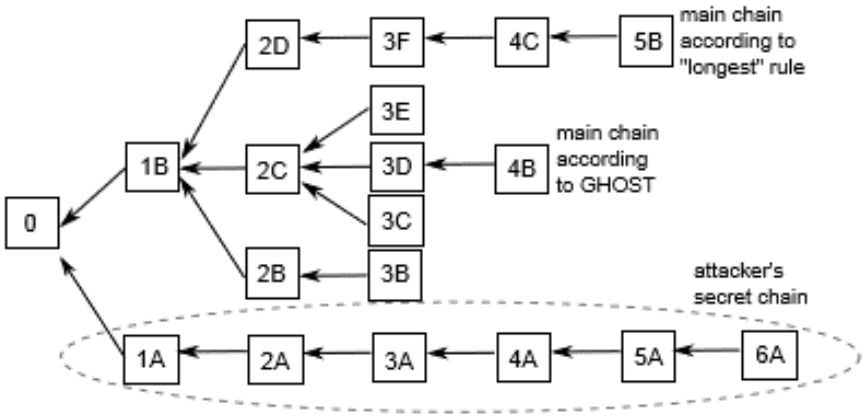


Figure 19, an illustration of GHOST protocol (from Sompolisky et Zohar, 2015)

Another solution is proposed by Eyal et al. (2015) who suggest the Bitcoin NG protocol. In this implementation, scalability is achieved by introducing new rules for block creation: instead of having just one type of blocks, Bitcoin NG distinguishes between *key blocks*, which are mined just as Bitcoin blocks are, and *micro blocks*. When a node successfully solves the proof-of-work and mines a key block, that very node is elected as leader and allowed to further add micro blocks to the chain. These micro blocks do not require computations, they can be attached freely by the elected leader node. Anyway, a limit is set such that micro blocks cannot be timestamped in the future nor in a way that the difference with their predecessor is inferior to a threshold. This way, the protocol prevents malicious leaders winning the election from populating the blockchain with a big number of micro blocks and secures a limit until the next leader is elected, every 10 minutes like in Bitcoin.

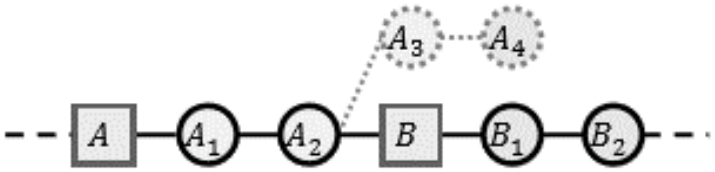


Figure 20, conceptualization of forks in Bitcoin NG protocol (from Eyal et al., 2015)

Forks can happen, as elected nodes validating micro blocks keep appending them to the key block they mined, new key blocks could be mined by other nodes, making all micro blocks with greater timestamp orphans. Finality of transactions is therefore guaranteed when the propagation time for micro blocks to the rest of the network is guaranteed. Despite general agreement in the literature about Bitcoin NG improvements, doubts were cast on security and the possibility of DDoS attacks carried out on the leader node as, for the time it is elected, it is in charge of a centralized management of the blockchain (Tschorsch and Scheuermann, 2016).

In addition, an increasing number of nodes in both the protocols increases the computational power required by each node and the network latency, making large scale adoption a challenge (Luu et al. 2016).

These newer protocols show that efficiency in throughput can be achieved with better communication or different rules regulating forks and validation, so that interval between blocks can be reduced without hindering security or finality. Despite not reaching this objective themselves by effectively launching altcoins with a full implementation, we will later show in section 3.6 that more recently developed protocols might achieve the desired outcome.

As a successful implementation, we shall mention the SegWit (segregated witness), a soft-fork which was implemented in Bitcoin in August 2017. The protocol modification tweaks another parameter which we have not explicitly mentioned this far: transaction dimension. In equation (3.2), it is evident that a decrease of the average transaction size could positively benefit the throughput. With SegWit, the total amount of space taken up by each transaction was reduced by relocating the signature from the input space to the end of the block in a segregated Merkle Tree structure, called the witness. With its implementation, block size was scaled up to 4MB as a result from freed up space in the blocks (which formally remain 1MB big), blockchain size was reduced by 60%, while also transaction malleability was prevented, as we will see in the security dedicated part (for reference, see under SegWit 2015).

3.2.3 Sharding protocols

Sharding protocols, as the name suggests, aim at splitting the workload nodes have to carry out by dividing them in subsets, thus achieving faster consensus and enhancing

throughput[28]. Luu et al. (2016) propose a sharding protocol for open blockchains called ELASTICO, whereby the network is partitioned in smaller committees, each of which processes a separate set of transactions, called *shards*. To guarantee security, the number of committees is scaled with the amount of computational power at disposal of the network, so that the number of nodes per committee is kept constant. To reach consensus within the committee and about the set of transactions to include in the block, a simple byzantine consensus protocol is used. Proof-of-work consensus is used instead to identify and set up committees based on their computational power. Results found by simulation confirm that this protocol is scalable since the number of nodes does not impact performance, and that computational power has a linear relationship with transactions throughput. According to the authors this would allow to reach a number of TPS that is 1000x that of the Bitcoin network.

However, performance achieved by ELASTICO come at the cost of leaving open security issues. As pointed out by Kokoris-Kogias et al. (2018), this protocol does not counter effectively failure probability under an adversary attack; it does not provide a bias-resistant proof-of-work selection, because miners can selectively discard the latter; it does not secure transaction atomicity, such that unvalidated shards will cause a permanent loss of funds; and finally, it forces nodes to store the state in full, as they keep changing the committee they belong to.

Gencer et al. (2017) propose Aspen, a higher-level sharding protocol to plug onto Bitcoin NG, which aims to further scale the protocol by splitting the state into services. Instead, other solutions such as OmniLedger (Kokoris-Kogias, 2018) bring in a horizontal scaling, still applying sharding, while providing better performances than other available solution without the cost of scale, decentralization, or security.

Even if we lack the technical skills to independently evaluate these newer proposals, we note that research is very active in this regard and results seems promising: many other protocols that we will not describe in detail (such as ByzCoin, by Danezis and Meiklejohn, 2016, or RSCoin, by Kokoris-Kogias et al., 2016) propose enhanced throughput and scalability leveraging sharding protocols, and relevant cryptocurrencies such as Ethereum are planning to implement newly released sharding protocols to achieve scalability[29].

3.2.4 Sidechains

Moving out of the protocol area, we shall now consider sidechains as a solution to throughput and scalability. Sidechains are separate blockchains attached to the main network

[28] https://medium.com/edchain/what-is-sharding-in-blockchain-8afd9ed4cff0
[29] https://cointelegraph.com/news/ethereum-to-combine-casper-and-sharding-upgrades

with which they communicate leveraging a two-way peg. From a practical standpoint, a user could send his token to a special address in the main network; the coins would then be locked and released on the sidechains[30]. Sidechains play a role in network scalability and throughput as they allow to process transactions in separate network, relieving some of the computational effort, storage, and traffic from the main network.

Pegged sidechains were firstly proposed by Back et al. (2014). The aim of the authors was to provide interoperability to the many protocols spreading in the blockchain environment, contributing to puzzlement and misunderstanding of the technology, while tricking investors. They compare this fragmentation to an internet where every website offers a different version of the TCP/IP protocol and forces users into it to browse the content. The solution mainly focuses on improving the interoperability of different chains, and, just as a consequence, can benefit scalability too. To allow interoperability, they suggest that funds from a chain (the parent chain, namely, Bitcoin) can be locked up, produce a cryptographic proof (simplified payment verification, SPV) that the lockup happened and finally communicate this proof onto the sidechain unlocking assets on it. In addition, the process contains two more periods: the *confirmation* and the *contest period*. In the confirmation period users locking up funds have to wait until sufficient proof-of-work has been produced in the parent chain so that the operation finality is completely secure; this is to prevent that attacks brought on the parent chain cannot have repercussions in sidechains too.

Then, the contest period follows: in this time frame, the user has to wait before he can spend the coins in the sidechain, because if the block containing the proof of funds' lockup ends up being in an involuntary fork that is abandoned (this event is a chain reorganization), altcoins generated could be double spent, once for each of the two blocks in different forks. Therefore, further wait time is requested until a proof that the block is finalized is available. This idea would allow a fixed correspondence between the parent chain coins and the sidechains' ones, as the value of all coins in the sidechain is determined by the amount of locked up coins in the parent chain. To speed up exchanges, as confirmation and contest period can take up to 2-4 days in total, Nolan (2013) proposed a faster way to exchange coins, which is similar to a Forex market trade, but carried out in a peer-to-peer fashion on the blockchain. The mechanism described is as follows: a user A willing to buy sidechain assets creates a transaction on the parent chain, which can only be reversed after e.g. 48 hours automatically, or by both parties' signatures. The same is done by his peer B willing to sell these assets. The transactions can be unlocked once a party know his counterparty signature. Therefore, when the sidechain assets are signed by B, A can unlock them with his signature; then, A's signature is revealed, and B can unlock the coins in the parent chain independently from A. Obviously,

[30] https://hackernoon.com/what-are-sidechains-1c45ea2daf3

this process can happen not only between parent chain and sidechains, but also between two different sidechains.

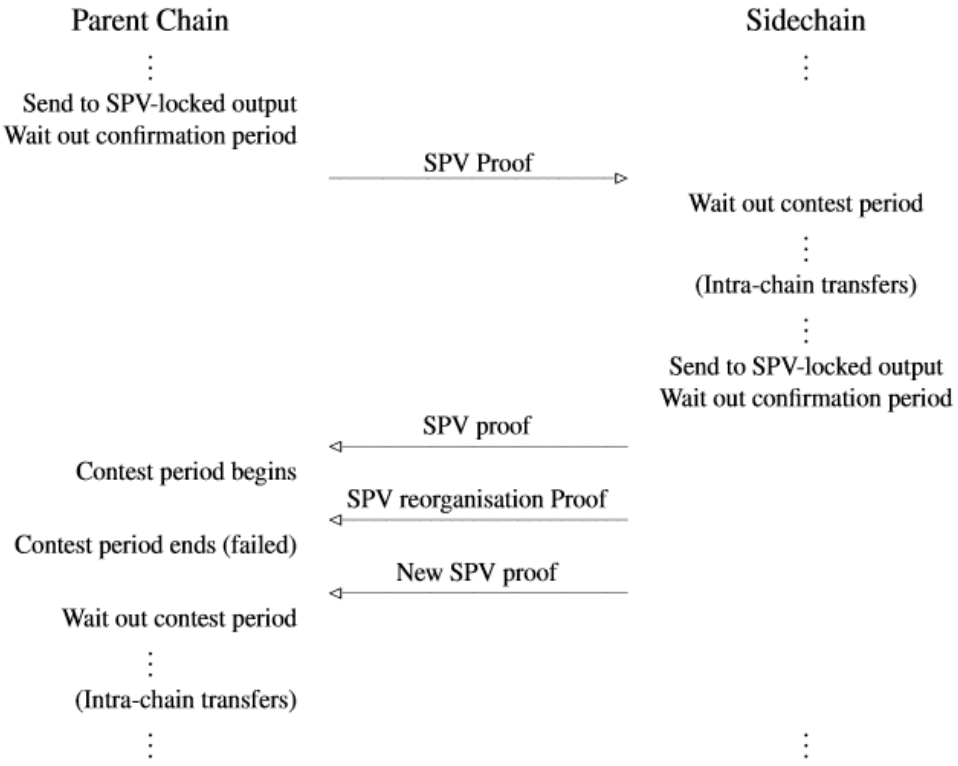


Figure 21, a view of funds moved between chains (from Back et al. 2014).

Finally, Back et al. (2014) highlight three open problems which should be addressed in sidechains research. The first is a necessary coordination between miners: they should distribute their computational power among the various chains according to the asset value of the main chain that they represent, otherwise, attacking disregarded chains could become too easy. Secondly, an excessive number of sidechains would totally destroy any desirable benefit in terms of throughput. In fact, if users needing to exchange value on chain use different sidechains and do not want different assets, they are forced to always transmit operations onto the parent chain, thus creating many duplicate transactions in the three different chains. At last, cross-chain transactions increase validation latencies, rendering a single-chain process optimal, if available.

Dilley et al. (2017) put to practice the pegged sidechain concept proposing the Strong Federation protocol. The latter operates as a complimentary protocol to the Bitcoin blockchain that creates sidechains able to transact assets in a trustless environment using a multi

signature cryptography. Asset movements in the side chain are faster thanks to the limited number of participants allowed to the federation, speeding up the transaction validation process. This also increases privacy of the users as anonymity is enhanced in the federated sidechain. Application of this protocol is put to work in the Liquid product offered by Blockstream which, among other things, enables inter-exchange transactions for cryptocurrencies exchange[31].

3.2.5 Off-chain solutions

Another research path explores off-chain transactions to take out most of the workload from the blockchain onto alternative networks that can provide better performances. The most popular example is constituted by the Lightning Network, an off-chain protocol that complements Bitcoin (or any other cryptocurrency enabling smart contracts) to allow much faster and instant confirmation transactions, making it a candidate especially in the payment use case. This protocol was first described by Poon and Dryja (2015): they suggested that two users open a bilateral transaction channel. This channel is opened off-chain but is secured on-chain by pledging a Bitcoin amount and locking it up for a certain amount of time, i.e. as long as the payment channel is opened. During this time, the two users involved can transact off-chain with one another as far as the amount transacted do not exceed the coins pledged on-chain. When the transactions are concluded or when the period is over, the beneficiary (i.e. the party who was paid) can upload the transaction on-chain and receive his payout. Off-chain transactions are secured by the payor signature and can get cashed out by the payee by signing them and transmitting them to the blockchain network. If both parties sign a new transaction, all past transactions are automatically invalidated so that only the last available transaction can be transmitted. So far, it could seem an unpractical solution, since it requires each user to create a channel, i.e. deposit and lock up his Bitcoins on chain for a certain amount of time, every time he wants to pay, for each person he wants to pay.

Actually, the Network tolerates 3-party payments, meaning that a party can pay a 3rd party who he has no open channel with, by passing through a common peer that has an open channel with both the 1st and 3rd party. To enforce security, the payment is carried out only upon the knowledge of a cryptographic hash, that has to be transmitted as a proof to the payee by the intermediary party. The process can be extended to n-party payments, where each party represents a node and bilateral open channels are leveraged to reach the final beneficiary of the payment. At the moment, the network is in Beta phase and is accessible as further developments and implementation steps are carried out. Nevertheless, it is not exempt from issues: a recent DDoS attack managed to take down roughly 1/5 of the active nodes, reducing

[31] https://www.blockstream.com/liquid/

their number from 870 to 1050 ; besides, many concerns are cast on payment finality as reportedly often payments fail, and users have to resort to the on-chain channel while invalidating off-chain transactions .

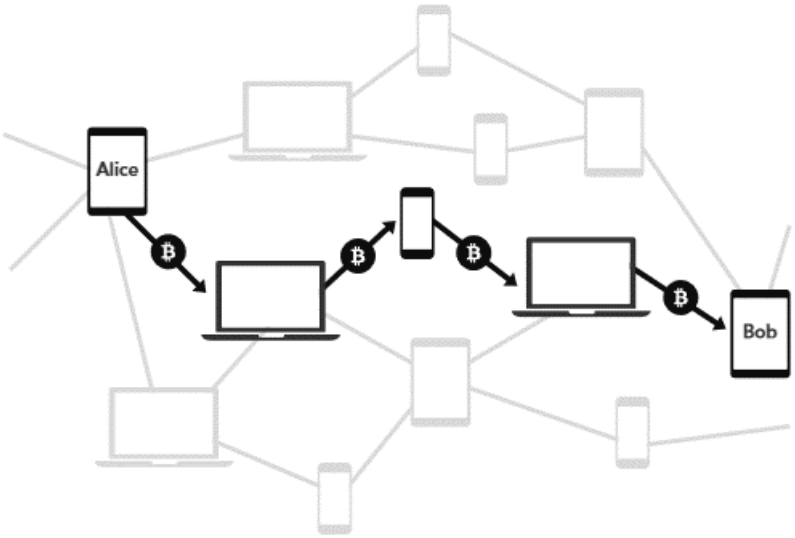


Figure 22, the transmission of a peer to peer payment through bilateral channels from Alice to Bob (from lightning.network/lightning-network-summary).

Off-chain solutions are still a promising field which could enable a competitive throughput, compared to traditional legacy systems, and it shall be closely monitored as the project advances in the implementation phase.

3.3 Security

Blockchain technology achieves higher level of securities compared to traditional centralized infrastructures thanks to its distributed architecture and its intrinsic resistance to DDoS attacks. Nevertheless, even blockchains are not exempt from attacks to itself or to its users. In this section, we shall review literature related to open security issues, proposed solutions and solved problems.

3.3.1 50%+1 attack

The most notorious attack cited even by Nakamoto in his paper (2008), is the 50%+1 attack. Every blockchain achieves consensus by somehow having validators vote on the correct status of the ledger. This vote is generally carried out proportionally to the hash rate at the validator's disposal, so that voting has a cost, i.e. the energy and hardware cost to perpetrate

the validation, remunerated by fees and newly minted native assets on the blockchain. Thus, the incentive scheme keeps validators on the honesty track. However, a malicious validator could attack the blockchain by voting on a version of the ledger that includes favorable transactions for himself, such as double spending transactions. This is possible if the attacker manages to obtain the majority of votes, that is, the majority of the hash rate.

Beikverdi and Song (2015) note that, despite the apparent difficulty in claiming the hash rate majority in such a big network, there are significant trends of centralization in Bitcoin and other cryptocurrencies in general. In fact, the hardships in the user interface with traditional clients and technical skills required to use them contributed to the surge of centralized cloud wallet services hosting users private key while providing better user interfaces, charging small fees on operations. On the other hand, the way Bitcoin mining works contributed to the formation of large mining pools: indeed, Bitcoin miners receive a reward in new coins and fees only if they are the first to solve the cryptographic problem associated with the proof-of-work. Instead, if they fail, they get nothing. This causes a great deviation in mines' returns, especially if they have little hash rate at disposal, since the successful solution to the problem is statistically more favorable as the hash rate increases. To stabilize returns, association of small miners rose, proposing to group all hardware as a single entity, and then distribute rewards based on the amount of hash rate each party brought in. This way, returns are smaller, as they are shared, but they are flowing in constantly. Therefore, the probabilistic incentive design in blockchains is favoring centralization of validators, making a 50%+1 attack a concrete threat. The authors also analyze this threat by calculating the average concentration in the mining industry, finding that the centralization of mining pool peaked in October 2014, reaching the 33% threshold. More recent studies, however, challenge this centralization threat. For instance, Cong et al. (2018) find that, despite initial increasing trends in centralization, mining industry mechanics brought to a mining pool diversification and the non-dominance of a single mining pool: over-time this trend seems to continue, hinting at concurrent economic forces which suppress excessive centralization.

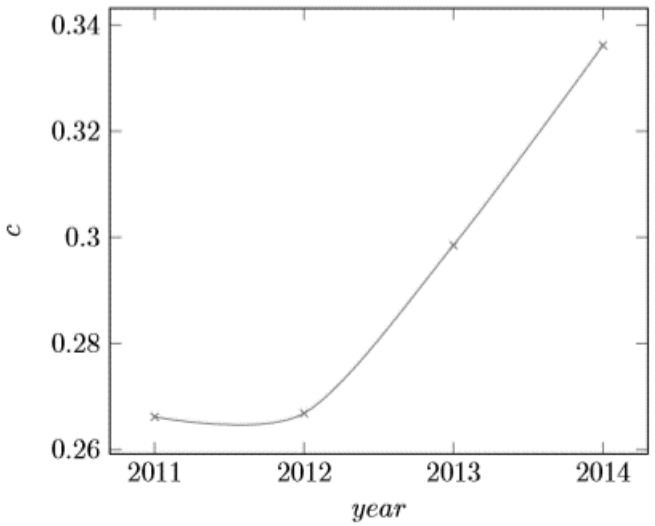


Figure 23, centralization trend in the mining industry (from Beikverdi and Song, 2014)

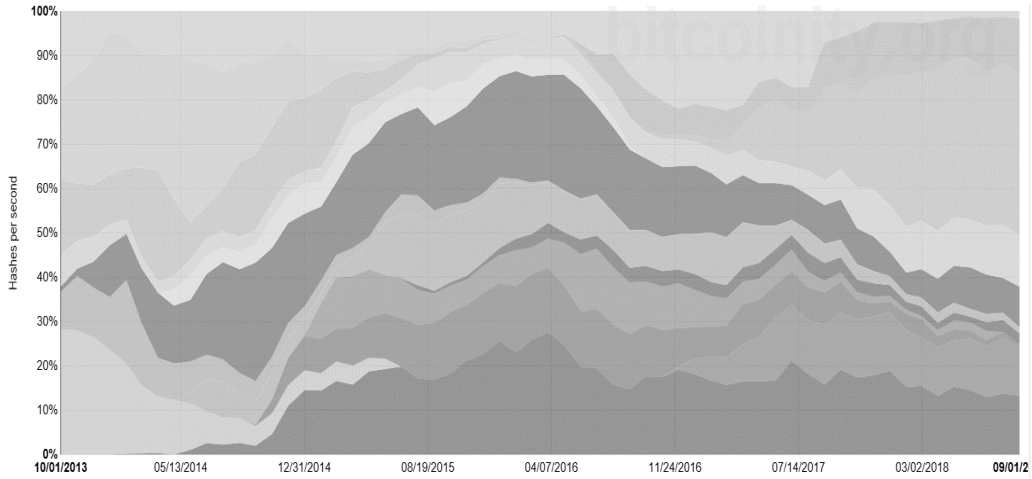


Figure 24, Bitcoin network hash rate percentage distribution in the last 5 years (from Bitcoinity).

Also, they confirm the presence of a strong economic and risk incentive for miners to join pools, but they also note that changing pools is just as easy as changing one parameter in the mining script. Actually, empirical results show that bigger mining pools typically charge higher fees to the mining community, while also showing a slower increase in the hash rate. Conversely, smaller pools tend to grow faster, probably due to newer hardware or smaller fees incentives, thus catching up bigger ones in term of hash rate. Empirical data available online also confirms both trends of the previous studies: until 2014 big mining pools were surging in hash rate, controlling a maximum of 35% of it; since then, competition from other pools lowered centralization. Nowadays, most of the hashing power is attributed to unknown entities (36,6% i.e. independent miners or independent mining organizations), and mining pools all stay below the 20% threshold, averting a 50%+1 attack.

Monitoring mining pools' concentration is central to Bitcoin and blockchain security in general. As documented by Eyal and Sirer (2014), a mining pool with sufficient hash rate could mine blocks and keep them private instead of broadcasting them to the network. This way, a fork would be created: until the adversary mining pool chain is longer than the honest miners' chain, it is kept secret. Just when the length of the honest chain is close to the adversary one, the latter is revealed, all mining incentive is collected by the malicious mining pool, and honest miners would end up wasting their resources as they mined a forked chain which will be reorganized and thus, abandoned. This attack, called selfish mining, can happen if the adversary mining pool controls the majority or is close to the majority of the hash rate. The authors find that selfish miners revenues increase super linearly with their size and are well above honest miners' one. Therefore, even honest miners are incentivized to join the selfish pool, creating a vicious cycle and a concentration of the hash rate well beyond majority. The authors also propose a back-ward compatible protocol improvements changing the way blocks

are propagated and reducing the probability of a selfish mining attack. However, no selfish mining attack has been carried out so far, probably due to the impossibility from selfish miners to construct an adversary chain faster than the honest mining pools: in fact, even with the highest percentage of hash rate achieved by a single mining pool (35%), building an adversary chain faster than the remaining 65% honest majority is probabilistically unlikely. Consequently, the risk of failing in the creation of an adversary chain that shall be longer than the honest one is a disincentive to carrying out a selfish mining attack, because failure would mean a waste of the hypothetical adversary pool resources and an opportunity cost in fees coming from the non-communication of the blocks kept private. Still, should a mining pool get close to the 50% threshold, this attack would become feasible.

Garay et al. (2015) further highlight problems related to the 51% implying that it would be possible even at lower percentages of hashing rate: indeed, Nakamoto supposed this threshold by raising the theoretical assumption that the network is perfectly synchronous. Yet, the adversarial bound starts to drop as the network desynchronizes. Network desynchronization could be achieved by an attacker trying to spoof messages between the nodes, forcing honest miners to waste their hash rate on alternative and obsolete version of the blockchain. The authors propose a protocol improvement that would improve messaging communication and enhance security of the network against this kind of less-than-50% attack.

Concluding the section, we observed that 50%+1 attack is a serious open threat public blockchain are prone to. In addition, researchers found that this threshold can even be reduced under certain circumstances, such as network desynchronization or the presence of a selfish mining pool. Yet, initial concerns in mining pools' centralization trends were averted by recent research and empirical data available online, witnessing to a crescent decentralization of the hash rate, together with authoritative models supposing an impossibility of excessive centralization due to the economic incentives design for the participant do mining pools and newer hardware production. This scenario could change if the blockchain were to be adopted by institutions: as a hypothetical scenario, western banks adopting a public proof-of-work blockchain are prone to attacks coming from adversary nations, interested in the destruction of the system rather than in an economic incentive. Still, the attack does not end upon reaching the 51% threshold, since such a small majority could only mine 7 more blocks a day to their adversary chain, probabilistically speaking. This hash rate majority has to be sustained while the two competing blockchain would actually fight each other with DDoS attacks and all kinds of open software bugs to control the majority (Antonopoulos, 2017).

3.3.2 Transaction malleability

In blockchains, transactions usually carry the signature of the author willing to transfer his coins to the output address; however, the authenticity of the signature itself is not proved, leaving a space open to the malleability attack, meaning that the signature is mauled by an attacker intercepting, altering, and rebroadcasting the transaction, so that the originator is tricked into thinking the transaction was not confirmed, while it actually happens with a delay. Contrarily to the majority attack, malleability attack is by far more relevant and has happened several times, where attackers targeted centralized exchanges and managed to steal thousands of dollar worth of Bitcoins, such as Mt. Gox exchange in 2014[32].

Decker and Wattenhofer (2014) define a malleability attack as an alternate version of a double spending attack: instead of being the sender of funds, the attacker is in this case the receiver. When the payor broadcasts the transaction to the network, the attacker seizes it, alters the signature without invalidating it and rebroadcasts the modified transaction to the network. Then, either one of the two transactions has a chance of being validated and included in a block. Should the mauled transaction be validated, the payor would not see a change in his account, thinking the transaction was not actually validated: in fact, the hash of the transaction would be changed as the different content of the signature would produce a totally different hash. So, the payor referencing to transactions' hashes to compute his account balance would be tricked into thinking no funds are actually moved, and he will then send another transaction. A successful malleability attacker manages to double the Bitcoins the victim sent him. The Bitcoin Core client is not susceptible to this attack as it references all validated transactions to compute account balances, rather than only the issued ones. Instead, possible victims could be centralized services that use a custom client computing account balances solely considering issued transactions' hashes, as was the case for Mt. Gox. The author detected a sharp increase in malleability attack after the announcement by Mt. Gox concerning the issue, with a total number of Bitcoins involved of roughly 302,000. As a solution, a more careful implementation in custom clients is advised, so that account balances are not computed just on signed transactions but on all transactions present in the ledger.

Further research is performed by Andrychowicz et al. (2015). The authors experimentally tested the difficulty in mauling a transaction, and the capabilities of major Bitcoin wallets to handle these mauled transactions. Their findings suggest that performing a malleability attack is easy, whereas, most centralized safekeeping services have weak implementations causing a mismanagement of similar transactions, if an attacker tries to exploit them. Furthermore, they suggest a simple method to prevent the mauling of a transaction: together with it, a

[32] https://www.investopedia.com/terms/m/mt-gox.asp

malleability-resilient refund transaction is created, so that in case of an attack funds are transferred back to the payor address. This method does not require modifications to the Bitcoin protocol but encumbers the blockchain with duplicate transactions to increase security.

Still, the malleability issue was solved by the implementation of the SegWit soft-fork. In this update, which we already discussed in the scalability section as it was improving space allocation inside each block, the dispatchment of signatures into the segregated witness, beside freeing up space, also render a malleability attack impossible. In fact, the signatures are no longer attached to the transaction, so that an attacker cannot modify them and rebroadcast the transaction a second time effectively (SegWit, 2017).

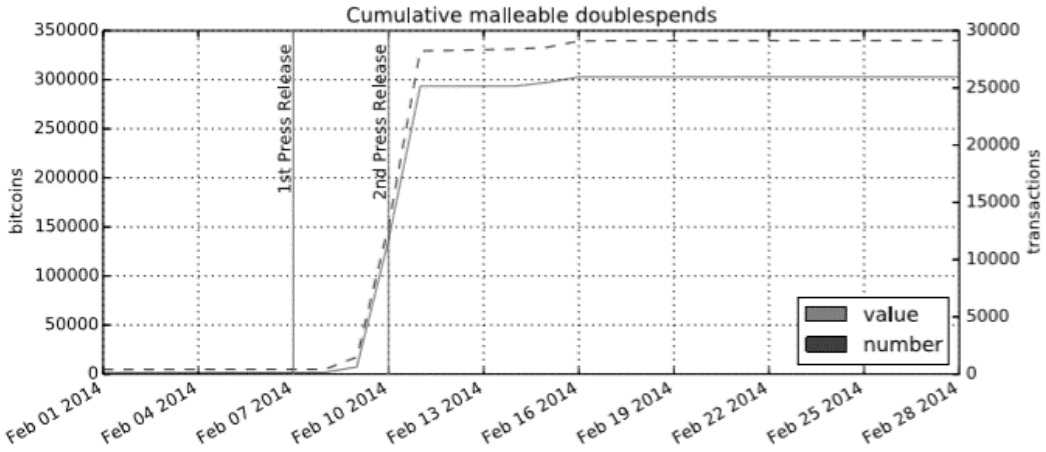


Figure 25, trends in the double-spends mauled transactions (from Decker and Wattenhofer, 2014).

In conclusion, the malleability attack posed a serious threat towards centralized services using custom clients, and it was responsible for great coin thefts happening in the past. Particularly, the exchange Mt. Gox was hit so hard by this attack that it was forced to file for bankruptcy. This attack was definitely solved in 2017 with the SegWit protocol update, putting it out of the list for blockchain security threats.

3.3.3 Authentication

In this section, we review the literature surrounding cryptographical attacks on users' key pairs, and the authentication factors required by centralized services which could be hacked with traditional techniques employed for centralized databases, not exposing the security of the blockchain infrastructure, rather that of the users. Then, also the aspect of regulated for institutional accounts authentication is considered.

Bos et al. (2014) assess the strength of Bitcoin signatures, generated with the ECDSA (Elliptic Curve Digital Signature Algorithm): when a user creates a new account, the protocol assigns to him a key pair which is used to sign transactions. Specifically, user A willing to pay user B must sign the transaction with his private key and refer to B's public key as target address. Then, B can unlock funds using his private key and verify the provenance of funds by checking that A's public key is matching the private that signed the transactions. The protocol can be used by anyone and it randomly generates keys, based on an integer (called nonce). The authors downloaded a set of transactions from the available blockchain data and found 15,291,112 unique public keys. They used this set as a reference while trying to detect users' private keys: to do that, they applied the ECDSA algorithm using either small integers, 256-bit scalars, and the set of scalars available in the Debian OpenSSL vulnerable keys[33]. The results were stored and compared with public keys, leading to a detection of 3 addresses. Then, the authors scanned the dataset looking for repeated ephemeral nonces which could enable an attacker in the computation of private keys. Indeed, the author found 158 addresses sharing ephemeral nonces and manage to compute the associated private keys. The aggregate value stored in these 161 accounts is of 0.00031 Bitcoins, their value is lower than the fees needed to "withdraw" them to another account. More interestingly, the authors found that 10 of these accounts were deprived of Bitcoins by a single account using, like the author, duplicated nonces for transactions. They found that this account might have stolen over 59 Bitcoins ($48,000 USD, at the moment of the attack). In conclusion, the ECDSA generation has flaws that could be leveraged to steal Bitcoins from unconscious users; no key custody service can stop this attack, as a perfect duplicate of the keys is generated and can be used to hijack funds. The only solution to this flaw in the key-generating algorithm would be to adopt a different or better secured algorithm, changing the Bitcoin protocol. Still, these attacks are extremely difficult to succeed, as the number of possible keys in the elliptic curve is huge: an attacker could be spending a lot of time in performing a blockchain analysis, generating random keys, with little to no reward, like it happened to the authors of the paper.

Another kind of attack that involves users' keys and is to some extent easier to carry out is the theft of keys. In fact, the only way users have to move and dispose of their Bitcoins is by means of their private keys. Consequently, a user storing keys by himself is fully responsible of his cryptoassets, meaning that losing the keys would cause a loss of the assets. Then, many users, especially the non-tech-savvy ones, prefer to resort to centralized services to store their keys, such as wallets. However, neither wallets are considered secure, especially if they have a one factor authentication: the theft of users' credentials, DDoS attacks, and data leaks can easily expose users' private key stored in a centralized manner, causing the partial or total loss

[33] A set of keys that was found to be vulnerable: https://wiki.debian.org/SSLkeys

of their accounts balance. Actually, the number of malwares and spywares was found to be increasing with Bitcoin popularity (Litke and Stewart, 2014).

Garavaglia (2018) classifies wallets as: hot wallets, if they let users access their funds from the internet, and cold wallets if their only function is to store keys in a secure way and they are thus offline (e.g. a piece of paper with a QR code representing the keys, a hardware with no internet connection etc.). Furthermore, wallets can be divided in custodial wallets, if it fully intermediates users in cryptoassets storage and transfers, guaranteeing the impossibility of key loss, and non-custodial wallets that let the users oversee their keys. This classification shall be useful when assessing the proposed solution as security enhancement.

Mann and Loebenberger (2015) propose a safer protocol for hot wallets. In fact, the authors notice that a thief aiming to steal Bitcoins just needs to get his hands on the wallet, like with physical money; in addition, as Bitcoin faces larger adoption, attackers will get more sophisticated, trying to replicate attacks similar to the ones carried out on the banking system. As a solution, they suggest that the wallet be storing private keys on two different pieces of hardware so that a hacker would have to control both in order to track back the original private key. To do so, a two-factor authentication could be introduced, similarly to the one used by banks nowadays, meaning that the wallet is in charge of the custody of just one piece of the private key, while the other share is stored independently on a different piece of hardware, like a smartphone. Then, transactions can only be signed if the payor has access to both pieces of hardware. Yet, the procedure to secure this two-factor authentication is not simple: attackers to online banking often infects the user's hardware with a trojan which modifies the victim's DNS resolver, so that the attacker becomes an intermediary between the end user and the bank. In the moment of the authentication, he can also trick the victim into installing a malicious app on his smartphone, so that also the second factor is neutralized. Therefore, to secure the second factor, the author propose that the desktop wallet produce a QR code which is then scanned by means of the smartphone; during this phase, the phone wallet verifies that the public key from the desktop certificate matches the public key in the QR code, thus preventing any malicious intermediary that infected the user's desktop. This wallet scheme is fully compatible with the Bitcoin protocol, indeed the authors managed to create a fully functioning prototype, solving possible security gaps in centralized wallets facing attacks.

Bamert et al. (2014) recognize the same problem in Bitcoin security, noting that bitcoins thefts have an increasing trend. Yet, they consider any device connected to the internet not secure for Bitcoin key storage, as it can always be reached by malwares and spywares, jeopardizing the safety of the funds. So, they propose an alternative solution: instead of using a two-factor authentication, they suggest that the keys be stored on a hardware token, named BlueWallet, which is able to communicate with internet-connected devices via Low Energy

Bluetooth signal. This way, the only risk is the theft of the physical device, no digital attack can be launched on the device: in fact, the device only serves as a mean to sign transactions on a connected desktop wallet client. Transactions details are reviewed on the BlueWallet hardware, and the user can evaluate them before inserting his secret PIN and authorize the transaction. Another interesting feature proposed is that the device can be used as an alternative to traditional credit cards or cash, since it can be used in conjunction with a point of sale device to sign Bitcoin payments. In conclusion, a cold wallet like that proposed by the authors can set to zero cybersecurity threats coming from malware and spyware sent by attackers to gain hold of victims' private keys. However, physical devices are open to a whole different series of attacks outside the digital world: theft of the device, losing the device and malfunctioning or breaking down of the device are all possibilities that can destroy the users' access to their Bitcoin account. A copy of the private key still needs to be conserved possibly in another identical or different type of cold wallet to ensure a secure access to funds.

In conclusion, there are three open problems with authentication. The first is with the ECDSA generating Bitcoin keys which may have open flaws; still, attacking Bitcoin at this level is very hard and can often result in a wasted effort for the attacker. A more concrete attack is represented by the theft of users' signatures, which cause a total loss of the funds connected to one's account; to solve this problem several keys custody solution have been proposed, but, especially in the case of cold wallets, it seems an old fashioned way to safekeep assets, whereas better positioned solutions are those leveraging a digital hardware, such as a smartphone, to solve the issue as in the current e-banking environment. In general, though, Bitcoin authentication problems seem to be more relevant than in traditional banking, as Bitcoin transactions, once carried out, can never be reverted, unlike credit cards or other banking operations.

3.3.4 Other attacks

In this section we will present those papers studying other attacks that can be brought onto blockchain users which are not strictly related with the technology itself, as they are present and possible in other IT areas, or attacks that area brought on accessory blockchain technologies. These attacks are mainly DDoS attacks on centralized services, scams targeting the final users, and finally attacks aimed at smart contracts.

Vasek et al. (2014) perform an empirical study about reported cases of DDoS attacks on Bitcoin centralized operators, inspecting Bitcoin-related forums between 2011 and 2013. They find that 142 attacks of such kind were reported, where the mostly common targeted services are currency exchanges, eWallets, financial operators, gambling operators, and mining pool with a hash rate share of at least 5%. The reason behind these attacks is mainly competition

within the industry: for instance, large mining pools are attacked by competing mining pools trying to facilitate the rip off of blocks' rewards; currency exchange can be attacked by brokers or large trading clients that try to benefit from artificially manipulated cryptocurrency prices; eWallets are attacked by other concurrent wallet services trying to put off their current customers. In conclusion, the authors find that centralized services are often prone to DDoS attacks, but they also notice that these services are often employing defense systems such as Amazon, Incapsula or CloudFlare, showing their awareness of the issue, especially, as this protection is found to be proportional to the amount of attacks that were brought on. Centralized services are not immune from attacks and they should take cybersecurity measures to protect themselves as their relevance grows.

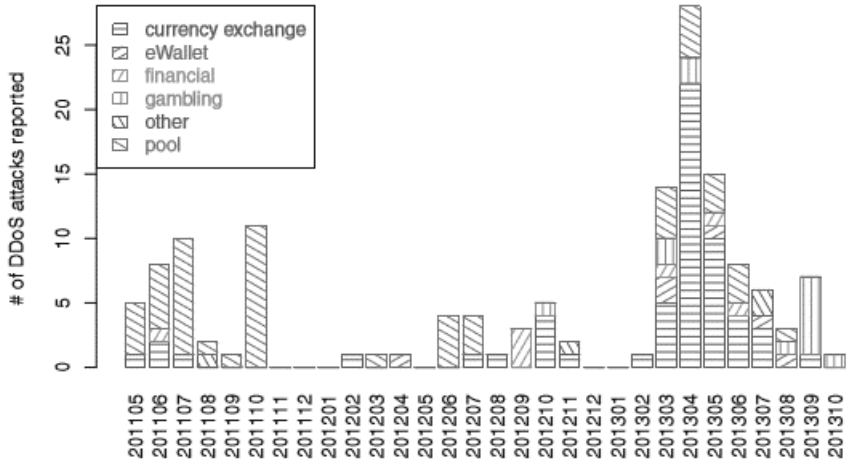


Figure 26, reported DDoS attacks and target platforms hit. The most relevant platform are exchanges in a peak of trade (from Vasek et al., 2014)

Lim et al. (2014) review all types of secondary attacks that can be carried out on blockchain users. The first documented attack they present is the distribution of malicious code to infect mining devices: these malwares are invisible to users as they reroute all mining incomes directed to them onto attackers' addresses without displaying anything to the victim. Other malwares attack can be brought on centralized services, such has happened to a Korean exchange that was infected by a trojan sabotaging security programs and allowing the attackers to hijack funds transferred by the exchange into their own wallets. Then, in line with the literature reviewed so far, they also find a consistent presence of DDoS attacks, especially on exchange with the aim of disrupting the continuity of the service. Ultimately, the authors conclude that blockchain ecosystems are open to attack to users, and the fact that a regulating authority is not present means that all precautions need to be taken by the users alone, and the responsibility for theft or losses is only on them.

Vasek and Moore (2015) perform an analysis of Bitcoin frauds and scams, finding that 13,000 victims have been stolen a dollar-equivalent amount of $11 million in Bitcoins. They classify Bitcoin scams into four categories: Ponzi schemes, mining scams, scam wallets, and fraudulent exchanges. Ponzi schemes are usually advertised as High Yields Investment Programs (HYIP), where victims are asked to deposit their funds that would be invested returning outstanding yields, up to 1-2% *daily* returns. Instead, money is not invested but distributed immediately as new subscribers of the program join in: the scheme keeps on running until the number of subscribers is growing, when growths settles, all funds are stolen by the scammers. In addition, the authors find that this kind of fraud goes unpunished, as was not the case for other centralized currency systems that were trialed in courts. Moving on, mining scams are those promising the delivery of a mining hardware against advanced payment, or the purchase of such hardware and the distribution of mining profits. Despite the business model of such investments is sustainable on paper, some turn out to be scams as no equipment is ever delivered nor are rewards from mining activity. The third type of fraud is scam wallets. This eWallets are operated by a malicious player that tricks users into thinking the wallet is normal and smoothly running. Actually, when funds are deposited a threshold check is carried out: if funds are under a certain threshold, they are correctly stored in the wallet and the user thinks it is correctly operated; if funds are above a certain threshold, they are moved to the owner's wallet and thus stolen. Finally, exchange scam exists: these are false exchanges that leverage very convenient exchange rates, low fees and credit, debit and PayPal funds acceptance to complete the purchase and attract more users. Yet, upon receiving the money, no cryptocurrency is delivered, and money is stolen. This study is useful to note that many malicious operators take advantage of naïve users and their possible misunderstanding of the technology or of the investment products offered. These trends are relevant as, in many countries, cryptocurrencies are not watched over by law, so that victims are often abandoned to themselves and cannot report the fact to the authorities. The positive aspects of blockchain is that scammers are unable to hide, and their operations are clearly recorded on the ledger: therefore, with similar researches, it is possible to expose scamming activity and help users gain a better expertise in detecting scams.

As we mentioned, we shall also consider in this sections attacks that are brought on scripts that can be written within the blockchain, typically known as smart contracts. Luu et al. (2015) test the securities of such scripts and the extent to which their execution can be enforced by the system. They find a problem they name *verifiers' dilemma* which occurs to miners in the case of long scripts requiring the employment of a large computational effort. Indeed, miners should execute scripts to validate them and add them to the blockchain, but the incentive they get from the validation might be inferior to the effort required to run the scripts, thus, from a game theory perspective, the optimal decision would be adding the scripts to a block without

verification. Only Turing-complete scripts are susceptible to this attack, in fact, Turing-completeness includes the possibility of introducing loops in the script, which, if not correctly programmed, can be never-ending, blocking hardware in charge of the computation. This is the case of cryptocurrencies such as Ethereum. To protect against computationally expensive scripts, gas is introduced, so that the user, who is interested in the script execution, has to pay a fee for the computational power needed. If the fee included in the script transaction is exhausted, the computation stops: it is the users who has to correctly compute the gas needed to attach to the script. Nevertheless, the authors find that an attack can still be carried out with no costs. If a miner correctly validates a block, he can also be including a non-verified transaction to it, and then propagate it to the rest of the community. Usually, if invalid transactions are included into a block, they are rejected by the other honest miners who will seek a new block with only verified transactions. In this case though, honest miners are unable to verify the transaction as it contains very expensive computations and they might just accept it without checking its correctness. On the other hand, the attacker is not incurring in any cost as the gas needed for the computation would be anyway given to him who is the miner of the block and entitled to gain the attached fees. The authors suggest that the incentive systems for Turing-complete scripts be redesigned to prevent this situation.

Luu et al. (2016) finds other securities issues in smart contracts, in particular in the presence of a bug in the script: a hacker could leverage that to hijack the execution into his favor. A very careful implementation is therefore needed, as funds attached to smart contracts are locked until the contract is executed, and the contract cannot be modified unless careful programming allows it before it is stored in the blockchain. The authors conclude that Ethereum semantics needs improving: out of 19,366 smart contracts analyzed on the blockchain, 8,833 are deemed vulnerable to bugs. Among these, the authors also detected the famous TheDAO bug, which led to a $150 million loss for parties involved.

Daian (2016) describes how a simple coding mistake, a bug in the contract programming, allowed a hacker to steal most of TheDAO funds. TheDAO was an Ethereum smart contract project, acronym for decentralized autonomous organization, that was aiming at giving users shares of participation in the project based on the amount of Ether they deposited, and then they were able to vote on investment TheDAO should spend these resources based on their contribution, in a sort of decentralized governance (Smith, 2018). However, the source code of the contract had a flaw in the fact that a function responsible for splits could cause recursion: so, by executing the split function over and over again *before* the reward was collected, would generate infinite rewards as the account balance would be updated only at the end of the function.

All in all, from the literature review about security, we find that blockchains are a very secure infrastructure. The problem arising in security have either been solved (like with the SegWit soft-fork) or are far from realization (as the 50%+1 attack). Yet, other attacks exist that are targeting the final users or centralized services operating around blockchain ecosystems. This kind of attacks are particularly frequent and lucrative as, in many countries, authorities have not issued any regulation to protect blockchain users against these kinds of thefts. Therefore, particular care to fend off these menaces is requested to users who are the sole responsible for their cryptoassets, for their correct safekeeping and usage. Further problems raise in the case of cryptocurrencies tolerating Turing-complete scripts, as any sum attached smart contracts written in the blockchain can be considered as an incentive for an attacker to find bugs in the code, making the usage of complex smart contracts in public blockchains very expensive.

3.3.5 Proof-of-stake security issues

In this subsection of the security analysis, we present open issues that concerns proof-of-stake only blockchains. In fact, if the issues presented so far are common to *any* kind of blockchain, there are further complications that come up if we consider proof-of-stake blockchains alone.

A first security concern is advanced by Houy (2014a) who analyzes the proof-of-stake consensus from a game theory perspective. He maintains that the PoS is conceptually flawed, in fact an attacker can easily obtain the 51% of the currency available just by controlling the credible threat to carry out an attack. If that happens, all users of the currency would immediately sell their assets to the attacker for a very low price, otherwise, in case of a malicious control of the blockchain, the cryptoassets would be worth zero. Therefore, game theory suggests that users selling their assets to a potential attacker for a very low price be an optimal decision, just because the credible threat of an attack would otherwise cause a zero payoff for them.

Yet, Tschorsch and Scheuermann (2016) oppose to this theory: the attacker would still have to buy the cryptoassets at a price which is more than zero, to gain nothing but the disruption of the currency value as a result, so of the money he ultimately owns. This concern for the attacker is a deterrent in the first place and provides safety to the users, as they no longer consider the attack a credible threat. The sale at minimal price of the cryptoassets is averted, and the attack is no longer possible.

Another critique to the security of proof-of-stake as a consensus system is put forward by Poelstra (2014): an attacker controlling a significant amount of stake could buy the keys that

were used at some earlier consensus history point. Consider that an attacker at early stages of the PoS cryptoassets signs to validate a block. At a later stage, he could corrupt the singers of that early block to reveal their keys, so that he has the possibility to fork the blockchain from there and attack the system with an alternative chain where he has full control. Yet, there is no real risk this happens as: forking at a previous point implies that the chain provided by the attacker is shorter than the real chain as blocks are added with a fixed time frequency, and, most importantly, no attackers would have incentives to do so as the annihilation of the cryptocurrency value would bring no benefit to him.

More concrete attacks that we should take into consideration are listed by Siim (2015). The author points out two main attacks that can be carried out in a proof-of-stake environment: the grinding attack and the nothing-at-stake attack. In the former, the validator can try to bias the election mechanism typical of a PoS protocol in his favor, to be elected with higher probability compared to his peers. It can be carried out either by grinding the validation parameters until the attacker finds ones that can get him elected more often, or, in some protocols, by producing signatures in the current block (where the validator has already been elected) until he has the certainty that his signatures are chosen again in the next block, so that he has the absolute certainty to always be in charge of the validation and is in control of the system forever. This problem can be easily solved by requesting validators to deposit their stake well in advance and not using information that can be manipulated as a source data for randomness[34]. The second attack, nothing-at-stake, is harder to solve. Since there are no resources that need to be spent to mine new blocks, when a fork occurs, all miners are incentivized in mining on all versions of the history, as they have no economic disincentive in doing so. If this happens, an infinite number of forks will be produced with all miners that simultaneously work on all of them, generating confusion on the real history of transactions, and fragmenting the value of the chain, as each fork is considered valid, facilitating a 50%+1 attack.

This latter attack still struggles to find a solution in most implementations. Bentov et al. (2017) suggested that proof-of-misbehavior be introduced to penalize miners trying to validate with their signature two different conflicting block headers by deducting their pledged stake. This approach though has open issues, such as the risk that validators, by pledging their stake in advance, could try to collude among themselves. Also, it requires nodes to be frequently online to get a secure view of the correct chain.

We presented this section to highlight that proof-of-stake blockchains have reduced security compared to proof-of-work ones, so, security at trade-off with other factors when

[34] https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs#how-does-validator-selection-work-and-what-is-stake-grinding

considering the implementation. However, we will show in the wasted resources section that newly proposed proof-of-stake protocols can effectively deal with these open issues, possibly solving most of the existing problems for PoS protocols.

3.4 Usability, versioning and forks

In this section, we group three issues loosely connected with one another. By usability, Swan (2015) refers to the hardships which users have to deal with when trying to use blockchain applications and clients. So far, we already discussed the fact that most users prefer using centralized wallets rather than the original Bitcoin client, Bitcoind. Indeed, original application are poor in graphics and sometimes counterintuitive. Nevertheless, companies like Circle and other FinTech are developing user friendly applications, so that most passages requested for the use of a blockchain are automatic; for instance, in many centralized wallets applications there is no need to write the full 16-character alphanumeric address of the recipient, but the target of the transaction can be specified by other means (such as the email address). In general, also from our empirical experience, purchasing cryptocurrencies is generally hard, it requires opening an account at an exchange completing all the KYC procedures requested, then, they could be used straight from the exchange if it also provides a wallet service, or they must be moved in a wallet copy/pasting the 16-character address. Finally, if one would like to use them in dAPPs online (such as Cryptokitties[35]) a browser extension is needed to allow communication between the browser and the user's blockchain address.

In this regard, Eskandari et al. (2015) highlight how it can be complex for a non-technical user keeping track of his private keys. In fact, every time a Bitcoin transaction is completed, the unspent transaction output (usually referenced as UTXO) cannot return in the same Bitcoin address starting the transaction. That is, when a payment in bitcoins is carried out, it either uses all the available funds in the starting account, or any unspent spare coins are sent to a new account whose private key is communicated to the payor; a new account is generated by default from the protocol to enhance users' privacy as we mentioned in the privacy section. Consequently, users have to face the complex management of multiple private keys associated to multiple accounts. We saw in section 3.3.3 the different approaches to give users a friendly key storage solution. Anyway, according to the authors, the preferred choice for users remain centralized services, as cold wallets, despite safer, represent a trade-off with usability as multiple keys got to be brought offline and physically stored, which, for small transactions, represent a serious nuisance for usability.

