POLITECNICO
DI TORINO

MASTER THESIS

Master's Degree in Engineering and Management

A.Y. 2019/2020

How technology is reshaping financial services: Blockchain use cases in the banking industry

STUDENT NAME: Francesco Damico

TUTOR'S NAME: Elisa Ughetto

Contents

1 Introduction to FinTech

Since the global crisis in 2008, the financial industry has seen an explosion of new entrants into the market. Technology-focused 'Fintech' firms have sought to disrupt the established order of financial services, changing the dominant operating models and competitive dynamics of an industry that, in the 50 years prior, had seen remarkably little change in market structure. This is why fintech is not a new industry, it is instead just one that has evolved very quickly.

Described in a very few words, *Fintech is the application of technology for financial services*. Even though this definition is the most used among users all over the world, it is not quite precise. Just talking about technology in finance is limited, it should also always come along with the term User experience, commonly named UX. Consider, for a while, the traditional banks. During the last 20 years they have developed and integrated a lot of technology in their solutions and they have made faster the services offered to their customers. However, this technology has remained tricky, not approachable and consequently not easy to use for banks' everyday clients. The result is that, de facto, they have not really brought innovation in the society.

There are essentially three main characteristics that make fintech companies unique: Accessibility, simplicity and transparency. The first refers exactly to the accessibility of customers to financial services beyond the regulatory wall of the banking system. The term accessibility refers both to reduction of bureaucracy for the clients to take advantage of their platforms and the real openness of financing for younger or smaller companies, which might not meet banks' eligibility requirements.

The second feature that is outlining fintech startups is the easiness brought about an innovating user experience, that merge both business and IT departments of these companies. By being involved in a platform – that most of the time is just a mobile app - a normal customer is able to exploit financial services as easily as listening music on Spotify or enjoy a movie on Netflix. Everything is becoming extremely minimalistic and intuitive.

The third characteristic is the transparency. The adopted pricing strategy for financial services (e.g. charge of a fee for a money transfer or a withdrawal) is tendentially more competitive than the one offered by traditional banks. Of course, this might be due to the hugely higher costs sustained by normal bank, such as, among the others, the personnel cost in a branch. Transparency refers also to the clearness with which alternative services are proposed to the customers, that are able to easily understand the price at which the service is offered, its description and the conditions under which it can be terminated. It might be obvious to clearly get these types of information when signing a contract with a company for a bank account, but it is not. Just think at the thousands of

documents you need to "read" and sign any time a banking relationship has to be set up: the price to be paid (e.g. for any transaction carried out) is not so clear. Part of the motivation for the emergence of fintech is that, while information technology has made everything – from computers to cars – cheaper and more functional, the unit cost of financial intermediation has apparently not changed much in over a century. It has been estimated[1] that the unit cost of financial intermediation in the US has remained at about 2% over the past 130 years. Thus, one promise of fintech is the unveiling of cheaper ways to overcome financial contracting frictions and lower the cost of financial services to improve consumer welfare. The areas that fintech covers can be broadly described as:

1. Credit, deposits, and capital-raising services;
2. Payments, clearing and settlement services, including digital currencies;
3. Investment management services (including trading);
4. Insurance.

Part of the technological backbone of fintech is the Blockchain technology. The use of this technology along with other technological advancement is intended to lower search costs of matching transacting parties, achieve economies of scale in gathering and using large data, achieve cheaper and more secure information transmission, finally to reduce verification costs. The discussion on the Distributed ledger technology will be approached in the following chapter.

In order to define the size of Fintech, one useful growth measure to use is venture capital (VC) investment in fintech companies. Data quoted in an International Organization of Securities Commissions' (IOSCO) report[2] indicate cumulative investments of over $100 billion in more than 8800 fintech companies as of November 2016. On an annual basis, global fintech investments increased at a steady pace between 2014 and 2017 from $19.9 billion to $39.4 billion. In the first half of 2018, the global fintech sector raised $41.7 billion, which surpassed the amount for all of 2017.

There are also many interesting stylized facts about fintech: using European data from the academic paper[3] of Thakor, Anjan V., the following correlation have been highlighted:

1. Investments in fintech companies are higher in more financially developed countries.
2. Use of electronic payments is higher in countries where a higher fraction of the population holds an account with a financial institution.

[1] **Philippon, Thomas. 2019.** *On Fintech and Financial Inclusion.* 2019. p. 3. E2, G2, N2.
[2] **International Organization of Securities Commissions. 2017.** *Research Report on Financial Technologies (Fintech).* 2017.
[3] **Thakor, Anjan V.** *Fintechandbanking:Whatdoweknow?* s.l. : Journal of Financial Intermediation. pp. 4-8.

3. Investments in fintech companies are higher in countries with less competitive (more concentrated) banking systems.
4. Investments in fintech companies are higher in countries with higher lending interest rates and lower deposit interest rates

Collectively, these stylized facts tell us that the opportunities for fintech seem to be greatest in the most financially developed countries in which larger percentages of the population are banked and where banking earns higher rents (due to lower interbank competition). This is intuitive. Banking rents tend to be high in countries in which banks are used a lot, which provide an inducement for fintech investments to get a share of the rents. However, there is still something missing in order to get an overall view of fintech industry. In fact, venture capital investments in this sector entail that fintech companies might be able to provide a reasonable high interest rate as return. The next paragraph aims to answer the question "How Valuable Is FinTech Innovation?"

1.1 The value of Fintech innovation

Despite the widespread interest in FinTech, little is currently known about how it will affect the value of these innovative companies and those of the investments carried out by venture capitalist and other investors. For the purpose of providing a large-scale evidence on the occurrence and value of Fintech innovation, in this paragraph is going to be analysed the study published by A.Chen and B.Yang of the Georgia State University, whom constructed a data set of published FinTech patent applications over the 2003–2017 period with the scope to analytically demonstrate the change in value that a Fintech company has had after the application of patents. These data came from the Bulk Data Storage System (BDSS) of the United States Patent and Trademark Office (USPTO) and includes both the full text of each patent filing and identified information on original patent assignees.

Since there is still not a shared definition of what really is the "Fintech", one of the key goals of the study was thus to develop an objective, data-based definition and classification of FinTech innovation. To this end, it was exploited the rich textual data in the sample of patent filing documents. The first step was to assemble a new lexicon of finance-related terms and use it to narrow down the set of patent filings to those relating to financial services. Then, several families of machine-learning algorithms were applied to the textual data to identify FinTech innovations and classify them into seven key specific categories. The result was that FinTech ultimately consists of the set of recently developed digital computing technologies that have been applied or that will

likely be applied in the future to financial services, and can be found mainly in seven categories: cybersecurity, mobile transactions, data analytics, blockchain, peer-to-peer (P2P), robo-advising, and IoT.

The following evidences coming from the data set were immediately highlighted:

i. Publicly traded companies as a group have driven only a minority of FinTech innovations. Indeed, private companies and individuals account for about 62.7% of FinTech filings in the sample. Of the FinTech filings from companies, about 57.8% are in fact from technology companies outside of the financial services industries;
ii. Among the seven FinTech categories, cybersecurity and mobile transactions have experienced the most total innovation over the sample period;
iii. Blockchain, that will be deeply analysed in the second chapter, is currently the smallest but fastest-growing category of FinTech innovation.

The valuation approach was based on observed stock market responses to USPTO disclosures of patent filings. Using this valuation approach, it is examining how much firms in the financial services sector stand to gain from their own FinTech innovations. The calculations show that a FinTech innovation's private value (i.e., the value accruing to the innovator) is typically large and positive. For instance, in 2017, the median private value of a FinTech innovation is about $46.7 million, which is much higher than the median private value of $3.1 million for other financial innovations. Overall, the FinTech innovation types that are most valuable to innovators are blockchain, cybersecurity, and robo-advising. processing, brokerage, asset management, and insurance. Calculations show that, for the financial sector as a whole, the typical FinTech innovation brings positive value. The value effects are driven by two key factors:

1. How inherently disruptive is the underlying technology;
2. Whether the innovator poses a competitive entry threat to the industry. Consistent with theories of disruptive innovation (e.g., Christensen 1997; Christensen and Raynor 2003; Downes and Nunes 2013), it was found that a FinTech innovation tends to destroy significantly more industry value when its underlying technology is disruptive and when it originates from a young, nonfinancial firm ("FinTech startups").

From the viewpoint of incumbent firms, theoretical considerations suggest that disruptive innovation by potential entrants can be especially harmful to industry's market leaders, which are sluggish in adapting to change and focused on existing customers (in case of fintech, these are mainly banks a large financial institutions). However, industry-wide disruption might be

advantageous to market leaders because, compared to rivals, they have larger scale economies and more financial resources with which to innovate new lines of business. The study supports the latter prediction and also suggest that market leaders' ability to avoid harm from disruptive outside innovation is strongly linked to the amount of resources that they devote to their own research and development (R&D).

In the concept of the study, it is important to note that not all the key technologies among the seven categories above mentioned are automatically qualified as being FinTech. Indeed, technologies are partly defined by their intended use. For being included in the study, it is required that the actual (or intended) main use case of a technology lies within the field of financial services in order for the technology to be considered FinTech. Thus, a new blockchain designed for supply-chain management or a new machine-learning algorithm for predicting weather patterns would not be considered FinTech since the primary intended applications of these innovations do not fall within the domain of financial services.

To construct a sample for the study, BDSS was firstly used to obtain information on the 4,680,587 total patent applications published by the USPTO between January 1, 2003 and September 7, 2017. Of these, 2,243,484 patent applications are identified in BDSS as having been filed by public firms, private firms, and individuals located in the United States. Then, International Patent Classification (IPC) codes were gathered, associated with each patent application and then restrict the sample to applications belonging to either IPC Class G or IPC Class H. The union of these very broad patent classes ("Class G&H") covers the areas that are potentially related to digital computing, which is a technology that underlies all FinTech categories as discussed previously. With this restriction, it was obtained a sample of 1,181,162 Class G&H patents filed by U.S. companies and individuals. The first step was filtering this huge number of patents by exploiting supervised machine-learning methods to classify patent filings based on their textual data. To build the list of filtering terms, two publicly available glossaries were used: Campbell R. Harvey's Hypertextual Finance Glossary and the Oxford Dictionary of Finance and Banking, 5th Edition, published by Oxford University Press, for a total of 11,196 filtering terms. In addition, words that have recently gained recognition as financial terms, such as "bitcoin," "cryptocurrency," and "crowdfunding" have been added. The final list had a total of 487 unique finance-related terms. The next step was to apply the filtering list to the sample of all Class G&H patents filed by U.S. companies and individuals. Specifically, we retain patent filings that meet two requirements:

i. At least one filtering term appears in the title, abstract, summary, or claims sections of the filing;
ii. Different filtering term appears anywhere in the filing document.

Using this filtering strategy, it was obtained a total of 67,948 patent filings that were potentially related to financial services.

The literature on corporate innovation has recognized that stock price reactions can be used to study the value of new patents. What is less well appreciated, however, is that the price response to a patent event reflects a surprise component: market investors may anticipate an event's future arrival and partially incorporate this anticipation into a firm's stock price today. Thus, without correcting for rational anticipation, the abnormal stock-price reaction to a patent event will give a biased estimate of the intrinsic value of the innovation. The market may anticipate not just one future innovation during a given time period, but possibly two, three, four, or more. The following step was to outline a method for recovering the underlying value of a FinTech innovation in the presence of anticipation of multiple innovation events. The method is sufficiently general that it can be used with different models of patent count data (Poisson, negative binomial, zero-inflated Poisson, etc). However, for simplicity, the study focuses on the well-known Poisson count distribution used by Hausman, Hall, and Griliches (1984) and others in studies of patenting activity[4].

Let V_0 be the intrinsic value of a firm without a patent event and let V^* be the incremental value of one patent event to the firm. Assume the number of patents, N, that will occur during the time interval $[t, t+T]$ follows a Poisson count distribution:

$$\Pr(N=m|I_t)=\frac{\lambda^m e^{-\lambda}}{m!}, \quad m=0,1,\ldots$$

where I_t is the information set of market participants at time t. Let the incremental time $t+T$ value to the firm be mV^* if exactly m patent events occur. Then the ex-ante market value of the firm before any patent event occurs is:

$$\bar{V}_0=V_0+\sum_{m=1}^{\infty}\frac{\lambda^m e^{-\lambda}}{m!}\left(mV^*\right)=V_0+\lambda V^*$$

[4] **Jerry A. Hausman, Bronwyn H. Hall, Zvi Griliches. 1984.** *Econometric Models for Count Data with an Application to the Patents-R&D Relationship.* 1984. p. 6.

Assuming that the patent events are independent, then the occurrence of one patent event yields a conditional distribution over total end-of-period patents that is effectively a Zero-Truncated Poisson distribution:

$$\Pr(N=m|N\geq 1,I_t)=\frac{\lambda^m e^{-\lambda}}{(1-e^{-\lambda})m!},\quad m=1,2,\ldots$$

Therefore, the ex post market value of the firm after one patent event occurs is equal to

$$\begin{aligned}\bar{V}_1 &= V_0+\sum_{m=1}^{\infty}\Pr(N=m|N\geq 1,I_t)mV^* \\ &= V_0+\sum_{m=1}^{\infty}\frac{\lambda^m e^{-\lambda}}{(1-e^{-\lambda})m!}mV^* \\ &= V_0+\frac{\lambda}{1-e^{-\lambda}}V^*\end{aligned}$$

From the equations above, it follows that the incremental value of a patent is given by

$$V^*=\frac{\Delta\overline{V}}{\frac{\lambda}{1-e^{-\lambda}}-\lambda}=\frac{e^{\lambda}-1}{\lambda}\Delta\overline{V},$$

where $\Delta\bar{V}=\overline{V_0}-\overline{V_1}$ is the observed change to the market value of the firm upon occurrence of the patent event. The last equation gives a straightforward method of calculating the incremental value of a patent, V^*, from observational data. In particular, the observed market value change $\Delta\bar{V}$ can be computed from abnormal stock price reactions, and the Poisson intensity parameter λ can be estimated from an empirical model of patent counts like in Hausman, Hall, and Griliches[5]. To construct time-varying estimates of the intensity parameter λ in the above model, it was fitted a series of Poisson regressions using innovator-year panel data on patent filing counts. In the case of public firms, for a given technology category *k* was estimated the following regression using maximum likelihood estimation (MLE):

[5] **Jerry A. Hausman, Bronwyn H. Hall, Zvi Griliches. 1984.** *Econometric Models for Count Data with an Application to the Patents-R&D Relationship.* 1984. p. 8-9

$$\log(\lambda_{i,k,t}) = \alpha + \beta_1 Size_{i,t} + \beta_2 RD_{i,t} + \beta_3 RD_{i,t-1} + \beta_4 RD_{i,t-2} + \beta_5 RD_{i,t-3} + \beta_6 Age_{i,t} + \beta_7 PriorFinTech_{i,t} + \beta_8 PriorOtherFinancial_{i,t} + \beta_8 PriorNonFinancial_{i,t} + \gamma_i + \delta_t + \varepsilon_{i,k,t}$$

where *i* and *t* are indices for the innovating firm and year, respectively. In the regression, $Size_{i,t}$ is total assets (in 2003 dollars); $RD_{i,t-n}$ is R&D expenditures n+1 years prior to the current year (in 2003 dollars); *Age* is the number of years since founding of the company; $PriorFinTech_{it}$, is the company's stock of FinTech applications before year t; $PriorOtherFinancial_{i,t}$ is the company's stock of non-FinTech financial applications before year t ; $PriorNonFinancial_{i,t}$ is the company's stock of nonfinancial filings in Class G&H before year t; and γ_i and δ_t capture innovator and year fixed effects, respectively. All nonindicator variables are in a natural log form.

	Cybersecurity (1)	Mobile trans. (2)	Data analytics (3)	Blockchain (4)	P2P (5)	Robo-advising (6)	IoT (7)	Other financial (8)
Total assets	0.943***	0.907***	−1.277**	−35.903*	−0.355	2.017**	1.410	0.776***
	(0.193)	(0.349)	(0.541)	(20.399)	(0.486)	(0.827)	(0.887)	(0.066)
R&D	0.073	1.753***	−0.172	59.590**	1.988	4.745	−2.000	−0.042
	(0.304)	(0.557)	(1.720)	(29.945)	(1.362)	(3.061)	(1.724)	(0.140)
R&D_1	0.048	−0.673	1.908	34.657**	3.738	−3.871	2.863	−0.094
	(0.300)	(0.660)	(2.245)	(16.662)	(2.336)	(3.456)	(2.490)	(0.204)
R&D_2	−0.236	0.364	0.287	−22.221**	−7.361***	−0.350	−5.094	−0.091
	(0.288)	(0.662)	(2.050)	(10.288)	(2.344)	(2.692)	(6.064)	(0.228)
R&D_3	−0.273	−0.935*	−1.241	29.204**	2.111*	0.407	6.846	0.047
	(0.248)	(0.514)	(1.443)	(14.246)	(1.129)	(1.565)	(5.348)	(0.168)
Age	−0.201	−0.093	−3.693**	37.648	−0.295	−5.210*	−12.298***	−1.194***
	(0.591)	(1.329)	(1.514)	(139.437)	(2.107)	(2.658)	(2.827)	(0.250)
Prior applications (FinTech)	0.111	−0.092*	0.244	−5.566	−1.126***	−0.447	0.541*	0.300***
	(0.110)	(0.174)	(0.309)	(3.711)	(0.339)	(0.430)	(0.279)	(0.040)
Prior applications (other financial)	0.253**	0.197	0.358	27.971**	1.243***	0.405	0.378	0.018
	(0.101)	(0.176)	(0.278)	(12.487)	(0.305)	(0.513)	(0.278)	(0.038)
Prior applications (nonfinancial)	0.123*	0.035	−0.332*	−22.240*	0.010	0.010	−0.972***	0.172***
	(0.069)	(0.135)	(0.201)	(12.153)	(0.200)	(0.333)	(0.242)	(0.034)
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Observations	1,757	1,757	1,757	1,757	1,757	1,757	1,757	2,852

Figure 1 Poisson count models of FinTech and financial innovation for public firms (source: How Valuable Is FinTech Innovation?- Georgia State University)

The last step was to examine how much value is analytically created for filling companies. Taking as an example publicly traded financial companies, the following strategy was aimed to calculate how much value they obtain from their own FinTech patent filings. To infer these "private values," it was combined the Poisson intensities estimated above with cumulative market- adjusted abnormal returns (named CARs) around news of patent filings. Specifically, for an innovation of technology

$$V_{i,k,t}^{*,Own} = \frac{e^{\hat{\lambda}_{i,k,t}} - 1}{\hat{\lambda}_{i,k,t} \times n_{i,t}} CAR_{i,t} M_{i,t},$$

type *k* filed by company *i* and published on date *t*, the empirical analogue of equation of V^* yields an estimate of the innovation's value to the company:

where $\lambda_{i,k,t}$ is the predicted firm-level innovation intensity from the Poisson regressions previously estimated; $n_{i,t}$ is the number of filings by company i that are published on date t; $CAR_{i,t}$ is calculated over a 4-day window starting 2 trading days before the publication date t; and $M_{i,t}$ is the firm's market capitalization 5 trading days prior to date t. Innovation values estimated the equation above are converted into 2003 U.S. dollar values.

The table down below reports summary statistics for private values of innovation within nine different groups: the seven distinct FinTech categories, the set of all FinTech innovations, and the set of non-FinTech financial innovations. The table also reports mean CARs for each of the nine groups. As seen in the table, FinTech innovations create economically sizeable private value: the average value to the innovator is $19.7 million, and the median value is $35 million. By comparison, non-FinTech financial innovations yield a much lower median value of $2.3 million, although the average value is close to that of FinTech innovations. Across innovation categories, the mean CARs are mostly positive. The mean and median private values for some categories have opposite signs, suggesting a high degree of skewness in the distributions. Nevertheless, the median values are almost all positive, with the sole exception being data analytics. The largest median values are in blockchain ($98.1 million), cybersecurity ($52.9 million), and robo-advising ($49.1 million).

		Mean	Value				
Innovation type	*N*	CAR (%)	Mean	Median	SD	p10	p90
Cybersecurity	643	0.26	57.7 (0.410)	52.9 (0.004)	1,658.4	−819.8	902.6
Mobile transactions	271	0.42	43.1 (0.456)	18.9 (0.092)	1,013.8	−607.7	707.9
Data analytics	181	−0.31	−98.1 (0.492)	−45.3 (0.166)	1,803.8	−715.2	663.4
Blockchain	42	0.24	−105.9 (0.544)	98.1 (<0.001)	975.2	−653.8	264.5
P2P	95	−0.33	−30.1 (0.772)	1.2 (0.874)	884.0	−668.6	744.6
Robo-advising	54	0.04	93.5 (0.322)	49.1 (0.278)	791.9	−1,142.3	1,096.6
IoT	86	0.30	−20.8 (0.916)	32.2 (0.096)	973.4	−397.1	540.9
All FinTech	1,372	0.17	19.7 (0.592)	35.0 (<0.001)	1,439.9	−668.6	734.1
Other financial	2,719	0.20	20.7 (0.676)	2.3 (0.588)	3,141.0	−1,081.0	1,206.5

Figure 2 The private value of FinTech innovation (source: How Valuable Is FinTech Innovation? - Georgia State University)

After evaluating how the value of fintech can be found out in analytical terms, the obvious question to raise is: why is the fintech revolution happening now? The current environment of fast change has three main pillars: a changing macroeconomic and regulatory environment, the rapid evolution of technology, and shifting customer expectations.

1.2 Changing Economic and Regulatory Landscape

The financial crisis raised a lot of doubts about the safety and transparency of the whole industry so that regulators sought to improve the reliability of the system. The consequence was the introduction of a regulatory burden on financial institutions that led them to include, mandatorily, risk management team and compliance initiatives that caused product and process innovation to be slower and less flexible. As a result, finance has become the heaviest regulated industry. In the same time, a number of regulators have tried to encourage the raise of a renew competition such as the Financial Conduct Authority in the United Kingdom. The FCA works alongside the Prudential Regulatory Authority (PRA) in regulating the financial services industry in the UK. Whereas the PRA is mainly responsible for the prudential regulation and supervision of banks, building societies, credit unions, insurers and major investment firms, the FCA is responsible for the regulation of those financial services firms not supervised by the PRA such as asset managers and independent financial advisers. The FCA's overall objective has been to make the financial systems

to be sound, stable and resilient, with clear pricing information that consumers can easily understand. To support this primary objective, the FCA has three operational purposes: to secure an appropriate degree of protection for consumers, to protect and enhance the integrity of the UK financial system and to promote effective competition in the interests of consumers. From a macroeconomic point of view, the dramatic decrease of interest rates in the years following the financial crisis created a low-yield environment that significantly increased the flow of funds into alternative asset classes like venture capital. These flows helped increase the availability of funding for a wide range of new innovators including fintech entrepreneurs and revolutionary startups, that have never managed nurture their ideas in the industry since barrier to entry in the banking system were too difficult to cross upon.

1.3 A fast pace technology environment

At the same time, rapid technological advancements have created a fertile environment for alternative approaches to a range of financial activities, from onboarding and retain bank customers to allow bank transfers in just a few seconds. Large financial institutions were among some of the earliest private sector entities to make significant investments in information technology, that technology remains at the core of their business, most large institutions have acquired significant legacy technical debt. This means these institutions are deeply invested in inflexible systems that are often 40 or more years old. Migration away from these systems would be extremely challenging and costly for these institutions, and following the financial crisis, investments of this sort bordered on impossible.

These legacy systems made it difficult for financial institutions to keep pace with some of the exciting new opportunities presented by the rapid evolution of technology. While some financial institutions recognized the potential of engaging with customers via new platforms like smartphones, leveraging cloud computing, or even exploring new trading strategies enabled by artificial intelligence (AI), actual implementation was extremely difficult within an operating model constrained by 40-year-old mainframe systems.

