Critical-Chains

Collaborative Project

Project Start Date 1st July 2019 Duration 36 Months

Deliverable D2.1

Technology & Watch Update

Published by the Critical-Chains Consortium

Version 9.0 Date 10-03-2021

Project Coordinator: Professor Atta Badii (University of Reading)

Dissemination Level: Public

Work Package Task: WP2

Document Responsible: JR

Contributors: All Partners

Status: Draft

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Abstract

This document, deliverable D2.1 (Technology & Watch Update) examines the evolving Fintechs innovations and the future of financial intermediation as spurred on by the disruptive forces arising through the new Fintechs, the advent of Blockchain technology and Crowdfunding establishing tokenomics, the new mobile money payment industry based on e-wallets for mobile payments and the developing Small Loans and Micro-financing market. The deliverable is grounded on a detailed analysis of the evolution of the financial and insurance sectors and relevant technologies and business models. A salient observation here that speaks of the rapid pace of change in this landscape is that nowadays some 89% of customers are using mobile phone payment systems and Fintechs applications for bank transfers. For insurance, Insurtechs have shown strong growth with many customers linking smart devices and buying products such as micro-insurance or peer-to-peer insurance. Fintechs and Banks are heavily regulated, with new European directives such as for example the Payment Service Directive 2, and, several Cloud services regulations. The regulatory mechanisms are catching up with the Blockchain and Artificial intelligence based business models but not necessarily with the rapidly evolving new forms of intermediation some of which have been operating in a regulatory vacuum for at least some of the time.

Responsive to the Pull-Push market forces and operational requirements in which the traditional bank services as well as new Fintechs and intermediations have to integrate and thrive, Critical-Chains has proposed Authentication, Accountability, Transaction Flows Modelling, Anomaly/Fraud Detection, Cyber Security and Blacklisting as the candidate X-as-a-Service capabilities set to support the emerging financial sector services.

Consistent with the central objective of this deliverable, the work on this deliverable has culminated in the penultimate chapter taking a specific **Challenges & Needs** Analysis perspective of the emergent Financial Services eco-system, factoring in the disruptive pressures that have impacted the Financial Intermediation and Payment Industries over the last decade. This has provided an initial indication of the Stakeholders' market-gaps-responsive requirements to inform the iterative Critical-Chains design requirements as set out in Deliverable D2.3 (Specifications & Architectural Design) as well as suggesting possible exploitation opportunities as shall be explored within Deliverable D7.8 (Business Modelling, IPR and innovation Management).

Deliverable D2.2 Document History

Versioning			
Version Number	**Date**	**Contributors' name and organisation**	**Changes**
V0.0	(11-19)-08-2019	UREAD-methodology, domain knowledge Resources, Deliverable Structure	Notes and foundational tutorial resources and references to support the Methodology, Structuring and Content.
V1.0	19-08-2019	JR	Initial Draft
V2.0	15-11-2019	All partners	All partners add relevant contributions
V3.0	26-11-2019	JR	Unifying all contributions
V4.0	06-12-2019	RINA-C	Review of draft
V5.0	20-12-2019	JR	Review and compilation of initial draft for review
V6.0	02-01-2020	JR/UREAD	Pre-finalised
V7.0	07-01-2020	JR/UREAD	Pre-final reviewed
V8.0	09-01-2020	UREAD	Penultimate Chapter added and finalised for submission
V9.0	10-03-2021	JR	Addressing project review suggestions re References
V10.0	14-03-2021	UREAD	Fixing additional Ref links & minor edits throughout

Internal Review History

Internal Reviewers	**Date**	**Comments**
Alper Kanak	03-01-2020	Reviewed and approved.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Table of Contents

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

1. Executive Summary

This document, deliverable D2.1 (Technology & Watch Update), presents an analysis of the State-of-the-Art (SoA), State-of-the-Market (SoM) and State-of-the-Practice (SoP) within Fintechs applications and Distributed Ledger Technologies. This leads to useful insights into the evolving business models and advances in technology within the financial domain. The deliverable comprises of 14 chapters with main themes of each chapter outlined as follows:

Chapters 1 and 2 present the introduction to the contents of this deliverable by setting out the background and the scope.

Chapter 3 sets out the approach adopted in this deliverable consistent with methodologically-guided framework for requirements elicitation and prioritisation as followed by Critical-Chains. This is to underpin the work for all the deliverables so as to ensure an iterative stakeholder-centred specification and prioritisation of all the requirements.

Chapter 4 provides the evolutionary history of ICT support for the financial and insurance sector. It presents detailed information on how the current technologies support the general banking sector for clearing, settlement, loans, investments and self-audit.

Chapter 5 presents the technology trends specifically for Fintechs support for Inter-Bank operations and determines audit and compliance procedures.

Chapter 6 focuses on the European Banking Regulatory Mechanisms Evolution.

Chapter 7 provides information for the current banking processes transformation responsive to European Directives. This chapter gives details for the Payment Services Directive 2 (PSD2), Cloud service regulations, Blockchain regulations, and Artificial Intelligence (AI) regulations.

Chapter 8 examines the Pull and Push forces in the Fintechs Market responsive to the Regulatory and Market Demands.

Chapter 9 sets in context the transformative responses to Distributed Ledger Technology trends within the financial sector.

Chapter 10 provides trends and technologies supporting the latest Fintechs innovations. It sets out information about current authentication schemes in Online Banking systems, Audit, and Compliance Technologies.

Chapter 11 presents the analysis of the cyber security issues and cyber-attacks against financial infrastructures. It lists and analyses the most critical attacks on financial infrastructures.

Chapter 12 provides information about current technology trends in Artificial Intelligence, Machine Learning Technologies, Blacklisting, Anomaly Detection, and Flow Modelling.

Chapter 13 takes a conclusive Challenges and Needs analytic perspective of the emergent Fintechs and the new intermediation landscape to arrive at initial Stakeholders' market-gap-responsive requirements which have informed the Critical-Chains design requirements as set out in Deliverable D2.3 (Specifications & Architectural Design) as well as highlighting the exploitation opportunities to be considered for D7.8 (Business Modelling, IPR and innovation Management).

Chapter 14 concludes this deliverable.

2. Introduction

2.1. Background

The Project Objectives are to develop an integrated effective, accessible, fast, secure and privacy-preserving financial contracts and transactions solution. This is to protect against illicit transactions, illegal money trafficking and fraud that can take place through the banking system clearing and financial transactions settlement process. Thus, the objectives of the project are in the public interest. The planned Research and Innovation work involves the use of the following data types of the participants for respective purposes as outlined in this section:

- Anonymised Inter-bank data relating to funds transfer as required for clearing funds;
- Anonymised funds transfers from sender to receiver accounts;
- Anonymised user-expressed system requirements and usability evaluation data;
- Minimal profiling data as essential for anonymised users' requirements and usability clustering analysis, or, anonymised transactor's transactions clustering and aggregated analysis
- Facial Images encrypted and stored for authentication and identity management. This is needed to support authentication, auditability and accountability. The "Critical-Chains" system will not have any access to the encrypted images but will receive the results of the success or failure of the authentication process.

The technologies to be deployed consist of:

- transaction and financial data flows analytics and modelling of the financial transactions clearing and claim settlement processes;
- secure and smart use of Blockchain for data integrity checking by involving financial institutions in the distributed Blockchain network;
- cyber security protection of Inter-Banks and Internet Banking, insurance and financial market infrastructures;
- Privacy protection through secure access supported by embedded systems and Internet-of-Things security.
- Critical-Chains is to be validated using four case studies aligned with three critical sectors: banking, financial market infrastructures, the insurance sector, and, Highway Toll collection. The validation will include evaluating system reliability, usability, user-acceptance, social, privacy, ethical, environmental and legal compliance by scrutiny of the geo-political and legal framework bridging the European economy with the rest of the world. The Consortium represents a strong chemistry of relevant expertise and an inclusive set of stakeholders comprising end-users (customers), CERTS, the financial sector (Banks & CCPs) and the Insurance sector

2.2. Scope of this Deliverable

The scope of this deliverable is to provide a conclusive analysis of the evolving techniques and advances in the State-of-the-Art (SoA), State-of-the-Market (SoM) and State-of-Practice (SoP) of the financial services and technologies and through this to offer insights on stakeholders' needs for ICT support to enable them to thrive in the emerging financial services marketplace in a way that is cost-efficient, secure and compliant with the regulatory requirements.

3. Methodology

The Critical Chains consortium uses the UI-REF methodology (Badii, User-intimate requirements hierarchy resolution framework (UI-REF) 2008) (Badii, Fuschi, et al. 2009) to underpin its approach in ensuring stakeholder-centred requirements elicitation and prioritisation. Within this framework, the inclusive iteration of the requirements and use-cases to be supported by the Critical-Chains solution stack has to be mindful of the State-of-the-art (SoA), State-of-the-Market (SoM) and State-of-Practice (SoP) related **Challenges and Need** of the stakeholders; this is to inform the evolutionary design requirements.

Accordingly this deliverable, D2.1 (Technology & Watch Update), has undertaken the essential analysis of the evolution of SOA, SOM and SOP as related to the banking sector services, the new Fintechs, and, Intermediation innovations as well as the evolving pull-push forces, including the disruptive pressures arising from the advent of Blockchain technology and Crowdfunding (tokenomics), and the new mobile money payment industry based on e-wallets for mobile payments and the developing Small Loans and Microfinancing market.

In this way the mission through this deliverable has been to analyse the emergent landscape of the banking services and payment industries in the marketplace and examine the implications of the Challenges and Needs of the stakeholders and the technological support required to ensure efficiency gains as well as security and accountability in full compliance with the regulatory mechanisms. Thus this deliverable has set out to provide an integrative analysis of the evolution of the financial sector technologies and business models as well as the regulatory environment. Furthermore it has examined the relationship between the above eco-system and the envisaged Critical-Chains X-as-a-Service support services such as Authentication and Accountability, Transaction Flows Modelling, Anomaly Detection, Intrusion Detection and Blacklisting in the context of Critical-Chains integrated IOT and Blockchain solution architecture.

Accordingly the central objective here has been to arrive at insights at SOA-SOP-SOM-inclusive stakeholder requirements including the regulatory compliance requirements given the highly, but not necessarily uniformly, regulated environment of the traditional financial sector and, payment industries including all mobile money and tokenomics business models.

Thus this deliverable has informed Deliverable D2.3 (Specifications & Architectural Design) and through its update as planed is intended to provide the relevant new insights responsive to the evolving needs of the stakeholders’’ marketplace to feed into the iterative requirements engineering process.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

4. Evolutionary History of Information and Telecommunication Technology (ICT) Support for the Financial and Insurance Sector

4.1. Fintechs Support for Intra-bank Operation

The term "Fintechs" refers to the use of technology to deliver financial solutions and its origin can be traced back to the "Financial Services Technology Consortium", a project initiated by Citigroup around 1990 to facilitate technological cooperation efforts (Hochstein 2015). However, it is only in recent years that the sector has attracted the focused attention of consumers, industries and regulators. The term now refers to a large and rapidly growing industry that in the EU will probably reach a total value of 800K USD in 2019 as the total values of Fintechs deals (FINCH CAPITAL 2019).

While the term "Fintechs" refers to the application of technology to banking and finance, this is not an inherently novel development. In the late 19th century, the first period of financial globalization was the result of the combination of finance with technology such as the telegraph, railroads and canals, underpinning financial interlinkages across borders and allowing rapid transmission of financial information, transactions and payments around the world. In the banking sector the use of telegraph or telephone facilities allowed banks to link head offices with branches in different locations with the aim to centralize and balance the demand of loanable funds across their network.

That lasted until the beginning of the First World War. During this period, technology such as the telegraph, railroads, canals and steamships underpinned financial interlinkages across borders, allowing rapid transmission of financial information, transactions and payments around the world.

However, greater use of telegraph or telephone facilities also resulted in both internal and public price related information becoming homogeneous. Banks could link head office with branches in different locations, allowing more centralization and the balancing of supply and demand of loanable funds across their network rather than at each area centre.

At the end of the 1930s, the first tabulating machines were purchased to address the growing volume of transactions and enhance working conditions and productivity of the staff working in the banking sector. This trend was reinforced by the purchase of additional adding and listing machines that supported the growing network of branches and agents. However, the potential of these machines, as well as punch-hole 'accounting' machines, as mechanisms for recording and updating transactions were not fully exploited until after the late 1940s and early 1950s.

In the 1950s and 1960s, Banks introduced computers relied on US-based suppliers of accounting machines such as IBM and Xerox both to keep up with growth in business volume and, at the same time, to solve some very specific problems in bank operations (Arner, Barberis and Buckley 2016).

Two important milestones that arguably marks the commencement of the modern evolution of today's Fintechs are: the 1966, when a global telex network was providing a fundamental infrastructure for communications and the 1967, when the Automatic Teller Machine (ATM) was introduced for the first time in UK. Between 1968 and 1980, banks became one of the world's dominant customers for computer-based applications the impact of computers was felt throughout the organization rather than in specific departments.

Meanwhile, the increasing complexity and volume of financial transactions eventually led to the development of Database Management Systems or DBMS. The role of the DBMS was to overcome the limitations of conventional filing systems by providing a generalized, structured and integrated body of data that could be read and updated in a controlled, efficient, and reliable way.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

As a result of all the innovations during this period, customers were able to use banking services at any point in the retail branch network while the previous arrangement limited transactions to the customer's own branch or required telephone approval for remote transactions.

However, it was the emergence of the World Wide Web (WWW) that set the stage for the next level of development, beginning in 1995 with the first banks providing online account checking. During the following years, internet banking grew up as a new way through which customers can use different kinds of banking services ranging from bill payment to making investment. By 2005, the first direct banks without physical branches emerged (e.g. ING Direct, HSBC Direct) in the UK.

In parallel, the diffusion of mobile devices across the population paved the way to the mobile banking revolution, which in its earliest form was only based on SMS services offered by banks. After smartphones were introduced, with WAP (Wireless application protocol) support allowing the use of the mobile web, the first European banks started offering mobile banking on this very platform to their customers. In 2011 the first mobile apps offering account checks and recent transaction history, were available on the Apple and Android App stores and since then, mobile banking has only travelled upwards. Combining near-field communication technologies (NFC) widely available in recent smartphone models with advancements in security standard for payments (i.e. tokenization standards), big tech firms has launched mobile wallet solution, allowing customers to make contactless payments only using their smartphones.

During recent years, other disruptive innovations are changing the technology landscape, also impacting the way banks run their business. One of the most important is the Blockchain technology, invented and launched in 2008 by Satoshi Nakamoto, a seasoned and anonymous Fintechs enthusiast. The tech has in the last decade alone evolved so much as to giving rise to what many know today as cryptocurrencies (virtual money), such as Ethereum and Bitcoin.

Cloud technology is one of the most recent forms of technology in the Fintechs industry, that offers advantages such as economies of scale, flexibility, operational efficiencies and cost effectiveness (Board 2019). Cloud technology is characterized by a network of remote servers, typically accessed over the internet, for the provision of IT services. Currently financial institutions mainly use the cloud for HR, CRM and financial accounting services. However it is expected in the next few years that also services as consumer payments and credit scoring statements will be offered through cloud services.

The last technological development that it is worth to mention in relation to financial services is the spreading use of APIs to allow different software applications to communicate with each other and exchange data directly, without the need for human input. Even if APIs are a quite old concept in computer engineering, they have become the de facto standard for sharing data. "Open APIs", deployed by banks in order to be compliant with PSD2 regulation will facilitate immediacy and service improvements in payments.

4.2. Front Desk to Back-Office Operations

Some of the technology innovations discussed above drastically changed the processes adopted by banks to run their business. Since the late nineteenth century, bank customers entered the banking system directly through retail bank branches. Telephone exchanges between bank managers and customers were used as early as the 1890s but in spite of this, service remained largely unaffected by technology with the front-office relationship controlled locally though asynchronous, analogue systems such as paper-based records and pass-book control. In order to secure services such as loans or establish credit ratings, long-term relations of individual customers with the bank retail branch were needed. After the installation of the first punch-hole accounting machines, increasing the size of the branch network and divesting under-performing agents then became a priority.

This resulted in the branch network quickly turning into the main point of contact with retail customers while, internally, there was a growing need to supply top management with prompt (i.e. quarterly) financial information. Thus, the introduction of a process-directed automation dominated the period of 1950s and 1960s, aiming at undercutting the cost of labour-intensive administrative tasks. During this period, the typical financial sector computer installation consisted of a central excel, dedicated to sequential batch processing of computer readable instructions dealing with separate processes such as providing a service for handling customer transactions, standing orders and other clerical procedures. Computer applications were therefore concentrated on back-office operations, because this allowed controlling a growing mountain of paper-based transactions in central locations where labour costs could be reduced through dedicated staff and automation. Later, investment banks organized into front, middle and back offices, each of which perform different tasks (RETAIL BANKING ACADEMY 2014):

- The Front Office is a direct interface between the customer and the bank through channels such as call centres, branches, ATM, and mobile channels. It acquires new customers and tries to create a long-term relationship with them interpretation their expectations and needs.
- The Middle Office is not directly facing customers but acts as an enabler of the bank's processes performing several tasks such risk assessment and compliance checks. Risk management activities could include evaluations about credit risks for example in lending to a customer, money laundering risks assessment for example in accepting a deposit. Middle Office also ensures that all banking operation are compliant with regulations, ethical principles and guidelines that the bank has adopted.
- The Back Office, like the Middle Office, is not directly facing customers but enables the banks' processes by recording and storing the information generated during the operation. The Back Office manages different types of information database in order to facilitate payment services or processes a loan application.

A technology innovation that is deeply changing how Front Office, Middle Office and Back Offices work, is Artificial Intelligence. According to recent reports (Autonomous Research LLP 2018), AI implementations are going bring large cost reductions. Front offices are already replacing service a part of their front desk operators using chatbots and virtual assistants. Anti-fraud, risk assessment and compliance checks performed by Middle Office usually takes some time, in some cases also several minutes, but the trend in all the types of financial services is to go towards operations and transactions that are completed in near-real-time (namely a bunch of seconds). Thus, the business need is to perform all the required anti-fraud, risk assessment and compliance checks in near real time as well and this can be achieved only with a complete redesign of processes and tools used by the Middle Office.

Many banks have put in place numerous initiatives to improve also back office operations, essentially moving on two levels: at high level they are going on acting with programs that aims to redesign operations in a digital and end-to-end sense; on the other hand they are acting at low level, with limited and targeted interventions on specific processes and individual tasks. In this context, the automation driver is becoming increasingly important, as it can contribute to enhance operational efficiency and improve performance, even qualitative, of the processes managed. The widespread perception is that technology innovation such as Robotic Process Automation could have a very strong impact on the paths in progress, allowing rapid intervention on the automation of specific tasks, with positive impacts on direct processing of costs, on the risks due to human errors, on peak management and on average processing times.

4.3. Clearing

Clearing is the process of guaranteeing financial market transactions between the execution of the transaction and its settlement. Technically, clearing is the process of establishing positions, including the calculation of net obligations, and ensuring that financial instruments, cash, or both, are available to secure the exposures arising from those positions. Clearing is performed by Central Counterparties (CCPs), which are financial market infrastructures that interpose themselves between the counterparties to the contracts traded on one or more financial markets, becoming the buyer to every seller and the seller to every buyer. Clearing allows counterparties to trade with each other anonymously without worrying about whether their counterparty will honour the trade. In addition, in the event that a counterparty goes bankrupt, clearing allows the market to continue trading without the bankruptcy spreading to other counterparties (EACH 2019).

The main benefits of clearing can therefore be summarised as follows:

- Efficiency: CCP Clearing reduces the obligations between counterparties by netting offsetting positions. This netting process reduces counterparty credit risk and liquidity needs between those clearing members involved in those transactions.
- Risk management: CCP Clearing independently manages the risk of counterparties through risk modelling and ensures there are resources available to absorb potential losses that could result from the default of a clearing member, limiting any potential contagion to other CCP participants.

4.4. Settlement

In the field of payments, settlement is an act, which discharges obligations between two or more parties. The settlement asset is transferred between the parties concerned, with or without the use of a settlement agent. Settlement methods vary, with a choice between gross and net settlement, and between real-time and designated-time settlement.

For a payment instruction in a payment system, settlement occurs when funds are transferred from the payer’s bank to the payee’s bank. Settlement discharges the obligation of the payer’s bank vis-à-vis the payee’s bank in respect of the transfer.

As regards settlement finality, a payment is considered final when it becomes irrevocable and unconditional. The rules of each individual payment system define the precise moment at which finality occurs. Finality may occur the moment payment instructions are entered into the system and technically validated, the moment the payment instruction is processed, and the resulting balance is settled, or at any point between those two extremes. In real-time gross settlement (RTGS) systems, the time lag between the submission of a payment and the point of finality is kept short. This reduces uncertainty as regards the possibility of the sending bank failing between the initiation and completion (i.e. settlement) of a payment.

In net settlement systems, and in RTGS systems with offsetting algorithms, it is essential for the legal system covering the system and its participants to recognise netting or offsetting as a valid form of settlement for payments (European Central Bank 2010).

4.5. Loans

The reasons for the centrality of loans in the banking ecosystem must be sought in the following circumstances:

- Bank loans are the main and most important source of coverage for European companies’ financial needs; this source, by nature, is quick to access and, above all, is flexible (loan contracts not standardized);
- Loans are the most effective way to initiate "customer relationships": their intensification impact, among other things, the bank overall business (deposit multiplier) and its business of brokerage; loans feed both the interest margin and that of intermediation (more and more often loans are the material underlying the securitization processes);
- Loans are the fundamental element that justifies, in general, the existence of intermediaries; a part of the external financing of the companies can only be insured by those intermediaries who guarantee confidential information.

The fundamental problem of the loan activity is twofold: on the one hand, the assessment of the repayment capability of the individual debtor (hence the risk associated with the single operation that can turn into loss for the bank); on the other hand, the identification of the best possible combination of transactions, taking into account the risk-–performance relation of each of them. These two elements define the two fundamental aspects of a bank's lending activity:

- Risk assessment of the single operation (selection of loans); and
- The construction of the loan portfolio in its complex (loan policy), composed by the decision on the size of wallet and the distribution among the individual operations (aspects of the diversification, of the division and of the credit splitting).

4.5.1. Loan Origination process

Loan origination is the process by which a subject applies for a loan to a lender, in line with its specific requirements and procedures, in order to obtain a certain amount of money. This process encompasses all the steps from loan application up to disbursal of funds (or declining the application). Loan origination is a specialized version of new account opening for financial services organizations, with certain people and organizations getting increasingly specialized in loan origination (e.g. mortgage brokers).