[35] https://www.cryptokitties.co/

Another usability issue is the one concerning smart contracts. Actually, according to the Smart Contract Alliance (2018) there are several jurisdictional problems when two entities subscribe a smart contract, aiming to give it legal validity. Firstly, there must be a clear definition in the programming code about the jurisdiction of reference: many nations do not share common requirements on legally binding elements for a contract, making it hard for cross border smart contracts to work properly. Secondly, a clear reference to identities is needed, so that signatures can be considered valid. Also, in no jurisdiction a contract can be accepted with reference to unknown entities such as anonymous alphanumeric addresses. To solve the latter problem, we remind the suggestion in section 3.3.3 about institutionally issued addresses: in this way, entities would be univocally identified. Other problems arise in case modifications have to be made. All contracts are legally binding but can undergo modifications under certain circumstances which are specified in the contract itself. Smart contracts cannot be freely modified as they are stored in a blockchain, thus, a set of rules needs to be included to ensure future modification before the contract is uploaded. Finally, smart contracts need to be understood by both parties to be enforceable. This last point is particularly hard to accomplish when a smart contract is signed between a business and a consumer (B2C). Indeed, between two businesses both can form expert technicians able to understand the implication of the contract they are supposed to sign. Instead, in a B2C context, most of the people cannot understand the programming language smart contracts are written in, and an annex written in discursive language cannot be provided as the one to one relationship between the two contracts cannot be guaranteed. Therefore, usability strongly hinders the adoption of legally binding smart contracts: implementation has to happen in the company back-end systems, so that front-end users are not exposed to the contract. Still, the company is fully responsible for the smart contract correct functioning and assumes all the associated risks in case of malfunctions, explained in section 3.3.4.

In terms of versioning, Swan (2015) means the issue of cross-chain communication. In fact, often a common chain is split for administrative purposes and new chains keep sprouting in the forms of altcoins or private-permissioned applications. We have already showed studies solving this problem in section 3.2.4 concerning sidechains. Pegged sidechains could definitively solve the issue by introducing the chance of cross-chain communication. So, the resolution lies in newly developed and functioning sidechain protocols.

Forks, instead, are an issue for two reasons. Antonopoulos (2014) describes two kinds of existing forks and that each creates a problem for blockchain adoption at scale.

1. Involuntary forks that happen when two miners solve the PoW at a small-time distance from one another, generating two blocks with different block headers. Due to network latency, some of the nodes receive one of the blocks, some the

other. In this scenario, two blockchains are formed which are identical up until the point where the two competing blocks are.

2. Voluntary forks happen every time a protocol update is done. Reasons to update the protocol can be relevant to the issues we are describing in this chapter, to bugs or unwanted situations originating in the blockchain normal operation. They are further divided in two:
    a. Soft-forks are protocol updates ensuring reverse compatibility on previous blockchain history and does not actually bring to a fork of the chain. This is because new software can process both new and old transactions, incentivizing miners and the community in general in the adoption of the newer protocol so as to avoid losing shares and fees from transactions carried out with it.
    b. Hard-forks are protocol updates that cannot ensure reverse-compatibility with the history in previous blocks. Consequently, a fork is inevitable, and one chain will have the new protocol, while the other chain will keep the older protocol.

The issue with voluntary fork is partially solved in the Bitcoin protocol (Nakamoto, 2008), by the introduction of the rule that forces miner to compute on the locally longer existing chain. So, the chains remain split and so do the miners: some of them works on a version, some on the other. This situation goes on until one miner group outperforms the other, creating a new block faster. In this case, all nodes and miners will discard their obsolete shorter version of the chain and work on the new longer one. This resolution though has a dramatic impact on transactions' finality: a transaction can be included by a miner in a block and will result finalized if that block is attached to the chain. However, as we just explained, the version of the blockchain with such block can be discarded in case it is a shorter fork, invalidating the transaction. The transaction is not deleted and will be added in the next blocks by miners as the fork is resolved. However, this means that transactions in blockchains might not achieve finality for more than 10-20 minutes. Yet, these events are quite rare thanks to the long block time chosen in the Bitcoin blockchain. The trade-off with scalability is evident: more frequent blocks increase forks and hinder finality; slower blocks ensure finality but reduce the number of TPS the blockchain can process (Antonopoulos, 2014).

Decker and Wattenhofer (2013) show empirically that involuntary forks are quite rare events in the Bitcoin blockchain. They show that the probability distribution of a block creation is a Poisson process, since the block creation is an expected event occurring every 600 seconds on average. Then, plotting the histogram of the minted blocks against the time passed from the previous block gives an exponential distribution. Beside protocol values for block discovery, the other factor influencing forks is the speed of propagation in the network: the

faster messages are delivered between node, the faster can miners align and work on new blocks. Putting together the two, the authors find that the probability of a fork in Bitcoin is of 1.78% roughly. The first evident result is that the probability of two consecutive forks is extremely low; the second, that faster message propagation in the network can reduce forks.

Protocol improvements were presented in section 3.2.2, such as GHOST, the Bitcoin NG protocol, or the simplified and faster messaging presented by Decker and Wattenhofer (2013) themselves as partially answering the issue. In the next section we shall see other better functioning and more recent protocols that, among other things, completely solve the problem.

As for voluntary forks, they cause issues in terms of security. Upon splitting the chain into two, a user will have currencies duplicated on both chains. At this point, he might want to spend his currencies only on one of the two, while saving the others. To do that, he needs to sign transactions with his key in the version of the ledger he likes the most. An attacker could then launch a replay attack, coping the signatures of transactions also on the other ledger, so that he can dispose of the user's coins on the other ledger. To fend off replay attacks, forks need to be carried out in a cautious way, including defensive measures in their protocols, such as putting an identifier on transactions of either one of the two chains, so that the other rejects identical transactions. Therefore, frequent hard forks undermine users' security (Song, 2017).

Notorious hard forks happened in most cryptocurrencies, usually as a means to keep the old protocol rules by the community that is unhappy with new ones, or to introduce new rules the majority of the community is not aligned about. The HowToToken Team (2018) provides a list of Bitcoin hard forks, showing that most initiatives finding little consensus in the community end up being driven out of the market by the small interest coming from investors. For instance, Bitcoin XT and Bitcoin Classic are traded at a close to zero price. More recent forks such as Bitcoin Cash (traded at 420$ per coin), that was created by a series of users' that were opposing to the implementation of the SegWit protocol change, are still enjoying success but prices graph show a slow but steady decrease as time passes, just as it happened with XT and Classic. So, it emerges that, beside representing a threat to security, hard forks are also destroying token-holders' value.

3.5 Wasted resources

Swan (2015) refers to this problem of wasted resources as connected to the computational effort requested to miners. As seen, proof-of-work requests miners to solve an arbitrary difficult puzzle to attach a block and claim their reward; the more computational power miners' have at their disposal, the more the likelihood that they find the solution. Mining hardware drain electrical power which in 2015 had an estimated cost of around $15 million,

more recent sources count a 73.12 TWh yearly average, with a cost of $3.6 billion[36], the yearly equivalent of a small country energy consumption[37]. Also, all the computational effort carried out is practically useless beside guaranteeing trust on-chain.

Cong et al. (2018) not only agree with the energy issue in proof-of-work but also stress that the incentive mechanism itself forces miners into a vicious cycle where more and more computational power is bought. In fact, they maintain that mining companies aim at profit maximization, like any other. To achieve it, they need do obtain more computational power than their competitors, which can be done by increasing the amount of hardware, so the quantity, or by buying more sophisticated hardware, thus the quality. Better devices provide miners with a higher hash rate, increasing their chances to mine a block and get their reward. However, the hash rate of a device is directly proportional to its power consumption: miners are theoretically incentivized in increasing their hash rate to mine more blocks than competitors, but, by doing so, they also keep increasing the resources wasted and the costs of the proof-of-work which are matched by high fees on transactions. Their hypothesis is supported by empirical evidence: as shown in Figure 27, in the last 2 years the hashes per second the Bitcoin network was able to compute increased drastically; a similar trend exists for the energy consumption[38].

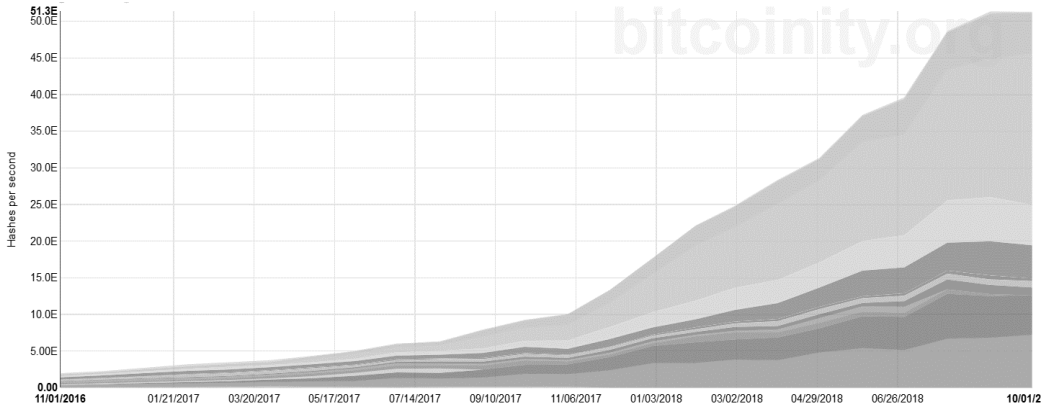


Figure 27, Bitcoin network hash rate increase in the last 2 years (from Bitcoinity.org)

To solve the open issue with energy consumption, we detected 5 different approaches in the literature. Some papers propose better incentive schemes and new economic models for miners, so that the vicious cycle can be interrupted (Wang and Liu, 2015); some suggest simple and environmentally friendly modifications to the Bitcoin protocols (Paul et al., 2014); others advances hypothesis of new cryptocurrencies employing the hashes required in a smarter way

[36] https://digiconomist.net/bitcoin-energy-consumption
[37] https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#6c8d298a1bc8
[38] https://digiconomist.net/bitcoin-energy-consumption

(King, 2013); a few papers find methods to increase the performance of mining hardware in terms of energy efficiency, flattening the line of proportional relationship with the provided hash power (Anish, 2014; Barkatullah, 2015); finally, proof-of-stake is proposed as an environmentally friendly upgrade to proof-of-work (Salch, 2018).

Wang and Liu (2015) note that the race towards a higher hash rate is limited by the deflationary nature of the Bitcoin protocol, which decreases the number of newly minted bitcoins assigned to the block validator by half every set years, thus, according to the authors, miners will increase their computational power up until the reward will be worth the cost, then they have to start reducing it or some of them will be driven out of the market. Conversely, Cong et al. (2018) instead maintained that this would not happen as fees would instead increase. Then, they also develop a model examining the best place for miners to obtain economic efficiency from their hardware: they consider mining pools as the best options, whereas in some countries, such as Italy, the high costs of energy cannot give a positive reward.

Paul et al. (2014) propose a modified version of the proof-of-work algorithm: instead of awarding the first miner finding the right nonce for the requested difficulty, which on average takes 10 minutes, miners are asked to compute the block header for only 2 minutes, and the miner finding the header with the most zeros is awarded. So, it is not a race towards the difficulty set by the protocol, but a timed lap rewarding the best performing (or luckiest) miner. The authors assume that this can regularize the speed at which blocks are produced, and, most importantly, reduce the energy consumption by roughly one fifth, as the time spent on hashing is exactly one fifth of the current time (from 10 to 2 minutes).

King (2013) suggests that proof-of-work hashing be substituted with useful computation rather than random ones: from his perspective, the hash rate miners are capable of can become a positive externality, for instance, towards the scientific community. In his modified version of the proof-of-work protocol, miners are asked to compute prime numbers' chains, known as Cunningham chains or bi-twin chains. This way, instead of computing random hashes for the sole purpose of matching the required difficulty and validating the chain, King shows that also useful work can be done by looking for more prime numbers and help out researchers from the field of numbers theory. Similar systems can be designed as long as the proof-of-work function solution is not repeatable, so that at each new block miners start back at the same point.

Anish (2014) analyses the performances of GPUs and CPUs in both illegal and legal mining, in both single and pooled machines. He finds that the main reason for the sharp boost in hash rate is mainly due to the high-performance machines employed in mining pools as opposed to the normal devices available to common users, such as pcs. One among the first of such devices coming on the market was Goldstrike 1 (proposed in a paper by Barkatullah et al,

2014); these devices outperform common ones by far, not only in the hash power, but also in the efficient usage of energy. In fact, a liquid cooling system and a better architecture allow for a faster dissipation of power.

At last, as Saleh (2018) suggests, the most effective way to avoid the waste of resources on a proof-of-work is probably not doing a proof-of-work. As we described, alternatives exist to reach agreement upon the verified blocks: the proof-of-stake. In proof-of-stake, no computation is carried out as verifiers mine new blocks just by locking up some of their coins. The issue with PoS protocols is related to security, as we have seen, regarding the nothing at stake attack. The author shows with an economic model that the nothing at stake attack is not possible by introducing bounds to the users who can perform the proof-of-stake validation. By so doing, he finds that the larger the reward given, the smaller the bounds to the users' stake eligible for the validation. So, he considers proof of stake a viable consensus mechanism under an economical perspective, provided the incentive scheme designed is complaint with his findings. Indeed, King and Nadal (2012) proposed a mixed PoW/PoS protocol, where validators are chosen not depending on the hashing power they dispose of, but also considering their coin age, that is, how long they have had their coins for. The result is an environmentally friendly cryptocurrency, called Peercoin. The proof-of-work is proposed just in the early stages of the currency to provide the security needed to start the chain (as at first most people have very little coin age). In the long run, coin minting will stop and will be completely overtaken by the PoS protocol based on coin age. However, the authors do not respond effectively to the issues of nothing at stake attacks, leaving an open threat to the currency. Similar proposals of PoS blockchains have been analyzed by Bentov et al. (2014) who mathematically showed that security premises of such early proof-of-stake protocol deployments are far from the PoW ones, concluding that none as of 2014 can compete.

To conclude this section, we showed that proof-of-work blockchains are very resource intensive, and the competitive setting in which incentives are distributed constantly drives up resource consumption, costs for the validation and fees, in a model that seems very far from sustainability and long-term adoption. Weak solutions to this problem are identified by the literature in new energy-efficient devices, soft modifications to the protocol, or new ways to employ the computing power externality generated by miners. Stronger solutions include modifications to the incentive mechanisms in PoW blockchains to discourage the hash race, and the development of secure PoS blockchains. In the next section, we shall present newly designed PoS protocols that seem to successfully solve most of the open security issues for the kind of validation.

3.6 New PoS protocols

So far, we reviewed the main issues and research directions in proof-of-work protocols, such as the one employed by Bitcoin, Ethereum and most other public blockchains, since it is the only one that is credibly secure, as opposed to proof-of-stake protocols which have issues especially in the case of forks. Yet, a number of new proof-of-stake protocols have been proposed and is on constant improvement in recent years (2017-2018). These protocols are effectively managing to deal with the security challenges posed by the PoS, while solving PoW issues in limited scalability, wasted resources and involuntary forks. In this section, we shall review the most discussed in the scientific community: Ouroboros (Kiayias et al., 2017) and its upgrades in Ouroboros Praos (David et al., 2017) and Ouroboros Genesis (Badertscher et al. 2018); Algorand (Gilad et al., 2017); Snow White (Daian et al., 2016); and FruitChains (Pass and Shi, 2017).

Starting from Ouroboros (Kiayas et al., 2017), a typical proof-of-stake protocol is implemented, where at each validation a new stakeholder is elected based on the available stake that he locks up. The innovation lays in the way security problems such as the grinding attack and the nothing-at-stake attack are stopped. Firstly, the grinding attack is not possible as the randomness of the selection is ensured and secured by a multiparty coin-flipping protocol, as opposed to previously proposed selection methods that were either deterministic or used a collective flipping, thus not effectively averting grinding attacks. The timeline is divided in fixed snapshots of stakeholders called epochs. Secondly, the nothing-at-stake attack is avoided by using a combinatorial notion of *forkable strings*, the authors perform an analysis which prevents adversaries from the validation of multiple chains in case of forks, preventing such attacks. Finally, a novel incentive system is proposed such that participants following the protocol rules is an approximate Nash equilibrium, also preventing attacks such as block withholding and selfish mining. In conclusion, the authors mathematically prove the security of their blockchain protocol, noting that according to experimental tests conducted it could support up to 257 TPS, 20x the performances of Bitcoin. In further studies, the protocol was improved: Ouroboros Praos (David et al., 2017) even tolerates an adversary corrupting a dynamical set of stakeholders, as long as there is an honest majority, and adversaries controlling message delivery and artificially creating delays; Ouroboros Genesis (Badertscher et al., 2018), besides including the modifications of Praos, also considers the dynamic availability of the network, that is, what happens when a new party joins in. In previous Ouroboros implementations, as well as in Snow White, newly joining party have to take the protocol from other participants as trusted and suppose that it is being passed on by an honest node; instead, Algorand requires explicit knowledge of an estimated offline parties' number. In Genesis, a new chain selection rule allows parties to always bootstrap the protocol from the

genesis block, ensuring its authenticity. The Ouroboros protocol is currently adopted by Cardano, 8th cryptocurrency in market capitalization.

Algorand (Gilad et al. 2017) instead proposes a new model for Byzantine Agreement with the interesting properties that: new players can be selected at any time to substitute old ones, without affecting the time to reach consensus; it ends in agreement after a loop with at most 3 recursions. So, Algorand have users participate in a random lottery, safe from grinding attack, as the only parameter influencing results is users' stakes, the larger they are, the higher the chances to be elected. The protocol selects 1000 (for scalability purposes) winning users who have to reach agreement on the block proposed by a selected validator. Provided 2/3 of the money belongs to honest users, Algorand can ensure consensus is reached and the majority of the users is honest. According to the mathematical model developed by the authors, the probability that Algorand blockchain forks or that it is overtaken by dishonest nodes in the lottery election process happens with probability lower than 10^{-18}, that is less than one on a thousand trillion. Therefore, Algorand not only secures a fast PoS protocol, but it also ensures that payment finality is present, preventing any kind of involuntary fork in the blockchain. From a scalability point of view, the number of nodes taking part to the network is not influencing the speed of the consensus as always 1000 validators are selected, then, it just influences the probability of becoming a validator. Currently, Algorand is under a marketing promotion and will become a cryptocurrency during next year.

Finally, Snow White (Daian et al., 2016) is another secure protocol studied to ensure securities in a proof-of-stake environment, particularly taking into account the issues of: sporadic participation, that is, the elected leader might not show up or be online at the time of validation; posterior corruption, influencing the elected leader after they voted for blocks, with the aim of creating a fork of the chain where they have full control of the election process; developing a novel formal approach to evaluate mathematically the security assumptions of their model to ensure its robustness. To our knowledge, Snow White is not part of a cryptocurrency project, nor is it employed by existing currencies.

In this section, we showed that despite the many open issues of PoW and PoS protocols, newly modelled proof-of-stake protocols are being developed (or are already partially deployed in cryptocurrencies on the market) that solve most of them. Problems may still be present in cross-chain communications and including metadata in transactions in a privacy-respectful manner, but here, too, research is under way to selectively disclose sensitive data to certain authorities. Break-throughs could come in the next 1-2 years when these protocols will be fully operational in cryptocurrencies, possibly opening the path to public blockchains adoption.

3.7 Consortium blockchains

In this section, we will describe consortium blockchains: private and permissioned systems that are offered to companies and financial institutions willing to cooperate in their industries to leverage some of the benefits of blockchain technologies. So, the main differences in these kinds of blockchain protocols is that they are private and installed on proprietary servers, owned by the companies involved, constituting the nodes of the network. The most notorious applications are Corda, engineered by the R3 consortium, Hyperledger Fabric, offered by the Linux foundation, Quorum, an adaptation of the Ethereum protocol by JPMorgan, and Ethereum private implementations, as the Ethereum protocol is open-source, it can be freely downloaded and adapted to run in private and permissioned environments.

To get a better grasp on private blockchain functions, we analyzed the Corda protocol as presented by Brown et al. (2016). The features of the ledger are very similar to those of Ethereum: it is possible to represent a state through a contract. The main difference is that this contract cannot send or receive messages or have any kind of autonomous interaction, it only serves to store information and can be referenced in transactions. The contract contains metadata and transactions contain clear references of the entities involved, so that compliance with institutional needs is guaranteed.

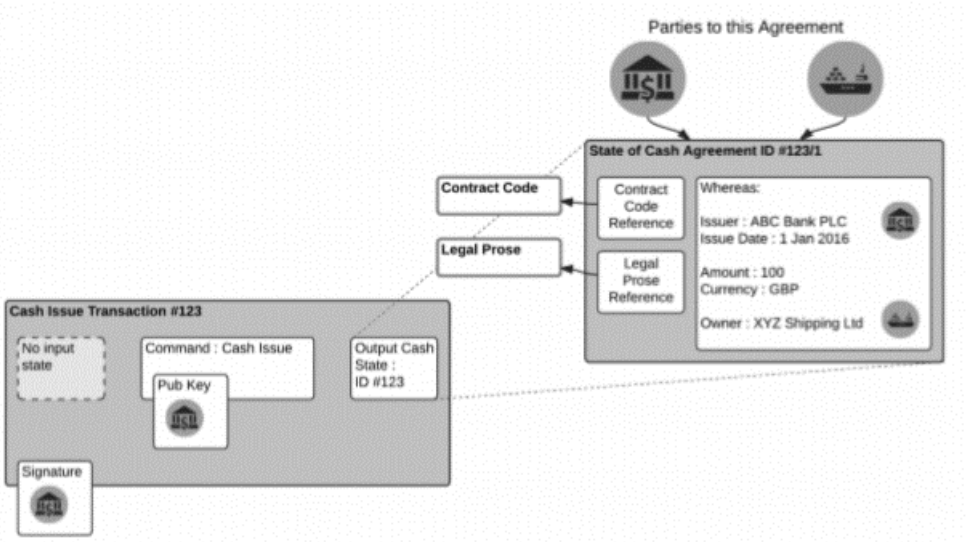


Figure 28, A transaction of cash issuance and the referenced contract originated by it (from Brown et al., 2016).

In Figure 28, a cash issuance transaction from a bank toward a shipping company is exemplified. The transaction generates the contracts which is referenced in it. The contract carries all the relevant information regarding parties involved, the amounts, the currency, the

issue date, the reference to the contract code, and most importantly to the legal prose accompanying the code. In fact, to rapidly resolve disputes, Corda allows to attach a legal prose to contracts, so that the validity of the contract can be easily ascertained in a court. Besides, Corda does not force participants (nodes) to have a full copy of all available information; instead, to protect privacy, only some of the information are put on the ledger, depending on the institutions' need to share them. Also, privacy is protected by zero-knowledge proofs, so, even transactions and data being shared cannot be decrypted by participants that are not involved in the transactions, while they can still verify its validity. Besides, the paper by Ateniese et al. (2014) is put to practice in Corda: a doorman, chosen by the network governance, is put as a chief of the identity issuance, granting keys to participants such that they are unambiguously identifiable. From a technical perspective then, the system is described in depth by Hearn (2016). The main features differencing the system from a public blockchain are two. First, it is not a blockchain, indeed, transactions are not batched in blocks, but they are processed on a one-to-one basis by notaries (who are the Corda-equivalent for miners): this is possible because no proof-of-work or stake are necessary to reach consensus. This leads us to the second features, that is the presence of notary nodes. One or more participants are elected upon the launch of the network as notaries, with the role of verifying (that is, preventing double spending), ordering and timestamping the transactions received. This is possible if the network is implemented in environments where a certain degree of trust exists among participants, such as banks of the European Union. In areas where trust is less robust, a BFT agreement might be introduced. So, notaries guarantee maximum speed in transaction processing, whereas BFT can provide more reliability in context with little trust, in trade-off with throughput. From the analysis of the Corda protocol for distributed ledgers, we noted that almost all of the problems concerning public blockchains have been solved: anonymity is guaranteed, still embedding all necessary KYC data in transactions; scalability is achieved by using a notary system; forks are not happening as there is no blockchain at all, usability is constantly updated and IT functions of participant banks are trained by the R3 consortium; no resources are wasted as the notary system or the BFT agreements prevent the need of a PoW. The only issue which is still open has to do with security: security is not guaranteed by the system, rather by its operators who are in charge of its cyber resilience; still, in case of data breaches, attackers will only be able to see data of one of the nodes and its counterparties, as we mentioned; other information are encrypted and verified with zero-knowledge proofs. Thus, security is not much different from current banks' systems. In recent developments, interoperability was also included, with the launch of CordaNet, allowing different private networks to interact with one another.

Croman et al. (2016) already noted that in a consortium blockchain scenario, consensus is reached just through a general byzantine fault-tolerant protocol, rather than an election

mechanism governed by proof-of-work or proof-of-stake. Evaluating the performances of a simple BFT protocol to reach consensus, the authors find outstanding performances compared to public blockchains: latency is in the order of milliseconds as the time needed to update the network is much smaller since the number of participating nodes is far smaller than those of a public blockchain (Bitcoin counts around 2000 nodes). Secondly, throughput and TPS are in the order of thousands and tens of thousands as the number of participating nodes diminishes, this is thanks to the faster consensus, and the small latency of the network. Finally, fees are basically non-existing, as in the worst-case scenario, with 64 nodes, 10 million transactions cost just $3.95.

Pongnumkul et al. (2017) perform a comparative analysis of two among the aforementioned permissioned blockchains, that are Hyperledger Fabric and Ethereum private blockchain. Performances are evaluated in terms of throughput and scalability, concluding that Hyperledger Fabric is by far superior to Ethereum private implementations. Indeed, Hyperledger outperforms Ethereum private in response time under high workloads (10,000 transactions), proving to be up to 10 times faster. The same happens as for latency, which also at small workloads is half of that of Ethereum private. Throughput analysis shows that Hyperledger confirms transactions in batches of 500, with a quite steady processing time of 3.57 seconds per batch, validating all transactions within a minute; instead, Ethereum validates the first transaction only after 361.61 seconds due to the high latency, and the following transactions are validated within 100 seconds after that. The only parameter Ethereum proves better is in handling concurrent transactions (i.e. transactions in conflict with one another), handling up to 50,000 concurrent transactions as opposed to Hyperledger crashing after 20,000 concurrent transactions. The authors conclude that the platform choice in private context has to be evaluated carefully, by firstly testing performances and relevant parameters to the use case. In general, they also note that private blockchains are by far more performing than public ones.

The takeaway from private ledgers analysis made clear that they are by far more efficient platforms compared to public blockchains, and they have none of the problems mentioned. In addition, Corda also allows for interoperability and cross-chain exchanges among different businesses and industries. On the other hand, it is evident that such systems require a strong governance and a high degree of centralization; for instance, the R3 consortium was set up by banks themselves and there are full-time employees working at the development, the marketing and the engineering of the infrastructure. Where possible, private ledgers are run on private networks too, rather than on the internet: projects such as SIA Chain will give even more privacy and security to the institutions adopting this kind of technologies. Private ledgers have little in common with the architecture of public blockchains, but they are better poised to serve institutional players with high performance, data privacy, and regulatory compliance.

3.8 Conclusions on technical limits and solutions

In this section, we put together the key points of the chapter. We investigated public blockchain platforms and we found that their widespread adoption is hindered by many issues. Nevertheless, research is on the way to find solutions to such open problems, and many promising proposals have already been made and some also implemented to fix some of them. The main issues in place are tradeoffs between security and scalability-wasted resources, between centralization and usability: we showed that PoS protocols ensure faster transactions and no energy consumptions, but are considered unsafe in many circumstances; we showed that despite cryptocurrencies claims of being decentralized, centralized services such as wallets or mixing services are still needed not only to ensure users' privacy, but also to let non-tech-savvy users adopt a technology which would otherwise be too complex to master.

Yet, there are very promising research paths that could break up these tradeoffs. Firstly, using sidechains and allowing cross-chain interoperability could allow users to avoid excessive usage of exchanges, store a single cryptocurrency and pick a different blockchain for the type of transaction they are carrying out: Zcash if they seek anonymity, Bitcoin if they transact large amounts and need high security, PoS coins if they transact small amounts and want low fees, etc. Secondly, the Lightning Network could significantly boost scalability and throughput in any blockchain by validating only certain transactions on-chain, while most of them are processed and validated off-chain; however, it still does not answer to the wasted resources issue. Lastly, novel PoS protocols managed to achieve high security standards by developing new mathematical models, solving the issues of scalability, wasted resources and in Algorand case, forks. In the next 1-2 years, these improvements shall undergo further testing and then it will be possible to establish which of them (if any) can bring public blockchains to a better competitivity.

In the meantime, also private platforms have been developed by consortia and proved to be much more efficient than public ones as many of the blockchain principles are left out in this context, and thus also many of the problems. There is no decentralization, no strong consensus protocol, and no blocks, as transactions are not batched. We shall refer to these platforms as private distributed ledgers; for simplicity, we shall use the acronym DLT.

All in all, as of now, public blockchains are too far from solving technical issues, let alone the implementation of communication standards needed by financial players to make a transaction valid and compliant with regulatory requirements. Therefore, from the technical analysis we expect financial institutions to focus on DLT platforms, the same goes for startups aiming to interact with such institutional players.

3.9 Blockchain adoption

In the review of technological constraints hindering the adoption of BCT, we highlighted that performances are low for public blockchains and some problems still await a solution, whereas private systems are more mature. Nevertheless, according to many studies and news articles (Wüst and Gervais, 2017; Peck, 2017; Floyd, 2017; The World Economic Forum, 2018; Carson et al., 2018), the overall performances of the technology are largely inferior to those of a traditional fully-centralized database. In fact, centralized servers can process up to 50,000 TPS for economic agents (Floyd, 2017), comparing to the 1,200 TPS (Carlyle, 2018) offered by the faster private blockchains, let alone the public ones.

In this section, we shall review the literature proposing logical constraints to consider when evaluating the implementation of a blockchain technology versus that of a traditional database in this section3.9.1. Then, in section 3.10, we model a general framework putting together the contributions by the different authors and expanding them by introducing the technical constraints discussed in Chapter 3. The developed framework will be employed in Chapter 3 to validate on a case-by-case basis the financial initiatives coming from the collected data.

3.9.1 Architectural Constraints

As for any other technology, it is evident that simply checking the performance capabilities of BCT to elect it as the solution for a given use case is not enough: first, an assessment of the use case is needed to verify that traditional technologies such as centralized database are unfit. The need to share data and have synchronized distributed ledger has to be much stronger than any performance advantage a traditional database can offer.

In our analysis, it is vital to distinguish projects that could have been implemented on a centralized technology compared to those that actually needed a distributed ledger. Starting from the technical review to the many news articles[39-40] reporting of illegitimate or scamming blockchain adoptions, even to the scientific literature describing the benefits of adding the word to one's resume (Kursh and Gold, 2016), we must distinguish between legitimate and deceptive use cases to provide a sensible mapping of viable use cases in the financial industry.

[39] https://www.theguardian.com/technology/2018/jan/30/blockchain-buzzword-hype-open-source-ledger-bitcoin

[40] https://www.businessinsider.com/how-to-tell-ico-scam-blockchain-2018-7?IR=T

To do so, we start by reviewing several studies investigating this issue: Wüst and Gervais (2017) provide a flow chart to determine whether BCT should be adopted and what kind of blockchain best suites the use case.

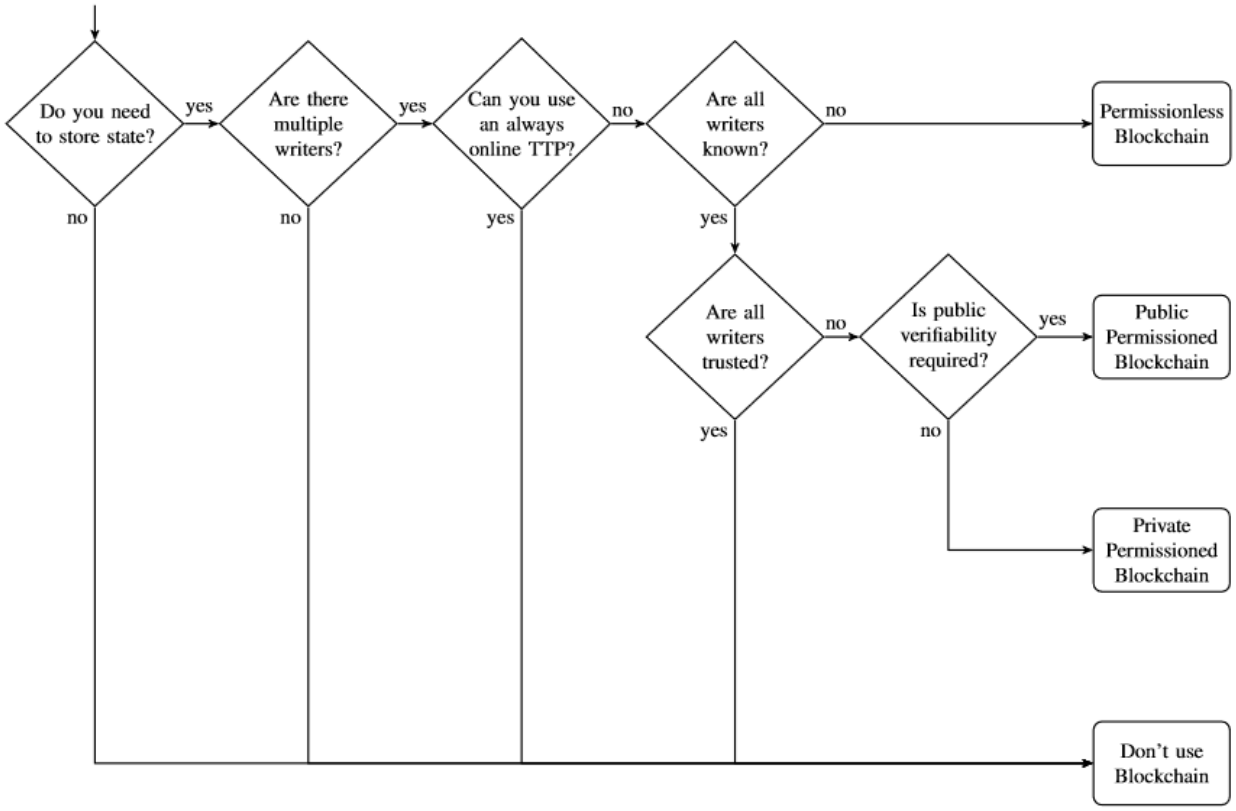


Figure 29, a flowchart to assess logical constraints of BCT from Wüst and Gervais (2017).

The first question is whether any piece of data needs to be stored at all; if that is not the case, neither BCT nor a traditional database are a solution. Secondly, if there was a single source of truth updating the ledger, no consensus mechanism would make sense, and a centralized database would better suite the case.

The next step depends on the presence of an always-online trusted third-party (TTP). In case a TTP can be addressed at any time, blockchain technology is outperformed by delegating the writing function to the TTP which can then make information available to all parties involved. By doing so, the only writer would be the TTP, taking us back to the previous step in the flow chart, meaning that the TTP should implement a centralized database with read access to other participants. Then, a permissionless blockchain should be used if there are unknown writers; to a permissioned blockchain if all writers are known, but not trusted; to a shared write-access database/cloud if all writers are trusted.

However, further researches demonstrated that BCT is not suited for *any* use case where there is no TTP, but only those where the ledger can take on three functions a TTP usually performs (Mainelli and Smith, 2015):

- Recording: keeping a record of transactions in case of disputes;
- Transacting: preventing duplicate transactions (i.e. double spending);
- Validating: confirming the existence of tradable goods and membership of the trading community.

Locher et al. (2018) argue that the first function can be performed by any kind of database. The second function can be performed by DLT considering past transactions. The third function is use case-dependent: blockchains can provide a validation services only if two criterions are met by the use case.

1. *(Object Creation Criterion) Any use case meets the object creation criterion if and only if, for any digital object on the ledger, it holds that the object has been defined at t = 0 or object creation is consensus-based.*

This means that any asset on the blockchain has to be either generated when the protocol is set up and not in any second moment, or that it can be generated in a second moment if a consensus-based protocol ensures that the blockchain participants all agree on the asset generation. For instance, in a blockchain recording land ownership of a state all land is digitalized at the moment of set up and no further addition are made (as there cannot be creation of new land); in Bitcoin instead, all coins are generated according to the consensus protocol of the proof-of-work, that is, when miners find a new block they get newly minted bitcoins as a reward. On the other hand, considering e.g. a problem of vegetables tracking that would be tokenized on the blockchain, new assets cannot be created by consensus, but only by recording newly harvested vegetables manually, making it a bad use case for a blockchain. In other words, blockchains cannot assess the validity of transactions if assets are not native, or not completely recorded in the moment of deployment. The second criterion is:

2. *(Internal Predicate Criterion). Any use case meets the internal predicate criterion if and only if all predicates [41]of the use case are internal.*

Indeed, if the truth of records cannot be assessed by just inspecting the ledger's state, a TTP is inevitably required to provide this verification. Let us consider two use cases, one

[41] A predicate is defined by the authors as a function mapping each record of the ledger in a Boolean value (true or false). An internal predicate is obtained if and only if its output can be reached by only examining the records contained in the ledger.

meeting and one not meeting the criterion respectively. Any virtual currency meets the criterion as these assets only exist as result of ledger transactions, which are consequently internal to the ledger. Instead, a tracking system monitoring the provenance of food products does not meet this requirement: the predicate "where is the tracked good?" cannot be proven true or false just by looking at the state of the ledger, but external predicates (such as a GPS signals, reports from suppliers, etc.) need to be considered. A GPS signal can be hacked, or the sensor could be detached from the goods, falsifying the positioning; suppliers instead could lie when writing on the ledger, as they are untrusted parties.

Thus, the recourse to an external predicate jeopardizes the core benefits of a distributed ledger, such as trust, being tamper-proof, and the reliability of the records, making the use case unfit for BCT.

Peck (2017) also produces a very similar flowchart to address the need or not of BCT, with analogous conclusions. Furthermore, he adds a distinction between the performances of the various technological solutions: a centralized database offers the highest transaction speed; a permissionless blockchain has very low transaction speed as a consensus mechanism and many nodes communications are involved; a permissioned blockchain offers medium transaction speed as consensus mechanism is simplified and there are fewer nodes compared to a permissionless one.

Also, in a paper by the World Economic Forum (2018) a flowchart gives directions on BCT adoption to guide the user not only strategically, but even on the performance of the technology. In particular, the scalability issue is taken into account, discouraging the adoption in case rapid performances are requested (transaction confirmation in millisecond) or a large amount of non-transactional data needs to be stored (as data is duplicated on the blockchain). We have seen that this is the case for public blockchains, whereas private blockchains are rapidly increasing their performances, driven by the competition among companies and consortia in the sector. Other logical questions are in line with the researches presented so far.

Lastly, Fridgen et al. (2018) provide an action design research approach to generate and consequently evaluate blockchain use cases. This is because they consider blockchain a "solution in search of a problem", therefore, much more emphasis is put on the use case/problems generation, rather than beginning from the technology. The approach is aimed at in-house usage for companies willing to innovate their business with BCT. There are six practical steps to be taken according to the authors: (1) Understand the technology, that is inviting an expert to lecture a selected group of employees on the topic; (2) Get creative-unbiased, where the participants start discussing potential use cases for their business/function; (3) Glance in the market, to spot current projects and PoC deployed by other companies; (4) Get creative-informed, where use cases are generated again after looking

at what is currently available on the market; (5) Structure ideas, by clustering them and giving priority to most suitable; (6) Prototype, i.e. pick the most promising idea and discuss a possible business model to accompany the implementation.

3.10 Adoption framework

We reviewed structured approaches that answer the question whether adopting a blockchain is a valid idea or not. All researches are aligned with similar flowcharts and differ just slightly depending on the parameters they consider; besides, we found that Locher et al. (2018) research can integrate these frameworks with further insights on the presence of a TTP. To study financial use cases, we propose a framework merging the studies reviewed so far with those TTP criterion mentioned.

Furthermore, we shall also include the results of the technical review, that is, the issues still open with public blockchains are taken into account when directing the choice between a public or a private platform. Privacy is not achievable on public blockchains, neither so, the attachment of metadata or attribution information, forcing any use case involving financial institutions to be moved on a private platform.

Scalability is only achieved to some extent by permissioned platforms, as they are in control of the number of nodes, can run on a private network avoiding most bandwidth issues and have a considerable throughput as consensus is not to be reached, but a notary is in charge of validation. In terms of security, public blockchains are safer and more censorship-resistant than private ones. In addition, finality, governance managing updates, resources used, and fees paid are much lower/non-existent in a private environment. Finally, as we mentioned, metadata and attribution data cannot be attached to transactions on permissionless platforms, making them unsuitable for financial intermediaries or other companies that share the same requirements. To sum up these results, we provide a flowchart in Figure 30.

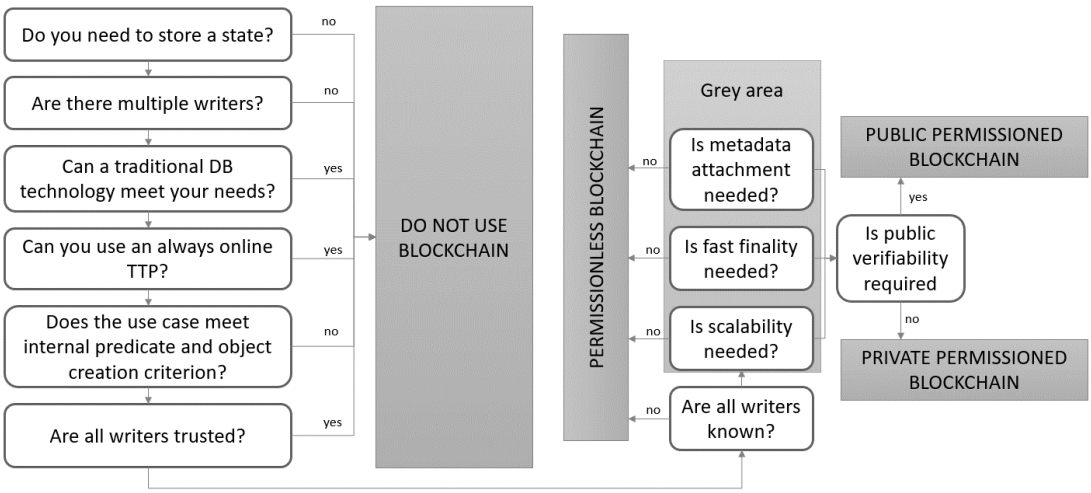


Figure 30, flowchart guiding the use case selection for blockchain technology

We note that the grey area section refers to the fact that improvements are underway in public blockchains to allow finality and scalability even for this kind of blockchains, possibly leading to a market deployment in the next 1-2 years. Therefore, questions in the grey area should be constantly reviewed in consideration of research developments, as finality and scalability might be achieved also by public platforms. In addition, public verifiability could also be dealt with in public blockchains with zkSNARKs protocols. Anyway, up to now public blockchains cannot give an adequate answer to these questions, causing the majority of use cases to fall into the permissioned platforms' area.

CHAPTER 4
FINANCIAL INSTITUTIONS CLASSIFICATION

In this chapter, to properly assess and categorize the areas of application for blockchain technology in finance, we shall review the literature surrounding financial institution classification in section. Our analysis is aimed at finding possible clusters for financial institutions, so that when discussing blockchain application we can indicate which application each institution should consider.

In section 0, we give a preliminary definition of financial institutions, considering why they are important in a sound economy and the role they play at a general level. This is important to consider, as public blockchains advocate for disintermediation, but certain services can only be offered by a centralized institution.

In section 4.2, we examine the first of the classification proposed in the literature, that is, classification by function, where financial institutions are clustered based on the services that they typically offer.

In section 4.3, we discuss a classification based on the risk of the assets present in financial institutions' portfolios. It is alternative to other classifications as players carrying out the same services, might be very distant in the risk they detain.

In section 4.4, we review a classification by governance. Illustrated by an Italian paper, it considers legal definitions and the ownership composition of shares to determine clusters for the intermediaries.

In section 4.5, we end the chapter by selecting the classification by function, not really to cluster financial institutions in groups as our original objective was: in fact, nowadays, we

show that most intermediaries engage in many functions, overlapping one another. Therefore, we conclude that classifying blockchain application looking at intermediaries is irrelevant, while it is more sensible looking at the activity themselves.

4.1 Financial institutions

This dissertation section at giving an overview of the financial sector as it appears nowadays. The main goal is the identification of the different financial actors and of the functions they are engaged in. In this way, we can have a clear view of the environment in which we are questioning how the BCT could be applied: we can understand who the main players which might be interested in this new technology are, how to classify and differentiate them, and which functions they perform.

4.1.1 Definition

First, a definition of financial institutions is necessary. They are described as the channel between individuals or corporations which have a surplus with the ones having a shortage of funds (De Hann et al. 2009).

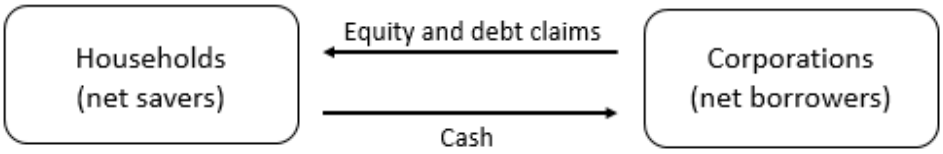


Figure 31, Flow of funds in a world without FIs (adapted from Saunders and Cornett, 2008)

While linking these two parties, they allow a more efficient flow of funds. If we imagine a world in which financial institutions do not exist, savers who want to invest their money in a firm would have to monitor the actions of that firm to assess they are not wasting the investment. These checking activities would result being very costly as they require time and expenses to collect high-quality information. Thus, the attractiveness of buying a firm's securities would reduce and the flow of funds would be quite low (Saunders and Cornett, 2008).

Financial intermediaries can rely on their expertise and on economies of scale and scope to generate process efficiency. They reduce transaction costs performing two main functions: sharing information and facilitating the management of risk (Oldfield and Santomero, 1997). In doing so, they provide services as asset transformer or broker. Asset transformation activities include purchasing claims issued by corporations, such as equities, bonds, and other

primary securities, and finance them by selling financial claims as deposits, insurance policies, and so on, to investors.

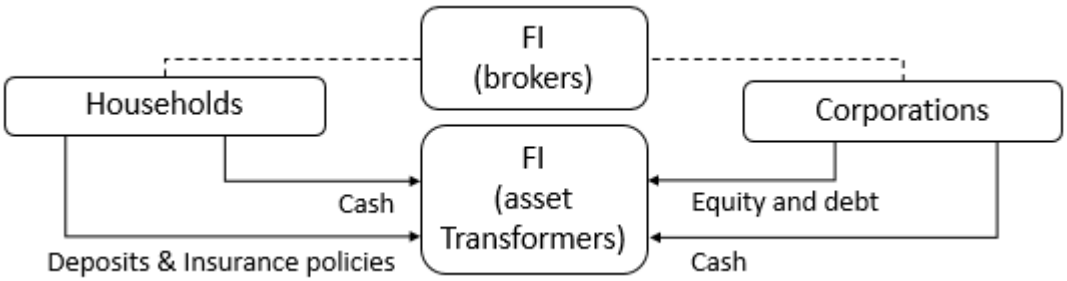


Figure 32, flow of funds in a world with FIs (adapted from Saunders and Cornett, 2008)

Brokers instead reduce information imperfections between the two parties of a transaction, thus reducing its costs. Thanks to specialized skills, they are able to interpret cross-sectional and intertemporal information. In exchange for this service, they are compensated with a fee (Battacharya and Thakor, 1993).

4.2 Classification by function

Developing a classification of the financial institutions aims at grouping together actors with similar characteristics. Most of the scientific literature propose a subdivision of the actors of the financial world based on the functions they perform and the activities they carry out. However, we have encountered also other ways in which they are categorized, focusing for example on their form of governance or on the risks they face.

Considering the functional perspective, we can make a first differentiation between depository and non-depository institutions. The former comprehends commercial banks and saving institutions whose main portion of funds comes from customers' deposits. Nowadays, however, the distinction between these two groups has become blurred, as many non-depository institutions expanded their services and started proposing offerings which compete with those of commercial banks (Greenbaum et al. 2015).

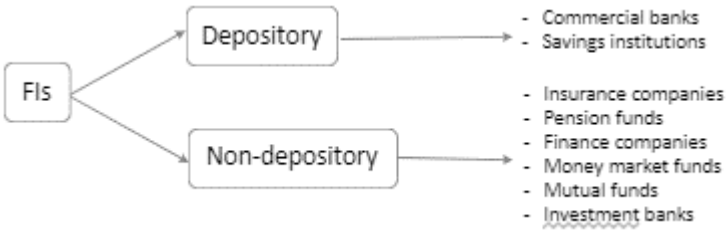


Figure 33, depositary and non-depositary FIs (adapted from Greenbaum et al. 2015)

4.2.1 Depository institutions

The depository institutions' products are registered in both sides of their balance sheets: loans on the asset side and deposits on the liability side (Saunders and Cornett, 2008).

Commercial banks activities include accepting deposits and making loans. From the assets side, they have four major earning areas: business loans (or commercial and industrial lending), securities, mortgages, and consumer loans. On the other hand, form the liabilities' side, a main characteristic of banks is their high leverage, meaning that a high percentage of their assets are funded by debt, either deposits or borrowed funds (ibidem).

Within this group, we can make a further classification of the banks:

- *Retail*: they are engaged with private individuals and small businesses and tend to specialize in residential mortgages, consumers loans and local deposit base.
- *Wholesale:* in this case loans and deposits, which are much larger than in the retail commercial banking, are mainly devoted to medium and large corporate clients. Therefore, they are usually bigger than retail banks. Within this group we can also include money centre banks. The latter heavily rely on non-deposit or borrowed sources of funds and mainly participate in foreign currency markets, thus being exposed to foreign exchange risk.

Depending on the asset sizes of different banks, their balance sheet composition may vary significantly. For instance, big banks make proportionately more commercial and industrial (C&I) loans and less real estate loans than retail ones (ibidem). A commercial bank might also act as a trust company. This is an organisation which assume the responsibility to manage financial products on the behalf of a person or a business, whose goods are transferred under the administration of the fiduciary (Testo Unico della Finanza, 1998).

The purpose of savings institutions is performing credit activities and collecting individuals' savings and remunerate it through low risk investments, mainly mortgages and other securities. Originally, they were born as no profit organisation, but in recent times they have become more and more similar to commercial banks. In the Italian scenario, with the 'Legge Amato-Ciampi' enacted in 1990, indeed, saving institutions have been rearranged: the credit and the charity function were separated leading to the creation of two different entities (Sala et al. 2010).

We can list two different groups of these institutions:

- savings associations which are more concentrated on residential mortgages

- savings banks which, besides residential mortgage assets, hold commercial loans, corporate bonds, and corporate stock as well (Saunders and Cornett, 2008).

4.2.2 Insurance

Individuals and corporations rely on insurance to protect themselves from adverse events. Insurance's clients are known are policyholders. The latter pay a regular amount of money, known as premiums, to buy financial protection from the occurrence of certain specific events (Hull, 2015). Usually, insurance use this collected premiums to invest in securities such as corporate bonds and stocks (Oldfield and Santomero, 1997).

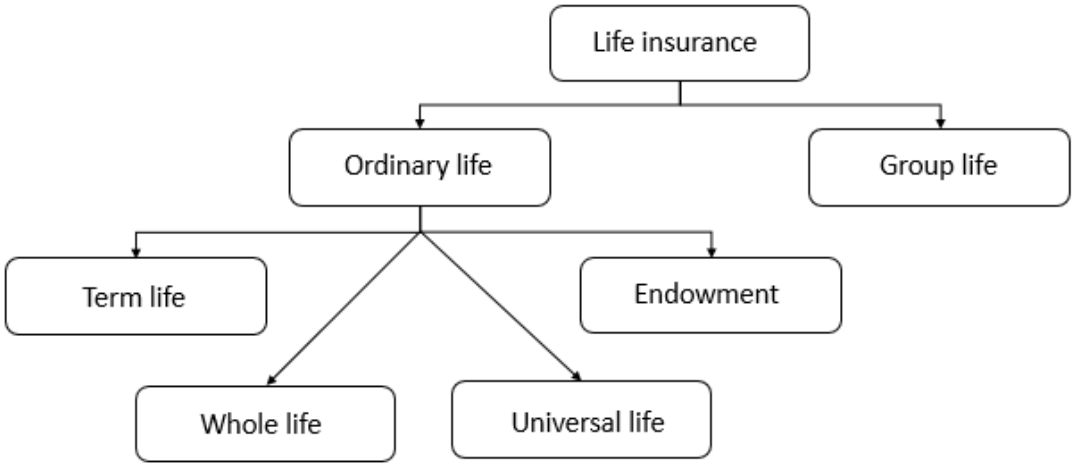


Figure 34, life insurance typologies (adapted from Saunders and Cornett, 2008)

Three major groups belong to the insurance industry: life/health insurance, property/casualty insurance and reinsurance (Santomero, 2001). In this section we will analyse more in details the different typologies mentioned above.