1.4 Change of customer expectations

Another fundamental element to take in consideration is the shift of customer expectations brought about technology companies dealing in other industries. The main examples could be observed from Uber, Airbnb and WeChat. These companies conditioned consumers to expect digital services to be timely, customized, reliable and always ready to use. When compared to these offerings, a growing number of people began to see financial services as outdated and resistant to

change, since today managing personal finance is not as instantaneous as get a ride on Uber, booking a room on the other side of the world with Airbnb or paying your home bills through WeChat. A study conducted by Scratch over 10,000 Millennials reveals that 53% don't think their bank offers anything different than other banks and about 1 in 3 are open to switching banks in the next 90 days[6]. This environment, together with the fall of reliability following the financial crisis in 2009, have driven customers to looking for alternatives, hopefully with new fintech offerings.

The combination of the three elements just described has led banks, insurers, asset managers and other incumbent financial institutions to re-evaluate the competitive threats they face. It has also forced them to begin reimagining the ways in which technology could aid them in delivering value to their customers.

1.5 Fintech and Digital payments

Until a few years ago, the digital payments market had been one of the pillars of technological innovation driven by traditional financial institutions. Then, as discussed in the previous paragraph, tech companies entered a tense leg in the sector so as to deform it in a very little time, a true disruptive innovation that made lever on a single clear element: the customer experience together with the UX and UI (user experience and user interface, respectively)

The growing diffusion of these digital payment methods are making the use of cash less and less frequent in both developed and emerging economies. As pointed out from the World Payment Report 2019 (carried out by Capgemini), global non-cash transaction volume grew at 12% during 2016-17 to reach 539 billion US dollars – the highest amount in the past two decades. In advanced economies, this is the continuation of a long-standing trend of digitization where accepting digital payments has become both easier and less expensive for merchants increasing the variety of sellers who accept noncash payments and decreasing the minimum ticket size they require for customers to use these payment methods.

The major drivers of this impactful trend include growing adoption of mobile payments, diffusion of the contactless technology, and digital innovation from both technology players and incumbent financial institutions. Over the years, it is quite clear that FinTechs have been enabling banks to enhance their capabilities and to always looking for digital and process innovation. Moreover, they are also modifying their business models to emerge as direct competitors or even partners, depending on the target and the context. Amid the competitive business model arisen and

---

[6] "The Millennial Disruption Index" *Viacom Media Networks,* 2013, https://www.bbva.com/wp-content/uploads/2015/08/millenials.pdf.

adopted from these new entrants, one of the biggest threats is the segment-focused value propositions: means that the services are mainly addressed to specific portion of the market and the effects makes the fintech company very close to the customer. An example to consider could be Adyen, a global payment company founded in 2006 and headquartered in Amsterdam that helps businesses and merchants to accept e-commerce, mobile and point-of-sale payments. These payment methods include international credit cards, local cash-based methods and offers also risk management and local acquiring.

As a consequence of incoming new competitors, several Big techs, such as Apple and Alipay (powered by Alibaba, the biggest e-commerce company founded in China by Jack Ma) have started collaborating with established financial institution to leverage the existing infrastructure and capitalize on their customer base.

Among the others, Alipay is collaborating with Finland's ePassi, the first and most popular mobile payment method for all the kind of employees' benefits in the Nordic countries. Other partnerships have been established with Norway-based Vipps, Spain's MOMO, Portugal's Pagaqui, and Austria's Bluecode, with the purpose to adopt a unified QR code in order to uniform the region's fragmented mobile payment landscape. All the six digital wallets have five million users combined and around 190,000 merchants in their payment networks in Europe.

On the other hand, Apple has settled a cooperation with Mastercard and Goldman Sachs to launch into the market the Apple Pay, which is characterized by no transaction fees, lower interest rates and advanced security for the customers.[7] The list of Bigtech becoming partners of incumbents in the financial industry does not stop here: Microsoft partnered with Yes Bank and Mobikwik in India to enable P2P payments over its Kaizala mobile chat-based platform, Amazon took a partnership with JP Morgan, Bank of America in the US, Bank of Baroda in India, and Western Union to offer a variety of services, such as checking accounts, SME lending support, and payment transfers; Google Pay has extended its partnership with 15 more banks across Asia, Europe, and Australia; WeChat (another huge Chinese tech company) partnered with BNP Paribas and Wirecard in Europe and is facing expansion into the United States as well.

[7] Apple press release, "Introducing Apple Card, a new kind of credit card created by Apple", March 25, 2019, https://www.apple.com/newsroom/2019/03/introducing-apple-card-a-new-kind-of-credit-card-created-by-apple/

As a result, with digital payments acceptance and volumes growing rapidly, it is no surprise that payments are a big business. According with an analysis carried out by McKinsey in 2017, global revenues from payments were US$ 1.9 trillion[8], and is expected that payments is going to become a $2 trillion business by 2020. Figure 3 shows the percentage increase, year by year, of the global

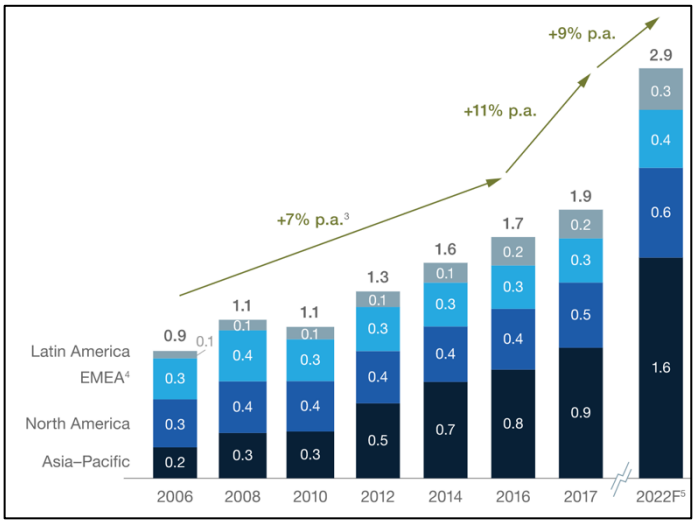

Figure 3 Global payment revenue in trillion of US$ (Source: McKingsey)

payment revenue for the four different continents.

But while new technologies have driven increased payment volumes, they have also led to increased levels of competition for payment revenues. When combined with increased regulation of payment transaction fees, this has placed significant pressure on margins for providers of payment facilitation services.

In order to discuss in detail the technologies that are restructuring the banking and payment industries, in the next paragraph will be introduced the blockchain technology, which is likely the most innovative disruption brought from fintech companies.

[8] "Global Payments: Expansive Growth, Targeted Opportunities," accessed January 5, 2019, https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-expansive-growth- targeted-opportunities.

2 Blockchain in Finance

Among the enormous amount of different technologies that are reshaping the financial services, blockchain is by far the most popular. It has received a significant amount of analyst and press attention over the last few years as this emerging technology holds significant potential. Use cases are many and varied: ranging from programmable to voting records. Cryptocurrencies were the first application of this technology, and in doing so introduced an entirely new set of businesses, jobs and vocabulary to the world of digital payments.

In order to understand the significant interest around crypto assets and the claim that it holds the potential to transform the financial system, it is needed to first opportunely understand the technology that enables these assets to function. The study of cryptocurrencies entails the analysis of bitcoin, which is by far the most visible and larger asset in terms of capitalization. Bitcoin is also where the innovative underlying technology of the blockchain was first introduced and developed, acting also as a source code for other assets that are exploiting its infrastructure through a process of replication and variation. Indeed, the majority of cryptocurrencies are largely clones of bitcoin or simply feature different parameter values (e.g. different block time, currency supply, and issuance scheme).

Differently from what has been described in the previous chapter about the fintech and digital payments as an alternative to money transfers, blockchain and the currencies which are based on it cannot be consider money, properly. Cryptocurrencies are legally defined, by the US Financial Crimes Enforcement Network directive issued early in 2013, as “convertible digital currencies” or alternatively as a “digital equivalent of cash” (according to the European legislation EC/2009/110 on electronic money). Even though these two legal definitions can be adopted to those crypto assets that are directly convertible to official currencies employing digital marketplaces (that will be discussed in the next paragraphs), digital cash cannot still be considered money. In order for an asset or a payment vehicle to be named as money, it has to be the universal means of exchange and standard of value at least in the geographic area of a state or the economic area of a market; neither is the case for any of the cryptocurrency in circulation[9].

The term blockchain is usually explained by using the example of a distributed ledge. A distributed ledger is a database that is consensually shared and synchronized across multiple sites, institutions or geographies. It allows transactions to have public "witnesses," thereby making a cyberattack more difficult. The participant at each node of the network can access the recordings shared across that network and can own an identical copy of it.

[9] **Papadopoulos, Georgios. 2015.** *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments.* [ed.] Erasmus University Rotterdam. Rotterdam : s.n., 2015. pp. 154-156.

In effect, traditionally a transaction process is supported by central operators, who record the movement of data in a ledger and maintain a consistent view on the property rights of the different users involved. Each intermediary therefore stores and manage every single transaction of data. The process is mainly based on the reputation of the central institution and participants consider it an adequate subject to manage the operations. For this reason, it is customary to indicate reliable intermediaries such as governments, banks, insurance companies, and notaries with the title of Trusted Third Party (TTP).

However, the direct control exercised by the institution exposes users to the following main risk: by keeping the register centrally, the intermediary constitutes a Single Point of Failure (SPOF), potentially exposed to the partial or total loss of the information kept. With the adoption of a blockchain system, there is anymore the need for a TTP for the management of an exchange process. The figure 4 shows a graphical difference between a distributed technology (peer-to-peer system) and a standard centralized system (client-server based), where a single actor is in charge of managing and validating every occurring transaction.

As it might be captured by the name 'Blockchain', the transaction data are stored in blocks

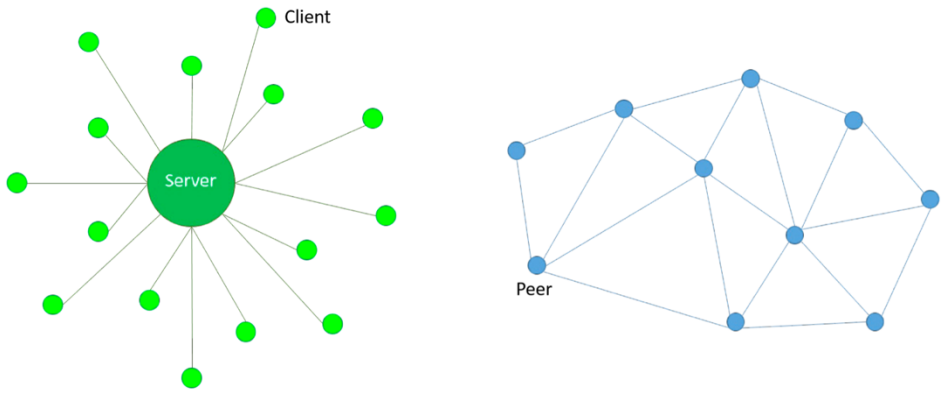

Figure 4 The comparison between a server-client based system (on the left) and a peer-to-peer system (on the right) (Source: Blackport)

(block-) closely linked together (-chain), to complete and define a ledger, distributed in numerous copies among the nodes of the network. The concept of node refers to any subject connected to the network by means of a dedicated communication device (e.g. modem).

The information is thus replicated on a high number of independent subjects (Figure 5), or peers, and the consistency of the data is guaranteed through a consent algorithm. Thanks to these technological properties, participants can cooperate in a trust less way: the security of the system is not entrusted to a central body that is considered reliable, but it is instead established by the goodness of the protocol (algorithm) used by the participants.

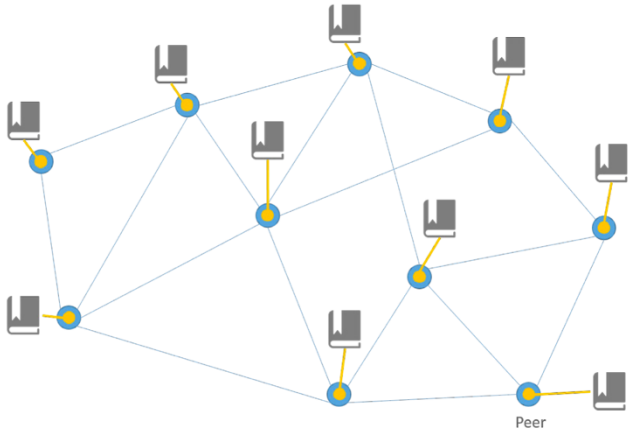

Figure 5 Ledger distribution: each node (peer) is able to check and keep a copy of the file (Source: Reply)

A blockchain system, implemented effectively and supported by a sufficiently distributed network, may bring numerous advantages. Among them:

1. None of the participants has the power to act opportunistically with respect to the rest of the network;
2. There is no possibility of censorship and exclusion;
3. The register is not kept by a single body but replicated in many copies. It is updated and kept consistent by the computers on the network. As a result, it is practically impossible to record information leaks.

In particular, the validation of a transaction and its subsequent inclusion in the blockchain are operations carried out by the network nodes themselves, which thanks to an advanced consensus algorithm, maintain a common vision on the status of the register. At the same time, the use of state-of-the-art cryptographic tools allows to verify the validity of each individual transaction. The blockchain therefore represents a public and reliable data source thanks of its technological properties.

Another feature that differentiates a blockchain system from a centralized system is the programmability of transactions. Generally, a blockchain system integrates as a mean of exchange a cryptocurrency, i.e. a digital token transferred on the basis of a cryptographic evidence. The ability to include personalized information in payment messages enriches the cryptocurrency of new

properties: tokens become means of digitally representing other types of assets, from fiat currencies and financial securities to physical assets such as real estate or vehicles.

The fundamental characteristics of the blockchain, together with the relative strengths highlighted in the previous paragraph, have allowed an increasingly widespread diffusion of this technology, a phenomenon particularly evident during 2015. The diffusion was driven by the FinTech sector, which immediately captured the great potential and applicability of the model in different areas. In fact, there are numerous initiatives on the blockchain world by financial institutions, which typically are activated in four main ways:

- **Internal development:** establishment of research laboratories or working groups for the testing of proprietary blockchain solutions.
- **Venture Capitalist (VC)**: investment in startups active in the blockchain world both through VC operations and directly.
- **Partnerships:** launch of partnerships with reference companies in the blockchain sector, so as to accelerate the acquisition of know-how and launch exploratory projects on technology.
- **Consortium:** joining a consortium of financial players (eg R3 CEV) or cross-industry (Hyperledger Project) with the aim of defining de facto standards that can be interoperable with all the other members. It is particularly interesting the case of the american startup R3 CEV at the head of a consortium named Distribution Ledger Group which in December 2015 had 42 among the world's largest financial institutions, united by the study of protocols and standards for the use of blockchain in financial services. The R3 CEV consortium is based on the idea of being able to carry out blockchain projects regulated by common standards, gathering the contributions and opinions of the member institutions. In April 2016, the R3 company had already implemented at least eight different Proof-of-Concept (PoC) projects to show how a blockchain registry, in this private case, can support a wide range of processes and facilitate operations. The areas explored by the PoCs are mainly focused on Digital payments, Trade finance, Corporate bond, Repurchase agreement and assurance product.

2.1 A brief description of the underlying technology

The elements that allow the operation of a blockchain system are described here in a simplified way. In particular, the basic technological principles can be grouped in the following areas, briefly explained in the following paragraphs:

- **Network nodes:** the roles of the participants in the network and how they interact with each other.

- **Encryption underlying transactions:** the tools that allow you to certify each exchange. Cryptography is at the core of DLT, in particular for blockchain implementations. Each new data entry, i.e. a transaction record, is "hashed", which means that a cryptographic hash function is applied to the original message. A hash takes data of any size input and computes a digital fingerprint similar to a human fingerprint that cannot be changed unless the data itself is changed. The hash output is a so-called 'digest' of a defined length which looks random and unrelated to the original input but is in fact deterministic. This means that for one original input only one hash is possible, and it is highly improbable for another input to have the same hash value.7 Hashing also applies a time stamp to the original message. These transaction hashes are collated into a 'transaction block' that can contain any number of transactions but typically has a limited total size.8 The hash enables detection of any tampering of the underlying transaction data, as when a hash is computed again, it will produce a different hash than the originally generated hash
- **Trust between nodes:** the main methods used to bring participants together in the final version of the register.

2.1.1 The nodes of the network

A blockchain system differs from a centralized system primarily by its particular network configuration. While in a trusted scenario the members of the network all depend on a trusted intermediary with a client/server logic, in a distributed context the serving operator is replaced by an infrastructure of independent peers linked by an equal communication logic (peer-to-peer). The interdependence between the nodes is enabled by the ability of each participant to cover multiple roles simultaneously: since each subject act both as a client and as a server, no node is central to the others and the effort for the provision of network services is shared. This concept is applied to the main nodes of the network, which constitute a first level of participants in the network. The actors of this level are called "*full nodes*" because they keep a complete copy of the blockchain registry locally. By adopting a broader view of the system, it is also necessary to take into consideration the subjects who interact with the network without keeping a copy of the ledger.

Generally, saving a copy of the blockchain registry on your device requires a very large storage space, often not available on portable devices such as smartphones. Extending the network model is therefore necessary to include all types of network participants. As shown in figure 6, the nodes that do not store a copy of the ledger, also called *"light nodes",* constitute a second hierarchical level in the network, which relates to the first level nodes with a client/server communication logic.

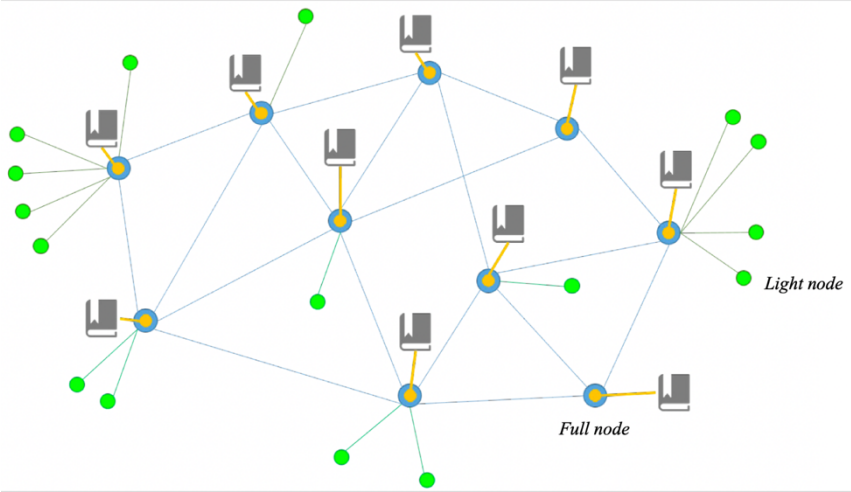

Figure 6 A graphical view of Full nodes and Light nodes inside a network (Source: Reply)

The result is a "distributed" system, intermediate between a decentralized and a centralized system. Moreover, each node, regardless of its level, can play one of these two roles within the blockchain network:

- **Wallet node:** this role involves the management of a set of addresses that identify the node inside the network, together with the sending and receiving of transactions with respect to other users.
- **Miner node:** this category is, unlike the previous one, fundamental for the functioning of the system. The role of miner in fact provides for direct participation in the consent algorithm, with the execution of verification and confirmation of transactions sent by the users. The term miner is inherited from the Bitcoin protocol and has entered common use to indicate participation in the writing of the register. In fact, to update the status of the blockchain, Bitcoin uses a computational work that is rewarded with the distribution of new cryptocurrency: it is as if the participants "mines" the bitcoins with their computing power, just as a miner gets some gold through a work of extraction (mining).

2.1.2 The cryptography underlying the transactions

The members of the P2P network actually constitute an economic system, where each member takes part of a group of subjects authorized to carry out internal transactions. In a blockchain system, the methods of issue and transfer are regulated by the particular protocol adopted (e.g. Bitcoin, Ethereum, etc.). Exchanges are certified thanks to the application of a digital signature on the single transaction: this guarantees the authentication of the sender, the impossibility of rejection and the integrity of communication on the basis of cryptographic evidence. The technology involves the use of a key that can be publicly disclosed *"public key"* and a "*private key"* kept secret by its owner. In the Bitcoin protocol, for instance, each key is created through the ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm, a generation process that, starting from a private key of a predetermined length, produces a public counterpart in a deterministic way. If it is quick and easy to repeat this generation operation, it is impractical on a computational level to reverse the process and go back to the generating private key.

The blocks are so signed with a digital signature, which binds the sender to the contents of the block. The distributed ledger technology (DLT) uses 'public key cryptography' for digital signatures, which is a common method that is used in a wide array of other applications, such as HTTPS internet protocol, for authentication in critical applications and also in chip-based payment cards. Digital signatures are widely accepted as equivalent to physical signatures by law in many countries. As introduced previously, each network participants have a private key, which is used for signing digital messages and only known by the individual user, and a public key which is public knowledge and is used for validating the identity of the sender of a digital message. The public key is also used to identify the recipient. These concepts help explain the fundamentals of DLT. The process by which data is recorded in a blockchain-based distributed ledger is by forming an append-only chain of 'transaction blocks' in chronological order that contains hash digests of the transactions (digital messages) to be added to the ledger, a proof-of-work (or a different consensus mechanism output), and a digital signature of the hash by the sender's private key, and public keys of the sender and the intended recipient of the transaction. This chain starts with the first-ever entry in the ledger (the 'genesis block') and each appended block contains hashed information of the previous block, setting the chronological order of the chain. Each block contains a unique "proof-of-work" protocol, a reference to the previous block that determines the correct chronological

ordering of blocks, a series of hashed digests of transaction information which cannot be changed, and a digital signature. The blockchain structure[10] is shown in figure 7.

Once a new block is added to the chain via a specified consensus mechanism, the chain cannot retroactively be changed, and blocks cannot be deleted or amended without redoing the proof-of-work protocol for each block. This means that as the chain grows in length, this becomes progressively more difficult because all nodes are constantly competing for solving proof-of work puzzles and adding new blocks to the chain. In doing this they only consider the transaction blockchain that reflects the greatest amount of computational work. Each successful addition to the chain is broadcast to the entire network and all nodes have an up-to-date copy of the entire blockchain.

Thanks to the adoption of a digital signature system, each subject is able to:

- Become identifiable on the P2P network through a unique address;

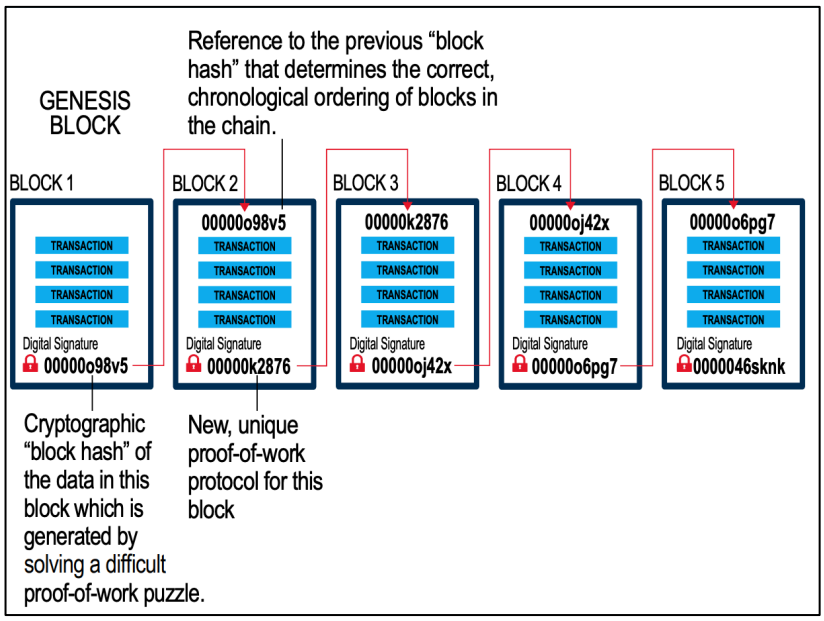

Figure 7 Blockchain structure (Source: World Bank Group)

- Communicate the address generated to receive a specific amount of cryptocurrency;
- Send tokens deposited on an existing address to a recipient address by digitally signing a new transaction. As mentioned above, the message cannot be subsequently repudiated by the signing sender.