4.5.2. Credit risk: processes and tools

The loan activity exposes the bank to risks of loss - partial or total - of the loaned capital in the event of the debtor's final insolvency (economic risk) or financial costs due to unexpected tensions in the liquidity management, following delays in capital payments or interest at the agreed due dates (financial risk).The conjunction between economic risk and financial risk contributes to determine the quality of the loans, which can span on scale that includes, in decreasing order of quality, live loans, problem loans, bad debts and doubts outcomes.

With respect to the assessment, assumption and management of risk, the process can be summarized in three core phases in which the bank processes data and information:

1) Deferred benefits

From the moment in which the bank decides to disburse the loan, to the moment in which they are returned (in one or more solutions depending on the type of contract) there is a period of time that exposes the bank to the relative uncertainty concerning the repayment of the funds and the deterioration of the creditworthiness of the subject.

2) Information asymmetry

The purpose of the loans, as regards the requesting companies / families, is to finance projects / investments that may have different duration. The quality of these projects is unknown to the bank (lender of the loans) both before disbursement (ex-ante) and after delivery (ex post, or if the investment has been successful, or if the project has changed becoming riskier). This condition is physiological, strictly speaking connected with the loan disbursement activity, and, therefore, it must be managed by the intermediary with ad hoc procedures.

- Information asymmetry (ex-ante) and adverse selection

  In a context of ex ante information asymmetry, the bank is in a position to provide loans, which potentially, could finance both "good" and "bad" investments in outcome terms. The bank therefore tends, as a defensive strategy, to raise interest rates to recover from losses deriving from borrowers of "bad" funds. In this approach, less risky (but also less profitable) projects tend to be excluded as applicant company should bear an increase in costs with the same revenues.

  How can this risk be managed?

- Screening: The ex-post information asymmetry and the moral hazard

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Once the loan for the bank is disbursed it is difficult to know if the borrower has had, or has, opportunistic behaviours (ex. finance a project riskier than that presented at the time of the request reliance)

- Monitoring Credit risk: the tools of analysis
  - Selection of initiatives to be funded (definition of internal rating)
  - Definition of the rate: The rate applied is defined on the basis of the risk (rating assigned), of the expected profitability on the risk capital absorbed by the loan, as well as the financial and operational costs associated with the transaction; Management and monitoring (i.e. control and periodic review of relationships);
  - Portfolio management

4.5.3. The risk assessment

The first phase of the risk assessment largely coincides with the traditional credit check. The assignment of a rating summarizes the risk perceived by the bank in association with a loan.

Risk assessment is basically a problem of processing of available information and is the core of credit evaluation criterion adopted by each bank; basically, it is composed by the following two phases:

- Screening: Before the loan is granted, a selection is made on credit applications, to check if all relevant criteria are satisfied
- Monitoring: During the life of the loan, a surveillance action is implemented.

The risk of the single loan, once assessed and assumed, can be managed by deciding whether to keep it, because it integrates effectively with the portfolio loans possessed, or to transfer it (with securitization or recourse to credit derivatives) if its characteristics do not coincide with the combinations desired risk-return.

The quantity and quality of available information obviously depends on:

- institutional factors (the reliability of accounting information available; the willingness of the company to provide confidential information, the ability of the bank to produce internal information, the possibility to consult digital databases - such as the Central Risks database - to detect the applicant's debt exposure to the system);
- The configuration assumed by the bank-company relationship and by the intensity of the client relationship that links the second to the first.

Customer relationships indicate the existence of a business relationship between bank and customer from which an intense and complete exchange takes place, extending to a variety of banking services. Thus many benefits can be realized for the contractors, among which the most important are the stabilization of the cost of financing for the company and access to information reserved for the bank; finally, these benefits can be transformed into a number of different incentives, aimed at guaranteeing that the relationship remains over time and extends to all possible services.

In general, the composition of the loan portfolio is described according to the following key elements:

- the category of beneficiary companies,
- the technical form,
- the expiry and name of the unit of account.

The composition of the loan portfolio depends on the choices that the company has made in relation to the size and structure of the organizational structure of the bank, and to the characteristics of the credit demand expressed by the markets in which the bank operates.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

4.5.4. Types of loans (classification)

The different types of loans can be classified as follow:

- **Cash and short-term loans:** Aimed at financing investments in operating working capital (inventories, customer loans, etc.), which can also be financed through supply credits (the company grants payment extensions to customers and obtains extensions from suppliers); Noteworthy, risk of use for purposes other than those for which they are issued and, generally, they do not require the release of collateral; cash and short-term loans include:
    - Opening of credit in bank account
    - Depreciation on credits
    - Anticipation on pledge
    - Transactions in financial securities
- **Signature credits**, which implies the payment of a fee;
- **Family loans**
    - Mortgage loans
    - Consumer credit
- **Medium / long-term loans:** aimed at hedging capital investments fixed (fixed assets); these are characterized by higher risk of corporate default when the higher duration of the loan and typically require the issue of guarantees; medium/long-term loans include:
    - The mortgage
    - Leasing
    - Pool Pooled loans

4.5.5. State of the art of the Loan Origination software, tools and IT solutions

Loan Origination software solutions are developed to manage lending tasks such as origination, underwriting, closing and documentation for various type of final users like banks, government agencies, credit unions, and private lenders. This type of software could also include built-in components for regulatory compliance and risk assessment monitoring.

Loan Origination software is strictly connected to Banking Systems software, Financial Risk Management software, Loan Servicing software and Mortgage and Loans software.

State of the art of the Loan Origination software, tools and IT solutions (Large players)

The banks and large companies usually adopt Credit Process Management System (CPMs) custom internal platform in order to manage credit risk processes. CPM solutions are usually based on the BPM standards, allowing configuration of both processes as well as all the credit product parameters.

This kind of system are based upon a SOA architecture, in order to simplify integration with Bank's internal systems and databases.

CPMs are developed to support each stage in the credit-granting process, from simulation to verification and decision-making, and eventually to the disbursing of funds.

Such solutions also serve after-sales processes, such as annexes, monitoring and soft debt recovery and management procedures. The CPMs systems are developed to be modular systems, which provides the bank with solutions that could evolve during its lifecycle.

Usually CPM's supports all major features associated with the process of loan origination such as Registration/ client search via integration with a CRM or a core system and, Credit simulation (based on built in business rule engine), Credit application, Document management, Client verification – Credit Information connector, Credit analysis, Multi-level decision support, Disbursement conditions verification and After-sales service. CPMS are usually fully integrated within the Bank systems like briefly illustrated in Figure 1.

State of the art of the Loan Origination software, tools and IT solutions (small players)

Even for small Players the loan origination is a critical part of any lending business because all the subsequent processes such us collecting the data about possible customers, analysing it carefully , selecting the eligible borrowers, and, obviously, evaluating all credit risks originate from it.

In most cases, origination process is what makes the loan issuing a time consuming and demanding process, both for loan officers and for the clients.

Big player, such us traditional big banks, which are slowly approaching to the Fintechs revolution, are the most impacted in the landing market because the borrowers now have a choice to find an alternative that require less time and effort.

That is why in 2019 the transaction value of alternative lending, such us small player Fintechs services providers, is already estimated to be around 267 Million US Dollars.

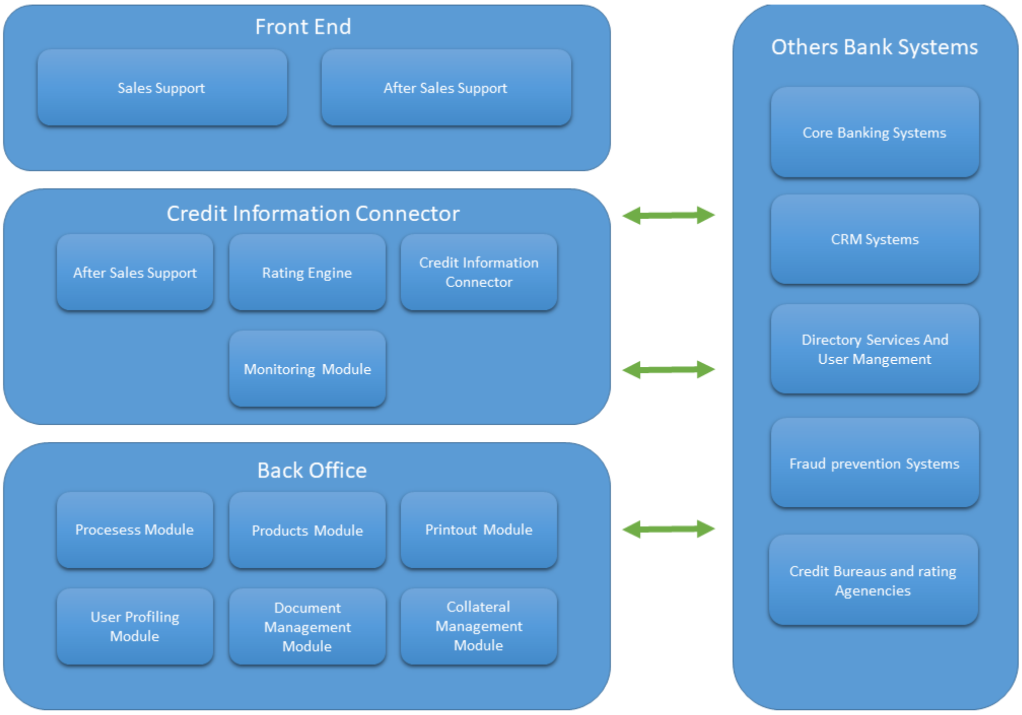


Figure 1. Example of CPMS Platform

In such a context, it is worth remarking that unlike traditional big banks, smaller operators and all kinds of alternative lenders do not have the resources to create a custom internal IT platform to manage the whole lending processes, but, at the same time, they need high quality IT automation in order to keep the cost low, maintaining a small staff with high success rates, in order to compete effectively with the big players.

That is the reason why they are relying on IT suppliers, which are providing them with ready-made solutions that will address their specific needs.

All the elements that characterize the loan origination process described above are digitalized and automated, and, more importantly, consumed in an “as a service model” by the small players.

This way a small player does not need major endowments or multiple branches to take care of all loan origination steps. All the providers are claiming to reduce operational costs, improve time-to-funding, and to have all the functionality an operator need, in any case, there are different level of maturity of the functionalities. Some platforms are good at automating only a part of the steps listed above, some lack security, while others only fit particular business models.

We have performed a small qualitative analysis based on the most important factors that a small player typically considers crucial when choosing loan origination solution provided by third party suppliers such as:

1. Security Aspects
2. Provide Regular updates
3. Provide Full process automation or not
4. Provide integrations with external databases
5. Provide free trial

Here below the most important suppliers offering this kind of solutions on the market.

TurnKey Lender

TurnKey Lender is an intelligent cloud-based software solution that automates the whole lending process, including automation of collateral management, risk management, debt collection, loan servicing, reporting, supervision, and regulatory compliance. The loan origination function takes care of all the steps listed above, at the same time including integrations with the major credit bureaus and external databases to make informed decisions about the borrowers. One of the most important and unique features of this company's origination solution is its interesting use of AI and machine learning. Advanced AI algorithms are used in order to learn about each business' clients and evolve to make more of the right credit decisions with reduced risks. The logic responds differently to different loan applications and evolves intelligently over time. Is it possible to customize the system with alternative scoring models that are easy to install with internal APIs. The platform easily deploys from the cloud and can be customized by each client. Customization is intuitive and can be done by the representatives of the customer or under TurnKey Lender's supervision. This platform is tailored for the alternative, SME, peer-to-peer and direct lenders, auto financing, mortgage, community banks, and credit unions.

Cloud Lending Solutions

Cloud Lending Solutions is also a solution that aims at helping lenders reduce operational inefficiencies through automation and configuration.

The solution exists in the form of Salesforce apps and include a set of plugins/applications that can be used. The solution for origination is named "CL Originate". It has a set of functionalities that support lenders in managing origination processes including file management, underwriting, decisioning, credit analysis, and approvals.

The strong points of CLS are the fact that it is cloud-based platform with good configurability. The weak point is that the system collects data, but risk evaluation is not actually supported by the tool, because only a small part of the loan decisioning pipeline is automated. In any case it is Possible to integrate the system engine with third-party data sources.

Even if CLS declares to provide an end-to-end solution, their platform come as separate set of packages for: portals, loans, leases, origination, marketplaces, and collections. The primary target users of this solution are commercial, consumer and small business lending.

Some of the major constraints of the platform are that there is no free trial, the platform is not truly all-in-one, and it does not provide so much flexibility.

CloudBnq

CloudBnq is a web-based solution providing some loan origination features for lenders. The solution functionalities are: lending campaign creation and management, loan application collection, review, decisioning

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

and application completion. The weak point is that the system leaves complex aspects like risk evaluation and underwriting to the final user.

LendingPad

LendingPad is not an end-to-end solution. It only works as a point-of-sale and loan origination system. The product is mainly aimed at lending professionals in general, be it small banks. The Platform covers things like service level agreements, document storage, real-time reporting, workflows customization, and obviously loan tracking.

The risk management and automation of the processes are the weak point of the solution in fact LendingPad can work as an addition to existing functionality such us internal custom risk evaluation solution. The strong point of this system is that it has interesting features useful for warehousing activities, post-closing tracking, and tracking of loan characteristics.

Encompass

Encompass platform for loan origination is one of the big market players. It is a tool suite that allows small lenders to choose the modules they need. The solution includes functionality for compliance, integrating with external software providers, custom screens tailored to individual personas. The strong point of the solution is to provide lenders with a flexible tool that fits different business processes and operations.

Calyx Point

Calyx Point is developed to target lenders such us small banks or credit bureaus. With regard to origination process, the key functionality is the loan processing which gives to the final user a score for each client, loan submission control, online application, and an audit trail. The weak point of the system is that it does not have a good compliance and fee management mechanism and additionally it is not cloud-based. According to the user's feedback, the system has a rather steep learning curve and is not always stable when it comes to processing and storing data.

HES Lending Software

Multiple modules that cover different stages of the lending process for consumer and business lending compose the HiEnd Systems product. The solution is developed around a "semi-custom" approach that let HES to implement changes into the system to meet the specific needs of a specific client. The solution offers a free trial.

LoanDisk

Like TurnKey Lender, HiEnd Systems utilizes AI for credit scoring, but in their case, the algorithms need at least initial 1,000 issued loans to be trained.

4.6. Self-audit

The importance of internal audit in financial institution was demonstrated during the recent financial crisis started in US in the 2000s. It is believed that many of the corporate scandals that broke out in that period are the result of the fact that the senior management were able to manipulate financial statements without being controlled and the results has been catastrophic defaults of many important financial companies. In recognition of the lessons learned from the recent past, the legal framework in relation to corporate governance standards has been overhauled with the aim to spell out and to enforce a set of basic principles about how to implement a good corporate governance. These basic principles are pursued at the international level through guidelines from the Basel Committee of Banking Supervision, a global standard setter for the prudential regulation of banks. Table 1 summarize the basic principles as the output of the work released by the Basel Committee in 2012 (Al-Matari, Hassan and Alaaraj 2016).

Table 1. Basic principles by the Basel Commitee in 2012

PRINCIPLE NAME	EXPLANATION

1- Internal audit responsibility	An effective Internal Audit Function provides independent assurance to the board of directors and senior management on the quality and effectiveness of a bank’s internal control, risk assessment and governance systems/processes
2 -Independence	The bank’s Internal Audit Function must be independent of the audited activities
3 -Competence	Professional competence is essential to the effectiveness of the bank’s Internal Audit Function
4 -Integrity	Internal auditors must act with integrity such as The IIA’s International standards for the professional practice of internal auditing
5 -Charter and authority	Each bank should have an internal audit charter that promotes an effective Internal Audit Function as described in Principle 1
6 -Scope of activity	Every activity (including outsourced activities) and every entity of the bank should fall within the overall scope of the Internal Audit Function
7 -Adequate coverage	The scope of the Internal Audit Function’s activities should ensure adequate coverage of matters of regulatory interest within the audit plan
8 -Established internal audit function, Part I	Each bank should have a permanent internal audit function, which should be structured consistent with Principle 14 when the bank is within a banking group or holding company.
9 -Board of Directors role	The bank’s board of directors has the ultimate responsibility for ensuring that senior management establishes and maintains an adequate, effective and efficient internal control system
10 -Audit Committee role	The audit committee, or its equivalent, should oversee the Internal Audit Function
11 -Head of Internal Audit role	The head of the internal audit department should be responsible for ensuring that the department complies with sound internal auditing standards and with a relevant code of ethics
12 -Reporting structure	The Internal Audit Function should be accountable to the board, or its audit committee, on all matters related to the performance of its mandate as described in the internal audit charter
13 -The Internal Audit function as the third line of defence	The Internal Audit Function should independently assess the effectiveness and efficiency of the internal control, risk management and governance system
14 -Established Internal Audit function, Part II	To facilitate a consistent approach to internal audit across all the banks within a banking organization, the board of directors of each bank should ensure that either the bank has its own Internal Audit Function or holding company’s Internal Audit Function performs internal audit activities of sufficient scope at the bank
15 -Impact of outsourcing on the Board of Directors	Regardless of whether internal audit activities are outsourced, the board of directors remains ultimately responsible for the internal audit function

These principles underline the need for a financial corporate to have an internal audit function with sufficient authority, stature, independence, resources and access to the board of directors.

An effective internal audit function can really help in reducing the risk of loss and reputational damage to the bank but must normally face several challenges. First, the increasing number of national and international rules and regulations that affect the entire financial services industry. Internal audit functions need to stay current on the changing regulatory landscape to keep pace with the expectations of their regulators also engaging with industry associations and creating networks of knowledge sharing in order to identify how peers are addressing new challenges.

Other important roles of an internal audit function are the following (KPMG 2016):

- Perform assessments on behalf of business lines to identity deficiencies and then track issues and monitoring remediation’s
- Assess whether policies, procedures and the control environment are kept current to changing regulatory requirements
- Provide a high level view on the effectiveness of the risk management and compliance functions.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

5. Fintechs Support for Inter-Bank Operations

New technologies and business models make it possible for auditors to analyse large amounts of company financial data and test 100% of company transactions instead of testing only a sample. These tools will enable auditors to perform advanced analytics to gain deeper insight into the company's operations. Data analytics for example may also allow auditors to better track and analyse their client's trends and risks against industry or geographic data sets, leading to better assessments throughout the audit process so that auditors can spend more time scrutinizing more complex and high-risk areas that require increased judgment.

The public view of auditors to enhance trust in the audited information of the companies and help capital markets system function with greater confidence. Auditors' practice is under strict regulations, professional codes of conduct and auditing standards, and are independent of the entities they audit. They apply objectivity and professional scepticism to provide reasonable assurance about whether an entity's financial statements are free of material misstatement and, depending on the engagement, about whether a company's internal controls over financial reporting are operating effectively. An audit involves an assessment that recorded transactions are supported by evidence that is relevant, reliable, objective, accurate, and verifiable. One of the most disruptive technology that can really help accounting and auditing practices is Blockchain technology.

The acceptance of a transaction into a reliable Blockchain may constitute sufficient appropriate audit evidence for certain financial statement assertions such as the occurrence of the transaction (e.g., that an asset recorded on the Blockchain has transferred from a seller to a buyer). Generally, accepted auditing standards, to ensure the reasonableness of statements, require auditors to perform certain procedures. All audit procedures then have to be stated on a company's accounting ledger. As one can imagine, this process could be very expensive, especially in complex businesses. It is true that the cost to the public of relying on faulty financial statements can be many times bigger, but the Blockchain can eliminate, or at least reduce, both of them. Blockchain allows to compare accounting entries between two trading partners, without affecting data privacy. This system has been also called "Triple Entry Bookkeeping": it is an enhancement to the traditional double entry system. All accounting entries are not registered separately in different sets of books, but they are recorded as a transfer between wallet addresses in the same ledger and then cryptographically sealed by a third entry to create an interlocking system, impossible to destroy or to falsify. By adopting this system, audit process would be less expensive in terms of time and costs, since auditors would be able to verify a large portion of data easily, quickly and in a more accurate manner. In practice, it is possible that two or more of the accounting and audit firms would be the validators on a permissioned distributed ledger used to process and record triple entry accounting records.

Blockchain would greatly reduce the opportunities for earning management (backdating sales contracts to a prior reporting period or amortizing operating expenses over long period) and it could allow promptly to spot related party transactions. Furthermore, the market could rely on the integrity of a company's financial statements since revenue and expense cannot be falsified. In fact, transaction have to be confirmed by the counterparty through the cryptographic process. Stakeholders could access the firm's financial data in order to take decisions based on accessible, reliable and immutable records. The result of all this structure would have a positive effect on stock prices, borrowing rates, and several other factors. Smaller enterprises could take advantage of triple entry bookkeeping to prove economic activity to outside stakeholders, such as banks or angel investors with much less costs.

5.1. Audit & Compliance

The Audit is a procedure that organizations should use in order to reach a continuously productivity improvement in their organization. The definition is:

A set of actions and procedures to control an organization. They aim to test and prove that processes are being conducted effectively and follow due control mechanisms. They also aim to detect opportunities for improvement in the audit process (Veyrat 2019).

The main principle of an audit process is the Deming cycle that is based on PDCA: a repetitive four-stage model for continuous improvement (CI) in business process management (ISO9001) (Hammar 2019). These categories are:

- **Plan:** Establish objectives and processes required to deliver the desired results.
- **Do:** The do phase allows the plan from the previous step to be done.
- **Check:** During the check phase, the data and results gathered from the do phase are evaluated. Data are compared to the expected outcomes to see any similarities and differences.
- **Act:** Also called "Adjust", this act phase is where a process is improved. Records from the "do" and "check" phases help identify issues with the process. These issues may include problems, non-conformities, and opportunities for improvement, inefficiencies and other issues that result in outcomes that are evidently less-than-optimal. Root causes of such issues are investigated, found and eliminated by modifying the process. Risk is re-evaluated. At the end of the actions in this phase, the process has better instructions, standards or goals. Planning for the next cycle can proceed with a better base line. Work in the next do phase should not create recurrence of the identified issues; if it does, then the action was not effective.

The audit process, based on PDCA approach, is composed of four phases (University of Pittsburgh, Internal audit department 2019): planning, fieldwork (execution phase), reporting, follow-up.

- During the planning phase, it is important to establish contact with the client in order to gather the background information and identify risks. In addition, the auditor defines the audit methodology and objective. Depending on the type of audit and the amount of audit work planned, an entrance meeting may be scheduled with the head of the unit and any administrative staff that may be involved in the audit.
- Once the audit is planned, the auditor gathers evidence to accomplish audit objectives assessing the adequacy of internal controls and compliance, conducting interviews, reviewing documentation and processes, testing transactions and documentation. It may be necessary for the audit team to conduct interviews with departmental personnel and to review departmental records and practices. Throughout the audit, audit clients will be informed of the audit process through regular status meetings and/or communications.
- The third step consists of writing a report that details the audit scope and objectives, results, recommendations for improvement, and the audit client’s responses and corrective action plans. If recommendations are made, written responses are requested of the audit client in order to detail a corrective action plan to resolve the problem and its root cause, the person responsible for implementing the corrective action and an expected implementation date. If necessary, an exit meeting will be held to provide an opportunity to resolve any questions or concerns the audit client may have about the audit results and to resolve any other issues before the final audit report is released.
- The follow-up phase is performed when corrective actions to resolve an audit issue will not be accomplished until after the audit report has been finalized. In these cases, follow-up will be performed on the previously reported recommendations to determine whether corrective action plans have been effectively implemented and that expected results are being achieved. Depending on the severity of the audit issue, follow-up activities could include interviewing staff, reviewing updated procedures or documentation, or re-auditing the processes that originally led to the audit issue.