Usually, life insurance lasts longer than the other categories, and its payments depend on the policyholder's death (Hull, 2015).

Ordinary life insurance addresses individuals and different options exist for clients:

- Term life: in this case the insurance payments are contingent on the policyholder's death. The term life insurance lasts a predetermined period of time and in the event that the policyholder dies, the appointed beneficiary is given the face amount of the policy, otherwise no payments are made (ibidem).
- Whole life: it differs from the previous one as in this case a pay-out is guaranteed. Policyholder has to provide regular premium payments until death to ensure

his/her beneficiary a pay-out from the insurance company (Saunders and Cornett, 2008).

- Variable life: a whole life insurance variant, in which premiums paid are invested in funds chosen by the policyholder, such as mutual funds, equity funds or bond funds, thus the pay-out depends on the funds' return (Hull, 2015).
- Universal (variable) life: in this case premiums and maturity can be changed by policyholders without the policy lapsing. A minimum return is guaranteed, but the policyholder has also the possibility to choose a variable form, in which money paid are invested on funds (Saunders and Cornett, 2008).
- Endowment: this insurance lasts for a predetermined period of time. The pay-out is guaranteed and is given to the policyholder if the end of the period occurs before his/her death, or to the beneficiaries, otherwise. (Hull, 2015).
- Group life insurance: in this case many individuals are grouped under a single policy. Usually they belong to a specific group, for example they might be employees of the same company. This category can take advantage from economies of scale (Saunders and Cornett, 2008).
- Credit life: lenders rely on this insurance to protect their credits against the borrowers' early death, before the debits being paid back (ibidem).
- Annuity contracts: in this case regular payments or a lump sum paid by the policyholder for a certain period of time are then converted in the future into pay-outs from the insurance. Individuals usually buy this product to guarantee themselves further incomes besides pension.
- Accident/health insurance: While life insurance protects against mortality risk, health insurance protects against illness risk. In Italy, the National Health Service automatically covers all citizens and legal foreign residents through funds deriving from taxes. Moreover, Italians have the possibility to complement their medical assistance with private health insurance. Around 6 million people are covered by some form of private assistance, which mainly addresses services excluded in the public one. There are two form of private coverage, corporate and noncorporate. The former is offered by a firm to its employees and sometimes enlarged to their families too, while the latter is bought by individuals.[42]

Property/casualty insurance usually lasts one year and can be renewed at the end of the period, with premium adjustment if the insurance company assesses that the expected pay-out has changed (Hull, 2015).

[42] International Health Care System Profiles, https://international.commonwealthfund.org/countries/italy/

Property insurance offers protection against physical losses or damages from fire, theft, etc. Casualty insurance instead protects against legal liability exposures. However, in recent times, this difference has become more and more blurred as insurers are offering combined property and liability insurance into single policy packages (ibidem).

The greatest risk the insurance company can meet is not having enough money to cover claims. Therefore, they can protect themselves against it through the reinsurance services. An insurance company, called ceding company, pays a fee two a second insurance company, called reinsurer, which commits to be respirable for some of the risks that have been insured by the former. In this way, the ceding company is allowed to write more policies than they would do otherwise. Another reason for relying on this service is the increased protection against what are known as catastrophic loss. Examples of this kind of damage are heart quake, hurricane, which hit many people. Thus, they may cause several concurrent claims, resulting in difficulties for the primary insurance companies to support these financial provisions (Rejda, 2004). Another method through which these companies can deal with catastrophic events are particular financial instruments, known as catastrophe (CAT) bonds, which allow them to share with the market these risks.

4.2.3 Security firms and investment banks

The main tasks carried out by this category of institutions are the assistance of companies and governments in raising debts and equities, the provision of advices in different corporate activities, and the trading of securities (Greenbaum et al. 2015). Investment banks commit to originate, underwrite and place new securities on the market. They also advise corporations regarding mergers and acquisitions (M&As), reconstruction and other financial decisions. Securities firms instead undertake the same activities but with existing securities, thus in the secondary market (Saunders and Cornett, 2008).

The securities, which are not only corporate ones, but also government, municipal and asset-backed, can be underwritten through private or public offerings. In the first case, the banks place the securities with institutional investors, in exchange for a fee (ibidem). In the case of a public offering, instead, the investment banker can act on a best-effort or a firm commitment basis. With the best effort underwriting, the bank acts for its own account, thus as a principal. It purchases the financial instrument at one price with the purpose of selling it to public investors at a higher price. While in firm commitment underwriting, the bank acts for other name account, naming as an agent, on a fee basis related to the success in placing the issue on the market (Gveroski et al, 2009). Moreover, investment banks result being very useful in assisting in mergers and acquisitions, searching and assessing values of possible

merger partners, advising good terms of merger agreement, and underwriting new securities to be bought by the target firms (Saunders and Cornett, 2008).

Securities firm commit instead in market making, which means creating a secondary market in an asset. Even in this case, they can act as principal, thus trying to profit on the price movements of securities, or agent, profiting from the bid-ask spread, which is the difference between the buy and the sell price of a security (Hull, 2015).

In recent years, commercial banks subsidiaries specialized in investment banking activities have been born, thus making the boundaries between commercial and investment banks blurred (ibidem). Moreover, many investment banks have started offering products similar to the commercial banks' ones. For example, they offer individuals deposit-like cash management accounts (CMAs), which broker can directly manage to buy and sell securities, making this offering more attracting than the commercial banks' one. Money are, indeed, directly taken from the CMA when an investor buys a security and put back in it when the investor sells securities.

There are other actors included in this category. *Discount brokers* perform trading activities for on- or offline customers without complementary services of advisory. Trading activities can also be performed directly by customers without a broker as intermediary through dedicated platforms offered by *specialized electronic trading securities firms*. *Venture capital firms* are institutions which collect money from individual investor or other financial institutions to fund small, new businesses (Saunders and Cornett, 2008). *Società di Intermediazione Mobiliare* (SIM) are other institutions, which besides banks and securities firms, are focused on offering investment services. As explained for investment banks, they can act on their own account, by carrying out deals and underwriting activities, or on someone else's account, through selling and brokerage (Testo Unico della Finanza, 1998).

4.2.4 Funds

In this category we group the specialized institutional organisations whose goal is involving individuals and organisations with a limited amount of money and limited knowledge in the trading activities in the world of investing. Indeed, they pool together resources of different actors and invest them in a diversified portfolio of assets (Gveroski et al, 2009). The small investors can take economic advantage from these funds as they are able to generate economies of scale, thus reducing the transaction costs and commissions with respect to the ones they would have paid if directly investing individually (Saunders and Cornett, 2008). Moreover, thanks to the portfolio diversification, they face low risks and can rely on the institution's specialisation for what concern the investments' management (Gveroski et al,

2009). There are different typologies of funds, mutual and hedge funds. They both pools together money of different investors, but the latter is subjected to less regulation.

Mutual funds can be evaluated based on their time orientation as short-term or long-term funds (Saunders and Cornett, 2008), or on the variation in their number of outstanding shares, as open-end or close-end funds (Hull, 2015). Bond funds, comprised of fixed income capital market debt securities, equity funds, made of common and preferred stock, and hybrid funds are long-term oriented. Short term funds, instead, are usually taxable or tax-exempt money market mutual funds, funds which contains various money market securities (Saunders and Cornett, 2008). The difference between close end and open-end funds is that the former is made of a fixed number of outstanding shares, while the latter are continuously ready to sell new shares and redeem existing ones. Thus, the NAV, the Net Asset Value, of the two portfolios is calculated differently. The Net Asset Value is the value per share of the fund on a specific date or time, based on the closing market prices of the securities in the portfolio. In the case of open-end funds, the NAV of shares is calculated as the market value of assets net of liabilities, divided by the number of outstanding shares. While in the case of close end funds, the demand for the shares is also taken into account. If it is high, then the fund is traded at premium, meaning that it can be traded at more than the fair market value of the securities, otherwise it is traded at a discount, that is at less than the NAV of the shares (ibidem). The close end funds are traded on a stock exchange similar to the trading of corporate stock. Among them, we can for example, highlight REITS, which are Real Estate Investment Trusts, companies specialized in investments in real estate companies' shares. Among mutual funds, we can also include another category known as ETFs, Exchange-Traded Funds. As close-end funds, they are traded on a stock exchange. The difference between the two is that the ETFs follow the market indexes, meaning that there is no appreciable difference between their trading prices and their fair market value, thus their management costs are lower, and they are considered more attractive to investors than close-ended funds (Hull, 2015).

Hedge funds are less subjected to regulation with respect to mutual funds. Indeed, they have the possibility to adopt investments strategies which are not allowed to mutual funds, such as short selling, derivatives, hedging and leverage. They are addressed only to sophisticated individuals and organisations[43]. This kind of funds usually take different level of risks. They can be aggressive, thus aiming to produce high returns while taking significant risk, usually through investments based on anticipated events, or risk moderate, with only a portion of the portfolio being hedged (Saunders and Cornett, 2008).

[43] Borsa Italiana, https://www.borsaitaliana.it/notizie/sotto-la-lente/fondohedge.htm

There are different institutions committed in offering collective funds in Italy, as it is explained in the 'Testo Unico della Finanza' (1998), known as a group as OICR, Organismi di Investimento Collettivo del Risparmio. Società di Gestione del Risparmio and Gestore di Fondi di Investimento Alternativi are respectively the ones managing mutual funds and hedge funds. Moreover, there are also other investment organizations which are constituted as limited companies, whose only scope is to invest their capital. They are named SICAV and SICAF, Società di Investimento a Capitale Variabile/Fisso. The latter bind its participants for the entire life of the society, while the former allows them a reimbursement whenever they want it. They can both be managed autonomously (autogestione) or by external entities chosen by the society (eterogestione).

Finally, a pension plan is a fund which has similarities to some of the products offered by life insurance companies (Hull, 2015). As for what is done with annuity contracts, indeed, people pay regular contributions for a certain period of time to receive lifetime payments after their retirement. In Italy, the number of workers relying on this form of integrative income has reached 8.3 million in 2017, with an annual increase of 7.1% (Covip, 2018).

4.2.5 Finance companies

We can group in this category all those institutions which can be considered as competitors of depository institutions, though they do not rely on deposits as a source for funds. Their main function is indeed making loans to both individuals and corporations, but their source of funds is short- or long- term debt. The institutions specialized in financing corporations, through for example leasing and factoring, are known as business credit institutions. Instead, the ones focusing on individuals are sales finance institutions and personal credit institutions. The former offer loans to clients of particular retailer and manufacturer, while the latter to consumer usually considered too risky by commercial banks (Saunders and Cornett, 2008). Moreover, microcredit institutions exist with the purpose of offering financing in limited amounts to both individuals and businesses. They are respectively known as Operatori di Microcredito sociale or imprenditoriale (Testo Unico della Finanza, 1998). The Testo Unico della Finanza (1998) recognizes two main organizations offering payment services, the payment institutes and the Istituti di Moneta Elettronica (IMEL). The former can work under a limited operativity, with a maximum amount of transacted money in the previous 12 months of 3 million euros, or a full one, thus not having limitations. The latter issue digital money and offer related payment services support.

4.2.6 Financial markets' intermediaries

In the financial markets, actors trade between one another derivatives and other financial products. We can identify the exchange market and the over-the-counter market. The latter has usually much larger transactions than the former and its participants are free from the contractual terms of the exchange market, thus can negotiate any deal. In this context, there are institutions which mitigate the participants' risk which are the clearing houses in the exchange markets and the central counterparties in the OTC markets. They both deal with the two participants of a transaction, standing between the two traders by buying a financial product from one of them and selling it to the other one, so that they do not have to interact between each other and to worry about the creditworthiness of the counterparty.

4.3 Classification by risk

As mentioned above, most of the scientific literature proposes classifications of financial institutions based on the activities they carry out and the functions they perform. Still, some researchers have also tried to find other way to group them homogeneously. Hess and Laisathit (1997), indeed, evaluated if the investors' perception of the risks the firms are facing could be a good factor for classification and compared it with the SIC code classification.

SIC stands for Standard Industrial Classification, and through the related code, made of one to four numbers, the various industrial sectors are subdivided based on their main areas of activities. The primary SIC code of a firm identifies its primary line of business. In Europe this code has been used for the derivation of the corresponding European digit version, known as NACE, which is further translated in the Italian ATECO. As one derives from the other, the logic for the classification is the same, but NACE and ATECO codes are more detailed and based on European or Italian requirements respectively. The first two digits represents the division, the third the group, the last one the class to which the company belongs. The purpose of this classification is having a univocal identification of all the firms (Istat, 2009).

The two authors developed a two-factor analysis of the monthly holding period returns on the stocks exchange-traded financial firms gathered by the SIC list, whose code starts with a number comprised between 60 and 67, representing the financial division. The data are collected among the firms in the list from 1981 to 1988. The two factors taken into consideration are bond-holding period return and the equity-market return. The research led to the generation of 10 different portfolios with similar risk exposures. If compared with the SIC codes, we can easily assess there is no correspondence between two classification methods.

There are indeed firms with the same risk exposure which belong to different SIC groups and vice versa.

Therefore, the risk exposure assessment can be considered an alternative method for clustering financial firms. Its use might be limited to those activities in which the risk is a predominant factor for efficiency. Moreover, the evaluated risk is subject to the investor perception, therefore the classification might results not be univocal, considered therefore as another limitation in its adoption (Hess and Laisathit, 1997).

4.4 Classification by governance

The governance is considered by Gillan and Starks (1998) as the set of rules, incentives and factors which guarantee, through the firm management, its survival and an adequate return to its shareholders. The ownership of the bank is the main factor which differentiate its governance structure (Zazzaro, 2001). As we can see from Table 3, there are many possible combinations of ownership. There are three possible owners of a bank: the state, foundations or private companies. The State can perform the role of owner of a bank, if at least 30% of the financial institution's share are in its hand. *Public banks* instead started to appear in the 90s after the enactment of the 'Legge Amato-Ciampi', according to which banks controlled by foundations could turn into limited companies, by separating the banking institution from the foundations.

<table>
<tr><td rowspan="3">The first three shareholders belong to the same category</td><td rowspan="3"></td><td>State</td><td>Foundations</td><td colspan="4">Private company</td></tr>
<tr><td></td><td></td><td>Financial institutions (others than banks)</td><td>Non-financial institutions</td><td colspan="2">Other banks</td></tr>
<tr><td>State bank</td><td>Public banks</td><td>Pure banks</td><td>Industrial banks</td><td>Network banks</td><td>Group banks</td></tr>
<tr><td rowspan="2">The first three shareholders belong to different groups</td><td>Mixed (the first shareholder owns at least 5%)</td><td>/</td><td>Quasi-public</td><td>Quasi-pure</td><td>Quasi-industrial</td><td>Quasi-network</td><td>/</td></tr>
<tr><td>Composite (no one owns at least 5% of shares)</td><td>/</td><td colspan="4">- Public company
- Popular cooperative</td></tr>
</table>

Table 3, financial institution classification by governance (adapted from Zazzaro, 2001).

Private banks might have different typologies of owners, such as non-financial institutions or other financial ones. In the former case it assumes the name of *industrial bank*, as the main shareholder is usually a manufacturer or a retailer firm. The company might take economic advantage of this control, considering the bank its privileged funding channel. Instead, among

the banks controlled by financial firms, we can classify the pure banks and the network/group banks. The difference among them is that the pure banks are controlled and guided by actors other than banks, which are committed solely in financial activities. The Network and group banks are a set of banks which own one another some of their shares. They share the same board of directors and some other representative roles. The difference between them is that the in the former category the participants are juridically independent of each other, while in the latter they depend on the parent company of the holding.

When the shareholders do not belong to the same category but the one controlling the highest number of shares has at least 5% of them, banks are known as mixed. Considering the group to which the main shareholder belongs, we can classify the banks similarly to the structure explained above. Differently, composite banks are the ones in which no shareholder has more than 5% of ownership. We can differentiate between popular cooperative and public company. The former's owners are the bank's users or workers, while the latter is owned by the general public.

4.5 Conclusion

The purpose of our analysis is finding the most suitable classification of financial institutions to evaluate the application of BCT. The classification by risk seems suited for a risk-related research and entails the difficulty of computing the portfolio risk for each institution of interest; it is therefore complicated and not relevant for our research. On the other hand, classification by governance is country specific (i.e. the paper is relevant only for Italy), and again does not comply with our objectives. Indeed, we aim to differentiate the various actors of the financial environment to assess whether BCT could be a useful instrument and whether it could bring any advantage to them.

Considering this, a categorization of the FIs by functions and activities performed seems to be more suited for our goal. We found that the most thorough scheme on institutions and their functions was reported in Saunders and Cornett (2008) in Table 4. The initial conclusion we can draw by this image is that nowadays financial institutions are no longer specialized in only one function. Indeed, today the universal bank is the most widespread model of banking institution, engaging in the provision of many different financial services and products, combining retail, wholesale and investment ones. Even insurance companies largely overlap with depository institutions and securities firms. Consequently, we shall abandon the initial idea of reviewing blockchain application by the type of institution, instead, we shall focus on the *services offered* to propose a relevant classification for financial intermediaries. Looking at the table, this means switching our focus from the horizontal to the vertical subdivision.

Function / Institution	Payment services	Investment products	Deposit & Lending	Supply chain finance	Insurance products	Fiduciary Services	KYC
Depository Institution	X	X	X	X	X	X	X
Insurance Companies	X	X	X	X	X	X	X
Securities Firm	X	X	X	X	X	X	X
Finance Companies	X	X	X	X	X	X	X
Fund Companies	X	X			X	X	X
Financial Intermediaries	x	X			X	X	X

Table 4, functions performed by FIs (adapted from Saunders and Cornett, 2008).

Following this scheme, each function will be analyzed more in detail in the following chapters, aiming to understand how they are performed nowadays and whether there are criticalities in the processes which might be solved by the adoption of the BCT.

All in all, we found that the classification by function is more of a historical heritage, that is not relevant if we try to cluster institutions nowadays. Still, it is relevant for our thesis at it provides a clear mapping of the *functions* carried out by intermediaries, that we will use to describe potential blockchain application.

CHAPTER 5
FINANCIAL SERVICES AND THE ROLE OF BLOCKCHAIN

In this chapter, we shall review, for each of the functions outlined in Chapter 4, the current processes against blockchain-enabled processes. In section 5.1, we present general results of our empirical research. We show how they were classified, the numbers we dealt with and how subsequent tables presenting them in detail will be organized.

Then, all the even sections following 5.2 deal with the as-is services offered by banks. Academic literature is reviewed, as well as other sources such as industry reports and interviews to give a detailed map of current processes. The focus of these section is that of highlighting criticalities and inefficiencies in current processes to find whether the analyzed blockchain applications can solve them.

On the other hand, all the odd sections following 5.3 tackle the application of blockchain technology, respectively, for each of the areas in even sections. To define such applications, we scouted startups including blockchain-related terms on CrunchBase and downloaded a database which we refined as explained in Chapter 2. At the same time, we looked for established firms' initiatives on the main cryptocurrencies and blockchain-related news websites, constructing a second database. In each of the even sections, first, we present the aggregated data for the specific financial area we are inspecting, then we present outstanding initiatives, referring to specific use cases and specific startups. Also, we give a mapping of blockchain enabled processes, representing how the technology can possibly cut costs and useless steps in as-is procedures.

Finally, we conclude with section 5.16, where we put together all the technology's contributions in the single areas to give a general picture of its impact in financial services,

possible threats to incumbents coming from disruptive startups, and new products that incumbents will be launching in the next years.

5.1 Presentation of results

As we explained in the methodology, we conducted a double research to find blockchain-related initiatives: one on startups companies by inspecting CrunchBase website with the terms "blockchain", "DLT", "cryptocurrencies", "cryptoassets", "Bitcoin"; the other is a set of news article we collected from CoinDesk, Blochckain4Innovation, Bitcoin Magazine, Cointelegraph , Cryptocoinsnews and ETHnews, reporting tests, products and adoption by companies focused on blockchain technology and DLTs. From this two sets we excluded startups and companies that had no role in finance, either because they were not financial intermediaries, or because they were putting forward projects that had nothing to do with the services listed in section 5.5. The result consisted of two databases: 247 startups performing blockchain-enabled financial-related activities, and 292 financial intermediaries testing the technology in various areas.

Area	Total Funds Received		% of Total Funds Received	Number of startups
Payment	€	824.625.154	26,63%	66
Investment products	€	1.722.861.661	55,64%	114
Lending	€	307.667.896	9,94%	21
SCF	€	65.699.421	2,12%	7
Insurance	€	13.241.000	0,43%	8
Fiduciary Services	€	54.225.162	1,75%	7
KYC	€	103.155.012	3,33%	20
Other	€	5.065.000	0,16%	4
Total	**€**	**3.096.540.306**	**100%**	**247**

Table 5, aggregated view for the startups' database. For each area, the table reports total funds received (in euros), the percentage of the funds received over the total, and the number of initiatives.

In Table 5, we present results coming from the startup database. In each section we will report data for the specific sector, also, complementing it with the average financing received. Startups received a consistent amount of financing, amounting to almost €3,1 billion; this number takes into account both funds gathered from venture capital financing, and funds gathered through ICOs (Initial Coin Offering) which we discuss in detail in section 5.5.1. Furthermore, in all subsequent sections we will refer to the percentage of funds received against the total to evaluate the relevance of the area, rather than the number of startups. Indeed, we shall consider such percentage as a weight to the relevance of the area we are

discussing. It is already evident that payment and investment products are the area that gathered the largest amount of funds, accounting alone for 80% of the total. We will discuss the reason for this disproportionate investment in sections 5.3 and 5.5. We also added the *Other* area to include those startups that were offering services specifically for financial institutions, but they were accessory services that did not corresponded to a specific function. The same was done for the companies' initiatives. We shall discuss the content of the *Other* area later in this section.

Area	Number of news	% of total
Payment	119	40,75%
Securities	85	29,11%
Lending	15	5,14%
SCF	24	8,22%
Insurance	14	4,79%
Fiduciary Services	3	1,03%
KYC	31	10,62%
Other	1	0,34%
Total	**292**	**100,00%**

Table 6, aggregated view from the news database. For each area, the table reports the number of news, and their percentage over the total.

Table 6 presents results for the companies' database. In each section we will report the number of news we found, completed by additional data about the nature of the initiative. Specifically, we distinguished between:

- Announcements: if the company announced their interest in a certain area or announced the intention to launch a PoC in the future, the piece of news was classified as an announcement.
- PoC: as proofs of concept, we classified all the news that reported a successful or unsuccessful test in a specific area.
- Operative: all the news that reported the launch of a product based on a DLT platform were classified as such.

The distinction allowed us to identify the areas where the number of PoC and operative services were more consistent, meaning that the technology is already available for use.

Ultimately, we did not create a section for the news and the startups falling in the *Other* category, but still considered relevant to report their role: all these 5 initiatives are focusing on document management, that is, provide a notarization service. Documents are registered on a blockchain and timestamped as a proof of their existence and mutual signing by involved parties. In fact, after the upload on-chain, data becomes immutable, meaning that neither of

the parties can modify it. This service is used for certain agreements financial institutions perform, such as loan contracts or insurance policies. Yet, the service is not strictly financial, as it can be applied to any contract in any other business, and more, the blockchain serves as a mere duplicate of information for extra proof that they exist, and they have not been modified. The technology is not changing the as-is process, just increasing the trust embedded into it.

5.2 Payment services

A payment occurs when one economic agent transfers value to another agent to discharge a debt. A payment system is the set of instruments, technical arrangements, procedures and rules used to transfer value. To process payments, payment systems usually take two steps:

1. Clearing, that is transmitting, reconciling and, in some cases, confirming payment orders prior to settlement. This process can include netting of payments and the establishment of final positions for settlement.
2. Settlement, that is the release of payment obligations between two or more parties by transferring funds between them.[44]

Payments can be carried out with: a net settlement, meaning that, upon prior agreement, obligations owed by an agent are written off using obligations due from other participants; or with a real time gross settlement (RTGS) which entails an immediate transaction of funds, considering transactions on a one-to-one basis.

The payment system can be split in the wholesale (interbank payments) and retail (consumer payments) systems (Kahn & Roberds, 2009).

5.2.1 Wholesale payments and reconciliation

The wholesale system has recently turned itself to the RTGS configuration as opposed to the net payment system: the latter was generating a too high systemic risk for the participants, despite advantages in the liquidity management.

The systemic risk is originated from highly connected systems, where the failure of a single party can bring about a relevant risk of failure for all other parties, with the possibility of triggering a domino effect. This is the case of a net settlement system, as all payments are batched by a clearing house, typically cleared at the end of the day and settled the day after.

44 https://www.bankofcanada.ca/core-functions/financial-system/canadas-major-payments-systems/

They are planned considering the liquidity incoming from counterparties: a single point of failure could wreck the planned liquidity allocation of the system. Yet, this configuration has advantages in terms of liquidity: payments are netted during the clearing process, meaning that banks have to allocate smaller liquidity than in a RTGS and just by the end of the day (Intraday Liquidity Management Task Force, 2000).

In a RTGS system instead, there is virtually no systemic risk, as payments are all carried out in real time with clearing and settlement happening simultaneously; thus, liquidity planning is not dependent on other parties' failures. On the downside, liquidity has to be allocated immediately when the payment takes place and in larger amount since they are not netted by amounts due from the counterparty. To support the liquidity management of all parties involved, RTGS system allows for overdrafts under certain conditions; for instance, the Fedwire[45] allows for intraday overdrafts, whereas other systems (BOJ-NET, TARGET2, CHAPS[46]) allow overdraft only against eligible collateral.

Conversely, CHIPS, LVTS and multicurrency CLS systems[47] have adopted modified versions of net settlement in conjunction with particular queuing arrangements, thus trying to maximize the extent to which payments can be netted (McAndrews and Trundle, 2001; Willison, 2005).

A typical interbank transaction happens as follow: each bank has a mirror account that represents its position with the national central bank; when a payment takes place between two banks (A and B) as a result of a customer request, bank A will debit payor account, credit its own mirror account at the central bank notifying the instruction of the payment. The central bank will then debit bank A's mirror account, credit bank's B one and further payment information. At last bank B will debit its central bank account and credit the payee account. The central bank is used as a settlement authority as it is trusted to fulfill its debts and even issue more currency if needed (Wüst & Gervais, 2017).

It is noteworthy that the use of RTGS systems for interbank payments requires a close connection of payments with monetary policy. Indeed, the policy interest rates are basically the prices that the central bank is asking to provide funds (liquidity) over the RTGS in the form of a reverse transaction the following day. In addition, the usage of RTGS systems requires a form of intraday liquidity, complementing the traditional overnight monetary policy (Kahn &

[45] The RTGS system operated by the Federal Reserve Banks in the USA.

[46] These are the RTGS systems of Japan, Eurozone, and UK respectively, operated by the qualified central banks.

[47] CHIPS (clearing house interbank payment system) is a secondary system used for non-time sensitive transactions and operated by the homonymous private clearing house; LVTS (large value transfer system) is the RTGS system of Canada, owned and operated by Payments Canada; CLS is an international settlement provider for the FX market.

Roberds, 2009). This is to highlight the relevance of the wholesale payment system: not only is it crucial for systemic risk mitigation, but it is also a tool for the enforcement of central banks' policies.

Yet, not all bank payments are immediately transmitted to the national RTGS system: actually, most payments are constituted by small account movements between bank clients (consider a credit card payment for a coffee). In this case, payments are managed as account movements between banks, or, if it is available, they are transmitted to a clearing house taking care of batching them and, when possible, netting them too.

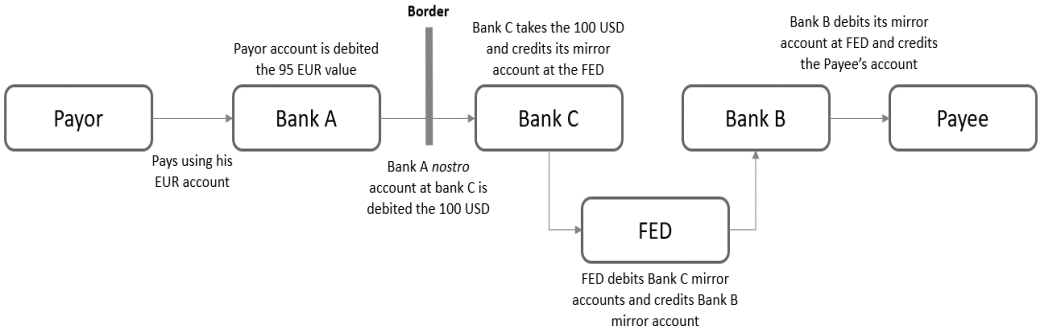


Figure 35, a representation of an international payment of 100 USD from a EUR bank account (adapted from Wüst and Gervais, 2017).

Interbank payments complexity increases for international payments as cross-currency operations are required. For instance, in a payment from Euro Area to the USA there is no central bank available to operate the settlement. Instead, at least 3 banks are usually involved (A, B and C): the bank of the payor, of the payee and an intermediary bank. Bank A has a dollar account (the *nostro* account) in bank C, which is called correspondent bank and is in charge of intermediating A dollar transaction. When the payor sends the payment, bank A debits his account, and credits the mirror account in bank C, implicitly buying dollars (or its own Euro account if dollars are already available in the mirror account; this allows transaction batching to some degree). Then a domestic interbank payment between C and B happens as described above, using the FED as a settlement authority.

5.2.2 Retail payments

The retail system is quite onerous due to widespread use of cheques. Anyways, increasing use of electronic payments is driving efficiency, and ATM or cross border credit card

transactions or ACH[48] payments are enabled to happen routinely. On the other hand, electronic payments are also raising the risks and impacts of frauds and loss of privacy (Kahn & Roberds). Retail payment systems provider are usually for profits firms which, as purveyors of information goods, are largely affected by economies of scale; thus, the industry is significantly concentrated (Varian, 1998).

The focus of the literature in retail payments is centered on the pricing when using credit or debit cards. The agreement on electronic system efficiency is widespread, but paper alternatives are often cheaper for merchants than card options. In fact, whereas the price for cards payment lays invisible to purchasers (due to no-surcharge rules), merchants are requested to pay fees to the card companies, called "merchant discounts". Furthermore, when cards are provided by associations such as MasterCard or Visa, an interchange fee is paid by the merchant's bank to the purchaser's which comprises a large part of the merchant discount (Chakravorti, 2003; Hunt, 2003; Rochet and Tyrole, 2004; Evans and Schmalensee, 2005; Rochet and Tyrole 2006).

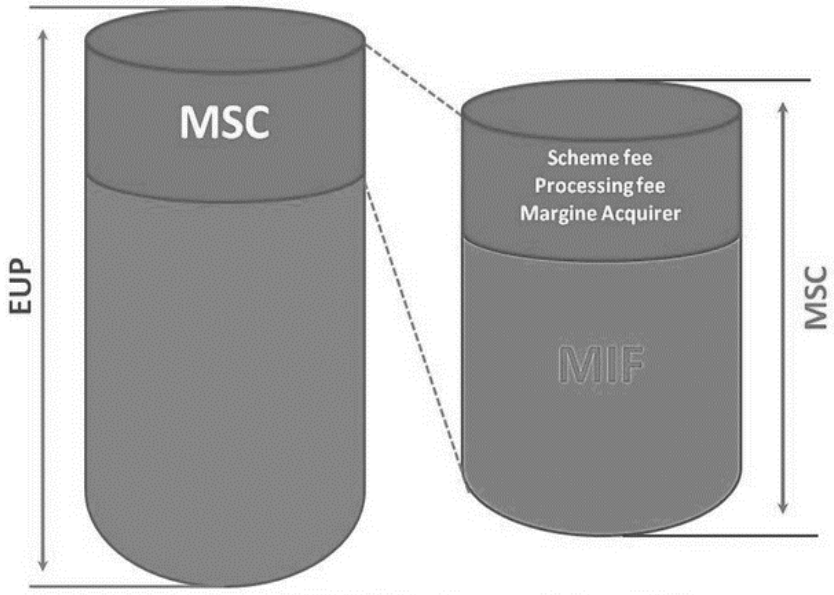


Figure 36, Representation of merchant service fees (including the multilateral interchange fee (MIF)) against end-user price ((EUP); (Garavaglia R.,

[48] Automatic clearing house payments, a global network to process digital payments as opposed to the traditional paper cheque system. A financial institution sends batched payments started from originators to the ACH network on regular intervals which are then cleared and settled by qualified institutions (e.g. Federal Reserve or The Clearing House in the USA) to the benefit of the receivers. ACH network is run by The Electronic Payment Association [https://www.nacha.org/ach-network].

https://www.pagamentidigitali.it/ecommerce/le-nuove-commissioni-dei-pagamenti-con-le-carte-capiamole-meglio

Anyways, a number of studies found increasing trends in credit card usage by consumers, and that many factors, such as income, age, and education, influence payment method choice (Gerdes et al., 2005; Klee, 2006; Mester, 2006;). The Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions (in conjunction with other regulations like PSD2[49]) is an example of effort by regulators to increase competition among payment service providers, and card issuers, forcing them to increase transparency in fees, imposing a limit on interchange fees (0.2 and 0.3% of the transaction value on debit and credit cards respectively), and easing requirements for new entrants. The ultimate objective is a reduction in merchant fees and the increase of digital payment acceptance. Authoritative studies found a positive effect of the regulation documenting an increase in card payment acceptance (measured as transactions per terminal) and a drop of merchant fees (Ardizzi & Zangrandi, 2018).

5.2.3 Money transfer

In this section, we consider money transfer which does not fall strictly under the definition of payment but uses similar channels to be carried out. We refer in particular to C2C (consumer to consumer) non-commercial transactions. Most of these payments are handled by newborn payment service providers, such as PayPal, which allow for instantaneous money transfer between their own accounts, whereas they recur to the ACH systems for external account transfer, e.g. credit an external bank account (Gonzalez, 2004). These platforms suffer from the walled-garden problem, i.e. it is impossible to achieve communication between one another, only money transfer within the same platform are possible. As an example, transferring money from PayPal to Alipay is impossible without recurring to traditional bank accounts. Despite efforts from companies to sign deals and allow inter-platform transfers, a truly seamless environment is still far (Higgins, 2017).

Further problems arise in the C2C transfer if we consider remittance. A remittance is the funds an expatriate sends to his or her country of origin via wire, mail, or online transfer. These peer-to-peer transfers of funds across borders are economically significant for many of the countries that receive them[50]. In 2017, the remittance flows amounted to $466 billion worldwide, considering only officially recorded data, that is global remittance likely exceeds

[49] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[50] https://www.investopedia.com/terms/r/remittance.asp

this figure by far. The abovementioned problems are caused by de-risking practice of many commercial banks: due to AML/CFT and KYC regulatory requirements, many institutions decided to dodge compliance risks by shutting accounts in countries or sectors posing serious risks in these regards. In fact, most remittance operations are carried out through third party agents, which make regulatory compliance and reporting a hard task. Thus, the transaction fees towards LMICs (low to middle income countries) remains very high, around 7.1% of the transaction amount, while the Sustainable Growth Target to be achieved by 2030 is set at 3% (World Bank Group, 2018).

5.3 Blockchain-enabled payments

Now, we are going to examine the results obtained from our empirical researches to identify possible BCT application in the payment service landscape.

Number of startups	Average financing	Total financing	Percentage of total
66	€ 13.518.445,15	€ 824.625.154	26,63%
Amount of news	**Operative**	**PoC**	**Percentage of total**
119	20	59	40.75%

Table 7 reports data for payments startups: the number of initiatives average financing received (in euros), total funds received (in euros), and the percentage of the funds received over the total. For companies, it reports the number of news for payment initiatives, how many of the projects are already operative, which are PoC and the percentage over the total amount of news.

The table above summarizes the results obtained from our databases. On the first line, the information regarding the startups are provided, while the data in the second one refers to the news we have registered. Concerning the startups, we inserted the total amount of money collected by all of them, both trough or without ICOs. This value has been used to calculate the average financing for each initiative, dividing it by the total number of startups. However, not all the startups disclose information regarding their collected funds, thus, we have also calculated the real average by subdividing the total financing by only those which revealed it. Referring to the second line, we have divided the number of news between the ones presenting already operative projects, the news describing Proof of Concept, and the remaining part refers to announcement of future activities. In both cases, the last column represents the percentage of startups/news which refer to a specific function over the total.

We can notice that 66 startups are currently focusing on payment-related services, accounting for 26.63% of the total. This is quite a high percentage; indeed, payment is considered one of the most promising area in which blockchain might be applied (Deloitte

Development, 2017). The average financing is quite limited with respect to the other areas we will analyze in the following chapters, considering that 28% of the total amount has been funded through ICO by nine startups (each of which has been granted €21.8 million on average) and that only five of them did not disclose funding. Of these initiatives, 39 propose solutions for P2P money transfers, especially for cross-border remittances. Moreover, 26 of them provide wallets in which cryptocurrencies can be held and used for payments[51].

On the other hand, the application of BCT in payments is the one with the highest number of related news, with a total amount of 119. BCT originally was born with the purpose to transfer value without the need for middlemen. Currently the major costs related to payments are due to the fees and the operations needed for transferring them through intermediaries, this way BCT is considered to be beneficial in the context. Among these pieces of news, 20 are already operative while 59 are Proof of Concept. Financial institutions are mainly testing the applicability of BCT in cross-border and wholesale payments, which nowadays results being costly and time consuming. Commercial banks are collaborating with startups on P2P solutions to favor remittance and financial inclusion of highly unbanked countries.

5.3.1 Areas of application

Following, we will provide a more detailed description of the possible application of BCT in payments, reviewed through our databases. In both cases we can conclude that BCT might bring benefits mainly in cross-border transactions, between different currencies, as the current process is time consuming and costly due to the presence of many intermediaries.

Among the startups, we have registered Lightning Labs[52]. The latter is studying the lightning network to improve the performance of the bitcoin transfers. We have already described it in the Chapter 3 of this dissertation as a solution to the limited network capacity. With it, two users can open an off-chain bilateral network between them by depositing a certain amount of bitcoin in an on-chain balance. This money can be exchanged between the parties as many times as they want until the network is open; no transactions are saved on the blockchain. Once they decide to close their network the last off-chain update of the balance will be registered on chain. The bilateral networks can be connected with one other, allowing exchange of value between two members off-chain, even though they are not directly connected with each other. This solution allows faster bitcoin transaction, as there is no need of waiting consensus every time.

[51] Remaining initiatives in different areas are either examined on a one by one basis or did not reported how blockchain was employed in their solution, so they are not discussed.

[52] https://lightning.engineering/

P2P value transfer is one of the initiatives which obtained more interested by startups (39 projects), but also by financial institutions, especially commercial banks. Many of them refer to remittances. Nowadays, making payment form one country to another requires the presence of many intermediary banks which allow the conversion of a local currency to the destination one. The number of these intermediaries grows a lot if we refer to developing countries. All these passages usually require many days and high fees to be paid, up to 12%, thus resulting in costly and time-consuming processes. Moreover, the Financial Stability Board (2018) found that, because of money laundering or terrorist financing, remittance is considered as a high risky sector by banks, which limits their operations, and are continuously closing bank accounts over the last few years. Cryptocurrencies are considered as a medium between two parties and if combined with BCT-based instrument, such as smart contracts, they can reduce the costs and the time required by remittances.

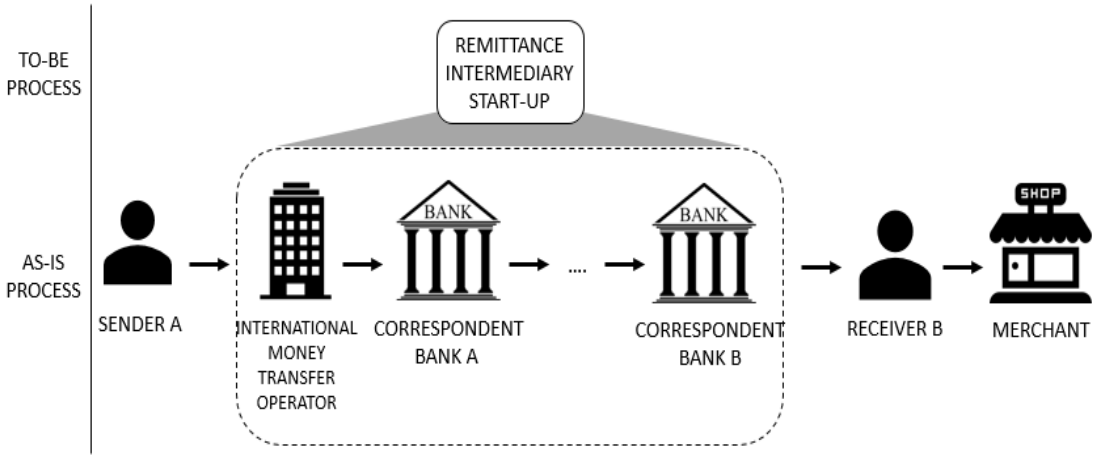


Figure 37, AS-IS and TO-BE cross-border remittance transfer process

Moreover, KYC and AML regulations can be met through the use of the BCT to validate individuals. Startups are proposing to be the only intermediary necessary to move funds from the sender to the receiver. The initial currency is indeed converted by the firm into bitcoin, as done by Rebit[53], or another proprietary token, as in the case of Bitpesa[54], then transferred to the destination and converted again into the local currency. In this way, the transfer no longer needs to pass through correspondent banks, saving in conversion, transaction costs and time. Costs are reduced to 1-3%, moreover, the to-be process will occur instantly. A proposal for safer remittance has been also advanced by Suremit[55]. The latter exploits a blockchain

[53] https://rebit.ph/
[54] https://www.bitpesa.co/
[55] https://sureremit.co/

instrument, the smart contracts, to ensure that the value sent will be used only for dedicated purposes, adding a greater level of security for the clients.

Many of the startups (26 projects) are developing wallets which allow their users to keep different currencies, both fiat and crypto ones. They allow for the exchange of value between peers, which can be individuals but even online shops, if the latter add the acceptance of cryptocurrencies as a payment option. Sometimes, these wallets are combined with cards, supported for example by Visa as in the case of the startup TenX[56], to support retail payments in physical shops through cryptocurrencies. Though a faster settlement period, the retail payments through cryptocurrencies have some limits which hinder their diffusion. As also mentioned in a report by JPMorgan (2018), crypto retail payment requires two conditions to be a widespread solution: being trusted and being accepted and used by both merchants and buyers, both of which are not met by cryptocurrencies. Concerning the former, the lack of trust is due to their volatility, which do not ensure merchants to obtain the same sum of money requested in the moment of the order when receiving them. To overcome this problem, startups and firms are now trying to develop different solutions: on one hand, they ensure the receiver to fix the price of the product to the exchange at the moment of the order, on the other hand they are trying to create what are known as stable coin which are not subject to volatility as cryptocurrencies. The second above mentioned big issue which has to be solved is the adoption cycle, which means that both the merchant and the client should accept the same payment method to use it. However, merchants do not prioritize cryptocurrencies acceptance due to the niche of clients who use them, thus consequently limiting the consumer adoption. Another hassle perceived by merchants is the lack of regulation regarding cryptocurrencies as a medium of payment.

A third problem is the transaction cost related to cryptocurrencies payments. Currently, for example, a bitcoin transaction costs around 50 eurocents, while an Ethereum transaction can exceed this cost but it ultimately depends of the kind of transaction (toward/from a smart contract, to an address, etc.).

As we have seen, the main problem of P2P money transfer is the need for both the sender and the receiver to own the same wallet. In the last years, several different proposals have been introduced into the market. Thus, individuals should own a plethora of different wallets, both in the case of fiat- and cryptocurrencies, to be sure they can exchange money with anyone. The startup Circle through its CENTRE product is intended to solve this issue by providing a solution which can connect different wallets together, as we can read form its whitepaper: *"CENTRE enables crypto exchanges and wallets around the world to interoperate. By exchanging price-stable tokenized value using a standard protocol across blockchains and*

[56] https://tenx.tech/en/

fiat rails, and it enables those wallets to leverage services for compliance, identity, and risk management via well-defined interfaces for service providers which plug into the network. The technology provided by CENTRE supports tokenized fiat money through asset-backed stable coins and enables high transaction throughput by employing optional state channel implementations." (Centre, 2018).

Centre is a platform leveraging the blockchain in order to connect wallets which are not integrated with one another and which do not share common currencies. Following, an example of how Centre works:

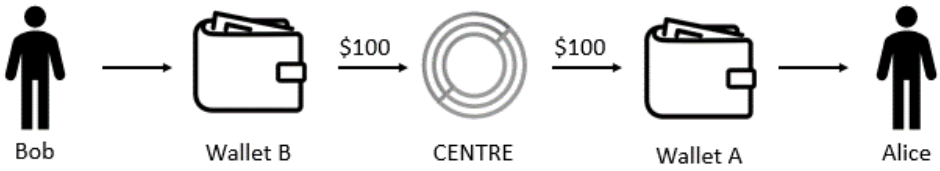


Figure 38, Centre inter-currency P2P payment

Bob in India uses Paytm and wants to send the equivalent to $100 to Alice, who instead uses Vipps. These two wallets' bank account receive money respectively from Bob's bank account and Alice's one. The money is therefore digitally hold in the wallets. The latter define prior to the beginning of the transactions an exchange rate between the fiat coins and the stable Centre coins. When Bob sends a request for payment to Alice, Centre exchange Bob's fiat currencies into Centre's stable coins, which are instantly transferred to Vipps and exchanged into Alice's fiat currencies. The latter are charged in Alice's wallet in few seconds. During the process, identity checks and validation are performed so that if any control fails, the transaction is aborted before any transfer of value occurs. This way, P2P cross-border payments are highly facilitated, eliminating the need for many intermediaries through bank transfers, instead allowing the interoperability among digital payment providers.

A similar approach has been used by IBM with Stellar in IBM World Wire[57] to connect financial institutions and to allow instant messaging, clearing and settlement of transactions. They do not require correspondent banks as intermediaries, speeding up the process and reducing its associated costs. The banks have to connect to the IBM system. The sender has to define the initial and the final currency in the transfer and the digital asset it wants to use as an intermediary. Once the transaction begins, the initial currency is converted into the digital asset which is then converted into the final currency. As we read in the IBM whitepaper (2018): "*It all takes place in a matter of seconds and is immutably recorded onto a blockchain for clearing*".

[57] https://www.ibm.com/blockchain/solutions/world-wire

Ripple[58] is also threatening Swift allowing a direct transmission of the transfer without the need of initial messaging through Swift. Not only does it exclude the messaging provider, but also, as done by IBM, the Foreign Exchange Providers, allowing a seamless process between the parties. Other initiatives come worldwide from central banks. They are mainly studying with the support of big consultancy firms, such us Deloitte, Accenture of Price Waterhouse Cooper, the applicability of BCT for the wholesale payment process.

Central banks developed 11 projects since 2016 which explored blockchain adoption, as we can see from Figure 39. These projects are strictly related to one another as the results of one bank are used as an input by another one to further advance the studies. One topic of the studies is the applicability of the BCT for interbank large value transfers in the Real Time Gross Settlement system, in which each bank represents a node of the chain. Many of the currently available blockchain platforms have been tested to prove their performance and their compliance with the requirements needed by the financial processes. Ethereum is not a possible solution as a permissionless platform as it does not allow either privacy or scalability through a Proof of Work mechanism, though providing resiliency as there is no single point of failure.

The Proof of Concepts which applied permissioned version of the blockchain instead show the capacity to sustain the current volume of RTGS transactions of the banks, by moving away from a Proof of Work consensus mechanism. Without the latter, the finality of the transaction is no longer probabilistic, but it is determined thanks for example to the introduction of a validator node in the network, in the form of a notary, as done in project Jasper phase II. This choice compromises the resiliency, introducing a single point of failure in the decentralized platform. Other trade-offs have been encountered in subsequent trials between for example privacy and speed/scalability in respectively project Stella I and Ubin II. The Liquidity Saving Mechanism has also been tested on the BCT, with positive results. The latter goal is the improvement of the coordination of incoming and outgoing payments to support the efficient intraday flow of payments. Among the platform, Corda has been the only one not presenting scalability concern, which instead have been encountered with Hyperledger Fabric due to its bilateral channels and with Quorum, whose Zero Knowledge Proof slowed down the process.

One of the big challenges of the wholesale payment with respect to retail and corporate transaction is the liquidity management. Therefore, some of the central banks have studied a system to perform liquidity savings through decentralized netting. It has been proposed for all those payments in which the sender is willing to accept settlement delay in favor to liquidity savings. At first, project Jasper II proposed a solution which still relied on a centralized design, through a notary node. The process consists of two phases, the inhale and exhale phase. During

[58] https://ripple.com/

the former, all the nodes pay the notary node just before the netting algorithm runs. In the latter phase, the algorithm returns to the participants their net balances. The other experimentation has been performed by project Ubin, which used the LSMs to solve gridlocks. The latter occur when a participant of the system does not have sufficient funds to fulfil its obligation. Different solutions have been tested suing Hyperledger, Quorum and Corda; the latter could perform the highest level of decentralization in the gridlock resolution process. Nevertheless, the results showed that a truly decentralized design is unlikely to be developed as it hardly supports stressed scenarios.

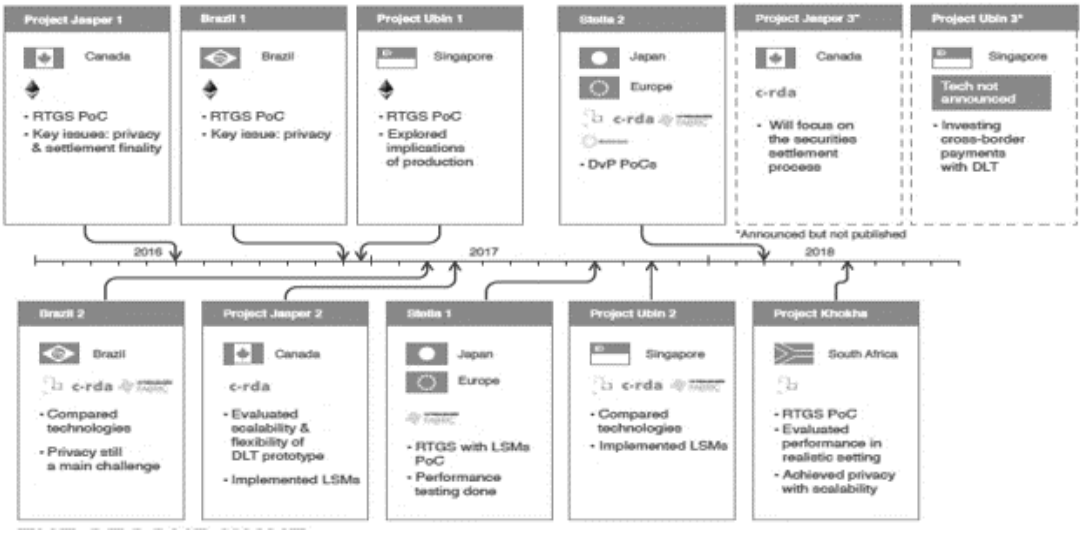


Figure 39, Central Banks BCT projects since 2016 (from Project KhoKha Whitepaper, 2018)

Another application of the BCT has been tested to allow intraday and real time liquidity management of *nostro* accounts. As mentioned in the Swift report (2018), "*34 % of the cost of an international payment is related to Nostro trapped liquidity caused by the absence of real-time data to optimize intraday liquidity management*". The purpose of the Proof of Concept developed by Swift in collaboration with other 34 banks is therefore the resolution of this problem: to evaluate if the applicability of BCT can lower trapped liquidity and thus decrease its related costs by real-time reconciling the Nostro account. With real-time data about transactions, banks may avoid both over funding and over usage of liquidity, thus ensuring better client experience through quicker payments.