Each address is like it represented a cryptocurrency container, which fills up when funds are received, and empties when funds are authorized to be transferred to a recipient address. The

[10] **World Bank Group. 2016.** *Distributed Ledger Technology (DLT) and Blockchain.* International Bank for Reconstruction and Development. 2016. pp. 8-10.

activities of address management, reception and authorization of new transactions through digital signature all belong to the wallet function, managed via software with a dedicated application.

2.1.3 The trust on the protocol

By accepting the rules of the protocol, the nodes adopt a common system to determine which miner will write a new block of transactions to the blockchain. Having described the ways in which participants can identify and exchange transactions, it is necessary to illustrate how blockchain technology allows participants to converge on a common state of the register, or to guarantee an agreement between the parties in a permission-less context. Specifically, the consent algorithm has to make "expensive" and impractical to control the writing process in the register, ensuring that the miner/writer of the block is chosen in a substantially random way among the participants. By observing the most popular blockchain protocols, the consensus algorithm chooses the miner in one of the following ways (Buterin, 2014):

- **Proof-of-work:** confirming a new block of transactions requires miners to perform a certain amount of work, usually associated with solving a problem. The puzzle must be "moderately difficult to solve but easily verifiable" (Franco, 2015). The winning node is generally rewarded with a pre-established quantity of newly issued cryptocurrency.
- **Proof-of-stake:** The probability of "winning" in this case is not linked to the computational ability of the miner but to other parameters, such as the amount of cryptocurrency owned by the node: imagine a lottery system where the chances of winning of a node are directly proportional to the volume of cryptocurrency that the node controls. Generally, proof-of-stake blockchain systems include distribution processes, useful for assigning an initial amount of cryptocurrency to nodes.
- **Reputation based:** the consensus algorithm takes into consideration the degree of authority established by the nodes on the network, giving relevance to the number and intensity of the relationships maintained by each entity. In this way, the confirmation process is more influenced by the nodes that participate in the network more actively.

In conclusion, it is useful to retrace the main steps for carrying out an operation on a generic blockchain. The registration process is divided into the following macro-phases:

1. **Broadcasting of new transactions**: Participants fill in and send new transactions by entering the destination address, any amount to be transferred and authorize the operation by entering their *digital signatures* with a private key;

2. **Formal correctness check**: The network nodes receive the operations and verify the authenticity of the digital signature with which the sender authorized the operation; valid transactions are considered the transaction as *pending*;
3. **Construction of a new block:** the validating nodes collect the pending transactions within a block created ad hoc, which is subjected to the operations of confirmation required by the consent algorithm or protocol;
4. **Block confirmation in the chain:** Once the block meets the confirmation requirements, it is proposed by each validator node to the rest of the network. Thanks to the consensus algorithm, a majority agreement will be reached for choosing the block to insert at the end of the chain;
5. **Verification of the operation:** every user who has access to the ledger can verify the status of the operation itself. To consider the operation as verified, it is necessary to wait for the confirmation of a sufficient number of blocks that make it statistically impossible to remove the operation from the shared ledger (e.g. for Bitcoin it is necessary to wait for at least 6 further blocks to be mined).

In summary, through the integration of digital signature and a consent algorithm, a blockchain protocol has the ability to manage the updating of the register, gradually updating it with new transactions.

2.2 Blockchain for interbank payments

Blockchain technology offers a very wide spectrum of applications and is still being continuously explored by vendors, financial institutions and startups. In particular, possible application opportunities are considered for banking institutions, that are among the most involved in the study of innovation and in knowledge-sharing activities, such as R3 CEV and Hyperledger Project introduced in the previous chapter.

The use case described in this section referred to the question: *How do banks pay each other? And how the system can be improved?* Payment systems facilitate commercial and financial transfers between buyers and sellers and for this reason are important components of a country's financial system. They comprise a set of financial institutions, supporting technological infrastructures and setups which share rules, processes and standards to make payments efficient and secure. In spite of the adoption of international standards, unfortunately every country's payment system has its own features, reflecting banking and financial history as well as the technological development of information and communication infrastructures.

Financial institutions communicate with each other through a messaging and routing system (MRS). Transactions, labelled with codes identifying the beneficiary's bank, are routed through automated clearing houses (ACHs) which manage the transmission and reconciliation of payment orders and determine the final balances to be settled. Usually, transactions are settled in different systems according to the type of payments and instruments, namely large value (RTGS), retail (RPS) or securities (SSS), through the debiting/crediting of the accounts of the parties involved in the transaction. Accounts are generally opened at central banks to ensure settlement finality for each transaction and foster trust and confidence in the whole system.

The *Real-time gross settlement (RTGS) system* is a specialist funds transfer system where the transfer of money or securities takes place between financial institutions on a "real time" and on a "gross" basis. Settlement in "real time" means a payment transaction is not subjected to any waiting period, with transactions being settled as soon as they are processed. "Gross settlement" means the transaction is settled on one-to-one basis without bundling or netting with any other transaction. "Settlement" means that once processed, payments are final and irrevocable.

When a typical transaction involves two parties with accounts belonging to two different banks, a central bank is needed. To make the argument easier, imagine an example in which Alice holds an account in bank A and wants to send money to Bob, who holds an account on bank B. This kind of transaction takes place on the country's, normally State-owned central bank, which holds accounts that are owned by the country's associated banking institutions, like bank A and bank B in the example.

Adopting this model, transfers between banks are done through the central bank. Bank A has an account with funds on the central bank, the same for bank B. When Alice initiates a US$ 5 transfer to Bob's account two main steps are executed:

1. Bank A tells the central bank its intention to transfer US$ 5 to bank B. The central bank, then, stops owing bank A this amount and now owes it to bank B.

2. Finally, bank A tells bank B about this transaction describing the amount and who is it destined to. Bank B will understand it and, knowing that the US$ 5 that just entered their central bank account belongs to Bob, now owes Bob this amount.

However, there is still a limitation: central banks will not support abroad transfers, nor other currencies than the country's official one. With this limitation, banks had to start looking for ways to transfer money across countries. When the parties of the transaction belong to different countries

which do not share common infrastructures and/or procedures, the payment cycle is similar to that described above, but the international MRS functions as a hub where all transactions are managed, playing an even more central and critical role in the smooth functioning of the system. In this case, settlement can even not occur in the account systems of a central bank, and obligations can be handled by bilateral banking accounts (correspondent banking). Such a method can also be used between banks belonging to the same country, leveraging the services of common network infrastructures. For historical reasons, only one company is currently playing the role of the international MRS, namely SWIFT (Society for worldwide interbank financial telecommunications).

SWIFT is a messaging network that financial institutions use to securely transmit information and instructions through a standardized system of codes. SWIFT assigns each financial organization a unique code that has either eight characters or 11 characters. The code is interchangeably called the bank identifier code (BIC), SWIFT code, SWIFT ID, or ISO 9362 code. To understand how the code is assigned, let's look at Italian bank UniCredit Banca, headquartered in Milan. It has the 8-character SWIFT code UNCRITMM[11]. As powerful as SWIFT is, it is only a messaging system – SWIFT does not hold any funds or securities, nor does it manage client accounts. Within three years of introduction, SWIFT membership had increased to 230 banks across five countries. Although there are other message services like Fedwire and CHIPS, SWIFT continues to retain its dominant position in the market. Its success is attributed to how it continually adds new message codes to transmit different financial transactions. But how it makes money? SWIFT is a cooperative society owned by its members. Members are categorized into classes based on share ownership. All members pay a one-time joining fee plus annual support charges which vary by member classes. SWIFT also charges users for each message based on message type and length. These charges also vary depending upon the bank's usage volume – different charge tiers exist for banks that generate different volumes of messages.

In order to exchange messages, the underlying technology is called FIN. FIN enables financial institutions to exchange individual structured (MT and ISO 15022 message formats) financial messages securely and reliably (Swift s.d.)[12]. FIN is used by over 11,000 financial institutions and their corporate customers worldwide to exchange over 31.3+ million messages per day across a wide range of business areas within the banking and securities industries. FIN value-added processing includes:

[11] **Investopedia. 2019.** How the SWIFT System Works. [Online] 2019. https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp.
[12] **Swift.** About ISO 20022. *The standard of the future* . [Online] https://www.swift.com/your-needs/industry-themes/iso-20022/supporting-standards.

- Message validation to ensure messages are formatted according to SWIFT message standards
- Delivery monitoring and prioritisation
- Message storage and retrieval

In the second half of the twentieth century, when electronic payment systems were created, all stakeholders (financial institutions, ACHs, settlement systems and so on) were looking for a fast, automated, secure, easy and low-cost way to operate their financial and commercial transactions. Hence, they set up infrastructures that directly connected financial institutions and operators (banks, ACHs, settlement systems and so on), through some information and communication technical companies (Service Providers), mainly owned by the same banks. The result was a 'closed' system of financial entities (mainly banks or bank-owned entities) where a bank receiving a message from another bank could be sure of the authenticity of the sender and of the integrity of the message. The system's security architecture reflected the structural 'trust' shared by the participants. As a consequence, once 'in', there was no need to closely control messages flowing between participants, as the sender and the receiver trusted each other as well as their messaging and routing systems. For example, with regard to the cross-border interbank payment system where, as mentioned above, the MRS is provided by SWIFT, a payment message going from Bank A to Bank B is not subject to any other authorization control when entering/exiting the SWIFT network. Controls are eventually implemented only in Bank A's own infrastructure and completely rely on Bank A's ability to make its infrastructure safe. Figure 8 shows the message flow for a common interbank and cross-border transaction.

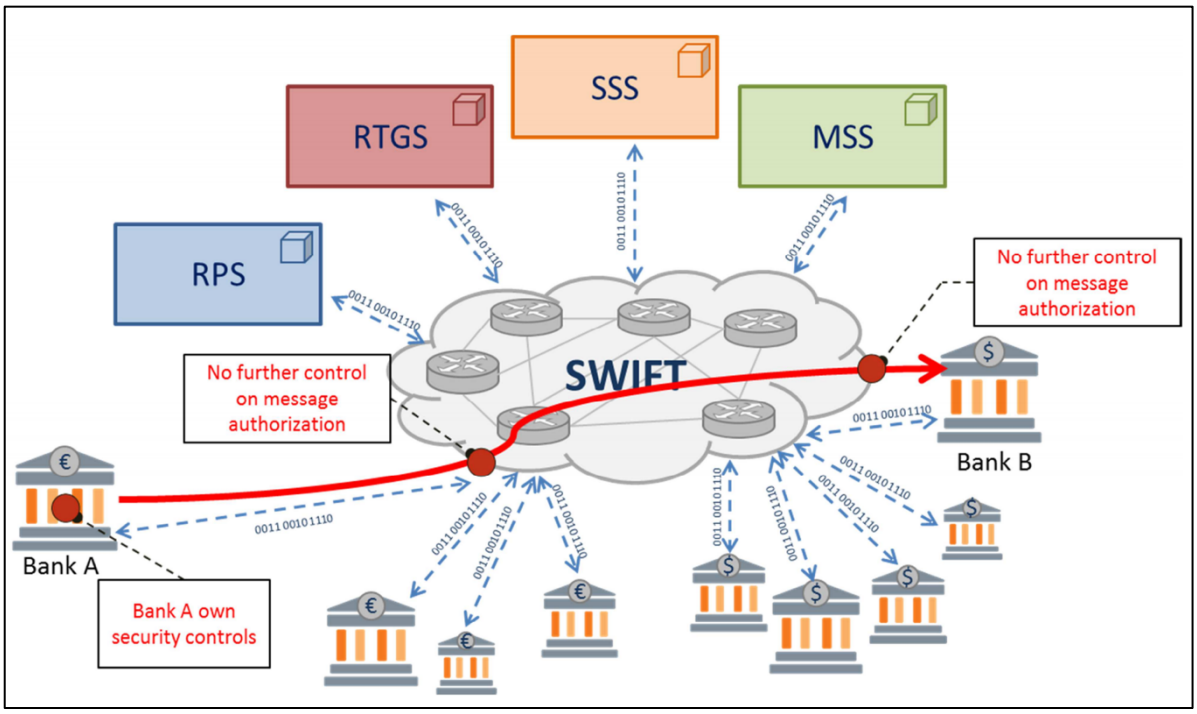

Figure 8 Message flow through the Cross-border/International Payment System (Source: Banca d'Italia)

But how the blockchain can be involved? The result of the sequence just described is that interbank payments often rely on data processing by intermediary clearing firms (in the case above, just by Bank A security controls), which involves a series of complicated steps that make the process lengthy and costly. In fact, individuals and SMEs in developing economies face uncertainty, high costs, and long delays in making inter-bank, cross-border payments, which, as have been discussed, are typically conducted across a network of correspondent banks or money transfer providers. Cross-border payments through correspondent banking channels are restricted to banks' business hours and are subject to transaction fees at three different points in the process: fees charged by the sending institution, fees charged by the receiving institution, and fees charged for the inter-bank, cross-border transfer (this could be through several intermediaries, each charging their own fee).

That's why point-to-point payment can also be improved using blockchain technology[13], thus eliminating the need of intermediary link by financial institutions that act as third-party. By creating a distributed network for cross-currency funds settlement that replaces the correspondent banking network, DLT can remove inefficiencies in the current system and offers potential for significant cost reductions, especially in the cross-border, interbank leg of the transaction. By lowering

[13] **Chen Liang, Ye Guo. 2016.** *Blockchain application and outlook in the banking industry.* School of Economics, Xiamen University. 2016. pp. 7-8.

settlement costs and increasing efficiency of cross-border transfers, DLT could potentially help in bringing down the price of remittances even further.

In a blockchain and cryptocurrency system, since normally these transfers are P2P transactions finalized directly between users or participating institutions, the role of the current intermediary like Automated clearing house would be greatly reduced. In fact, it would be possible to use a blockchain register shared by the subjects of the same banking group, authorized to operate transactions on a private blockchain. The banking branches would participate in a consensus mechanism by following a specific protocol, which would guarantee a common and consistent version of the data, and the settlement of the operations almost in real time, without the need of an intermediary institution.

The scenario takes in consideration the use of Bitcoin protocol and it is explained in figure 9. It would be as follows: the sender initiates the payment and the amount of money to be transferred is immediately converted in Bitcoins using a digital wallet or an exchange platform. Then, the role of the miners is crucial: as described in the previous chapter, they perform a fundamental activity for the entire value chain that leads to transaction verification and maintenance of the ledger. In fact, using some exchange services (platform) that allow real-time conversion of funds, both parties view at the end and at the beginning of the transaction the amount in fiat currency, respectively at the time of sending and receiving.

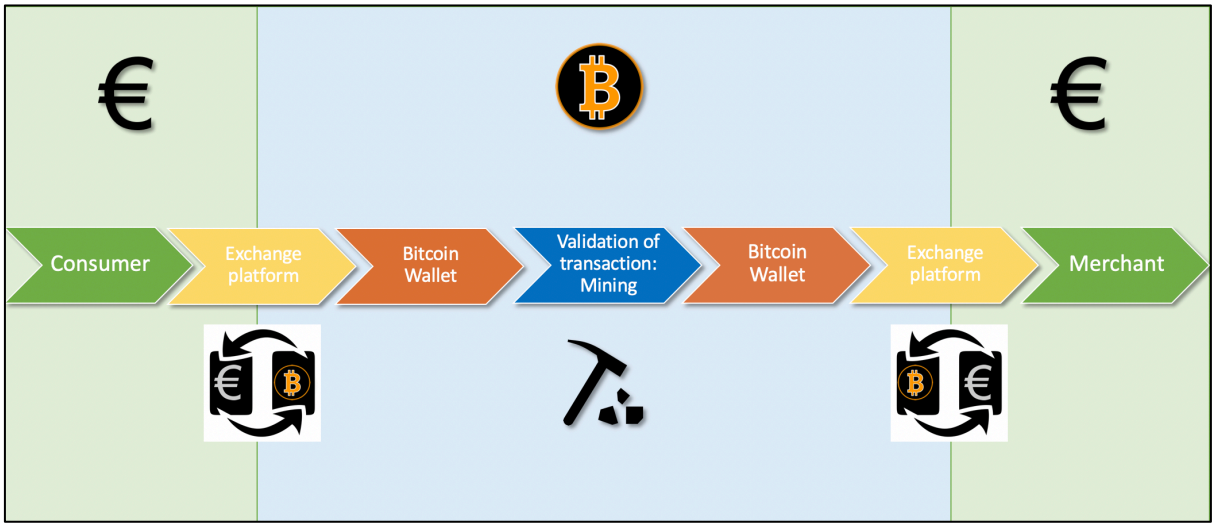

Figure 9 Transfer of funds between a consumer and a merchant using a blockchain-based technology

This use case can be extended to subjects belonging to different banking groups or to the case of cross-border payments. The traditional scenario entails the maintenance of multiple reserves to minimize the risk for each payment channel and the active role of a third party to verify, certify and authorize transactions, like the ACH or central banks.

The result is that it is possible to establish a permissioned protocol shared between various subjects even belonging to different banking groups and allowing, for example, to directly perform cross-border transactions, reducing significantly the capital required by the counterparty intermediary and lowering the process fees of transactions.

A similar platform is Ripple, a protocol that integrates an international payment system in which financial institutions can participate in the consensus mechanism as validator nodes. Indeed, Ripple is a platform run by banks, financial institutions and payment providers working to speed up remittance transactions. Differently from other blockchain protocol, Ripple is a *permissioned* public ledger where only a subset of trusted network participants is able to maintain the integrity of the ledger. Distributed ledger systems can be open (*permissionless*) or permissioned, and there are fundamental differences between the two. Bitcoin and Ethereum are the most prominent examples of completely permissionless blockchains, where network participants can join or leave the network at will, without being pre-approved or vetted by any entity. All that is needed to join the network and add transactions to the ledger is a computer with the relevant software. There is no central owner and identical copies of the ledger are distributed to all network participants. In permissioned DLs, members are pre-selected by someone – an owner or an administrator of the ledger – who controls network access and sets the rules of the ledger. Permissioned DLs, which regulate network access, typically do not require a computing power-intensive proof-of-work to verify transactions but rely on different algorithmic rules to establish consensus among members. In permissionless DLs, which don't regulate network access, there is no requirement of any trust between the participants and a complicated proof-of-work is hence used to generate consensus about ledger entries. In contrast, in the case of a permissioned DL, the administrator bears the responsibility to ensure that the participants in the DL are reliable. In permissioned DLs, any node can propose an addition of a transaction, which is then replicated to other nodes, potentially even without any consensus mechanism. Figure 10 shows a scheme in which it is possible to distinguish the characteristics of permissioned and permissionless system

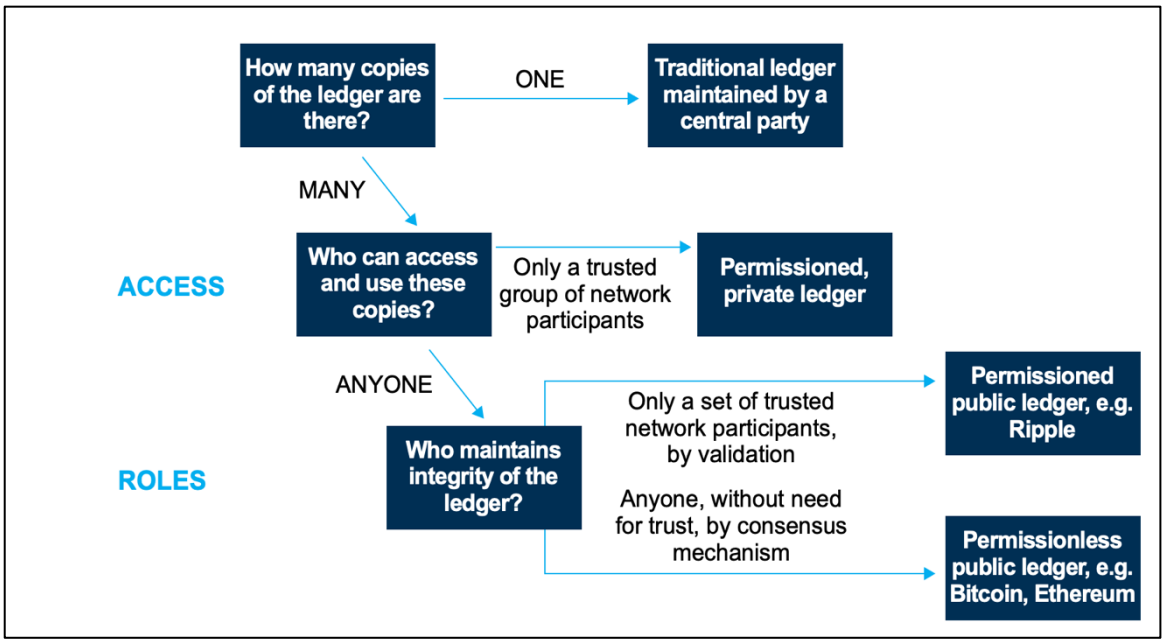

Figure 10 A schematic comparison between permissioned and permissionless DLT (Source: Handbook of blockchain, digital finance and inclusion)

2.2.1 Ripple's system

Within the Ripple system, money isn't actually transferred from one place to another only the promise of payment is transferred. There are at least four members involved in a transaction: a sender, a recipient and two gateways. These gateways (validators/ servers) are typically financial institutions such as Bitstamp and TheRockTrading. The Ripple network is a relatively large network where not everyone using Ripple knows and trusts one another. To get around this, Ripple uses chains of trusts to interconnect Ripple gateways[14]. Chains of trust are essentially link between two gateways that trust each other, although there can be indirect links of trust between gateways as well. Ripple gateways transport payment IOU[15] information to each other using https: the same protocol that banks already use for secure online credit card payments. 3 to 4 seconds after a payment is made, the Ripple network triggers the gateways involved in the transaction to update their ledgers. The token used for representing the transfer of value across the Ripple Network is called XRP. To protect the XRP Ledger from being disrupted by spam and denial-of-service attacks, each transaction must destroy a small amount of XRP. This transaction cost is designed to increase along with the load on the network, making it very expensive to deliberately or

[14] **Cata, Justin. 2018.** *Medium.* [Online] 23 July 2018. https://medium.com/@jcata018/everything-to-know-about-ripple-part-1-how-ripple-works-f7404aa4a8d1.
[15] An IOU (abbreviated from the phrase "I owe you") is usually an informal document acknowledging debt. IOUs usually specify the debtor, the amount owed, and sometimes the creditor.

inadvertently overload the network. The current minimum transaction cost required by the network for a standard transaction is 0.00001 XRP It sometimes increases due to higher than usual load. The transaction cost is not paid to any party: the XRP is irrevocably destroyed. Since no new XRP can ever be created, this makes XRP scarcer and benefits all holders of XRP by making XRP more valuable.

According to Ripple protocol (consensus whitepaper), rather than mining, Ripple works by consensus. The Ripple system isn't operated by Ripple Labs and is a peer to peer system, in which participating devices all connect to the network. Some nodes just make and receive payments for their users while others operate as validators carrying out the consensus process. These validators "look" at the ledger, which is a snapshot of the current state of transactions on the network and agree upon the current state utilizing the Ripple Protocol Consensus Algorithm (RPCA). The Ripple Protocol consensus algorithm (RPCA), is applied every few seconds by all nodes, in order to maintain the correctness and agreement of the network. Once consensus is reached, the current ledger is considered "closed" and becomes the last-closed ledger. Assuming that the consensus algorithm is successful, and that there is no fork in the network, the last-closed ledger maintained by all nodes in the network will be identical. The RPCA proceeds in rounds. In each round:

1. Initially, each server takes all valid transactions it has seen prior to the beginning of the consensus round that have not already been applied (these may include new transactions initiated by end- users of the server, transactions held over from a previous consensus process, etc.), and makes them public in the form of a list known as the *candidate set*.
2. Each server then amalgamates the candidate sets of all servers on its UNL, and votes on the veracity of all transactions.
3. Transactions that receive more than a minimum percentage of "yes" votes are passed on to the next round, if there is one, while transactions that do not receive enough votes will either be discarded, or included in the candidate set for the beginning of the consensus process on the next ledger.
4. The final round of consensus requires a minimum percentage of 80% of a server's UNL agreeing on a transaction. All transactions that meet this requirement are applied to the ledger, and that ledger is closed, becoming the new last-closed ledger.