There are several types of audits that can be conducted (Bragg 2018). For example, we can list the following: compliance audit, financial audit, construction audit, information systems audit, investigative audit, operational audit, and tax audit.

We are interested in the first one. The compliance audit is an examination of the policies and procedures of an entity or department, to assess if it complies with internal or regulatory standards. This audit is most commonly used in regulated industries or educational institutions.

Regular compliance audits (iAuditor 2019) help organizations firstly ensure a safe working environment complying with government requirements and safety protocols intended to promote a secure and stress-free workspace. Secondly, they contribute to increase productivity managing production downtime and boosting profitability. Moreover, legal issues, penalties and other consequences, as disruption or even operation cessation, will be prevented and continuous operation guaranteed. Finally, a continuous and iterative compliance assessment help establish a good reputation gaining public trust and dominate the industry you belong to by staying aligned with industry protocols.

During an audit, the auditor needs to obtain sufficient, relevant and useful evidence to effectively achieve the audit objectives. A compliance audit checklist (iAuditor 2019) is a tool used by external and internal auditors to determine the organization’s compliance with government regulations, industry standards, or internal policies. It helps gather significant data and photo evidence to discover gaps in processes that can be improved in order to meet requirements. When used appropriately, an audit checklist will easily identify areas of concern and allow management to take corrective actions to fix the problem.

In the banking industry, there are many kinds of regulations required for bankers to follow and comply. Most of the central banks required commercial banks to perform the compliance audit to verify that they are complying those law and regulation set. The entity may also have its internal audit in order to review the entity’s internal policies and procedures are complying and effectively follow.

The demands on compliance within the financial industry are ever increasing. Since 2016, more than 52,000 international regulatory changes have been introduced and, since 2008, financial institutions have shelled out $204 billion in fines and infractions (J. Chang 2019). Financial institutions must secure customer information and must ensure customer data is disposed of appropriately. Moreover, they should anticipate cyber security threats and other hazards that might influence systems and networks and put controls in place to prevent illicit access and protect the institution and its customers.

In the regulatory landscape, the key challenges to which compliance functions need to face are (Piovan, Pirondini and Vidussi, RegTech: Get Onboarding The challenges of compliance 2019):

- **Managing Regulators**: Respond to regulatory requirements promptly, protecting both the brand and reputation;
- **Compliance Strategy**: Lead the strategic decision-making process from a regulatory compliance standpoint;
- **Compliance Operations**: Reduce compliance costs by promoting transparency and managing inefficiencies in paper-driven processes adopting digital solutions;
- **Consumer Protection**: Implement new solutions to increase the protection of the customers.

In this context, financial institutions will require more process and system enhancements, and technology solutions to assist and support them in putting in place an effective and dynamic compliance framework that is responsive to market and regulatory developments. They need to identify areas where operational improvements are needed and internal controls over financial reporting should be strengthened. Technologically advanced solutions are needed to disrupt the regulatory landscape that is constantly changing.

6. European Banking Regulatory Mechanisms Evolution

Between 2007 and 2009, the global financial crisis had a significant and lasting impact on the economic system, which immediately highlighted the need to reform supervisory systems in order to strengthen cooperation between responsible sector authorities at national level and their coordination at European level. At European level, in November 2008, the Commission mandated a group of experts, chaired by Jacques de Larosière (ec.europa.eu 2009), to formulate guidelines on how to strengthen European supervisory mechanisms to better protect citizens and restore confidence in the financial system. In their final report, presented in February 2009 (Merli 2009), the experts recommended a number of reforms to the structure of supervision of the financial sector in the Union, with the measures contained in the 2010 Supervision Package creating the new European Supervisory Authorities (ESAs), the European Banking Authority (EBA), the European Securities and Markets Authority (ESMA) and the European Insurance and Pension Fund Authority (EIPOA).

6.1. PSD1 e 2

The Payment Services Directive (Directive 2007/64/EC), also known as the PSD (European Parliament 2007), defines a modern and coherent Community legal framework for electronic payment services. More specifically, it responds to the following objectives:

- to standardize rights and obligations in the provision and use of payment services to lay the legal foundations for the implementation of the Single Euro Payments Area (SEPA);
- to regulate market access to foster competition in the provision of services; to ensure greater protection of users and greater transparency;
- to encourage and increase the use of electronic and innovative payment instruments to reduce the cost of inefficient instruments such as paper and cash.

On 13 January 2018, the Payment Services Directive (EU) 2015/2366, known as PSD2, came into force and has been fully applicable since 14 September 2019 (Deutsche-bank 2019). The main innovation introduced by PSD2 compared to the previous PSD is the possibility for holders of a payment account accessible online to use services made available by authorized third parties to access the information of their accounts, even if held with different institutions. The primary objective of the PSD2 is to create a single integrated market for payment services, regulate digital payments, strengthen the security of the system and ensure transparent competition. PSD2 introduces new security requirements for access to bank account and for the provision of electronic payments. In fact, PSD2 provides for the use of high security standards, through a mandatory provision that requires the verification of identity through two or more authentication tools. The EU has introduced the PSD2 in order to create a level playing field and a more democratic banking environment, to increase competition and innovation in the market between Member States, as well as to strengthen consumer protection and improve the security of internet payments and account access. The PSD2 is the concrete expression of the Open Banking project as it allows to open up banking APIs, or an application programming interface, to authorized third parties. It is a set of formalized commands that allow software applications to communicate with each other in a uniform way and to use basic tools to create customer-centric services that can safely access bank data and offer new innovative services and products. Banks thus compete not only with banks but also with anyone offering financial services.

6.2. GDPR

In terms of data protection, it is necessary to go back to the 90's with Directive 95/46/EC which was adopted on 24 October 1995, with the specific aim of harmonizing the level of protection of the rights of individuals with regard to the processing of personal data and remained the main legal instrument of the European Union on data protection until 2002 when it is accompanied by the 2002/58/EC Directive (ePrivacy). This 95/46/EC Directive presents shortcomings, due to the evolution of technology, and automated processing. Seven years after the Directive 2009/136/EC, has amended it with regard to the processing of personal data and the protection of privacy in the electronic communications sector.

On May 25th, 2018, Regulation 2016/679, approved on 16 April 2016, became fully applicable in all European Union countries (European Parliament 2016). More commonly known as the GDPR (General Data Protection Regulation), the EU Regulation overcomes the previous Directive 95/46/EC on privacy. The GDPR came into force as a primary standard, without the need for any specific transposition and replacing the legislation currently in force in the individual member countries. The GDPR applies to all organizations, companies or members of the professions, which collect, store and/or process personal information and which offer goods or services to EU citizens residing in the EU or which monitor the behaviour of EU citizens residing in the EU. This regulation is particularly relevant at the banking level because it regulates the large mass of data with a high content of sensitive information, which all banks and Fintechs companies store and then extrapolate drawing economic benefits such as customer profiling (Famularo and Magazine 2018). The GDPR does not make substantial changes but strengthens the rules for the protection of personal data of individuals. The stated aim, as well as making the legislation unique in individual states, is to adapt the rules on privacy to the latest technological developments, such as the spread of social networks and smartphones. The aim is to limit the use of personal data or at least make the conditions of use as transparent and inspectable as possible and also to severely sanction the misuse of data (Irwin 2017). The strengthening provided for by the GDPR focuses on accountability, i.e. the accountability of data controllers, who must adopt proactive behaviour demonstrating the actual adoption of measures to ensure the application of the regulation. The GDPR then introduced the concept of privacy by design, the impact assessment, i.e. the assessment of the risks that the processing could involve on the freedoms and rights of data subjects, as well as the new figure of the Data Protection Officer. Privacy by design privacy by default (Cyberlaws 2019) essentially means starting a new project, of any kind, having in mind from the outset the required privacy and security requirements and that, automatically, the options for the greatest possible protection of the data are set by default. The role of the Data Privacy Officer or Data Protection Officer, who may be an employee or even an external subject, is of central importance in the view of the GDPR. It is in fact a top figure, whose appointment has become mandatory in public bodies and entities that perform processing that require the continuous, regular and systematic monitoring of data on a large scale. The DPO, while not replacing the controller and the owner of the treatment, has a vital role and precise tasks for the protection of personal data. In particular, the DPO will have to provide the necessary advisory support to various actors including the controller, the controller and the processors; it will also have to monitor the adoption of the Regulation and the security policies, as well as cooperate with the supervisory authorities, acting as a point of reference and single contact between the parties.

6.3. CRR

At the end of the 1990s, it became clear that the regulatory environment in which the banks operated was unregulated, and an attempt was made to remedy the situation in Basel, Switzerland, by the same name. Basilea I introduced the minimum capital requirement, i.e. increased deposit protection. In addition, a coefficient was introduced to measure the financial strength of each individual entity. This was remedied by Basilea II, which came into force in 2008 and improved the calculation criterion for measuring the debtor's risk of insolvency by introducing various types of risk (Blueoceanfinance 2019). Capital requirements for banks and investment firms are part of the single banking union code and implement in 2010 the EU legislation with Basilea III agreement. The Regulation, which is directly applicable in all EU Member States, lays down prudential capital, liquidity and credit risk requirements for investment firms and credit institutions. The Regulation requires banks to set aside sufficient capital to cover unexpected losses and remain solvent in a crisis situation. As a basic principle, the amount of capital required depends on the risk associated with the activities of a particular bank. The Capital Requirements Regulation refers to this principle as an "own funds requirement", expressed as a percentage of risk-weighted assets. Risk-weighted assets' means, in essence, that safer assets are allocated less capital, while riskier assets are assigned a higher risk weight. So, the riskier the assets are, the higher the amount of capital

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

the bank has to hold aside is. Financial institutions must have minimum liquid assets to cover net outflows of liquidity under severe stress over a 30-day period (Consilium.europa.eu 2019). From January 1st, 2014, banks are required to make public the number of employees of each of their institutions and their net banking income (hypo-alpe-adria.it 2015). All systemically important European banks must report their profits, taxes paid, and public contributions received. In addition, from 2015, banks are required to disclose such data unless the Commission, by means of a delegated act, decides to defer or amend the relevant provisions.

7. Current Banking Processes Transformation Responsive to European Directives

Generally speaking the technology innovation have always had redefined how humans interact with each other and their way of running a business, consequently also the banking sector has not been immune to that transformation process.

The emergence of new technology such as Open APIs, cloud services, block chain and AI technologies into the banking market, has pushed the driven of volumes of digital data, giving rise to new market players, roles and business models.

Given the potential of these technologies to significantly change the whole banking sector, regulators in Europe are working continuously to define and refine laws in order to take the opportunities and manage risks of that technologies. On the other hand, if banks want to take advantage of these market opportunities, they will have to adapt their internal processes to the new regulations that in some cases pose some strict constraints.

7.1. Current regulatory picture in Europe and present and future obligations for Banks.

7.1.1. Payment Services Directive 2 (PSD2)

The regulation introduces, among other things, additional requirements for banks including one for strong customer authentication on the majority of electronic payments and the new role of “third-party providers” (TPPs) in traditional banking process.

This latter aspect requires banks to securely provide their client’s data to TPPs exposing that data using for example a set of public APIs.

Said that it is quite clear how in Europe the PSD2 directive has become the major driver of the adoption of Open Banking API from the banks because starting from September 2019, the regulation is forcing banks to give TPPs access to customer accounts, with their explicit consent, through a different dedicated interface.
While not mandatory, it is commonly accepted that a set of APIs could provide compliance with regulation in the most and effective way. Thus, Banks are moving towards the adoption of various kind of Open APIs solutions in order to be compliant with these aspects of the Regulation. It is important to underline that all of the potential commercial benefits that banks could receive from the adoption of the regulation depend on a minimum level of API standardisation in order to bring their customers innovative solutions in a safe and secure manner at the same time containing costs.

Unfortunately, the Open API solutions are not defined at the regulatory level in Europe; in fact, PSD2 does not cover the functional or technical details of the interface that TPPs should use to connect with banks.

As a result, independent market initiatives have emerged to fill in the gap, such us the Berlin Group’s NextGenPSD2 that is the only API standard that was cross-border from its very first version.

Other implementations are the CMA Open Banking API (UK), STET API (France), and the API specifications published by the Slovak, Czech and Polish banking associations.

The Berlin Group and STET are in advanced convergence discussions and have agreed to full alignment on any future developments.
Another fundamental aspect of the regulation is that it opens the door for other market actors to access user data that was prerogative of the banks since now.

This implies a significant level of trust and security and accountability of those accessing bank data. It also means banks being able to ensure that a party accessing client data or initiating payments is authorised at the same time having an audit trail. In EU TPPs are subject to authorisation leased by the European Banking Authority (EBA), which is maintaining a centralised register.

Meanwhile, ETSI completed a standard for EU qualified certificates as defined in the eIDAS regulation in May 2018 that meets secure communication requirements under PSD2.

7.1.2. Cloud service regulation in Europe

The following regulations establish rules for the adoption of cloud technologies in general:

- **The EBA Recommendations on outsourcing to Cloud Service Providers December 2017**: which establishes the security measures and controls for using cloud, e.g. access and audit rights, security of data and systems, location of data and processing.
- **The European Commission (EC) Fintechs action plan March 2018:** which mentions a number of actions, including the proposal for a regulation on a framework for the free flow of non-personal data in the EU, which aims to remove unjustified data localisation restrictions (e.g. relevant to the use of cloud).

The banking sectors is moving toward the adoption of cloud service in order to reduce operating costs, but this choice not relieve a bank of its own responsibilities with respect to security aspect of data. Financial institutions' cloud service agreements must comply with the data protection regulation and cybersecurity guidelines as well as banking-specific outsourcing rules and requirements. In Europe, the EBA recommendations on cloud outsourcing state that this could be reached by modifying banks internal process through the adoption of proper outsourcing contracts at the same time monitoring its own cloud services provider's activities balancing between security and innovation. With regard to data localization aspect, it is important to underline that while the data hosted by a CSP could reside in multiple geographical there are some EU regulations requiring confining data in a specific region for security purpose. One example in that sense is the GDPR regulation that set certain requirements for personal data transfer outside of the Europe region conditioning the choices of the banks about CSPs providers that must comply with those requirements. It is important also to underline that at the same time the European Commission's proposal for a framework for the free flow of non-personal data is a step forward towards removing the barrier relating to data localisation restrictions let the banks to have much freedom of choice. With regard to audit rights, current European regulation requires banks to be able to access and audit data when it is physically located on a server within the CSP's network. The EBA's cloud outsourcing recommendations mandate that banks must not only ensure that their CSPs fulfil all regulatory requirements, but that any subcontractors of those CSPs do also. This poses a big challenge for the banks that have little control over the nature of a CSP's completely outsourcing chain. Fortunately, the EBA's report on outsourcing could provide a way out for the Banks, recognising alternative solutions to onsite audits such us: pooled audits, third-party certification and third party or internal audit reports available by CSPs.

7.1.3. Blockchain Regulation in Europe

The following regulations or actions establish rules for the adoption of block chain technologies in general:

- **The European Commission (EC) Fintechs action plan March 2018:** The European commission is evaluating legal, governance and scalability issues, support interoperability, standardisation efforts, including use cases of Blockchain, and its applications in the context of the Next Generation Internet.
- **European Parliament's Draft Resolution on Blockchain:** which provides recommendations for the creation of a strategic plan for building Blockchain-based infrastructure among EU countries. It is important to underline that Blockchain technology is having a major impact on the banks because it may lead to improved transparency and security at the same time reducing the costs. According to some estimates, the banks will save costs associated with cross-border payments, securities trading and regulatory compliance at US$15–

20bn a year by 2022. The EU Blockchain Observatory and Forum (which was launched by the European Commission in February 2018) should help realize further engagement in this field, by monitoring trends, developments and expertise to foster the investigation of cross-border cases of block chain use. Typically, Blockchain use cases focus on existing bank services and processes so the majority of regulation and law should remain applicable to a Blockchain solution such as civil law for contracts and banking regulations for industry processes securities transactions, payments, client data and security in general.

At the same time, the regulators are currently assessing Blockchain use cases and its potential impact on the banking industry in order to create a secure legal framework for emerging applications. The Financial Stability Board (FSB) is working together with the Committee on Payments and Market Infrastructures (CPMI) in order to identify critical issues that regulators need to address. The CPMI released a report that evaluate the potential impact of block chain on payments, clearing and settlement in February 2017, which confirmed the need for a legal framework, while calling for robust governance structures and data controls. Moreover, it is important to consider how the GDPR (applicable since May 2018) can affect the adoption of Blockchain application, including in the banking industry. Indeed GDPR was conceived based on the idea that all data related procedures, from the collection to the storage and processing stages, are realized centrally, not a decentralised ledger. Moreover, the GDPR ensures the right to data subject to have their data erased or amended on demand, which is not the case of constantly growing, append-only databases, as in the case of Blockchain applications. Additionally, the concept of “data controller”, requested within GDPR prescriptions as a role that is responsible for data use and protection, is difficult to guarantee in an open, permission less Blockchain. Finally, the fact that GDPR prescribes that data can only be transferred to third parties outside the EU if the location in question offers equivalent levels of protection, calls for specific considerations and appropriate strategic solutions in order to be ensured within a distributed ledger environment.

Another relevant aspect to consider are the potential conflicts of law related to cross-border transactions for which the competent jurisdiction and applicable law might not be easy to determine in the case of a distributed ledger considering traditional criteria of legal certainty of ownership rights. As, cross-border transactions are an area where Blockchain offers significant potential, in March 2018, the European Commission proposed a set of common conflict of laws rules on the third-party effects of assignments of securities claims, suggesting that the law of the country where the assignor has its habitual residence will govern the third-party effects of the assignment of claims. This approach aims at introducing legal certainty in order to promote cross-border investment and contribute to market integration.

7.1.4. Artificial Intelligence Regulation in Europe

The following regulations or actions establish rules for the adoption of Artificial Intelligence technologies:

- **EC communication on Artificial Intelligence for Europe March 2018:** which aims at fostering AI’s adoption and capabilities development in Europe, while promoting socio-economic changes and ensuring appropriate ethical and legal framework to promoting innovation and respects the Union's values and fundamental rights (i.e. accountability and transparency). This is particularly relevant as AI and machine-learning techniques have been frequently used in capital markets domains, gaining increasingly attention for its applications in the recent years. As concerns the banking sector, AI is expected to provide major benefits in terms of revenue growths if appropriately implemented considering relevant regulatory trend and challenges. Indeed, because this technology requires the availability of large quantities of data, as well as new high-performance computing and networking (e.g. cloud computing), data privacy regulations remain a primary relevant point of reference. In this domain, the EC’s European Group on Ethics in Science and New Technologies (EGE) considers ethics as a core point to be addressed by fostering the definition of a common, internationally recognised ethical and legal framework for the design, production, use and governance of

AI. This evolution of the ethical and regulatory framework is particularly relevant as until now, the available regulations are not up to date respect to the performance and potentialities of AI technology, in particular in the banking and capital market sector, which can constrain the employment of AI solutions in this domain. Among other, the application of AI solutions in the banking sector should take into account algorithms accountability, information (raw data and elaborations) privacy management, transparency towards clients (letting them know whether they are dealing with humans or digital artefacts) and potential limits to what AI systems can suggest to a client (e.g. for investments decisions).

Considering the possible applications of AI in the banking sector, new rules should be defined as to minimize constraints to technological progress while guaranteeing the appropriate protection of rights and conditions. Promising steps in this direction include the EC's review of the current financial services regulatory framework, trying to determine its future fitness for emerging technologies such as AI. To appropriately address this point, banking operators will have to be prepared to conduct stress testing of algorithms, including via the use of Sandboxes simulating how AI solutions would react to extremely high client demand or how would it treat anomalies. Besides AI algorithms reliability, as previously mentioned, data privacy is a relevant point to take into account as, typically, customers are willing to provide banks with their financial data in change of improvements in the service but there might be potential resistance or obstacles in the collection of further data useful for AI computations (e.g. social media related data).Moreover, it is similarly important to consider how the output of customer analysis should be protected, ensuring the anonymity of individual consumers while facilitating the safe and efficient use of big data for better services, finding the appropriate strategic and technological solutions for this purpose.

Given these considerations, and in order to ensure transparency and appropriate use of AI, including in the banking sector, most recent developments at EU level include the EC's EGE launch of a process towards a common, internationally recognised ethical and legal framework for the design, production, use and governance of AI, including principles for responsibility, rule of law and accountability, protections against risks stemming from 'autonomous' systems, safety and privacy. In a medium term perspective, a core aspect to be addressed will also be related with the aim of ensuring that all decisions made using AI are explainable, transparent and fair, which currently is only initially addressed through industry based initiatives such as the Institute of Electrical and Electronics Engineers' policy paper and Google's DeepMind.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

8. Fintechs Market Pull - Push forces responsive to the Regulatory and Market Demand

8.1. What are Push and Pull Factors in Business

Push and Pull Factors in Business defined as various aspects of directive forces for companies/corporations who decide to expand abroad and enter international markets for a variety of reasons. The different objectives at the time of entry should produce different strategies, performance goals, and even forms of market participation. However, companies often follow a standard market entry and development strategy. The most common is sometimes referred to as the "increasing commitment" method of market development, in which market entry is done via an independent local partner. As business and confidence grow, a switch to a directly controlled subsidiary is often enacted. This internationalization approach results from a desire to build a business in the country-market as quickly as possible and by an initial desire to minimize risk coupled with the need to learn about the country and market from a low base of knowledge.

There are several drivers of international business. The driving forces that motivate companies/corporations to expand abroad may be classified into pull forces and push forces. The pull forces are proactive which pulls the business to foreign markets. The push forces, on the other hand, are reactive forces that promote the companies to go international (UKEssays.com 2017).