The tests, which was conducted in Swift sandbox, showed the expected real-time liquidity monitoring and reconciliation. Nevertheless, the overall results were not satisfying. To be applied in real-life, some stringent requirements must be met, which unlikely will occur. First, all Nostro account services have to shift from batch to real-time liquidity reporting and processing. Moreover, all banks should upgrade their back-office applications to be able to

provide real-time updates to the platform. Two conditions which will hardly occur soon. Today only 44% of cross border payments over Swift are indeed confirmed in real time (Swift, 2018), thus this kind of change as well as the applications upgrades require great investments to be done. Another result was the strong dependency of the technology on existing capabilities and business models. Again, to obtain a widespread adoption, all institution should follow the same value proposition and should re-engine their existing system for monetary movements. A necessity which is extremely limiting as it imposes a massive change of the current state. A fourth problem is generated by the design of the system, made of bilateral channels between a member and every other parties, for privacy and consensus reasons. With the increase of the participants, the number of channels will increase exponentially, generating performance hassles.

Andreas Hauser, senior business product manager for intraday liquidity management, cash management at *Deutsche Bank,* discussed his opinion regarding the PoC and revealed that *"from our viewpoint the project revealed that what really drives value for Nostro real-time liquidity monitoring and reconciliation isn't the blockchain technology itself. For example, real-time monitoring and reconciliation can similarly be achieved by connecting the proprietary systems of provider and user via APIs"*[59].

Concluding this section, we can assume that BCT application in payments achieves improvements in cross-border payments between different currencies, as it can cut down both costs and time with respect to the existing systems. Moreover, it can allow higher financial inclusion of developing countries, given the possibility to transfer remittances in an easier way. Both startups and existing firms are focusing on this field, the former from a P2P point of view, while the latter both for commercial as well as for wholesale value transfers.

5.4 Investment products

An investment product is a product offered to investors based on an underlying security or group of securities that is purchased with the expectation of earning a favorable return.[60] Therefore, the study of investment products and related literature implies that of securities, and the institutions responsible for associated operations, that is, depository institutions, insurance companies, finance companies, and securities firms (Saunders and Cornett).

Securities can be classified in 3 major categories:

[59] https://www.bankingtech.com/2018/05/swift-blockchain-test-promises-bank-benefits-but-one-size-does-not-fit-all/

[60] https://www.investopedia.com/terms/i/investment-product.asp

1. Equity, representing the ownership interest held by shareholders in an entity (a company, partnership or trust), realized in the form of shares of capital stock, which includes shares of both common and preferred stock. Equity securities do entitle the holder to some control of the company on a pro rata basis, via voting rights.
2. Debt, corresponding to borrowed money that must be repaid, with terms that stipulates the size of the loan, interest rate and maturity or renewal date. They include government and corporate bonds, certificates of deposit (CDs) and collateralized securities.[61]
3. Derivatives, whose value is derived from an underlying asset, typically, stocks, bonds, commodities, currencies, interest rates and market indexes.[62]

The borders of these categories become thinner as we consider hybrid instruments such as convertible bonds, equity warrants or similar products. The Advisory Group on Market Infrastructures for Securities and Collateral (2017) defines processes related to security trading as: issuance, clearing and settlement, asset servicing, collateral management, and regulatory compliance.

5.4.1 Issuance

In a typical issuance arrangement, a corporation approaches an investment bank indicating that it wants to raise a certain amount of finance in the form of debt, equity, or hybrid instruments such as convertible bonds. The securities are originated complete with legal documentation itemizing the rights of the security holder. A prospectus is created outlining the company's past performance and future prospects. The risks faced by the company from such things as major lawsuits are included. There is a *road show* in which the investment bank and senior management from the company attempt to market the securities to large fund managers. A price for the securities is agreed between the bank and the corporation. The bank then sells the securities in the market (Hull, 2008).

First, the sale of securities requires their registration in the books of a CSD (Central Security Depository). The operational process whereby a security is made eligible within an issuer CSD includes the introduction of the new security in the securities database of the CSD. The database should include the following mandatory information: International Securities Identification Number (ISIN) of the financial instrument; Legal Entity Identifier (LEI) of the issuer; other securities reference data that are required for validation of settlement instructions, reporting and securities lending (either optional or mandatory according to CSD

[61] https://www.investopedia.com/terms/s/security.asp
[62] https://www.investopedia.com/terms/d/derivative.asp

rules) such as: short name, long name, classification of financial instrument, country of issuance, currency denomination, issue date, final maturity date (where applicable), settlement type (e.g. face amount or units), minimum settlement (where applicable) and settlement multiple (where applicable). The recording of the issuance in book entry form is usually performed using an issuance account, which introduces the securities into the intermediated holding chain. The issuance is represented by the debit balance of the issuance account that records the exact number and amount of securities issued and made available in the settlement system.

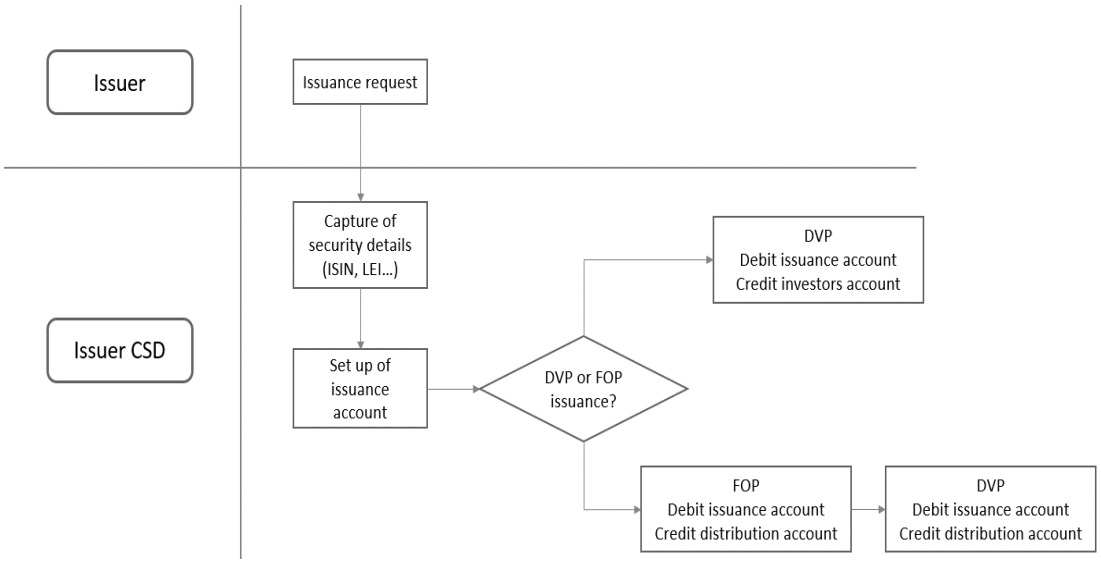


Figure 40, a representation of the issuance process (adapted from the Advisory Group on Market Infrastructures for securities and collateral, 2017).

The balance of issuance could be updated as result of a corporate action that increases or decreases the amount or the number of securities of the issue (e.g. capital increase/reduction, bonus issue, redemption, merger, stock split, etc.) through the processes of mark-up and mark-down.

Finally, the securities are credited to investors account following two alternate operational models. In the first model, securities are debited directly on the issuance account and credited on the account of the participant. The corresponding cash movements to the issuer (if any) are settled on a delivery versus payment (DvP) basis by using a cash account associated with the issuance securities account. Under the second model, securities are transferred free of payment (FoP) from the issuance account to a distribution account, and only then between the distribution account and the investors' account, again on a DvP basis. This process is usually carried out if the issuer appointed an intermediary for securities distribution, so, the

distribution account is opened in his name (Advisory Group on Market Infrastructures for securities and collateral, 2017).

5.4.2 Clearing and settlement

As seen above, after the issuance process is completed, clearing and settlement processes take place to finalize the actual transfer of assets ownership from issuance or distribution account to investors account, or from investor to investor accounts for secondary market trades.

The importance of an efficient securities settlement system lies in the safer transfer of ownership of assets against payment. The significance of settlement derives from the fact that it must be viewed as a subset of transaction costs facing an investor in effecting a trade. Such systems must be developed in a way to minimize the risks involved in securities transactions and it must offer lower costs, which do not hinder the intention to trade securities (de Cavalho, 2005; van Cayseele and Wuys, 2005).

A definition of clearing is provided by de Cavalho (2005): clearing of a securities transaction confirms the legal obligation from the trade. Clearing involves the calculation of mutual obligations of market participants and determines what each counterpart receives. Clearing houses, CSDs, or international central securities depositories (ICSDs) are the providers of clearance.

The clearing process could be overtaken by a central counterparty (CCP), a service offered by clearing houses. A CCP is an entity that interposes itself between the transactions of the counterparties in order to assume their rights and obligations, acting as buyer to every seller and seller to every buyer. The original legal relationship between the buyer and the seller is thus replaced by two new legal relationships: between the CCP and the buyer and between the CCP and the seller. The substitution of the original counterparty by a new contractual counterparty is called a contract novation. Thus, the CCP takes over the counterparty risk and guarantees the clearing and settlement of the trade (Kroszner, 1999; 2004).

A different approach is adopted by CCP for derivatives, as the clearing process lasts until the settlement of the derivative product on its maturity date. A derivatives CCP collateralizes, or *margins*, the financial performance exposure that the CCP has to each of its clearing members. This is called performance bond collateral, and it is based upon the historical price volatility of the instruments, multiplied by the number of open (unliquidated) positions that a clearing member has with a CCP. By setting the performance bond collateral requirements at levels that anticipate a likely one-day market (price) movement, a CCP should have any potential liquidation risks reasonably well collateralized before the fact. Should a clearing

member fail to satisfy its financial obligations to a CCP, that CCP would declare the clearing member to be in default and would transfer or liquidate its positions, liquidate the relevant performance bond collateral, and apply the proceeds to cover the costs of liquidation. Should the costs of liquidation exceed the proceeds of the performance bond collateral, any residual loss would be covered by the very substantial financial assets held in reserve. Clearing members satisfy their performance bond (initial margin) collateral requirements by depositing eligible assets (which are largely composed of cash, governmental Treasury securities, and equity securities) with the CCP (McPartland, 2009).

For a definition of settlement, we refer to Schaper (2007): settlement is the exchange of cash or assets in return for other assets or cash and transference of ownership of those assets and cash. A CSD is the organization that performs these functions. Some post-trade services are not related to a securities transaction but are needed on an ongoing basis to administer securities on behalf of the owner. The process of settlement is typically linked with custody and safekeeping.

A description of the clearing and settlement process is carried out in a report by The Giovannini Group (2001). It starts after a securities trade has been executed and can be divided into 4 operations:

1. **Confirmation** of the terms of the trade as agreed between the buyer and seller. For centralized exchange this operation is usually automated and electronic, based on data submitted by the counterparties. Instead, for OTC transactions confirmation is reached directly between the buyer and the seller by electronic means; in this latter case efforts are under way to reduce complexity and minimize errors to limit the number of times information need to be communicated between various participants.
2. **Clearance**, by which the respective obligations of the buyer and seller are established. As said, it is carried out by a CSD, a clearing house or an international CSD (ICSD). As for payments, clearance can be carried out on a gross or net basis. When clearance is carried out on a gross basis, the respective obligations of the buyer and seller are calculated individually on a trade-by-trade basis. When clearance is carried out on a net basis, the mutual obligations of the buyer and seller are offset yielding a single obligation between the two counterparties. Accordingly, clearance on a net basis reduces substantially the number of securities/payment transfers that require to be made between the buyer and seller and limits the credit-risk exposure of both counterparties. A netting facility is generally provided by a CCP; it offsets all obligations and reduces all

outstanding residuals to a single debit/credit between itself and each member (rather than a multiplicity of bilateral exposures between members).

3. **Delivery**, requiring the transfer of the securities from the seller to the buyer. Securities are nowadays dematerialized, and their transfer happens in the form of digital book entry updates, i.e. by updating investors (or issuer if the transaction takes place in the primary market) accounts held at the CSD or ICSD.
4. **Payment**, requiring the transfer of funds from the buyer to the seller.

Delivery of securities and payment of funds may occur simultaneously but only when both delivery and payment have been finalized is settlement of the securities transaction achieved. Settlement procedures that only allow securities to be transferred to the buyer on condition of payment being received by the seller are known as 'Delivery versus Payment' (DVP); this method of transfer implies a settlement on a one-by-one basis, only by resorting to a CCP's netting facility can securities be traded on a net basis. In a 'Free of Payment' (FoP) transaction, securities are exchanged against other securities and no payment is carried out. Often, settlement finality can be assured only after the transfer of securities ownership from the seller to the buyer has been formally registered (Mills and Nesmith, 2008). Many CSDs offer registration as an additional service.

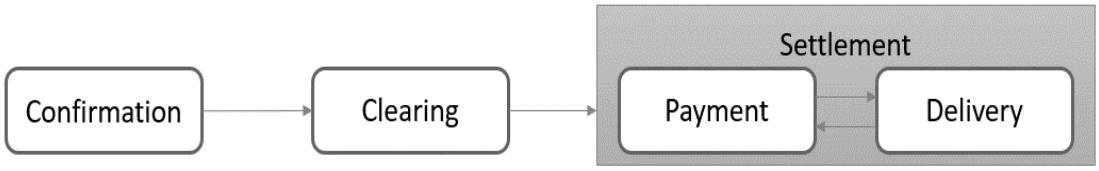


Figure 41, clearing and settlement process (adapted from The Giovannini Group, 2001)

Despite the linear representation above, the operational clearing and settlement process is quite complex and involves many intermediaries. Further complexities are introduced if the transaction happens in an international context.

To show this, let us consider e.g. a trade of a domestic equity share. In this example, the investor initiates the trade through his usual broker (1). The broker (1) will seek a counterpart broker (2) on the local stock exchange. If the facility is available, the trade may be novated to a CCP. The investor will use his custodian (B) to interact with the national settlement system and the national cash clearing system, typically the central bank.

Concerning foreign operations, the whole process is complicated by a number of factors, such as the absence of a common currency, requiring a Forex transfer, and the need to resort to foreign brokers and intermediaries to carry out the trade. The actors involved in a cross-border equity transaction are the investor who initiates the trade via his usual local broker (A)

and settle it through his local custodian (B). In this example all three of the actors are located in the same country. As the equity trade takes place in a foreign country, local broker (A) will use a foreign-country broker (1), who will seek a counterpart broker (2) on the foreign-country stock exchange. If the facility is available, the trade may be novated to a CCP. The local broker (A) will need a foreign-country custodian (Y) and a foreign-country cash clearer. The local custodian (B) will need a foreign country custodian (X) as well and yet another cash clearer. The national central bank of the foreign country may be involved in the cash leg of the trade settlement. We can conclude that clearing and settlement of securities are complex processes that involve a large number of players beside buyer and seller, and, despite difficulties in computing transaction costs, evidence from the literature agree that foreign transactions are more expensive than domestic ones, due to the increasing number of intermediaries (van Cayseele & Wuys, 2005; Schaper, 2008; The Giovannini Group, 2001). As well, time to finalize these operations are long and constrained according to regulation so that all participants are aligned and reconciliation of all separate database storing account information can take place.

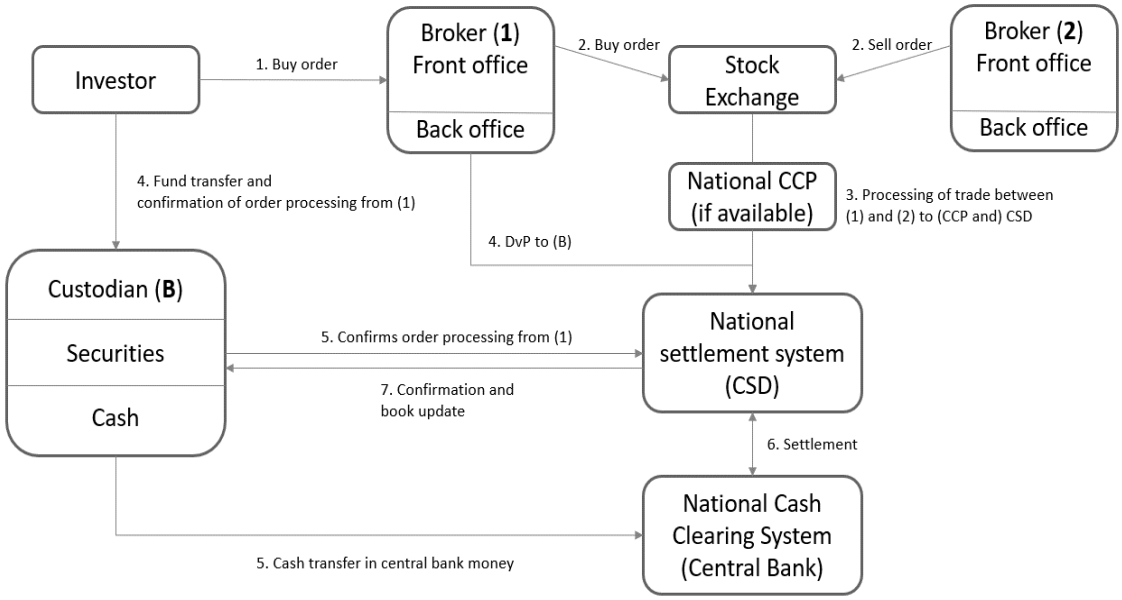


Figure 42, operational clearing and settlement in a domestic equity transaction (adapted from The Giovannini Group, 2001)

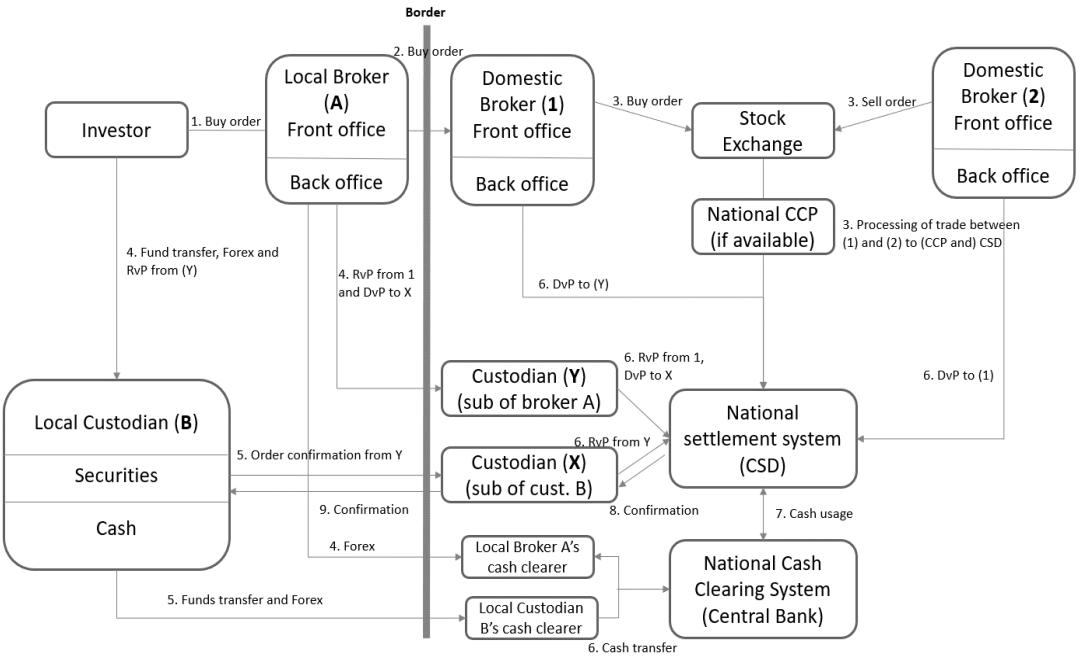


Figure 43, operational clearing and settlement in an international equity transaction (adapted from The Giovannini Group, 2001).

Depending on the product traded, time for settlement can span from T+1 to T+3 (Chiu & Koeppl, 2018). A response to these kind of issues in international trading was given by the EU commission which launched Target2-Securities (T2S), a centralized gross settlement (or DvP) system for the European securities, which settles transactions directly in central bank (ECB) money. The main objectives of T2S are cost reduction in European cross border trades as they used to be up to 10 times higher than domestic ones; increasing market integration and process standardization across EU; facilitate collateral and liquidity management for international banks operating in the EU (instead of assessing collateral and liquidity for each country, a pan-European view is enabled).

Before 2008, many processes were duplicated, and the market was fragmented in national security depositories keeping their own securities account and resorting to TARGET infrastructure to perform payments and allow for a DvP. With the introduction of TARGET2 (T2), the new RTGS settlement system operated by the ECB, all cash accounts were centralized in the ECB and access was granted to any CSD in the EU. Then, since 2008, even securities accounts were centralized in a common platform at the ECB, thus allowing CSD to communicate transactions on the T2S platform and obtain settlement by the end of the day in central bank money. However, many central banks in other countries reject this system as they are not willing to let private institutions (the CSD) control payments in central bank books. Nonetheless, the result of T2S was an effective cost reduction of European cross-border

transaction from 0.45€/2.30€ (minimum and maximum) of a foreign transaction to a fixed 0.28€ per transaction (Schaper, 2008).

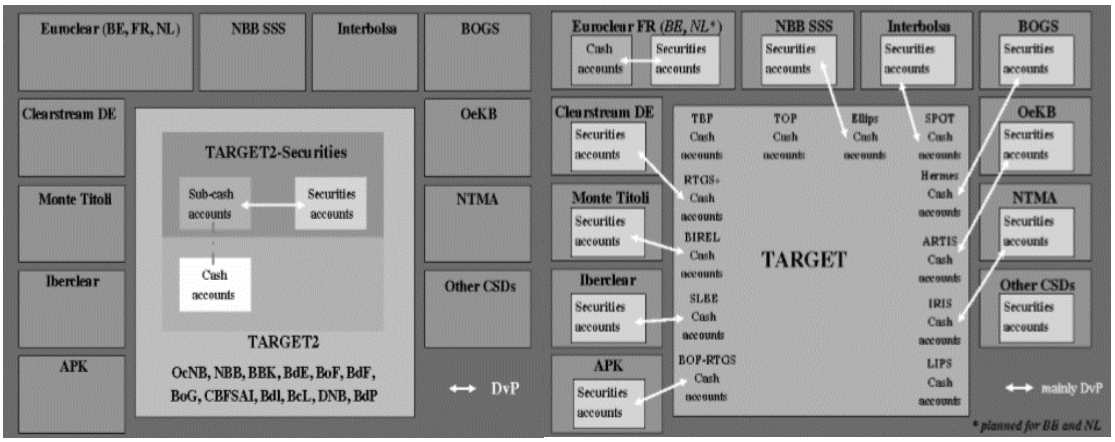


Figure 44, a comparison of T2S market infrastructure (left-hand-side) with pre T2 and T2S market infrastructure (right-hand side. From Schaper, 2008).

Despite the efforts, settlement times and costs are still relevant for domestic and EU transactions, and very high in international (i.e. inter currency) transactions.

5.4.3 Asset servicing

Asset servicing is an activity involving all the actions required to manage securities when held at an intermediary: custody services and related corporate action processing, tax processes, registration processes, shareholder identification processes and general meeting processes as well as value added and ancillary services[63]. Typically, asset servicing involves a large set of intermediaries. Actions are taken by the issuing company, handed over to its CSD, passed on to the many investors CSD, and finally handed down to investors. Instructions are still transmitted by fax and a fragmented IT infrastructure hampers reconciliation and makes procedures prone to errors[64]. The Advisory Group on Market Infrastructures for Securities and Collateral identifies 3 groups of actions an issuer can take (a.k.a. corporate events).

1. **General Meetings**: this process starts with a notification from the issuer to all investors, be them bond or securities holders (in the respective bondholders or shareholders meetings). Instructions can be of voting by attendance, correspondence or proxy voting. However, the instructions sent by investors to

63 https://www.ey.com/Publication/vwLUAssets/New_opportunities_for_asset_servicing/$FILE/ey-new-opportunities-for-asset-servicing.pdf

64 https://www2.deloitte.com/global/en/pages/financial-services/articles/asset-servicing.html

the general meeting need to be validated according to the CSD securities accounts: for instance, votes need to be weighed based on the number of shares held by each investor.

2. **Distributions**: these are cash or securities paid by the issuer to the investors, according to their rights. Independently of the means of payment, the process is the same: the issuer announces the distribution at least two business days before the ex-date[65], the record date follows the ex-date by at least a settlement cycle minus one business day, and the payment date should be the closest as possible to the record date, preferably the next business day. More complexities come up in case the distribution is associated with other instruments such as options.
3. **Reorganizations**: these corporate actions entail the redemption of a securities and the issue of a new one against a payment to the investor. Here, too, the sequence starts with an announcement, a last trading date is set, as well as a record date and finally a payment date. There could be also voluntary reorganizations including options that might include even a tender date and lengthen the overall process.

5.4.4 Collateral management

Collateral is a property or other asset that a borrower offers as a way for a lender to secure the loan. If the borrower stops making the promised loan payments, the lender can seize the collateral to recoup its losses. Since collateral offers some security to the lender should the borrower fail to pay back the loan, loans that are secured by collateral typically have lower interest rates than unsecured loans[66]. In this section, we examine how securities can be used as collateral, especially to reduce credit exposures in the derivatives market and in central bank lending (marginal lending facility).

Margin calls may happen if the value of the posted collateral falls below the agreed threshold: in this case further collateral needs to be posted in order to meet the minimum maintenance margin. Similarly, if the value of the collateral becomes larger than the requested amount, part of it can be released from the agreement and becomes available to the owner for sale or for other collateral agreements[67].

According to Chen et al. (2017), following the financial crisis of 2008, market authorities are pressing for an increasing usage of collateral, especially in the non-cleared OTC derivatives

[65] The ex-date is the date on which the seller, and not the buyer, of a stock will be entitled to a recently announced dividend (Investopedia).
[66] https://www.investopedia.com/terms/c/collateral.asp
[67] https://www.investopedia.com/terms/m/margincall.asp

market: here a credit support annex (CSA) provides all standard terms that apply to all the transactions entered by involved counterparties (Zapada, 2013).

If the literature is unanimous on the effectiveness of collateral (Bliss and Kaufman, 2006; Cherubini, 2005; Gosh et al., 2008; Gregory, 2010), new risks arise in collateral usage, such as operational, liquidity and market risk. These risks are attached to the collateral posted, e.g. an illiquid collateral may prove hard to recoup in case of borrower default; especially in the case of securities as collateral, market risk is well present with price oscillations that may cause a drop in the value of collateral, making it unfit for the coverage of the principal; finally, an optimal management of the collateral is undermined by procedural and similar errors (Chandrashekar, 2008; DTCC, 2014). Portfolio reconciliation tools enable participants to evaluate risks by reconciling positions and calculating the exposure of the trade, these are the basis for a subsequent margin computation. Then, margin calls need to be matched between supply and demand side, managing any possible dispute arising from claims on the valuation process.

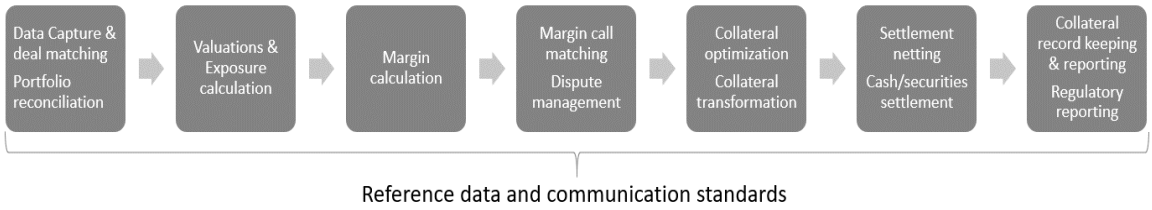


Figure 45, Typical functions of the collateral management process (adapted from DTCC, 2014).

The amount of collateral posted can be optimized by pooling it to meet various exposures, and allocating it efficiently, depending on price, risk, liquidity and financing costs. Another form of management is collateral transformation, that is, trading ineligible collateral for an eligible one: e.g. if securities are the only form of collateral available, but the agreement only accepts cash as collateral, the transformation entails the sale of securities to obtain the cash amount to post. The following step, netting and the actual settlement of collateral (restitution or transfer) is becoming increasingly complex as collateral is placed in segregated accounts (separate from the brokers' accounts) and transactions are settled among these accounts: their increasing number and a lack of common regulation across countries makes settlement difficult. Reporting is another crucial aspect and has to be communicated under common standards, which is currently not happening, forcing firms involved to put effort in data harmonization. The key inputs to achieve efficiency are communication standards, such as standard messaging platforms to communicate calls and common settlement platforms, and a good quality reference data which is used to compute e.g. the value of the collateral posted, and, if the source is not unequivocal, it often leads to disputes (DTCC, 2014).

5.4.5 Regulatory Compliance

Lastly, a compulsory activity in the post-trade environment is that of reporting. In Europe, EMIR[68] requires reporting a wide set of data about derivatives transactions, as well as counterparty information on the institution conducting the transaction and data on collateral. Also, this data has to be updated several times during the lifetime of the derivative, and repeatedly reported every time it happens. Other regulations (MiFID II, MiFIR, and SFTR) request more data on the trading activities conducted or managed by financial institutions.

According to the Advisory Group on Market Infrastructures for Securities and Collateral (2017), much information provided entails long and manual procedures: for instance, the liquidity coverage ratio (LCR) is often included in reports to ensure that banks have sufficient amounts of high-quality liquid assets and can face economic stress. To compute that indicator and other similar parameters, data is often pulled from isolated database infrastructure, manually reconciled, and only then is the ratio computed and reported. The process gets even more complex as the number of parties involved in transactions increases: data might have to be reconciled from companies' ERPs systems, CCPs' database, banks' database; then, a set of business intelligence tools is applied by each of the interested parties, replicating the effort, and only now it is reported. Therefore, different access control of the various systems where data is stored can hinder smooth reporting procedures.

5.5 Blockchain-enabled investment products

Having explored the vast area of services that are involving investment products and thus securities trading, we shall now examine how blockchain could improve procedures for each of the services described in the previous section. From our database, it results that this area is the most crowded in both startups companies and institutional initiatives. There are 114 startups in this field, with 71 of which reporting received funds for an average of €24.3 million, and the highest total in financing, with €1.7 billion received.

The main focus of startup companies is on exchanges: 64 of these companies allow the purchase and sale of cryptoassets. A set of 26 companies then offers services to both private and institutional investors, proceeding to asset tokenization, smart contracts design for structured product creation and investment platforms for such tokenized assets. The

[68] European regulation targeting the reporting requirements for CCP and over-the-counter derivative contracts; https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012R0648

remaining 24 are engaged in compliance requirements for cryptoassets, advisory, and real estate investments.

Number of startups	Average financing	Total financing	Percentage of total
114	€ 24.265.657,20	€ 1.722.861.661	55,64%
Amount of news	**Operative**	**PoC**	**Percentage of total**
85	5	43	29,11%

Table 8 reports data for investment product startups: the number of initiatives average financing received (in euros), total funds received (in euros), and the percentage of the funds received over the total. For companies, it reports the number of news for investment product initiatives, how many of the projects are already operative, which are PoC and the percentage over the total amount of news.

Concerning firms, 85 initiatives were found, with 43 PoC and 5 operative platforms, accounting to 29,11% of the total. All these 48 initiatives tested blockchain for investment products issuance, trading and settlement, from equity, to bonds, to asset-backed securities. All of them reported very successful results in the speed up of the settlement process, the streamlining of data for regulatory compliance, and the automation of most asset servicing procedures.

To describe blockchain-enabled processes in the following section, we also reference to relevant industry reports (Oliver Wymann, 2016; Pinna, 2016; Advisory Group on Market Infrastructures for Securities and Collateral, 2017).

5.5.1 Areas of application

As we mentioned, the focus of startups is on exchanges[69]. These platforms are very similar to regulated markets, in that they allow trading of cryptoassets in an orderly manner, communicating prices of various assets to investors, and recording bid-ask spreads in their book. The fundamental difference is that cryptoassets are public as they are present in public blockchains, thus they are not held at a custodian bank, and a CSD is not needed to set up accounts for the issuance process. Indeed, to issue a cryptoasset one needs to create a new protocol and set up new nodes, if a new coin is created, or pick a programmable coin and create a smart contract allowing the creation of new tokens (such as for Ethereum with ERC-20 tokens) which can be then sold through an ICO (Initial Coin Offering). The issuance process is regulated in few countries: in Europe, only Switzerland[70] and Estonia[71] differentiate the rules

[69] Such as ADAX, Coinbase,Kraken, Binance, OKEx, Huobi, Bibox etc.
[70] https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/
[71] https://www.fi.ee/index.php?id=21662

cryptoassets have to comply with by the function they serve. They both divide tokens in payment, utility, and asset tokens; of these, only asset tokens are considered as securities and imply the release of a prospectus, and KYC procedures when selling to investors. Payment tokens are considered as money, and their only use is as a means of payment or value transfer. Utility tokens serve to provide access to an application or a service based on a blockchain infrastructure. Asset tokens represent assets such as debt, equity or change their value based on an underlying asset, so they are derivatives. They are assimilated to uncertificated securities (or rights) for which the only requirement is to maintain a book with details on the number, denomination, and the creditors are recorded; regulators recognize that these requirements can be achieved digitally by a blockchain. The only issue with asset tokens is that the creditor has to be recorded, so the exchange is responsible for communicating to the company the identities of the parties transacting, somewhat increasing the complexity of the process, and increasing the costs because of KYC requirements.

Yet, trading becomes much simpler: instead of exchanging messages between various institutions (CCP, CSD and custodian), the settlement is instantaneous and operated by the blockchain protocol, as for payments, while the DvP procedure is taken care of by the exchange itself, as cash is deposited on the exchange account, or a credit card is linked to it, and it is then used to allow the payment. So, the whole process happens directly between two investors, and no other intermediaries beside the exchange are involved, either in national or international trades. Transactions also comply with law as long as KYC requirements are respected by the exchange which has to collect identity information of its customer while financial ones are managed by banks, as moving cash in and out of the platform is linked with the user's bank account. This way, the investors trading can be identified, and KYC/AML procedures are respected. Startups offering exchange services are the most in number and in financing, probably due to the success of the business model: exchange services typically charge a fee on every trade in cryptocurrencies which is summed to the transaction fee requested by the public blockchain protocols. Due to high oscillation in the market over the last few years, the come into existence of derivatives product on some of these currencies[72], and the trading performed by hedge funds and possibly by institutional investors too[73], a large number of players were involved in trading, making exchanges very active and profitable.

Another activity in which startups engaged in is asset tokenization[74]. This service allows to transform a physical good, a service or a digital asset into a token. The latter are usually

[72] https://www.cnbc.com/2017/12/17/worlds-largest-futures-exchange-set-to-launch-bitcoin-futures-sunday-night.html

[73] http://fortune.com/2018/10/15/fidelity-launches-company-help-hedge-funds-big-investors-trade-crypto/

[74] Golden Currency, GoldFinX, GoldVein, Copernicus Gold,

securities, for physical assets, companies require that they are deposited in a safekeeping unit, or, if the startups already dispose of the asset to be digitalized, tokens are distributed against payment. We found that the second type, those startups offering tokens against a physical asset they hold, are more common, as tokenizing a digital asset held by an investor is a lot harder: the company needs to withdraw, evaluate the asset, and only then issue a corresponding token amount. Should this process be flawed, the model would be in contrast with our framework, since the internal predicate criterion would not be met. Examples are of companies digitalizing gold that go through an evaluation process before releasing to the customer a tokenized equivalent of their deposit; this is done also by automatic gold ATMs automatically evaluating and storing the good. This could increase the ease for commodity trading, as these systems can be set up in a public blockchain environment and accessed by any investor. Nevertheless, the market is quite fragmented as many companies exist offering this service, but they lack interoperability.

Offering smart contracts to assess structured products entails the automation of asset servicing and reporting procedures: some startups[75] focus on this segment to create structured products for underlying ERC20 tokens. For instance, a positive effect could be that of automating margin trading; a lender can post a cryptoasset to a smart contract on a set interest rate which can be borrowed by a trader for the purpose of short selling the asset and returning it at a later date. The trader posts a margin (in the form of other tokens) as deposits, and then, when he returns the borrowed tokens plus interest, he will be able to get his deposit back. This way of handling margin trading could be beneficial as any investor detaining assets can lend them to increase profitability and hedge against the risk of losses, whereas traders aiming to short sell would benefit from a larger offering of token loans, with the higher competitions reducing costs.

The last set of startups offers advisory, real estate investments and compliance requirements. Advisory aims to the guidance of companies in launching a novel ICO, so, these startups offer a service that is very similar to that of investment banks, but in the cryptoassets world. They do not use blockchain themselves, rather offer advisory in how to correctly leverage financing through it, so we will not study them in deep. We shall also overlook real estate startups as they do not comply with the correct blockchain usage proposed by our framework: they do not respect the internal predicate criterion. Their business model focuses on simplifying real estate investments by creating tokens that have properties as underlying, making a sort of tokenization of properties. The issue is that properties' value has to be assessed by experts who could have non-unanimous judgements; besides, properties can drop in value due to external factors: use, environmental changes etc., which are hard to manage

[75] https://dydx.exchange/

with a blockchain. A different and probably more effective solution is that of leveraging ICO to build new properties, this way token-holders are given lower transaction fees compared to traditional methods (which usually do not contemplate the possibility of selling shares in the project at all as they are closed-end funds). On the other hand, leveraging this method might not be beneficial for the constructors who would have to get advisory for ICO issuance, plus, as these are investment tokens, standard securities' regulation applies. Still, this model could be applied to any investment fund, increasing the ease in trading its share and giving investors a better liquidity. Compliance startups, instead, created new protocols that allow the issuance of tokens through an ICO, while attaching all relevant metadata and attribution data required to deposit the raised capital in a financial institution.

Financial institutions instead are mainly concerned with the potential of moving securities on private blockchains to simplify the processes described in the previous section, while driving down costs. The issuance process would still be taken care of by CSD as they carry legal liability for the correct procedure, whereas in public blockchains the issuance process is up to the issuer and the correct implementation of smart contracts, thus leaving the distribution to no specific entity beside the ledger. This would mean that CSD could join forces in a single DLT environment, or that there could be various (e.g. national) private DLT environments where CSD only are allowed to perform the notary function and to register newly issued securities in the system. In addition, according to regulation, non-tradeable securities do not have to be necessarily issued by a CSD but can be issued by other financial institutions who record them in their books. DLTs adoption could highly benefit this area as many exchanges are trying to put securities on-chain, instead of leaving them in paper-form at notaries' offices[76]: the decreasing number of intermediaries, and then, of costs, could bring a more favorable access to capital for SMEs. The fact that CSD has still to be involved in the process is strictly due to regulation requirements, alternatively, a set of rules for the issuance could be embedded in the private blockchain network, as it happens for public blockchain, making the existence of a CSD obsolete.

About clearing and settlement, here too DLTs can have a great impact on the current infrastructure. In fact, through smart contracts it is possible to hold still one of the two leg of a transaction until the other is delivered; therefore, a DvP model is easy to implement on a DLT system. However, different opportunities arise as the payment scheme is considered: under T2S, DvP is ensured by the ECB in central bank money. Without explicit consent of the ECB in participating and issuing money in a DLT system, the coordination between the

[76] https://www.borsaitaliana.it/borsaitaliana/ufficio-stampa/comunicati-stampa/2017/blockchain.htm

settlement in the DLT in commercial banks' money and one in central bank money to make the transfer final.

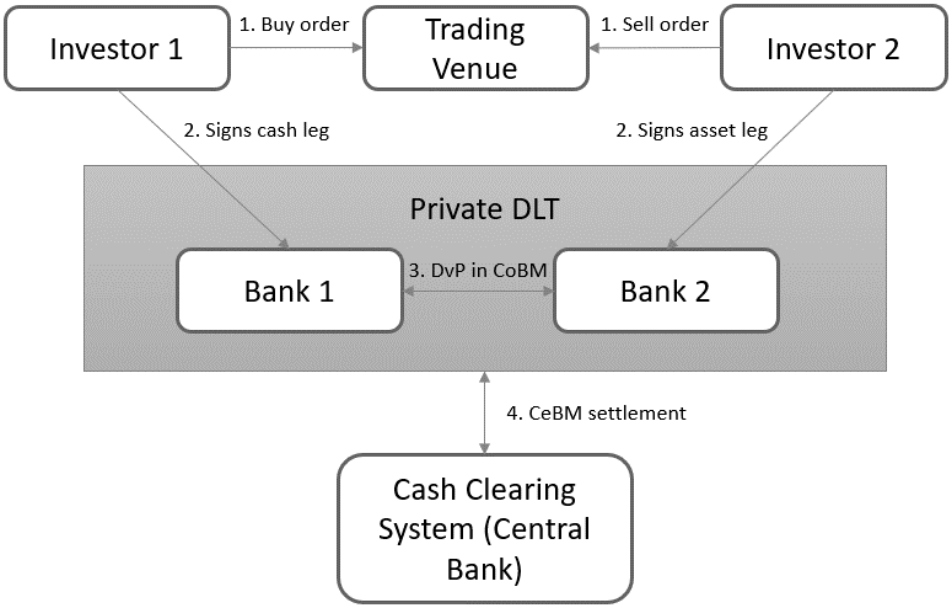


Figure 46, settlement in a private DLT (adapted from Advisory Group on Market Infrastructures for Securities and Collateral, 2017; and Oliver Wymann, 2016).

In Figure 46, the case in which settlement happens in CoBM first is considered, with a technical account at the CB reflecting movements of the distributed ledger; should the CB participate in the DLT system, settlement would be effective in CeBM on ledger. This latter scenario would be similar to that of public blockchain, where the cryptocurrency can be used to purchase secondary tokens with immediate DvP, and final settlement, not involving any risk in a counterparty failure. We note that the ledger takes the role of custodian banks, CCP are no longer needed to ensure the DvP as it is managed by the ledger, unless derivatives are being traded; finally, CSD are considered part of the DLT network, they do not have an active role in trading as their accounts are automatically reconciled, the sole purpose they still have is that we described in the issuance. The other advantage, beside the cost and complexity reduction, is that settlement can happen within seconds from the issuance of the order, as opposed to the current T+1,2,3. Other possibilities exist in the configuration of a private DLT but exploring all of them goes beyond our scope.

Considering asset servicing, the presence of a DLT could greatly simplify the processing and transmission of information along the holding chain: an event notified by the issuer to the issuer CSD is then passed on to the intermediary in charge of custody and only then to the investors. If all these actors were part of a DLT system, all their books would be reconciled,

and such hierarchical interaction would be replaced by a direct access to the ledger. Besides, corporate actions processing could be largely automated by the adoption of smart contracts: from income distribution, to tax withholding (WHT) procedures, computing the correct rate for each country automatically, eliminating all WHT agents and driving a reduction in credit and operational risk, to simplified settlement of securities consequent to corporate actions (e.g. right issues).

Also, collateral management can be impacted by the presence of smart contracts. As we explained, in collateral management operations there is a lack for univocal communication platforms, especially at international level. Most procedures are still notified with emails and creating an international collateral pool is not possible without bilateral agreements with local CSDs and custodians, resulting in an exponential opening of nostro accounts. DLTs could enable the usage of smart contracts automating most of the actions required to manage collateral: first, all adopting institutions would be connected and benefit from a unique collateral pool, secondly, automation is achieved by giving trusted information sources to smart contracts, so that possible margin calls are computed and notified by the contract itself, and just require a validation by the requested party to enable the operation. If the DLT is also in charge of securities settlement operations, it will be possible to fully automate the process even without requiring a validation: smart contracts could move securities according to margin requirements on their own. The limit to this model is obviously the cyber-resilience of such contracts and their correct implementation, as we explored in section 483.3.

Finally, compliance is the last aspect we discussed in investment products. DLTs have an impact in this area too, even though they do not address all the existing problems we highlighted before. Indeed, if settlement is completed on a DLT, reporting would be largely scaled back, as transaction data and ownership could be visible just by a ledger inspection. The regulator could be made part of the ledger to inspect himself relevant data and compliance requirements. Yet, not all reporting can be automated this way: many transactions, such as those on derivatives regulated by EMIR, where the derivative itself is not emerging from a settlement of an underlying asset, so, manual processes and communication with regulators might still be required.

All in all, most areas of investment products could radically change in the face of a DLT adoption by financial institutions. Issuance, settlement, asset servicing, collateral management and trade reporting could benefit from the instant settlement, the shared data and the automation through smart contracts this technology allows for. On the other hand, startups are also ripping off good profits in this area thanks to trading services. They cannot be considered a threat to incumbents due to the non-compliance with regulation, although many companies managed to raise funds through utility-token ICOs in certain jurisdictions.

The possibility to settle securities in near real-time has also many consequences in other areas, for instance in lending and supply chain finance, as we shall see in the next sections. Because of these advantages many exchanges launched projects to put securities on-chain: SIX (Switzerland exchange), ASX (Australian Stock Exchange), Nasdaq (in the US), LSEG (for non-tradable securities in Italy), SGX (in Singapore), Tradewind (in India, backed by ISX for commodity trading, mainly gold), HQLAx (in Germany by the Deutsche Börse to manage collateral). The benefits of such projects could rapidly fall onto liquidity seekers, such as large corporates, but also SMEs, that are typically put off from raising equity capital due to the traditionally high costs involved compared to the funds they need.

5.6 Deposit and lending

The lending business is carried out by many financial institutions. The largest portion of the market is held by depository institutions, such as banks, that engage in consumer, real estate (mortgages), corporate and institutional (C&I) loans. Other institutions that may engage in lending are: insurances offering policy loans, i.e. loans which utilize a customer life insurance policy as collateral; finance companies, typically offering small consumer loans to favor purchase and drive sales of the products offered; securities firms and investment banks both also engage in lending, usually focusing on corporate loans; finally, pension funds could also perform business loans to invest assets under management (Saunders and Cornett, 2008).

Considering the general role of financial intermediaries, matching deficit entities with surplus entities, lending is one of the most important tools to fulfill their part (Hull, 2015).

In this function, banks mainly serve as monitoring and information-related services provider, to solve information asymmetries arising in a lending scenario (Dermine, 2017). In fact, when lending, a person or an institution enters the so-called principal-agent problem, that is a situation where the agent (borrower) can influence with its actions the principal (lender) (Jensen and William, 1979; Mitnick, 2006). This issue relates closely with the moral hazard problem which entails an opportunistic behavior on the side of the agent to achieve higher returns while sharing no risks with the principal. That is the typical case of a loan or an insurance policy.

These problems in the agency and contract theories have long been studied in the economic literature. Holmström (1979) studied efficient contractual agreements in a principal-agent relationship under various assumptions about what can be observed, or contracted upon, by the two parties. He concluded that when payoff alone is observable, optimal contracts are deemed to be second-best, generating a moral hazard problem. This issue can be mitigated by creating additional information systems (such as in cost accounting)

or using other information about the agent's actions. By so doing, the contracts can be improved.

It follows that lenders are forced to monitor the borrower's actions to generate information about his behavior and mitigate moral hazard or design an incentive system such that it is in the borrower's best interest to act properly, without overexaggerating the positive qualities of his collateral or project (Harris and Raviv, 1978; Shavell, 1979).

Leland and Pyle (1973, pp. 382-384) deem this function as the main reason why financial institutions exist; information providing firms could be in place and solve any information asymmetry problem giving rise to the principal-agent problem. However, two issues hamper this kind of companies. The first is the appropriability of returns by the firm, the well-known "public good" aspect of information. Purchasers of information may be able to share or resell their information to others, without diminishing its usefulness to themselves. The firm may be able to appropriate only a fraction of what buyers in totality would be willing to pay. The second problem in selling information is related to the credibility of that information. It may be difficult or impossible for potential users to distinguish good information from bad. If so, the price of information will reflect its average quality. And this can lead to market failure, if entry is easy for firms offering poor quality information. Firms which expend considerable resources to collect good information will lose money because they will receive a value reflecting the low average quality. When they leave the market, the average quality will further fall, and equilibrium will be consistent only with poor quality information, much as Akerlof's (1970) market for used cars will result in only "lemons" for sale.

Both these problems in capturing a return to information can be overcome if the firm gathering the information becomes an intermediary, buying and holding assets on the basis of its specialized information. The problem of appropriability will be solved because the firm's information is embodied in a private good: the returns from its portfolio. While information alone can be resold without diminishing its returns to the reseller, claims to the intermediary's assets cannot be. Thus, a return to the firm's information gathering can be captured through the increased value (over cost) of its portfolio.

Diamond (1984) furthers researches on intermediaries and information gathering with relevant findings on the costs one must sustain to close the information gap. In fact, by defining as K the cost to obtain information and prevent moral hazard by the borrower, it is hardly possible that a large group of lenders (m) can afford to pay it individually: a cost of $m \cdot K$ would arise, and it should be covered completely by the interest paid by the borrower. Excluding the case of free riding, where no monitoring takes place, the most reasonable choice is to delegate the monitoring to a financial institution, so that the cost K is sustained only once,

while providing the intermediary with a delegation incentive D. In this setting, delegated monitoring pays off if[77]:

$$K + D \leq \min[E_{\tilde{y}}[\varphi(\tilde{y})], (m \cdot K)].$$

In addition, Diamond demonstrates that this delegation cost approaches zero as the number of borrowers (i.e. the amount of diversification in the financial institution portfolio) tends to infinity. Indeed, the probability that the average return ends up in the lower tail of the distribution is monotonically decreasing as the number of borrowers increases. Thus, the cost of monitoring sustained by a financial institution tends to K, and its centrality in a principal-agent setting is demonstrated.

If Leland and Pyle tackle the information asymmetry present before the deal is signed and suggest that an optimal way for the borrowers to signal their goodness is investing part of their own assets, Diamond models the ex-post information asymmetry solved with the delegated monitoring of the contract.

Another feature of lending through a bank is that of being able to withdraw money whenever it is needed while still gaining a positive interest on the capital deposited. Instead, without banks, a withdrawal from an investment would cause a zero or negative return, as it is usually not as liquid as a deposit (Diamond and Dybvig, 1983).

5.6.1 Loan classification and issuing process

After highlighting the role of financial intermediaries in the lending environment, we shall now overview how loans are classified, and how they can be managed. A basic classification of lending products (Bhat et al., 2016) differentiates loans depending on the target to whom they are granted. They consequently define mortgages, loans issued against a real estate collateral, consumer loans, when issued to private individuals, and corporate, if the borrower is a corporation.

A second classification distinguishes between the features of the loan: open-ended loans such as credit cards and lines of credits allow the borrower to access funds with no particular reason beside the need for liquidity; closed-ended credit is conversely granted for a specific project o reason, and for a limited amount of time. Another distinction is made between secured and unsecured loans, depending on the collateral that may be attached[78].

[77] Where y is the aleatory return the borrower has from his project, so E is the expected value of the probability distribution Phi on the return.

[78] https://www.thebalance.com/seven-types-of-loans-960034

Alternatively, lending products are classified according to the risk for the lender to lose money. The risk arising from a loan portfolio is called credit risk. Credit risk is the probable risk of loss resulting from a borrower's failure to repay a loan or meet contractual obligations. Traditionally, it refers to the risk that a lender may not receive the owed principal and interest, which results in an interruption of cash flows and increased costs for collection[79]. To assess this risk and to reduce information asymmetries credit scores are in place (Dietrich and Kaplan, 1982; Dermine, 2017): credit scores are statistical figures which evaluate a consumer's creditworthiness based on his credit history. Lenders use credit scores to evaluate the probability that an individual will repay his debts. They are computed referring to the so-called 5 Cs: credit history of the customer, his capacity to repay, amount of capital, the loan's condition and the associated collateral[80].

A different process to evaluate credit scores is provided by the literature (Jarrow and Yu, 2001; Kang and Kim, 2005); it consists of five steps: Rating, Costing, Pricing, Monitoring, Work Out. The objective of the rating is to ascertain the borrower's default risk. To this end, banks perform a credit evaluation before they lend money to a customer. In addition to the personal credibility check, a creditworthiness evaluation is conducted to determine a loan's probability of default (DP). The aim of costing is to quantify the expected loss (EL, measured in currency) from lending based on probability of default (DP) and loss given default (LGD, measured in percent).