In order to achieve correctness, given a maximal amount of Byzantine failures[16], it must be shown that it is impossible for a fraudulent transaction to be confirmed during consensus, unless the

[16] A Byzantine failure is a condition of a computer system where components may fail and there is imperfect information on whether a component has failed. The term takes its name from an allegory, the "Byzantine Generals Problem" developed to describe a situation in which, in order to avoid catastrophic failure of the system, the system's

number of faulty nodes exceeds that tolerance. The proof of the correctness of the RPCA then follows directly: since a transaction is only approved if 80% of the UNL of a server agrees with it, as long as 80% of the UNL is honest, no fraudulent transactions will be approved. Thus, for a UNL of n nodes in the network, the consensus protocol will maintain correctness so long as:

$$f \leq (n-1)/5$$

In which f is the number Byzantine failures. In fact, even in the face of $(n-1)/5+1$ Byzantine failures, correctness is still technically maintained. The consensus process will fail, but it will still not be possible to confirm a fraudulent transaction. Indeed, it would take $(4n+1)/5$ Byzantine failures for an incorrect transaction to be confirmed. This is the bound for weak correctness, and the former the bound for strong correctness. It should also be noted that not all "fraudulent" transactions pose a threat, even if confirmed during consensus. Should a user attempt to double-spend funds in two transactions, for example, even if both transactions are confirmed during the consensus process, after the first transaction is applied, the second will fail, as the funds are no longer available. This robustness is due to the fact that transactions are applied deterministically, and that consensus ensures that all nodes in the network are applying the deterministic rules to the same set of transactions.

For a slightly different analysis, let us assume that the probability that any node will decide to collude and join a nefarious cartel is Pc. Then the probability of correctness is given by $p*$, where:

$$p^* = \sum_{i=0}^{\lceil(\frac{n-1}{5})\rceil} \binom{n}{i} p_c^i (1-p_c)^{n-i}$$

This probability represents the likelihood that the size of the nefarious cartel will remain below the maximal threshold of Byzantine failures, given Pc. Since this likelihood is a binomial distribution, values of pc greater than 20% will result in expected cartels of size greater than 20% of the network, thwarting the consensus pro- cess. In practice, a UNL is not chosen randomly, but rather with the intent to minimize pc. Since nodes are not anonymous but rather cryptographically identifiable, selecting a UNL of nodes from a mixture of continents, nations, industries, ideologies, etc. will produce values of pc much lower than 20%. As an example,[17] the probability of the Anti-Defamation League and the Westboro Baptist Church colluding to defraud the network, is certainly much, much smaller than 20%. Even if the UNL has a relatively large pc, say 15%, the probability

actors must agree on a concerted strategy, but some of these actors are unreliable. In a Byzantine failure, a component such as a server can inconsistently appear failed, presenting different symptoms to different observers. It is difficult for the other components to declare it failed and shut it out of the network, because they need to first reach a consensus regarding which component has failed in the first place.

[17] **David Schwartz, Noah Youngs, Arthur Britto. 2018.** *The Ripple Protocol Consensus Algorithm.* s.l. : Ripple Labs, 2018. pp. 3-5.

of correctness is extremely high even with only 200 nodes in the UNL: 97.8%. A graphical representation of how the probability of incorrectness scales as a function of UNL size for differing values of pc is depicted in Figure 11. Note that here the vertical axis represents the probability of a nefarious cartel thwarting consensus, and thus lower values indicate greater probability of consensus success. As can be seen in the figure, even with a pc as high as 10%, the probability of consensus being thwarted very quickly becomes negligible as the UNL grows past 100 nodes.

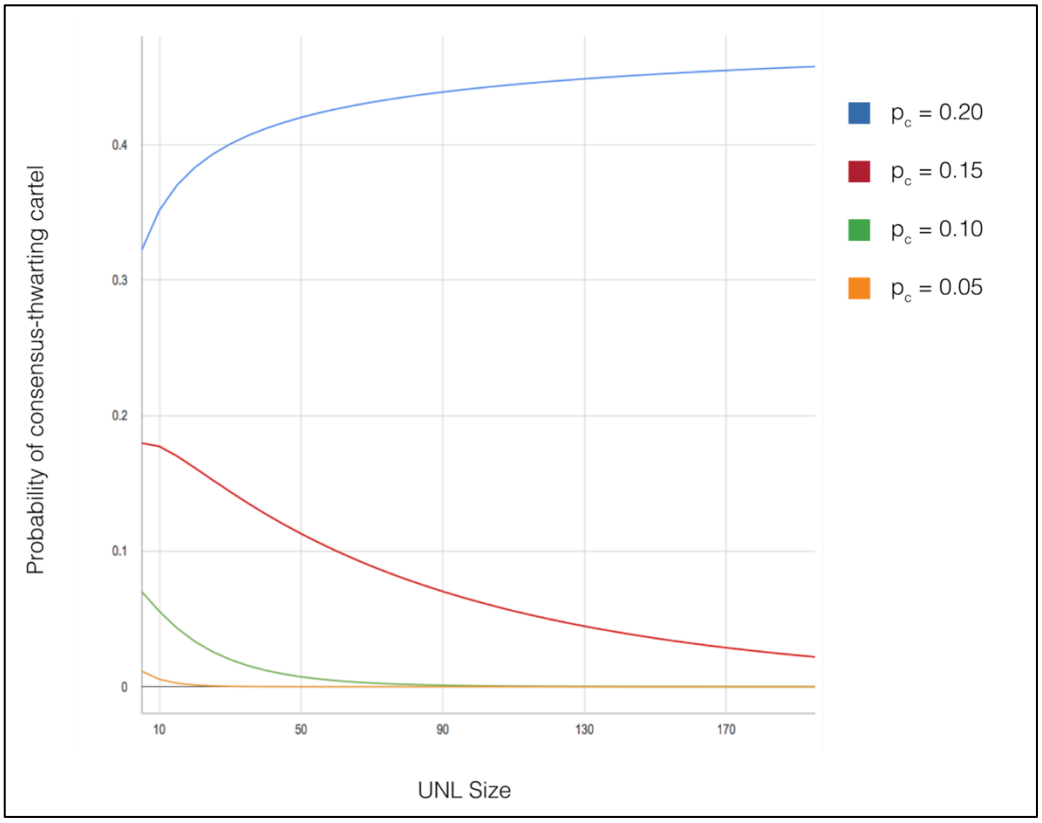

Figure 11 Probability of a nefarious cartel being able to thwart consensus as a function of the size of the UNL, for different values of pc, the probability that any member of the UNL will decide to collude with others. (Source: Ripple consensus protocol)

2.3 Blockchain for Trading securities

Beyond the area of payments, blockchain technology could bring important points of innovation and process optimization also for the entire value chain of financial services. The paradigm can be revolutionary for the various activities that characterize the management of security (e.g. shares, bonds, options), from the initial stages preceding the moment of execution and matching of orders, up to the final settlement that certifies the transfer of ownership asset. The attention gained by the financial institutions for this field of application, as well as the study of specific use cases within the research consortia (e.g. R3 CEV), is demonstrated by the recent publications of leading institutions in academic research (e.g. London School of Economics, 2016).

The record-keeping functions offered by the protocol allow to represent different financial instruments in a shared digital format. At the same time, the ledger can trace the asset ownership passages with dedicated records, automatically saved for each trading operation.

The exchange of financial instruments is in fact a very rich process from an information point of view, which associates a heterogeneous group of metadata with each transaction. The information directly describes the operations carried out or provides non-transactional indications. For example: Purchase / sale order data, data that identify and describe the exchanged asset and data of intermediary bodies.

In the value chain of the current scenario, taking into consideration the process limited to the phases of insertion, order allocation and matching on an exchange platform, the metadata are fragmented on proprietary systems, often requiring an effort of reconciliation between individuals' bodies. Sometimes conflicts are also encountered internally within company structures, where it is not unusual to come across stratified or "silo[18]" architectures.

This underlying misalignment can be mitigated by reporting metadata on a common ledger, in an inter-institution collaboration scenario.

Moreover, it is particularly interesting to evaluate the role of intermediaries and custodians. the current model makes transactions safe by almost eliminating counter-party risk. This is done at the price of exposing the holding of securities to custody risk. Indeed, investors nowadays hold securities through chains of custodians and are exposed to risk of any of these failing.

Getting briefly into the past history, when computers were first introduced into financial markets there was a lot of excitement and urgency about replacing paper with electronic settlement. The transformation was not easy, however. It took almost 10 years for the electronic settlement system CREST to come live (Micheler e Heyde 2016). It turned out that the reform did not lead to the creation of a new system from scratch that may have reflected the possibilities offered by the technology. As it turned out the system that was created closely resembled the paper settlement and holding system. The existing framework was effectively preserved with the slight change that communication by paper was replaced with communication by electronic instructions. The providers of the infrastructure remained in place and their processes were repeated on computers instead of paper ledgers. The availability of almost instant electronic communication has had an additional and surprising effect. When securities were transferred by way of paper, investors used to have their name entered on the issuer register. It took some time for a transfer to be recorded on the register, but the investor had a direct connection with the issuer. While settlement of trades was

[18] A silo structure refers to partitioning logic. Silos are the compartments that make up the information architecture of a website.

cumbersome, it was easy to hold securities and exercise rights arising out of them. The introduction of uncertificated (electronic) securities changed that balance. Settlement times were reduced allowing the speed of transferring securities to increase, but the holding of securities and the ability of investors to exercise their rights has become significantly more complex and riskier. Investors have become separated from issuers through intermediation. A framework emerged whereby the names of investors were removed from issuer register and replaced by nominees who hold securities on trust for investors or, more likely, other intermediaries.

As just discussed, the principal risk in securities markets is settlement risk, where the seller of a security fails to deliver the security while receiving payment or where the buyer of a security fails to deliver payment while receiving the security. To deal with such risk, securities settlement systems have been put in place in many markets to ensure a delivery versus payment (DvP) mechanism where the settlement of the cash and the securities leg in a trade are intrinsically linked.

These systems are typically organized around a specialized third party, called the Central Securities Depository (CSD), which transfers legal ownerships of securities against payment. Many practitioners believe that blockchain or distributed ledger technology (DLT) has the potential to radically transform securities settlement. As will be introduced down below, the key innovation is to have a shared database of securities ownership that can be updated without relying on multiple, specialized intermediaries or a third-party infrastructure. Settlement risk can be contained by employing smart contracts that are built to automatically provide DvP in the absence of a central authority.

With blockchain technology a new technology for keeping securities registers and for updating them has become available. The technology has been said to make it possible for trading, clearing and settlement to merge into one real time process that does not involve relationships with multiple intermediaries. There is no need for separate trading, clearing and settlement venues. There is no exposure to the risk of any one central provider failing. Buyer and seller can interact directly with each other. They can exchange securities and cash directly and in real time. The adoption of a decentralized ledger, whose copies are sufficiently distributed and aligned thanks to a consent algorithm, guarantees the immutability of the information and standard access rules to the data for the audit operations. The exchange flow can be redesigned by managing the transfer of the asset entirely on the blockchain. The asset is digitally represented with identification metadata and can be transferred by inserting this information content into a dedicated transaction. By consulting the blockchain it will be possible to verify the issuance of the transaction from a certified address, in this case controlled by the body authorized to issue the asset. Figure 12 shows the trading flow for

an exchange of securities exploiting a distributed ledger technology: seller and buyer sign their orders with digital signature respectively and publish them on the ledger blockchain. Once registered, thanks to an external algorithm, the matching between the orders entered is established. In terms of user interface not much needs to change. Investors would access their portfolio like they are now through a computer or through some other electronic device. But while at present the interface they see is a record keep by an intermediary who is connected to another intermediary who is connected to yet another intermediary, what they see in a distributed ledger/blockchain environment would be the master record.

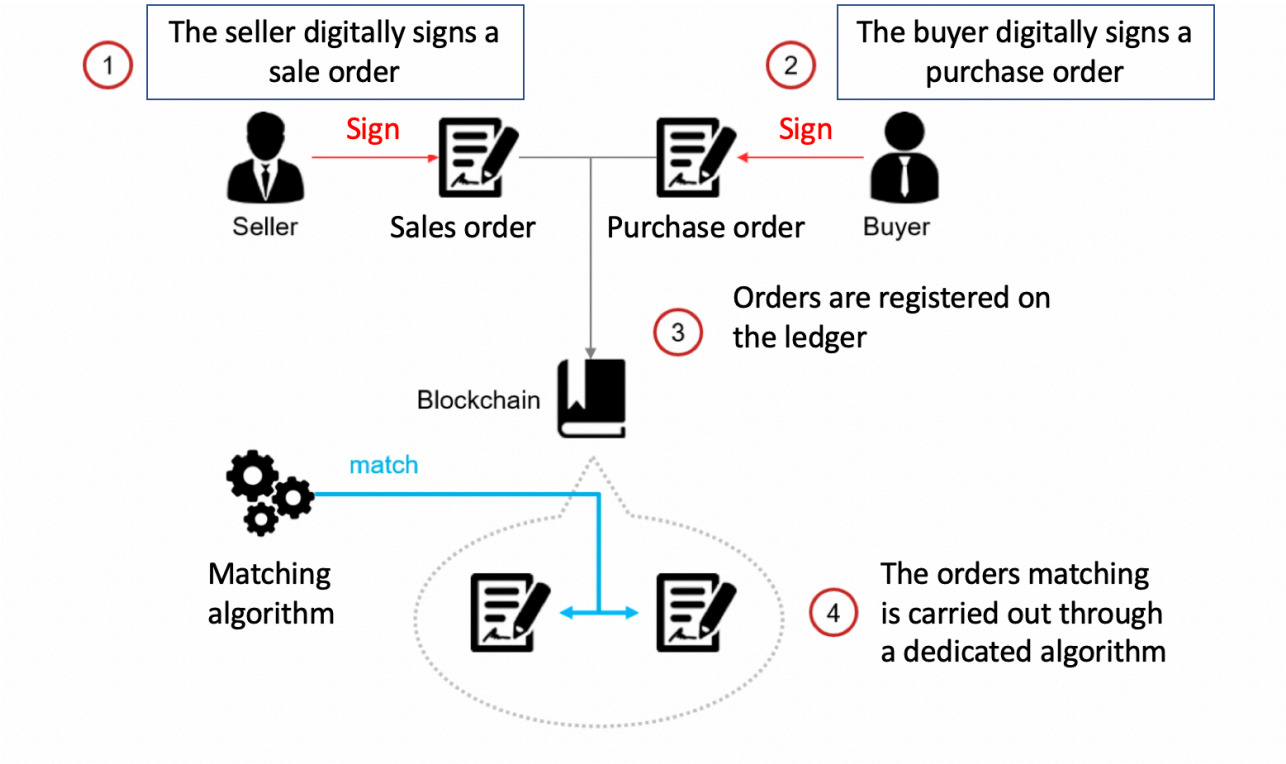

Figure 12 Trading flow by exploiting the blockchain ledger (Source: Reply Technology)

The advantages of the solution are mainly:

- Direct negotiation of the asset, with a reduction in process times and costs;
- Reduction of the risk associated with custody activities: ownership of the asset is established with state-of-the-art cryptographic tools, without any possibility of repudiation of transfer operations.

There is, of course, a risk that the computers break down or will be hacked into, but because every node has an identical copy of the ledger that risk has been referred to as very small.

But what is the structure of the blockchain (represented in figure 10) that acts as an alternative intermediary between the users? The system should not rely on any existing blockchain design, but rather build a model of a hypothetical blockchain for securities settlement that has three distinctive features:

I. It is assumed that the blockchain handles ownership transfers of both securities and payments. This enables a DvP mechanism and, thus, the blockchain has the potential to directly rule out settlement risk.

II. It is assumed that the blockchain is permissionless. There are no designated, third parties that are in charge of updating the information stored on the blockchain.

III. The design of the blockchain controls the speed of settlement. The *block time* determines how frequently a batch of securities transactions is being settled, while *block size* controls the maximum size of each batch. Participants will select how fast they would like to settle by posting transaction fees to have their transactions incorporated into a block.

In order to understand these principles, it is worth to better understand the concept of block size and block time. *Block time*, in the context of cryptocurrency, is a measure of the time it takes to produce a new block, or data file, in a blockchain network. It is the length of time it takes to validate the existence of a new batch of bitcoins. Theoretically, each network has its own defined block time (Frankenfield s.d.)[19]. For instance, both in bitcoin blockchain and Ethereum blockchain, there is an expected block time and an average block time. In bitcoin, the expected block time is 10 minutes, while in ethereum it is between 10 to 19 seconds. It has already been discussed that both bitcoin and ethereum use a proof of work based distributed consensus algorithm. The expected block time is set at a constant value to make sure that miners cannot impact the security of the network by adding more computational power. On the other hand, the average block time of the network is evaluated after *n* number of blocks. If it is greater than the expected block time, then the difficulty level of the proof of work algorithm will be reduced, and if it is less than the expected block time then the difficulty level will be increased. That's the core design principle behind block time. The level of the protocol difficulty varies with the time, according to the following formula:

new_difficulty = old_difficulty X (2016 blocks X 10 minutes) / (the time took in minutes to mine the last 2016 blocks)

[19] **Frankenfield, Jake.** Block Time. *Investopedia.* [Online] https://www.investopedia.com/terms/b/block-time-cryptocurrency.asp.

This formula tries to evaluate the speed of the mining network and find out how much it deviates from the expected level. The expectation is to mine a block in 10 minutes. In the above example, if the average speed of mining the last 2016 blocks is 8 minutes — then the new *difficulty factor* will be greater than one, so the current difficulty level will be increased. In case the average is above 10 minutes, then the factor will be less than 1 and the difficulty level will be decreased for the next 2016 blocks. The difficulty level is re-evaluated after every 2016 blocks, that's roughly after every 2 weeks. Figure 13 shows how the difficulty level changed with the time from the inception of bitcoin. In other words, the difficulty level reflects how difficult the proof of work calculation with respect to the difficulty value set at the beginning — which is 1. For example, the current difficulty is 678,760,110,083 — which means if we mine the blocks at the same hash rate, which was at the time of the 1st block, then it would take more than 678 billion times to mine a block with the current difficulty. But in practice, since the computational power thrown into the bitcoin mining improved vastly, the time takes to mine a block is kept at a constant number (which is 10minutes), by increasing the level of difficulty. During the first five years of bitcoin, the difficulty level increased from 1 to 50 billion.

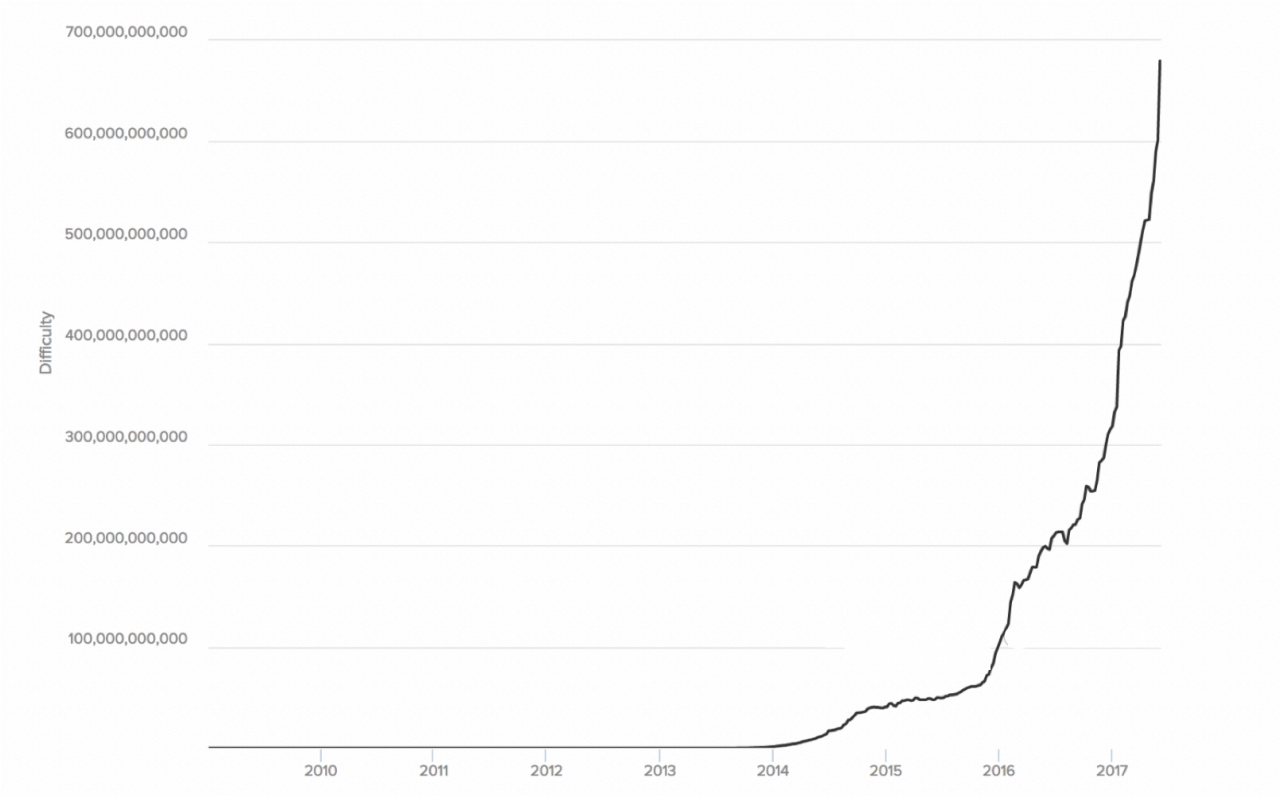

Figure 13 Change of difficulty level in mining blocks since the Bitcoin inception (Source: Coindesk)

Coming back to our record-keeping system that keeps track of securities ownership as well as payments related to securities trades, for securities trades to be settled, the transaction

information (transfer of ownership and payment) needs to be recorded on the blockchain. To this end, the investors involved in the trade communicate this information to a peer-to-peer network that is charged with updating the blockchain. The competition among miners to win the computational race helps to protect the integrity of the blockchain. After a securities transaction has taken place and has been communicated to the network, an investor can still undo it by creating a *fork* on the chain, which is an alternative history of records. If the investor trying to fork wins the competition, he can convince the entire network that the transaction has not been conducted. To avoid such settlement fails, the blockchain system needs to offer large rewards to make the mining competition sufficiently difficult. A blockchain can generate fees by limiting the speed at which it is updated. through the design of the blockchain, by restricting the block size (how many transactions can be included in each new record) and the block time (how frequently new records are incorporated). When investors have a desire to settle early, slowing down block time and making blocks smaller creates congestion on the blockchain. Investors are then willing to pay larger transaction fees in order to get into blocks faster and, hence, settle their trades faster. In essence, congestion makes fast settlement scarce, turning a public good into a club good. Overall, it is optimal to choose the block time and block size that jointly minimize the time to settle all transactions over a trade period, while still generating sufficient fees to rule out settlement fails (forks).

2.4 Blockchain-based settlement and post-trading activities

As-is Scenario

Post-trading activities include all the services provided after the execution of security purchase and sale orders (e.g. stocks, bonds or options), from the matching operation on the exchange platform, to the final settlement phase. Generally, the support activities for the insertion and execution of the order are not included in this definition and characterize the actual trading phase. The sequence of activities that make up the value chain of the security market is shown in Figure 14:

Figure 14 The value chain of financial trading processes

Current post-trade settlement arrangements that rely on a designated third party tend to be slow and inefficient. This is mainly related to the nature of dispersed information in the trading process and the costs of reconciling this information, because many intermediaries operate back office systems that are incompatible with other financial market infrastructure. Currently, indeed, financial intermediaries keep multiple separated records of the same information. It should be emphasized that the driver of high Backoffice costs in securities markets is not the cost of storing redundant data but rather the redundancy of business processes. A study conducted by the consultancy firm Oliver Wyman for SWIFT estimated there to be global costs of $5-10bn for clearing activities, $40-45bn for settlement, custody, and collateral management (of which $39bn is paid to market players in the custody chain), and $20-25bn for post-trade data and analytics. The table represented in figure 15 shows what are the total amount of costs for each section of the value chain for trading and post-trading activities.