8.1.1. Pull/ Proactive Forces- Attractiveness of the Foreign Markets:

- **Profit advantage due to increase in volume:** For companies, mostly in developed countries, which have been operating below their capacities, the developing markets offer immense opportunities to increase their sales and profits.
- **Low wage/ cheap labour attraction:** Many multinational companies (MNCs) are locating their subsidiaries in low wage and low-cost countries to take advantage of low-cost production.
- **Taking advantage of growth opportunities:** MNCs are getting increasingly interested in the number of developing countries as the income and population are rapidly rising in these countries. Foreign markets, in both developed countries and developing countries, provide enormous growth opportunities for the developing country firms too.
- **Growth of regional trading blocs:** Regional trading blocs are adding to the pace of globalization. WTO, EU, NAFTA, MERCOSUR, and FTAA are major alliances among the countries. Trading blocs seek to promote international business by removing trade and investment barriers. Integration among countries results in inefficient allocation of resources throughout the trading area, promoting the growth of some business and decline of others, the development of new technologies and products, and the elimination of old.
- **Declining trade and investment barriers:** Declining trade and investment barriers have vastly contributed to globalization. The free trade regime, business across the globe has grown considerably. Goods, services, capital, and technology are moving across the nations significantly (Kirkwood 2009).

8.1.2. Push/ Reactive Forces- Compulsion of the Domestic Market:

- **Saturation of domestic demand:** In advanced markets, the number of products tend to saturate or decline when the market potential is almost fully tapped. Often international operations are undertaken by businesses to counteract the saturation by acquiring resources from foreign countries, to diversify their product range and to expand sales.
- **Scale economies and technological revolution:** Due to technological advances the unit production costs have drastically be decreasing, allowing economies to produce in large-scale operations. This requires economies of scale to further leverage foreign markets, additionally to the domestic market.
- **Technological revolution:** In recent years, significant technological developments arose in communication, transportation and information processing. This includes the emergence of the Internet and the World Wide Web.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

- **Competition as a driving force:** While there is often little competition in foreign markets, a domestic market might have too many competitors. Therefore, businesses tend to go to international or foreign markets to gain first mover advantage.
- **Government policies and regulations:** Internationalisation of some companies is also triggered by government policies and regulations. While some governments offer incentives and support to attract domestic companies to invest into foreign markets often regulations are also hindering companies to establish a market.
- **Strategic vision:** Many companies are going to international markets to grow their business, become more competitive and to gain strategic advantages over their competitors (Kirkwood 2009).

8.2. Push-Pull Forces in terms of Fintechs

After a record-setting 2018, the first half of 2019 got off to a quiet start for Fintechs investment globally which mirroring a trend seen in the broader VC (Venture Capital) market. The steep drop-off in investment reflected the lack of blockbuster deals such as the $14 billion raised by Ant Financial or Vantiv’s acquisition of Worldpay for $12.9 billion during H1’18. Global uncertainty, regulatory changes in China, and the US-China trade tensions likely also contributed to the decline. Fintechs investment in the Asia Pacific plummeted during the first half of the year, driven by uncertainty and increased regulatory scrutiny in China. Meanwhile, despite the ongoing concerns around Brexit, Fintechs investment got off to a very strong start in Europe. While well off the pace required to match 2018’s massive investment record, Fintechs investment in the Americas was also very good during H1’19 (Pollari and Ruddenklau 2019).

After some difficulties in 2018, Blockchain-based cryptocurrencies got a fresh breath of life in H1’19 with Facebook’s announcement of Libra which is expected to launch in 2020. The new cryptocurrency is being jointly driven by the Libra Association, which is a consortium of big internet organisations. While payments continued to draw the most significant attention from Fintechs investors across most jurisdictions, H1’19 also saw the continued maturation of the Fintechs industry as a whole and the broadening of its definition. Areas like Wealthtechs, Proptechs, and Regtechs also grew on the radar of investors (Pollari and Ruddenklau 2019).

Insurtechs continues to attract large funding rounds and had a banner year in 2018 in terms of funding, with 14 Insurtechs deals at $100 million or more. The strong pace of investment showed no sign of easing in the first half of 2019. Globally, in the first 6 months alone there were 74 deals with a total value of $1.15 billion. Insurtechs solutions are continuing to expand, with the industry rapidly embracing artificial intelligence. Lemonade, for instance, uses its bot, Maya, to help expedite the claims process and formulate the best insurance plans for customers. On-demand insurance is also on the rise, with many insurance companies now offering some form of on-demand service (Pollari and Ruddenklau 2019).

Digital banking Fintechs is mature, willing to expand and continued to draw significant venture capital interest during H1'19, not only in Europe but globally. Digital banks in Europe have matured quickly, with a number now focused on international expansion. OakNorth, for example, is expected to use the funds from its latest funding round to fuel expansion into the US. A number of UK and Germany-based challenger banks are also looking to expand outward, including Monzo, which announced plans to offer services in the US; Revolut, which announced the launch of a beta version of its app in Australia; and N26, which recently announced plans to launch its retail banking service in Brazil (Pollari and Ruddenklau 2019).

Challenger banks were also a hot topic in the Asia Pacific during H1’19, with the issuance of eight digital banking licenses in Hong Kong (SAR), China and Singapore’s announcement that it will also issue up to five digital banking licenses. These licenses are expected to spur ongoing interest in challenger banking in the region (Pollari and Ruddenklau 2019).

8.2.1. Blockchain in Fintechs

Last year Fintechs saw more investment that is private by count within the Blockchain and cryptocurrency space than ever before. This year is turning out a little differently, with good reason, a slower investment pace after any such single-year surge is only to be expected, given reversion to the mean. More importantly, it must be noted that even this year's slowing activity is on pace to yield 300+ transactions, more than any other year. Pairing that pace with the return to normal levels of VC invested, it is clear that investors are simply biding their time while the flock of heavily funded Blockchain companies in the past 2 years proves which solutions actually work (Laszlo 2019).

8.2.2. Security Aspects of Fintechs

Analyses in Fintechs intersection with other key arenas have produced intriguing insights, particularly the overlap between Fintechs and cybersecurity. Pure-play solutions in this realm are not quite as common as one would suspect, hence the overall levels of private investment are more muted than others, but over the past few years, and they have been quite persistent and robust. This year is on pace to record potentially a slight new high in volume, as companies tackle the vexing and pressing problems of securing financial value chains from myriad threats (Bedri 2019). Attacks on Fintechs companies have risen significantly year to year. Money laundering investigations and owners' fights bring more risks and threats available to public eye. Global money laundering and tax evasion schemes are discovered. Digital currencies have been stolen and lost because of use insecure environments. Security conditions have a significant impact on the Fintechs sector.

8.2.3. European Market Demands

While overall Fintechs investment in Europe dropped in H1'19 Strength of the UK's Fintechs sector provides resilience. Despite ongoing concerns related to Brexit and a government leadership election, the UK continued to attract a significant amount of Fintechs funding during H1'19. UK-based firms accounted for six of the top ten Fintechs deals in Europe at mid-year, including an $800 million investment by the SoftBank Vision Fund into Greensill Capital, the $717 million acquisition of payments firm WorldFirst UK by Ant Financial and a $440 million raised by OakNorth led by the Softbank Vision Fund (Shanghai Diarong Financial Information Services 2019).

While M&A activity in the UK was sparse compared to other locations, the region saw companies using other means to allow early investors to exit. In May, global money transfer company TransferWise issued $292 million worth of private shares to BlackRock, Lead Edge Capital, Lone Pine Capital, and Vitruvian Partners. The company now valued at $3.5 billion is considered the most valuable Fintechs in Europe (Shanghai Diarong Financial Information Services 2019).

On the other side European challenger banks targeting global growth and the Fintechs companies in Europe are maturing quickly, with a number now focused on international expansion. For example, OakNorth is expected to use the funds from its latest funding round to fuel expansion into the US, and while the company is an SME-focused bank in the UK, it is focusing on B2B opportunities for growth. A number of UK and Germany-based challenger banks are also looking to expand outward, including Monzo which has announced the plans to offer services in the US, Revolut has also announced the launch of a beta version of its app in Australia, and N26 has recently announced plans to launch its retail banking service in Brazil (Pollari and Ruddenklau 2019).

In conclusion, unlike other regions, Europe has seen not only consistent pacing of deal volume, but also a surge in deal value associated with corporate players. Outliers certainly skewed that total, but it does speak to corporate players' eagerness to gain exposure at the late stage to Fintechs companies that are emerging as category leaders.

9. Financial Sector Transformative Responses to Distributed Ledger Technology trends

9.1. Definition of DLT

Distributed ledger technology (DLT) is a giant append-only log file replicated across a set of participating nodes. When a new log entry is to be appended, participating nodes vote on whether it complies with the DLT's rules and come to an agreement regarding the admission and the order of new log entries. This agreement is known as consensus, and the protocol ensuring it is called the consensus protocol. Access to information can be granted to anyone (public ledgers) or restricted to specific users or groups (permissioned ledgers). The "Blockchain" term, refers to a specific implementation of distributed ledger technology (DLT), whose distinctive feature consists in grouping individual transactions in "blocks", each one joined to the preceding and following one, forming a long "chain" of transactions, set in chronological order. Blocks are linked together using cryptography, therefore ensuring integrity of data over the time.

What makes DLTs a disruptive technology is that they offer a tamper-proof database where trust emerges through the collaboration of a set of computers, rather than through an institution or organisation, that imposes trust from the external world onto the system. A distributed ledger can be roughly considered as a digital registry of information, replicated and shared through a network, among a number of peers. These features can be of great value for financial applications, paving the way to the implementation of innovative exploitation scenarios.

DLTs' most innovative breakthrough is the creation of trust based on many generally untrusted nodes. This is achieved through sophisticated consensus mechanisms, which are central to the operation of DLTs. Several DLT consensus mechanisms have been devised, having significant differences, yet a common goal: enabling the entire network to decide unanimously and inadvertently on which records to include next, and in which order, into the DLT. The protocol constitutes, essentially, a voting mechanism used for filtering and ordering the records that are stored into the DLT.

The ledgers' policy on which nodes can act in which roles, places the ledgers into two broad categories: permission less and permissioned. In permission less or open ledgers any computer that has network access may join the ledger, taking up any role. That is, it may opt to participate as a validator to contribute to building consensus, as a verifier to read and locally verify blocks, or simply as a user and issue new transactions. In permissioned ledgers, a node needs to be authenticated and authorized to take up certain roles. For instance, a ledger could restrict the validators to a predefined set of authorized nodes but let any node to locally verify the correctness of the ledger.

Smart Contracts bring ground-breaking innovation to the DLT world. Rather than using DLTs' decentralized trust model for offering just an immutable decentralized append-only data store, they exploit the mechanisms to provide a tamper-proof decentralized "world computer". Through smart contracts, DLTs are promoted from special-purpose tools serving a single application to general-purpose platforms, allowing developers to deploy and execute custom code that may implement arbitrary application logic.

DLT is essentially a process, where distrustful parties can use technology to conduct their business without relying on a centralized trusted third party.

9.2. Commercialization of Blockchain/DLT

Blockchain and distributed ledger technology will continue to be an area of exploration inside and outside of traditional financial institutions. The new trend, however, will be transitioning from patent filing, proof-of-concept experiments and limited-function niche applications to broader applicability and live production with the aim of commercializing investments.

The varied Blockchain/DLT-based use cases Fintechs's and financial institutions attempt to commercialize take more time than planned. It will be five to 10 years before there is marketplace consensus around the financial applications best suited for Blockchain/DLT solutions. Until then, we will see Fintechs's and financial institutions continue to experiment but in a way that is less academic and more conscious of Blockchain/DLT as a cost-cutting, fraud preventing or market expanding solution—in other words, with a focus on how Blockchain/DLT offers clear-cut advantages over conventional technology solutions.

9.3. Customer Service through Chatbots

The application of artificial intelligence is a Fintechs trend on its own and takes many forms (like reducing fraud and false positives in payments processing), but the most exciting and tangible AI trend is automating customer service through chatbots—embedded within apps or through social media.

The West is light years behind the East—especially China and Japan—in adopting chatbots, and financial institutions have been slow to adopt the technology. The Fintechs's and financial institutions recognize the power of AI-powered chatbots that get smarter over time, eventually supporting full conversations through advanced speech and natural language processing capabilities.

When this happens, AI-powered chatbots will deliver benefits beyond the obvious human labour cost saving, providing true virtual assistance—including transactional capabilities, advice based on individual behaviour patterns and even opening accounts. Financial businesses providing these smart chatbots will capture the added benefit of rich data to target offers and anticipate their customers' needs—creating a continual feedback loop and building. AI-powered chatbots will incorporate sentiment analytics, enabling responses that match human tone and emotion, and even mimicking geographic accents—giving customers the experience of communicating with a "person" just like them.

9.4. The Last Mile in Digitizing Financial Services

Nearly all Fintechs's and many financial institutions enable customers, consumers and businesses, to conduct most of their financial business digitally. Yet, there are gaps in digital service—most notably in account opening and particularly for business customers—requiring personal visits to branch offices.

If financial institutions do not have end-to-end account opening digitization on roadmaps, they should. Beyond being a significant convenience for customers—who, increasingly, are not just digital-first but digital-only in handling their finances—digital account opening is an extreme advantage for online-only challenger banks and online lenders, which have perfected digitization of customer-facing activities and live and die by their UX.

The last mile digitization trend also extends to the back office—upgrading operations to support digital delivery and, most importantly, blasting through the siloes that are remnants of legacy software and prevent financial institutions from effectively accessing and using their own data.

9.5. Biometric-Based Fraud Prevention

Biometrics-based fraud protection is a trend that will gain momentum. It should have happened sooner given the soaring growth in digital financial services and ecommerce, which beg for biometric customer authentication. On the other hand, biometric-based fraud prevention is complicated on levels beyond technology—cost, standardization and, importantly, culture.

The old businesses will not expend funds to replace a fraud-prevention system until its cost becomes greater than the cost to change. We are not there yet, but the writing is on the wall. Fraud is a huge problem and fraudsters are getting smarter in exploiting vulnerabilities. The current systems of authentication are not adequate to address the present and future challenges.

The market, which has pushed back on biometrics for reasons of privacy, is becoming desensitized as it is common to use fingerprints to open mobile devices, have retinas scanned when crossing borders and open computers via facial recognition. Then, there is the weight of numerous and cumbersome passwords. How much easier is it to authenticate identify with something you always have with you—your finger or palm, retina or voice—vs. a “secret” code?

In 2019, biometric-based fraud prevention—as part of a multi-factor authentication program—is no longer a trend Fintechs’s and financial institutions can avoid.

9.6. Fintechs's and Financial Institutions Playing Cat and Mouse

We will continue to see financial institutions working individually and collectively on capital-intensive development efforts, like Blockchain/DLT. For other tech development—especially with targeted audiences like consumers or SMEs—the cat-and-mouse game will continue with financial institutions carefully watching promising Fintechs’s and moving quickly on strategic acquisitions to enhance their capabilities. Fintechs's with solid vision, backed by great execution, will be rewarded. Fintechs's without a viable value proposition or poor execution will continue to burn cash (Gengler 2018).

9.7. Benefits from Using DLTs in Financial Sector

Replicating and spreading data across a network of peers through DLTs, rather than keeping them managed and stored by a single, central entity brings with it great advantages and a new set of points of attention to take into account, while delivering digital financial services in innovative ways.

Transparency in operations greatly benefits from DLTs, as any party allowed to do it – thanks to cryptography - will be potentially able to see any changes to the data, therefore rendering extremely difficult to tamper with them without all the other peers being aware of it.

Therefore, trust between parties is technologically enforced for the benefit of everyone: no one is the owner of the entire service delivery infrastructure, no one has exclusive ownership of data, and no one can repudiate transactions validated by cryptographic techniques.

Nowadays most of financial institutions have their own internal validation and reconciliation processes and systems, which is a very inefficient and costly practice: by adopting DLTs for securely sharing data between parties, near real time, cost-effective reconciliation processes could be obtained.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

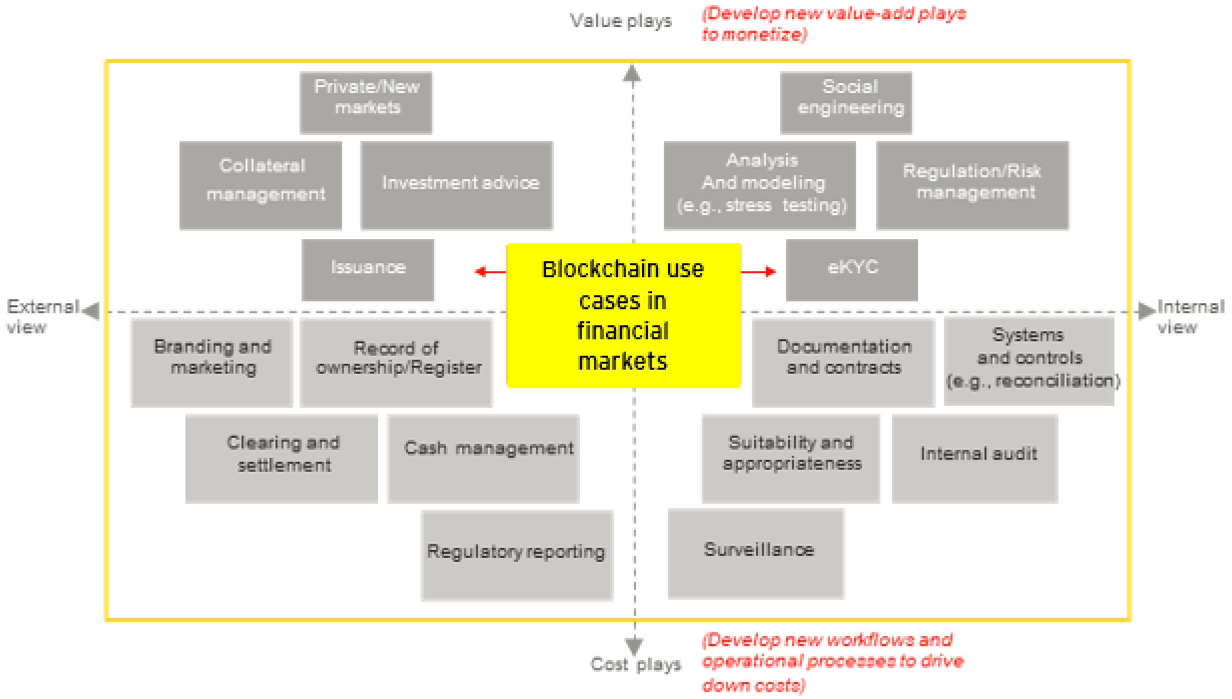

Value plays
(Develop new value-add plays to monetize)
Private/New markets
Social engineering
Collateral management
Investment advice
Analysis And modeling (e.g., stress testing)
Regulation/Risk management
Issuance
Blockchain use cases in financial markets
eKYC
External view
Internal view
Branding and marketing
Record of ownership/Register
Documentation and contracts
Systems and controls (e.g., reconciliation)
Clearing and settlement
Cash management
Suitability and appropriateness
Internal audit
Regulatory reporting
Surveillance
Cost plays
(Develop new workflows and operational processes to drive down costs)

Figure 2. EY (2019), "Blockchain use cases in financial sector"

By using DLTs which supports Smart Contracts, transactions can be processed automatically according to agreements established between parties, which defines a set of rules thanks to which the ownership of an underlying value or asset can be automatically transferred. This mechanism has plenty of applications in financial institutions, which is a contract-based world. Automating the enforcement of contracts' clauses, based on a secure, shared, tamper-proof set of rules, implemented through smart contracts, can bring significant savings by improving efficiency and by reducing disputes between involved parties. See Figure 2 for the overview of Blockchain use cases in financial markets

9.8. Benefits for using DLTs in the Securities market

There are several potential applications of DLTs in the securities market that are currently under thorough evaluation by domain's experts. Some general benefits, natively brought by the adoption of these novel technologies, could significantly increase process transparency and efficiency, while distributed apps can increase data and service resilience, therefore generating direct cost savings in the following areas:

9.8.1. Settlement cycle

Direct interaction between issuers and investors, or a lower interaction between them and a small number of intermediaries, securely mediated via DLTs, could dramatically improve efficiency by shortening the service delivery chain and reducing the number of actors involved in the process. Furthermore, the number of collaterals needed for the settlement will be significantly lowered and kept on hold for a shorter time. Finally, Asset Management and Servicing will be simplified by issuing securities directly on DLTs and consequently easing to track their ownership.

9.8.2. Near-real-time Operations and Access to the market

DLTs somehow introduce a standardized and easier way to integrate operators worldwide and working around the clock, could push the globalization process of the securities' market. Accessing the market will not only be easier from a technological point of view: small and medium enterprises (SMEs) could issue securities directly through DLTs, gaining access to funding and to a wider (global) pool of potential investors, which could possibly offer them the opportunity to expand their business.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

9.8.3. Automation

Once involved parties agree upon a set of rules and validate a Smart Contract, which enforces its operations on distributed ledgers could be fully automated in a high-trust context, reducing operational costs and mitigating the risk that potential disputes could arise. These considerations strongly apply to Reconciliation processes, which requires accuracy, non-repudiation, repeatability, certification of data and full transparency on operations.

9.8.4. Compliance and Reporting

DLTs can be used to build “live reporting” systems, potentially demonstrating an evidence-based compliance to authorities, competent bodies, auditors, interested parties, simply by putting (or hash-linking) “digital evidence” on public ledgers, rendering them tamper-proof and non-reputable. Compliance could be demonstrated on a day-by-day basis and regulators for financial sector could even have visibility on operations in near real time when needed, therefore again dramatically improving transparency and process’ efficiency.

9.9. Let us stay grounded when talking about financial processes

Even considering the great enthusiasm and potential for DLTs’ application in financial world, one should consider there are still important aspects that needs careful reflection. First, let us again consider the significant example of issuing securities directly on a public ledger, to carefully assess the impacts. Issuing securities, includes a number of other important activities besides just recording the newly issued ones: for example, the need for bookkeeping and notary functions still remains, for making sure that no unwarranted securities are created and that only publicly issued securities are actually traded. It is extremely important to keep a high level of trust between the issuer and the buyer of the security. Central securities depositories are usually responsible for this function and even if, in the future issuers will directly interact with investors via a DLT, an accountable body/institution would still be needed to validate the transaction, exactly as is the case today.

In *delivery versus payment (DvP)* scenarios, the settlement process requires that transferring of securities, takes effect at the very same time the agreed payment is executed. This is done to mitigate the risk that in a trade, one of the parties misses to deliver the security, while the other party has already delivered the cash yet. TARGET2-Securities platform (T2S), a system strongly wanted by the European Central Bank, currently supports central securities depositories (CSDs) in increasing their efficiency and competitiveness while regulating settlements and – at the same time - contributing to integrate and harmonise the highly fragmented securities settlement infrastructure in Europe. T2S currently supports secure Delivery versus Payment operations, because the platform holds both the central banks’ cash and securities accounts eliminating settlement risk. On DLTs similar measures should be implemented, for example by leveraging on virtual currencies and smart contract technology, but this is still far to be possible, mainly due to lack of specific regulation.