Figure 47, A representation of the credit scoring process

Loss given default is the expected loss when a borrower goes bankrupt. It depends on the so-called credit equivalent (CE, measured in percent), and the loss severity (LS, measured in percent), which is the expected loss of the exposure expressed as a percentage. The latter mainly depends on the value the bank estimates receiving if it calls in security on a loan and subsequently sells it. In the pricing phase, the identified costs are integrated into the credit conditions. By charging every borrower a premium based on his expected loss, the average loss in lending can be compensated for (Stein, 2005). During the loan period, the credit is watched

[79] https://www.investopedia.com/terms/c/creditrisk.asp
[80] https://www.investopedia.com/terms/c/credit_score.asp.

and changes in credit risk are monitored. If a borrower's expected loss increases, the reasons for this need to be analyzed and measures of correction taken. Bad credits are handled in the work-out unit of the bank. The objective in the work-out phase is to reduce the losses and, if possible, to get the borrower back on track (Weber et al., 2008).

According to the risk classification (Dermine, 2017), the risk associated with a loan increases the relevance of the financial intermediary assessing it. Loans associated with small risks are in fact 'information insensitive', meaning that the information asymmetry has a low impact on the contractual relationship. This kind of loans are usually associated with a large collateral that could range from a real estate (and the loan is a mortgage) to a security (generally government bonds associated with low risks). Therefore, in case of borrower's default, the lender is insured by the value of the collateral which he can possess and sell to cover up for the loss. Riskier loans instead, such as uncollateralized (or collateralized with a small loan-to-value collateral) loans, are information sensitive and consequently need a risk monitoring service by the intermediary, and, in case of defaults, specific competences in NPLs (non-performing loans) management and portfolio restructuring.

From an interview with a bank employee, we mapped the current process to issue a mortgage, to highlight possible criticalities and inefficiencies. First, a customer has to bring to the bank branch a set of documents confirming his identity (ID, health card, family state etc.), which have to be physically scanned into the bank system by an employee, as well as financial data such as the last two salaries, and possibly also a declaration of the employer. Finally, documents concerning the property have to be presented, such as the presence or not of an existing mortgage on the property, property planimetry and so on. Once an employee gathered all this data, he forwards property information to an expert in charge of the evaluation, and other customer identity and financial data to the risk function of the bank which performs a background check looking for other possible loans and debts contracted by the customer. If everything is aligned with the customer self-declaration, a different function of the bank takes the decision on the issuance, considering financial parameters, job terms, customer solvency and, most importantly, the property evaluation by the expert. If approved, a notary then proposes a preliminary relation which is approved by another responsible function and the contract is finally signed.

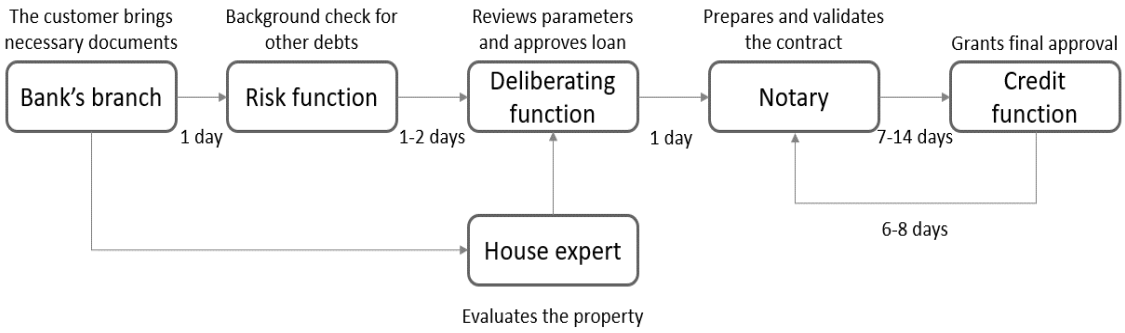


Figure 48, the process of an Italian bank to grant a mortgage loan

As we can see from Figure 48, the process is quite slow and takes around 4 weeks. Anyway, most of the delays and inefficiencies are not really imputable to the bank, rather, they depend on the presence of external figures such as the house expert and the notary who introduce the most delay in the process. Indeed, for a common loan, which is not a public act and these people are not involved, the process is much faster and typically takes 2-3 days.

5.6.2 Securitization: definition and classification

A fundamental tool to manage loan portfolios is asset securitization. Securitizing a loan allows financial intermediaries to close gaps in their interest rate spread, increase liquidity of their portfolios, gain fees as servicing agents for the sale, and helps mitigate regulatory requirements, such as capital or reserves requirements (Saunder and Cornett, 2008).

Securitization can happen in three different forms. Pass-through securities entail the securitization of a loan portfolio with subsequent purchase from investors; the latter are entitled to a fraction of all principal and interest payments due by the borrowers, based on the fraction of securitized loans they purchased. A second tool is the CDO (collateralized debt obligation or, in case of mortgages a CMO, a collateralized mortgage obligation) which is constructed to be more attractive to investors by mitigating the prepayment risk: in fact, bondholders are divided into classes, and, in case of early payments by a set of borrowers, only one class at a time is repaid the principal, while others still retain the investment for a longer period of time. Usually, classes more exposed to prepayment also get smaller coupons, due to the shape of the interest rate term curve, and also the smaller credit risk in case of NPLs. Finally, the last type of securitization is done via asset-backed securities (ABS or, in case of mortgages, mortgage-backed bond, MBB). The main differences with the other two are: the fact that they remain in the issuing institution balance sheet, and the non-existing link between the cash flows arising from the loans and those coming from the securities. Practically, the financial institution selects a group of mortgages in its balance sheet and pledges them as

collateral against the MBB issue. A trustee (another institution) keeps the value of the collateral up to date and guarantees it exceeds the principal of the bondholders (DeMarzo, 2005; Choudhry and Fabiozzi, 2004; Vink and Thibeault, 2008).

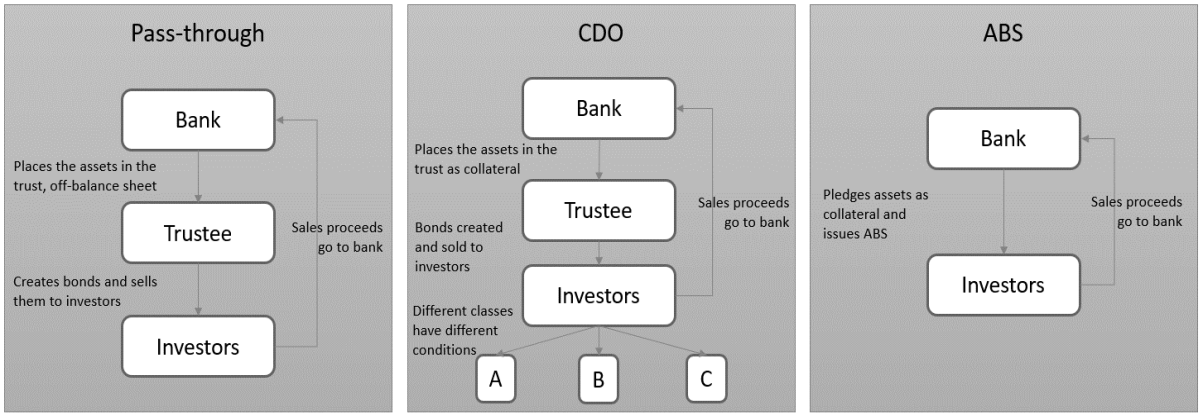


Figure 49, A representation of different securitization possibilities.

Usually, CDO have ABS or MBB as underlying, so they can be seen as a particular type of ABS issued by a trustee[81].

5.7 Blockchain-enabled deposit and lending

Now, we shall examine the results from our database to identify possible applications of the technology in the lending services. We noted that 21 startups are dealing with lending-related projects, with a considerable amount of financing, near to €20 million each, and thus a total financing of almost €308 million, none of which through ICO. Of these startups, 19 engaged in lending platform that allow P2P lending through public blockchains, the loans can be collateralized by cryptoassets, or non-collateralized with a higher interest. Also, 2 startups offer tools for banks to manage syndicated loans and loans portfolio, from private auctions management to loans securitization.

On the other hand, 13 institutional initiatives for loans on DLT are focused on syndicated loans management, and 2 on credit score ratings. There are 15 initiatives in total, representing the 5.14% of the database, with 2 operative initiatives and 8 PoC. The gap with the percentage of startups initiatives might be explained by the fact that no PoC was tested in the field of traditional loans, and no additional services on cryptocurrencies were considered by banks, most likely because of compliance risks and possible law infringements. Instead, startups

81 https://www.investopedia.com/ask/answers/040715/what-difference-between-collateralized-debt-obligation-cdo-and-asset-backed-security-abs.asp

focused on crypto-securitized loans are more in number and their business model is effectively sustainable, as it refers to banks' securitized loans, so also the financing received is quite high.

Number of startups	Average financing	Total financing	Percentage of total
21	€ 19.229.243,50	€ 307.667.896	9,94 %
Amount of news	**Operative**	**PoC**	**Percentage of total**
15	2	8	5,14%

Table 9 reports data for deposit and lending startups: the number of initiatives average financing received (in euros), total funds received (in euros), and the percentage of the funds received over the total. For companies, it reports the number of news for lending initiatives, how many of the projects are already operative, which are PoC and the percentage over the total amount of news

5.7.1 Areas of application

In this section, we will give a better detailed view of the projects and their possible impact on financial institutions' business model. Beginning from startups, the most widely spread and successful application in terms of financing is, as we mentioned, the construction of securitized loan platforms: borrowers are requested to deposit a certain amount of eligible cryptoassets (usually Bitcoin or Ethereum) to receive a loan in fiat currency. This model is similar to that of securitized bank loans, with the main difference being that of the securitizing asset, that is, cryptocurrencies, and the usage of smart contracts to streamline the whole process. In fact, the eligible tokens are deposited in a smart-contract-managed account, where they are returned in case they price up or a further deposit request is forwarded to the borrower in case their value decreases below a threshold. Should the borrower not respond to the deposit request in due time, the smart contract will move the asset in the account of the lender. The lender could be either the platform itself, or it could be any investor interested in this kind of products, depending on the startup business model. The advantage of this tool is that it provides liquidity while allowing borrowers to retain their investments in cryptocurrencies, so that they can still benefit in case of price increases. It is interesting to note that credit score is not computed, increasing the overall speed of the process and making the funds available within days from the collateral deposit even for new customers.

The main drawback in this application is the large value of collateral that has to be deposited: in fact, due to the high volatility of crypto assets, most platforms offer low loan to

value[82], typically around 30-40%, and also have a quite high ARP, around 5-10%[83], meaning that to use the product one has to expect a price increase higher than 10% to have any chance of ripping off some profit at all.

Another business model encountered among startups is that of trusted lending circles. These constructs allow a group of trusted peers[84] to create a circle on the platform, which is corresponded by the platform creating a smart contract to manage the circle. Rules are set, such as the monthly amount to deposit. Then, when the circle starts, the group of peers begins to deposit the agreed monthly amount, and, when certain thresholds are reached, the deposited amount is handed out to a random peer which is selected as the winner. When this happens, the funds deposited are exhausted and the deposit starts again from zero. The purpose of this mechanism is to allow certain individuals in the circle to obtain the sum they are saving toward much earlier than they could on their own. However, also this model has some drawbacks: as noted, trust in the peers participating is needed, so that they will keep on depositing even after they are elected winners; otherwise, untrusted parties could take on a selfish behavior and leave the circle upon winning the money. Besides, blockchain is not really enabling a new business model, as the same could be done on a centralized database: the only advantage for customers is that the startup is not directly managing the money. But since they are creating the smart contract needed to assess the circle rules, trust in the correct implementation of such contract is needed. Still, this kind of startups could impact microcredit offerings by banks and finance companies.

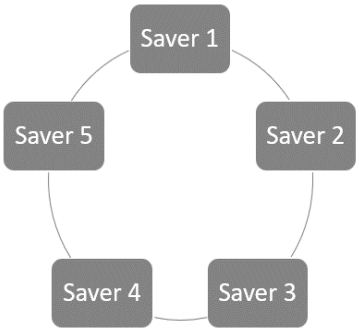
Lastly, applications exist in the field of loan management. In particular, we report a startup working to the development of a CordApp (an overlay application running on Corda) that allows the exchange of loans between financial institutions. Indeed, as we reported, the chances for an institution to sell part of its loan portfolio are either of selling it in a bilateral agreement, or that of a securitization open to other institutional investors in a private placement. This startup offers a marketplace that integrates directly with Corda nodes, allowing financial institutions to trade loans in their portfolio in an open market instead of going through the slow procedure of bilateral agreements. The application also plans to offer further services in the future, such as the management of loans securitization through a tokenization. Indeed, tokenized ABS and MBS could benefit from all the advantages listed in the security section, such as instant settlement, ease of issuance, and low trading costs; in

[82] Loan to value (LTV) is the value of the loan divided by the value of the cryptoassets deposited: requiring 50,000$ would entail a deposit of 125,000$ worth of Bitcoin (if LTV amounts to 40%).

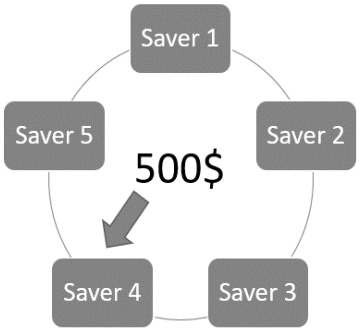
[83] Such as on https://nexo.io/.

[84] Note that a certain degree of trust is a prerequisite and is not fully managed by the blockchain.

addition, they would be traded on the private market platform which is open to all financial institutions in the Corda network.



5 savers need 500$ each to make a purchase; so, they start a lending circle, each depositing 100$ a month for 5 months



After the first month saver 4 is elected winner and receives the 500$ needed. He will still keep depositing 100$ for the next 4 months.

As for institutional initiatives, most of them are dealing with syndicated loan management. A syndicated loan is a form of debt usually utilized by large corporations requesting for large amounts of capital; in a syndicated loan, instead of a single bank, multiple banks offer the loan. Actually, blockchain could help in this regard by streamlining the stipulation of contractual terms of the loan: the corporate customer could view all conditions from a single interface, available as a second layer app in a private blockchain. Here, all terms of different banks are available and can be browsed and discussed without the need of phone calls or emails, as it happens in traditional procedures[85]. Also, there is an advantage for banks who could have a faster tool to define contractual terms with other participating banks, keep their position reconciled with peers, as well as receive interest payments in a simpler way thanks to the usage of smart contracts automatically splitting the tranches due.

The last use case developed by institutions is that of automatizing the credit scoring procedure: the blockchain could benefit this complex process by storing a customer rating on it, shared with other institutions to assess past history, while artificial intelligence algorithms analyze data that goes beyond financial information, but also includes social network activities and similar. Then, this data would be used as the input for a smart contract, allowing the calculation of the credit score and the decision whether to issue a loan to a demanding customer within minutes. Announcement surrounding this possibility are quite recent and therefore the validity of the hypothesis remains on a theoretical level.

Altogether, we found several initiatives in the lending area, the most promising being in loan portfolio management, and syndicated loan management. Nevertheless, it seems that

[85] https://www.finastra.com/news-events/press-releases/finastras-fusion-lendercomm-now-live-based-blockchain-architecture

blockchain can hardly affect traditional lending procedures such as credit scoring or mortgage issuance, at least, not without the help of other technologies like AI. Benefits in this area may come from the KYC procedures, so, they will be discussed in that section. Startups do not seem to be threatening incumbents in this field, rather, most of them are aiming at a collaboration, since they are developing their products as application to run on private and permissioned networks.

5.8 Supply chain finance

Supply chain finance (SCF) is at the evolutionary frontier of financial services that are closely related to the supply chain cycle. These services leverage the use of documents, orders and contracts traded between companies, granting them the access to better payment terms and thus to a cheaper form of financing that generates liquidity and improves their working capital (Templar et al., 2016). A thorough definition is proposed by the Global Supply Chain Finance Forum (2015): *SCF is the use of financing and risk mitigation practices and techniques to optimize the management of the working capital and liquidity invested in supply chain processes and transactions. SCF is typically applied to open account trade and is triggered by supply chain events. Visibility of underlying trade flows by the finance provider(s) is a necessary component of SCF.*

To optimize the working capital management, companies aim at the maximization of free cash flow (FCF), by reducing idle or locked up capital. This allows them to increase their internal funding ability and enterprise value. To achieve this objective, a key aspect is the reduction of the C2C (cash to cash cycle):

$$C2C\ cycle = DSO\ period - DIH\ period - DPO\ period$$

Where DSO are the days sales are outstanding, DIH the days inventory is held, DPO the days payments are outstanding (Hofmann and Belin 2011). To maximize C2C then, every company will set to a minimum the DIH period, and then try to increase the DSO by delaying payment to suppliers and reduce the DPO by speeding up the collection of account receivables. However, these objectives are conflicting as every company would try to pay later and get paid earlier, reaching an impasse. The presence of financial intermediaries offering SCF programs release this tension and allows the maximization of the C2C cycle (Hofmann and Zumsteg, 2016).

Another key aspect of the definition is open account (O/A) trade. These accounts are often required to exporters by importers, as they entail the shipment of goods before the payment is

due (usually in 30-90 days). O/A trades grant more flexibility than letter of credits (L/C)[86], bank payment obligation (BPO)[87] and other intermediation products, while on the other hand, risk exposures and working capital needs might be increased. Nevertheless, these instruments usage is surging compared to traditional products (GSCFF, 2015).

5.8.1 SCF techniques

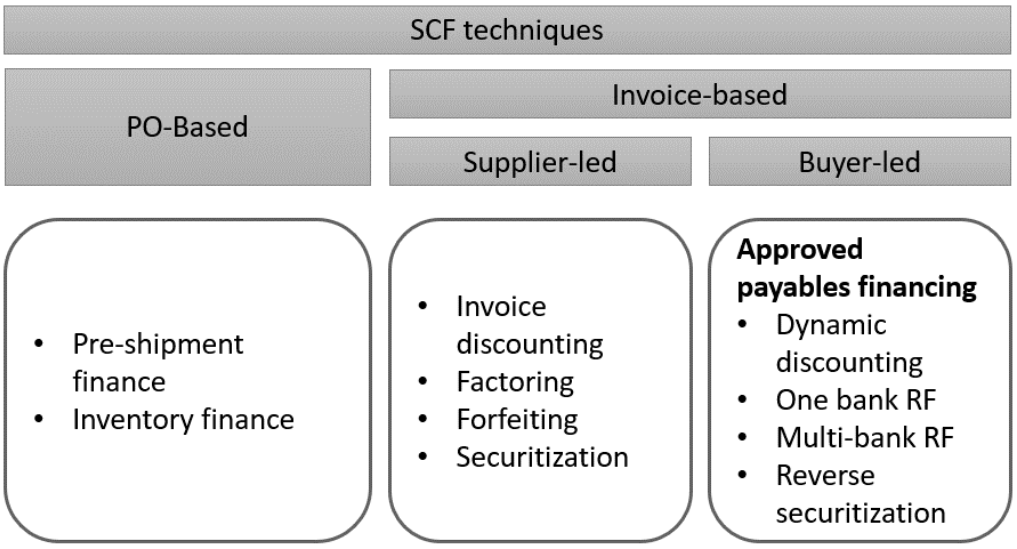


Figure 50, a scheme of SCF techniques classification

All kind of documents, contracts and orders traded between members of a supply chain can be used to initiate a financing solution. Camerinelli and Bryant (2014) provide an extensive classification of SCF techniques, which can be divided in PO-based (purchase order) or invoice-based depending on the documents used as collateral, and the supply chain event triggering the financing.

PO-Based

PO-based solution can be triggered pre-shipment or as products are held as inventory. With pre-shipment financing, the PO represents the evidence of repayment before production

[86] A letter of credit is a letter from a bank guaranteeing that a buyer's payment to a seller will be received on time and for the correct amount. In the event that the buyer is unable to make payment on the purchase, the bank will be required to cover the full or remaining amount of the purchase (Investopedia).

[87] Launched in 2013, the Bank Payment Obligation (BPO) is a standardized, irrevocable payment instruction which uses ISO 20022 data structures. The BPO offers buyers and sellers a way to secure and finance their trade transactions, regardless of size, geography or industry. It combines legally binding rules with electronic messaging and matching capabilities (Swift website).

or shipping for the financing provider. The funds usually cover the working capital needed for the order's execution, such as raw materials, wages or packaging costs. In the case of inventory finance, the financing is usually confined to finished goods where a buyer has already been identified and for which a PO has already been issued. In this case, the financing party provides funds against the inventory (as collateral) or by way of a sale and repurchase agreement for the duration of the transaction. Similarly, for these financing instruments, the intrinsic risk is higher than for invoice-based financing techniques due to the financing party being engaged in the very early stages of the transaction (Camerinelli and Byrant, 2014).

Invoice-Based

Invoice-based financing techniques represent the largest share, with an estimated 80-90% market share, whereas the remaining market share is held by inventory and pre-shipment finance instruments that are more specialized and not as widely practiced outside of certain industries. Depending on whether the program is initiated by the buyer or the supplier, it is possible to distinguish between supplier-led and buyer-led financing instruments.

In a supplier-led architecture, the financing program is initiated by the supplier and is set up to finance the receivables of the vendor company. For invoice discounting instruments[88], the collection of the receivables remains under the control of the supplier, and the buyer is usually not informed of the sale of the invoice (i.e. undisclosed assignment). The classical factoring[89] or forfeiting[90] instruments also fall under the supplier-led category, but the buyer is usually informed of the transfer of the title, and the collection is managed by the financing party. At last, securitization could be adopted: in a securitization scheme a SPV (special purpose vehicle) is formed with the sole purpose of acquiring the account receivables of a specific supplier (usually owed by multiple buyers) at a discount, financing the acquisition by transforming the assets in asset-backed securities (ABS) sold on the capital market; this way, the efficiency of an open market can be leveraged, i.e. reduction in capital exposures of parties involved, better prices and lower risks (Leonard, 2015; Miler, 2007).

[88] Invoice discounting is the practice of using a company's unpaid accounts receivable as collateral for a loan, which is issued by a finance company (GSCFF website).

[89] Factoring is the sale at a discount of receivables to a finance company (the factor), which is then in charge of collecting them (GSCFF website).

[90] Forfaiting is the discount of future payment obligations on a without-recourse basis, in other words, forfaiting is discounting of trade related receivables secured with trade finance instruments such as bills of exchange, provisionary notes or deferred payment letter of credit (GSCFF website).

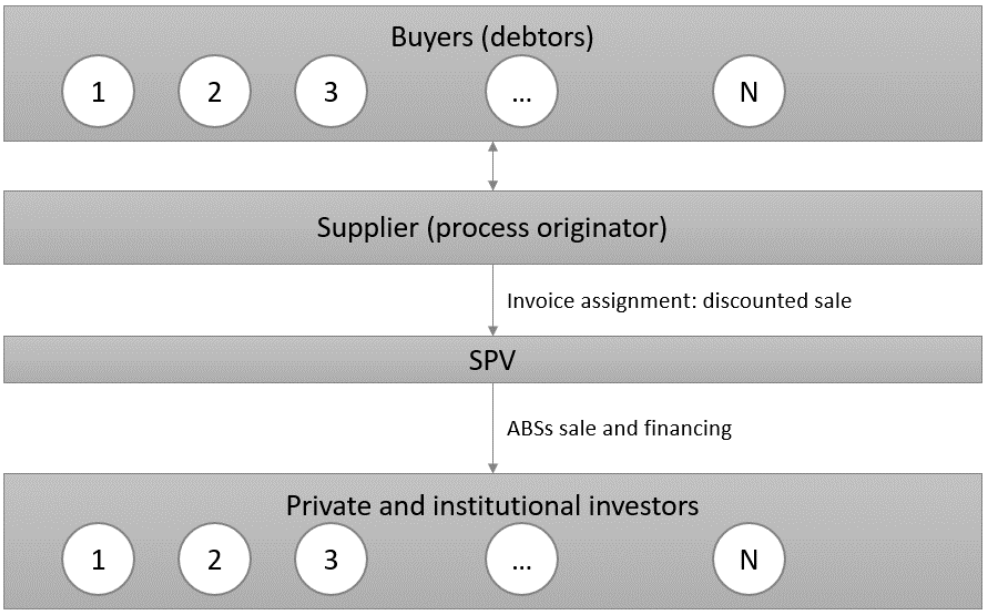


Figure 51, a scheme for supplier-led securitization; in a buyer-led one suppliers are creditors, the only buyer is the originator.

In a buyer-led program, a usually large buyer starts himself the process of factoring (i.e. *reverse factoring, RF*), asking the supplier which receivables he would like to have paid immediately at a discount; these techniques are named *approved payables financing*, as the supplier approves certain receivables only (GSCFF, 2015). This operation is therefore collaborative and lets small suppliers benefit by the better credit scores large buyers typically achieve; represents lower costs for banks that have to assess the credit worthiness of the buyer only, and not worry about the (many) suppliers; it is faster as buyer discloses information directly so that banks can release funds immediately (Seifert and Seifert, 2009). Still, according to Camerinelli and Bryant (2014), approved payables financing only accounts for 20% of the invoice-based market, but they have a strong growth potential. Reverse factoring can be done resorting to a single bank (one bank RF), or to a group of banks (multi-bank RF) which finance the operation through a SCF fintech platform; thus buyer and suppliers gain the advantages of not being dependent on a single institution, and access a wider range of products that would be otherwise limited by the bank geographical scope, product portfolio or credit lines limits (Zakai, 2015).

Other buyer-led techniques are: dynamic discounting, that is the financing of receivables directly from the buyer, meaning that the buyer himself is investing in the supplier in exchange of a discount or an interest rate; and reverse securitization, which is a securitization started by the buyer, and, as opposed to a supplier led securitization, there is a single debtor (i.e. the buyer) so the credit score assessment and KYC procedures required to perform the operation

are easier to carry out; but, on the other hand, the diversification effect is nullified (Miller, 2007).

5.8.2 Criticalities and inefficiencies

Hoffman et al. (2018) identify the main barriers hindering a smooth deployment of supply chain finance techniques in three different factors.

The first is in the case of payables financing, and it is KYC requirements: whenever banks start a new relationship with a supplier or a buyer, before they can offer services, a thorough assessment of its identity, business and customers have to be carried out, so as to protect the financial systems from money laundering and terrorism financing (AML and CFT). These procedures are quantified in a cost of 500 to 2000€ per customer, meaning that a bank willing to join a program involving 50 or more companies can result in very significant costs. Their conclusions are supported by surveys from ICC Global Trade Finance (2014) and APEC (2015) according to which the main reason banks reject supply chain finance programs are due to excessive burdens in KYC procedures.

Second, in case of approved payables financing, the key driver pushing buyers to resort to this solution is accounting treatment. Account payables are not considered as debt contracts for balance sheet purposes, therefore, companies leveraging this financing instrument can benefit from a reduced financing cost in the long run due to unchanged debt ratios. However, if buyers start a supply chain finance program with a bank, accounting rules force the buyer to reclassify payables to bank debt, removing the advantage. So, the second impediment is in accounting treatments.

Lastly, the third barrier is constituted by high transaction costs in both supplier- and buyer-led securitization financing. The issue with this program is dictated by the large number of intermediaries who are taking part in the process. As we have seen with securities' inefficiencies, CSD, custodian banks, or clearing houses are needed to manage the issuance and post-trade process. This largely drives high transaction costs in the securitization, making it hard to offer public placements: usually up to 10 investment banks are involved to drive competition in the private placement, and they participate with transactions amounting to at least €1 million to cover these high costs.

5.9 Blockchain-enabled Supply chain finance

In this section, we explore the data we gathered to map valid supply chain finance initiatives among companies and startups, and to see whether the issues reported by the literature can be addressed by blockchain technology.

Supply chain finance startups account for 2.12% of the total financial investments, with a total capital collected of almost $65.7 million. There are not many startups in this area, but the average amount of financing received is high, keeping in mind that only one of these was financed through an ICO (gathering $8.9 million), while 3 of them did not disclose funding.

Number of startups	Average financing	Total financing	Percentage of total
7	€ 16.424.855,25	€ 65.699.421,00	2,12%
Amount of news	**Operative**	**PoC**	**Percentage of total**
24	1	13	8,22%

Table 10 reports data for SCF startups: the number of initiatives average financing received (in euros), total funds received (in euros), and the percentage of the funds received over the total. For companies, it reports the number of news for SCF initiatives, how many of the projects are already operative, which are PoC and the percentage over the total amount of news.

Startups are focused on services such as payment service provision (3 startups), invoice financing (2 startups) or both of the two (2 startups). As payment service providers, startups leverage blockchain to offer clients real time settlements and low transaction costs for large B2B payments. Blockchain is used in the background to allow the process between two users owning an account with the startup. Instead, for the invoice financing, we identified two different types of business models. One is just supporting and streamlining data about invoices on chain to simplify the financing process, reduce its costs, and enable it for small and medium enterprises that would be otherwise put off by the prohibitive charges. The other one, instead, is proposing a P2P model for invoices securitization: invoices' hash is recorded on the blockchain, and the asset is tokenized at a value established by the startup company; successively, investors are able to purchase the tokens at the defined price, and then trade them freely on the secondary market.

Initiatives by financial institutions in this area are greater in number compared to the total, as they amount to 8,22%, that is, 24 initiatives. Of these, only 1 is operative, 13 are proof of concept, whereas the others are announcements. Though, according to the news, 3 of these tests will be turned in operative products by the end of 2018 or the beginning of 2019. The significant gap with startups initiatives might be explained by two factors. First, the fact that

supply chain finance projects require an extensive network of banks providing the financing, but also very large corporate companies or a high number of SMEs supplier firms that demand funds; without it, it is impossible to create business conditions to launch a SCF program. Secondly, startup companies are often interfacing with public blockchains, which cannot offer satisfying requirements for financial operators in terms of compliance, as we have seen in the technical analysis. Corporate initiatives are focusing on specific tests, such as putting on-chain factoring products and account receivables, or the development of large platforms that should engage also other institutions in comprehensive SCF programs.

5.9.1 Areas of application

As we mentioned, the first area startups are applying blockchain is in the management of payments across businesses. As PSP they allow for fast to instant settlement for large tranches of money among businesses. Nevertheless, according to our framework, these companies are either not working on blockchain or have an ill-constructed business model: paying through BCT is feasible for large payments, but it still requires an intermediary, that is, in this case, the startup company charging fees on the transactions. Startups require companies to use a credit card or their credit line to move funds to their app, then, payments can be processed instantly, and the counterparty receives the money in its account on the app.

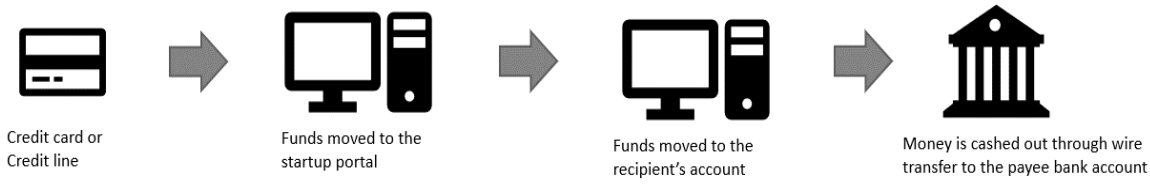


Figure 52, traditional B2B transaction through a digital PSP intermediary

As we can see from the figure, there are many flaws in the process proposed for the adoption of a blockchain: first, an always online TTP is present, that is, the PSP. Secondly, the process is not necessarily less expensive compared to a traditional bank transaction: unless a consistent amount of money is kept in the PSP's platform, a constant need for account reload and unload through the traditional bank account is needed. Also, even if a large capital is kept on the platform, fast payments work only if the counterparty is also using the platform, otherwise a common wire transfer forwards the payment to the bank. As we have seen in the payment section, the usage of blockchain technology might be needed to PSP so as to allow interoperability and transfer of funds among each other without recurring to a bank, but a single PSP has little room for blockchain employment, and a centralized database is preferable.

A second area of application is the streamlining of data and invoices on-chain. This application is not only followed by startups, but it has also been the object of testing by many financial institutions. A number of advantages exist in this regard. The first use case is the streamlining of bank sureties (*fideiussioni*). These tools are a guarantee that the bank will cover the obligation taken by the importer in case he fails in its fulfillment. The issue with the instrument is that banks and insurance companies providing the service transmit certificates via certified email to the exporter, who has to verify the validity of the document before he actually ships goods, a process that can take up to 10 days[91]. Blockchain can support this process by putting bank sureties on the ledger and identifying them by a unique hash. When the exporter receives the document via certified email, he can doublecheck the authenticity inspecting the bank ledger and verifying that the hashes corresponds in a matter of minutes.

The second use case encountered is that of letter of credits: blockchain allows for a streamlined management of such documents, removing the need for manual reconciliation by looking at certified email. In fact, documents can be transmitted on the blockchain platform where all parties have shared access, as opposed to the current system where each actor has to check the document received and update the information on his own centralized server[92].

Another impactful application is in factoring. Factoring procedures present many problems for banks and entrepreneurs at the moment: on one side, invoices can be presented to more than one institution asking for financing, causing a double spending issue (1b. in Figure); on the other hand, entrepreneurs are forced to interface with a single bank, which could finance only part of the transaction, and they do not have the chance to resort to other institutions for the remaining part. Multi-bank reverse factoring was enumerated above by Camerinelli and Byrant (2014) in the list of available products, as fintech platforms exist, providing multiple banks with the opportunity to join a shared program. Anyway, this only happens in buyer-led SCF programs, and it is not possible to think of a supplier-led multi-bank factoring: as of now, banks redirect (4. in Figure) the payment from the buyer referenced in the factoring operation to their own account to avoid the supplier company taking hold of the money and adding its credit risk to the process; doing this on a multi-bank scale is nowadays impossible.

Instead, with blockchain, invoices can be recorded on the ledger, producing a unique hash; banks participating can view the hash and, in case a fraudulent supplier tries to double spend them in a different bank, the hash function of the document would produce the same result, effectively detecting the double spend attempt. Also, blockchain could allow multi-bank

[91] https://we-trade.com

[92] For instance, https://www.cnbc.com/2018/05/14/hsbc-makes-worlds-first-trade-finance-transaction-using-blockchain.html

factoring with the introduction of smart contracts: bank can keep track of the amounts financed by other institutions and decide whether join providing their own funds. When the payment is received by the supplier, it is automatically split by the smart contract between participating banks, making the process costless and automatic, increasing the financing options for companies.

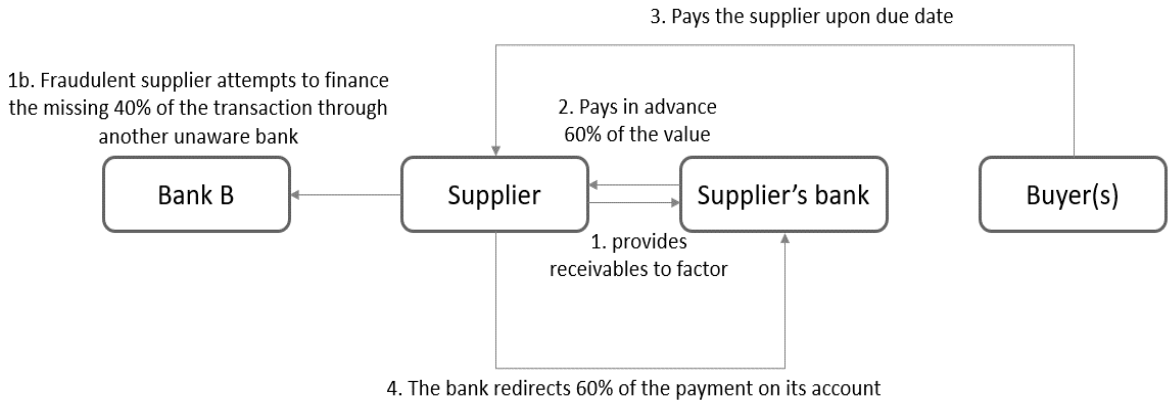


Figure 53, as-is factoring process

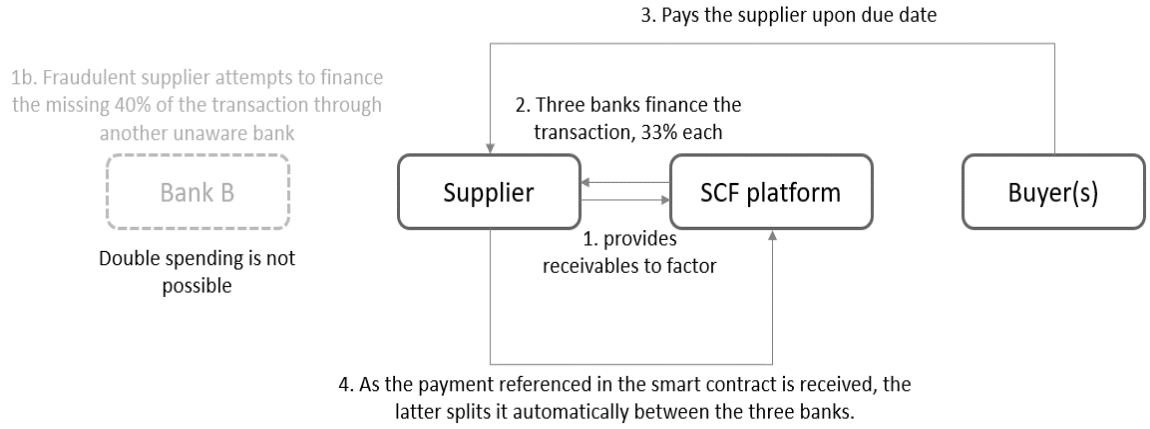


Figure 54, blockchain-enabled factoring

In addition, blockchain could address also KYC requirements: once the credit rating of the receivables is assessed by one bank (usually corresponding to the supplier's rating), it can be shared among participating banks through the ledger, provided they pay a fee to access it. This could dramatically reduce compliance costs for banks as they are shared across institutions and allow to service a larger portion of the market, such as small-enterprise suppliers, who are underserved because low transactions amount cause difficulties in covering costs (Nassr and Wehninger, 2015). The same benefit can be carried onto the multi-bank reverse factoring, where, like we discussed, KYC costs are also high, especially as the number of participating

suppliers grows (Hofmann et al., 2018), thus allowing banks to increase the serviced market as well as the availability of funds.

Finally, the last application we mentioned is that of P2P invoice securitization. A set of issues arise in this use case, as it is proposed by the startup companies. First, it lacks the necessary instruments to dialogue with the banking infrastructure, as they all leverage the Ethereum public blockchain to perform the securitization: from our technical analysis we already shed light on the fact that public blockchains do not allow the inclusion of metadata and the attribution principles necessary to identify parties. Because of that, a correct KYC procedure cannot be carried out by banks. This means that all the money gathered by companies recurring to a direct tokenization of invoices cannot be deposited on a bank account, unless the companies perform KYC procedures themselves on the investors buying their invoices. This is a remote possibility, as a series of issues arise:

- Companies do not usually perform KYC procedure, they might lack competences to do so and it would drive high unnecessary costs.
- Companies could have troubles finding private institutions that buy their products, as they are not assisted by a bank in the issuance process, so, they would have to sell it in a public placement, making the KYC assessments of the many investors unsustainable and unprofitable.
- There are few countries around the world which regulated cryptoassets, only companies of those countries could access this business model.

Consequently, the proposal of such startups is not only unlikely to be profitable at the moment, but it is also unpracticable in many countries around the world. Nevertheless, it shows great potential if banks were to adapt this business model in a private regulation-compliant blockchain. As we have discussed in the securities section, the adoption of blockchain could strongly impact issuance, post trade processes, compliance activities and possibly also payments. If these breakthroughs are put to practice, standard and reverse securitization programs could largely benefit from the cost reduction in the process, allowing even SMEs, typically with lower amounts in their invoices, to take part to this funding instruments and unlock better financing conditions. Also, current players profiting from such financing tool could take further advantages thanks to the cost reduction, faster procedures, and faster liquidity, if settlement occurs in T+0 instead of T+3. A 3 days reduction in a 30-days instrument represents 10% of the overall time, making even shorter-term securities attractive products.

All in all, supply chain finance seems to be one of the areas that could be more impacted by the adoption of blockchain technology, not only because banks are about to launch real products in the next months (e.g. UniCredit reported in an interview that its We-Trade

platform will be fully operative by the end of the year), but also because most of the processes are impacted by the possibility of adopting blockchain. Furthermore, we did not examine the advantages of integrating tracking blockchains with supply chain finance platforms, which could significantly reduce risk by giving a granular view of the shipping procedures and reduce cost of financing. Disregarding this solution was driven by the impossibility of effectively tracking real world assets with a DLT, as shown by the framework in Chapter 4: assets do not respect the internal predicate criterion, so, as of now, it would be impossible to deploy such solution. Should this issue be overtaken, it would then be possible to further increase the efficiency and automation of SCF blockchains, by using smart contracts that automatically move cash depending on the status of the goods and their physical location.

On the other hand, there are several limitations for blockchain technology adoption in SCF. As we have seen from the news, many institutional players are launching their own private blockchain platform, going against the possibility of fully cooperative business models. For instance, UniCredit is launching We-Trade platform in a consortium counting many other banks such as UBS, Santander and others, while Intesa Sanpaolo is partnering in Marco Polo project, a concurrent platform including different players such as ING, BNP Paribas and others. These projects will be described in detail in the following chapter, when we will discuss the interviews we have done to Italian banks. The divisions in the market can destroy the benefit of adopting a blockchain, as communication between the two consortia are still operated in a conventional setting. For instance, a UniCredit customer could not ask for a multi-bank factoring also including Intesa Sanpaolo. Finally, from the interviews it emerged that players offering such solutions are planning to sell them as complete products and infrastructures to other smaller players that could not allocate an adequate capital to participate in the development phase. This implies that nodes in the network are not actually peers, but there are strong hierarchies between them, and governance is still to some degree centralized in the hands of certain institutions (those developing the platform). This limit can be overcome if inter-chain communication is made possible in future research developments, allowing concurrent platforms to exchange data with each other, setting the only constraint in the institutions' willingness to do so.

Another minor problem is that of legal validity. There are no specific norms, at least in Italy, that address the validity and truthfulness of information recorded in a DLT platform. Consequently, this means that traditional method to communicate are requested, such as certified emails. We consider this as a minor problem because, as reported by SIA, the DLT platform can solve it by automatically detecting and importing this information on-chain with smart contracts and the correct software implementation.

5.10 Risk management and insurance

Risks are an integral part of all financial intermediaries' life. While providing financial services in imperfect market[93], indeed, they absorb risks associated with them. As we have already explained in previous chapters, market participants seek FIs' services because of their ability to provide knowledge and transaction efficiency, thus reducing frictions from asymmetric information and transaction costs (Santomero, 1997). Therefore, risk management plays a central role in intermediation as it can considered one of the factors affecting FIs' value (Schroeck, 2002).

Trading operations, for example, are among the ones generating the greatest risks for banks, baring the possibility of a value decline of financial instruments. Instead, insurances' greatest risk is that policy reserves are not enough to pay the claims to policyholders (Hull, 2015).

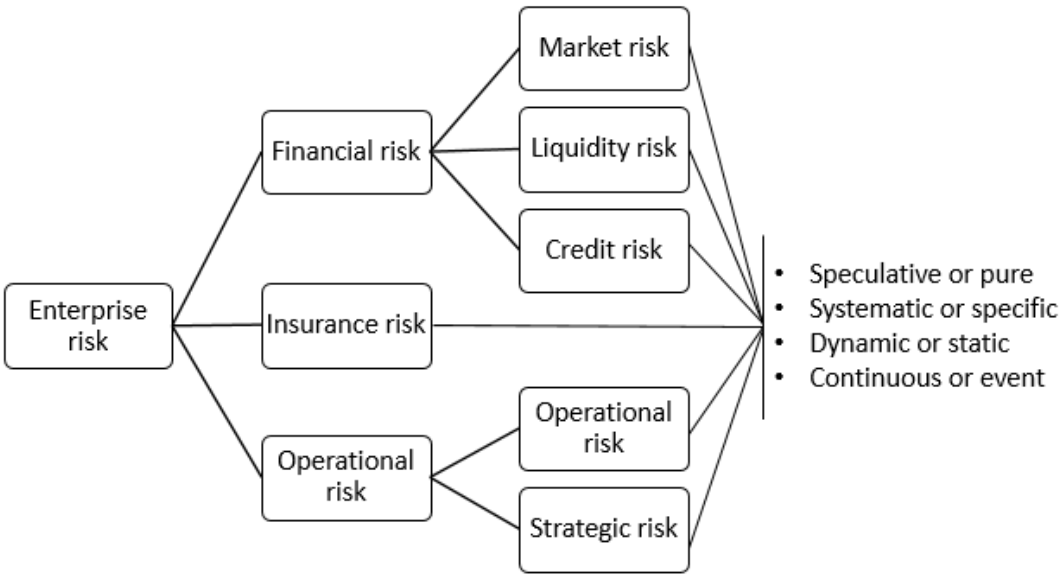


Figure 55, Risks typologies (adapted from Rejda, 2004; Koller, 2011)

Before going further in the description of the activities carried by risk managers, we should first provide a definition of risk. Even though there are many different typologies of risks, all of them have some common elements: the uncertainty about the future and at least one possible adverse outcome (Charette, 1990). As proposed by Vaughan (2008), '*Risk is a*

[93] An imperfect market is any economic market which does not meet the hypothesis established by Marshallian partial equilibrium model. It arises when prices and production can be influence by economic actors and when information is not known to all market actors. https://www.investopedia.com/terms/i/imperfectmarket.asp

condition in which there is a possibility of an adverse deviation from a desired outcome that is expected or hoped for'.

The risks faced by business firms can be named as *enterprise risks*. These include many different subgroups as it is showed in Figure 55. Financial risks can be defined as the uncertain occurrence of adverse event caused by changes of financial factors, such as interest rate, money value or foreign exchange rates. Among them we can list the market risks, the liquidity risks and the credit risks. The latter has been already explained in the chapter dedicated to loan activities. The liquidity risk is the possible lack of liquid assets for repaying duties when required. Market risks regard to the fluctuations of market prices, such as the ones belonging to commodities or to real estate, as well as equity prices (Rejda, 2004).

Operational risks concern all that risks related with the management of the firm, from both a strategic and an operational point of view. In the first case, the uncertainty regards to the possibility to implement the wrong strategy or to not being able to carry it out. In the second case, it both refers to wrong internal choices or executions or to external failures (Koller, 2011). All the above-mentioned groups can be classified in different ways.

A first distinction which can be made is between *pure and speculative* risks. The former leads only to losses, while the latter can have both positive and negative outcomes. Risk management usually deals only with pure risks, but with the Enterprise Risk Management, a relative new process helping managers in dealing with risks, speculative risks have started being considered too (Vaughan & Vaughan, 2008).

When the risk addresses a singular individual, a firm or an industry, it is known as *specific or particular*, while if it is inherent to the entire market or a large group within the economy is called *systematic or fundamental*. The latter are usually caused by economic, social or political phenomena. Examples of fundamental risks might be natural disasters or an unemployment cycle. As the latter cannot be treated through diversification, it is important being able to distinguish this typology from the former to being efficiently able to manage them (Vaughan & Vaughan, 2008; Rejda, 2004).

Depending on the cause generating the risk, which is known as *peril*, we can distinguish between *dynamic* ones, produced by changes in the economy, and *static* ones, all the others. Moreover, if the triggering event occurs or might occur frequently, such as changes in the inflation or in the exchange rate, it leads to *continuous* risks, otherwise, if it is a discontinuous episode, the associated risk is called *event* risk (Schroeck, 2002).

5.10.1 Risk management process

Risk management is the approach used to minimize the exposure to potential losses, by continuously assessing the risks the business firm is facing, which ones among them are to be prioritized and planning a mitigation action for them (Alberts and Dorofee, 2010).

A cyclic process is performed by risk managers as new risks may arise over time or previous ones might change, thus an adjustment of the plan is needed. Figure 56 represents the different steps composing this process. First of all, an adequate risk strategy of the firm must be defined. As the ultimate goal of a business is the creation of value, it has to ensure through an appropriate management of risk to preserve the operating effectiveness of its activities. This means that each institution has to set limits of acceptance for the risks and define therefore its risk appetite. The following step requires an assessment of the risk factors and the risk exposure of the firm. Information must be collected in order to effectively carry this activity out. Documents data and process flowchart of the firm can be analysed to have an overview of its past events and of the current operations, trying therefore to understand what and where risks affect the most. Risk Management Information System (RMIS) is an example of these instruments and it is a computerized databased used to store data and to use them for future predictions. Risk maps instead are tools used to analyse the different functions of a firm and assess where risks act. Lists of exposures and questionnaires can be other useful instruments (Vaughan & Vaughan, 2008; Rejda, 2004).

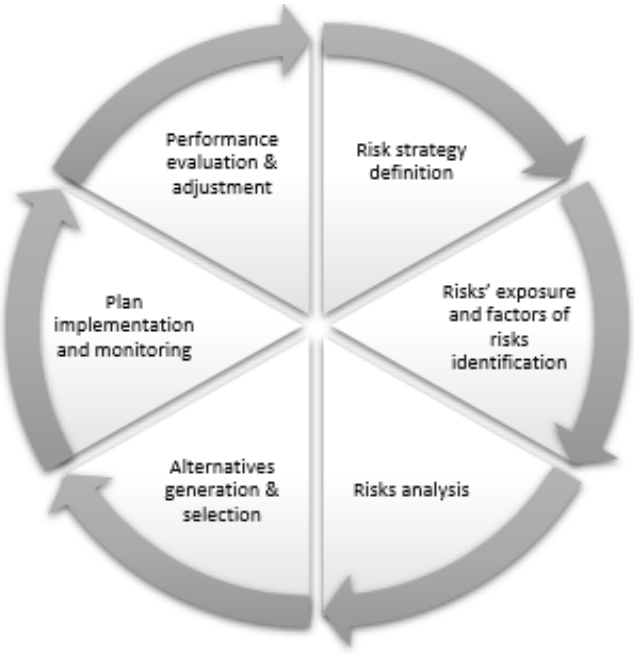


Figure 56, risk management process

Once the risks are identified, they should be analysed more in detail. Two factors have to be evaluated: the severity and the frequency. The former is defined as the size of the potential loss and we can distinguish four different typologies in decreasing order: catastrophic, critical, significant and important. The latter instead represents the number of times an event has the probability to occur, which in decreasing order are: likely to happen, possible, remote, and extremely remote. By combining these two elements in a graph, we can highlight three different areas of risks: critical, important and unimportant. This classification is used to prioritize the risks to be managed (Koller, 2011; Vaughan & Vaughan, 2008).

As we can see from Table 11, the level of severity and frequency are used to determine four different alternatives to react against risks. Depending on the values just calculated, the most suitable one can therefore be selected.

When frequency is high, the approach with which we deal with risk is known as risk control, whose purpose is the minimization of the risk of loss. On the other hand, the aim of the alternative approach, known as risk funding method, is to guarantee the availability of enough money to meet losses arising from the residual risks remained when risk control approach has been already adopted or cannot be adopted at all.

Severity / Frequency	Low	High	
Low	Retention	Transfer	Risk funding
High	Prevention & reduction	Avoidance	Risk control

Table 11, risk management matrix (adapted from Rejda, 2004)

Risk avoidance prevent a risk from originating. This choice should be taken when the direct management of risks would not carry any additional value to the firm or when no other techniques can be applied. A too intensive use of this approach might be limiting, as the institution could not being able to achieve its primary goals, avoiding carrying risky but profitable activities (Vaughan & Vaughan, 2008).