VALUE CHAIN		ACTORS					
		SELL-SIDE	EXECUTION VENUES (EXCHANGES, IDBs, CCPs)	(I)CSDs	CUSTODIANS	DATA & TECHNOLOGY PROVIDERS & OTHER 3RD PARTIES	TOTAL
Primary		$57 BN ECM: $20 BN DCM: $22 BN M&A: $5 BN	$1 BN				$55-60 BN
Client Coverage							
Execution	Commissions	$180 BN Cash: $53 BN Listed: $22 BN OTC: $108 BN	$13 BN		$4 BN	$3 BN	$190-210 BN
	Risk premiums						
	Financing						
Clearing			$4 BN		<$1 BN		$5-10 BN
Securities services	Settlement		$1 BN	$3 BN	$39 BN		$40-45 BN
	Custody						
	Collateral management						
Post trade data and analytics			$4 BN			$20 BN	$20-25 BN
Revenue		~$240 BN	~$24 BN	~$3 BN	~$44 BN	~$23 BN	~$330 BN

Figure 15 Revenue pools in capital markets ecosystem (Source: Company annual reports, Oliver Wyman analysis)

Financial intermediaries have to update their own accounts every time a new transaction takes place. They are then required to send any relevant results of this exercise to the interested parties, at different levels of the post-trade industry, in order that they can reconcile their own accounts to reflect the new situation and inform their interested parties of any changes. The securities flow between trading and settlement takes time, although execution of the matched settlement instructions at the settlement level can be instantaneous[20].

In order to understand the innovation that a blockchain-based technology can bring into the industry, it is important to analyse the as-is scenario and the intermediaries involved in a standard transaction. To begin, the industry of safekeeping and storing securities is called the *custody industry.* Today's multi-tiered custody industry is not something that was developed intentionally with a clear concept in mind; instead it has gradually evolved over time with ever-increasing complexity. It originally concerned the safekeeping of the physical representations of securities, however, one of the main difficulties with this was that when the ownership of a security changed

[20] **Pinna, Andrea and Ruttenberg, Wiebe. 2018.** *Distributed ledger technologies in securities post-trading.* European Central Bank. 2018. pp. 20-21, ECB Occasional Paper 172. 978-92-899-2335-4.

hands, the certificate had to be moved from the seller's custodian vault to the buyer's one. To resolve this, the approach of most countries was to introduce a so-called central securities depository (CSD) which would hold the assets for all the custodians in the country. This would allow the transfer of assets to be conducted simply by changing the owner in the CSDs books while the custodians remained to provide information regarding the customers transactions and in general being the link between the investors and issuers of securities. With the assets rendered immobile the dematerialization of the assets was the logical step forward, which allowed the ownership of assets to be represented only by entries in the books without any underlying physical certificates need being stored[21]. The common goal for all CSDs is to provide a definitive record of ownership of securities.

Although having extended the scope of their services since their conception, CSDs and custodians (whose role is now significantly marginalized and largely invisible to investors) still only make up a part of the puzzle that is the securities market. While securities do not actually move around the market anymore, since they are now immobilized by the CSDs, there are other important operations involved in the trade of securities, such as clearing and netting (performed at clearing houses), price discovery, and matching counterparties (performed at trading venues, e.g. stock exchanges).

Besides the custodians, CSDs, stock issuers and investors there are a few other participating entities when a settlement takes place. Firstly, both the seller and buyer of an asset will be required to use a *Stockbroker* (commonly named broker, for instance Plus500 or a bank such as Fineco) which has the required knowledge and access to a stock exchange. In addition, this middleman will introduce a fee in the form of commission. Secondly, the trade of an asset for cash is something that introduces a risk that one of the two parties might default after one part of the transaction has taken place. In order to alleviate this risk for the buyer and seller an additional institute called Central *Counterparty Clearing House (CCPs)* exists which takes on this risk themselves (in exchange for an additional fee). This institute takes control of both the asset and the funds before they are relayed to the buyer and the seller.

Figure 16 shows a high-level scheme of a trade process flow

[21] **Wall, Eric and Malm, Gustaf. 2016.** *Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository.* Department of Electrical and Information Technology , Lund University. Sweden : s.n., 2016. pp. 29-30.

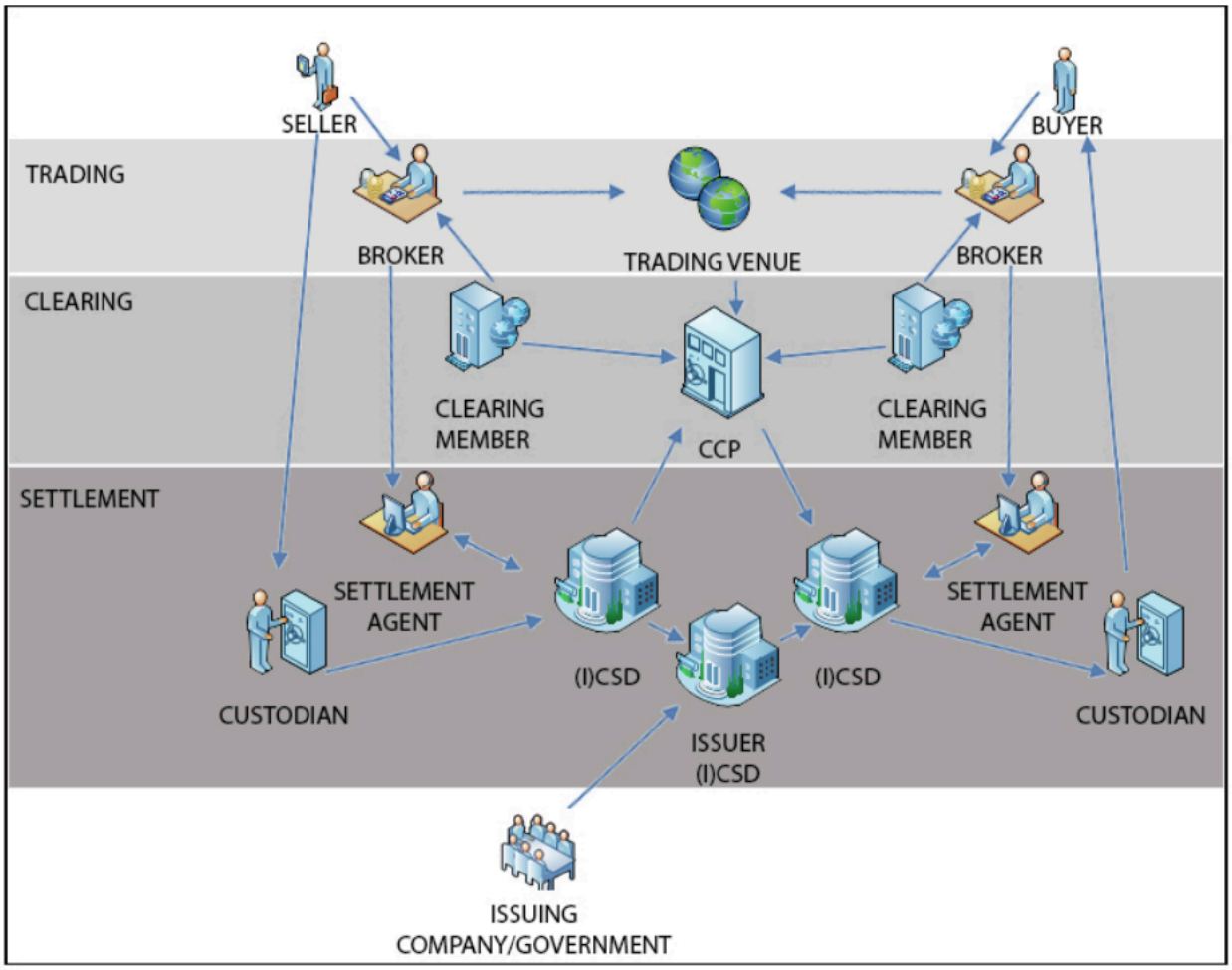

Figure 16 Trading and Post-trading flow: the AS-IS scenario (Source: European Central Bank)

The buyer and seller have to instruct their respective brokers as to their willingness to trade. The orders are routed to a trading venue where they can "cross" in the order book or on an alternative trading system and make a trade. Trade details are sent to CCPs performing reconciliation and netting while concentrating credit risk. The clearing house may thus, in some cases, become the central counterparty (CCP) to both final. Possibly at the same time, the members of the clearing house inform their respective brokers of their obligations and the brokers instruct their settlement agents. The settlement agent of the seller's broker receives the securities from the seller's custodian into its account, and credits them to the clearing house – which, for simplicity, we assume to have accounts in both the investors' central securities depositories (CSDs). The CCP then issues an instruction for the securities to be credited to the account of the buyer's settlement agent, who credits them to the buyer's custodian. It may be necessary to carry out a reconciliation between the investors' CSDs and the issuer's CSD, e.g. to allow the execution of the notary function and of asset servicing. Each of these steps may require a party's records to be reconciled with those of other parties at different levels of the value chain.

The clearing and settlement using these traditional processes are subjected to latency, risk and large operational costs. Current conventions maintained by the Depository Trust & Clearing Corporation (DTCC) in the U.S. and the European Commission of the EU are characterized by settlement times of a maximum of three days (T+3) and two days (T+2) respectively, reflecting the industry standards. The EU recently made the move from T+3 to T+2 days settlement through new systems called TARGET2 and TARGET2-Securities, a development which has taken eight years to achieve. The time and cost required for this change reflects how difficult it is to improve and advance the currently patched and multitiered financial system.

The limits of this infrastructure mainly derive from:

1. **Inefficiency** - the number of intermediaries is very large: in addition to users and their brokers, there is the presence of subjects with the function of trade allocation, exchange, security custody, clearing, risk management and settlement. Consequently, the costs for the execution of the individual activities and the time for completing the process increase. In fact, settlement can take place up to 3 days after the trading date (US example):
   Trading (T+0): The buy & sell orders are sent to the respective brokers; Brokers enter order data on the exchange platform; Matching and execution;
   Clearing (T+2): The Automatic Clearing House (ACH) checks the availability of funds and the ownership of security; The ACH records the execution of orders semi-automatically
   Settlement (T + 3): the execution of orders is confirmed to the brokers; The crediting of funds and the transfer of security to the respective custodians is finalized.
2. **Limited transparency** - the fragmentation of the processing flow is reflected at the information level. The transaction data and the logs of the individual activities reside on different platforms with restricted access, making it difficult to trace the changes in the state of security along its life cycle.
3. **Limited interoperability** - the systems used by each intermediary do not necessarily share the same operating standards. In fact, each actor has evolved independently, with different technologies and methods: this has produced a "silo" stratification of systems that are expensive to maintain and difficult to integrate.

To-Be Scenario

A blockchain-based technology can reduce information costs by providing a common, public ledger that can be accessed by and shared with all participants. This allows a blockchain-based system to also offer flexibility in settlement times and costs. It can introduce time-varying

settlement times that depend on actual needs of markets and participants instead of being based on technological constraints. As participants choose how fast to settle, they can either save costs by accepting longer lags or ensure additional benefits by settling faster for a higher fee. Recent analysis[22] suggest that distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between $15-20 billion per annum by 2022.

2.4.1 Process flow of single-ledger DvP

DvP in blockchain database structures will take different forms depending on whether or not the two exchanged assets exist on the same ledger or not. For example, if both cash and securities are tracked by the same blockchain, then delivery versus payment can be completed in a single transaction. The algorithm to apply in order to execute the transaction depends on the platform which it is performed into. Among the others, three open-source blockchain platforms are commonly used for these kinds of transaction: Corda, Elements, and Fabric. The example down below involves a transaction between two counterparties, Alice and Bob, who want to carry out an exchange of asset and cash. The transaction can be explained in 4 different steps (shown in Figure 17):

Step 1. Bob (original holder of the securities) creates the securities instruction (spending of the agreed amount of securities) and Alice (original holder of cash) creates the cash instruction (spending of the agreed amount of cash). At this stage, neither of the instructions has been signed yet.

Step 2. Bob sends his part of the instruction (securities instruction) to Alice without his signature. Alice verifies the contents of the securities instruction and combines that securities instruction with the cash instruction of his own, thereby creating a full set of instructions. Alice signs his part of instruction (cash instruction) and sends it back to Bob.

Step 3. Bob verifies the full instruction and signs his part of instruction (securities instruction) and submits the full-signed instruction to the consensus mechanism.

Step 4. Following the implemented consensus mechanism of the platform, the submitted full-signed instruction is verified and confirmed, and the results are written on the ledger. The verifications made by the two counterparties ensure validity with respect to their agreements, while those

[22] **Belinky, Mariano, Rennick, Emmet and Veitch, Andrew. 2018.** *The Fintech 2.0 Paper: rebooting financial services.* Santander InnoVentures. 2018. p. 15.

made by the platform ensure confirmation with respect to its consensus mechanism. Actual flow of transaction processing/commitment depends on the architecture of DLT platforms.

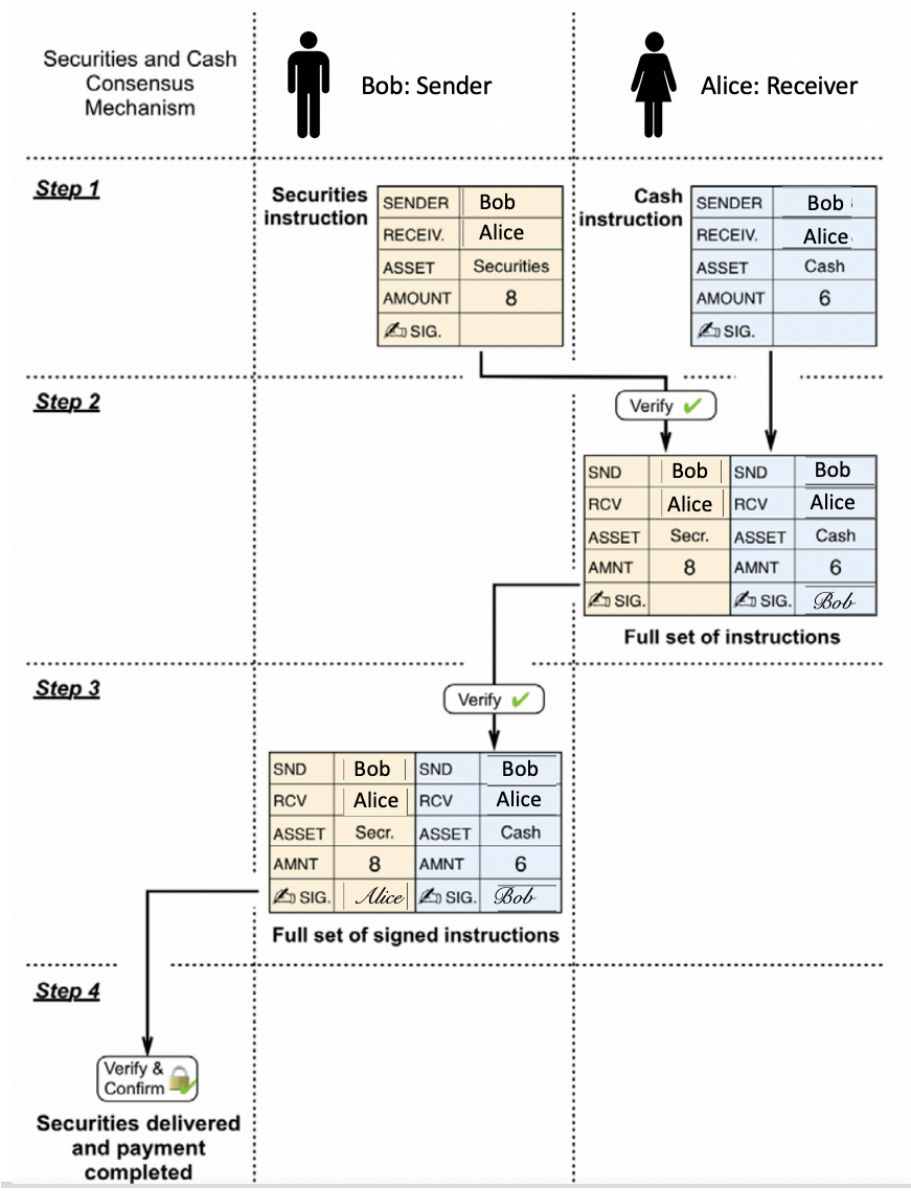

Figure 17 Process flow of single-ledger DvP (Source: Department of Electrical and Information Technology Lund University)

However, multi-asset ledgers are a relatively rare occurrence and the example above can be applied mainly among common transaction. The next step is therefore beginning by providing a description of how to approach the problem of achieving delivery versus payment in a scenario involving two different blockchains.

2.4.2 Process flow of cross-ledger DvP with HTLC

The idea behind the cross-ledger DvP is to use a *Hash Time Locked Contract* (HTLC). The HTLC is a class of payments that use *hashlocks* and *timelocks* to require that the receiver of a payment either acknowledge receiving the payment prior to a deadline by generating cryptographic proof of payment or forfeit the ability to claim the payment, returning it to the payer[23]. The cryptographic proof of payment the receiver generates can then be used to trigger other actions in other payments, making HTLCs a powerful technique for producing conditional payments. In the case of cross-ledger DvP the scope is to use HTLC for conditional delivery of securities and correspondent payment of cash. To be concrete, a *cryptographic hash function Y=H(X)* enables the two counterparties to block the assets to be delivered and a timelock[24] enables them to recover the assets when the process fails. As with the single-ledger process flow, the cross-ledger DvP process flow enables counterparties to directly match settlement instructions between counterparties by using cryptographic signatures[25].

Settlement is successful when participants follow the following steps:

Step 1. Bob (original holder of the securities) generates a secret X and its hash function Y=H(X). Bob shares Y with Alice. As long as a one-way hash function is used, it is impossible within reasonable assumptions for Alice to find X from Y. Bob creates the 1st securities instruction (spending of the agreed amount of securities). In this instruction, Bob specifies the following two conditions:

a. The receiver of the securities will be Alice if Alice provides X which satisfies Y=H(X) or
b. The receiver of securities will be Alice if two hours pass. Bob then signs it and submits the signed instruction to the securities consensus mechanism.

Step 2. Following the implemented consensus mechanism of the platform, the submitted 1st securities instruction is verified and confirmed, and results are written on the ledger in the securities DLT network.

[23] https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts

[24] It should be noted that the locking time of one asset (e.g. two hours) should be larger than that of the other asset (e.g. one hour) to prevent a counterparty refunding the assets while obtaining the other asset. For example, if the locking time of the 1st securities instruction is one hour and that of the 1st cash instruction is two hours, then assuming the flow of time of the two DLT networks is the same, Bob would be able to refund securities and obtain cash by not sending the 2nd cash instruction within one hour.

[25] **Bank of Japan, European Central Bank. 2018.** *Securities settlement system: DvP in a distributed ledger environment.* 2018. p. 14.

Step 3. Alice (original holder of the cash) verifies the content of the committed 1st securities instruction of Bob. Alice then creates the 1st cash instruction (spending of the agreed amount of cash). In this instruction, Alice specifies the following two conditions:

a. The receiver of cash will be Bob if Bob provides X which satisfies Y=H(X) or
b. The receiver of cash will be Alice if 1-hour passes. Alice signs it and submits the signed instruction to the cash consensus mechanism.

Step 4. Following the implemented consensus mechanism of the platform, the submitted 1st cash instruction is verified and confirmed, and the results are written on the ledger in the cash DLT network.

Step 5. Bob verifies the content of the committed 1st cash instruction of Alice. Bob then creates the 2nd cash instruction (obtaining of the agreed amount of cash) providing X, signs it and submits the signed instruction to the cash consensus mechanism.

Step 6. Following the implemented consensus mechanism of the platform, the submitted 2nd cash instruction is verified and confirmed, and results are written on the ledger in the cash DLT network.

At this point, the agreed amount of cash is transferred from Alice to Bob.

Step 7. Alice obtains X specified in the committed 2nd cash instruction of Bob. Alice then creates the 2nd securities instruction (obtaining of the agreed amount of securities) providing X, signs it and submits the signed instruction to the securities consensus mechanism.

Step 8. Following the implemented consensus mechanism of the platform, the submitted 2nd securities instruction is verified and confirmed, and results are written on the ledger in the securities DLT network.

At this point, the agreed amount of securities is transferred from Bob to Alice.

In cross-ledger DvP with HTLC, potential settlement fails could result in two different risk scenarios: In the first scenario settlement fails could occur, for example, where the 1st securities instruction and the 1st cash instruction is completed but Bob (receiver of cash and generator of the secret) does not submit the 2nd cash instruction within the predefined locking time (one hour). In this case, although the transfer of both cash and securities is not successful, neither of the

counterparties is exposed to principal risk as the assets are returned to the original holders after the locking time expires. The counterparties would, however, be exposed to replacement cost risk [26] and liquidity risk[27].

In the second settlement fails could occur during the process flow where one counterparty (here Bob) already retrieved the agreed amount of cash and the other counterparty (here Alice) did not complete the 2nd securities instruction within the predefined locking time (two hours). In this case the locking time for the latter instruction will expire and the original holder (Bob) can refund the locked assets (securities). Ultimately, this counterparty will hold both his refunded assets (securities) and the retrieved assets (cash) while the other counterparty will be exposed to principal risk. In this specific fail scenario only one leg of the transaction is settled and DvP will not be achieved. This scenario illustrates the weakness of HTLC and stresses the need for further developments.

2.4.3 Process flow of cross-ledger DvP with the two-phase commitment scheme

Behind the cross-ledger DvP by exploiting HTLC, it is possible to implement further solution in order to mitigate the risks above mentioned. In detail, the solution[28] that is going to be described down below has similar characteristics with the one previously illustrated and entails the usage of the Bitcoin protocol, but it can in theory be expanded to any blockchains as long they support similar cryptographic functions which allows its assets to be locked temporarily and provably on both sides of the transaction. In the solution scheme, Alice and Bob wants to trade cash for assets, but they are on different blockchains. Since the assets and cash cannot leave their respective ledgers, Alice and Bob hold a *key pair* with both ledgers, as shown in Figure 16.

[26] Until a securities transaction is settled a counterparty faces the risk of incurring the cost associated with replacing the original transactions.
[27] Liquidity risk (i.e. the risk that a counterparty will have insufficient funds to meet its financial obligations when due but may be able to do so at some time in the future) would arise in the case of settlement fails. Liquidity risk could also emerge depending on the way in which liquidity – either the cash leg or the securities leg in the DvP transactions – is available during the settlement process.
[28] **Back, Adam and Matt Corallo, Luke Dashjr. 2014.** *Enabling Blockchain Innovations with Pegged Sidechains.* Blockstream. 2014. p. 21. 5620e43.