Finally, if via DLTs, issuers would directly interact with investors; with no need for intermediaries (financial institutions), regulators should clearly define who would be responsible in case of technological failures and which stakeholders in the novel scenario should be subjected to regulations, in order to ensure the settlement system keeps stable.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

10. Fintechs Market Analysis

10.1. Changing Consumer Priorities

Digital transformation is reshaping financial services with incumbent and challenger banks that need to be attuned to the evolving expectations of their customers. Challengers particularly, have built themselves with a design-first approach and agile work processes, by keeping a technology forward mind-set; they are able to offer Fintechs services that are accessible, personalized, transparent and cost-effective. On the other side, incumbents are most responsive with a tendency to disrupt their own proposition by offering comparable Fintechs services, either through partnerships, acquisitions or in house development. In recent years, incumbents have brought their Fintechs versions of services such as online foreign exchange, online investments advice and management or peer to peer payments.

In effect, Fintechs has redefined the rules of the game in financial services. What was considered new and disruptive in 2015 has become a prerequisite for all the players in 2019. With so many participants now offering similar services, each company must strive to differentiate itself to attract and retain customers, whether by brand, price or execution.

For a company, stand out helps to have a keen appreciation of what Fintechs adopters want. As highlighted in Figure 3 adopters are much more willing than non-adopters to favour an online tool or app that allows them to view all their financial products in one place, they are more worried than non-adopters about the security of their personal data. Security concerns are less pronounced in Sweden, Germany, Belgium and the Netherlands, perhaps due to strong data protection regulations in those markets[1]. Overall, despite their security concerns, adopters are comfortable with online aggregator sites and all-digital branchless financial services.

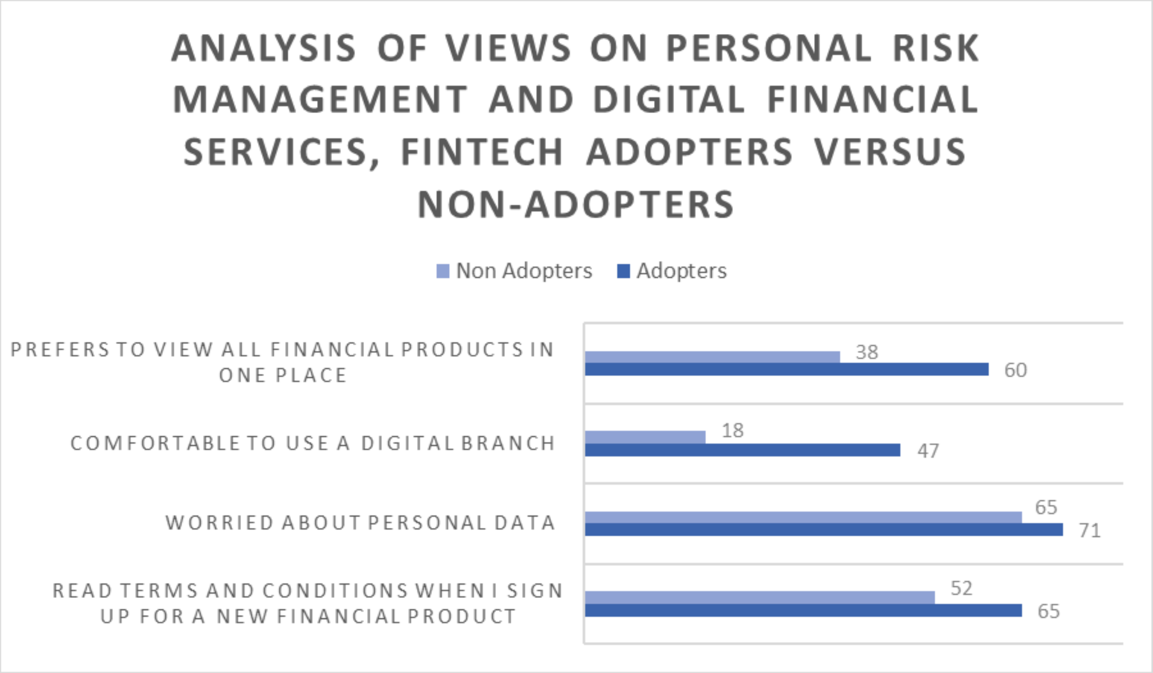


Figure 3. EY (2019), "Fintechs Adoption Index" – Analysis of Views on Personal Risk Management and Digital Financial Services, Fintechs Adopters vs. Non-Adoters

One of the maturation signs of Fintechs industry is the evolution in consumer priorities when they look for a provider. In 2018[2], 30% of adopters ranked the ease of opening an account as their top priority when selecting

[1] European Commission (2018), "Fintechs Action Plan"
[2] EY (2019), "Innovation in Banking"

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

a Fintechs provider, while only 13% said attractive fees or prices were most important. In 2019, priorities flipped with 27% ranking price first and 20% picking ease of opening an account.

China is an early forerunner of a global trend sparked by increased competition, improved onboarding experiences and the portability of data enabled by technology and in some markets changes of regulation. Fewer adopters chose better experiences and access to different and more innovative products and services, as their top reason for using a Fintechs challenger, perhaps indicating the increasing comparability and competitiveness of Fintechs services provided by incumbents. Nowadays, all providers have evolved from simply trying to lure curious or frustrated consumers with an easy set-up process to developing new strategies to retain existing customer and induce them to make educated choices.

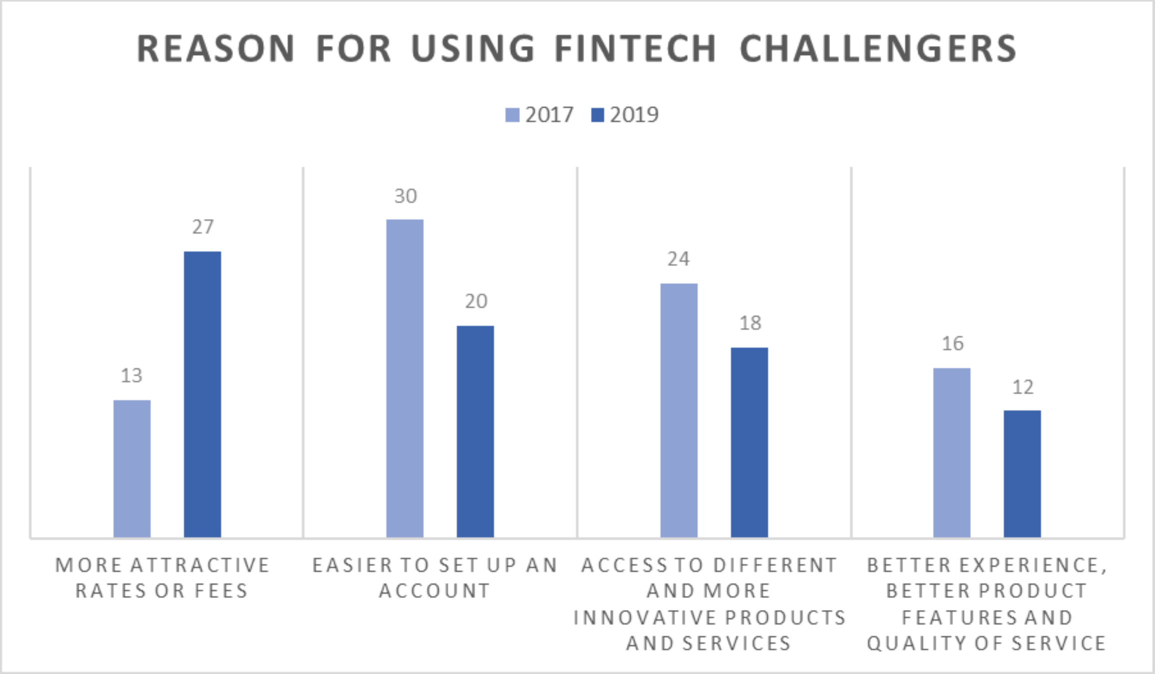


Figure 4. EY (2019), "Fintechs Adoption Index" – Reason for Using Fintechs Challengers

We also see an evolution in the attitudes of non-adopters. Lack of awareness and understanding continues to be the top reason for why consumers opt to use an incumbent financial institution rather than a Fintechs challenger and the reason is clear: non-adopters choose to remain with incumbent providers because they trust them more than Fintechs challengers. Trust is the top barrier to using a Fintechs challenger in markets such as Italy or France. As more incumbents offer their own Fintechs services, their ability to build on pre-existing trust takes on new significance.

10.2. Rise of non-financial services companies and the growth of ecosystems

Challengers and incumbents alike face a new competitive threat that comes from outside the financial industry altogether. Non-financial services companies such as retailers, technology platforms, and automakers are increasingly developing their own technology-enabled financial services offerings. These organizations build on existing relationships with customers to offer holistic propositions accompanied by complementary services, including activities such as insurance and lending that were once the exclusive purview of financial providers.

Non-financial service companies enter the game having already gone through their own transformations around innovative technologies. They have redeveloped their original consumer propositions to become faster, frictionless, cheaper and more convenient. Their successful transformation influence consumer perceptions and expectations toward financial offerings. 68% of consumers are willing to consider a financial product offered by a non-financial services company. They are most open to retailers (45%) and telecommunication firms (44%[3]) as service providers, and most willing to use money and transfer payment Fintechs services such as digital only banking and multi merchant eWallets.

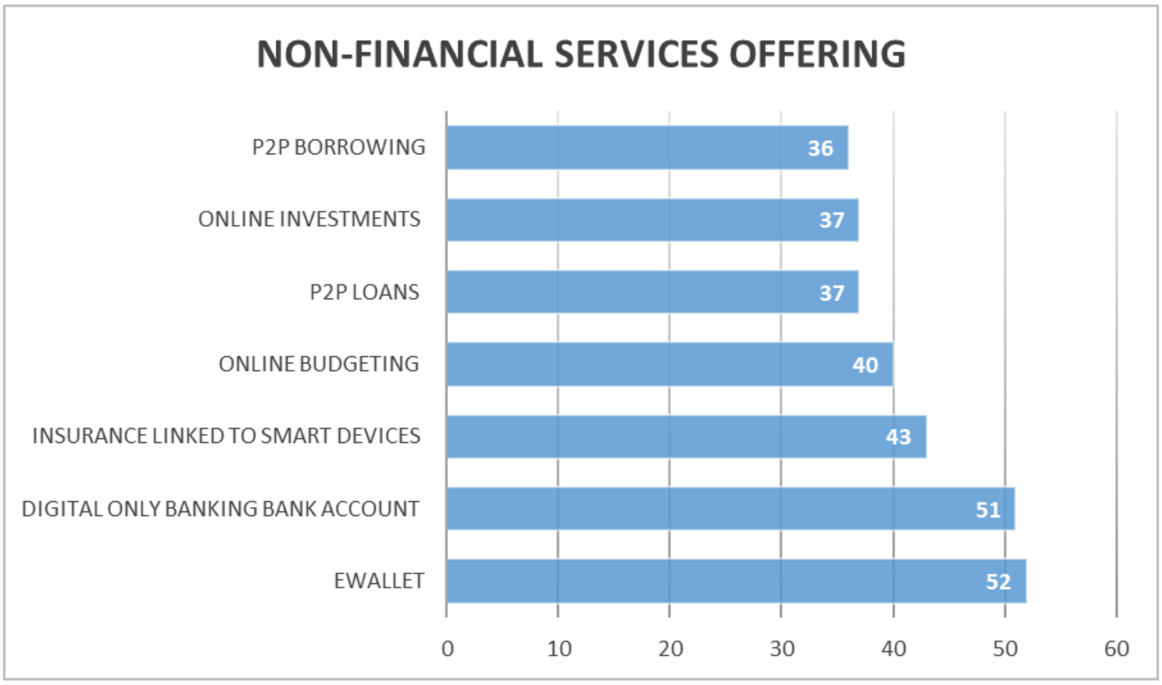


Figure 5. EY (2019) "Fintechs Adoption Index" - Non-financial Services Offering

Fintechs adopters are much more willing than non-adopters to consider financial products offered by non-financial services companies. However, even 30% of non-adopters are willing to consider a digital only bank account from a non-financial services company.

Many Fintechs proposition depend on the easy portability of data, such as during onboarding or in enabling real time account access. However, 46% of Fintechs adopters are willing to share their banking data with other organizations in exchange for better offers but they are hesitant when it comes to sharing data with non-financial services companies. Figure 5 presents a recent survey, conducted by EY, on non-financial services offering where eWallet still has the highest rank as compared to other services.

10.3. SMEs Fintechs users

Across different markets, European SMEs seems to be more restrictive on Fintechs services compared to China ones, that displays the highest adoption rate at 61%, followed by the US at 23%. When SMEs use a Fintechs. Because SMEs commit resources and personnel to select their vendors, the decision to use a Fintechs is deliberate and made in a professional context. SMEs adopt Fintechs to address specific business problems and provide credible solutions, they provide a good a good range of functionality and features, have services available 24 hours a day, and are easy to set up, configure and use. The results of the EY's latest survey on top reasons for using Fintechs in Europe by SMEs are illustrated in Figure 6.

[3] EY internal analysis

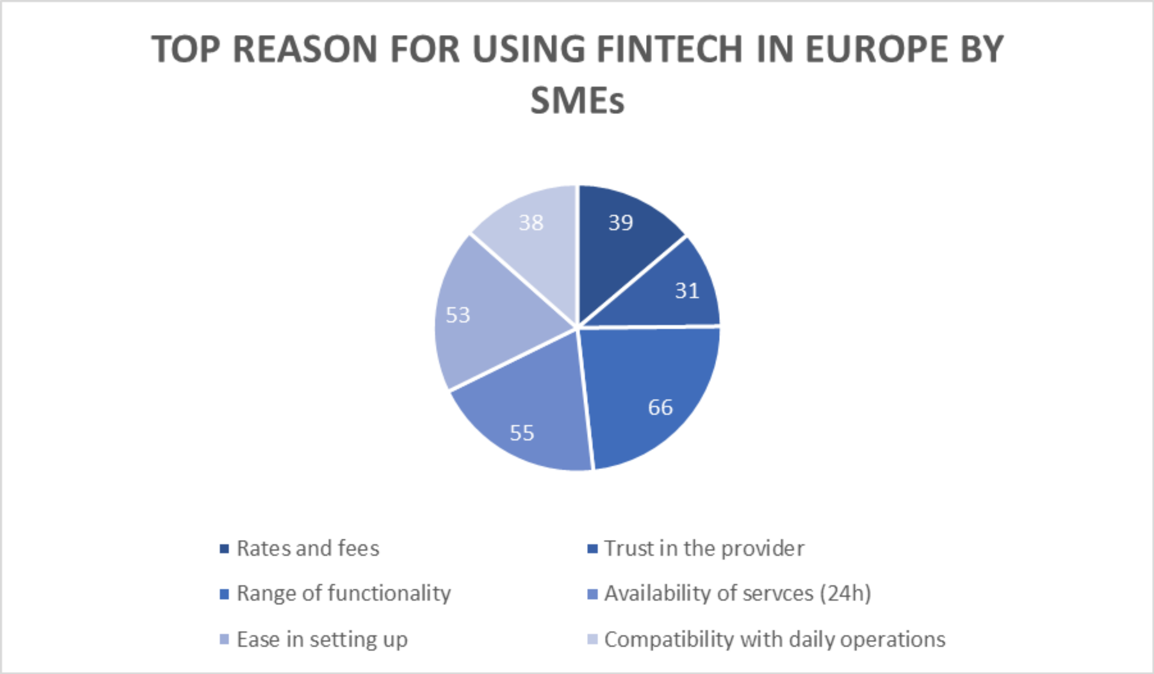


Figure 6. EY (2019) "Fintechs Adoption Index" – Top Reasons for Using Fintechs in Europe by SMEs

10.4. European Market[4]

Most EU Fintechs operates in the areas of payment and alternative finance and Europe has five Fintechs unicorns (Adyen, Funding Circle, Klarna, Revolut and Transferwise), each of them with a value of USD 1 billion or more. Europe's particular strength is in Business to Business (B2B) rather than Business to Consumer (B2C). There is not only more EU Fintechs in the B2B market, but it is also attracting most of the funding. Fintechs in B2C tends to have more visibility and is masking the success of Europe in this area. Financial incumbents initially struggled to find their place, and, for some years, Fintechs was seen as a "threat" if not as "the end of traditional banking". The rise of Fintechs in fact coincided with other phenomena such as the economic and financial crisis and the digital transformation of society. These phenomena, together with the adoption of new legislative measures, have radically changed the playing field in which incumbents have operated in the past and competition, especially in certain value chains, has increased.

Overall, therefore, the rise of Fintechs has quickly moved from being a threat to being an opportunity for traditional players. All have started to develop strategies for benefiting from the development of new, technology driven, financial products and services. The trend is towards more collaboration, complementarity and partnership between traditional players and new entrants.

Figure 6 presents the value of various sectors in billions where Fintechs is the champion and doubles the second sector significantly.

Figure 7 gives an overview of the value of Fintechs compared to other sectors.

[4] EY (2018), "Fintechs Ecosystem Playbook"

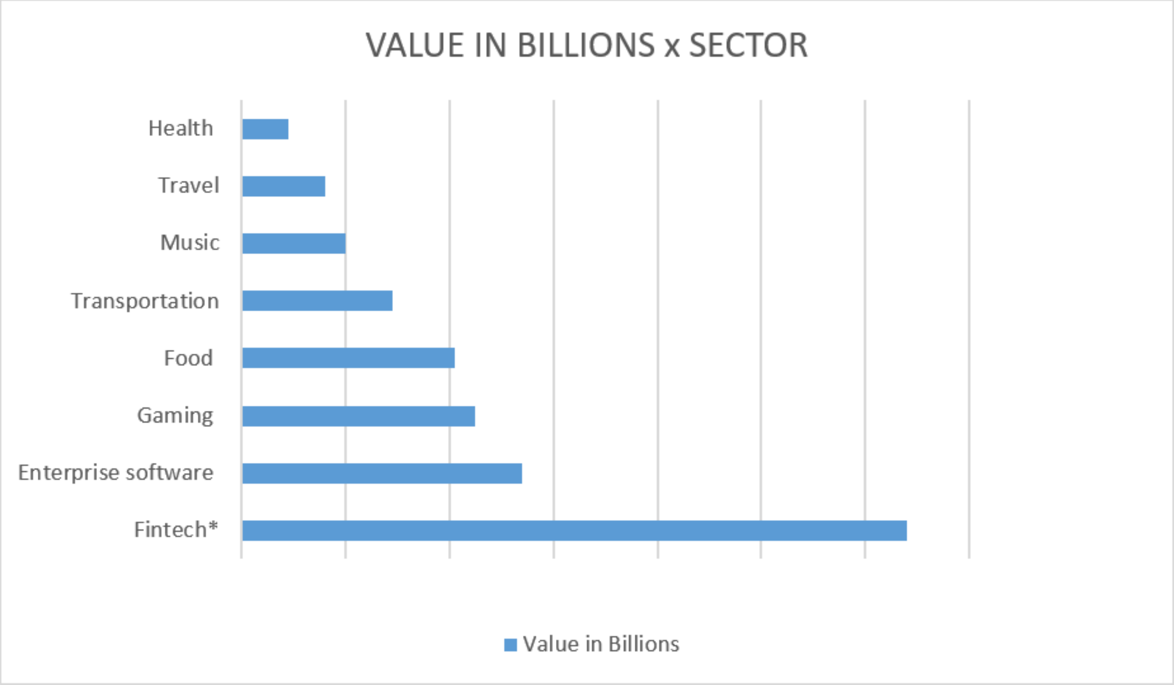


Figure 7. EY (2019) "Fintechs Adoption Index"; Value in Bilions x Sector including: banking & payments, Insurtech, Proptechs, enabling fintech platforms (es. r3)

From a geographical point of view, UK, Sweden, Germany, Ireland and Netherlands are the most developed countries in the EU. These countries have a mature Fintechs market, with the highest number of Fintechs companies as well as the highest Fintechs venture capital value compared to other countries examined. They also have a regulatory framework that favours entrepreneurs starting a business, a high innovation capacity and an entrepreneurial activity. They are economically developed with a high GDP/capita and put a particular focus on the financial sector, which is a key sector for Fintechs companies.

The UK has one of the largest financial centres in the world and London has the world's largest financial services sector. The UK ranks first in the EU in terms of the strength of the Fintechs ecosystem. However, after Brexit, Fintechs companies face uncertainty about the future of market access because of issues around passporting rules and the regulatory framework[5].

The German Fintechs market has seen strong growth over the last few years of more than 70%. The large number of incubators and accelerators established in Germany could lead to more companies being created in the Fintechs sector. If Brexit results in London will be positive, it is likely that Germany will be a draw for many Fintechs companies in future28. In terms of overall investment in Fintechs, Germany currently lags behind the UK[6].

In Sweden, the financial sector is one of the largest sectors by value in the Swedish economy. Sweden has a strong start-up ecosystem while many high-tech early adopters, and multinationals often choose Stockholm as a test market for the development of new products. The country has a steady government and a solid regulatory framework, which gives companies the opportunity to expand abroad[7].

Ireland is an international financial services hub. It has a dynamic technology sector, many financial services centres and a proactive ecosystem that can help Fintechs firms to grow. Fintechs is a key component of the Irish

[5] Deloitte (2016), "Driving Fintechs innovation in financial services"
[6] Gogardless, "What you didn't know about the German Fintechs"
[7] Investstockholm (2015), "Stockholm – Europe's No.2 Fintechs city"

IFS Strategy, the Irish Government's strategy for developing Ireland's financial services sector[8]. Ireland post-Brexit will serve as the EU's only native English speaking country.

In Netherlands, the Fintechs sector is growing fast but it is still small compared to the UK and Germany. The Fintechs sector is crucial for the Netherlands given that the contribution of the financial services sector to GDP is around 7%. The Fintechs sector is hindered by gaps in the rigidity of regulation and legal framework, regulatory execution/supervision and collaboration[9].

In France, investment in Fintechs has risen significantly over the past few years. The government is trying to encourage entrepreneurship and to boost innovation, and it has one of the highest rankings for starting a business. For instance, in 2015 alone, the government invested EUR 200 million in accelerators and incubators, as well as providing a range of grants designed to help new entrepreneurs to start-up businesses[10]. France has the potential to concentrate a large number of Fintechs companies as a result of Brexit. France has been showing signs of growth while the number of deals involving the UK has fallen since Brexit was decided, although the UK still occupies the leading position[11].

Estonia and Lithuania constitute interesting examples as they offer many digitized services to its citizens and businesses, it creates an online environment in an effort to make administrations work more effectively. Estonia is the first country to offer e-residency (a transnational digital identity available to those who are interested in creating and managing a business online). Some most innovative Fintechs in Europe has been created in Estonia (e.g. Transferwise) and it is one of the most developed countries in the sector of alternative finance[12].