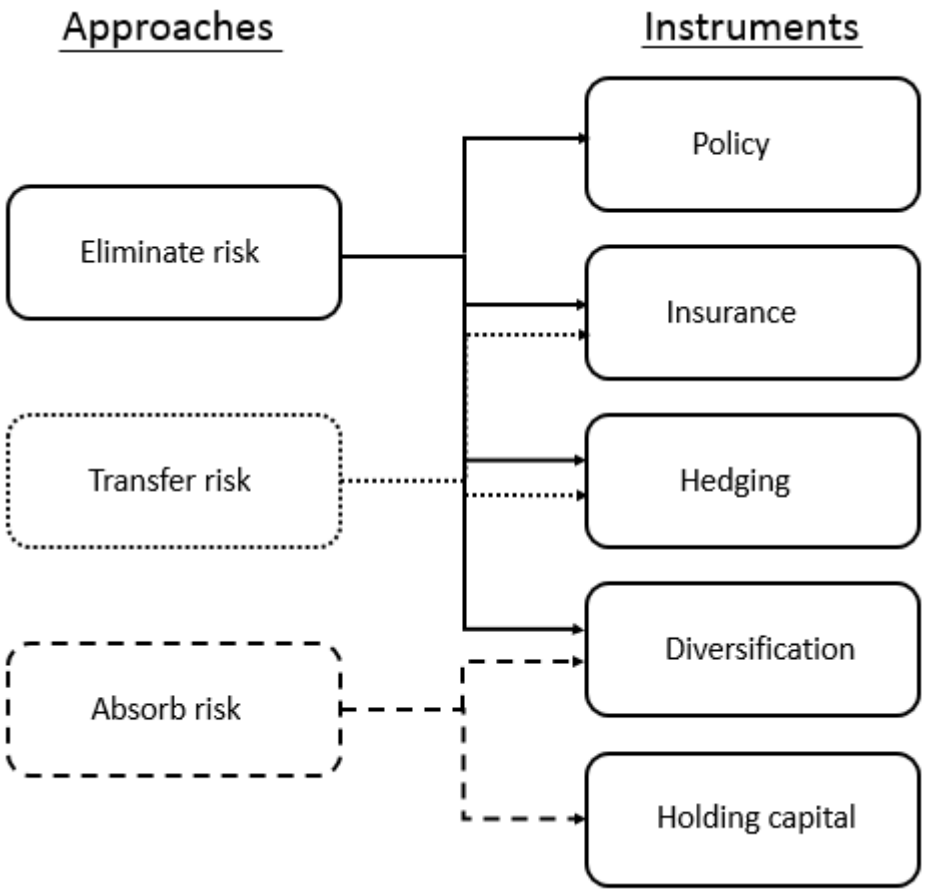


Figure 57, overview of ways to conduct risk management in banking

On the other hand, the risk can be completely or partially retained if two conditions are met: the losses are highly predictable, and the maximum loss is not severe. The choice of retaining losses can be voluntary or not; the latter occurs when no other risk treatment can be used (Rejda, 2004). The aim of risk prevention instead is the reduction of the likelihood of occurrence of a loss. The second intermediate approach to risk is the transfer. It can be done in two main ways, through insurance or non-insurance instruments, such as hedging for systematic risks or diversification for specific risks (Schroeck, 2002). Figure 57 represents an example of how and with which instruments a bank might approach to risk.

The fourth step of the process is the implementation of the chosen alternative. While implementing it, it should be continuously monitored, and its results should be reported. The purpose of controlling is to assess whether the taken decision is generating good performances or whether some corrective adjustments need to be made. Hence, it is necessary to evaluate if the risk management actions are meeting the overall corporate goals and if the operations are

going according to plans. The feedbacks are then used as input for the remuneration of the managers and as a starting point for the subsequent cycle (Koller, 2011).

5.10.2 Insurable risks

As we have seen, one of the possible ways to treat risks is through the use of an insurance. Yet, not all the uncertainty faced by a company are insurable. Firstly, insurance usually manage only pure risks. Moreover, risks need to meet five other specific requirements (Vaughan & Vaughan, 2008, Rejda, 2004):

1. There must be a large enough number of homogenous exposure units. The insurance companies, indeed, follow the law of large numbers[94] to make future predictions. Thus, exploiting a wide group of very similar cases, the estimations of future losses can be more accurate.
2. The chance of loss must be calculable. This prerequisite derives directly from the previous one. Thanks to the information the insurance firm can gain from the sample, it should be able to calculate with quite precision both the frequency and the severity of the risks. That is, it should be able to calculate an adequate value of the premium to ask to the policyholder.
3. The loss must be accidental and unintentional. As we just said above, the law of large numbers is based on random selected samples, thus, in order to obtain acceptable results from the predictions, the occurring events must happen by change, and not be caused on purpose.
4. The loss must be determinable and measurable. That means mainly that it must be hard to counterfeit it. In this context, it is advisable to introduce the concept of 'hazard'. The latter is the condition that creates or increases the losses. It can be physical or moral. The latter refers to dishonest behaviour of an individual which increases the frequency or the severity of a loss. Thus, this requirement is necessary to provide the insurer agent the capability to assess whether a claim is really covered by a policy or if it a fraudulent request for money.
5. The loss should not be catastrophic. This implies that many exposure units should not incur in an accident at the same time. Insurance, indeed, works through the concept of pooling, meaning that the losses of few are usually spread over a large group. Thus, it would have difficulties in supporting many concurrent payments, without an increase in the premiums. This condition is not as restrictive as the

[94] According to this, as the number of identically distributed and randomly chosen samples increases, then their average approaches their theoretical mean. http://mathworld.wolfram.com/LawofLargeNumbers.html

previous ones, as catastrophic events may sometimes occur. That is why some solutions have been developed to meet this problem. Reinsurance or financial instruments designed for this specific situation, such as catastrophic bonds, are examples of them. Moreover, insurance companies should avoid assisting people concentrated in the same geographical area, as they might be exposed to the same probable catastrophic loss.

Rejda (2004) proposes a definition of an insurance which perfectly summarises the requirements listed above, *an insurance is the pooling of fortuitous losses by the transfer of such risks to insurer, which commit to indemnify the insured for them*. Indemnification means that the insurance company economically supports the insured by bringing him/her to approximately her/his same financial position before the occurrence of the loss.

After defining which conditions a risk should meet in order to be insurable, we are going to describe which operations an insurance company undertakes to cover its clients against them:

- Rate making
- Underwriting
- Production
- Claim settlement
- Investments

As we have already explained in the chapter dedicate to loans, *rating* is the activity of determining the riskiness of a person or a company. The purpose of this operation is to subsequently determine an adequate price of insurance for them. Insurance rate, indeed, is defined as the price per unit of insurance. This activity is carried out by an actuary, who should be skilled in statistics and mathematics. He is in charge of calculating future likelihood of losses and then allocate them among the insured clients. Based on the rates obtained from the actuaries, the *underwriter* has to select and classify these values of exposure and then price applicants for insurance. The main responsibility of the underwriter is to guard against adverse selection. The latter is the tendency of people with higher-than-average exposure to losses to obtain an insurance at standard rates. Therefore, the underwriter should be able to identify the different categories of the applicants and charge extra premiums to the riskiest ones. Besides the exposure rates, the underwriter should collect as much information as possible about the candidates, compatible with the limitations of time and cost for obtaining them. Moreover, a keen sense of judgement is required to determine the adequate class for each exposure unit. An underwriter's additional task is the avoidance of concentration that might

generate catastrophic risks. This evaluation should be periodical in order to assess if any changes in risk exposures have occurred.

The *production* activities include sales and marketing. The agent in charge of them should sell insurance policy to the people indicated by the underwriter.

The *claim settlement* is a process during which the agent has to assess whether a request for reimbursement should be accepted or rejected. It is composed of four steps, as shown in the following image.

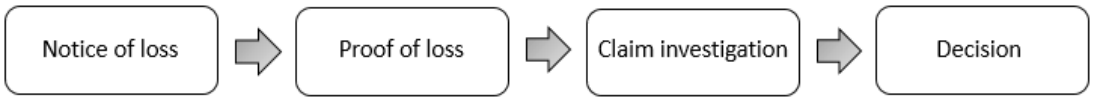


Figure 58, claim settlement process (adapted from Rejda, 2004; Vaughan and Vaughan, 2008)

Firstly, the insured has to notice to the insurance company the occurrence of a loss. The stipulated contract usually defines within which timeframe it must be declared, for example few days or hours. As a second step, the insured should provide documentation proving the occurrence of the damage. Then, the agent should examine whether a loss really occurred or whether it was due to a fraudulent action.

Hence, as we can see, the risk requirement of being measurable and determinable is of utmost importance. Moreover, the insurer has to evaluate if the claim respects the terms of the policy, such as, for example, if an injured physical property was completely covered, or if the cause of the adverse event was among the ones agreed in the insurance coverage. It is at this point that the insurer should also determine the amount of money that, where appropriate, would be released to the insured. In the end, after the completion of all the necessary evaluations, the insurer decides whether to deliver the payment or not.

Insurance companies collect large amount of money from premiums, which are usually not immediately needed for claim repayments. Therefore, instead of leaving them idle, the insurance companies commit in properly invest them. Bonds, mortgages and real estate are among the investment choices of insurance firms. As the money are needed for future clients' assistance, the primary requirement is the safety of the principal. Figure 58 represents an example of the operations usually carried out by an insurance company, which in this case refers to a property-casualty insurance, but the same flow can be adapted for all the other typologies we have examined in the previous chapter.

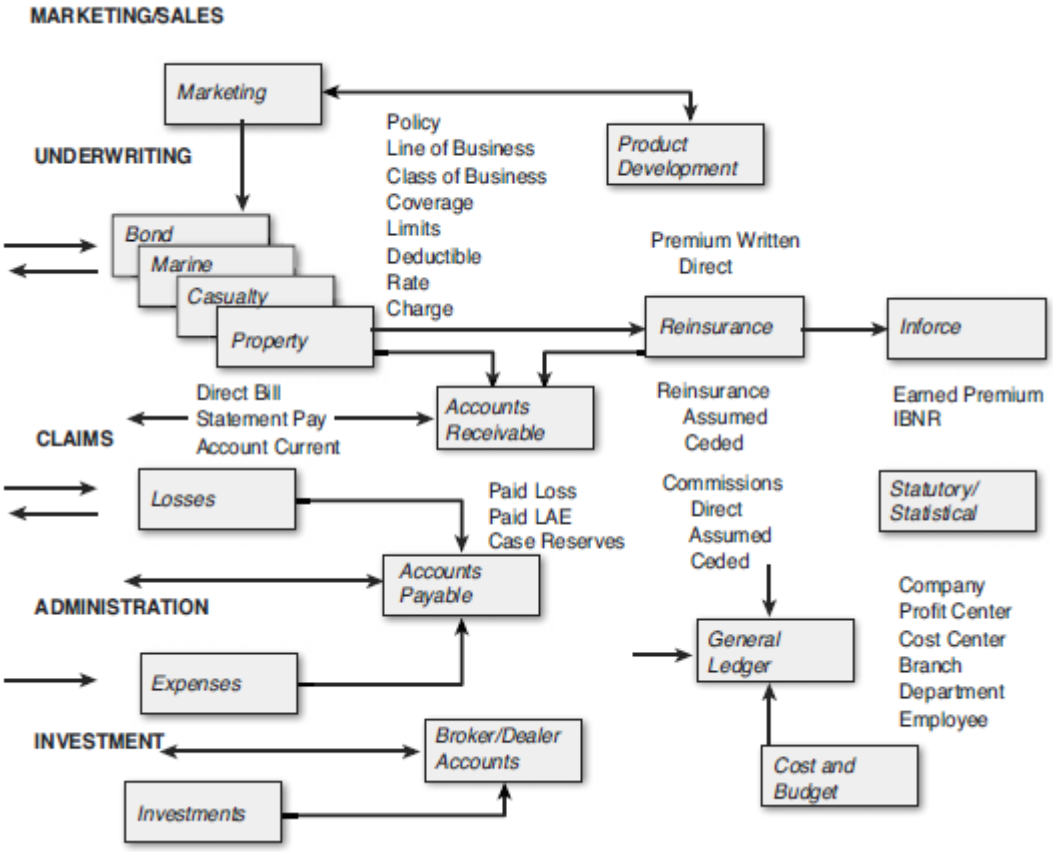


Figure 59, insurance company operations flow (from Vaughan and Vaughan)

5.10.3 New trends in insurance

As we have already said the two points of view of an insurance is the transfer of risk from an individual or a company to the insurance firm through the payment of a premium, and the risk reduction through the pooling. The latter is the risk-sharing mechanism in which members of a group agree to be collectively responsible for losses (Vaughan & Vaughan, 2008). Based on this consideration recent trends in the insurance industry are leading to the evolution of a new form of risk coverage, which is known as Peer-to-Peer insurance. It derives from the concept of self-insurance: an instrument which enables to achieve superior benefits, especially from an economic point of view, through an internally hold pool of risks rather than buying external insurance (Schroeck, 2002).

In P2P insurance, each member assumes a percentage of every risk underwrote by a member of the pool. The people who join together have similar insurance needs and starts with the same risk rating. Each of the member puts a certain amount of money into the pool. The advantage of this form of risk coverage is that usually premiums are lower than traditional

ones as there are lower costs to be sustained than the ones supported by big insurance companies. If a member of the team increases or reduces its riskiness level, then its premium would be risen or decreased with respect to the other members (Saha, 2016). In this context, there might be companies acting as brokers among the members, helping customer find others and create connections with them through their platforms or supporting in the management of the pool or in the claim settlement. Otherwise, the new wave of this trend is the self-governing P2P insurance, in which members directly manage the group and the claims[95]. The money pooled together is used as payments for claims. If no claims are made, then it returns to the members. The pool may provide a maximum limit to any insurer for a single loss. Otherwise, in the event of insurance claims that are too great to be covered, reinsurance can be used as additional support. Hence, depending on the typologies of P2P insurance and the possible additional used instruments, the money in the pool is used partially for paying the reinsurance premiums and/or the broker company, while the remaining part is used for claim payments or is given back to the members[96]. Besides economic factors, this risk sharing has additional advantages, such as the speed in managing claims and the ease of use, thanks to the elimination of the complex bureaucratic process of dealing with traditional insurers.

Insurance companies can also gather together, in what are known as reinsurance pool. This is an organisation which underwrites insurance on a joint basis, when single insurers alone may not have the financial capacity to write large amount of policies (Rejda, 2004).

5.11 Blockchain-enabled risk management and insurance

Now we shall review how startups and companies are using blockchain to bring in value in the insurance business.

Startups received little financing compared to other categories: the 7 reporting gathered funds received €13.091.000, amounting to 0,43% of total financing. Here, 3 startups provide skills and competences to insurance players willing to adopt blockchain technology, 4 provide customers with new products in a competition logic with traditional and new P2P insurers. The remaining one offers easier reconciliation and communication between the parties involved.

[95] https://www.the-digital-insurer.com/blog/insurtech-teambrella-and-the-third-wave-of-peer-to-peer-insurance/

[96] https://home.kpmg.com/xx/en/home/insights/2017/09/is-p2p-insurance-a-sustainable-business-model.html

On the other hand, companies were involved in 14 initiatives, 4,79% of the total, 3 of which are already operative, whereas 6 are still in a PoC phase. Traditional insurers focused their attention on the potential for blockchain technology to reduce costs and streamline information, applying it in maritime insurance (1 operative initiative), and reinsurance processes (1 operative initiative). Other areas being studied are healthcare insurance (2 PoC), life insurance (1 PoC) and travel insurance (1 operative initiative and 3 PoC).

Number of startups	Average financing	Total financing	Percentage of total
8	€1.870.142,86	€13.241.000	0,43 %
Amount of news	**Operative**	**PoC**	**Percentage of total**
14	3	6	4,79%

Table 12 reports data for insurance startups: the number of initiatives average financing received (in euros), total funds received (in euros), and the percentage of the funds received over the total. For companies, it reports the number of news for insurance initiatives, how many of the projects are already operative, which are PoC and the percentage over the total amount of news

Other applications reducing risks such as compliance risk, operational risks, liquidity risks etc. are mentioned in the other sections, depending on the risks generated by the specific process. Since we could not find any initiative specifically addressing this area, we shall now focus on insurable risks.

5.11.1 Areas of application

As we mentioned, 4 startups[97] are focusing on new P2P insurance products enabled by blockchain technology. The main difference between blockchain enabled P2P insurance and P2P insurance is the absence of a real intermediary since most of the processes are automated in smart contracts and deployed on a blockchain. New users have to insert certain parameters and their rating is computed via public code available on smart contracts, cutting the need for agents or brokers. The premia are therefore computed based on existing data and deposited in the smart contract's account. Should an incident happen, an expert or the community pooling premia has the chance to vote if a reimbursement should be paid and how much it should be, or if the claim is not eligible. If the payment takes place, a transaction is initiated by the smart contract towards the recipient account so as to cover the incurred damage. If the parties do not incur in any loss thanks to particular care to the insured good (such as careful driving in car insurance), the pooled money reaches an excess threshold and the smart contracts split the exceeding deposits between the insured, allowing a cash back to customers. Part of the money

[97] Such as: https://rega.life/ and https://www.wegroup.be/en-home

is still held by the smart contract and sent to the company as a fee for the model implementation, the payment of experts, the maintenance and other costs, so, even in the best-case scenario, the cash back will never be 100% of the deposited funds. According to the adoption framework, this business model leaves many open issues and is quite challenging in the implementation phase. First, a correct assessment of the claim seems unlikely only by digital means with current technologies: an expert could hardly tell the amount of damage a property has faced just by looking at pictures; secondly, customers could take an opportunistic behaviour and submit fake pictures to obtain undue reimbursements, and the startup has no capacity to prove fake claims. These issues are concerned with the oracle problem in smart contracts: untrusted source of information can interact with the blockchain to influence its actions, thus infringing the internal predicate criterion. In addition, serious concerns arise in the case of badly programmed contracts, as we explained in the technical analysis section. All in all, it seems that these companies propose interesting business models, but do not explain how they are planning to solve open issues with public blockchains that hinder the implementation.

A startup[98] that is instead collaborating with traditional insurance players aims to provide a shared data infrastructure for insurers, reinsurers, brokers and customers to remove the bordereau[99] process. The platform used the Quorum blockchain, but then moved to the Corda due to reported better performance and meeting privacy requirements. The product is live already since September 2017, allowing insurance companies, firms, reinsurers and brokers to avoid expensive reconciliation procedures, reduce operational risk due to communication mistakes thanks to the employment of a DLT infrastructure. A common solution to this issue is the employment of a software provider who can keep all data reconciled in his own centralized database; however, this entails that a disproportionate amount of power and knowledge is detained by the centralized entity, something that insurers can circumvent by implementing a DLT solution. Furthermore, the startup is planning on the release of new products in the future, such as smart contracts managing and preventing the abuse of underwriting authorizations, reinsurance arrangements controlled on the ledger, smart contracts automatically reimbursing claims, and automation in settlement after the approval of a claim still through smart contracts.

Considering traditional insurers' projects, we shall first review the operative ones. The first is a project by Maersk, a shipping company, that created a blockchain to platform to record transactions in the maritime transport. This solution has strong implications for maritime insurance, as having all parties verify where the goods are and who is managing them

[98] https://www.blocksure.com/

[99] The production of an extract containing all transaction information from an institution. It is then transmitted to other parties involved so that data can be reconciled.

is a great advantage to reduce risks; especially, in case of claims it is easy to assess correctness and ownership. The main reported issue with the platform, which is already operative, is the little participation from Maersk competitors who maintain that resorting to Maersk platform and paying fees to access it would further increase its leadership in the industry. So, as in trade finance, also in this area we find that solutions developed autonomously by one player might end up missing the benefits of a ledger shared across the industry.

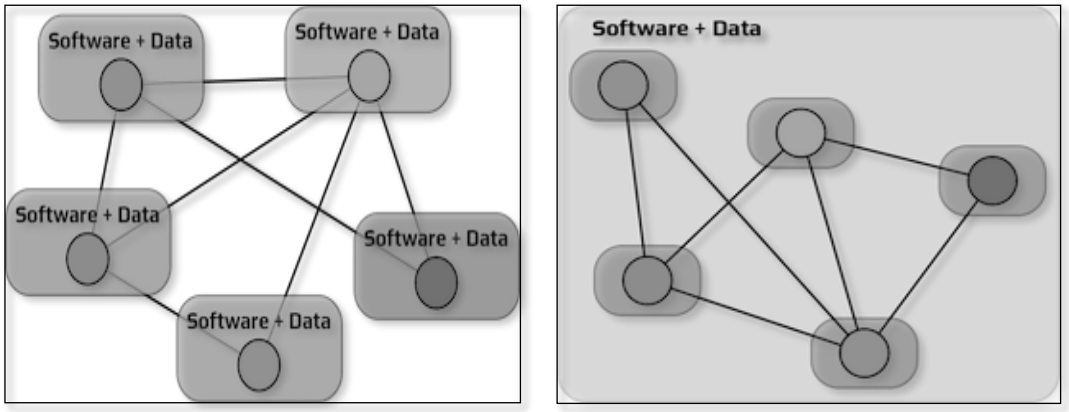


Figure 60, current interactions in the bordereau process (left-hand side, each circle represents a different actor) against blockchain-enabled borderau (right-hand side).

Another live initiative is that of B3i insurance consortium[100], which is also deployed, allowing to streamline reinsurance information and transactions across all parties involved. Typically, in a reinsurance setting a cedent, a broker and a reinsurer are involved. Using a DLT infrastructure communication and transactions between parties can be easily recorded and reviewed removing the need of reconciliation and other expensive and error-prone processes, such as the already explained bordereau. Besides, the application also manages settlement of relevant accounting data and asset transfers which are digitally traced by the ledger.

Finally, AXA launched a travel insurance which reimburses claims automatically[101]. Indeed, the insurance company tested a blockchain infrastructure that shares data with airports and aircraft companies. When a customer subscribes the insurance product, a new smart contract is created in the Ethereum public blockchain with relevant information about the company, the flight and the conditions under which a reimbursement is foreseen, e.g. only for delays greater than a certain threshold. The smart contract also has access to aircraft companies' database, where it can read relevant data. If a flight is actually delayed, and its delayed status is confirmed after the departure time, the smart contract detects this information in the aircraft companies' database and automatically triggers a reimbursement

[100] https://b3i.tech/our-product.html
[101] https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy

for the client by sending a confirmation to AXA servers which then trigger the payment in fiat currency. In this kind of solution, some problem still exists concerning the public blockchain where the smart contract is deployed, which could cause relevant fees for the company to run the code and exposes the product to risks, such as forks or presence of bugs in the smart contract code. Anyway, fees are probably much lower than those of the traditional process which entails paperwork, a large effort for the customer to detect if he is eligible for the reimbursement, and a double-check by the insurer to verify that the customer is actually eligible so that it can grant the payment. As for risks concerning the smart contracts, the code can be tested, and professionals exist to check its robustness, so, it can be limited.

Other projects concern bancassurance[102], that is, banks leveraging their customer base to sell specific insurance products. In this area, blockchain is employed to streamline information and transactions between customers, banks and insurance companies, in a similar fashion to the reinsurance business. Other deal with health and life insurance[103]: in this area, only PoC have been developed so far, yet, there seems to be a high potential for blockchain technology, as it can provide a unique ledger where both hospitals, insurances and customer can store and access selectively to information. This would be a great benefit for insurance companies and their customer in the streamlining of documents, receipts and other proofs of undergoing treatment in a health facility: with blockchain the customers would not be required to send their clinical reports to insurers, but just provide permission to access them on the blockchain, so that smart contracts can provide reimbursement for medical treatment automatically. Should DLT be applied in this field, a large cost reduction would benefit most parties involved; the bigger hindrance is the need to onboard many different operators in a single platform to make the adoption worth.

All in all, also insurance can have some benefits from blockchain technology adoption. As of now, the first applications and PoC are revolving around the streamlining of information and transaction data across different players in processes that require to do so. Pioneering application come in the field of travel insurance where the claim management is completely automated, thus reducing both the hassle for the customer and the costs for the insurer. Much bigger cost benefits could come if claim management through smart contracts could be effectively applied in other areas, still, the biggest issue to widespread adoption is that of finding trusted oracles to circumvent the internal predicate criterion. Indeed, information that is collected outside the blockchain to activate smart contracts is prone to errors, forgery and tampering: if such information gets on-chain and is processed by smart contracts, undue

[102] https://www.coindesk.com/big-four-chinese-bank-launch-blockchain-bancassurance-product

[103] https://www.coindesk.com/us-insurance-giants-unitedhealth-humana-launch-blockchain-pilot

reimbursement could be started, with irreversible transfer of funds to ineligible customers, a major risk for insurers. So, the most impactful applications in the insurance world are still on hold, waiting for experts to find a solution to the smart contracts' oracles problem.

5.12 Fiduciary services

Personal fiduciary services consist of all the offerings proposed by financial institutions committing to manage assets on the behalf of a third party, being this an individual or families. They are often referred to as private banking services, to distinguish them from the ones offered by retail banking. Indeed, the former usually builds with the client a one-to-one relationship, proposing solutions tailored to the customer's needs, while the latter provides mass customized products and services to its clients (Resti, 2003).

Private banking refers to clients with high capital availability, committing to manage their assets in order to maintain/increase their value. In Italy, the minimum sum required to ask for a private banker is 500,000 euros (BCG & AIPB, 2017). This characteristic distinguishes this offer from the personal banker, which instead addresses to investors owning lower income. Wealth management includes many services: not only the capital control, but also the evaluation of possible investments in real estates or in other luxury products, such as pieces of art, jewelry, or fine wine, as well as the legal, insurance and fiscal consulting. The private banker does not refer only to individuals for private ownership but also to entrepreneurs who wants assistance with their own working assets.

We can distinguish different typologies of client referring to the private banking (Zanaboni & Oriani, 2008; BCG & AIPB, 2017):

- Affluent: owning less than 1 million dollars
- Lower High Net Worth Individuals: owning between 1 million and 10 million dollars,
- Upper High Net Worth Individuals: owning between 10 and 25 million dollars,
- Very High Network Individuals: owning between 25 and 30 million dollars,
- Super-High Net Work Individuals: owning between 30 and 50 million dollars,
- Ultra-High Net Worth Individuals: owning at least 50 million dollars.

From a global point of view, 53% of the clients are affluent, but they represent only 11% in terms of managed wealth. Instead, only 9% of the client owns more than 10 million dollars but they represent 54% of all the managed wealth. Conversely, in Italy, 50% of the managed wealth belongs to people owning less than 10 million dollars (BCG & AIPB, 2017). The birth of the private banking sector is due to a recent trend: the concentration of the wealth in the hand of

high-class people, against the affluent. Therefore, the money belonging to the target clients of this sector are increasing, as well as their needs for advisors for an efficient management of their capital.

In Italy this trend, despite being present, is less strong, and the request for private bankers derives from the culture and the economic environment. Individuals tend to save money and there are several family SMEs, which require the assistance of a financial specialist to deal with the management of the capital from one generation to another (Polimeno, 2009). Indeed, the entrepreneurs represent around the 70% of the costumers of the private bankers (AIPB, 2015).

The private banking is a growing market. Actually, according to a Magstat Consulting research (2018) the financial asset managed by specialized operators grew by 4.9% between 2016 and 2017, from 869.5 to 912.5 billion euros. This amount has grown by 338.8 billion euros since 2008. In Italy, in 2017, 259 financial institutions were operating in this sector, comprehending banks, SIM, asset managers, SGR, insurance companies and consulting companies. It is a concentrated market, in which the first three, which are Fideuram, Unicredit and BPM, control 27.9% of the total, and the first 10 control 51.7% (Valentini, 2018). The process of wealth management consists in a continuous interaction with the customer to understand his/her needs and investment objectives, then evaluate his/her financial situation and propose diversified and ad-hoc portfolios.

5.13 Blockchain-enabled fiduciary services

In this area, we found very few startups and news regarding companies. Overall, there are 7 startups dealing with the topic which gathered very few funds, amounting to just 0,17% of the total. On the other hand, news from financial players are just 3, of which none operative and only 1 PoC that had no follow up, amounting to 1,03% of the total.

Number of startups	Average financing	Total financing	Percentage of total
7	€7.746.451,71	€ 54.225.162	1,75%%
Amount of news	**Operative**	**PoC**	**Percentage of total**
3	0	1	1,03 %

Table 13 reports data for fiduciary services startups: the number of initiatives average financing received (in euros), total funds received (in euros), and the percentage of the funds received over the total. For companies, it reports the number of news for fiduciary services initiatives, how many of the projects are already operative, which are PoC and the percentage over the total amount of news.

Actually, startups are not really using blockchain themselves in the initiatives, rather, they offer customers funds, analytics techniques and advisory in case they plan to invest in cryptocurrencies. Therefore, they can be seen as accessory services surrounding the world of cryptoassets. On the other hand, companies announced initiatives in the field, but only BNP Paribas[104] planned to launch a ledger to track fund distributions and ease the asset management process, especially in the servicing procedures. Nevertheless, this news has no follow up, despite being reported well over a year ago, no further announcements have been made in this direction, hinting that the project was probably dropped or postponed in favor of more promising ones.

In conclusion, this area does not seem to be very fertile for blockchain adoption: indeed, it is evident that blockchain and DLT best fit in a context where transactions take place, or something has to be recorded in an immutable and decentralized way. In this field, interactions happen bilaterally just between the private banker and the customer, and, according to our framework, the need for a blockchain is ruled out. Yet, we included these startups in our research because we think it could be an important are in future development: many hedge funds are already trading on cryptocurrencies, and the introduction of derivatives increased the possibilities of hedging excessive risks on cryptoassets. Incorporating competences and knowledge about this market could be positive for private bankers so as to expand their product offering, especially considering studies that explicitly show how the inclusion of differentiated blockchain investments can benefit on profit reducing the pressure on fees structure (Kaal, 2017).

5.14 Know Your Customer

In the previous sections we described the main functions financial institutions perform. Together with that, we happened to mention some important side activities that need to be taken care of to ensure the correct deployment of services. These are entailed with regulatory compliance with AML/CFT norms which can be summed up in the KYC requirements. In this section, we shall describe the current status of KYC procedures, and how blockchain can possibly improve them. Previously, we showed that financial institutions are highly subject to risks. The innovation brought in the financial sector has improved and eased money transactions, but on the other hand it has also enhanced those of illicit funds. According to the estimation of the United Nation's Office on Drug and Crime, these illegal transfers account for around 2 to 5 percent of the global GDP, which means 2 trillion dollars[105]. According to the

[104] https://www.coindesk.com/bnp-paribas-taps-blockchain-fund-distribution-platform
[105] https://nikegroup.it/it/articolo/aml/

Basel Committee on Banking Supervision (BCBS)[106], an adequate control over the banks' potential and already established customers is necessary for an efficient management of the banking risks and for preventing losses (Basel Commitee on Banking Supervision, 2011).

Over the years, many laws have been enacted to fight these problems, but despite substantial compliance investments to adapt to the requirements, the frequency and impact of illegal incidents remain significant. For this reason, regulators have further increased the pressure on banks regarding their clients' control (Memminger, Baxter, & Lin, 2016). In Europe, indeed, anti-money laundering directives have been passed since 1991, with some adjustments in 2001 and 2005 (AIRA, 2005). The fourth and last directive entered into force in June 2017, with a new set of rules to help financial entities to protect against the risks of money laundering and financing of terrorism. These requirements affect anybody who provides credit (King, 2018):

- Credit institutions, including car rentals and telecoms
- Financial institutions
- Auditors, external accountants and tax advisors
- Notaries, legal professionals
- Traders of goods valued over €10,000
- Gambling service providers

The requirements of this directive are the minimization of risks through the understanding of the customers and their financial dealings. The Know-your-customer policy, commonly referred to as 'KYC', is a compulsory framework for customer identification. An individual identity must be checked when (AIRA, 2005):

- a continuative relationship is going to be built
- sporadic transfers occur with a value equal or higher to 15.000 euros, no matter if with a single operation or with several ones
- there is a suspect of money-laundering or terrorism funding
- the collected data for a previous identification is considered as suspicious

KYC process is developed as follows:

[106] BCBS is the authority established by the central banks' governors of the Group of Ten countries in 1974 for providing enhancing cooperation on banking supervisory matters. https://www.bis.org/publ/bcbs213.pdf

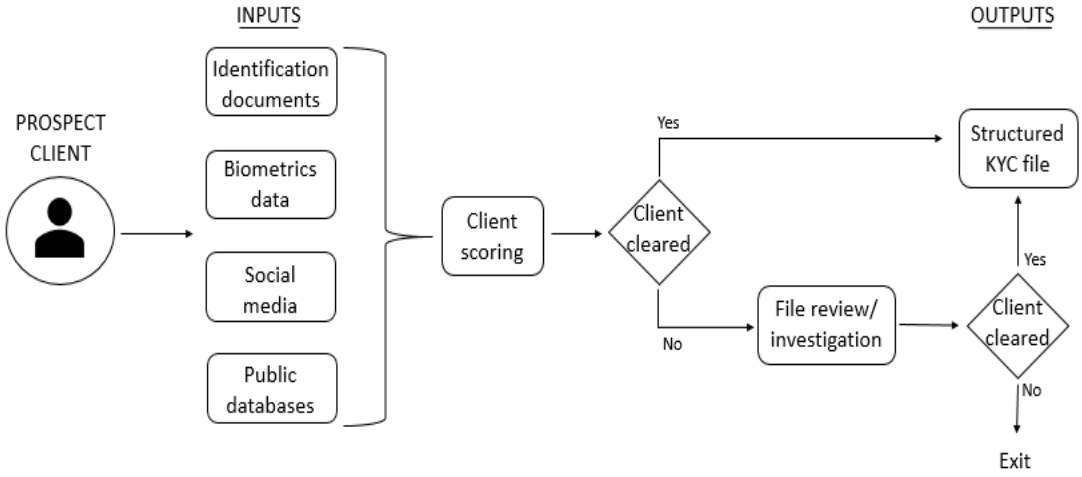


Table 14, KYC process (adapted from Memminger et al, 2016)

It starts with the checking of the client's documents for recognition. Still nowadays this task is often carried out manually and using paper, which results in being costly and time-consuming. However, a digital recognition is also possible. In this case, data are collected from many different sources. Official documents' information is combined with public ones such as credit and criminal databases, commercial registers and social media. Biometric checks, such as facial recognition and fingerprints are also used. The purpose of this task is having as many data as possible to score the client and, after some supplementary reviews, to profile it. Additional controls can also be executed: a confirmation certification from other financial institutions subject to the same directive may be required (Memminger, 2016; Thavanathan, 2017). Besides European countries, indeed, other countries worldwide commit to collaborate to guarantee the integrity of the financial structure[107]. This process does not ensure that all the requiring prospects will be accepted. It may happen that the individuals are not able to prove sufficiently their identity, thus being cut off from accessing basic services and rights. According to World Bank's 2016 ID for Development initiative, approximately 1.5 billion people around the world cannot prove their identity (World Bank Group, 2016). Being able to assess and record other types of information, such as the biometrical ones we mentioned above or medical treatments as vaccinations, would be an optimal solution for the inclusion of this part of the population. Combining different sources of information and share them in a unique register would facilitate the process of client acceptance (Patel, 2017).

The files regarding the identity of the customer and the risks associated with it must be subsequently saved and kept in the banks' databases. Moreover, they should be periodically revised to assess if any changes with respect to the ones in the data have occurred. The process

[107] Argentine, Australia, Brazil, Canada, Japan, Hong Kong, Mexico, New Zealand, Russian Federation, Singapore, USA, Republic of Sud Africa, Switzerland

described above is the example of how the rules set by the directives have been implemented. However, it shows some drawbacks:

- Building a new relationship with a prospect is a long and complex journey. According to a Thomson Reuters survey (2017), indeed, the customer onboarding time increases 22% in 2016 compared to the previous year.
- The costs associated with it are high. A study conducted by Bain & Co (2016) estimated that the costs for governance, risk and compliance account for 15/20% of the total banks' expenses to run them. In 2013, for example, JPMorgan added 5,000 employees to deal with compliance tasks and spent an additional $1 billion on controls. Thus, small institutions may have difficulties in coping with these expenditures (Callahan, 2018).
- Customers may be required to provide the same data several times to different institutions as they do not share the information. Moreover, data redundancy may occur among different functions of the same institution too, as they may not be connected through the same file record.
- Privacy issues may arise. Customers sometimes resent having to provide all the requested information and they may consider annoying the recurring requests for updates used to revise the data.
- Lack of passport or identity documentation access excludes people from being accepted and therefore registered by financial institutions. This leads these people to turn to other non-traditional financial instruments, not under the control of regular institutions and governments, thus increasing the risks of illicit actions.

Moreover, in May 2018 the GDPR, General Data Protection Regulation, came into effect. This 200-pages-paper defines how companies should manage, process and delete data, thus making the compliance with the AML and KYC regulation even more difficult (Blinking Team, 2018). The complexity lies in balancing between the need for protection obtained through the collection of more information about users and their activities and the respect for the same users' privacy, according to GDPR. Institutions should therefore adjust the way they gather, store and manage KYC data, which still results being essential operations. First of all, the KYC process must be completely transparent, clearly defining which data are needed, for what purposes and for how long they would be kept. Users must have more control over the information they provide, having the rights to delete them or to transfer them to other organisations and being notified if the data have been compromised in any way. To cope with this, more automation is needed. The increasing number of collected information must be ensured from being inappropriately shared, maintained, stolen or altered. Thus, automation

can minimize the risk of data manipulation and damage caused by human errors (Kennedy & Harney, 2018). An adequate solution to the problems highlighted above is an instrument which makes the process fast and easy-to-use, able to preserves customers' privacy and security, which prevents the redundancy of information through shared files among many institutions, and which includes many sources of information for people recognition. Through immediately available KYC information, financial institutions may spend more time in data analysis instead of collecting and checking such data (Patel, 2017). KYC utilities, like Swift's Registry108, can address inefficiency by splitting the costs of the compliance among many institutions and profiling customer once on behalf of all banks. Each member keeps the control over its own data, defining who can access to them.

5.15 Blockchain-enabled Know Your Customer

Blockchain could bring value in the correct management of KYC data and procedures, while still complying with GDPR regulation. In this area, 20 startups studied the impacts of DLTs on identity management and came up with advanced products, either with KYC specific platforms (7 startups) or with general identity platforms to serve financial intermediaries (13 startups). They gathered €103 million, 3,33% of the total.

Companies are testing blockchain for KYC procedures too, with 31 initiatives of which 1 is operative while the other 13 are PoC.

Number of startups	Average financing	Total financing	Percentage of total
20	€ 5.157.750,60	€ 103.155.012	3,33%
Amount of news	**Operative**	**PoC**	**Percentage of total**
31	1	13	10,61%

Table 15 reports data for KYC startups: the number of initiatives average financing received (in euros), total funds received (in euros), and the percentage of the funds received over the total. For companies, it reports the number of news for KYC initiatives, how many of the projects are already operative, which are PoC and the percentage over the total amount of news

Both startups and companies are focusing on the same application for blockchain technology: identity and KYC data. The current process for a company to manage customer

[108] Launched in 2014, The KYC Registry is a secure, global utility which nearly 4,000 correspondent banks and funds players use to contribute, share and consume a comprehensive set of KYC data and documents. The Registry helps financial institutions streamline the exchange of know your customer information to support KYC compliance.
https://www.swift.com/news-events/press-releases/swift-extends-kyc-registry-membership-to-all-supervised-financial-institutions

data is that of assessing and collecting initial information to store on their own server. If a customer interfaces with more than one company requesting personal data, the procedure and the data itself is replicated across multiple databases, making it difficult to keep the information up to date as each company would need to prompt the customer with update requests. The same goes for the KYC procedure: we showed in the previous section that if a customer wants to interface with different financial companies, at the moment, he is forced to present each of them with the data requested, duplicating the effort of the customer and costs across many institutions.

Blockchain could help reducing these costs and making the KYC documents registration happen only once for every customer, also enlarging the competition in the market as customers are no longer disincentivized in changing their current institutions for a different one by long and procedures. In fact, the technology could be leveraged by banks as follows: a private blockchain could be set up, where banks store customer data once they complete KYC procedures; then, should the customer visit a different institution, such institution could request access to the data stored on the ledger, with the authorization of the customer.

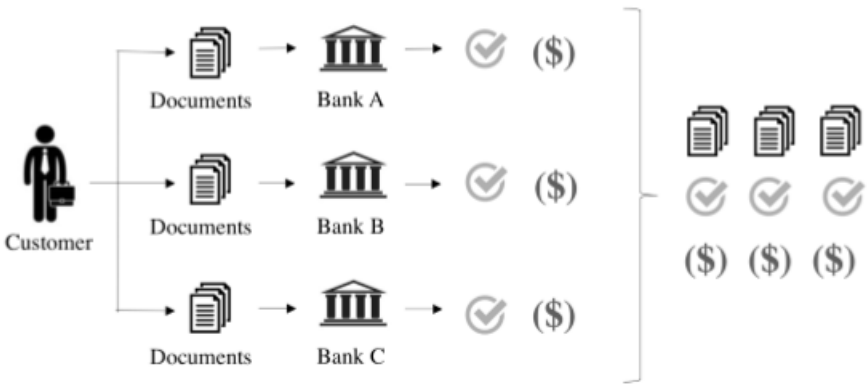


Figure 61, a representation of the current duplication in KYC procedures.

In this way costs would be sustained just by the first bank recording a new customer, whereas other banks would only need to pay a fee to see the data. To do so, the customer would have to share his private key with the institution he wants to access data. More efficiently, banks could set up a common interface that customers can access to share their data, such data all costs would be split among all banks, as shown in Figure 61.

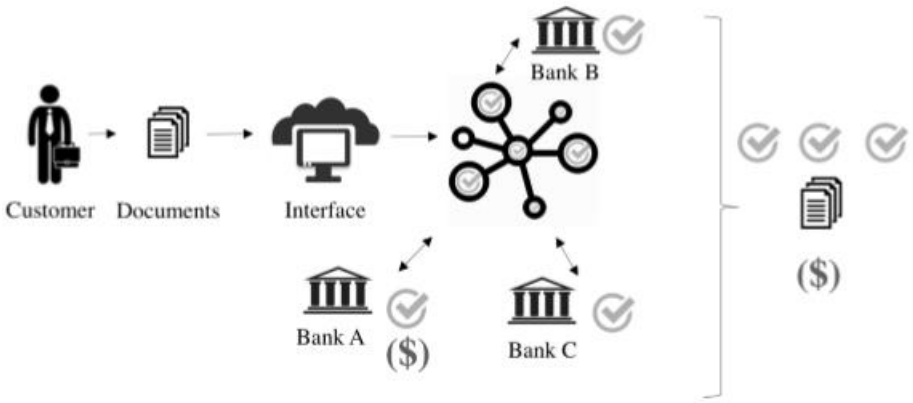


Figure 62, a representation of the to-be process for blockchain-enabled KYC assessment. Costs are shared rather than duplicated.

One could raise two issues with this configuration: the first would be that the usage of a common centralized database would be more effective than a DLT (as shown in the adoption framework), secondly, that data on a DLT is immutable so it cannot be cancelled to comply with GDPR requirements. In the first case, a centralized database would indeed be better performing than a distributed architecture, but a centralized database entails a centralized governance in an entity that has full access to all customer data and has a view of all banks' customers, thus being definitely non-GDPR compliant and reducing control and value single banks could generate with proprietary data. As also emerged from interviews, no bank is willing to work in such environment: a similar business model could have been achieved with technology existing also 20 years ago, but none implemented it for this very reason. Concerning GDPR requirements, we refer to Moser (2017): in general, GDPR applies to data that can be reconnected to a person's identity, so, a simple encryption of data is not enough to comply with GDPR due to the possibility of reconstructing the linkage with proportionate means. So, Bitcoin blockchain for instance does not comply with GDPR requirements. Private blockchains, instead, meet GDPR requirements as they are not publicly verifiable, and data is protected by the private network of the institutions involved. Cancellation can be achieved by eliminating the private keys needed to access data for each specific customer: if a client no longer wishes to conduct business with a certain institution and demands that his data is cancelled, the institution can erase the private key of such client from its database and it will not be able to access data anymore.

Finally, the benefits of economical KYC procedures can become enablers for different business processes that are now constrained by such high costs. One we mentioned already is in SCF programs: a bank looking to interact with multiple suppliers ends up spending hundreds of thousand euros just for these procedures. A single-time KYC can enable new opportunities and new products in the SCF area, driving down compliance risks and costs.

Another benefit we did not discuss is that of cross-border payments: due to de-risking practices[109], banks closed relationships with correspondent banks in many countries (Patel, 2017).

Driving down KYC costs could expand back banks' business in risky countries. This could be achieved by keeping records in a distributed ledger, setting up a single template to file data and reports, thus also achieving standardization. When a developed bank has to transact with a bank from a risky region, it will have access to its customers' relevant data, such as the kind of document provided, or the amount of the yearly transactions processed. With this data, the bank could judge better if a transaction can be carried out or too many compliance risks arise. At the moment, profiles are available only to banks with direct correspondent relationship, and clients' transaction details are limited to the customers' banks, so, with a DLT infrastructure supporting shared data, a big improvement could be attained in this area.

5.16 Adoption framework in financial services

In this chapter, we leveraged the empirical data gathered to show if and how BCT could solve existing issues in as-is financial processes or offer new products. From both our database we found that blockchain can be effectively applied to most financial areas: 242 startups received a total of €3 billion financing on blockchain projects, and 31 of the 292 financial intermediaries' initiatives are already operative, while 141 are PoC. Our detailed discussion of use cases showed that the areas of payments, investment products, supply chain finance and insurance are the most advanced, as 84,82% of the startups' funds concentrate on these areas, and 241 companies' initiatives were counted, of which 28 are already operative and 119 are PoC.

This allowed us to produce the framework in Figure 63, detailing where blockchain can have a beneficial impact in financial services. Fully feasible and already existing blockchain-enabled processes are encapsulated with a filled line. Processes where some limitations exist are surrounded by a dashed line, that is, claim management, because, as we discussed, only for yes/no policies it is possible to manage the claim automatically, since the assessment of a variable reimbursement is not automatable. The area where blockchain does not seem to have any application is that of fiduciary services, a fact we pointed out by inserting a grey box.

[109] Reduce compliance risk by not operating in certain countries, with certain currencies, or with certain customers.

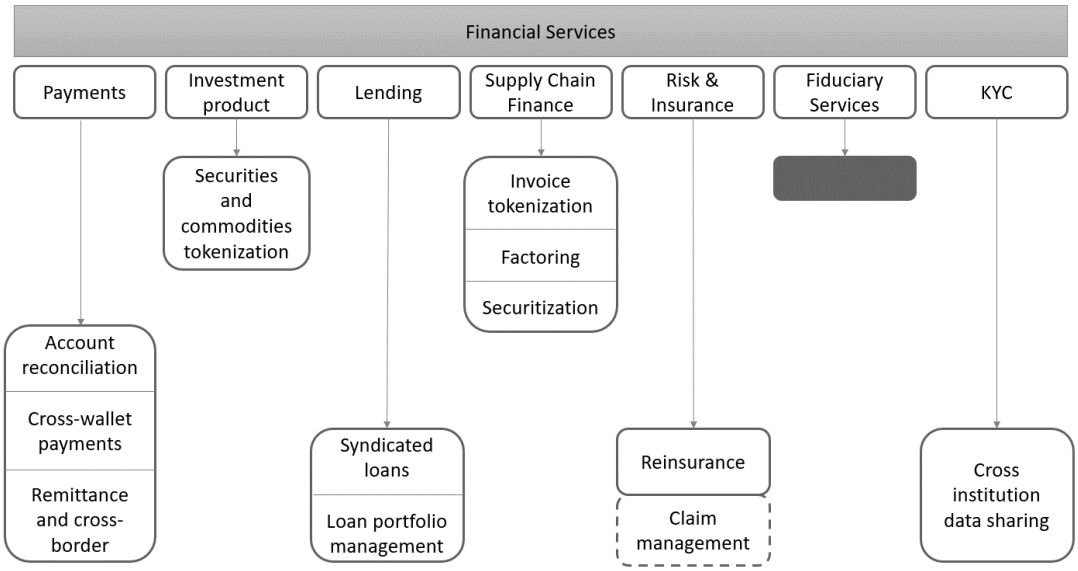


Figure 63, adoption framework for financial services from the review of international projects.

In the payment industry, blockchain efficiency cannot overcome that of central banks for national settlements or non-cross-currency settlements: as it was reported by the white papers of central banks' projects, centralized systems are by far more efficient, and the trust financial institutions have in national central banks makes blockchain technology unnecessary. On the other hand, as reported by news articles[110], a better process is that of reconciliation for non-SEPA payments, which entails manual operations and could be automated using BCT. Italian banks are ahead in this regard with the ABI LAB project, whereas no piece of news was found for other countries witnessing to similar initiatives. Among startups, the most financed project is that of Circle with the development of the Centre platform, allowing digital PSP to send value across wallets and across currencies too. Instead, retail payments cannot benefit from cryptocurrencies at the moment as transaction costs, settlement complexities and usability hassles make them worse compared to traditional credit card circuit payments, as anticipated from the literature review in Chapter 3 and now confirmed by the better performance of the absence of startups or companies' initiatives in this process

In the security sector, 199 projects were reviewed, the most financed among startups being cryptocurrencies exchanges, and tokenization platforms allowing companies to conduct ICOs. Industry white papers cited in section 5.5 show that tokenized assets are very close to securities but leveraging blockchain for their trading brings a large set of advantages and cost reductions:

[110] https://www.financemagnates.com/institutional-forex/technology/abi-lab-blockchain-project-moves-to-phase-two-after-initial-success/

settlement can happen close to real-time, while the only intermediary involved is an exchange, as opposed to the many parties in a traditional security settlement.

As for lending, the 21 startups operating on public blockchains propose business models that do not answer to the many practical problems posed by the technology that emerged in the literature review from in Chapter 3. Instead, startups working as dAPPs on private platforms propose compliant solutions or new products to incumbent intermediaries, in a collaborative vision. In particular, the unicorn Finastra is providing banks a DLT platform to manage syndicated loan contractualization and payment flows; LoanXchain is planning to launch an auction market for financial institutions to trade loans in their portfolio, as an additional tool to manage liquidity and as opposed to the current auction process which entails bilateral contacts and a long contracting before the deal can be closed, with future possible application in the securitization of loan portfolios.

Supply chain finance is also impacted by blockchain technology, as €67 million were gathered by startups and 24 companies' initiatives were found. From the news database, we found that financial institutions are working mainly on the factoring to manage invoices and avoid double spending. Future applications may lead to a faster and cheaper invoice securitization since the settlement in T+0 is of utmost relevance for this kind of products which have a short duration: reducing settlement from T+3 to T+0 for 30-days-lasting products is 10% of the time, thus allowing faster access to liquidity and 10% more daily interest paid to investors (as it was reported in industrial white papers in section 5,9). Still according to the news database, institutions are planning to launch operative platforms by the end of 2018 or in 2019.

Concerning insurance and risk management, the latter does not seem to be directly targeted by BCT since we could not find any project in this regard. Instead, insurance products can definitely take advantage from blockchain adoption, as we reviewed 22 projects in the area. As we showed in section 5.11, platforms are already operative, with a focus on streamlining data among the various actors involved in reinsurance process and the bordereau process. The technology could have a more impactful application in the automation of claim management, but technological barriers limit adoption. The only feasible use case we reviewed, which is already released in a product for European customers, is the automation of claim management in travel insurance by AXA. A smart contract on the Ethereum public blockchain collects data from aircraft companies and automatically reimburses customers in case of delays. PoC were also tested in the health insurance, again, to streamline information and documents between patients, healthcare companies and insurers, but the news do not report any operative product yet.

The only area where blockchain does not seem to play a role is that of fiduciary services, where we could not find any initiative employing the technology to change existing processes. Actually, we reviewed startups that were taking care advisory on cryptocurrencies, but no direct usage of BCT was done. We suppose that this is due to the bilateral relationship in fiduciary services which makes a blockchain infrastructure unnecessary.

Finally, with €103 million gathered by startups and 31 initiatives by institutions, we found that blockchain can be very impactful in an activity which all financial institutions have to carry out, but it is just accessory to the product they offer: KYC. The aim of these initiatives is to remove duplicate KYC procedures so that clients interfacing with different institutions would no longer need to repeat the process twice or more, enabling a cost reduction.

Altogether, we showed that blockchain technology has many applications in financial services and can impact significantly existing process. Financial institutions should consider the proposed framework to test blockchain applications and achieve efficiencies, cost reductions or launch new products not feasible with existing technologies.

CHAPTER 6
INTERVIEWS

In this section we are going to explore Italian Financial Institutions' positioning regarding BCT. The purpose of this work is twofold: first, we want to finetune the framework we developed in the previous chapter; secondly, we want to assess if Italian institutions are well-positioned with respect to the blockchain or not, evaluating whether they are approaching this new technology, and, in the event, which use cases they are studying.

In the previous section we have studied all the international BCT initiatives, from which we could define in which processes the technology might be efficiently applied, which others need further researches, and which instead could be better performed through traditional systems. At this point, we will interact with expert in the sector to understand their point of view on the application of this technology, thus comparing our results with their responses.

We have conducted direct interviews with representants of the major Italian Financial Institutions. Besides their opinion on the technology, they also presented us their projects. In this way we could check if further use cases would have been discovered or if they were aligned with the international ones.