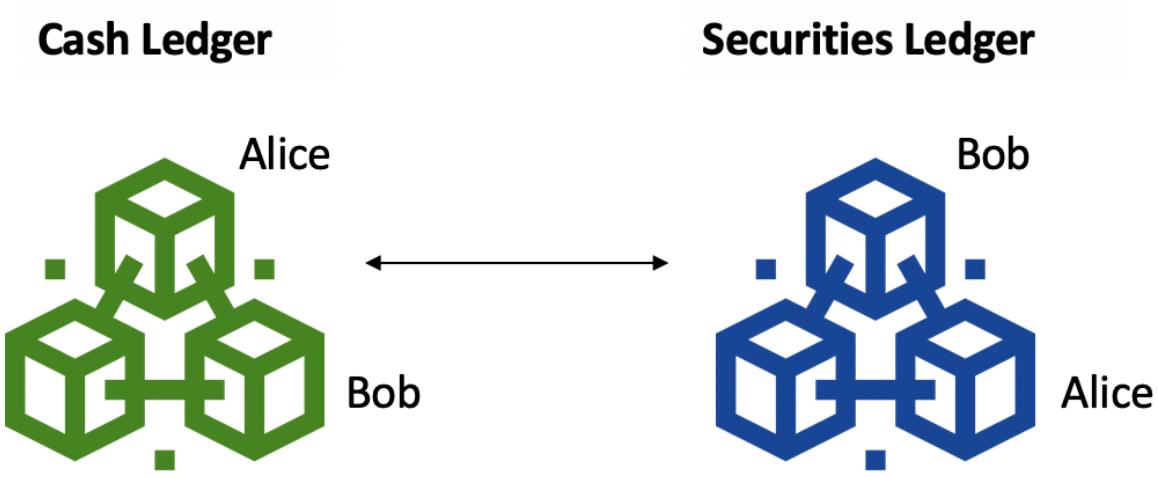

Figure 18 Alice and Bob hold a key pair on both the cash and securities ledger

Alice owns 10 units on a cash ledger (e.g. a cryptocurrency) and would like to trade them for assets (e.g. a security) on an asset ledger, which is a ledger with tokenized (tradable) assets. Bob owns 5 units of an asset on the asset ledger and would like to trade them for cash. As described above, Alice and Bob both has a key pair on each ledger denoted pkA for the asset ledger and pkC for the cash ledger. Alice chooses a secret α and creates two transactions:

1. Transaction 1 sends 10 units on the cash ledger to an output O1, such that the output is only spendable with a combination of α and a signature from Bob's pkC. This transaction is not transmitted to the network at once because if the transaction was transmitted, Alice would have no recourse if Bob drops out of the transaction scheme at this point, resulting in a situation where the funds would be stuck in O1.
2. Transaction 2 allows her to return the funds from O1 to herself if they have not been spent after 48 hours, that represents the locktime that has been already used in transaction with HTLC.

Since the output O1 is controlled by Bob's pkC, this transaction requires a signature from him. Therefore, she sends the unfinished transaction to Bob using a medium of her choice and asks Bob to sign it. Once this transaction has been signed and returned to Alice, she can now safely transmit transaction 1 to the cash ledger. At this stage, there is no risk to either Alice or Bob; since Bob does not know secret α he cannot spend O1, and Alice has a recourse of returning the cash from O1 after 48 hours if Bob drops out of the transaction.

As just happened for Alice, Bob creates two transactions:

3. Transaction 3 allows Bob sending 5 units on the asset ledger to an output O2, which is spendable with Alice's pkA in combination with the secret α which she only knows. If Alice spends O2 she will reveal α, which in turn will allow Bob to spend O1. Similarly to transaction 1, this transaction is not transmitted to the network at once because if the transaction was transmitted, Bob would have no recourse if Alice drops out of the transaction scheme at this point, resulting in a situation where the funds would be stuck in O2.
4. Transaction 4 allows Bob to get back the assets from output O2. This transaction will however only have a locktime of 24 hours. This is to prevent Alice from delaying the spending of O2 until the locktime is about to expire. By introducing this time difference between the locked transactions, Alice can only subject herself to risk by waiting for the locktime to expire, since Bob will be able to return O2 24 hours before Alice will be able to return O1.

Now, Bob can safely transmit transaction 3 to the asset ledger since he can return O2 after 24 hours if Alice does not spend it, and if she does spend it, she will reveal α, allowing Bob to spend O1. The transmitting of transaction 3 concludes the *commitment phase* of the cross-chain DvP scheme. Alice and Bob can now enter the *execution phase.* Alice begins by sending Bob's assets to herself by spending O2 using her pkA and α.

5. Transaction 5: Alice sends this to a new output O3 on the asset ledger which only she controls. As explained, when Alice spends O2 she reveals α on the asset ledger blockchain (publicly readable). Bob now has at least 24 hours (thanks to the time difference between the locktimes) to spend O1.
6. Transaction 6: Just as Alice, he spends O1 by creating a new output O4 on the cash ledger which only he controls and sending Alice's cash to this output.

Transaction 6 concludes the *execution phase* and the DvP has now completed. The figure 19 and 20 shows the scheme just described:

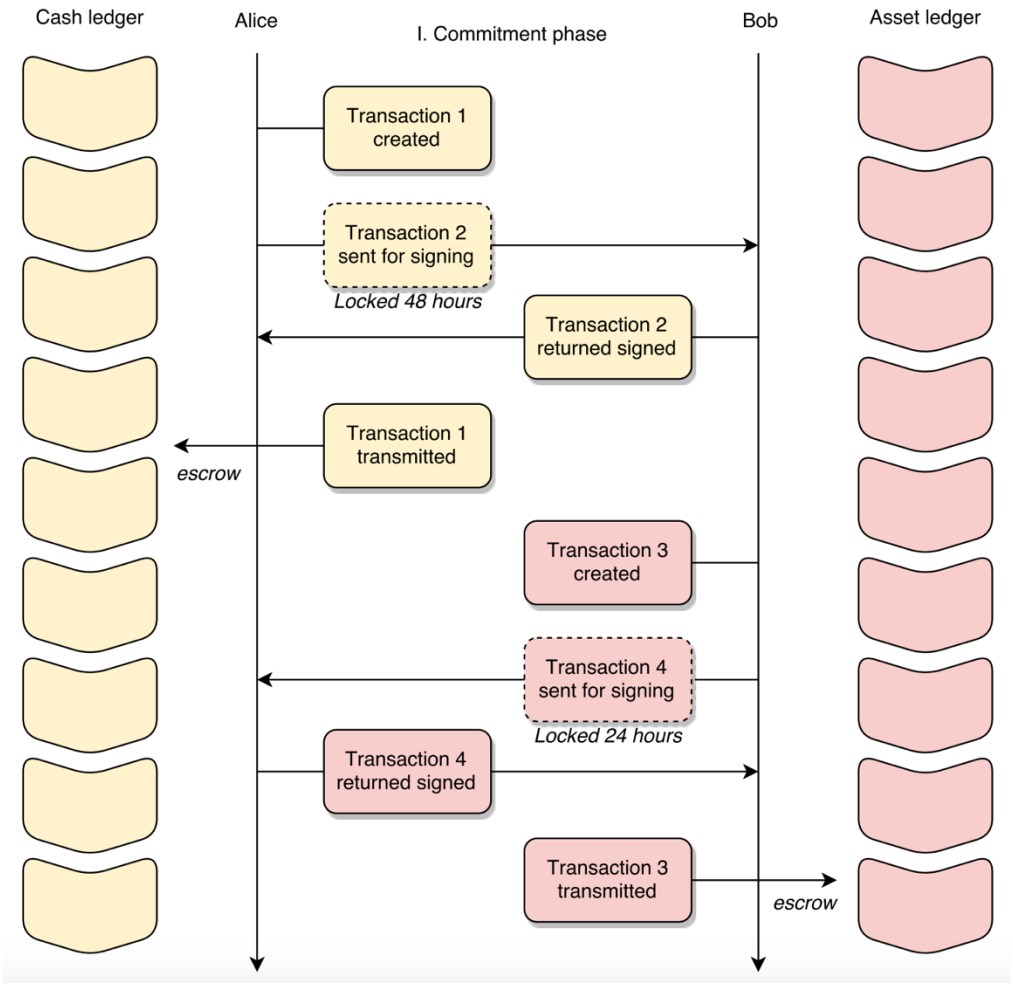

Figure 20 Commitment phase. Alice and Bob escrow assets and cash on their respective ledgers (Source: Department of Electrical and Information Technology Lund University)

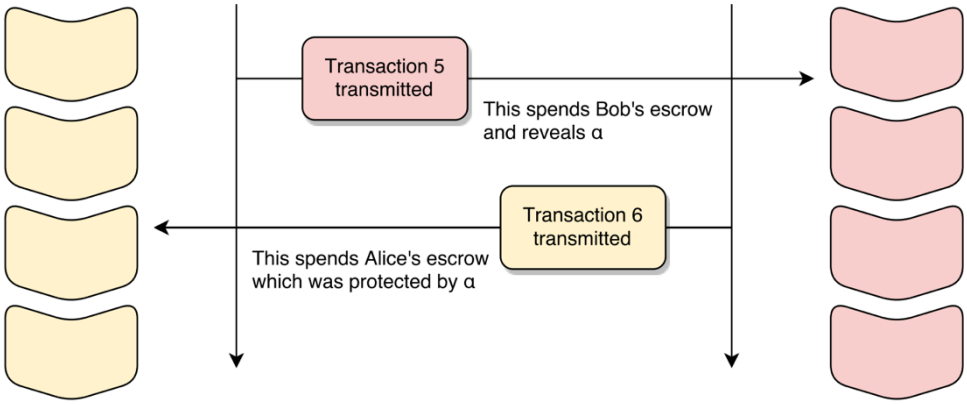

Figure 19 Execution phase. The transaction is completed. (Source: Department of Electrical and Information Technology Lund University)

This scheme is devised such that cross-chain DvP can be achieved atomically. Atomic trades imply that the trade either succeeds completely or fails completely, such that delivery does not happen

without payment and vice versa. In contrast to traditional DvP, this is ensured by the cryptographic features of blockchain technology rather than by the grace of a trusted intermediary.

2.5 Blockchain for credit services

A third macro area of blockchain application concerns the provision of advanced credit services. For example, an institution can take advantage of the programmability aspects that a cryptocurrency offers for the management of multi-actor application scenarios in which the transfer of funds is bound by particular conditions such as:

- Finalized credits: the availability of the funds can be programmed by the institution (e.g. only towards predefined subjects, during a pre-established period of time);
- Provision of trade finance services: the funds are deposited with a guarantee institution and transferred only if the counterparties meet the established contract terms. An example of application is the issue of a letter of credit[29] by an institution to facilitate an international commercial exchange
- Management of loyalty & couponing programs;

This third kind of application might be particularly interesting for small and medium enterprises. Indeed, in many countries Small and Medium-sized Enterprises (SMEs) are the backbones of their economy. Their role is crucial to worldwide economic and social developments, with more than half of the overall world population working in such companies. In the Netherlands for instance, more than 90% of the Dutch companies are SMEs and together they produce 60% of the added value of the Dutch economy (Statista 2019)[30]. SMEs however are confronted with a number of important challenges, including limited access to bank loans, inefficient procedures and lack of information necessary to conduct business efficiently. Since the banking (credit) crisis of 2008, banks are inherently risk averse, so their tolerance for SME lending has become relatively low. Last year's report from the World Bank (Meijer 2019)[31] estimated that 70 percent of small, medium, and micro-enterprises are unable to access the credit they need. While the global demand for SME credit stand at $2,38 trillion, the truth is, only a fraction (about 15%) of businesses actually get the loan that they request from banks.

[29] A letter of credit, or "credit letter" 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 a payment on the purchase, the bank will be required to cover the full or remaining amount of the purchase. It may be offered as a facility.
[30] Statista. (2019). Tratto da https://www.statista.com/statistics/818704/number-of-smes-in-the-netherlands/
[31] **Meijer, Carlo R.W. De. 2019.** A game-changer for Small and Medium-sized Enterprises. *Finextra.* June 2019. https://www.finextra.com/blogposting/17380/blockchain-a-game-changer-for-small-and-medium-sized-enterprises.

2.5.1 Finalized credit

Credit or finalized loan means a form of financing corresponded by an institution to a customer for the purchase of a specific good or service. The use of blockchain allows to constrain the availability of the funds programmatically, by inserting "clauses" within the payment messages in favour of the beneficiary of the loan. Generally, the credit process involves the following steps:

1. The customer must inform the lender in advance by indicating the product or service that he undertakes to purchase together with the supplier's name;
2. The lender issues the credit directly to the supplier indicated by the customer;
3. The customer settles the credit with the lender.

In a normal credit service, it is difficult to constrain the availability of funds with identified subjects. This becomes even more complicated if you want to set additional spending conditions, such as allowing the use of funds only for limited periods of time or when personalized conditions occur, verifiable with the support of proprietary or external data sources. The programmability of the transactions can be exploited, for instance, for the management of payments to suppliers of a certified supply chain. Thanks to the use of a multi-signature address, the customer's transaction is authorized by the lender only and only if destined for a recognized supplier. This is the case, for example, in which a bank that is preparing to finance an organic producer of bio-products, who must purchase raw materials selected exclusively from suppliers belonging to a reference consortium. Furthermore, from the literature researchers have outlined these conditions for a given application to be well suited to use blockchains:

1- Application involves transactions which have multiple stakeholders (parties) in different organizations[32]
2- Data involved in a transaction is distributed across the multiple parties[33]
3- The transactions are decentralized, yet permit instant feedback[34]
4- The application requires strong levels of trust among the parties involved in a given transaction[35]

[32] **de la Rosa, J. L., Torres-Padrosa, V., el-Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L., & Miralles, F**. (2017). A survey of blockchain technologies for open innovation. Proceedings of 4th Annual World Open Innovation Conf. WOIC (pp. 14-15), San Francisco, CA, USA.
[33] **Biggs, J., Hinish, S. R., Natale, M. A., & Patronick, M.** (2017). Blockchain: Revolutionizing the global supply chain by building trust and transparency. New Brunswick, NJ: Rutgers University.
[34] **de la Rosa, J. L., Torres-Padrosa, V., el-Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L., & Miralles, F**. (2017). A survey of blockchain technologies for open innovation. Proceedings of 4th Annual World Open Innovation Conf. WOIC (pp. 14-15), San Francisco, CA, USA.
[35] **Rennock, M., Cohn, A., & Butcher, J. R.** (2018). Blockchain technology and regulatory investigations. The Journal of Litigation, 35-44.

A possible result is that the credit disbursement process can be divided into the following steps shown in figure 21:

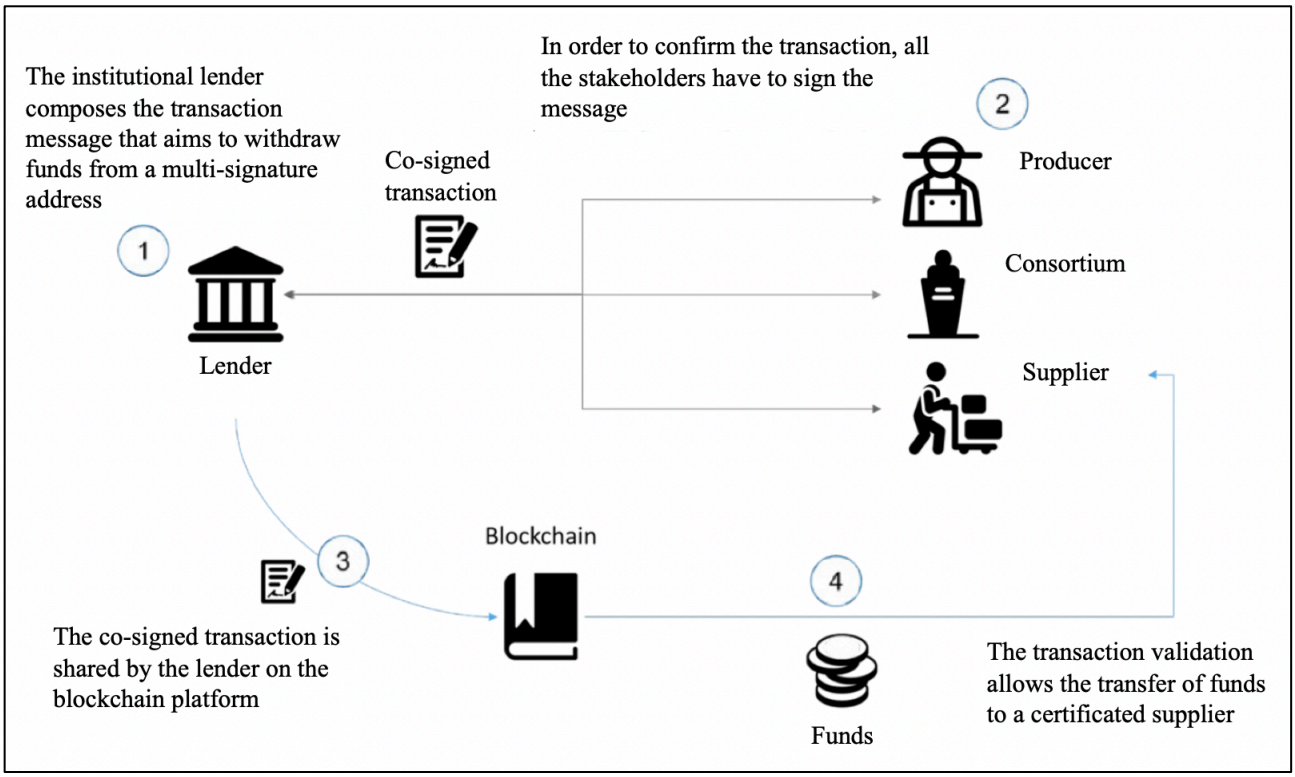

Figure 21 Credit financing exploiting the blockchain technology (Source: McKingsey)

The funds are destined to the supplier through a multi-signature address, binding the availability to the authorization of the stakeholders involved, including the lender, the supply chain consortium and the organic producer. This solution allows effective credit negotiation, as it is publicly certified on the reference blockchain. Moreover, in the same transaction, it is possible to manage the customer's balance to the fund provider or to postpone it later. The main benefits offered by this solution are:

- Effective risk management for the lender: the funds are disbursed to the benefit of a client selected for creditworthiness, and spent by a certified supplier;
- Greater transparency towards all the stakeholders involved, who can check the payment terms on the blockchain.

The immediate effect and result of the use case just described is that the distributed ledger technology might be exploited, according with the four conditions mentioned above, also in a more complicated process in the banking industry as that of the mortgage lending. By definition, A mortgage is a debt instrument, secured by the collateral of specified real estate property, that the

borrower is obliged to pay back with a predetermined set of payments[36]. Mortgage lending process starts with a potential property buyer submitting a mortgage application and ends with the lender's decision. It is a multi-step process and involves multiple parties in reaching the final decision. Down below are described the main participants of a mortgage lending application. It is quite clear that the procedure goes through an important number of different intermediators:

Borrower(s)	The person or persons completes an application for a loan with the intent to either buy a new property or refinance an existing home; and provides documents on request of the loan officer and loan processor
Loan Officer	Interfaces with the borrower to provide rates and determines prequalification
Loan Processor	Starts collecting documents from the borrower to get the loan into underwriting, and initiates orders with other parties such as an appraiser
Underwriter	Reviews borrower's creditworthiness, the property condition, and all documents related to the loan and provides approval/denial based on the mortgage company's underwriting guidelines
Appraiser	Typically, not affiliated with the mortgage company, appraises the value of the subject property
Property Inspector	Hired by the borrower to inspect the subject property for defects or damages to assess required repairs prior to closing
Title Agent	Provides title insurance and acts as the escrow agent that facilitates the final closing of the loan, transfers funds, etc.

Under systems like this, records of data are distributed across multiple parties involved in this common transaction. It is noted[37] that this kind of work that involves intermediaries are often rife with problems resulting in inefficient work that is liable to cause the following problems: adding cost through fees and delays, creating redundant through and onerous paperwork and opening up opportunities for fraud and crime.

Following are described a sequence of steps for managing a mortgage lending application with the use of a DLT:

Step 1. Distributed ledger transaction is created for the applicant. A record of necessary fields is created to enter data about the application. This is named the "genesis block" (Michael Nofer 2017)[38], even shown in figure 21.

[36] https://www.investopedia.com/terms/m/mortgage.asp
[37] **Tapscott, A., & Tapscott, D.** (2017). How blockchain is changing finance. Harvard Business Review, 2-5.
[38] **Michael Nofer, Peter Gomber, Oliver Hinz, Dirk Schiereck. 2017.** *Blockchain.* Springer Fachmedien Wiesbaden, 2017. pp. 2-4.

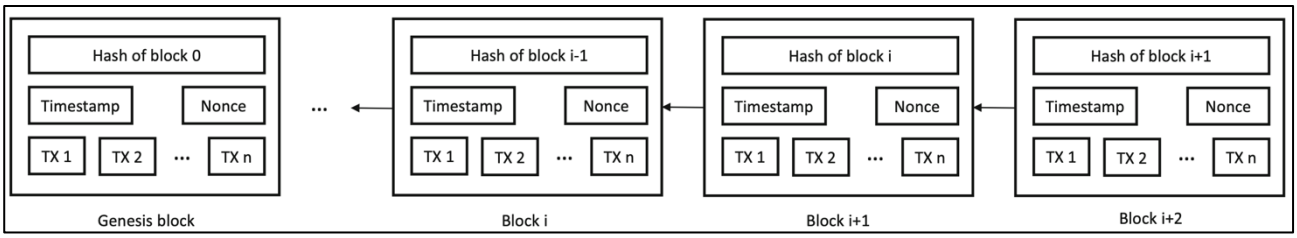

Figure 22 An example of a transaction (TX1) in a Genesis block (Source: How Blockchain Will Change Organizations, Tapscott)

Step 2. Checking borrower information, DLT is updated with borrower information and decision is made to pre-approve the mortgage. A note to be made here is that pre-approval does not guarantee final approval of loan as final approval is contingent on other additional factors as will be explained later. DLT is updated with the decision made and the digital signature of the authority who made the decision.

Step 3. Supporting documents collected from the borrower and other borrower information are added in the DLT. The supporting document could include credit history, proof of ability to pay the mortgage payment, employment record, prior years earning, debt/earning ration and other information. All information is entered in the DLT and secured through public and private keys.

Step 4. Review of all documents, checking underwriting guidelines and recording in DLT. This step works as a validating process as the underwriter validates the submitted document and records the findings in the DLT.

Step 5. Information sent to the appraiser, appraiser estimates the value of the house, creates appraisal block in the DLT. The appraisal often includes comparison with other similar properties and the valuation decision.

Step 6. The building inspector inspects house and record information in a block in DLT. The inspection checks the house for any damages that may affect the value of the house. The intent at this step is to grant a mortgage amount that is consistent with the value of the house. Notes from the inspector included and all information recorded for the property inspector record in the DLT.

Step 7. This is the final step in the mortgage lending process and at this point, a decision is made and if approved the funding for the mortgage is granted. The decision is made after all involved parties complete their transactions, record them in the DLT and approve them with their digital signature. Both public key and private keys are used and are reflective of the development, thus the consensus model is applied here in the mortgage lending application process.

The technological complexity of the use case just illustrated includes the multiple signature management and requires the use of a communication channel parallel to that used for sending and receiving blockchain transactions; this dedicated channel, for example secure 'Http' communication, allows actors to exchange the message privately and co-sign it.
Lastly, the use of advanced blockchain components can enable the development of unprecedented credit instruments for the AS-IS scenario, binding the availability of the funds disbursed to personalized rules.

2.5.2 Trade Finance

In general, financing and risk mitigation services belong to the trade finance category for counterparties involved in a commercial exchange. A typical process in the trade finance sphere is, for example, intermediation that facilitates the exchange between an online seller and a customer, or, from a B2B perspective, the service that allows two commercial parties to complete a transaction securely. In both cases, the intermediary of the exchange is the supplier of the escrow[39] service which enables the execution of the transaction only when both parties comply with the terms of the underlying commercial agreement. Trivially, this translates into verification by the intermediary that the buyer has made the payment for the goods exchanged, and that the seller has delivered the product to a courier for shipment.
With the introduction of a dedicated blockchain solution, the counterparties define the terms of the exchange and deposit them on a permanent information layer. The logic defined within the smart contracts[40] establishes shared and unchangeable criteria for conducting the exchange. For example, the integration of a multiple signature system allows to constrain the transfer of goods and the execution of payment to deposit service providers. Finally, in a more advanced scenario, it is possible to enable automatic execution of operations in response to the state of delivery of the goods, monitored with a system that certifies the passage of the asset along the distribution chain on the blockchain.

[39] Escrow is a legal concept describing a financial instrument whereby an asset or escrow money is held by a third party on behalf of two other parties that are in the process of completing a transaction. Escrow accounts might include escrow fees managed by agents who hold the funds or assets until receiving appropriate instructions or until the fulfillment of predetermined contractual obligations. Money, securities, funds, and other assets can all be held in escrow. A similar process would be a fully funded documentary letter of credit. It is often suggested as a replacement for a certified or cashier's check.
[40] A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. The code and the agreements contained therein exist across a distributed, decentralized blockchain network. The code controls the execution, and transactions are trackable and irreversible.
Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism.