Despite Europe, Fintechs is a truly global phenomenon and government around the world started to explore the opportunities arising and reap benefits offered by this new industry. New hubs are developing in cities like London (e.g. Level39) or Milan (Fintechs District) to attract this ecosystem becoming a city phenomenon, particularly in Europe[13]:

- Estonia: Tallinn
- France: Paris
- Germany: Frankfurt and Berlin
- Ireland: Dublin
- Lithuania: Vilnius
- Luxembourg: Luxembourg
- Netherlands: Amsterdam
- Sweden: Stockholm
- UK: London
- Italy: Milan

10.5. Technological excursus

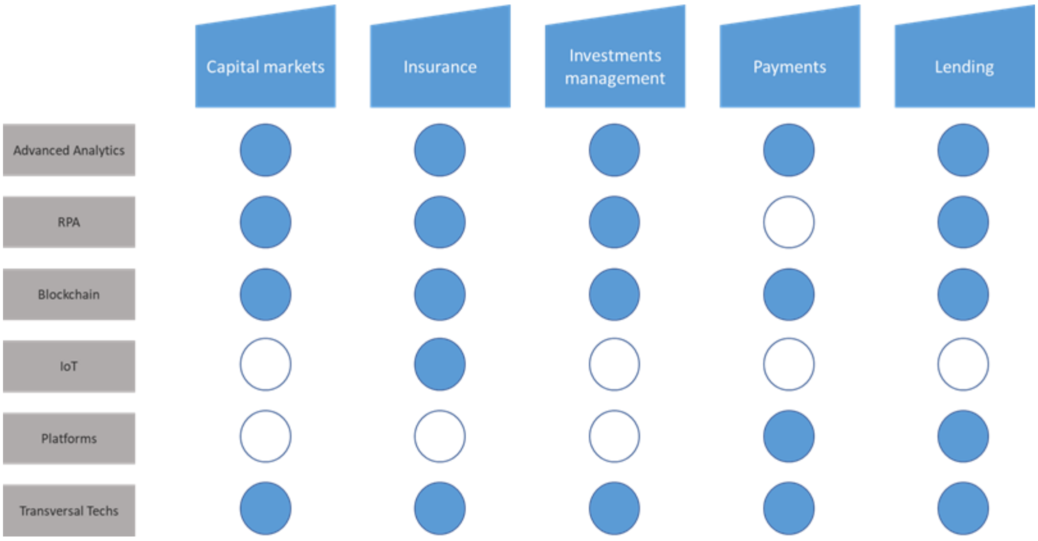
Technologies does not have the same maturity level as most of them are at the early stage of development, so, it is difficult to predict which of these technologies will have the largest impact on financial services. Some of them will impact more than others, for example artificial intelligence, in particular RPA is expected to have a great impact on capital markets, insurance, investments management and lending by providing benefits such as enhanced customer experience and cost savings. As summarised in Figure 8 advanced analytics is one of the technologies that is already impacting all the financial services providing advantages such as better risk

[8] IFS Ireland
[9] Holland Fintechs (2016), "Barriers to Fintechs innovation in the Netherlands"
[10] KPMG (2016), "Rise of entrepreneurship in France"
[11] CB Insights (2017), "European Fintechs Trends"
[12] OECD (2017),"Economic surveys Estonia"
[13] EY Internal Analysis

management and product development. Similarly, platforms will have a significant impact on payments and lending, High-frequency trading (HFT) on capital markets and IoT on insurance. Blockchain also is expected to transform the financial services by bringing trust, transparency and security for customers and increased efficiency in the interaction of financial services actors. Besides, Regtechs is expected to impact all financial services as it can help them meet their regulatory requirements and enhance their efficiency.

There are also some transversal technologies such as APIs, cybersecurity systems, cloud solutions, electronic authentication that are expected to have a cross-cutting impact on all financial services. Cybersecurity and cloud solutions are already used in several areas as they facilitate several business processes and enhance the security. Blockchain and advanced analytics will also have a cross cutting impact on all the financial services, however, they are expected to affect specific activities of the value chain of each financial service.

The challenge for the incumbents is to understand the different technologies that can reshape their future and explore ways in which they can benefit from them. Those companies that make use of these enabling technologies are pursuing competitive advantage by improving customers' experience, enhancing the efficiency of their operations and by developing personalized products.



	Capital markets	Insurance	Investments management	Payments	Lending
Advanced Analytics	●	●	●	●	●
RPA	●	●	●	○	●
Blockchain	●	●	●	●	●
IoT	○	●	○	○	○
Platforms	○	○	○	●	●
Transversal Techs	●	●	●	●	●

Figure 8. EY internal Analysis on Use of Technologies in most Frequent Financial Services

10.6. SWOT Analysis

The SWOT of Fintechs industry is briefly presented in Figure 9. As seen in the SWOT there are many strengths of the Fintechs sector in Europe having capacity to create new opportunities. On the other hand, weaknesses are threatening the sector relatively less as compared to the opportunities. Projects like Critical-Chains and other investments and partnerships with more stakeholders may resolve the problems related to the competition with other developed countries, penetration in emerging markets and legislative barriers.

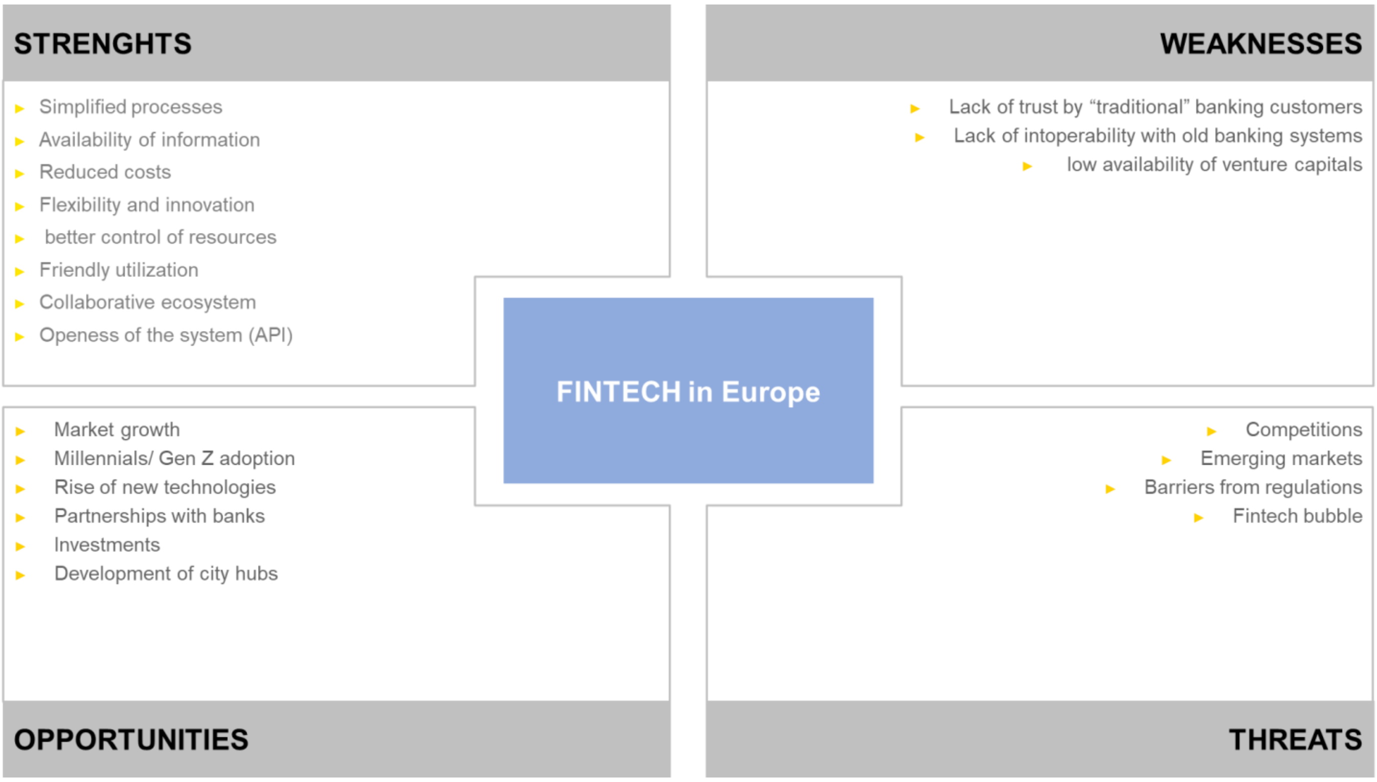

STRENGHTS
Simplified processes
Availability of information
Reduced costs
Flexibility and innovation
better control of resources
Friendly utilization
Collaborative ecosystem
Openess of the system (API)
WEAKNESSES
Lack of trust by "traditional" banking customers
Lack of intoperability with old banking systems
low availability of venture capitals
FINTECH in Europe
Market growth
Millennials/ Gen Z adoption
Rise of new technologies
Partnerships with banks
Investments
Development of city hubs
Competitions
Emerging markets
Barriers from regulations
Fintech bubble
OPPORTUNITIES
THREATS

Figure 9. SWOT Analysis of Fintechs Sector in Europe

10.7. Porter's Five Forces Analysis

Porter's five forces analysis, as outlined in Figure 10, is used to analyse the competition of a business. It basically draws five main forces to determine the market and shows in what direction it might be more successful to expand to avoid too challenging markets.

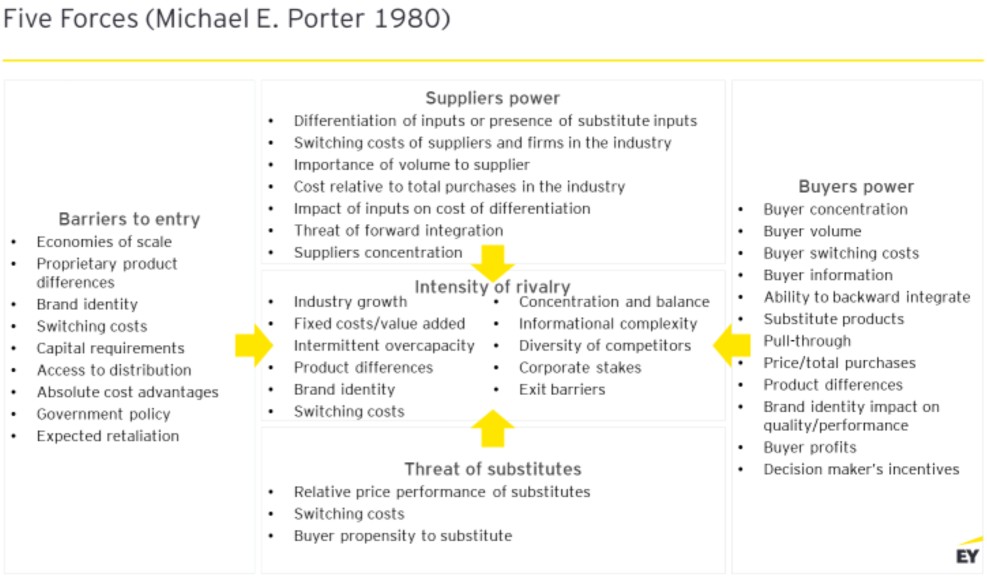


Figure 10. Porter's Five Forces

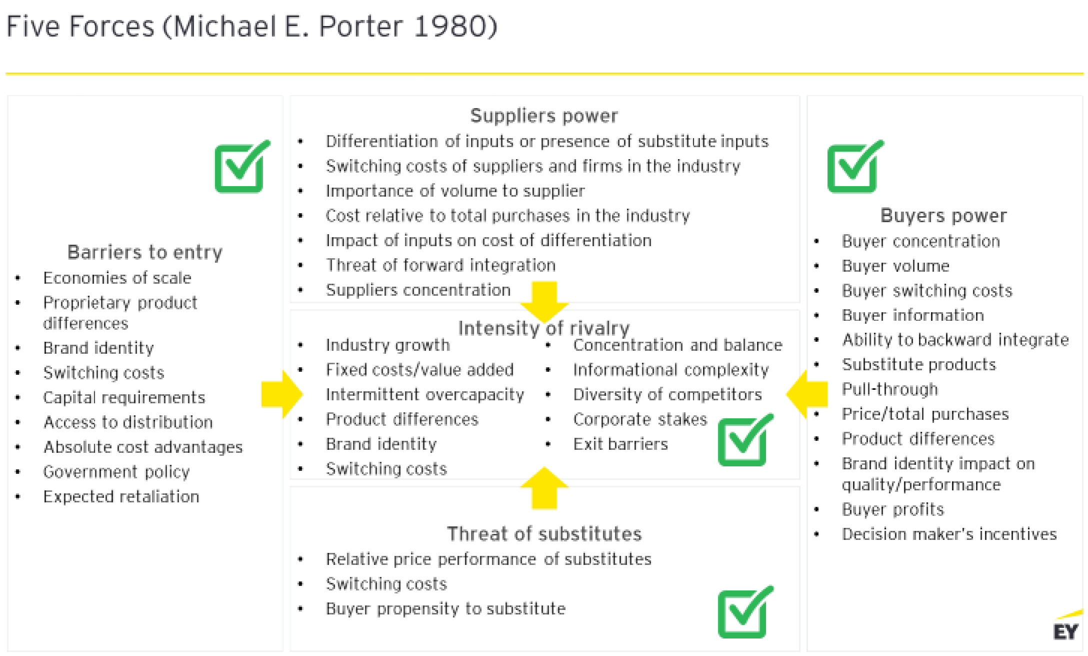
In the traditional financial industry, all five forces have a low power, thus leading to low overall rivalry:

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

- Obtaining a banking licence is hard (barriers to entry)
- Customers can hardly influence financial products (buyers' power)
- Banks are not depending on their asset suppliers (suppliers' power)
- Everybody is dependent on fiat currencies (threat of substitutes)
- The majority of power is held by only a few big players (intensity of rivalry)

When considering Porter's five forces analysis for Fintechs, peer-to-peer decentralised financial solutions, Blockchain and crypto currencies, four out of five forces now have a higher power, that quickly changes the level of rivalry (see Figure 11):

- It is very easy to join (see all the ICOs during 2017). Moreover, it is a lot easier to obtain a banking license now (at least in US and EU) (barriers to entry)
- Customers can decide on the currency when using crypto currencies (buyers' power)
- Direct payment solutions and crypto currencies are the actual substitutes of traditional banking solutions and fiat currencies (threat of substitutes)
- The new technological advances allow a healthy market supply and demand, increasing the rivalry and players in the market (intensity of rivalry)



Five Forces (Michael E. Porter 1980)

✓ Barriers to entry
- Economies of scale
- Proprietary product differences
- Brand identity
- Switching costs
- Capital requirements
- Access to distribution
- Absolute cost advantages
- Government policy
- Expected retaliation

Suppliers power
- Differentiation of inputs or presence of substitute inputs
- Switching costs of suppliers and firms in the industry
- Importance of volume to supplier
- Cost relative to total purchases in the industry
- Impact of inputs on cost of differentiation
- Threat of forward integration
- Suppliers concentration

✓ Intensity of rivalry
- Industry growth
- Fixed costs/value added
- Intermittent overcapacity
- Product differences
- Brand identity
- Switching costs
- Concentration and balance
- Informational complexity
- Diversity of competitors
- Corporate stakes
- Exit barriers

✓ Threat of substitutes
- Relative price performance of substitutes
- Switching costs
- Buyer propensity to substitute

✓ Buyers power
- Buyer concentration
- Buyer volume
- Buyer switching costs
- Buyer information
- Ability to backward integrate
- Substitute products
- Pull-through
- Price/total purchases
- Product differences
- Brand identity impact on quality/performance
- Buyer profits
- Decision maker's incentives

Figure 11. EY internal analysis "Porter's five forces - Fintechs considerations"

10.8. State-of-the Art in Fintechs and Trends

The financial sector is characterised by some relevant degrees of reluctance towards innovation, as well as relevant burdens against interoperability. The operational/administrative procedures are reasonably secure but at the same time highly complex and burdensome. In parallel, the policy and regulatory environment is opening up and fostering the enlargement of the financial services' market, promoting interoperability and exploitation of data and information for creation of services as Fintechs and Insurtechs.

These patterns are also influenced by the growing mobility of people (e.g. for working reasons) and the spread of services provided over mobile devices, which require unprecedented levels of flexibility and usability.

Specifically, we define Fintechs as organizations that combine innovative business models and technology to enable, enhance and disrupt financial services. The Fintechs industry has grown up and grown out. No longer made up of only start-ups, Fintechs today is a host of seasoned companies that offer a broad array of financial services and operate on a global stage.

As given in Figure 12 according to EY Fintechs Adoption Index (EY 2019) 96% of global consumers are aware of at least one money transfer and payment through Fintechs service and 3 out of 4 customers use one of these services. In addition, according to this research, 48% of global consumers use an Insurtechs service. Therefore, we can presume that awareness of these new services is now very high.

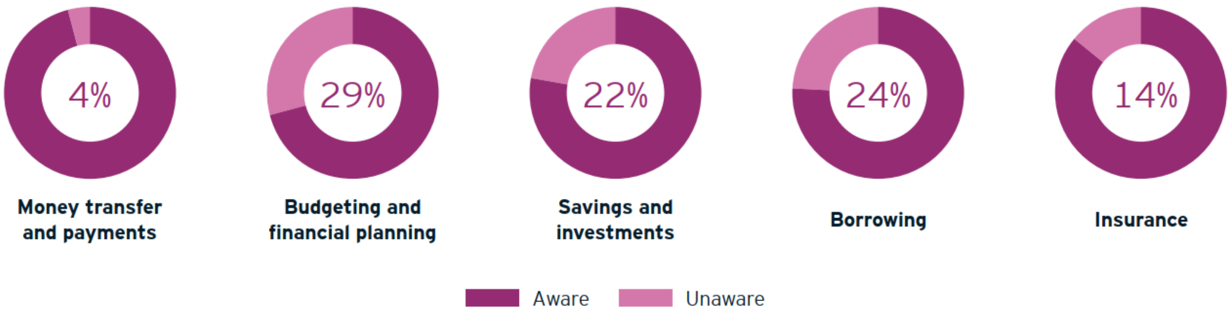


Figure 12. EY (2019) " Fintechs Adoption Index "

We tend to define a Fintechs adopter as someone who has used two or more major service, since this indicates a habitual change in behaviour in a way that use of a single service does not. We can also see two main types of Fintechs propositions: “disrupted” and “invented”. A disrupted service is one that has historically been offered by incumbents, such as automotive insurance or foreign exchange trading. Fintechs providers use technology to disrupt these services by offering consumers a more compelling offering such as enhanced capabilities, convenience, or lower prices and fees. This profoundly changes customer expectations in the process, pressuring incumbents to develop their similar services to stay competitive and retain market share. An invented service is one that did not exist before but is now possible by technology and alternative business models such as peer-to-peer lending and mobile phone payments. Some invented services fill niches in the market, and others have the potential to redefine and transform entire financial subsectors.

The general assumption tends to group Fintechs services into five categories: money transfer and payments, budgeting and financial planning, savings and investments, borrowing and insurance. The awareness is high across all categories, but particularly for money transfer and payments. Consumers showed surprisingly high levels of awareness for “invented” Fintechs services [quoted Fintechs companies are part of EU and American market] (i.e. Revolut, TransferWise, Stripe, Splitwise, Satispay).

Globally, 89% of consumers are aware of the existence of in-store mobile phone payment systems and non-bank money transfers driven by Fintechs. This category is the most commonly used service, with 75% of consumers using at least one service. In China, for example, this adoption rate jumps above the 95%. Key to their popularity is the ease of setting up an account, however the same is not true for other services – some markets restrict or regulate services such as investing in equity platforms (i.e. Robinhood, Stash, MoneyFarm, Acorns) and lending on peer-to-peer platforms (i.e. Upstart, Funding Circle, LendingClub, Peerform, SoFi) which slows adoption in those areas.

Insurtechs continue to show strong growth as well with nearly half the consumers globally linking smart devices or buying products such as micro-insurance or peer-to-peer insurances (i.e. Lemonade, Trov, Guevara, Inspeer, Yolo, Oscar). Here, non-financial services organizations often facilitate consumer Fintechs adoption, such as equipping cars with “black boxes” to provide data for telematics insurance or providing apps on mobile phones that consumers can use to steps and gain fitness discounts on their health insurance (i.e. Oscar Health, Carrot, Healthy Virtuoso).

Change in ranking of top five financial services since 2015 can be seen in Figure 13. There is a significant grow in insurance services where money transfer and payments and borrowing keep their ranking still.