For the selection of the Financial Institutions to be analyzed we considered two conditions: they should be Italian native and listed in the Borsa Italiana. Besides these obtained results, we decided to contact other Italian banks currently taking part in the ABI Lab BCT project, whose consortium is the one mostly including Italian banks. Though being all contacted by email, we received the answer of nine banks and one insurance company, whose representants regarding the blockchain have been contacted though phone calls.

Besides these interviews, we received the answer from other two banks, which stated that they are not currently studying the BCT, being anyway an interesting information for our analysis. These banks are Cassa Centrale Banche and Bancoposta.

Our sample is therefore composed by:

1. Banca Intesa Sanpaolo
2. Banca Unicredit
3. Banca Nazionale del Lavoro
4. Credito Valtellinese
5. UBI Banca
6. BPER Banca
7. Che Banca!, Gruppo Mediobanca
8. Banca Sella
9. Banco BPM
10. Cattolica Assicurazioni
11. Cassa Centrale Banche
12. Banco Posta

Before starting the interviews, a questionnaire has been prepared in order to have a common scheme every time which could fulfil all our research topics. The interviews were semi-structured, thus leaving the possibility to deepen the conversation when relevant or not clear topics were dealt. We did not, indeed, strictly follow the order of the predetermined questions, instead we initially left the interlocutor to talk about their current researches, then based on his words we either added further questions to the list or we exchanged their orders.

Nineteen questions have been prepared to make of fully covering the research sub-question. They can be divided into four groups.

The first part of the interview was completely led by the respondents, who described in detail their projects regarding BCT. We deepened our understanding asking whether particular factors have led them to choose a specific use, therefore we asked the reason behind their decision. Depending on the use case they are applying the BCT, more specific and detailed questions have been asked, especially whether they encountered the same issues we have highlighted during the analysis of the international initiative, and in case how they solve or softened them. Moreover, we asked which kind of blockchain they used for their researched, such as Ethereum, Hyperledger, or other, and which kind of platform they prefer or mostly use between permissionless and permissioned. In the end, we asked about the 2018 budget allocated for blockchain researches.

Then, questions regarding the organization behind their studies on the blockchain were asked. In particular, the interest was on the process which led them to enter in contact with this new technology, which function within the firm firstly moved into this new technology and

which one/s currently is/are working on it. Moreover, we asked whether the blockchain is being studying from more a technological or a business point of view, or both.

If not already mentioned, questions regarding the obtained results were proposed. Especially, we were interested in the level of maturity of each project.

The last set of questions are focused on the personal opinion of the respondents regarding the today scenario. We wanted to evaluate their point of view about the BCT's potential based on their knowledge and expertise. Therefore, we asked them whether they consider blockchain as disruptive, which its main limits and benefits are and where they considered it could be applied the most. This way, not only did we gather objective information about what they are doing, but also subjective thoughts.

During the interviews, notes have been taken by both the interviewers, which subsequently have been unified. In this way we were sure to write down as much information as possible. In case of ambiguity, the written answers were checked though the record of the call.

The data collected was subsequently analyzed. A two-step analysis has been carried out: a within case analysis, with the purpose of extracting precise information from each respondent individually, and a cross-case analysis, to compare these data among all the participants in order to find similarities and possible patterns.

During the first phase, an Excel file has been prepared filled with the relevant material gathered, which was subdivided into sections: number of projects, projects' use cases, starting year, level of development of the projects, leading function, meaning the area within the firm which first moved into the BCT studies, currently active functions, meaning the areas which currently are working on BCT-based initiatives, external support, 2018 allocated budget, consortium participation, name of the consortium BCT preferred platform, and disruptive BCT potentiality. Moreover, other two sections have been added after reviewing the interviews, the need of government support and the need of dedicated regulation. Many respondents indeed shared these last opinions, thus we considered them a relevant information to be highlighted.

Then, the interviews were reported subdividing each into four main categories. After a brief description of the Financial Institution, we listed the details about its blockchain projects, such us the use case, the possible participation in consortium, the allocated budget and the starting year of the research. Then we provide information about the Financial Institution's preference between permissionless and permissionless platform. Subsequently the information about its organization in following the blockchain researches has been proposed. Lastly, the respondent's opinions have been written down.

In this way, we could analyze in detail each single case, evaluating whether they choose efficient use cases, understanding their level of awareness of the technology and their level of maturity in the researches.

Once the database was ready, we started comparing the information to discover both similarities and differences among the considered groups. In this way, we wanted to assess the level of maturity of the Italian financial institutions regarding BCT, and to draw a general picture of the Italian financial sector with respect to this new technology.

Firstly, we created a table in which we combined the respondents and the projects, subdividing the latter by following the classification of the activities we performed in the second phase of our research. In the way, we wanted to highlight where Italian financial institutions are mostly committed to. Then, we evaluated the various projects sorted by activity. Therefore, we analyzed together all BCT application in payments, then in the supply chain finance and so on, with the purpose of comparing them and assessing whether they are efficient or deceptive use cases.

After evaluating the goodness of the financial institutions' undertaken projects though the use of our framework and the obtained results of the previous chapter, we took into consideration the other pieces of information we gathered from the interviews we combined them to assess their level of awareness through an index, their level of commitment and the modality in which they deal with the BCT. These data were useful to final give a general overview of the Italian financial institutions' position with respect to this new technology, which is showed through a matrix.

6.1 Within-case analysis

Following, we will analyze more in detail each single case. For each of them we will briefly present the financial institution, then its BCT projects, the preferred blockchain platform, the internal organization referring the BCT and the opinion of the respondents.

6.1.1 Intesa Sanpaolo

Intesa Sanpaolo is a banking institution formed in 2007 from the merger between Intesa and Sanpaolo IMI, and it is the first Italian bank for capitalization. It offers both investment and commercial products. Moreover, it owns also a private banking and insurance division, named Fideuram.

PROJECTS

Concerning BCT, they started studying it in 2014, attracted by the increasing and diffused interest in cryptocurrencies. The traction towards this topic came from the innovation function. Currently, they have abandoned the studies on cryptocurrencies and have move towards the application of their underlying technologies through 10 PoC, which the most relevant ones refer to three areas: trade finance, capital markets and payments.

In trade finance they are collaborating in the Marco Polo consortium, while for payments in the ABI Lab ones.

Marco Polo is an open trade finance platform for financial institutions and offers new customizable trade finance applications. It ensures a more connected and secure technology infrastructure for the trade ecosystem. Marco Polo connects with the ERP system of the firms and with financial institutions through the BCT. All the data are securely saved on the ledger and the network allows the interoperability between different trade systems. It offers more transparency and real time visibility of data in the supply chain finance activities thanks to the use of the BCT, thus reducing risks, allowing trusted access to critical trade.

ABI Lab is instead working on offering account reconciliations of Italian Nostro account on the BCT. It aims to modernize a process whose regulation is dated 1978. It is an activity which does not directly impact the final client, but it is able to move financial institutions towards a collaborative ecosystem and towards the new technologies. The objective is that every bank will represent a node on the blockchain allowing therefore greater economic benefits for all. The project is led by ABI, who is the actor regulating this reconciliation process. This a good point as it provides the possibility to adapt current rules to the new technology, a necessity perceived by many respondents.

The interviewed underlined the extreme importance of the collaboration with other financial institutions as well as with technological providers to obtain the greatest benefits from BCT. Even in the other research area, capital markets, they are collaborating both nationally and internationally for the project's development. It is evaluating the application of Ethereum smart contracts in the collateralized derivatives market, to reduce the risk of delays and to automatically resolve possible disputes. This PoC is strictly connected with others which are trying to ensure privacy on the blockchain, with the use of state channels which allow counterparties to send messages about derivatives or by building private blockchains into a central counterparty clearing house (CCP) for trading derivatives. The product will be operative between 2019/2020 and it refers to both securities tokenization and account reconciliation.

They took part to tests performed by Swift for Nostro account reconciliation.

For 2018 they allocated 3 billion euros for BCT projects.

BLOCKCHAIN PLATFORM

In the last three years, they are moving toward private blockchain, especially to the one of Corda. The reason of this choice is attributable again to the intention of the institution to take part to group collaboration. R3 which built Corda is indeed considered a catalyst for financial institutions.

ORGANISATION

The interest towards the technology came from the innovation department. Formally, four people now dedicate to blockchain; nevertheless, all the function are time to time called to intervene to provide their specific know-how. Thus, the interviewed highlighted that the number is not representative of the reality. The studies are moved from both a technological and business point of view.

LIMITS

Three limits have been highlighted:

1. the technology is not diffused nor well-consolidated yet

2. high costs

3. lack of experts or competent staff

These problems create a vicious cycle hindering BCT adoption: until a large diffusion takes place, few institutions move towards BCT, but until anyone moves to BCT, a large diffusion cannot occur. Only overcoming the above-mentioned problems, he thinks the BCT can be disruptive.

OPINIONS

According to the respondent, the BCT has the potentiality to be a *disruptive innovation*, especially in all those sectors in which there are several data to be shared: healthcare, utilities and insurance. Concerning the banking sector, he considers the BCT can be mostly beneficial in the reconciliation process.

Moreover, BCT should not be study by a single entity, but it should be a system operation. To be economically advantageous, many institutions should collaborate and work together on it. That is the reason why, Intesa Sanpaolo has joint ABI Lab and Marco Polo. In Italy, regarding the banking sector, only big banks have the financial capabilities to work on it as it requires a high level of investments, which do not ensure an immediate return. The creation of consortiums is therefore beneficial as it allows to combine the efforts and the financial contributions of each member.

He also believes that government plays a crucial role in the technology diffusion. They can boost it through the introduction of dedicated regulations. On the other hand, he acknowledges the difficulty in developing ad-hoc norms, as the topic is complex and there is still no certainty on the use cases where it can be efficiently adopted. Thus, a regulation may be issued only after a certain degree of knowledge on the BCT possible applications will be reached.

6.1.2 Unicredit

Unicredit is one the largest banks in Italy and Europe. It was formed in 1998 from the merge between many Italian financial institutions, grouped in Credito Italiano and Unicredito. It is an Italian global bank, operating in 18 countries in Europe. It offers both commercial and investment banking services, as well as insurance products. Moreover, it operates also a private bank. It is the second leading bank in Italy, and the fifth in Europe. It is listed in Borsa Italiana.

PROJECTS

Unicredit is the bank that first moved in the blockchain world, in 2013. Currently, it is fully committed in the Wetrade projects, and it's the only Italian bank in the consortium. The project refers to supply chain finance for commercial, national and international transfers. The project does not focus only on the trade phase but also on the costumer identification and on payments, thus from the purchase order to the bill payment. It is an international project, which includes thirteen European banks, such as Banco Santander, HSBC, UBS, Societè Generale and others. It will allow European firms to commercialize with one another through a blockchain-based platform. With the first pilot 1.0, a transaction with Banco Santander has been implemented. Figure 63 represents how the trade process through Wetrade on blockchain works.

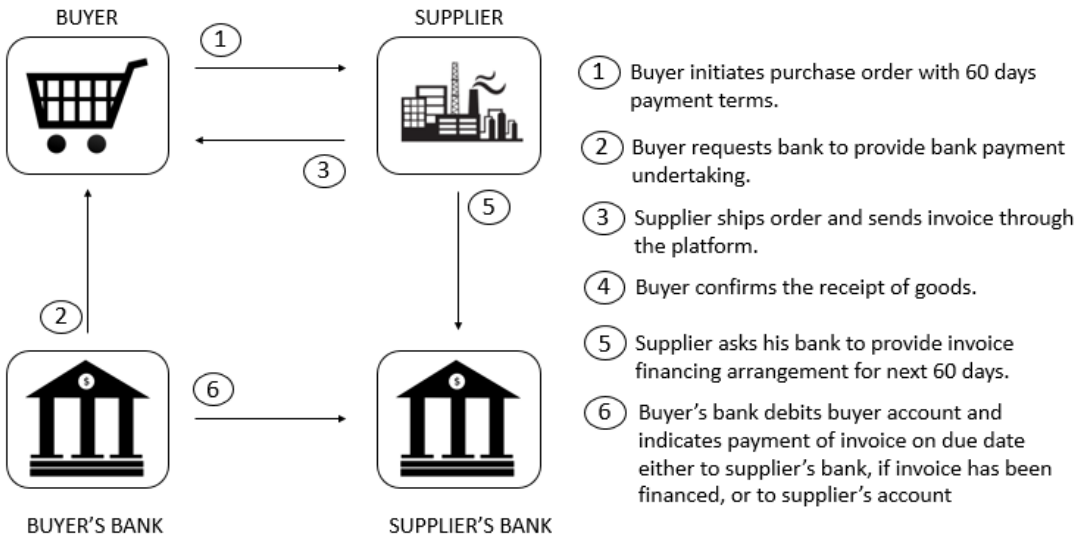


Figure 64, WeTrade supply chain finance process

The Austrian subsidiary is now collaborating with J.P.Morgan on a project about the Nostro account reconciliation.

They took into consideration to join Sia supply chain finance project, but it was in overlapping with WeTrade, thus they prefer the latter. Sia project refers only to the applicability of the BCT in the factoring activity. ABI Lab project instead is considered a limited market with respect to WeTrade, therefore they decided not to take part to it.

Initially, they were engaged in the Ripple payment initiative, which has been presented in the previous section, but then they decided to leave it on hold and to wait until it is more mature. Swift GPI is currently more advanced, but the blockchain experimentation has some limits as we have already described previously.

BLOCKCHAIN PLATFORM

They mainly focused on private/permissioned blockchain. They studied smart contracts on Quorum, but currently they are only referring to Hyperledger as it is well-positioned and for its industrial support.

ORGANISATION

The interest on BCT came from the commercial side of the innovation, wondering which useful applicability the BCT could be used for. The training phase has been driven from both a technological and business point of view. For the technological development they relied on the external support of a consultancy company, while everything connected, from the security to the compliance was studied internally.

LIMITS

In Italy the topic has not conquered many interests yet, thus they are referring to international collaboration with banks. they think they can obtain greater benefit with a European vision.

OPINION

The respondent considers KYC a good use case for BCT, though they are not working on it.

He thinks that BCT will be disruptive, as it already changed the financial sector vision and many actors have already invested a lot on it. There are great expectations coming from this innovation. The main benefits are the shared governance model between banks introduced thanks to the BCT with, for example, consortia.

6.1.3 BNL, Banca Nazionale del Lavoro

Banca Nazionale del Lavoro is one of the major Italian banking group. It was founded in 1913, and it became a subsidiary of the group BNP Paribas since 2006. It works as a commercial bank.

PROJECTS

They began working on BCT in 2015. At the beginning, it was a personal interest of few people within the bank, who started learning about it from the internet and internal researches. Currently they are working on two main projects: the account reconciliation on BCT, in membership with ABI Lab, and AML data sharing on BCT, in partnership with a startup.

They took part to conferences on this topic organized by SIA and R3. After a first period of learning and evaluation of the technology potentiality, BNL joint ABI Lab.

The respondent participated as a mentor in the BNP Paribas International Hackathon 2017, which was won by Spidchain. In this context, he got in contact with the latter and they established a research collaboration. Spidchain is an Italian startup which offers KYC SaaS and ID registry services through BCT. Thanks to this group work, BNL is also participating in a project regarding the sharing of data for AML. They are studying a way to transfer information between all the subsidiaries and the holding company of BNP Paribas, adding the possibility to sell these data to external parties in the event the client, and owner of these data, requires to.

BLOCKCHAIN PLATFORM

No preferences have been expressed, the choice between a permissioned or a permissionless form depends on the use case. With ABI Lab they are working on a permissioned version, while with Spidchain they are relying on the permissionless one, as there is the need for all the blockchain participants (the firms within the same banking group, BNP Paribas) to have complete visibility on the clients' information.

ORGANISATION

As mentioned above, the BCT started to be explored for personal interest of few people within the subsidiary. There is no structured division for the topic; currently, it is studied by the IT function, thus it is approached only from a technical point of view. Moreover, no other bank's function is involved time to time for collaboration. Therefore, the interviewed highlights the lack of interaction between the various functions within the bank. He works in the legal section and noticed difficulties in deal with the topic with his colleagues. Nevertheless, some internal meetings and courses have been organized to broaden the vision on the BCT not only from a technological point of view, but also approaching other themes, such as the GDPR and the data sharing.

Although in BNL there are few initiatives, BNP Paribas is working on some BCT projects. Thus, the research on the topic are limited to the holding companies, which is currently experimenting, and only when they reach some satisfying results, they will send directives on how to implement them. The Italian subsidiary has therefore few room for maneuver.

LIMITS

The respondent highlighted mainly internal limits to the banks, which hinder their BCT adoption. Little enthusiasm towards the technology, which is thought not sufficiently efficient yet. The limited interaction between the division and the study of the blockchain only from a technical point of view does not allow to identify useful use cases. Moreover, the geographical position of the headquarter, which is based in Rome, is considered limiting, as many conferences and research point of the topic are in Milan.

OPINIONS

The interviewed considers the BCT a disruptive innovation, although further researches are needed to find the best use cases for its application. In his opinion, it can work only if many institutions collaborate to create a unique system, as it requires several participants to generate financial efficiency.

6.1.4 Creval, Credito Valtellinese

Credito Valtellinese, also known as Creval, has been a cooperative bank since 2016, when it turned to be a limited company, listed on Borsa Italiana. It offers commercial as well as insurance products; moreover, it works also as a private bank.

PROJECTS

Creval started working on BCT in 2016 and it is currently focusing on four projects:

1. It is a member of the ABI Lab project on the account reconciliation.

2. It is participating with Sia in project related with the supply chain finance. In particular, it allows the factoring on the BCT favoring therefore the B2B market.

3. A PoC has been developed in 2017 to allow the implementation of online public auction on the BCT, through the public version of Ethereum. The user has to register online, then he/she can take part to the auction directly online thanks to the complete visibility of the others' offer on the public platform. Once the batch is won, it will be delivered thanks to the use of smart contracts. All the functionalities are ready, but they stopped as there are legal constraints for the real-life implementation. According to the current laws, to be legally binding, an auction must take place in a public area where free access to anyone is allowed. The encountered problem is that rules only refer to physical places, thus a renovation is needed, which could allow even digital environment to be considered as legally valid.

4. Notarization of home-banking clients' documentation. The project is being developed on the bitcoin platform, thus a permissionless version of the blockchain and it will be probably been release by the end of 2018.

The allocated budget for 2018 is €300,000.

BLOCKCHAIN PLATFORM

No preferences have been expressed even in this case. The choice between the permissionless or the permissioned version depends on the uses: if data has to be transparent and visible to multiple parties then the permissionless platform will be more suitable, otherwise when privacy has a crucial role, the permissioned version will better fit to the application.

ORGANISATION

Their approach to BCT first started with theorical training of a team made of 3-4 selected internal employees. No external, already competent resources have been hired. At the

beginning, it was an autonomous learning from online sources, then the process was fastened thanks to the external support of Reply. In this second phase 12 people were involved, who took part to two training days, one relative to the use cases in which BCT might be applied and another one on design thinking, besides the continuous technical learning. Thus, they first evaluate the technology from a theoretical point of view, identifying limits and possibilities, then they started experimentally practicing this knowledge.

The team looks at the BCT from both a technical and business point of view, with no dominance from neither of the two parts.

The interest is not limited to the dedicated BCT function but is spread also to the higher level of the organization, reaching also the Board of the Directors. Thanks to this diffused and deep internal knowledge, many projects have been developed.

The external support of Reply was exploited not only on the training phase, but for the empirical one. Reply helped in the infrastructure development of the Ethereum platform for the third above presented project, while the smart contract has been internally developed.

LIMITS

The small dimension of the bank represents an obstacle, as it makes difficult the participation to event and conferences about the BCT in Europe, which can be a useful instrument for learning and for entering in contact with other institutions working on the topic.

Moreover, as written above, the lack of dedicated regulation hinders the adoption of the BCT for some use cases. For example, the legal support of the notaries has been considered a limitation into all those situations in which a validation from a designated third party is required. Collaboration between financial institutions and legal ones are needed, and in particular new or adapted regulations should be introduced to allow the concrete implementation of the BCT projects.

OPINION

According to the interviewed, the technology can be disruptive, if its benefits can be widely perceived. The university have a fundamental role of communicators and should spread the knowledge about the technology to different sectors. Once different sectors' representative, especially the legal and government ones, are aware of the potentiality the technology can bring, the collaboration between the parties will occur and BCT will have the possibility to be widely used.

6.1.5 Ubi, Unione di Banche Italiane

UBI Banca S.p.a. is an Italian banking group, originally born as a cooperative bank, which then turned to be a limited bank through the merge of Banche Popolari Unite and Banca Lombarda. It is the fourth bank in Italy by number of branches. UBI Banca shares are listed on the Borsa Italiana. It offers services such as retail and corporate banking, leasing and factoring, and asset management.

PROJECTS

They started working on the BCT in 2015 with the external support of a consultancy firm, by studying a pilot related to P2P payments with the purpose of understanding the technology. The test of the pilot was internally implemented through transactions between five or six bank users. The pilot was not further developed as it required important investments, not worthy for the transaction volumes of UBI.

Later, they realized that BCT was not useful for in-house experimentations, but that it can really provide benefits if the bank is considered as a node of a broader system. Therefore, they stopped working alone on it, and they started joining all the national and international group study: Sia for factoring, ABI Lab for account reconciliation and another SIA project in collaboration with the Bank of Bari whose details were not revealed.

They are also evaluating to take part to one of the consortia studying the BCT applicability in trade finance, for example Marco Polo or Wetrade, and to subscribe to R3.

They do not have a dedicated budget for 2018, just for the innovation department, but it should be around €100.000/200.000 for subscriptions.

BLOCKCHAIN PLATFORM

For the banking sector, the permissioned form is considered the most suitable blockchain platform, as banks require limited data transparency, reserved access just to whom is granted. Banks should rely on Siachain as it allows these conditions to be met.

ORGANISATION

The initial interest came from the IT division, while business began to interact with the BCT only in 2018, when they started evaluating the entrance into other consortia. They do not have a dedicated team, but the innovation division in collaboration with the business is the one engaged with the researches. They have only one person fully dedicated on blockchain.

When considering a new use case, they start with a generic technical evaluation, not performed by any expert, they just evaluate the adequacy of the platform, then the commercial

division analyses the goodness of the business. They are not interested on the technology behind it, but they only perceive the final product, the services they could offer and the profit they could obtain with it.

Their objective is the monitoring of the state of the art about the BCT. For example, they take part to R3 conferences to understand the maturity level of the technology, which platform there are, and which ones have better applicability. They are interested in understanding the environment around the blockchain, so that they can be well-position.

LIMITS

They do not consider the blockchain as revolutionary from the technical point of view, but it is considered as an aggregator instrument and a business facilitator.

OPINION

Blockchain for internal experimentation is not considered an optimal solution, instead it would be better replaced by traditional technologies. Therefore, the great potentiality of the blockchain is its ability to be a catalyst and an aggregator of institutions. Only in this context it can bring economic benefits. Private initiatives need a certain level of central governance which can be obtained only though consortium, where the central authority decides about for example technical specificity, which will then be applied by the members.

They chose only to participate to group researches, for three reasons: from a business point of view, to be aware of what is happening around them, what other entities are doing; from a technical point of view, to understand the level of maturity of the blockchain and its possible form; from an organizational point of view, instead, to see how the other institutions are dealing with it.

6.1.6 Bper, Banca Popolare dell'Emilia Romagna

Banca Popolare dell'Emilia Romagna, also known as Bper, is the sixth Italian bank by assets. It is listed in Borsa Italiana. Bper group is made of other four banks: Banca di Sassari, Banco di Sardegna, Cassa di Risparmio di Bra and Cassa di Risparmio di Saluzzo. It operates as a private banking, as well as a commercial financial institution.

PROJECTS

They are dealing with the blockchain since 2015 and they are currently working on 2 projects: they are participating to the pilot implemented by ABI Lab, while the other one refers to the identity use case, but no details have been released nor by the interviewed nor publicly. Moreover, they have also scouting initiatives to identify other possible use cases and are also

studying the different existing platform to compare their performances and understand which be more suitable for financial purposes. In particular, they are focusing on the smart contracts on ETH.

No budget is allocated specifically to BCT, in 2018 just the subscription to the consortium has been paid, which is €100,000.

BLOCKCHAIN PLATFORM

According to the interviewed, the value added brought by private platform with respect to traditional ones is limited, while the public platform is considered the one which can generate greater advantage. The only one which might be used in its private version could be Ethereum.

ORGANISATION

The innovation division is the one working on the blockchain, which is moved by both a technical and a business point of view, though the initial pulse towards the BCT came from the IT.

For the identity uses, they are thinking to ask the external support of a consultancy firm.

LIMITS

The lack of regulation and standardization are considered as constraints to the diffusion of the technology.

OPINION

The blockchain is not considered a useful instrument for the financial sector. Instead, the respondent believes that the financial products should be offered as a support to other sectors, especially the automotive and the utilities. For example, a use case which is well considered is the RCA insurance pay per use. Thus, the financial products are complementary to BCT applications in other sectors.

6.1.7 Che banca! – Gruppo Mediobanca

Che banca! was launched in 2008 by Gruppo Mediobanca to enlarge operations in the retail banking segment, combining the financial expertise of the group with a strong component of digital innovation. The bank therefore provides its clients a model of multichannel distribution, through internet, call centers and physical branches. It offers commercial banks services and private consultancy support for investments and savings.

PROJECTS

Che banca! Is involved in 4 main projects:

1. it is a member of ABI Lab; thus, it is collaborating in the account reconciliation project.

2. a prototype is being developed about the digital identity, which might be operative in 2020. Some legal problems have been encountered in the distinction between natural or legal person.

3. another prototype about the loan exchange, but no information has been disclosed.

4. they are studying how to apply smart contracts in the mortgage disbursement in collaboration with Deloitte. They are not only evaluating the technical applicability, but also the compliance alignment and the legal validity of the product. Thus, it will require longer time, and it will be released probably after 2020 as many actors, such as notary and loan expert, must be involved. If realized, it may allow to obtain a mortgage in four to five days instead of a month.

Moreover, they are also member of R3.

The allocated budget amounts for €200,000.

BLOCKCHAIN PLATFORM

They are referring only to Corda, thus permissioned blockchain.

ORGANISATION

The formation and the initial interest came from the innovation division, whose people have also a business background.

LIMITS

The respondent believes that there are too high entry barriers into R3 consortium, from an economical point of view, which are not considered as justifiable.

OPINION

The BCT is considered disruptive, provided that authority will introduce specific regulation to allow a wider adoption of the technology. it is considered particularly suitable for KYC, capital markets and the energy sector.

6.1.8 Banca Sella

Banca Sella is a private credit institution founded in 1886. It owns the Sella Lab, which is the bank's innovation center committed to support open innovation and digital transformation processes in the financial sector. It offers commercial banking and private banking services.

PROJECTS

Banca Sella started working on the BCT in 2016, and two projects are currently in development:

1. it is a member of ABI Lab; thus, it is collaborating in the account reconciliation project,

2. it is studying the applicability of the technology in the notarization activity, to ensure an operation has been successfully completed or to digitalize physical assets. For example, they are thinking to apply it in the notarization of the public procurement to fight against corruption. With the BCT the operation would be encrypted, thus not transparent to all the participants, but their occurrence would be verifiable,

3. it is developing an API platform on DLT through Fabrick.

BLOCKCHAIN PLATFORM

No preferences have been expressed, though they are mainly working on permissioned platforms.

ORGANISATION

They are not relying on external support.

LIMITS

According to the interviewed, BCT cannot be applied in areas in which data often change, as it is not allowed. Immutability is indeed one of the main characteristics of the technology. A solution would be to introduce new data in the event that old information was no longer correct, but in this way an applied smart contract should be able to work both referring to old and new data, increasing therefore the complexity of its usage.

Another issue is the key custody. If managed with traditional technologies, there might be big risks for the GDPR compliance.

OPINION

A great advantage brought by BCT is the collaboration between the financial institutions, which although competing in the market, can extract more benefits through membership in consortia.

6.1.9 Banco BPM

Banco BPM was founded in 2017 through the merger between Banca Popolare di Milano and Banco Popolare. It is the third biggest banking group in Italy, after Intesa Sanpaolo and Unicredit. It offers commercial and investment services, and it works as a private banking, too.

PROJECTS

BPM is working on BCT since 2017, and it is currently committed in 2 projects, both of each are pilots:

1. it is a member of ABI Lab; thus, it is collaborating in the account reconciliation project.

2. it is studying the BCT applicability in factoring

Less than €100,000 have been budgeted for the BCT in 2018.

BLOCKCHAIN PLATFORM

Both permissioned and permissionless platform are considered as appreciable, depending on the use case, though they only focused on Corda, which is a permissioned one.

ORGANISATION

The interest came from the IT division, which is still the only one working on the technology. No dedicated people have been selected to fully study it. They are also relying on the external support of technology providers.

LIMITS

From their study, the platform is considered still inefficient, thus further researches are needed.

OPINION

They do not consider the BCT as disruptive, but only as an instrument to make current process more efficient. In particular, the BCT may allow time savings, for example in the data verification, and risk reductions, as well as a frauds reduction.

The most suitable use cases in the financial sector are considered cross-border payments and KYC, while other interesting ones are in the logistic sector, especially in the international trade.

6.1.10 Società Cattolica di Assicurazioni

Cattolica Assicurazioni is an Italian society controlling one of the major Insurance group. It has been listed in Borsa Italiana since 2000. It not only offers insurance products, but also collaborate with Banco BPM to create what are known as Bancassurance.

PROJECTS

They started to work on the BCT in 2016, and they are currently working on three projects:

1. They are collaborating with Ania for the applicability of the BCT in the car insurance. They created an Italian sandbox to study it. The blockchain is used to allow a blind auction between the insurance and the legal part for the claim's settlement. All the interactions are saved on the blockchain for legal validity. In this way, they can fasten the current process and make it more efficient, allowing the client to receive the amount of expected money as soon as possible.
2. They are studying the possibility to apply the BCT for microinsurance, exploiting smart contracts for the automatic payments realize. Especially they are testing its applicability for insurance on weather conditions. For the latter indeed, smart contracts are more easily applicable as these occurrences do not require any expert evaluation of the damage, or they have happened or not, thus being more objectively assessable.
3. They are collaborating with a startup for a product which can ensure the risk management, but no information have been realized about it.

BLOCKCHAIN PLATFORM

They do not have a preferred platform, instead they think the choice depends on the use case. They are indeed using a public platform for the second projects, while private forms for the other two. In particular, they are using Hyperledger for the Ania project.

ORGANISATION

There is no dedicated team for BCT within the company, but the BCT is a collaborative topic among the various internal units. They are approaching to it with both a technological and business point of view.

OPINION

They are currently working on initiatives which can make internal or external processes more efficient, thus they are focusing on application strictly related with the single company and its specific businesses. For this reason, they did not take into consideration to collaborate with B3i, which instead has an international scope.

They are in an experimentation phase, i.e. they are testing the applicability of the blockchain in processes which can be performed also by traditional technologies. Nevertheless, they do this for future expectations; indeed, they are convinced that the hashing logic as a reference point may generate great automation, efficiency and complete disintermediation. They know that the technology is not mature yet, but it is evolving in a fast way, thus they expect it to become disruptive.

6.2 Financial Institutions' BCT projects evaluation

Now, we will provide an evaluation of the ongoing financial institutions' projects, based on the results obtained in the previous, empirical section and on the framework for adoption we developed in chapter four.

Use cases	FI 1	FI 2	FI 3	FI 4	FI 5	FI 6	FI 7	FI 8	FI 9	FI 10
Supply chain finance	1	1		1	1				1	
Payments	2	1	1	1	1	1	1	1	1	
Insurance products										3
Deposit and Lending							2			
Fiduciary services										
Capital markets	1									
Others			1	2		1	1	2		

Figure 65, use cases of Italian Financial Institutions' BCT projects

Eight banks out of the nine interviewed ones are members of the ABI Lab BCT project on the account reconciliation. As written above, the results of the project will not generate a great change for the clients, but it can allow a strong modernization into the banking sector pushed

by a central regulator. The impact the project may have on the regulation is a great benefit, considering that many of the respondents feel the lack of laws inherent to the blockchain applications as a big issue. Moreover, the ongoing tests are reporting positive results, thus showing the technological efficiency of the application.

Two of them are also working on another application of BCT in payments: the reconciliation of Nostro account. Though currently presenting limits, the use case might be beneficial thus further researches are needed, as we have already expressed in the payment section.

The two biggest Italian banks, Intesa Sanpaolo and Unicredit, are working on blockchain-based supply chain finance group projects. As we have already previously reported, SCF finance seems to be one of the areas that could be more impacted by the adoption of blockchain technology. Nevertheless, many problems are hindering the full exploitation of its related benefits, especially the presence of opposing private blockchain platform on the market, going against the possibility of fully cooperative business model. Therefore, Wetrade and Marco Polo have great potential as they can simplify the current processes thank to the use of the BCT, but their chains do not interact with each other, preventing clients from trading with everyone. A customer relying on a Wetrade bank, Unicredit, cannot indeed ask for a multi-bank factoring also including Intesa Sanpaolo, which instead relies on Marco Polo.

One third of the interviewed bank is studying the possible application of the BCT in the factoring activity, supported by SIA. As we have seen, factoring on the BCT would generate several benefits as it can solve some current issues, such as the double spending problem, or it allows multi-bank factoring through smart contracts. Moreover, it can reduce KYC compliant costs, providing the possibility for the banks to share their data about a client in the exchange for a fee.

Five financial institutions out of ten are currently evaluating the BCT applicability in data validation and regulation compliance activities. Creval and Banca Sella are proposing a solution for client's data validation through automatic notarization. The one presented by Creval would be better performed by traditional database. Following our developed framework, no multiple writers are indeed committed in the notarization of the bank clients' data, thus the use case do not satisfy the second requirement for a blockchain adoption. The second solution, instead, refers to the notarization process in public procurement. In this case not only the bank, but also governmental entities are responsible for the process. Though being a suitable use case for the blockchain, it shows some limitation due to the current lack of dedicated regulation. The notarization process on the blockchain is not legally valid yet, as a central authority is still required to approve for example a contract. Other financial institutions are instead studying the possibility to facilitate the KYC procedure, generating client's digital

identity on the BCT. This kind of research may bring economic advantages only if many institutions collaborate in sharing their data, in exchange for fees. A good solution for implementation is the sharing of data between the different branches of the group, as BNL is doing in conjunction with the entire group BNP Paribas.

Che banca! is experimenting two different use cases, the blockchain for loan exchange and mortgage disbursement. We have already highlighted that the BCT can be beneficial in these two cases as it can allow a reduction in the time associated to the processes. They are both at an initial level of development, but the perspectives are optimistic.

Creval is also studying another different blockchain application with respect to the other financial institutions, the applicability of the technology for public auction. But this use case is not efficient according to our framework, it would indeed be better performed though a traditional database.

Concerning the insurance projects, they have great potentiality on the sector, though some limits still hinder their complete operativity. Indeed, the main benefits are the removal of reconciliation needs, and the automation of claim management. The former is already applied by some companies and its feasibility seems achieved, yet the impact on the business low according to interviews. The latter, instead, might drive a very relevant cost reduction in the sector, but technological hurdles limit the adoption only to a low number of insurance products.

As we can see, the application of the blockchain technology by the Italian Financial Institutions show an overall overlapping of the use case, besides few exceptions. Most of them are efficient application of the technology, signal of a careful analysis and evaluation of the topic.

6.3 Cross-case analysis

After analyzing each single case and evaluating the goodness of their undertaken projects though the use of our framework and the obtained results of the previous chapter, we are going to compare the financial institutions' information. In this way, we aim to highlight possible similitudes and differences between them, and to draw a general picture of the Italian financial sector with regard to the BCT.

We decided to evaluate the level of awareness of each financial institution. To do so, we decided to define an index ranging from 1 to 5, where 1 refers to a low level of awareness. The index is a weighted average of different information we gathered from the interviews.

- the year in which the financial institution started studying the technology,
- the number of studied use cases and their level of development,
- the allocated budget for the BCT projects
- the internal organization regarding the BCT.

The starting year of the studies has been considered as a component affecting the awareness as we may assume that the longer an institution has been studying a topic, the more consciousness it has acquired about it. The first financial institution focusing on the blockchain started in 2013, thus we assigned to this year the maximum score of 5, while decreasing values to the subsequent years, as we can see from the following table:

Starting year	2013	2014	2015	2016	2017	2018
Score	5	4	3	2	1	0

Table 16, index scores for projects' starting year

Another critical factor which influences the apprehension on the topic is the number of undertaken use cases and their level of development. If the application of the blockchain by an institution ranges over a high number of different functions, we can presume that the same one has a broader understanding of it. The player may have indeed evaluated more in depth the possibility of the technology, and having acquired more trust in it, as well as greater skills in dealing with it. However, this information alone may be misleading, as an actor might just pick up by chance some projects and test it, without having developed any previous evaluation and considerations. Therefore, we combined this data with the level of development of the correspondent project. We have identified five different possible states:

- not suitable for blockchain, for all those projects which could be better implemented through traditional databases,
- empirical no-result test, for those projects which have been implemented only for studying the underlying technology and acquire familiarity with it, or for those which have been put in hold or abandoned,
- theoretical evaluation of possible use cases, not subsequently implemented,
- proof of concept,
- already or soon operative.

Following the order of the above list, we assigned them scores from 1 to 5.

Each of the project is therefore assigned a score depending on its level of maturity, and then these scores are summed together. Considering that the maximum number of relevant projects developed by an interviewed financial institution is five, we obtained a point range

which goes from 1 in the worst case, i.e. in the event an actor is only studying a single use case, which appears not suitable for blockchain, to 25 in the best case, i.e. if a financial institution is operative (5) with five different blockchain applications.

The third considered factor is the 2018 allocated budget. In this case, we have assumed that the more an institution has invested on blockchain projects, the more it has been dedicated to them, thus the more knowledge about the topic it has gained. The range of the financial institutions' investments, which goes from less than €100,000 to more than €1 million, has been divided into five slots, to each of which has been assigned a value, as we can see from the following table (the budget is in euros):

Allocated budget	<150K	150-299K	300-449K	450-600K	>600K
Score	1	2	3	4	5

Table 17, index scores for projects' 2018 allocated budget

The last component of the index is the organization. To have an efficient impact on the firm and on the connected processes, a technological innovation should not only be studied with the focus on the technology, but also from a business point of view (Baden-Fuller & Haefliger, 2013). We considered this notion among the elements impacting the awareness, since only in the event that an institution applies it, it will have the possibility to gain benefits from the blockchain. Therefore, greater advantages can be obtained only if aware of the crucial importance of the business components. In this case, we allocated three different values. A 3 will be assigned when both IT and the business functions are collaborating on the projects, 2 when only the IT people are involved, and 1 when none of them is studying the blockchain, but other functions or no functions at all.

The final values of the index attributed to the financial institutions will range from 1 to 5, thus the second and the last constituents need conversion factors from a scale made respectively of twenty-five and three elements to the final one, made of five elements. A simple proportion can be performed to translate these values and therefore to obtain the conversion factors.

$x: 5 = y: 25$, where y is the score related to the use cases ranged between 1 and 25, while x is the correspondent score in a range from 1 to 5. Therefore, the conversion factor is 5/25, which is 0,20.

The same calculation can be applied for the conversion of the score regarding to the organization from a three-element scale to a five-element one, thus obtaining a conversion factor equal to 5/3.

After defining the component of the formula, we chose their correspondent weight. Since the second component of the formula, the one relative to the use cases, is made of two different type of the data, i.e. the quantities of projects and their level of development, we considered the index as comprised of five units. Therefore, the budget and the starting year have been assigned 1/5 of the weight, equal to 20%, each. Concerning the organization factor, it has been given a lower weight, since it does not directly refer to the understanding of the blockchain, but instead to a way to fully exploit it. On the other hand, the number of different projects assume a more relevant position for the apprehension process. Therefore, we attributed respectively a weight of 10% and 50% to them (keeping in mind that the latter is a double factor, thus each piece of information is given 25%).

The awareness index can be calculated with the following formula:

$$20\% \times \alpha + 50\% \times \frac{5}{20} \times \beta + 20\% \times \gamma + 10\% \times \frac{5}{3} \times \varepsilon$$

Where

α refers to the score relative to the *projects' starting year,*

β refers to the *use cases* score,

γ refers to the *2018 allocated budget score,*

ε refers to the *organization* score.

By applying this formula to the interviewed financial institutions, we obtained the following results:

	budget scores	organisational scores	starting year score	use cases score					tot use cases score	awareness index
1. Banca Intesa	5	3	4	2	5	5	5	4	21	4,40
3. BNL	2	2	3	5	5				10	2,33
4 Creval	3	3	2	1	5	4	1		11	2,60
5. UBI	2	3	3	2	5	4	3	4	18	3,30
6. Bper	1	3	3	4	5				9	2,20
2. Unicredit	5	3	5	4	5	3	3	2	17	4,20
7. Che Banca!	2	3	1	4	5	4	4		17	2,80
8. Sella	2	2	2	4	5	4			13	2,43
9. BPM	1	2	1	4	5				9	1,63
10. Cattolica Assicurazioni	1	3	2	4	4	4			12	2,30

Table 18, financial institutions' scores and awareness indexes

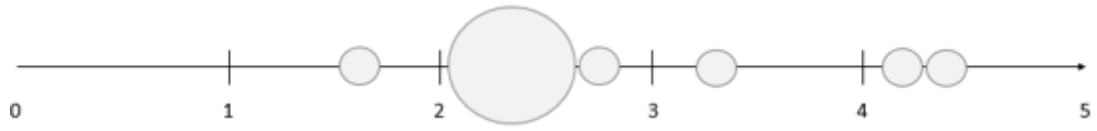


Figure 66, Financial Institutions' distribution according to the awareness index

In the image above, we wanted to show the numerousness of the Financial Institutions with a certain value of the awareness index. The small circle represents a single institution, while the biggest one comprises five Financial Institutions. It is clear that most of the respondents are still in a low level of awareness. This result is not surprising considering the novelty of the topic. As we have also seen in the previous chapter, many studies are still required to gain substantial advantages from the technologies. Banks therefore are still in a learning phase regarding the BCT, they approached it few years ago, and they are still testing its applicability. Some exceptions can be traced, whose levels of awareness almost double the one of the others. They began studying the BCT some years before the other, they are spending a great higher amount of money on it and they are evaluating several different use cases. These characteristics gave them the possibility to acquire more understanding of the topic. These differences are mostly due to their position in the financial sector with respect to the others. All the financial institutions with a score higher than three have currently a market share in Italy which is much higher than the others.

After having identified the level of awareness about the technology for the interviewed financial institutions, we decided to further analyze how they are approaching it. In this way, we want to define the position of the Italian financial institutions with respect to the blockchain. To do this, we combined two gathered pieces of information, the internal organization of the financial institutions concerning the studies on the blockchain, and the future expectations about it. Two scenarios have been considered: the blockchain as a disruptive innovation or as an efficiency enabler, which means that it is still considered a potential positive instrument but not able to fully change the current dynamics. For what concern the internal organization, we have defined three possible structure: a team completely dedicated to the blockchain, a non-structured function, which means that the BCT is studied together with other technologies, by people who are therefore not completely focused on it, and absent, for those cases in which the BCT is not studied at all.

In Figure 67, each financial institution icon represents a correspondent one among our contacts. We have defined four different typologies of institutions.

The revolutionist, which are the ones mostly convinced of the BCT potentiality and that have therefore a group of people completely dedicated on it.

The experimenters strongly believe the blockchain will be ground-breaking, but they have not fully dived into it yet. They are studying it through usually the innovation function, whose scope is to identify and evaluate new ways to improve the current processes and state of the institutions. They are taking part to many conferences on the topic to enter in contact with many experts and players which are more advanced with their researchers to gain from them useful knowledge.

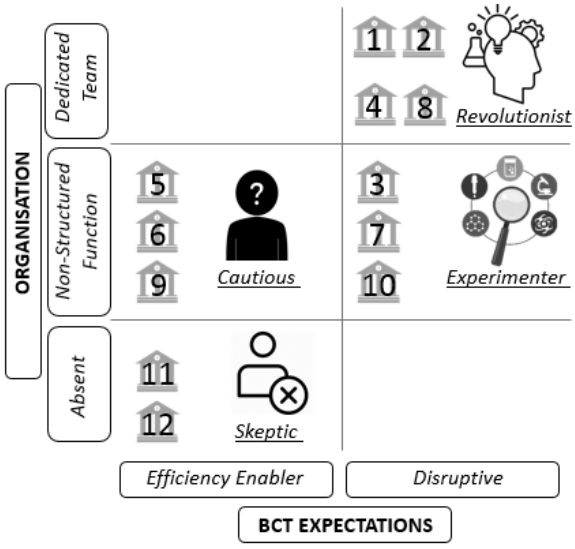


Figure 67, Organization-Expectations Matrix

The cautious expect the blockchain to have a limited impact in the future. They consider it as a useful instrument to be studied and to be used to gain efficiency, but they doubt it will not be able to overcome the current system. For this reason, their IT or innovation functions are partly focusing their attention on the technology and how it can be adapted to the existing ones. They also take part to conferences with the intention of increasing their understanding on the topic and to try to solve their doubts.

The sceptics are currently not studying at all the blockchain. Two may be the reasons behind this choice. On one hand, they might be small financial institutions which do not have sufficient money to be invested in this still early-stage innovation, which is not completely operative yet. On the other hand, they might be uncertain about the blockchain and its real-life applications. They are still not sure it will bring great advantages with respect to the traditional technologies. In both cases, therefore, they are waiting for other to study and test it, and they will approach to the BCT only once it will enter into the market.

As we can see, the majority of our respondents lay in the revolutionist area, followed by the cautious and the experimenters, while the sceptics lay in the last position. There is no great disproportion between the parties. We can highlight that the number of the institutions strongly trusting in the technology is little more than the ones thinking it will not be ground-breaking. This result points out the fact that probably the relative early stage of maturity of the blockchain technology may be the cause of suspiciousness of many institutions. Many researches should still be performed before obtaining certain results for its reasonable applicability. This opinion derives from the answers of the respondents. The lack of trust is often said to be dependent on the lack of sure use cases in which the blockchain can be

efficiently applied. We expect therefore that in the event in which the blockchain will reach a significant level of maturity the position of the left-side institutions in the matrix will change. Budget instead may often be one of the reasons for the organization structures. Having more money to be invested may guarantee also a greater number of paid employees dedicated to the topic.

To deepen our understanding of these choices we have also considered how the institutions, and more precisely their responsible functions, approach the BCT. We have analyzed if they are moved by more technical lenses or by a business vision. For this research we focused only on the interviewed FIs, as they are the only ones which organizationally arranged for studying the blockchain. The following image represents it:

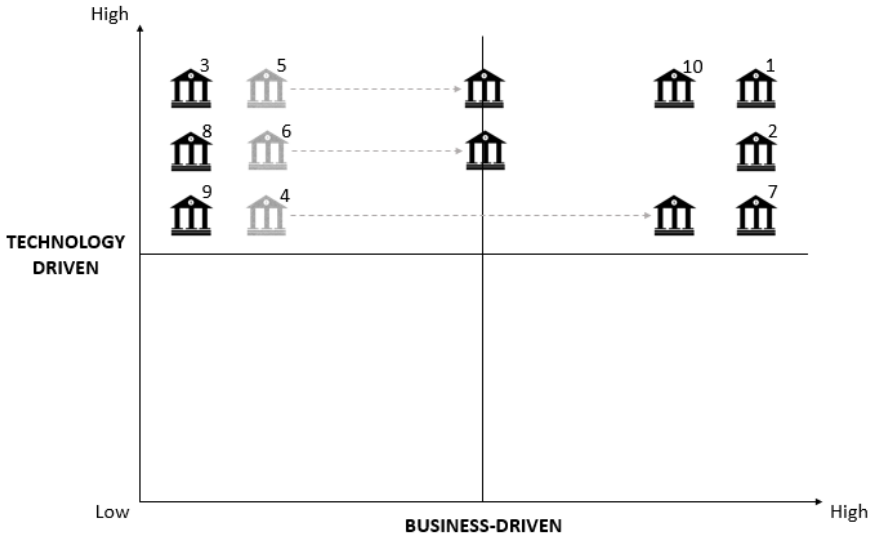


Figure 68, organizational approach to the BCT

The black icons represent the current position of the FIs, the grey owns their initial approach to the BCT. As we can see many of them started studying it from only a technical point of view, trying therefore to understand the characteristics of the blockchain, its limits and benefits. Half of this group recently began to take into consideration also the business prospective of the underlying technology, shifting from the upper-left side of the matrix to the right. While, the other three are still looking at the blockchain with technological lenses. Only three of the respondents have been also business driven from the beginning.

The lower part of the matrix is empty. Since the blockchain is a quite new technology, this result is not surprising. It should be studied in deep to be able to obtain economic advantages from it. Only when a product reaches a high level of maturity, it can be exploited only for its business applicability.

Concerning the preferred blockchain platform, 40% of the respondents consider the private form more suitable for the financial sector. The need for privacy is the primary reason of this consideration. On the other hand, public platforms fit better the use cases' requirements for 20% of the interviewed FIs. They indeed consider as necessary the transparency of data, for example to perform AML activities in collaboration with other FIs. Moreover, they believe that only public platform can offer a real disintermediation, through the distribution of power equally among the nodes. The last 40% of our sample thinks that the choice of the platform is strictly related to the use case in which it will be applied. Different activities have indeed different requirements which can be better met in some instances by public platform, while private ones perform better in other situations.

Another interesting point which has been recurrent in many interviews is the fact the virtuous cycle the blockchain has generated. To fully exploit its benefits indeed and to more easily obtain positive results, the FIs should collaborate with one another and become part of the blockchain network. Therefore, some consortia have been created with the purpose to jointly research on a specific use case applicability. The more FIs enter into these groups, the more advantages the blockchain can bring, the more the consortia attract other members and so on. The collaboration between financial institutions not only ease the studies on the topic, but create a better environment for the overall sector, impacting also on the services offered to the customers. They will indeed offer the possibility to clients of different FIs to interact with one another faster and easier. To do so the institutions run all the same software in a distributed way, where data can be shared. This collaboration between financial institution could not be achieved without the blockchain as a single entity governing the group should be needed, as we have already report in the insurance section of the previous chapter. This single entity entitled to keep all the relevant information of the parties would own extraordinary power and responsibility. All the entities would need to interact with this third party to enter in contact with one another, resulting in an expensive intermediated process.

6.4 Conclusion

Overall, we want to conclude by depicting the Italian financial institutions' position with respect to the BCT. From the analysis we have performed in this section, we can say that Italian institutions are generally interested in the topic, with different level of partecipation. Most of their studies are efficient application of the technology, signal of a careful analysis and evaluation of the topic. Nevertheless, the level of awareness of most of the respondents is still low, due to a limited activity or to a certain degree of suspiciousness towards this new technology. The cause of this result may be traced from the relative early stage of maturity of the BCT. The lack of trust is said by some respondents to be dependent on the lack of sure use

cases in which the blockchain can be efficiently applied. Some studies are still required to gain substantial advantages from the technologies. We expect therefore that in the event in which the blockchain will reach a significant level of maturity the position of the financial institutions will change. Budget can also be listed among the causes; indeed, all the financial institutions with an index of awareness higher than three have currently a market share in Italy which is much higher than the others. Having more money to be invested may guarantee greater possibility to study the topic.

To better visualize these results, we combine two information we have previously analyzed: the awareness index and the four typologies of the organization-expectations matrix.