In a B2B context, the most popular tools are the *letter of credit* and the *escrow account*. These are different contractual objects: if for the letter of credit the condition to be verified is the shipment of the goods, in the case of an escrow account a prompt verification of the quality of the supply is also required. For the purpose of the research, the analysis is limited to the case of the letter of credit, a bank transaction also called documentary credit. This particular service involves the interaction of two types of actors: the exchange counterparties and the bank intermediaries. The process is generally divided into the following phases:

1. Conclusion of a sales contract between buyer and seller in which terms and conditions of the commercial exchange are established.
2. Issue of the letter of credit from the buyer's bank to the seller's. With this operation the issuing bank guarantees the payment if the shipment is made by the seller.
3. Once the shipment has been carried out, the seller delivers the bill of lading received by the courier to his bank.
4. Once the shipping terms are satisfied, the bank pays the seller the payment previously guaranteed by the letter of credit.
5. The bill of lading is transferred to the buyer who can thus complete the collection of the goods sent to his address.

Although the service significantly reduces the risk of counterparties, the use of paper documents for notification considerably lengthens the process times. This may constitute a liquidity problem for the buyer whose payment funds are "frozen" in a guarantee deposit for the duration of the operation.

Recently, HSBC and Bank of America Merrill Lynch venture and financial technology consortium R3 separately reported that they have been able to generate ways by which Blockchain technology can be used to simplify trade finance processes. Furthermore, the two banks highlighted that they had partnered with the Infocomm Development Authority of Singapore to emulate a transaction of Letter of Credit. Thus, Blockchain technology is important for use in the area of trade finance as it offers solutions which include the ability to trace as Blockchain provides genuineness of products in the supply chain and the ability to be transparent as Blockchain guards against fraud and saves transaction reconciliation cost.

In June 2017, Michael D. Dowling, Alexander R. Thompson, Axel Levitan and Robert A. Severino applied for a patent named “International trade finance blockchain system”. The invented method includes generating a blockchain-based letter of credit (“BLC”) relating to a contract for a trade transaction between a seller and a buyer. The BLC defines documentary and supply chain

flow payment trigger events. The BLC is stored and accessible via a blockchain. A plurality of documentary flow events related to the BLC are tracked and recorded on the blockchain and are linked to the BLC. A plurality of supply chain flow events related to a physical status of a good involved in the trade transaction are tracked and recorded on the blockchain. Each of the plurality of supply chain flow events are linked to the BLC. Payment for the contract for the trade transaction is transferred to the seller in response to detecting occurrence of both of the documentary and supply chain flow events corresponding to the respective documentary and supply chain flow payment trigger events. Down below is shown a scheme of the payment flow: it is a block diagram illustrating a system (100) structured to perform a commercial trade finance transaction using a BLC. The system includes trade finance blockchain computing system (102), a trade finance blockchain (104), a buyer (106), an issuing bank (108), an advising bank (110), a seller (112), a good (113), a freight forwarder (114), and a shipping company (116), each being in operative communication via a network (118).

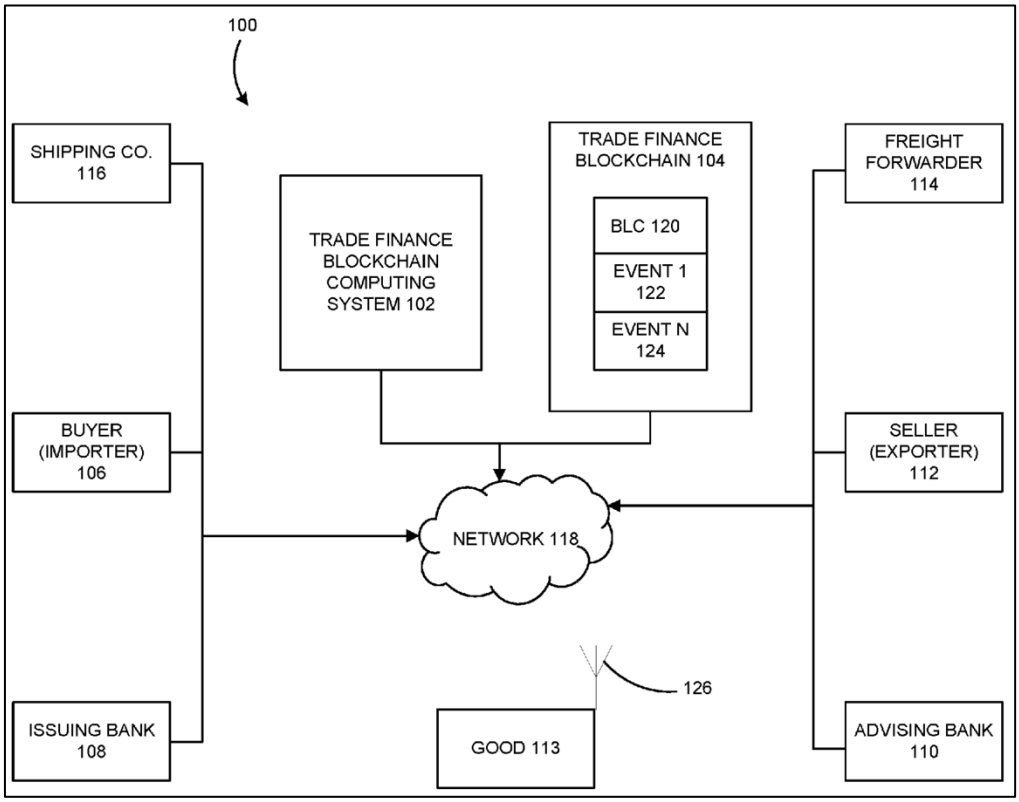

Figure 23 Scheme of the International trade finance system according to the patent application of Dowling et al.

With respect to the use cases above described, for trade finance the following have to be considered:

- Area of application: the scenario that has been mentioned requires that the solution be adopted by different banks;

- Technological complexity: the components used provide for the use of multiple signature technology and the integration of dedicated smart contracts;
- Complexity of switches: the switch process is expensive since multiple institutions are required to replace the current management system with a new infrastructure. As in the case of intra-bank transfers, if the application is internal to the domain of a single institution, the complexity of the switch is moderate and the times of realization faster.

2.5.3 Know Your Customer (KYC)

Financial organizations around the world are responsible for conforming and reporting on a number of business requirements from their local authority. One of the requirements, "Know Your Customer" (KYC) is incredibly time consuming and lack the automated customer identification technology and integration essential by teams to economically execute their work. Blockchain could provide a digital single source of identity data that allows for the flawless exchange of documents between banks and external agencies. This would possibly result in automated account opening, reduced resource and cost, though preserving the privacy of data that is lawfully required.

Usually the Know Your Customer verification process is associated with the subscription of financial services such as the opening of a current account or the purchase of an insurance product. In particular, this verification allows the service provider to:

- Know the true identity of the customer;
- Define a risk profile;
- Protect yourself if the customer uses the services offered for criminal purposes.

The adoption of a blockchain ledger allows identity managers to certify the attributes that make up the identification profile of each user on a decentralized register. This is particularly advantageous for the service providers, who, after being authorized by their customers to access the digital identity, complete the adequate verification activities independently. As briefly mentioned above, the KYC process generally consists of a series of verification activities that cannot be avoided by the institutes, envisaged by current international and national regulations on the prevention of money laundering and terrorist activities.

The documents required by law are generally proof of identity (e.g. identity card, passport) and proof of domicile (e.g. electricity bill). Sending the documentation, usually in paper form, is often a burdensome process, which on the one hand weighs down the user experience, on the other it slows

down the activation of the service, tied to the receipt of the documentation and the appropriate operations verification to be fulfilled towards customers.

The adoption of a blockchain system for the management of KYC verification allows to manage digital identities in a decentralized way, facilitating the individual activities of the process and offering greater independence to individual actors. Generally, three types can be identified:

1. **Identity manager**: an entity that recognizes the individual and issues him with digital proof of identity on the blockchain.
2. **Service Provider**: a company that provides a service for which user identification is required.
3. **User**: the subscriber, whose information is certified by one or more managers.

In the scenario, the customer has the control of his information, which is revealed to the service provider only during the subscription phase. Furthermore, thanks to an open source identity management application, it can choose which attributes to show and which to keep secret, storing separately the information that makes up its digital identity on the blockchain. Initially it will be easier to create an “internal” solution to be tested in corporate groups in which identity managers and service providers coexist. The implementation will be extendable later to a more systemic level in which actors belonging to different companies can relate to each other. A collaborative solution of this type allows to reach higher efficiency levels only with the adequate support of regulatory bodies: in the first instance, therefore, a regulatory effort is needed that incentives the different players to cooperate on the basis of common standards and best practices.

The flow of the verification process can be summarized in three main macro-phases: Registration, Submission and Verification, shown in the scheme in figure 24.

In the flow, the manager initially takes care of certifying on the blockchain the data that make up the user's digital identity, to whom control of the information is transferred. The data are stored on the ledger in an "encrypted" way and can be read by the service provider only at the time of subscription to fulfill the due diligence activities.

The main benefits of this solution compared to a traditional system consist in:

- Improved user experience: it is no longer necessary to send documentation, often in paper form, to activate the service;
- Reduction of times / costs for the service provider: direct access to data is now possible, subject to user authorization;
- Establishment of a collaborative system between stakeholders, with a reduction in brokerage costs and faster negotiations.

The same process can be replicated, with the necessary modifications, for the provision of atomic attributes by public or private bodies: the communication of information by an authoritative subject further enriches the user's e-identity and facilitates the subscription of heterogeneous services. All this constitutes an interesting business opportunity for recognized organizations that can become selected big data suppliers, accessible through an API service. For example, a university can certify a student's degree mark, or a banking institution can communicate the credit rating of one of its customers.

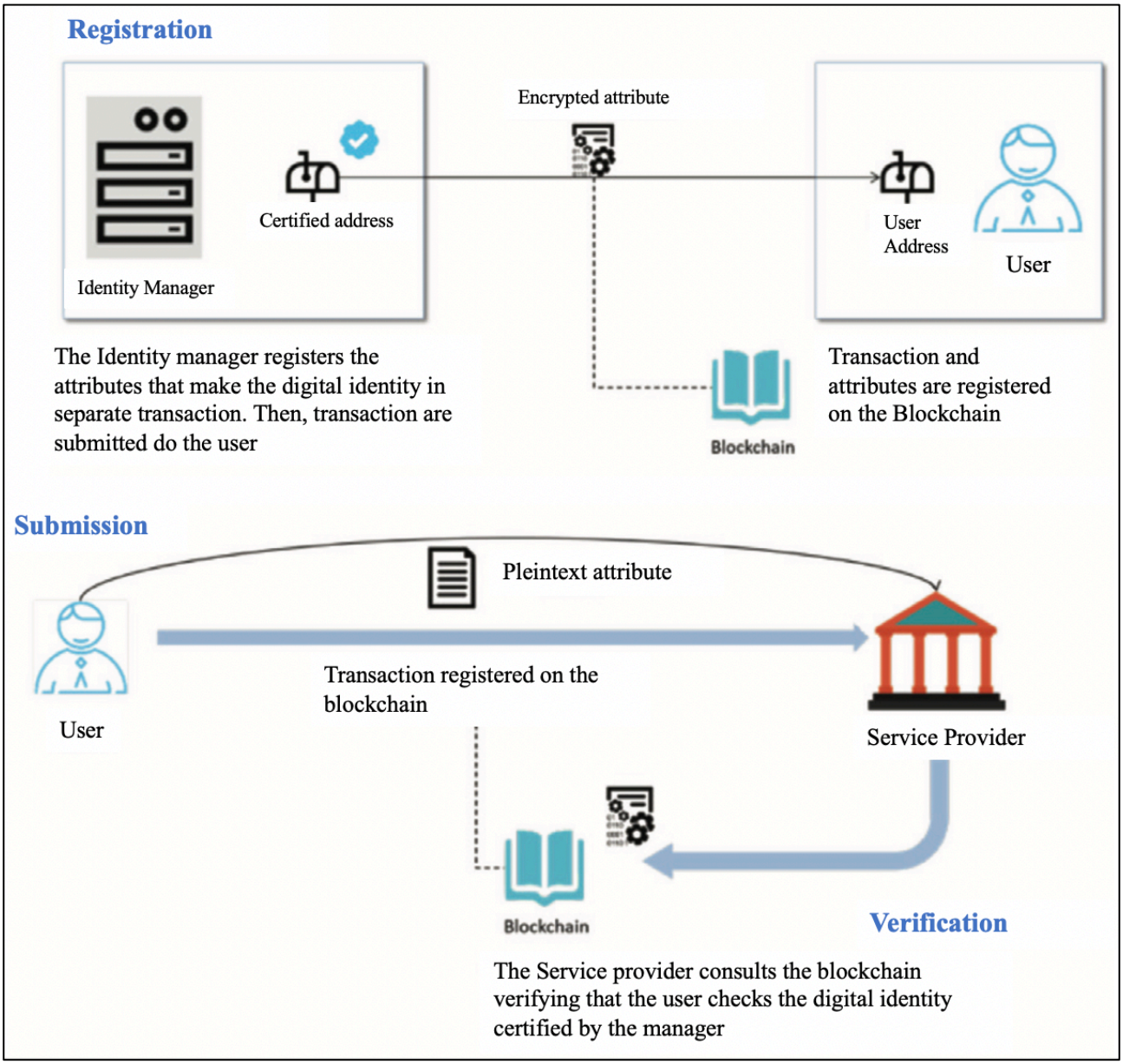

Figure 24 Activities for the management of digital identity with blockchain technology (Source: Reply technology)

The system just described acts as an interoperable and efficient solution compared to today's digital identity systems or competing digital implementations, still tied to proprietary management systems. De-centralized management and the possibility of extending the profile with new attributes open up new business opportunities for all potential identity providers. The blockchain solution clearly shows a disruptive nature and necessarily requires progressive adherence to the new standard by a wide and transversal system of actors, from identity providers to support technology vendors, up to user services.

3 Conclusion

In this final section the use cases illustrated in chapter 2 are classified by each macro process area in a two-dimensional matrix that has been used to graphically check the effectiveness of each use case. Before going into the detail of the representation, it is useful to introduce the two dimensions used, business impact and regulatory compliance, and to report the strategic guidelines for implementation oriented to a permissionless or permissioned blockchain.

A. Business Impact

Taking into consideration the value of the innovation type, it is possible to register two distinct polarities for this dimension:

- Business impact: "*Disruption*", the introduction of the solution profoundly redefines current processes, enabling the activation of new differentiated services for customers and new business opportunities for service providers.
- Business impact: "*Optimization*", the application does not encourage the development of new categories of service, but only contributes to increase the efficiency of current processes.

B. Regulatory Compliance

The second dimension looks at the level of needed compliance recorded for the use case in question compared to current regulations. In particular, the dimension becomes "High" if the as-is regulatory components facilitate the application of the solution; "Low" if, on the other hand, they involve some obstacles. The main regulatory components are the following:

- *Registration of property and intellectual property*: regulatory compliance is low if for the use case in question it is not possible to disintermediate the certification body.

- *Privacy*: there is a regulatory obstacle if the service provided requires the processing of sensitive data and if adequate verification procedures are necessary with respect to the data provided by the user.
- *Antitrust*: the regulatory barrier arises if the blockchain solution gives rise to monopoly situations, achieved both through the establishment of exclusive groups that define new operating methods, and with the definition of smart contracts for the use of a few individuals and anti- competitive for the remaining actors.
- *Anti-Money Laundering*: the use case involves the management of wallet components for the users of the application and exposes the organization to the risk of money laundering or financing of illegal activities.

C. Implementation Strategy

The approach to the use of technology can be diversified. The main strategic assessment is linked to the adoption of a completely open public system - permissionless - or a private solution in which there is a centralized control of the infrastructure. In the first case, as it was described in the second chapter, the information is stored in a register distributed on the nodes of a pre-existing P2P network. Unlike a permissioned system, there is no administrator who recognizes the participants in the blockchain layer and associates specific permission levels for each of them. It is important to underline how in this case the blockchain infrastructure and the application layer are clearly separated and participated by two distinct classes of subjects, each with its own business and cost model.

On the one hand, miners provide their computational power to process new transactions and update all copies of the ledger consistently. Furthermore, independent organizations develop applications above the blockchain and pay the miners for their execution based on the quality of the service requested: for example, faster processing, or greater use of resources, require a service fee higher for each transaction. This is the actual blockchain concept, in which the trust function is performed by a peer network, in which the nodes interact only by virtue of the reference open-source protocol. Choosing a permissionless system is preferable when:

1. The data must be stored permanently, and the transactions must be irreversible;
2. Nodes must have equal write rights, without the possibility of checking the permissions of each participant.

Permissionless systems like Bitcoin are to date blockchain implementations with the highest number of nodes and longevity. The high diffusion guarantees a high permanence of the data and

makes it practically impossible for an external attacker to change the transaction history to his advantage. At the same time, the use of a public system for B2C or B2C services in production entails for the institution the management of the cryptocurrency of the permissionless system considered. In fact, the purchase of cryptocurrency such as bitcoin or ether is necessary to operate on these networks.

The direct management of cryptocurrency involves compliance with the anti-money laundering legislation in force for the jurisdiction of reference. In general:

- If the institute operates exchange services directly between fiat currency and cryptocurrency, it must proceed to Know Your Customer (KYC) verification for all subjects requesting the services provided.
- If, on the other hand, the institution relies on external exchange platforms, the institution will take on the role of customer of the exchange and therefore will have to undergo firsthand the KYC verification operations and subsequent due diligence by the platform used.

On the contrary, the use of permissioned systems does not require the organization to meet specific compliance requirements. In fact, a private system does not require the purchase of cross-currency from an existing exchange market, but manages the assets generated and the utilities in a totally proprietary and closed way with respect to external currency systems.

In the case of a private blockchain, or permissioned, only recognized entities can participate in the system, whose permission levels for access to information and writing to the register are configured by a system administrator. This configuration may be suitable for a group of stakeholders who operate concurrently on the register, after signing a common policy. Probably, the policy will report the access requirements to the system, the permission levels of each individual participant and the methods of development and management of the support information system.

Here the business risk is not strictly delegated to a third party but shared between recognized actors who, thanks to an ad-hoc blockchain system, mitigate the possibility of information loss or tampering and eliminate data reconciliation activities. Supported by a blockchain implementation, the participants can develop on-top applications which, taking advantage of the trust layer established by the blockchain infrastructure at the base, offer value-added business functionalities, such as sharing services or applications for booking. In summary, a permissioned system is preferable when:

1. The transparency and audibility of the register must be limited to a group of identified subjects;
2. The participants are not all at the same level, but a permit system establishes a precise hierarchy between the network nodes;
3. The adoption of a permissionless system does not allow to operate with the desired latency and throughput levels (number of transactions per second).

Intra / interbank transfers

The definition of common standards for the transmission of payments is an important advance in terms of interoperability. At the same time, the definition of a more efficient operating model controlled by a consortium limited to some banks can undermine the level of competition in the banking sector. As anticipated, in this case the method of adopting the technology is the use of a permissible blockchain accessible by all members of the consortium.

Trading

The use of blockchain as a digital notary allows actors to certify information according to common standards. From a regulatory point of view, there are no particular obstacles for implementation which in this case would involve the use of a permissionless register.

Post-trading

In addition to the certification aspects, the possibility of automating financial transactions on the basis of operational rules encoded within smart contracts is added. The degree of automation and the customization possibilities just introduced promote the supply of new financial products and services. Here the blockchain solution potentially impacts a large set of actors, from banks to service providers (eg clearing, custody, etc.). Consequently, regulatory resistance (EMIR, MIFIR, SFD, CSDR) that could hinder a sectoral implementation of the solution cannot be excluded. The reference implementation model is represented by a permitted blockchain accessible only by the players in the supply chain.

Finalized credit

By binding the spendability of the funds with coded rules in financial transactions, it is possible to significantly limit the risk components associated with the disbursement of the loan. At the same time, a complete application of the use case involves sending funds in the form of cryptocurrency,

an activity currently not recommended by the supervisory authorities. In this case the implementation choices are oriented to cryptocurrency supported by permissionless blockchain.

Trade Finance

In addition to providing a decisive contribution in terms of risk mitigation, the solution makes it possible to make the execution of individual transactions more efficient thanks to smart contract components. From the regulatory point of view, it is necessary to verify the reference directives for the international regulation of documentary credit and the letter of credit (eg NUU rules established by the International Chamber of Commerce, or ICC). The reference system can be a permissioned blockchain reserved for a community. If, on the other hand, we consider a wider application perimeter, it is possible to refer to a permissionless system that also supports smart contract components (eg Ethereum).

Know your customer (KYC)

By introducing new methods for the registration and decentralized management of the digital identity, the solution favors the entry of new identity providers and makes a decisive contribution from the point of view of efficiency and interoperability. In fact, sharing a permissionless register of e-identity profiles entails the adoption of common standards for access to data and favors the reduction of the due diligence activities that precede the subscription of a service. From a regulatory point of view, a strongly impacted component is certainly that relating to anti-money laundering. In fact, the solution stimulates the definition of new ways of recording customer information for identity providers, together with the optimization of the due diligence processes, now conducted collaboratively between service providers (e.g. different financial institutions).

Once assessed all the use cases with respect to the "Business impact" and "Regulatory compliance" dimensions, the conclusion of this dissertation rely upon a graphical representation of a classification that is shown down below in a matrix scheme. Furthermore, in accordance with the guidelines just described above, the third dimension ‘implementation strategies’ indicates whether the specific use case lends itself more to the adoption of a permissionless or permissioned blockchain solution:

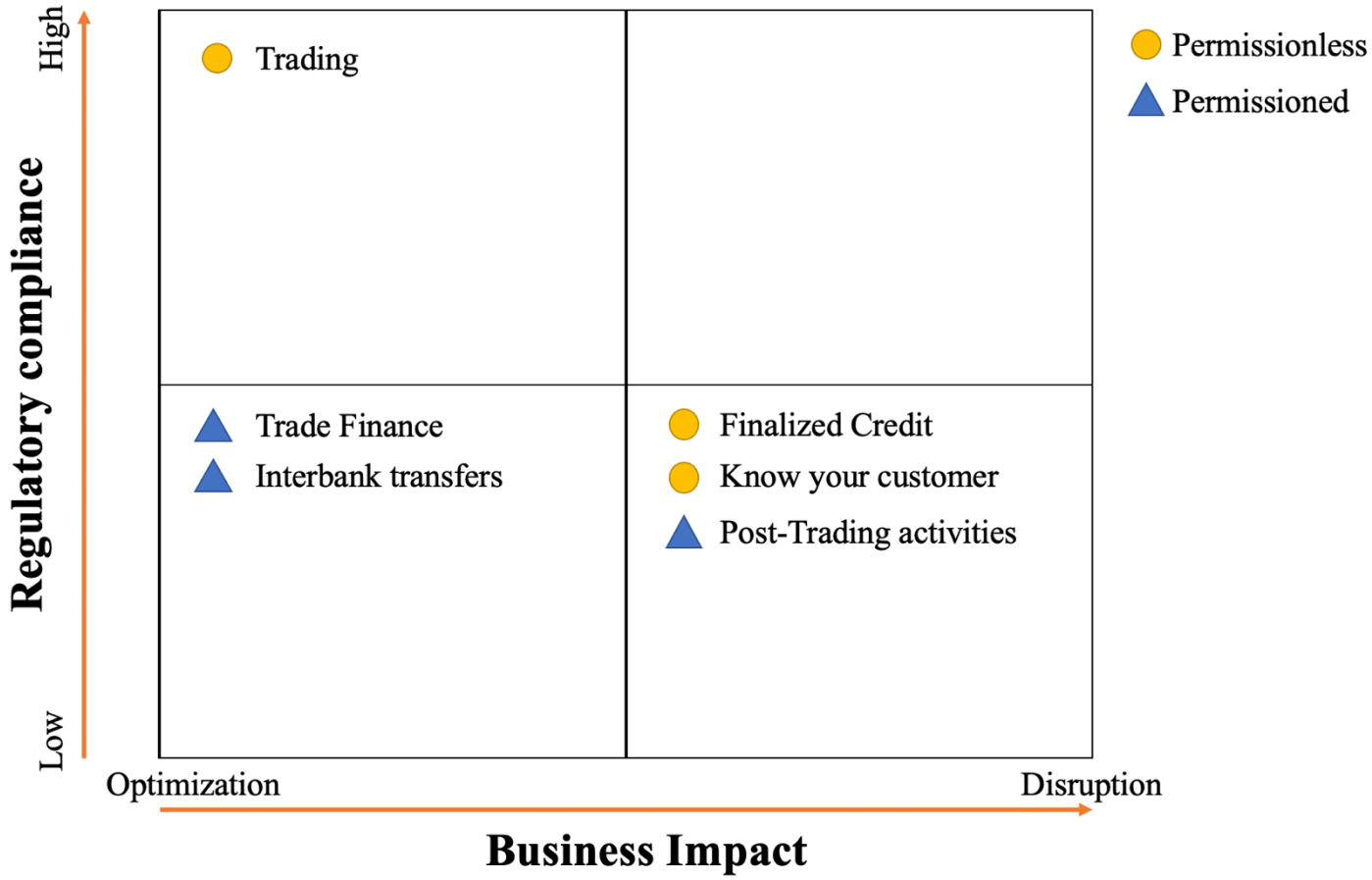

Figure 25 Matrix scheme resulting from the analysis of five different blockchain use-cases

Two main points of attention emerge from the matrix:

- In the use cases with a "Disruption" business impact, the regulatory components to be evaluated are numerous and involve some obstacles. Consequently, conducting "regulatory sandbox" type experiments, with the supervision and facilities of the regulator, can result in a useful approach to the implementation of the use case and its modeling with respect to existing regulatory constraints. In addition, a controlled experimentation phase allows the regulator to evaluate possible regulatory adjustments based on the recorded business impact.
- Applications that require the use of blockchains as efficiency drivers (Optimization), represented here by "interbank transfers" and "trade finance", likewise require a regulatory verification with respect to the intercepted components. However, autonomous testing, internal to a single bank, is initially an effective approach to test the degree of efficiency brought by the blockchain solution without clashing with the regulatory constraints inherent in a systemic application.