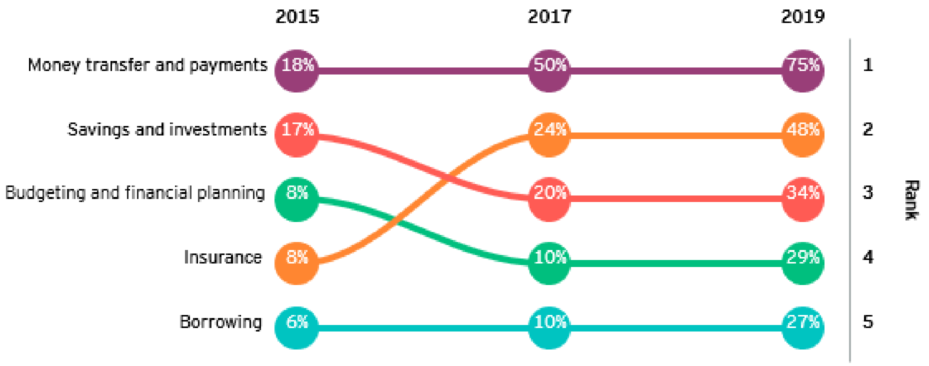


Figure 13. EY (2019) "Fintechs Adoption Index" – Change in Ranking of Top 5 services since 2015

37 privately held Fintechs unicorns have a combined valuation of approximately 142.17 Billion US-Dollars. Several start-ups raised mega-round investments, boosted their valuations and will use funding to expand into adjacent products. Going deep in 2019, it is possible to notice that more companies are poised to become unicorns as there is no shortage of well-funded, innovative start-ups driving trends listed below:

- **Banks, AI and machine learning powered platforms** to manage core processes, either paper or data sensitive, to analyse data, to provide decision-making support or to detect anomalies; to connect to customers, to increase empathy or provide powered automated assistance.
- **Open Banking, GDPR, MiFid II and PSD2** go live in Europe requiring banks to open APIs to customer data. Consumers are the biggest beneficiaries of this new regulations creating choices through competition and establish consistency around security protocols to protect them. Various Fintechs players in the market are developing platforms that can allow B2C, B2B or B2B2C connections. The Open Banking phenomena is spreading also in the Asia Pacific market thanks to a collaborative environment among banks, start-ups and especially regulators.
- **Lending platforms powered by data analytics** to reduce lending process time.
- **Personalized advice platforms** with simple UX design and simple decision-making processes to address wealth management, insurance or loan subscription. These platforms transform services that for many users seems complex and difficult to dominate into something that is almost playful.
- **Security and identity** linked in processes of client onboarding related to digital/cyber identity, biometric authentication and fraud detection.
- **Blockchain technology** applied into different spaces of financial services industry to optimize business processes by sharing data in an efficient and secure manner.
- **Payment technologies** ranging from cryptocurrencies to global currency account management.
- **SMEs** are becoming an increasing critical component for deals across the Fintechs ecosystem. Digital and challenger banks are looking to this opportunity for their frictionless engagement and low-cost services that can provide at scale.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

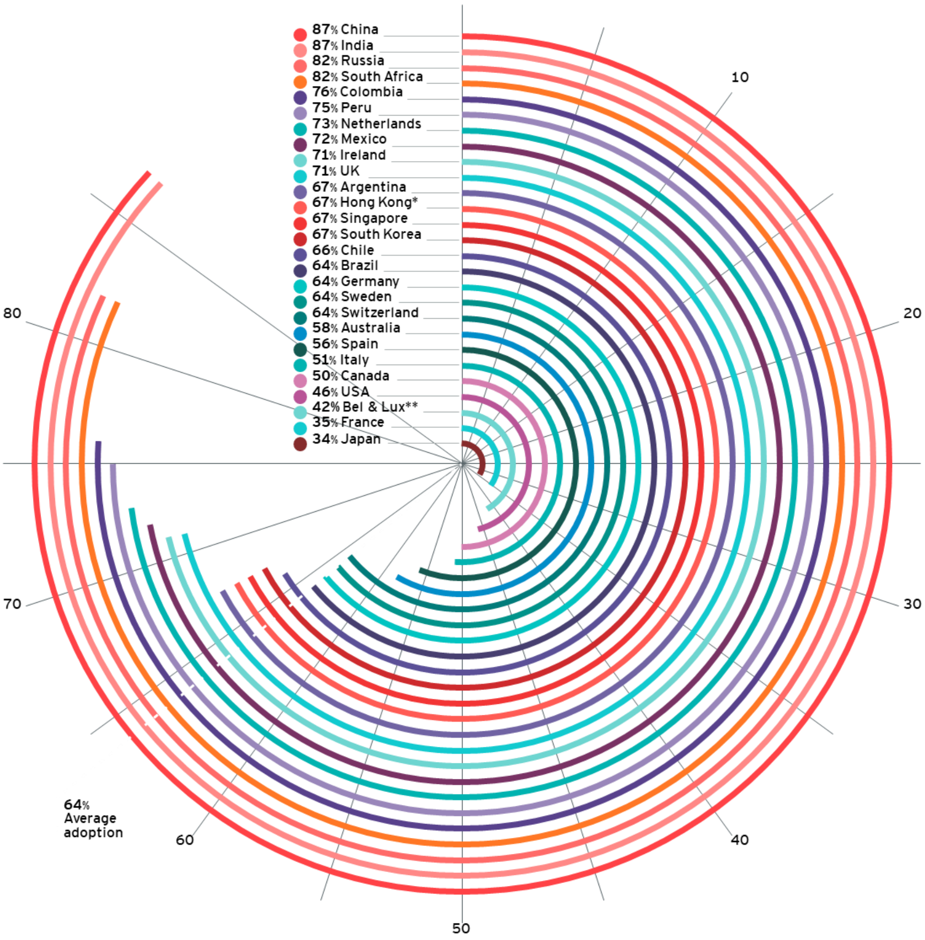


Figure 14. EY (2019) "Fintechs Adoption Index"

A country-wise Fintechs adoption index can be seen in Figure 14.

By looking back at the start of this revolution. Consumers wanted more flexible payment methods, better banking and access to financial advice at scale. Nowadays, they not only have those benefits but more choices than ever in other areas. Their demand is shifting, and Fintechs is iterating on product quickly by offering alternative financing sources and more. Consumers' preferences will of course continue to shift and will spur even more investment in this ecosystem.

In the context of the Critical Chains Framework, security remains an essential aspect, which not only need to be guaranteed at the current level, but also to be able to tackle emerging cyber-threats and challenges. The key functions of the finance sector are the safe storage and secure communications of assets. Technical security measures must therefore guarantee the confidentiality, integrity, accountability and availability of these two functions and protect their critical data and assets as well, taking into consideration an evolving threats landscape scenario. Aligned with this general overview, Critical-Chains will focus on following emerging areas by going beyond the existing state-of-the-art (SOTA).

Security has to be the top priority within the Fintechs community in order to properly safeguard institutional and consumer data. In addition, every company has the solemn need to protect the overall financial services industry infrastructure, especially because many financial transactions take place across an interconnected global data communications enterprise, which increases overall vulnerability.

Some of the core security related issues for which Fintechs companies must be adequately and proactively prepared include some of the following: data breaches, data loss, hijacking of accounts, denial of services attacks, insider threat, malware injection, insufficient due diligence, insecure APIs, abuse of cloud service and shared vulnerabilities.

10.9. Current Authentication schemes in online banking

A good authentication scheme is the first step to create a secure framework. It is most important that only authorized users can access their online accounts. Data breaches and hijacking of accounts do not only hurt the affected users, but also the financial institute that lost the trust of its customers and the Fintechs sector in general for the same reason.

Several two-factor and three-factor authentication schemes have been proposed over the last years. They all have their own strengths and weaknesses, but none seem to be secure against all types of attacks (Wazid, Zeadally und Das 2019). Even password guessing can lever out some two-factor authentication schemes and with more sophisticated techniques like man-in-the-middle-, insider-, user impersonation-, and replay attacks it is likely to find a weak spot in most authentication methods, including those using biometrics and smartcards.

Most commonly used for authentication in the finance sector are username and password, but also other methods like security questions, PIN, Virtual keyboard and One-Time-Passwords (OTP) are applied. The latter can be regarded as the most secure one out of the aforementioned (Bani-Hani, Majdalweieh und AlShamsi 2019). Two different forms of OTP can be applied, namely the automatic, where you receive an SMS with the code, and the synchronous, where you have a hardware token.

Using different devices for transaction initialization and confirmation is known to be particularly secure, but this aspect gets undermined by the trend of using smart-devices for everything, including mobile banking. The convenience of online banking via smartphone has caused the existence of multi-factor authentications, which do not reduce the risk of attacks as much as they should, because the whole scheme is located in one device (the smartphone) or even in a single app. The security means in such cases should include access barriers, repacking protection, a restrictive rooting policy, backup prevention, TLS pinning and obfuscation. Renowned banks, however, offer mobile banking apps that are easy to hack with well-known attacks, because they use single-device schemes without several of those security means and are, hence, vulnerable to system-level malware. Note, that it is compliant with the PSD2 to use such schemes (Haupert und Müller 2018).

10.10. Audit & Compliance Technology

Compliance technology can mean a variety of services that help organization stay up-to-date with standard and regulatory requirements.

10.10.1. IT Governance, Risk, and Compliance Management and Software Solutions

To manage the many growing and changing needs of IT compliance, many organizations implement solution strategies. An IT compliance solution should be adaptable in order to update it if regulations change. Moreover, it should allow for continuous internal investigation, dialogue, and education of those involved, and effectively manage any non-compliance issues.

The term GRC (governance, risk and compliance) combines the interwoven functions of IT compliance with the overarching responsibilities of corporate governance to enhance the activities of risk management. An IT GRC solution enables an organization to create and coordinate policies and controls and map them to regulatory and internal compliance requirements (Lindros 2017). These solutions, which are usually cloud-based, can support critical functions and provide micro and macro functionalities, automation for many processes, integrated features and controls and mobile solutions in order to increase efficiency, minimize complexity and reduce costs. Some of the feature could be (Smartsheet 2019):

- Vulnerabilities’ identification;
- Systems controls and application security functions;

- Quick recovery functions after failure or incident;
- Risk assessment and threat identification;
- Document and project management;
- Ongoing operations and maintenance management;
- Audit logs and authentication;
- Root cause analytics and forensics;
- Firewalls, network security, and malware detection;
- Change management and trouble ticket tracking;
- Disaster recovery;
- Email archiving.

GRC software can support multiple stakeholders, for example business executives that need to identify and manage risk and finance managers assigned to meet regulatory compliance requirements. Before the adoption of a software solution, the stakeholders need a clear plan, an assessment and a review of the goals, process and procedures already in place. In particular, they should identify compliance issues to be solved or strengthened in order to understand how employ the software to assist.

10.10.2. Regtechs

In the recent years, the regulatory compliance in Fintechs is supported by Regtechs (Piovan, Pirondini und Vidussi, RegTech: Get Onboarding The challenges of compliance 2019) (regulatory technology). It focuses on technologies that may facilitate the delivery of regulatory requirements in a more efficient and effective manner than existing capabilities. The Regtechs solutions may help Financial Institution in meeting compliance adherence in an “agile way”. The Regtechs realities collaborate with financial institutions and regulatory entities and use cloud computing and big data to share information.

Deloitte (Deloitte 2019) classifies the Regtechs solutions in 5 key areas: the “Regulatory Reporting” that enable automated data distribution and regulatory reporting through big data analysis, real time and cloud reports; the “Risk Management” that allows to detect regulatory and compliance risks, assess risk exposure and prevent future threats; the “Identity Management & Control” that provides solutions to facilitate counterparty due diligence, Know Your Customer (KYC) procedures and AML and anti-fraud screening and detection; the “Regulatory Compliance” that consists in automated real time monitoring and tracking of current state of compliance and upcoming regulations; the “Transaction Monitoring” that offers solutions for real time transaction monitoring and auditing.

The technologies involved are based on AI (Artificial Intelligence), RPA (Robotic Process Automation), Blockchain, big data and IoT and enable solutions to be agile, speedy, integrated and analytic.

AI and machine learning are useful to aggregate, manage and analyse huge amount of data. The interpretation of these solutions allows to supervise the financial institutions’ operability suggesting non-compliant points and automating risk assessment methodologies. RPA systems are used in controls execution and combined with GRC platforms to manage the information workflow. They allow to reduce costs and times by increasing effectiveness. Finally, the implementation of Blockchain is useful to store data in a secure, safe and immutable way (Russo 2019).

10.11. Use of HSMs and TRNGs in Blockchain- and IoT-enabled Fintechs Industry

The IoT and cyber-physical systems are merging with new trends like Blockchain in Fintechs industry. As the hardware and software-based techniques evolve, the decentralised mechanism of Blockchain has become more applicable in banking, insurance or financial market infrastructures. Smart contracts play a crucial role in applying Blockchain technology in Fintechs domain. In banking domain, financial transactions are verified in decentralised mechanism which brings the flexibility of 24/7 sustainability of banking operations enabling the multilateral and dynamic collaboration of parties within the rules of smart contracts. Such a flexibility has a very positive impact on increasing the effectiveness of multinational and milt stakeholder commercial relations. Similarly, in insurance domain, IoT-enabled evidence collection and on-site operations (e.g. when an accident happens) are stored in Blockchain-enabled automation frameworks which bring the accurate calculation of damage, non-repudiation and accountability throughout the complex insurance operations.

10.11.1. Recent status of HSMs and TRNGs

According to a recent trend report HSMs are growing fast and yet evolving from “Stars” to “Cash Cows” in today’s market (360researchreports.com 2018). According to Boston consultancy Group’s share/growth matrix (Morrison and Wensley 1991), “Stars” resemble the products with high growth rate and high share whereas the “Cash cows” present the mature products with low growth but high market share. Nowadays HSMs (including TRNGs) can be seen in between these two categories with less “question marks” because they now have a critical role in today’s ICT world. These products provide hardware-based security protection mechanism equipped with very fast unpredictable key generators, OTP, nonce and padding byte generators, symmetric and asymmetric cryptographic algorithms and hashing mechanisms. Such attributes enable very fast authentication mechanisms, database encryption, document signing, Secure Socket Layer (SSL), code signing, PKI/Credential managements, payments processing and application level encryption. The foremost HSM products have been branded by top companies like Utimaco GmbH, Thales e-Security, Futurex, Gemalto, IBM, Hewlett Packard Enterprise, Yubico, and Ultra Electronics.

TRNGs also present specialised solutions for limited purposes as compared to HSMs. TRNGs, as contrary to PRNGS, utilise full nondeterministic entropy sources generate unpredictable and unguessable random bit sequences. TRNGs can be either deployed on HSMs as embedded components or used as standalone peripherals aiming to create random data bulks for nonce or padding byte creation or one-time –password generation. TRNGs are relatively low-cost as compared to either HSMs, at the order of less than 100 USDs or a few hundred depending on their features; whereas HSM prices are usually between 20000-40000 USD. According to BCG matrix, standalone TRNGs are categorised as evolving from “Question Marks” to “Stars” because of their flexible use and speed in new areas like IoT and Blockchain infrastructures.

10.11.2. HSMs, TRNGs, CPS and Blockchain

HSMs and TRNGs play a crucial role in today’s market as they are becoming more aligned with Blockchain and cyber-physical security. The recent marketing trends indicate their increasing importance especially in two technological areas: (1) Cyber-physical systems and (2) Blockchain infrastructures.

HSMs and TRNGs in cyber-physical systems: As the number of connected devices in the IoT grows exponentially, the risk of manipulation of nodes in cyber-physical systems grows, too. This is totally valid in nearly all sectors, no matter if the connected device is health monitor, a connected car, a smart meter, or a smart phone. The only differing thing is about the consequences that may vary in potential severity.

In such CPS environments one of the biggest threats is the key injection which can be overcome by ensuring that each device has a truly unique electronic identity that can be the basis for the secure management of a device over its product lifetime. The certain solution is at semiconductor level (secure stick in silicon in Critical-Chains) where the unique identity is injected into the chip ensuring its production process (called key injection). In recent technology landscape, key injection is usually realised by secure initialisation of a device’s identity as it is introduced to the IoT via a PKI. Such a method includes the secure authentication of users to devices or device amongst each other, secure software updates, secure communication, secure storage of data within the device itself or secure databases and finally secure decommissioning at the end of the life cycle of the device. In such cases compromised, cloned or mismanaged keys form the three main attack vectors in CPSs. Use of HSMs (or partially TRNGs) may provide effective solutions against attack surfaces aligned with the attack vectors enabling

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

unique and unpredictable key generation, secure key storage, secure crypto-processing environments and built-in comprehensive key management.

Among current mainstream HSMs, Equinix (Smart key, BIG-IP), Yubico (YUBIHSM 2), nCipher (nShield), Gemalto and recently Thales (SafeNet), Atos (Horus), Utimaco (CryptoServer, SecuritySErver, TimeStampServer), SPYRUS (Rosetta Spycos), IBM (Cloud Hardware Security Module 7.0) are the foremost companies (brands) investing in HSMs for IoT and cloud use. According to BCG matrix such IoT-supported products are still far from “Cash Cows” but candidates to shine like “Stars” if they provide higher throughput, speed and practicality in IoT environments. IoT environments are still not comfortable as they are prone to many inferences and the communication infrastructures are still not very confident and effective for higher rates of data transmission. Bringing an additional security is still seen as sceptic for end user integrators. Nevertheless, with recent developments in Blockchain infrastructures (e.g. IOTA) HSMs specialised for IoT may bring in good profits and have an opportunity to expand further in a growing market.

HSMs and TRNGs in Blockchain infrastructures: Securing Blockchain infrastructures and crypto assets has never become more crucial than ever after the eruption of cryptocurrencies age. As the use of cryptocurrencies even in daily exchanges significantly increases, the need of fast and effective security in multi-signature and multi-authorisation schemes rises cordially. Moreover, it is forecasted that Blockchain can enable smart devices to become independent agents as it records a ledger of transactions between devices, web services, and even humans, The combination of Blockchain and IoT enables not only the accountability but also make machines to order stock, operate during the most economical times, pay for the delivery of new items, and solicit bids from distributors to name a few.

Smart contracts deserve the opening of a special parenthesis because they are becoming on the main use cases of Blockchain technology. Smart contracts bring the viability of contracts as they can even be programmed and describe an agreement. The details of a smart contract are recorded as living e-forms including set of instructions, prescriptions, preprogramed with the ability to self-execute and enforce the terms of a contract. Smart contracts allow many anonymous stakeholders to conduct business without the need or cost for an intermediary. However, as the triangular accountability model proposed in Critical-Chains offers, many enterprise applications require the parties to be known and authenticated.

Whatever the reason or area to use Blockchain, there is a strong need to provide strong identities and authentication for authorised access to Blockchain. Securing the core Blockchain as well as the communication across the Blockchain network is of privileged requirement in any Blockchain-enabled Fintechs domain. The weakest link is usually the wallet especially in cryptocurrency systems because the wallet manages the crypto assets and executes at the application level, which is closer to the wider attack surfaces of software vulnerabilities. This is also similar for smart contracts. Such problems can be solved by low-level hardware-based security solutions.

Big players in HSM and TRNG domain are aware of this big potential associated with the combined use of HSMs and Blockchain. Among these, Securosys (Primus), Thales and Gemalto (SafeNet), Utimaco, nCipher (nShield), IBM Cloud Hardware Security Module 7.0 are the foremost companies published their products claiming that these are Blockchain-specific HSMs. Although these products present a big potential they can be categorised still as “Question Marks”. Even though they have the potential to gain a significant market share the can become “Dogs” if they cannot prove how they differentiate from “Cash Cow” HSMs present what they bring in specific usages related to Blockchain infrastructures different than the mainstream products (even their own products). The marketing strategy putting forward the keyword “Blockchain” forward may attract customers at first glance but if the experts are not convinced with the specialised and appropriate use of new “Blockchain-enabled HSMs” there may be a negative impact in commercialisation of these products.

Hence, the BCG matrix depicted in Figure 15 presents where the mainstream and new generation HSMs and TRNGs position in the market. These technologies are not forming the entire solution stack. As these technologies are combined with advanced authentication mechanisms, financial/banking/insurance services, cryptosystems, cloud applications, AI-enabled Fintechs data management and evidence-based monitoring, new approaches for network security and intrusion detection, etc. the resulting CPS may come forward as new "Stars". Critical-Chains aims to foster innovative studies in related areas to come up with a "Star" and the roadmap to be upgrade to "cash cows" in the early post-project phases.

Amongst the entire product portfolio, ERARGE'S HSM namely PRIGM, which is equipped with a very fast hardware-based true random number generator, symmetric/asymmetric cryptographic algorithms and hashing tools can be seen as a start evolved from "question mark". It is expected that PRIGM can become a "Cash Cow" throughout or early after Critical-Chains because the underlying techniques are patented worldwide and promoted in top scientific conferences and journals so far. For the list of the patents visit http://ergtech.ch/research.html.

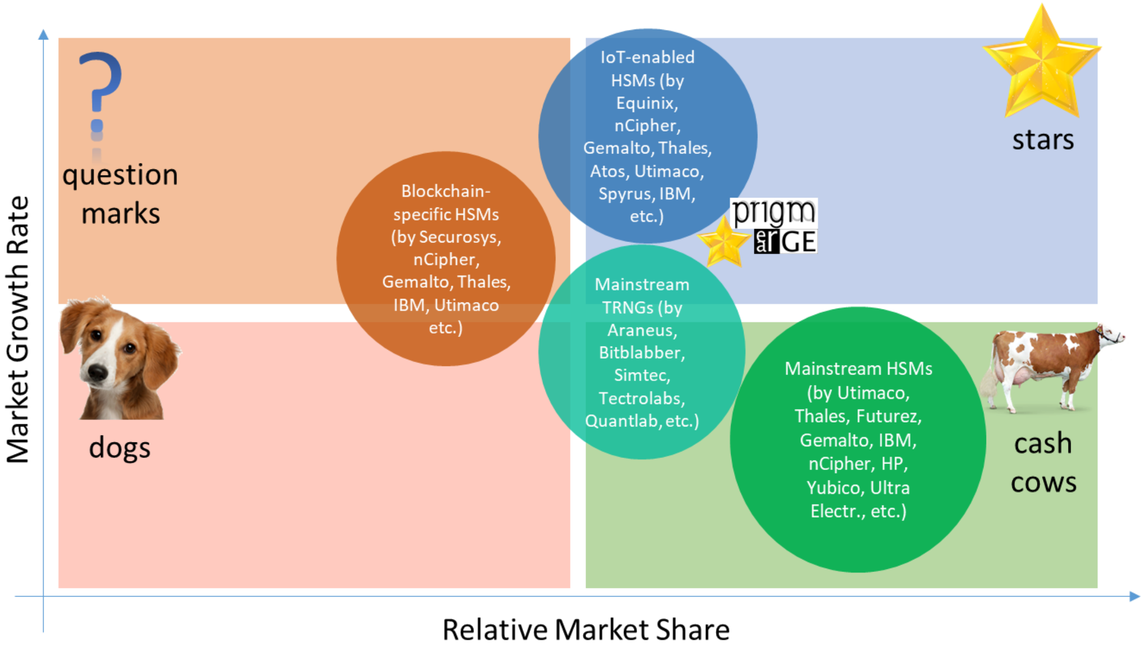

question marks
Blockchain-specific HSMs (by Securosys, nCipher, Gemalto, Thales, IBM, Utimaco etc.)
IoT-enabled HSMs (by Equinix, nCipher, Gemalto, Thales, Atos, Utimaco, Spyrus, IBM, etc.)
stars
prigm
arGE
dogs
Mainstream TRNGs (by Araneus, Bitblabber, Simtec, Tectrolabs, Quantlab, etc.)
Mainstream HSMs (by Utimaco, Thales, Futurez, Gemalto, IBM, nCipher, HP, Yubico, Ultra Electr., etc.)
cash cows
Market Growth Rate
Relative Market Share

Figure 15. BCG Matrix for HSM and TRNG market

The BCG matrix template plots products or product categories against two variables:

- Relative Market Share (horizontal axis) – the higher the market share, the more cash likely being generated. This measurement reflects a brand's competitive position and is usually expressed as their market share relative to their closest competitor.
- Relative Market Growth (vertical axis) – products with high market growth rate usually have higher earnings but also consume many cash and require investment to pursue and maintain that growth. Market growth is a good indicator of industry attractiveness and gives an indication of a product's future potential, overall market strength, and attractiveness to future competitors.