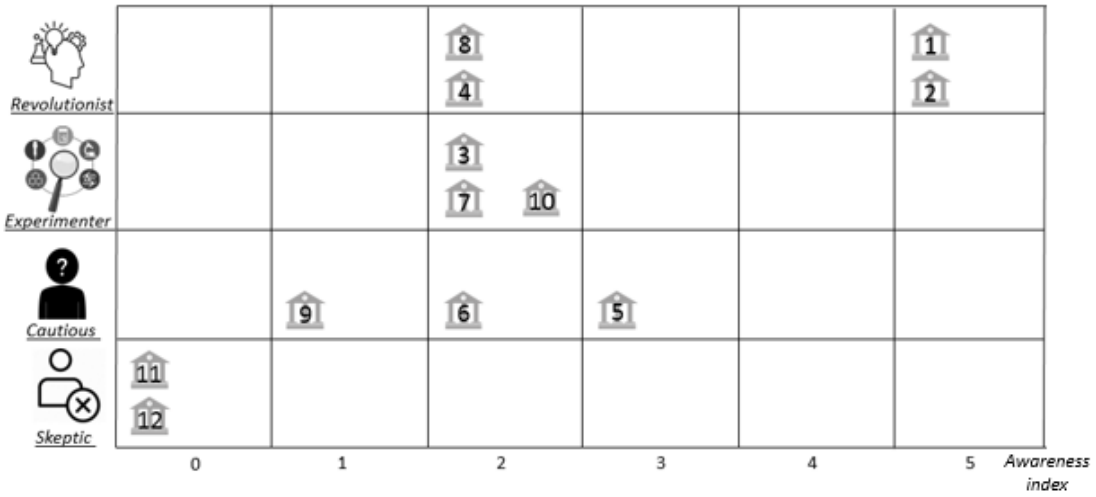


Figure 69, Italian Financial Institutions' position with respect to BCT

The lack of confidence the Italian financial institutions have towards the BCT is due to their limited commitment with it. Indeed, as we can see from the above figure, the more an institution studies it and puts greater effort in understanding its applicability, the more it is convinced of its potentiality. This consideration is auspicious for the development of the technology, since those which are more dedicated to working with it see beneficial changes in the future, which may disrupt the current context. As we have already said, the cause for the inactivity of many institutions is not due to a disinterest in the topic, nor to a deviation from it after ascertaining its uselessness or limitedness of efficiency advantages. Instead, it is usually due to a shortness of funds to be invested in BCT projects, thus, since the technology is still at its early stage of development, they are waiting for other to foster it, and then to enter into the context when a higher level of maturity will be reached. Considering the fact that still no use case has generally been implemented on a market with broad scope, they might even be uncertain about what the technology may bring in the future, whether it will be really disruptive or not. This doubt prevents their economic commitment. This group of actors

include both the ones little studying the BCT, the cautious, but also the sceptics. The latter have a lower level of awareness of the topic, to such an extent that some of them do not even know what blockchain is, or they have just heard the name, but they never deepened this news. Some of our respondents have reported this problem, highlighting the importance of university or other institutions to spread knowledge about the topic, and being moreover the generator of a network of actors which could collaborate and interact with one another to support their researches and speed up the learning path. A blockchain culture is therefore needed to support its widespread adoption.

As we have seen, most of the undertaken projects may be improvements for current processes, though further steps are needed to implement them on a larger scale. To do this in the Italian market, two institutions are leading the others. One of them is experimenting the applicability in several areas, thus trying to assess the different impacts the BCT can have in the financial activities, but mainly with a limited geographical scope, i.e. in the Italian market; on the other hand, the other one is instead focusing on a single use case, but with a more international background. They both can be beneficial for our financial sector since, on one hand they can give important notions about where blockchain can fit, on the other hand, they can take other institutions to a broader market.

Some players are already enthusiastic representants of this new technology, strongly believing in its capacity to disrupt the financial sector, as well as many others. Despite their strong passion, they have not invested a lot of money in it. Nevertheless, the participation to consortium, conferences on the topic or other events are the important instruments as of now. Though, due to the shortness of funds or the limitations coming from the higher level of a company, it is crucial to spread the knowledge regarding the blockchain and collaborate so that the sum of each institution's efforts can generate a strong fuel for the development of the innovation.

Overall, we can conclude that Italian financial institutions are still in phase of learning and testing, though there are two exceptions which participate more intensively in the operations regarding BCT. The researchers are proceeding at a fast pace, thus their level of awareness may change and increase soon, thanks also to the support of universities and other research entities, as well as to the collaboration among the parties.

CHAPTER 7
CONCLUSIONS, LIMITATIONS AND FUTURE RESEARCH

In this last chapter, we draw conclusions on the work done, highlight limitations and criticalities of our findings, and indicate directions for future research on questions that are still open.

In section 7.1, we sum up the findings throughout our work, the conclusions drawn from the technical analysis, the possible application of blockchain in finance with a mapping that shows the interested areas and what kind of processes can be improved.

In section 7.2, we point out limitations to our research. Indeed, the choice of data sources, the responses to the interviews we carried out, and the reliability of the websites we browsed might have created biases in our data, making the overall mapping not thorough.

Finally, in section 7.3 we point out what other research questions could arise from our thesis work, that are still unanswered by the literature, to find new directions for future researches and future works on the topics, for both academic and business study.

7.1 Conclusions

In our thesis, we explored the usage of blockchain in the financial world, with the purpose to answer the following research question: *In which application areas the BCT might be a beneficial instrument for the financial sector?*

In Chapter 3, we reviewed technical literature to identify issues with blockchain technology adoption in general: which are still in place and hinder widespread adoption and

which are already solved. This was done to develop an adoption framework for blockchain technology, independently from the sector of applicability. It was essential to later analyze the data gathered from startups' and companies' initiatives and filter those where blockchain did not make sense or whose problems were not considered. We combined technical literature information with that reviewing the technology from a strategic perspective, that is, whether it should be applied instead of a traditional centralized database architecture (Section 3.9).

Then, approaching the financial industry, we reviewed the literature concerning the classification of financial intermediaries in Chapter 4. Our aim was that of defining which institutions could be interested in the adoption of the technology. Yet, we found that literature classified institutions according to their functions, but such classification is nowadays more of an historical heritage, as most intermediaries are engaged in all the possible functions, making the classification not relevant. Therefore, we changed our approach: instead of focusing on the type of institution, we focused on the functions themselves. We would show how blockchain could be employed in payments, investment products, lending, supply chain finance, risk and insurance, fiduciary services and secondary activities: KYC procedures.

In the following two chapters we conducted our research and responded to the research question. We analyzed news articles, startups leveraging the technology, companies testing it, and interviewed experts in the Italian financial sector. In conclusion, we found that blockchain technology might have a disruptive impact on most of the areas in the financial industry (Chapter 5-6).

The projects mostly entail more efficient transactions and communications across institutions (Chapter 5). This need is caused mainly by the lack of shared infrastructure, causing centralized database to be frequently updated by manual intervention, giving room to mistakes and high costs to manage certain practices. Instead, a distributed ledger can make all participants aware at the same of the current status of operations. Also, DLT could disintermediate some areas, especially in the post-trade processing of securities, eliminating certain intermediaries, or simplifying their internal processes. What we found to be critical, instead, is the adoption for those activities where a highly-trusted centralized party exists, such as a central bank. In this case, DLT are not more efficient than centralized systems, and the fact that players do not have economic interest in the process they manage (i.e. they are regulators or governmental institutions), the need for trust to be in the system is not present, as it already exists within the centralized institution itself (Section 5.3).

The analysis of Italian financial institutions did not alter the framework defined in Section 5.16, created by the analysis of international sample. Instead, it confirmed it, as we documented that the most aware financial institutions in the field are working exactly on the same areas of international peers. In Figure 70, we report our conclusive findings in the

adoption framework: first, we defined generally in which situations blockchain is preferable to a traditional centralized database infrastructure and if a public or a permissioned version is more suitable. We used such framework to guide us in the selection of relevant blockchain projects as opposed to deceptive ones that did not justify blockchain adoption.

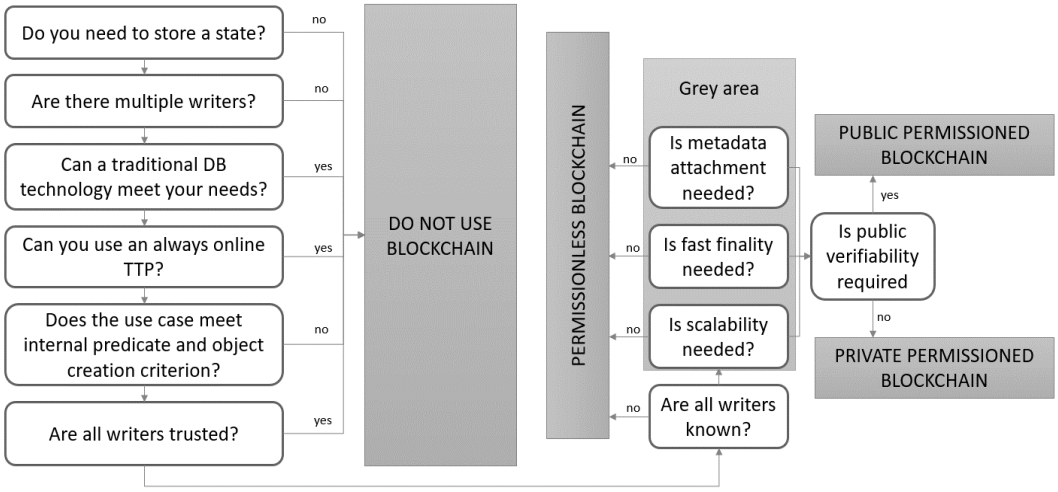


Figure 70, general blockchain adoption framework.

As a second step, we analyzed in detail the remaining initiatives and found that blockchain can be applied in financial services in the following processes.

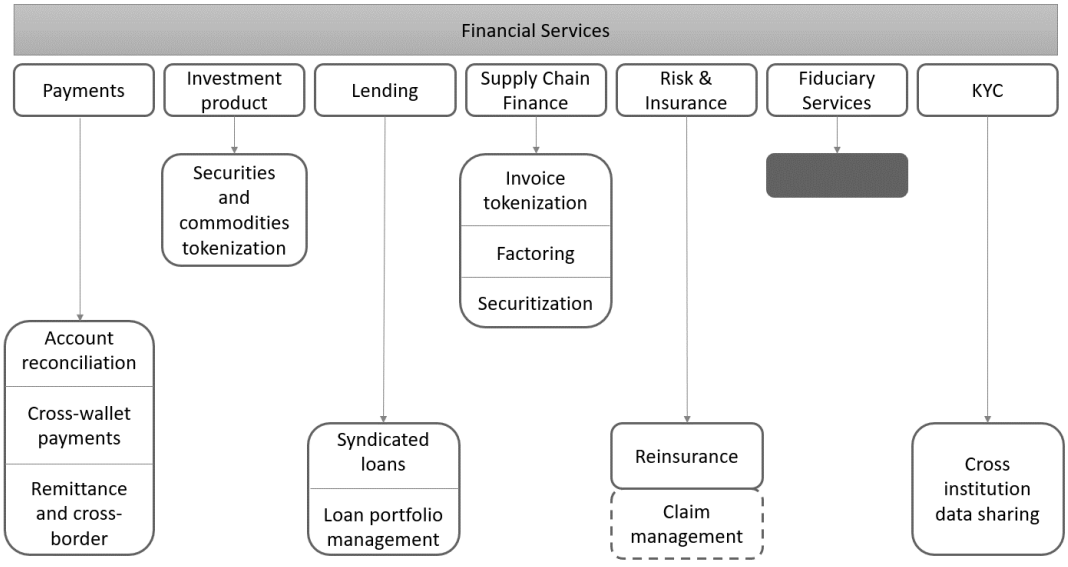


Figure 71, conclusive financial adoption framework.

So, in the payment area we found that blockchain can have a relevant impact in: account reconciliations, especially for those transactions that are not managed by the SEPA circuit. Also,

the technology could enable different wallet providers to transact with one another, opening up the market and freeing it from the platform logic. Finally, remittance and cross-border payments in general can benefit from the technology by removing the need for nostro accounts and correspondent banks. Instead, for national payments recurring to the current system managed by central banks is highly preferable (Section 5.3).

The technology might be disruptive in the investment products area, if securities are tokenized. Indeed, tokenized securities could be settled close to real-time, instead of the current T+1,2,3 standards. This is possible if the cash leg of the transaction is present on the ledger: this way, DvP is highly simplified, and the need for many manual operations (especially in the communication process among intermediaries) and book reconciliations are no longer needed. Also, smart contracts could automate most of the security management: from collateral management to asset servicing, to tax withholding (Section 5.5).

In lending, we couldn't find applications improving the current process either for mortgages or for unsecured loans. Yet, the technology is beneficial for back office procedures and, again, to avoid account reconciliations. It is used for syndicated loans management, simplifying interest payment by the borrower (through smart contracts automatically splitting tranches to the entitled lenders), giving lenders a view of the overall loan status and the servicing from other counterparties. Also, BCT could help loan portfolio management thanks to an application creating a marketplace for loans instead of the current bilateral agreement system. Besides, the same application could speed up loan securitization procedures (Section 5.7).

Supply chain finance can find higher efficiency with blockchain adoption. In particular, a DLT can store information about trading documents and bank sureties, proving their authenticity. Secondly, the tokenization of invoices on a blockchain would increase the efficiency of the current factoring process, by eliminating the possibility of double spending and the impossibility of having receivables financed by multiple banks. Finally, invoice securitization can also be easily managed with BCT by leveraging the advantage we mentioned for investment products (Section 5.9).

Risk is another area that is not specifically addressed by any project. Still, blockchain can have implication for risk management due to the real-time settlement opportunities: we shall discuss this in section 8.3. Insurance can benefit from the easier reconciliation in the reinsurance process where many actors are involved. Furthermore, claim management costs could be reduced by automating reimbursement decisions through smart contracts. So far though, technological limits are hindering the latter application, and most cases are of usage in simple insurances that can be answered by a yes/no question and do not entail the evaluation of a damage (Section 5.11).

In fiduciary services, we could not find any project, probably due to the lack of multiple players' interaction and the need of a one to one relationship that makes no sense to be disintermediated (Section 5.13).

Finally, the cost of KYC procedures could be driven down thanks to the sharing of the documents: instead of repeating the assessment for every institution, documents can be uploaded on a common DLT platform, and then users can grant selective access to the institutions they get into contact with. This cost reduction can drive value also in other areas such as in SCF programs: here, each bank might have to review KYC compliance for hundreds of companies taking part to the program, making it hard for small banks to sustain the cost, and for companies to use the instrument in case of high interests charged by banks to cover such high costs (Section 5.15).

From financial institutions interviews, we confirmed our knowledge in this area, as all the projects reported fall in the same areas of the international ones. Additionally, we found that few institutions are well positioned and about to launch new products, whereas others have little knowledge about the technology. Interviews also allowed to draw important consideration about benefits and limits of blockchain application in the reviewed areas (Chapter 6).

Altogether, the key takeaways from our research can be listed as follows:

- BCT is a disruptive technology in some financial areas. The main benefit is that of process automation, the elimination of manual reconciliation procedures, and the standardization of data stored in the shared ledger (Chapter 5).
- BCT projects are turning from PoC and tests to real products. Some have already been launched, some will enter production by the end of 2018 or in 2019 (Chapter 5-6).
- Public blockchains are not fit yet to either challenge or be leveraged by financial institutions. Instead, permissioned blockchain can be and are already being used (Chapter 3-5).
- Consequently, most startups working with public blockchains do not offer viable business models as they do not answer to open challenges posed by the technology. Instead, startups developing products on permissioned blockchains seems to be better poised to collaborate with financial institutions (Chapter 5).
- Some Italian financial intermediaries are in line with international institutions in the launch of blockchain products. Yet, most of smaller Italian banks are not fully aware of the technology potential and they configure themselves as followers (Chapter 6).
- The technology can drive value to smaller businesses and newcomers as it could disrupt the centralized platform logic. However, building consortia's infrastructure is a concept not rooted enough in current business and competitions logics, so, the process is slow and constrained. Mostly, just large institutions create blockchain

platforms, still leveraging their dominant market position to onboard smaller institutions for fees, making them clients instead of peers. Also, regulation is another limit to unlocking the full potential of the technology: the gaps in current laws or conflicting norms hinder a rapid adoption (Chapter 6).

- Globally, all actors in the financial industry should monitor the technology as its impacts on the sector are relevant and it is evolving fast (Chapter 3-5-6).

7.2 Limitations

In this section, we shall list the issues that might arise from our research methodology. We identified for each source of information relevant limits that might have had an impact on data population.

Firstly, for the startup database we reviewed startups only in the website CrunchBase which allows for data self-declarations. Therefore, the capital collected might be far from real values. Additionally, we missed many startups that use the technology and are not listed on CrunchBase or are listed but did not mention blockchain in the description, so did not show up on our search.

Secondly, the websites we used to gather the news were all grounded in the US or in Italy, meaning that the larger part of the news involved Italian or American institutions testing the technology. International initiatives reported were only present for large institutions that made the news internationally available. This might have implication with the interviews, the evaluation of the applicability of the technology and the awareness factor: some of the projects we came to know from the interviews were actually already present in our collection of news, making a small part of the data redundant rather than adversary. Yet, the two sources were still useful as they completed each other in answering our research question, as most of the data was not actually duplicate.

Finally, interviews mostly involved Italian retail and universal banks. Few other institutions outside the banking sector answered our interview requests. Consequently, the second instrument we used to map blockchain adoption in the financial area shows weaknesses in number and diversification of the population. Furthermore, the interviews were typically conducted only with 1 to 3 persons that were working on the blockchain topic, a factor which could have had an impact on data in terms of personal biases.

To sum up, data collection is to be considered non-exhaustive, and the answer to the question cannot be considered thorough, since considering a different set of websites for both the news and the startups could have led to partially different results. The same applies to the

interviewed experts: a different set could have led to a different mapping of the processes, let alone the trends reported by the awareness index.

7.3 Future research

We hope that with our thesis work we were able to shed some light on a cryptic technology that is widely discussed. In particular, we hope that our work could set up a framework to consider for future researches on blockchain adoption in financial processes. Now that the research question "*In which application areas the BCT might be a beneficial instrument for the financial sector?"* was answered, new questions naturally arise.

- What is the quantitative impact in term of costs and investments needed, for blockchain adoption in the areas we mapped? Which area grants the largest economic benefit?
- What are the implications for current monetary policies should securities or money be moved on a blockchain infrastructure? How could central banks liquidity facilities change?
- What are the implications for liquidity risk and liquidity management should institutions adopt a RTGS system for all payments and securities' trade?
- Which other industries might be impacted by the technology?

In general, the environment is rapidly changing, both because the technology is evolving fast (especially the permissioned versions) and institutions are continuously launching new products and tests to experiment applications in new areas. So, a constant monitoring is needed by researches to have a clear and up to date mapping of blockchain applications.

REFERENCES

AIPB. (2015). Private al servizio degli imprenditori. Milano Finanza.

AIRA, A. I. (2005). L'evoluzione della normativa antireciclaggio.

Akerlof, G., 1970, “The market for lemons”: Qualitative Uncertainty and the Market Mechanism. Quarterly Journal of Economics 89: 488-500.

Alberts, C., & Dorofee, A. (2010). Risk management framework. Carnegie Mellon University.

Ammous, S. (2016). Blockchain Technology: What is it Good for?

Andrychowicz M, Dziembowski S, Malinowski D, Mazurek. On the Malleability of Bitcoin Transactions. In: Brenner M, Christin N, Johnson B, Rohloff K, editors. Financial Cryptography and Data Security. vol. 8976 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2015. p. 1–18.

Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S., 2013. Evaluating user privacy in bitcoin. In: Sadeghi, A.-R. (ed.) FC 2013. LNCS, vol. 7859, pp. 34–51. Springer, Heidelberg (2013).

Anish Dev J. Bitcoin mining acceleration and performance quantification. In: Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on; 2014. p. 1–6.

Antonopoulos, A., 2014. Mastering Bitcoin. O’Reilly Media, USA.

Antonopoulos, A., 2017. How likely Bitcoin will become obsolete; Q&A session. Available from: https://www.youtube.com/watch?v=tBnC9AhKjws.

APEC (Asia-Pacific Economic Cooperation), 2015. Regulatory issues affecting trade and supply chain finance.

Ateniese G, Faonio A, Magri B, de Medeiros B. Certified Bitcoins. In: Boureanu I, Owesarski P, Vaudenay S, editors. Applied Cryptography and Network Security. vol. 8479 of Lecture Notes in Computer Science. Springer International Publishing; 2014. p. 80–96.

Atzei, N., Bartoletti, M., Cimoli, T., 2016. A survey of attacks on Ethereum smart contracts. Cryptology ePrint Archive, Report 2016/100. http://eprint.
iacr.org/2016/1007Back (A,), M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller,

A. Poelstra, J. Timo´n, and P. Wuille. Enabling blockchain innovations with pegged sidechains, 2014.

Baden-Fuller, C., & Haefliger, S. (2013). Business Models and Technological Innovation.

Badertscher (Christian), Peter Gazi, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. IACR Cryptology ePrint Archive, 2018:378, 2018.

Bamert T, Decker C, Wattenhofer R, Welten S. BlueWallet: The Secure Bitcoin Wallet. In: Mauw S, Jensen C, editors. Security and Trust Management. vol. 8743 of Lecture Notes in Computer Science. Springer International Publishing; 2014.

Barkatullah J, Hanke T. Goldstrike 1: CoinTerra's First-Generation Cryptocurrency Mining Processor for Bitcoin. Micro, IEEE. 2015; 35(2):68–76. doi: 10.1109/MM.2015.13.

Barriball, K., & While, A. (1994). Collecting data using a semi-structured interview: a discussion paper. Journal of advanced nursing.

Basel Commitee on Banking Supervision. (2011). Core Principles for Effective. Bank for International Settlements.

BCG, B. C., & AIPB, A. I. (2017). Il Private Banking nel mondo. Milano.

Beck, R., & Muller-Bloch, C. (2017). Blockchain as radical innovation: a framework for engaging with distributed ledgers. 50th Hawaii international conference on system sciences.

Bhat, G., Lee, J., Ryan, S.G., 2016, Using Loan Loss Indicators by Loan Type to Sharpen the Evaluation of Banks' Loan Loss Accruals. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490670.

Bhattacharya, Thakor (1993), Contemporary Banking Theory, Journal of financial intermediation.

Beikverdi A, Song J. Trend of centralization in Bitcoin's distributed network. In: Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2015 16th IEEE/ACIS International Conference on; 2015. p. 1–6.

Benedetti, M., Galano, G., 2016. The Blockchain Technology: Elements of novelty, properties, evolution. Available from: https://www.bancaditalia.it/pubblicazioni/altri-atti-convegni/2016-tecnologia-blockchain/Pres_Benedetti.pdf.

Bentov (Iddo), Ariel Gabizon, and Alex Mizrahi. Cryptocurrencies without proof-of-work. CoRR, abs/1406.5694, 2014.

Blinking Team. (2018). Adapting KYC (Know Your Customer) procedure to GDPR. Medium.

Bliss, R., and Kaufman, G., 2006. Derivatives and Systematic Risk: Netting, Collateral and Closeout. Journal of Financial Stability 2006, 2: p.55-70.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W.: Mixcoin: anonymity for bitcoin with accountable mixes. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 481–499. Springer, Heidelberg (2014).

Bos JW, Halderman JA, Heninger N, Moore J, Naehrig M, Wustrow E. Elliptic Curve Cryptography in Practice. In: Financial Cryptography and Data Security—18th International Conference, FC 2014, Christ Church, Barbados, March 3–7, 2014, Revised Selected Papers; 2014. p. 157–175.

Brown, R.G., Carlyle, J., Grigg, I., Hearn, M., 2016. Corda: an introduction. Available from: https://docs.corda.net/_static/corda-introductory-whitepaper.pdf

Buterin, V., 2013. A Next Generation Smart Contract & Decentralized Application Platform. Ethereum White Paper.

Cachia, M., & Millward, L. (2011). The telephone medium and semi-structured interviews: a complementary fit. QUALITATIVE RESEARCH IN ORGANIZATIONS AND MANAGEMENT: AN INTERNATIONAL JOURNAL.

Callahan, J. (2018). Know Your Customer (KYC) Will Be A Great Thing When It Works. Forbes.

Camerinelli, E., Bryant, C. (2014), Supply chain finance—EBA European market guide version 2.0. Available from: https://www.abe-eba.eu/media/azure/production/1544/eba-market-guide-on-supply-chain-finance-version-20.pdf.

Carlson, B., Romanelli, G., Walsh, P., Zhumaev, A., 2018. Blockchain beyond the hype: What is the strategic business value? Available from: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

Carlyle, James, Corda Performance: To infinity and beyond, 7 March 2018. Available from: https://www.r3.com/wp-content/uploads/2018/04/Corda-Performance-ENG.pdf

de Cavalho, C. (2005): Cross-Border Securities Clearing and Settlement Infrastructure in the European Union as a Prerequisite to Financial Markets Integration: Challenges and Perspectives. HWWA Discussion Paper 287.

van Cayseele, P., Wuys, C. (2005), Cost Efficiency in the European Securities Settlement and Safekeeping Industry. In: Clearing and settlement of financial markets.

Chandrashekar, K., 2008. Collateral Management: An Introduction. Wipro Technologies.

Charette, R. (1990). Applications Strategies for Risk Analysis. Intertext Publications.

Chen, H., Farias, V.F., Gutin, E., 2017. Dynamic Collateral Management. Available from: http://egutin.com/files/CollateralMgmt.pdf

Cherubini, U., 2005. Counterparty Risk in Derivatives and Collateral Policies: The Replicating Portfolio Approach. In ALM of Financial Institutions, ed. Tilman, L., Institutional Investor Books.

Chiu, J., Koeppl, T.V. (2018), Blockchain-based Settlement for Asset Trading. Electronic copy available at: https://ssrn.com/abstract=3203917.

Choudhry, M., Fabozzi, F.J., 2004. The Handbook of European Structured Financial Products. Wiley Finance.

Chuat L., P. Szalachowski, A. Perrig, B. Laurie, and E. Messeri. Efficient Gossip Protocols for Verifying the Consistency of Certificate Logs. In 2015 IEEE Conference on Communications and Network Security (CNS), 2015.

Circle, 2018. Centre Whitepaper.

Cong, Lin and He, Zhiguo and Li, Jiasun, Decentralized Mining in Centralized Pools (October 2018). George Mason University School of Business Research Paper No. 18-9. Available at SSRN: https://ssrn.com/abstract=3143724 or http://dx.doi.org/10.2139/ssrn.3143724.

Covip, Commissione di vigilanza sui fondi pensione, (2018), Relazione per l'anno 2017, available at:
https://www.covip.it/wp-content/files_mf/1533224551RelazioneAnnuale2017def.pdf

Croman (Kyle), Christian Decker, Ittay Eyal, Adem Efe Gencer, Ari Juels, Ahmed Kosba, Andrew Miller, Prateek Saxena, Elaine Shi, and Emin Gün. On scaling decentralized blockchains. In Proc. 3rd Workshop on Bitcoin and Blockchain Research, 2016.

Crosby, M., Pattanayak, P., Varna, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. Applied Innovation Review.

Daian, Phil, 2016. Analysis of the DAO exploit. Available at: http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/

Daian, (Phil), Rafael Pass, and Elaine Shi. Snow white: Provably secure proofs of stake. Cryptology ePrint Archive, Report 2016/919, 2016. https://eprint.iacr.org/2016/919.

Danezis (G.) and S. Meiklejohn. Centrally Banked Cryptocurrencies. 23rd Annual Network & Distributed System Security Symposium (NDSS), Feb. 2016.

David, B., Gaži, P., Kiayias, A., Russell, A.: Ouroboros Praos: an adaptively-secure, semi-synchronous proof-of-stake blockchain. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10821, pp. 66–98. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78375-8_3

De Hann J., Oosterloo S., and Schoenmaker D. (2009) European financial markets and institutions, Cambridge University Press, available at: https://forfreeshare.weebly.com/uploads/1/2/5/1/12515971/european_financial_markets_and_institutions.pdf

Decker C, Wattenhofer R. Bitcoin Transaction Malleability and MtGox. In: Kutyowski M, Vaidya J, editors. Computer Security—ESORICS 2014. vol. 8713 of Lecture Notes in Computer Science. Springer International Publishing; 2014. p. 313–326.

Deloitte Development. (2017). Collision or collaboration: What's on your payments radar?

Deloitte Development. (2018). Deloitte's 2018 global blockchain survey, Breaking Blockchain Open.

DeMarzo, P.M. 2005. The pooling and tranching of securities: A model of informed intermediation. Review of Financial Studies 18, 1-35.

Dermine, J., 2017, Digital Disruption and Bank Lending. Journal of European Economy, 2017.2: 63-76.

Diamond, D.W., 1984, Financial intermediation and delegated monitoring. Review of Economic Studies LI: 393-414.

Diamond, D.W., Dybvig, P.H., 1983, Bank Runs, Deposit Insurance, and Liquidity. The Journal of Political Economy, Vol. 91, No. 3: pp. 401-419.

Dietrich, R.J., Kaplan, R.S., 1982, Empirical Analysis of the Commercial Loan Classification Decision. The Accounting Review, Vol. 57, No. 1 pp. 18-38.

Digital Finance Observatory, 2016. Blockchain: Where are we and where will we go. Slide booklet. Available at: www.osservatori.net.

Dilley (John), Andrew Poelstra, Jonathan Wilkins, Marta Piekarska, Ben Gorlick, and Mark Friedenbach, Strong Federations: An Interoperable Blockchain Solution to Centralized Third-Party Risks, arXiv:1612.05491v2 [cs.CR], 6 Jan 2017.

Dimakis Alexandros G., Anand D. Sarwate, Martin J. Wainwright, Geographic gossip: efficient aggregation for sensor networks, Proceedings of the 5th international conference on Information processing in sensor networks, April 19-21, 2006, Nashville, Tennessee, USA [doi>10.1145/1127777.1127791].

Dimakis A. Sarwate M. Wainwright "Geographic gossip: Efficient averaging for sensor networks" IEEE Transactions on Signal Processing vol. 56 no. 3 pp. 1205-1216 2008.

DTCC, 2014. Trends, risks and opportunities in collateral management: A collateral management white paper. DTCC, January 2014, Available at: http://www.dtcc.com/about/managing-risk/collateral-management.aspx.

Eskandari (Shayan), Jeremy Clark, David Barrera, Elizabeth Stobert, 2015. A first look at the usability of bitcoin key management. USEC 15: NDSS Workshop on Usable Security (USEC) 2015, San Diego, CA, USA, February 8, 2015, Internet Society.

Eyal, I., Sirer, E., 2014. Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In: Christin N, Safavi-Naini R, editors. Financial Cryptography and Data Security. vol. 8437 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2014. p. 436–454.

Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse. Bitcoin-NG: A Scalable Blockchain Protocol. Technical report, CoRR, 2015.

Everett, M. R. (1995). Diffusion of Innovation. The Free Press.

Floyd, D., 2017. A Blockchain that Handles Millions of Transactions per Second? Available at: https://www.nasdaq.com/article/a-blockchain-that-handles-millions-of-transactions-per-second-cm895876

FSB, (. S. (2018). FSB Action Plan to Assess. Basel, Switzerland.

Garavaglia, R., 2018. https://www.blockchain4innovation.it/esperti/criptovalute/il-custode-e-responsabile-delle-chiavi-degli-appartamenti-o-di-cio-che-vi-e-contenuto/

Gilad (Yossi), Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. Cryptology ePrint Archive, Report 2017/454, 2017. http://eprint.iacr.org/2017/454.

Gillan S.L., Starks L.T., (2000), Corporate governance proposals and shareholders activism: the role of institutional investors, Journal of financial economics, available at:

http://mx.nthu.edu.tw/~jtyang/Teaching/Corporate_Governance/Papers/Gillan,%20Stark%202000.pdf

Ghosh, A., Rennison, G., Soulier, A., Sharma, P., and Malinowska, M., 2008. Counterparty Risk in Credit Markets. Barclays Capital Research Report.

Glaser, F. (2017). Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis. 50th Hawaii International Conference on System Sciences. HICSS.

Greenbaum S., Thakor A., Boot A., (2015) Contemporary Financial Intermediation, Academic Press

Gregory, J., 2010. Counterparty Credit Risk: The New Challenge for Financial Markets. Wiley, Chichester.

GSCFF (Global SCF Forum) (2015), Standard definitions for techniques of supply chain finance. Available from: http://supplychainfinanceforum.org/ICC-Standard-Definitions-for-Techniques-of-Supply-Chain-Finance-Global-SCF-Forum-2016.pdf.

Gveroski M., Risteska A., Dimeski S., (2009), The role of financial institutions as participants on the capital market, Annals of the "Constantin Brâncuşi" University of Târgu Jiu, Economy Series, available at: http://www.utgjiu.ro/revista/ec/pdf/2009-01/10_GVEROSKI_MIROSLAV.pdf

Hammond, S., & English, S. (2017). Cost of Compliance 2017. Thomson Reuters.

Hannay, J., Sjøberg, D., & Dybå, T. (2007). A systematic review of theory use in software engineering experiments.

Harris, M., Raviv, A., 1978, Optimal incentive contracts with imperfect information. Journal of Economic theory 20: 231-259

Hearn, Mike, 2016. Corda: a distributed ledger. Available from: https://www.corda.net/content/corda-technical-whitepaper.pdf

Herrera-Joancomartì, J., 2015. Research and Challenges on Bitcoin Anonymity. J. Garcia-Alfaro et al. (Eds.): DPM/SETOP/QASA 2014, LNCS 8872, pp. 3–16, 2015. DOI: 10.1007/978-3-319-17016-9 1.

Hess A.C., Laisathit K, (1997), A market-based risk classification of financial institutions, Kluwer Academic Publishers.

Hileman, Garrick and Rauchs, Michel, 2017. Global Blockchain Benchmarking Study (September 22, 2017). Available at SSRN: http://dx.doi.org/10.2139/ssrn.3040224.

Hofmann, E., Belin, O. (2011), Supply chain finance solutions: relevance, propositions, market value. Springer, Berlin.

Hofmann, E., Magnus Strewe, U., & Bosia, N. (2018). Supply Chain Finance and Blockchain Technology - the case of reverse securitisations . SpringerBriefs.

Hofmann, E., Zumsteg, S. (2016), Win-win and no-win situations in supply chain finance: the case of accounts receivable programs. Supply Chain Forum: An Int J 16(3): 30-50.

Holmström, B., 1979, Moral Hazard and Observability. Bell Journal of Economics 10: 74-91.

Holsapple, C., & Singh, M. (2001). The knowledge chain model: activities for competitiveness. In Expert System with Application (pp. 77-98).

Hoskinson, Charles, 2017. IOHK | Cardano whiteboard; overview with Charles Hoskinson. Available from: https://www.youtube.com/watch?v=Ja9D0kpksxw.

Houy, Nicolas, 2014a. It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency (January 2014). Available at SSRN: https://ssrn.com/abstract=2393940 or http://dx.doi.org/10.2139/ssrn.2393940

Houy, Nicolas, 2014b. The Economics of Bitcoin Transaction Fees, WP1407, (2014).

Hull J.C., (2015) Risk management and financial institutions, Wiley, available at: http://www.simonfoucher.com/MBA/FINA%20695%20-%20Risk%20Management/riskmanagementandfinancialinstitutions4theditionjohnhull-150518225205-lva1-app6892.pdf

IBM. (2018). Let's settle payments in seconds - not days. International Business Machines Corp.

ICC (International Chamber of Commerce), 2014. Global Trade and Finance survey: rethinking trade and finance. Available at: https://cdn.iccwbo.org/content/uploads/sites/3/2017/06/2017-rethinking-trade-finance.pdf

ISTAT, Istituto statistico nazionale, Vicari P., Ferrillo A., Valery A., (2009), Classificazione delle attività economiche Ateco 2007, available at: https://www.istat.it/it/files/2011/03/metenorme09_40classificazione_attivita_economiche_2007.pdf

Jarrow, R.A., Yu, F., 2001, Counterparty risk and the pricing of defaultable securities. Journal of Finance LVI (5): 1765–1782.

Jensen, Michael C. and William H. Meckling. 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics (October), 3(4): 305–360. Available from: https://www.sfu.ca/~wainwrig/Econ400/jensen-meckling.pdf.

Johansen H. D., R. V. Renesse, Y. Vigfusson, and D. Johansen. Fireflies: A secure and scalable membership and gossip service. ACM Trans. Comput. Syst., 2015.

Kaal, W.A., 2017. Blockchain Applications and Fee Structure Developments in Private Investment Funds. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959730

Kang, J., Kim, H-S., 2005, Pricing counterparty default risks: applications to FRNs and vulnerable options. International Review of Financial Analysis 14(3): 376–392.

Kennedy, C., & Harney, A. (2018). MiFID II vs GDPR: The Delicate Balance Between KYC and Data Privacy. Data Management Review.

Kiayias, A., Panagiotakos, G.: Speed-security tradeoffs in blockchain protocols. Cryptology ePrint Archive, Report 2015/1019 (2015). http://eprint.iacr.org/2015/1019.

Kiayias A., Russell A., David B., Oliynykov R. (2017) Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol. In: Katz J., Shacham H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10401. Springer, Cham.

King, C. (2018). Anti-Money Laundering: An Overview. In C. King, C. Walker, & J. Gurulé, The Palgrave Handbook of Criminal and Terrorism Financing Law. Palgrave Macmillan, Cham.

King, Sunny, Nadal, Scott, 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. Available from: https://peercoin.net/assets/paper/peercoin-paper.pdf

King, Sunny, 2013. Primecoin: Cryptocurrency with Prime Number Proof-of-Work. Available from: http://primecoin.io/bin/primecoin-paper.pdf

Kitchenham, B., Brereton, O., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature reviews in software engineering – A systematic. Information and Software Technology.

Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., And Ford, B. OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding. In Security and Privacy (SP), 2018 IEEE Symposium on (2018), Ieee, pp. 19–34.

Koller, M. (2011). Life Insurance Risk Management Essentials. Springer-Verlag Berlin Heidelberg.

Koshy, P., Koshy, D., McDaniel, P.: An analysis of anonymity in bitcoin using P2P network traffic. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 464–480. Springer, Heidelberg (2014).

Kroszner, R. (2004), Central counterparty clearing: History, innovation, and regulation. Federal Reserve Bank of Chicago.

Kursh, SR., Gold, NA., 2016. Adding Fintech and Blockchain to your curriculum. In Innovation Journal, Volume 8, Number 2, 2016.

Kuznets, S. (1940). Schumpeter's Business Cycles. In The American Economic Review (pp. 30(2), 257-271).

Leland, H., Pyle, D., 1977, Information Asymmetries, Financial Structure, and Financial intermediation. Journal of Finance 32: 371-387.

Leonard, J. (2015), Introduction to receivable securitization. The Secure Lender 2015 (June): 17-19.

li-Huumo, J., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology? PLoS ONE.

Lim IK, Kim YH, Lee JG, Lee JP, Nam-Gung H, Lee JK. The Analysis and Countermeasures on Security Breach of Bitcoin. In: Murgante B, Misra S, Rocha AC, Torre C, Rocha J, Falco M, et al., editors. Computational Science and Its Applications ICCSA 2014. vol. 8582 of Lecture Notes in Computer Science. Springer International Publishing; 2014. p. 720–732.

Litke, P., Stewart, J.: Cryptocurrency-stealing malware landscape (2014).

Locher T., Obermeier S., Pignolet Y., When Can a Distributed Ledger Replace a Trusted Third Party?, 2018. Available from: https://arxiv.org/abs/1806.10929.

Loeys, J. (2018). Decrypting Cryptocurrencies: Technology, Applications and Challenges. JPMorgan Chase & Co.

Luu L, Teutsch J, Kulkarni R, Saxena P. Demystifying Incentives in the Consensus Computer. In: Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security. CCS'15. New York, NY, USA: ACM; 2015. p. 706–719.

Luu L, Duc-Hiep Chu, Hrishi Olickel, Prateek Saxena, Aquinas Hobor, Making Smart Contracts Smarter, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, October 24-28, 2016, Vienna, Austria [doi>10.1145/2976749.2978309].

Mainelli (M.), M. Smith, 2015. Sharing Ledgers for Sharing Economies: An Exploration of Mutual Distributed Ledgers (a.k.a. Blockchain Technology). The Journal of Financial Perspectives, 3(3), 2015.

Mann C, Loebenberger D. Two-Factor Authentication for the Bitcoin Protocol. In: Foresti S, editor. Security and Trust Management. vol. 9331 of Lecture Notes in Computer Science. Springer International Publishing; 2015. p. 155–171.

Maxwell (2013a), G.: CoinJoin: Bitcoin privacy for the real world. Post on bitcointalk.org. https://bitcointalk.org/index.php?topic=279249.

Maxwell (2013b), G.: Really ultimate blockchain compression: CoinWitness. Post on bitcointalk.org. https://bitcointalk.org/index.php?topic=277389.

McPartland, J. W. (2009), Clearing and settlement of Exchange-Traded derivatives. Federal Reserve Bank of Chicago, Financial Markets Group.

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M., Savage, S.: A fistful of bitcoins: characterizing payments among men with no names. In: Proceedings of the 2013 Conference on Internet Measurement Conference, IMC 2013, pp. 127–140. ACM, New York (2013).

Meiklejohn S, Orlandi C. Privacy-Enhancing Overlays in Bitcoin. In: Brenner M, Christin N, Johnson B, Rohloff K, editors. Financial Cryptography and Data Security. vol. 8976 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2015. p. 127–141.

Memminger, M., Baxter, M., & Lin, E. (2016). Banking Regtechs to the Rescue? Bain & Company.

Meng-Jang Lin, Keith Marzullo, Directional Gossip: Gossip in a Wide Area Network, Proceedings of the Third European Dependable Computing Conference on Dependable Computing, p.364-379, September 15-17, 1999.

Miers, I., Garman, C., Green, M., Rubin, A.: Zerocoin: Anonymous distributed e-cash from bitcoin. In: 2013 IEEE Symposium on Security and Privacy (SP), pp. 397–411, May 2013.

Miller, A. (2007), Trade services - pooled payables securitization. Available from: http://www.gtreview.com/news/global/trade-services-pooled-payables-securitisation.

Mills Jr, David & Nesmith, Travis. (2008). Risk and Concentration in Payment and Securities Settlement Systems. Journal of Monetary Economics.

Mitnick B.M., 2006, The Origins of Agency Theory. Available from: http://www.pitt.edu/~mitnick/agencytheory/agencytheoryoriginrev11806r.htm.

Moser, J., 2017. The Application and Impact of the European General Data Protection Regulation on Blockchains. R3 public whitepapers.

Moser, M., Bohme, R., Breuker, D.: An inquiry into money laundering tools in the bitcoin ecosystem. In: eCrime Researchers Summit (eCRS), pp. 1–14, September 2013.

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

Nass, I., Wehninger, G., 2015. Unlocking SME finance through market-based debt: securitization, private placements and bonds. Financial Market Trends 2015 (2): 89-189.

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. Springer Fachmedien Wiesbaden.

Nolan T., Re: Altchains and atomic transfers, https://bitcointalk.org/index.php?topic=193281.msg2224949#msg2224949, 2013.

Oldfield G.S., Santomero A.M., (1997), The place of risk management in financial institutions, The Warthon School, available at: https://pdfs.semanticscholar.org/c288/33adcb4185ee67aa48877679053a142f1d86.pdf

Okoli, C. (2015). A guide to conducting a standalone systematic literature review. Communications of the Association for Information Systems.

Patel, N. (2017). Blockchain KYC/AML Utilities for international payments: A Regulatory Solution for Anti-Money Laundering and Financial Inclusion? r3.

Paul G, Sarkar P, Mukherjee S. Towards a More Democratic Mining in Bitcoins. In: Prakash A, Shyamasundar R, editors. Information Systems Security. vol. 8880 of Lecture Notes in Computer Science. Springer International Publishing; 2014. p. 185–203. Available from: http://dx.doi.org/10.1007/978-3319-13841-1_11.

Peck, M.E., 2017. Blockchain World - Do You Need a Blockchain? This Chart Will Tell You if the Technology Can Solve Your Problem. IEEE Spectrum 54 (10), 38–60 (2017).

Poelstra, A. Distributed Consensus from Proof of Stake is Impossible, in "Distributed Consensus", section 6, 2014.

Polimeno, V. (2009). L'analisi dei bisogni della clientela private. Professione Finanza.

Pongnumkul, Suporn, Chaiyaphum Siripanpornchana, and Suttipong Thajchayapong, Performance Analysis of Private Blockchain Platforms in Varying Workloads, 2017, IEEE.

Poon (J.) and T. Dryja. The bitcoin lightning network. https://lightning. network/lightning-network-paper.pdf, Nov 20, 2015.

Rejda. (2004). Principles of risk management and insurance. Pearson Education.

Resti, A. (2003). Il Private Banking. Bancaria Editrice.

Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework. Springer.

Rivest, R. L., A. Shamir, and Y. Tauman, "How to leak a secret," in Proc. 7th Int. Conf. Theory Appl. Cryptol. Inf. Secur. (ASIACRYPT'01), Dec. 2001, pp. 552–565.

Saha, A. (2016). Peer-to-Peer Insurance: back to basic. ResearchGate.

Sala G.A., Leardini C., Rossi G., Agnoli N., Zamboni M., Lo Presti D., Spiller C.N., Savi P., (2010), Fondazioni Bancarie Arte e Cultura: ruolo, risultati e prospettive alla luce di un'analisi territoriale, Franco Angeli, available at: https://www.francoangeli.it/Area_PDFDemo/365.833_demo.pdf.

Santomero A. 2001. "Deposit Insurance in the United States". Paper presented at the FITD Conference the Role of Deposit Insurance Within The Financial Safety Net. Rome (Italy), 2 July 2001.

Sathye, M., Nicoll, G., & Chadderton, P. (2017). Regulatory Focus on Competition and Innovation in Payments Services. Does Regulation Aimed at Encouraging Competition and Innovation Conflict with Requirements for KYC, AML, Etc.? Are the Two Sides Compatible? Swift Institute .

Saunders A., Cornett M.M. (2008), Financial Institutions Management: a risk management approach, Mc Graw-Hill, available at: http://www.bulentsenver.com/FIN5477/Financial_Institutions_Management_AntonySaunders_TextBook.pdf

Saxena A, Misra J, Dhar A. Increasing Anonymity in Bitcoin. In: Bhme R, Brenner M, Moore T, Smith M, editors. Financial Cryptography and Data Security. vol. 8438 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2014. p. 122–139.

Schaper, Torsten. (2007). Trends in European Cross-Border Securities Settlement - TARGET2-Securities and the Code of Conduct.. 50-65.

Schroeck, G. (2002). Risk management and value creation in financial institutions. John Wiley & Sons.

Schweizer, André & Lockl, Jannik & Fridgen, Gilbert & Rieger, Alexander & Urbach, Nils & Radszuwill, Sven, 2018. A Solution in Search of a Problem: A Method for the Development of Blockchain Use Cases, (2018). Available from: https://www.researchgate.net/publication/324603293_A_Solution_in_Search_of_a_Problem_A_Method_for_the_Development_of_Blockchain_Use_Cases.

SegWit, 2015. Sources available at these links:

https://prezi.com/lyghixkrguao/segregated-witness-and-deploying-it-for-bitcoin/;

https://github.com/bitcoin/bitcoin/blob/master/doc/release-notes/release-notes-0.13.1.md;

and for a naïve explanation: https://www.youtube.com/watch?v=DzBAG2Jp4bg.

Seifert, R., Seifert, D. (2009), Supply chain finance - what's is worth? IMD Perspectives for Managers 178.

Shavell, S., 1979, Risk sharing and incentives in the principal and agent relationship. Bell Journal of Economics 10: 55-73.

Siim, J., Proof-of-Stake, in Research Seminar on Cryptography, 2015.

Smart Contracts Alliance, 2018. Smart Contracts: Is the Law Ready? Available from: https://digitalchamber.org/smart-contracts-whitepaper/

Smith, Bryan, 2018. Three Ethereum forks you should know about. Available at: https://www.coininsider.com/three-ethereum-forks/

Sompolinsky Y., and A. Zohar. Secure high-rate transaction processing in bitcoin. In FC, 2015.

Song, Jimmy, 2017. Replay Attacks Explained. Available at: https://bitcointechtalk.com/replay-attacks-explained-e3d6d2ea0ab2

Spagnuolo, M., Maggi, F., Zanero, S.: BitIodine: extracting intelligence from the bitcoin network. In: Christin, N., Safavi-Naini, R. (eds.) FC 2014. LNCS, vol. 8437, pp. 452–463. Springer, Heidelberg (2014).

Stein, R.M., 2005, The relationship between default prediction and lending profits: integrating ROC analysis and loan pricing. Journal of Banking and Finance 29: 1213–1236.

Swan M. Blockchain: Blueprint for a New Economy. "O'Reilly Media, Inc."; 2015.

Swift. (2018). gpi real-time Nostro Proof of Concept: Can blockchain pave the way for real-time Nostro reconciliation and liquidity optimization?

Szabo, Nick, 1994. Smart Contracts. Available at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Templar, S., Hofmann, E., Findlay, C. (2016), Financing the end-to-end supply chain: a reference guide for supply chain finance. Kogan Page, London.

Thavanathan, J. (2017). Process innovation with Blockchain. Norwegian University of Science and Technology.

The Giovannini Group (2001), Cross-Border Clearing and Settlement Arrangements in the European Union.

Tschorsch, F., Scheuermann B., 2016. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. Published in: IEEE Communications Surveys & Tutorials (Volume: 18, Issue: 3, third quarter 2016): 2084-2123.

TUF, Decreto Legislativo1998: Testo Unico della Finanza (1998), Consob, versione consultata 2018, available at: http://www.consob.it/documents/46180/46181/dlgs58_1998.pdf/e15d5dd6-7914-4e9f-959f-2f3b88400f88

Valentini, P. (2018). In Italia le ricchezze delle private bank salgono del 4,9%. Tgcom24.

Vasek M, Thornton M, Moore T. Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem. In: Bhme R, Brenner M, Moore T, Smith M, editors. Financial Cryptography and Data Security. vol. 8438 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2014. p. 57–71.

Vasek M, Moore T. Theres No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. In: Bhme R, Okamoto T, editors. Financial

Cryptography and Data Security. vol. 8975 of Lecture Notes in Computer Science. Springer Berlin Heidelberg; 2015. p. 44–61.

Vaughan, E., & Vaughan, T. (2008). Foundamental of risk and insurance. John Wiley & Sons.

Vink, Dennis and Thibeault, André E., ABS, MBS and CDO Compared: An Empirical Analysis (September 9, 2008). The Journal of Structured Finance, Vol. 14, 2008, pp. 27-45. Available at SSRN: https://ssrn.com/abstract=1016854

Vom Brocke, J., Simons, A., Niehaves, B., Niehaves, B., & Reimer, K. (2009). Reconstructing the Giant: On the Importance of Rigour in Documenting. ECIS 2009 Proceedings, Paper 161.

Wang L, Liu Y. Exploring Miner Evolution in Bitcoin Network. In: Mirkovic J, Liu Y, editors. Passive and Active Measurement. vol. 8995 of Lecture Notes in Computer Science. Springer International Publishing; 2015. p. 290–302. Available from: http://dx.doi.org/10.1007/978-3-319-15509-8_22.

Weber, O., Fenchel, M., Scholz, R.W., 2008, Empirical Analysis of the Integration of Environmental Risks into the Credit Risk Management Process of European Banks. Business Strategy and the Environment 17: 149-159.

World Bank Group. (2016). Identification for Development. World Bank.

World Economic Forum, Blockchain Beyond the Hype - A Practical Framework for Business Leaders, 2018. Available from: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf.

Wüst, K., Gervais, A., 2017. "Do you need a blockchain?". Available at: http://eprint.iacr.org/2017/375.

Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016). Where Is Current Research on Blockchain Technology?A Systematic Review. PLoS ONE 11(10): e0163477. https://doi.org/10.1371/journal.pone.0163477.

Zakai, H. (2015), Platform power: eeny, meeny, miny, moe - with which provider shall I go? Available from: http://www.txfnews.com/News/Article/5238/Platform-power-Eeny-meeny-miny-moe-with-whichprovider-shall-I-go.

Zanaboni, B., & Oriani, M. (2008). Conoscere il private banking. Nuove tendenze, strumenti e soluzioni: organizzazione, relazioni con la clientela. Roma: Banca Editrice.

Zazzaro A., (2001), Specificità E modelli di governo delle banche: un'analisi degli assetti proprietari dei gruppi bancari italiani, Moneta e credito, pp. 487- 517, available at: https://ojs.uniroma1.it/index.php/monetaecredito/article/view/9963/9839.

Zepeda, R., 2013. The ISDA Master Agreement 2012: A Missed Opportunity? Journal of International Banking Law and Regulation: p.12-28.