3.1 The disruptive implication for financial regulators

In this new phase of financial innovation coming along with regulatory dynamics, this section aims to propose that disruptive innovation could provide a framework for considering the regulatory implications of Fintech deeply discussed in the previous chapters. It is helpful to develop a high-level view that may produce some insights for considering whether and to what extend regulatory intervention in financial innovation should take place.

As already cited, the types of innovation seen in chapters one and two are related to what has been described by the literature as disruptive innovation. With disruption, market leaders may fall behind, or even exit the industry, while leadership may be achieved by firms that previously had a minor role, by new entrants, or even by startups[41]. This framework may be more specifically understood as the development of innovation that first takes place at the low end of the market, which does not immediately threaten incumbents as it is just ra weak substitute. The innovation however distinguishes itself by new performance criteria to the market, such as convenience and portability, lower price and costs (e.g. lower costs of financial intermediation for trading securities explained in paragraph 2.3), or ease of use (e.g. the extremely user-friendly front end of new financial application for personal finance management). The gradual uptake by the market and development of economies of scale allow the innovation to become dominant, disrupting and replacing incumbents.

The result of disruption might be fundamental for financial regulator that look to three main characteristics of disruption that fall on *change* with *substitutive potential* that ultimately produces *structural impact*.

First, regulators should understand what kind of change in performance or value the financial innovation has been included in the market. For instance, in relation to substantive change, regulators should be interested if:

- New channels for meeting financial needs are being created, and where new, unlicensed intermediaries are introduced in the landscape;
- New financial needs are being defined and framed, and the market segment that is most impacted;
- Existing channels for meeting financial needs are being changed in forms or interfaces, and whether such forms or interfaces are captured within existing regulation;

[41] **Montagna, Marco Cantamessa Francesca. 2016.** *Management of Innovation and Product Development.* s.l. : Springer, 2016. pp. 13-15. 978-1-4471-6722-8.

- There are changes in legal technology, such as in defining legal relationships, property rights, enforcement rights, in order understand if any substantive change has indeed come about in banking or investment paradigms

Next, the disruptive innovation can be examined by regulators that take in consideration whether the change is significant enough to be monitored and considered for regulatory initiatives. The Fintech innovation anticipates a form of stealthy but dominant substitution. However, even if a change does become fully substitutive, since this significant migration affects the part of financial end-users, it is quite important that regulators should have great and precise attention.

Finally, regulators need to consider the structural impact of potentially substitutive forms of change. This is not easy to foresee especially if the change is only emerging. A typical example that has been discussed in chapter one is peer-to-peer lending and whether it will become substitutive for traditional bank credit channels. The market is still quite small compared to traditional bank credit at the moment, and the structural impact of such an industry is hard to foretell. However, the information analytics techniques and the investment model underlying the peer-to-peer lending products can become substitutive forms of change for how credit is created in the future.

3.2 Outlook of the next future: from product to customer and from customer to platform

As Fintech grew, it became increasingly more and more difficult to distinguish the hype from reality. Over the last several years, blockchain and crypto assets, roboadvisors and neobanks, and many of other digitization symptoms have become even more popular among trade media. Large global banks spun up corporate venture arms and digital incubators, investing in, acquiring, or copying solutions from emerging companies and start-ups.

The reasons are quite straight. First of all, finance is much simpler than most people think it is. Just like any other industry, there are factories that have the scope to produce products: banks that hold interest rate deposits or investment managers who make investment funds, or lenders and insurers that underwrite some risks for customers with capital. On the other hand, there are stores that sell the product: bank branches, financial advisors, insurance sellers or loan agents. Between these two extremes there exists a complex value chains of human beings, balance sheets and software, intertwined by industry rules and habits. But at the end, customers visit a shop and buy some financial products.

Digitization is taking place along the entire value chain. In the front office, consumer relationships are shifting from physical conversations to cell phones. Symptoms include European neobanks like the Revolut, in which a customer can easily open his fully digital bank account in just 10 minutes, or American robo-advisors like Betterment or Asian insurtechs like Ping An. More speculative interfaces use machine learning and natural language processing to generate chat and speech, instead of allowing people to interact with a live agent. The solutions offered with the digital revolution are a good start, but they are not the destination of the wave of Fintech. There is a direction that is guiding users all over the world to approach their bank account, and it is the one already introduced by the giants of distribution with their platforms. WeChat users can send text messages, buy, send money and invest from the same phone app. In the most popular platforms, which are provided by Google, Facebook, YouTube or other, the wide offer of services to the customer is fundamental. Financial products will be simple additional features that will lie within these service platforms.

Concerning the use of blockchain in financial services, the involvement of new stakeholders will be fundamental. Every manager, consumer, founder, investor and enthusiast should understand the speed with which banks will start implementing blockchain-based solutions to improve efficiency, security, competitiveness and how their consumers and shareholders interact within their corporate ecosystems. To get deeper in this concept, it is worth to explore the current position of the technology on the S-curve of adoption. In studying every industry, if it identifies a relevant performance indicator for its products, the evolution of this indicator will not proceed in a straight line but follow a sequence of s- curves. S-curves show that, when a technology emerges, performance is usually quite low, until a sufficient degree of maturity is reached. At this point, performance starts growing at a significant speed, until it eventually reaches a technological limit, (a performance level that cannot be overcome due to limitations that are intrinsic to have to embrace new technical solutions). The timing aspect is also important, since a premature investment may lead to unattractive returns from a financial point of view or — even worse — to erroneous choices in technology[42]. Throughout the 20th century every major mass-market technology that was near-universally adopted has exhibited some form of an S-curve, as indicated in the chart below where on vertical axes is represented the percentage of US citizens adopting the technology innovation. S-curves are becoming more compressed as technology advances, leading to more pronounced vertical growth adoption phases.

[42] **Montagna, Marco Cantamessa Francesca. 2016.** *Management of Innovation and Product Development.* s.l. : Springer, 2016. pp. 31-33. 978-1-4471-6722-8.

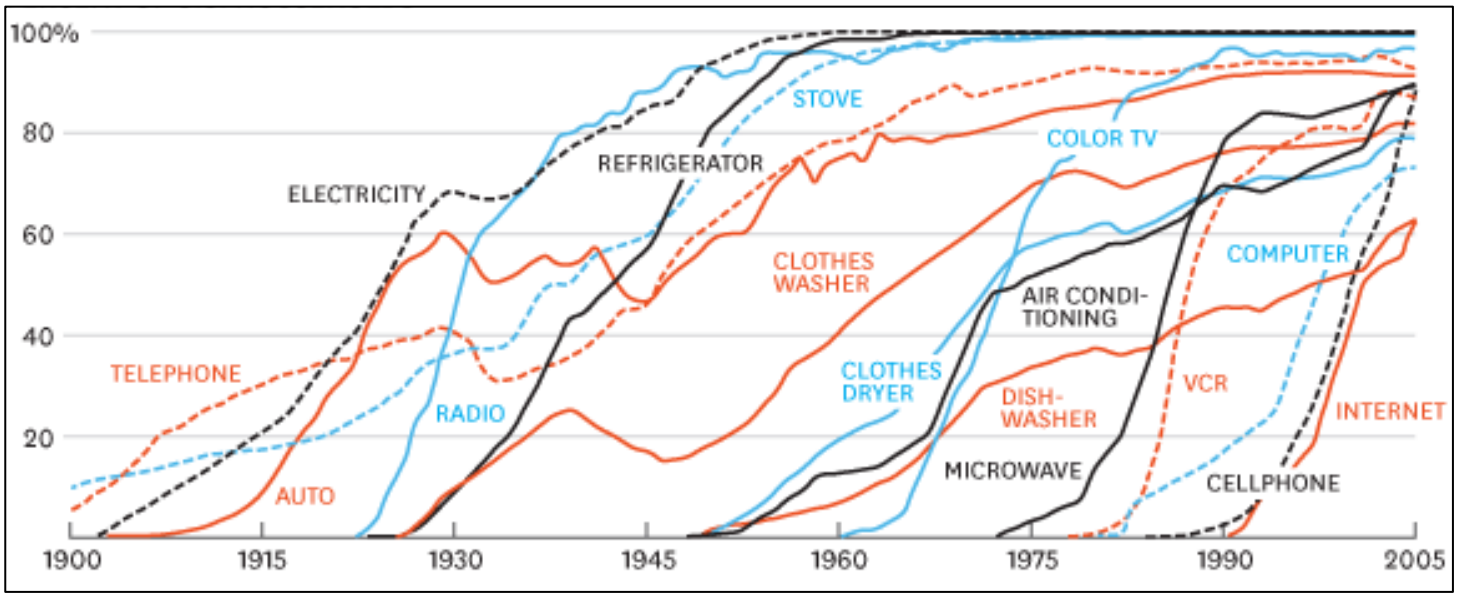

Figure 26 Consumption spreads faster today. Source: Michael Felton - The New York Times

Even though blockchain has emerged in a stadium of aggressive competition and rapid technological improvement, there is still much room for improvement in the foundations of the technology. To go deeper, it is worth to analyze the four phases a typical adoption of technology goes through: single use, localization, substitution and transformation[43]. Each of these phases is characterized by the novelty of the technology and the complexity of the coordination efforts it requires to make it workable.

Concerning the novelty, it mirrors the degree to which a technology is new to the world: the more novel it is, the more effort will be required to ensure that users understand what problems is solves. The second dimension is complexity as the level of ecosystem coordination involved: it might be related to the number and diversity of the parties that need to gather knowledge to get value from the technology itself.

[43] **Marco Iansiti, Karim Lakhani. 2017.** *The truth about blockchain.* s.l. : Harvard Business Review, 2017. pp. 7-8. R1701J.

At an overall view, it is quite immediate to understand that technologies that are low in novelty and complexity gain acceptance first. On the other hand, applications high in novelty and high also in complexity take decades to evolve but can transform the economy.

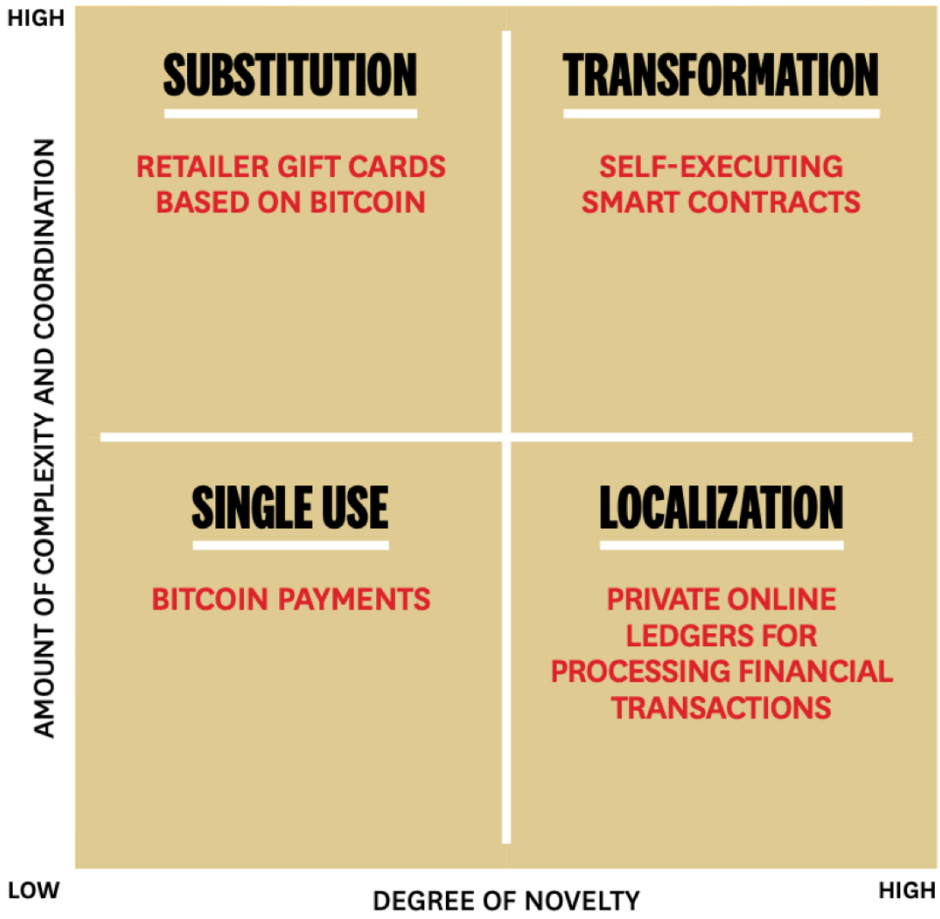

Figure 27 The four phases of application adoption. [Source: Harvard business review]

The details of each phase are described as follows:

Phase 1: Single use

The most straightforward application of blockchain that falls in this quadrant is Bitcoin. Here are present low-novelty and low coordination technologies that create better, less costly and highly focused solutions. In fact, even in its yearly days, bitcoin offered immediate value to the few people that adopted it: it was just an alternative payment method.

Phase 2: Localization

This second quadrant includes innovation that are high both in novelty but still not high in complexity. This is mainly due to the fact that the technology needs only a limited number of users to create immediate value, so it is relatively easy to promote their adoption. This is a characteristic of blockchain used nowadays in the financial sector, where a still limited network of firms requires

a coordination relatively modest. As have been discussed in section 2.3, financial institution such as Bank of America, Nasdaq, JP Morgan and the New York stock exchange are testing blockchain technology as a replacement for paper-based transaction in cross border and securities settlement.

Phase 3: Substitution

In the third quadrant application are relatively low in novelty but higher in complexity, because they might face barriers to adoptions: the processes that the technology wishes to replace may be too much embedded in organizations and institutions. A typical example are cryptocurrencies different from bitcoin, that requires every party that carries out monetary transaction to adopt it, challenging governments and institutions. Moreover, consumers have also to change their behavior and understand how to implement the new functional capability of the cryptocurrency.

Phase 4: Transformation

Into this last quadrant technologies high both in novelty and complexity. Should these innovations be adopted, it would result in completely change the nature of economic, social and political systems. Smart contract might be the most transformative blockchain application at the moment. These automate payments and the transfer of currency or other assets are based on certain conditions are met. In a Fintech application taken as example, a smart contract may enable a payment transaction between the supplier's and customer's banks as soon as a shipment is delivered.

The impact is so huge just because all the firms, from SME to big financial institutions are based on contract. If those contracts are automated, then the traditional firms' structure and processes will be revolutionized.

According with the study of IBM's institute for Business Value conducted on 3000 global C-suite executives over 20 countries, today the most of blockchain phases concerning the financial industry are included in the second quadrant, named "localization". In the research, 8% of the people are considered "early adopters" who are actively involved in blockchain applications. About 25% are considering the innovation but are not ready to deploy blockchain-based solutions. The remaining 67% can be considered late majority and laggards, that are not even considering blockchain as alternative solutions. Looking back at the S-Curve of adoption, these findings align with the S-Curve of adoption and place blockchain technology on the verge of drawing in the early majority

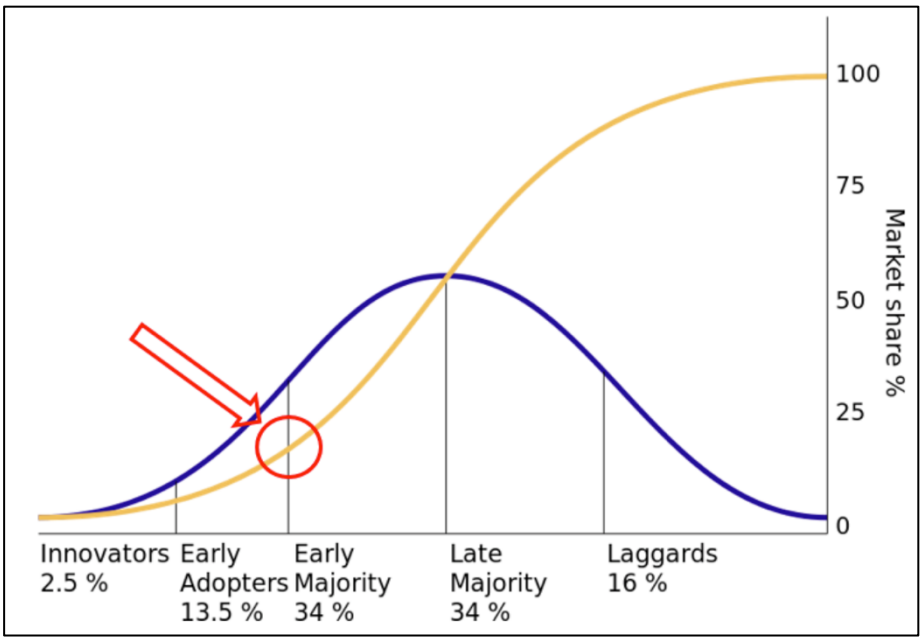

Figure 28 Blockchain position on the S-curve. Source: Hackeroon

Understanding where we stand in the technology adoption curve may help decision makers gain perspective on their concrete strategy and timeline for action. Of specific interest, as it was for electricity, the telephone or the internet, the S-Curve and identifying the current positioning of blockchain along the graph could heed the lessons of past successes and failures to preemptively respond to future trends.

Figures

References

Networks, Viacom Media. “The Millennial Disruption Index.” 2013.

Capgemini. “World payments report.” 2019.

Apple press. *Introducing Apple Card, a new kind of credit card created by Apple.* 25 March 2019.

Micheler, Eva, and Luke von der Heyde. *Holding, Clearing and Settling Securities Through Blockchain Technology Creating an Efficient System by Empowering Asset Owners.* London: LSE, 2016.

BitCoin Wiki. n.d. https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts.

Swift. 2019. https://www.swift.com/our-solutions/global-financial-messaging/fin.

Investopedia. 2019. https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp.

Investopedia. 2019. https://www.investopedia.com/terms/b/block-time-cryptocurrency.asp.

Statista. 2019. https://www.statista.com/statistics/818704/number-of-smes-in-the-netherlands/.

La Rosa, Marlon Dumas, Fredrik P. Milani. “Business Process Variability Modeling: A Survey.” 2017.

Baliga, Arati. “Understanding Blockchain Consensus Models.” 2019.

Mansilla-Fernández, José Manuel. *FinTech and Banking. Friends or Foes? (pp 25).* European Economy – Banks, Regulation, and the Real Sector, 2018.

Jerry A. Hausman, Bronwyn H. Hall, Zvi Griliches. “Econometric Models for Count Data with an Application to the Patents-R&D Relationship.” 1984, 6.

Henri Arsalanian, Fabrice Fischer. *The future of Fintech.* Palgrave macmillan, 2019.

Cata, Justin. 23 July 2018. https://medium.com/@jcata018/everything-to-know-about-ripple-part-1-how-ripple-works-f7404aa4a8d1.

Philippon, Thomas. “On Fintech and Financial Inclusion.” 2019, 3.

International Organization of Securities Commissions. “Research Report on Financial Technologies (Fintech).” 2017.

Thakor, Anjan V. *Fintechandbanking:Whatdoweknow?* Journal of Financial Intermediation, n.d.

Papadopoulos, Georgios. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments.* Edited by Erasmus University Rotterdam. Rotterdam, 2015.

World Bank Group. “Distributed Ledger Technology (DLT) and Blockchain.” International Bank for Reconstruction and Development, 2016, 8-10.

Investopedia. *How the SWIFT System Works.* 2019. https://www.investopedia.com/articles/personal-finance/050515/how-swift-system-works.asp.

Swift. *About ISO 20022.* n.d. https://www.swift.com/your-needs/industry-themes/iso-20022/supporting-standards.

Chen Liang, Ye Guo. “Blockchain application and outlook in the banking industry.” School of Economics, Xiamen University, 2016, 7-8.

David Schwartz, Noah Youngs, Arthur Britto. *The Ripple Protocol Consensus Algorithm.* Ripple Labs, 2018, 3-5.

Frankenfield, Jake. *Block Time.* n.d. https://www.investopedia.com/terms/b/block-time-cryptocurrency.asp.

Pinna, Andrea, and Wiebe Ruttenberg. “Distributed ledger technologies in securities post-trading.” ECB Occasional Paper 172, European Central Bank, 2018, 20-21.

Wall, Eric, and Gustaf Malm. “Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository.” Department of Electrical and Information Technology , Lund University, Sweden, 2016, 29-30.

Belinky, Mariano, Emmet Rennick, and Andrew Veitch. “The Fintech 2.0 Paper: rebooting financial services.” Santander InnoVentures, 2018, 15.

Bank of Japan, European Central Bank. “Securities settlement system: DvP in a distributed ledger environment.” 2018, 14.
Back, Adam, and Luke Dashjr Matt Corallo. “Enabling Blockchain Innovations with Pegged Sidechains.” Blockstream, 2014, 21.
Meijer, Carlo R.W. De. *A game-changer for Small and Medium-sized Enterprises.* June 2019. https://www.finextra.com/blogposting/17380/blockchain-a-game-changer-for-small-and-medium-sized-enterprises.
de la Rosa, J. L., Torres-Padrosa, V., el-Fakdi, A., Gibovic, D., Hornyák, O., Maicher, L. *A survey of blockchain technologies for open innovation.* San Francisco, CA, USA.: WOIC, n.d.
Biggs, J., Hinish, S. R., Natale, M. A., & Patronick, M. *Blockchain: Revolutionizing the global supply chain by building trust and transparency.* New Brunswick, NJ: Rutgers University, 2017.
Rennock, M., Cohn, A., & Butcher, J. R. *Blockchain technology and regulatory investigations.* The Journal of Litigation, n.d.
Tapscott, A., & Tapscott, D. *How blockchain is changing finance.* Harvard Business Review, n.d.
Michael Nofer, Peter Gomber, Oliver Hinz, Dirk Schiereck. *Blockchain.* Springer Fachmedien Wiesbaden, 2017.
Montagna, Marco Cantamessa Francesca. *Management of Innovation and Product Development.* Springer, 2016.
Marco Iansiti, Karim Lakhani. *The truth about blockchain.* Harvard Business Review, 2017, 7-8.
IBM. *Three ways blockchain Explorers chart a new direction.* IBM Institute for Business Value, n.d., 11-13.