Question Marks	Stars
High Growth, Low Share	High Growth, High Share These products have a high market share and are in a fast-growing industry. They bring in good profits and

Products with low market share but in high growth industries. Often associated with emerging markets. These products: • have the potential to gain market share and become stars • may eventually become *cash cows* when market growth slows • can become *dogs* if they do not succeed in becoming a market leader after a period of investment or the market growth declines. Suggested actions: Carefully analyse to see if they are worth investing in to increase market share. Consider investing for market penetration, market development, or product development; or divesting.	have an opportunity to expand further in a growing market. Stars help to assure the future of a company. These products: • are *question marks* that have gained market share and are improving. • can become *cash cows* as the market stabilizes. • may become *dogs* if they lose their competitive edge, and the market becomes obsolete (not uncommon in technology fields). Suggested action: Resource to maintain market position and growth. Consider vertical or horizontal integration options, investing for market penetration, market development, or product development.
Dogs Low Growth, Low Share Products with low market share in a mature, slow-growing market. These products: • usually generate minimal profit • are sometimes maintained for strategic purposes e.g., they provide jobs, have synergies with other business units, or are a defence against competitors. Suggested action: Consider eliminating these products by retrenching, divesting, or liquidating. Maintain (in special circumstances)	Cash Cows Low Growth, High Share Products with high market share but low growth. These products: • generate good profits and supply funds for future growth • were often *stars* in market which has now matured and slowed • do not have many opportunities to expand as the market is growing too slowly for investment to be worthwhile. • might become *stars* with further product development. Suggested action: Support to maintain their current market share. “Milk” while investing as little as possible. Consider investing in product development, diversifying, divesting or retrenching.

10.12. Recent Status of Authentication Schemes in Identity Management

Identity solutions play a crucial role in Fintechs operations where the user authentication and authorisation have been of top priority since the first deployment of Internet banking. Effective identity management and secure authentication are indispensable for such Internet platforms keeping fraud at bay, boosting trust, clicks and sales.

Although they are indispensable many digital identity solutions are not as efficient or effective as they could be. Multi-factor authentication features high security but, in the meanwhile, many large businesses have opted to create their own identity platforms or prune the complex security policies according to their actual needs. A typical example of this approach has been seen in banking sector where the banks are still insisting on sharing one-time passwords or codes via SMS in spite of the cyber threats like SMS forwarding attacks. One of the main reasons of this pertinacity is the practicality and ease of use of SMSs as many people are very accustomed to use mobile phones and SMS messages.

In order to increase the marketing advantage and the acceptance of practical tools for authentication, multi-factor authentication is adapted to real-life uses. For instance FIDO[14], an alliance focusing on providing open and free authentication standards, intends to reduce the reliance on passwords. FIDO specifications have been used for financial services and payments as fast and easy access with robust authentication security. The existing

[14] https://fidoalliance.org

solution providers believe that authentication with complex passwords is cumbersome but single gesture can be used instead for quick log on. The solutions work simpler with the same devices that people use every day and prefer using the same authentication with different services. Although such easy solutions bring high practicality, security concerns arise in parallel. Thus, even FIDO recommends U2F for relatively high security needs. As depicted in Figure 16 U2F presents a 2-factor authentication scheme where a token is used at least for just pressing a security button after a simple login or password stage.

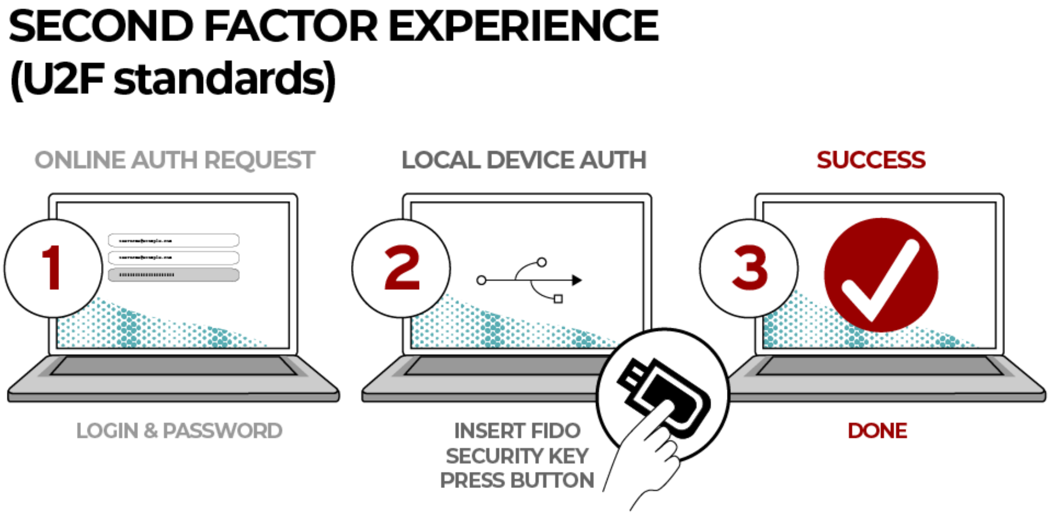


Figure 16. U2F standard in FIDO

The security level of Identity management systems (IDMS) may vary according to the usage area and the frequency of service usage. IDMSs have been widely used in many sectors but mostly preferred in Finance, Governmental/Legal, Social/Leisure, Travel, Home/Health & Family and in Professional Business. Figure 17, published in Australia, summarises the actual use of IDMS in these fields of operation[15]. As aligned with the Critical-Chains targeted domain, IDMSs are frequently used in daily online or card payments and weekly for log-in into account. In such cases the authentication should be fast and not cumbersome for better market uptake. In less frequent applications such as applying for a new banking product (credit card, e-wallet), insurance claim, or even for loan or mortgage or credit scoring, higher security with what-you-have (token), what-you-know (password) and what-you-are (biometric) is seriously needed. This is vital especially in transactions with big amounts.

In Europe, the eIDAS Regulation aims to create a single legal framework for recognising electronic signatures and identities throughout the EU. eIDAS is performed over an interoperability framework for the national eID systems to be recognized by public bodies across the EU. From the banking perspective, EU banks seriously invest in seeking the optimized solutions to use national eIDs in cross-border operations and to realise Know-your-Customer (KyC) initiative which are well-defined in eIDAS tools. Related trust services across Europe are electronic authentication, electronic seal, electronic time-stamp, electronic documents, electronic delivery services, and website authentication.

Similar to eIDAS, well-developed countries like USA, Canada, Japan, China have opted to make use of similar joint strategies to enable IDMSs synchronised within the country and also with the globe. Among these, the following ones are the foremost example banks (but not limited to) who are leading the market with successful case studies:

[15] A frictionless future for identity management, A practical solution for Australia’s digital identity challenge, White Paper, December 2016

- BBVA Compass (USA) applied tokenised authentication on real-time payments.
- Credit Union Association experimented a shared distributed ledger that gives members a cryptographic digital identity.
- Canadian Banks launched digital identity project SecureKey in 2012 and they recently announced that the project will be extended to run on IBM's Blockchain
- Capital One recently announced B2B digital identity tools for consumer verification.
- Deutsche Bank is now working on a project to bring universal digital identity to Germany.

According to the BCG digital identity survey[16] the key applications of IDMS in financial services are;

- Process automation; Customer self-service –through the Web or mobile applications (anywhere/anytime)
- Personalised products/services; New data types (such as location and usage information) available via mobile devices and sensors allow for an array of innovative products (i.e. data oriented insurance processing)
- Scoring & Rating; online data detailing purchases, commercial activities and social activities for accurate credits.

As illustrated in Figure 18, for the targeted marketing consumer sensitivity is still at medium level, which can raise "Question Marks" for the targeted sector. However, process automation has become "Cash cows" as many banks opted to apply customer self-service applications for the sake of minimising costs of face-to-face services in branches. For scoring and rating, there still exist debates on identity processing because the joint initiatives and exchange of customer information among competing banks are still problematic.

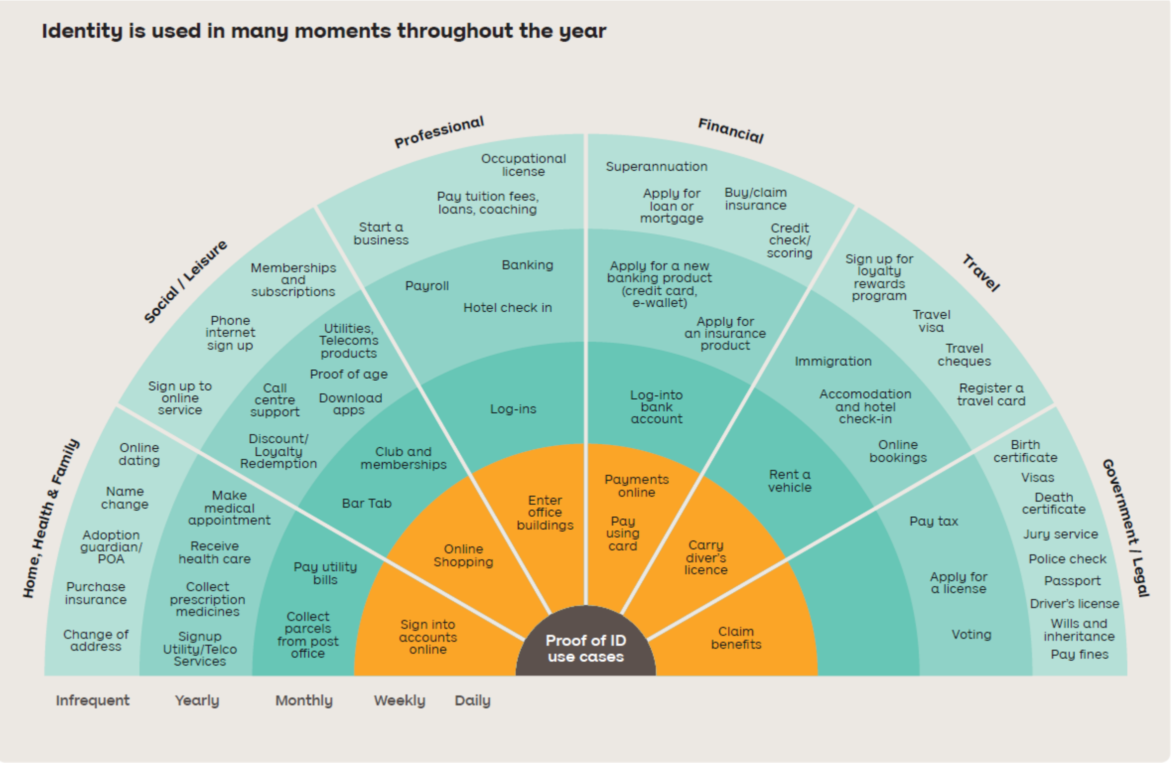
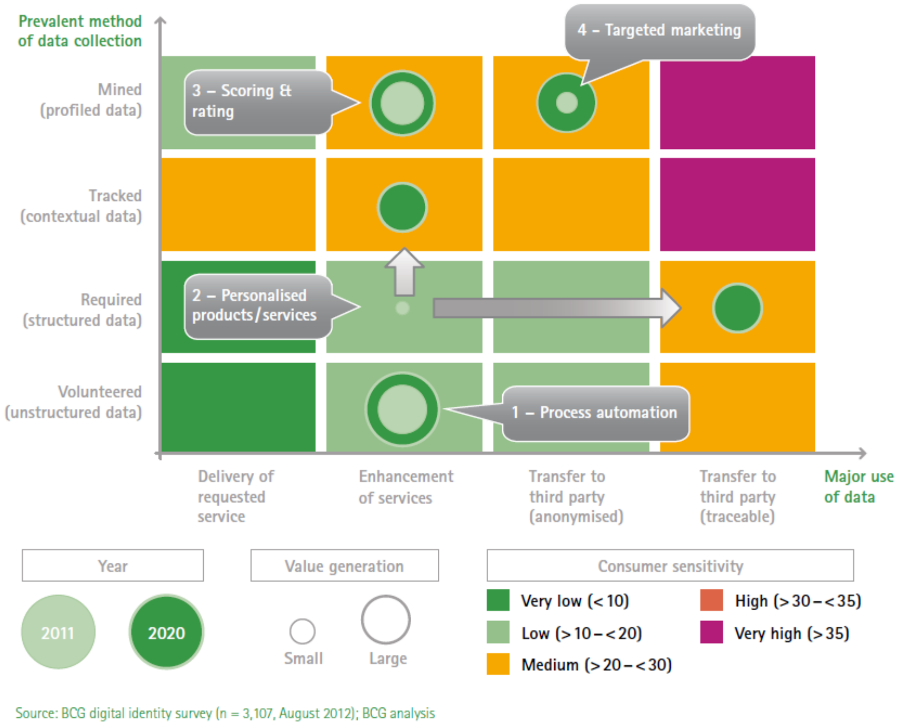


Figure 17. IDMS usage frequency in various fields

[16] https://2zn23x1nwzzj494slw48aylw-wpengine.netdna-ssl.com/wp-content/uploads/2017/06/The-Value-of-Our-Digital-Identity.pdf

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018



Source: BCG digital identity survey (n = 3,107, August 2012); BCG analysis

Figure 18. BCG digital identity survey related to online financial services

In accordance with the current state of market, there exist solutions that have become “Cash Cows”. Instead of elaborating the position of products in BCG matrix one by one, we prefer to give an overview of positions of widely used solution strategies (listed below) in the Boston matrix:

- **Something you know**: This is the conventional and the easiest way of authentication via password or PIN. Here, schemes like OTP, Challenge-Response mechanism, and Single-Sign-On are widely used even in cloud IDMSs. OpenID and Security Assertion Markup Language (SAML) are the two foremost protocols, which are widely preferred. Products or solutions relying on simply “Something you know” are definitely the “cash cows” in the market and they still have been preferred because of their ease-of-use. However, security concerns due to cyber-attacks, like cookie-replay attack, eavesdropping, elevation of privilege, spoofing, phishing or repudiation attacks, raise some “Question marks” about their future in the IDMS market landscape. They may become “Dogs” in not far future.
- **Something you have**: This term is commonly referred to token-based authentication. This scheme is surely more secure than password- or PIN-only solutions but requires a media that should be owned and carried by the customer. The majority of the existing solutions may rely on Public Key Infrastructure (PKI), smart cards, or mobile phones. With the recent advances on mobile banking applications, IDMS operating over mobile phones have become the “Stars” and improving to become “Cash Cows”. Smart cards, especially the ones equipped with NFC, are still preferable as many people like to carry a proof for the sake of confidentiality. However, these solutions are still problematic as such, token media can be stolen, lost or forgotten. Although they are more resilient as compared to password-only solutions, token-based methods are still vulnerable to attacks like skimming or eavesdropping. However, in anyway, token-based methods, seen as meta-solutions between the highest security and the highest practicality, are good candidates to stay as “Cash Cows”.
- **Something you are**: This is the most natural representation of an identity as it relies on personal biometric traits of a person. Research has already been reflected to the market especially in the last decade where many applications were deployed in finance domain. Biometric authentication is capable of mitigating attacks such as brute-force, dictionary attack, forgery or identity spoofing. Fingerprints, facial images, voice,

iris and vein patterns (palm or finger) have been applied in finance domain. Undoubtedly, biometrics bring additional security because biometric features are unquestionably linked with a person. Linking an identity with a PIN or token is a synthetic process and such data or media cannot represent a person in reality. However, biometric signals are prone to errors as they are not certain and open to noise and vulnerabilities. Some biometrics, like voice, may not be distinguishing enough or easily spoofed. Some of them require special scanners or hardware for signal acquisition (fingerprint, iris, vein). These challenges raise “Question Marks” for biometric authentication and its uses in daily financial operations. However, for critical missions, like credit checks, loans, transfer of big amounts, insurance claims, and biometric-enabled authentication can be preferred.

Figure 19 illustrates an overview of the marketing trends. The grey arrows indicate the trend direction and circles show the steady state. As seen from the tendencies, 2-factor authentication with password and token, especially with mobile phones, have become the mainstream authentication scheme. With advancements in FIDO, 2-factor authentication will be accepted as an undeniable standard. Biometric authentication is relatively sparse in the market. Biometric modalities like retina, DNA, ear shape, gait or gesture are seen as Dogs with the lowest market growth rate and market share. Such studies are usually stuck to academic developments. Contrarily, face and fingerprint authentication solutions are evolving from “Stars” to “Cash Cows” with the recent hardware and software developments in mobile phones. These biometrics outshine the others because mobile phones provide built-in scanners (cameras or sensors), and public acceptance is relatively high. However, although well promoted vein and iris scanning is still far from being a “cash cow” s they require special hardware and have less public awareness. Signature is still an option with some “question marks” due to its easy spoofing. Nevertheless, since signature is a common way of approval of a proof in real world, digital signature pads are still used in some services. Voice biometrics has a lower growth rate in IDMs because it is not a very robust and reliable biometric.

The 3-factor authentication scheme proposed in Critical-Chains will be based on hardware-based fast modules like true random number generation, key generation and cryptographic operations. The proposed method can easily be adapted to various levels of authorisation, even pruned to 2-factor or single-factor authentication. Such an elasticity will carry the solution from “Question Mark” to a “Star”.

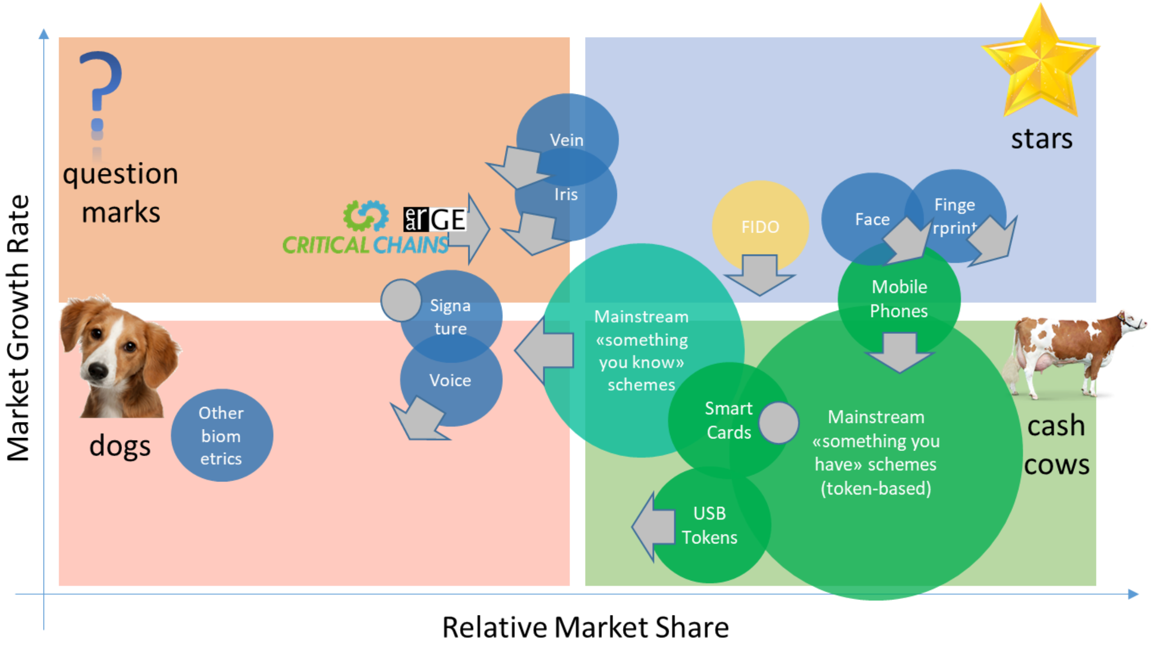


Figure 19. BCG matrix for authentication schemes in IDMSs

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

11. Cyber Attacks against Financial Infrastructures

Cyber incidents involving financial institutions have been dramatically increasing in recent years. According to a recent report (Kapersky 2018) published by Kaspersky in March 2019, there is a significant increase in cyber threats in 2018. For instance, Kaspersky Lab's anti-phishing technologies detected nearly 500 million attempts to visit different kinds of phishing pages. The number of users attacked by banking malware (like Trojans) was about 900 thousand with ~16% increase as compared to 2017. Similarly, the number of users that encountered Android banking malware tripled to 1.8 million worldwide.

Figure 20 provides an overview of the different attack types against financial infrastructures, between 2005 and 2019. In this period, a total of 38 major cyber-attacks (>30.000 affected customers) happened, where six where due to poor security, six were due to inside jobs, 19 happened because of hackers and seven attacks happened because of lost or stolen media.

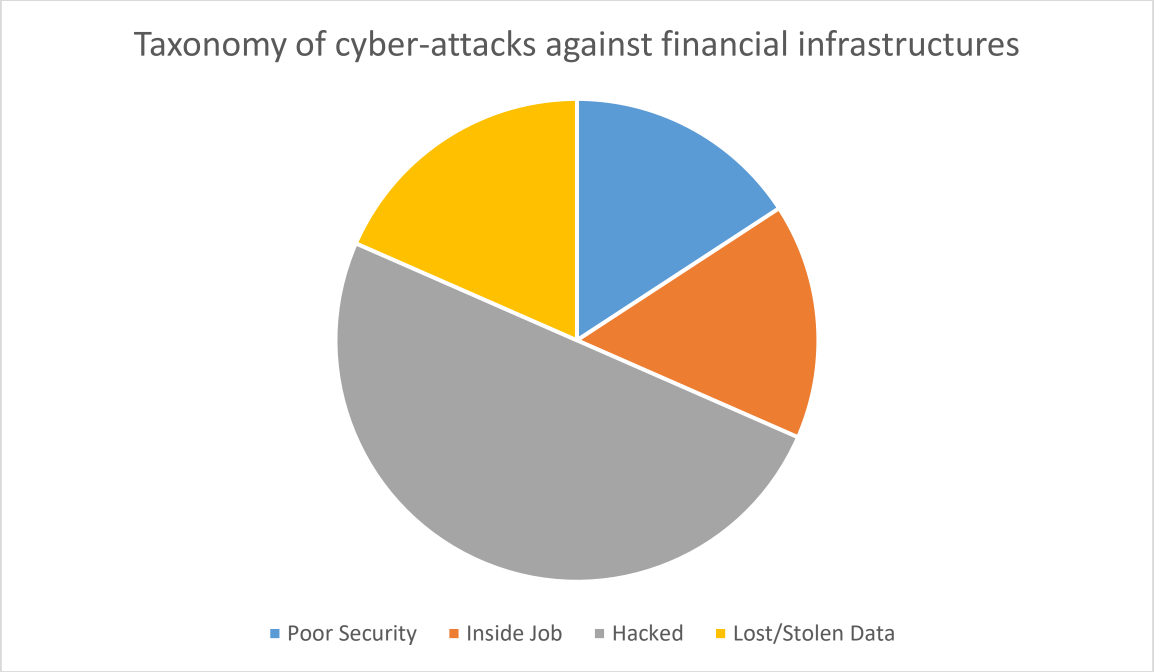


Figure 20. Taxonomy of cyber-attacks against financial infrastructures between 2005 and 2019

Table 2 presents the list of recent cyber incidents involving financial institutions (Carnegi 2017). The majority of the recent attacks are of type malware, phishing, DDoS or Password spray resulting with mostly data breach, money theft, private information loss, disruption of operations or espionage. The attacks show that the attacks are evolving as the Internet banking facilities increase, no matter what type or method.

Table 2. Some recent examples of cyber incidents involving financial institutions (Carnegi 2017)

Attack	Target	Type	Location	Date	Description/Impact
Ursnif Malware Attack	Japanese Banks	Malware (Theft)	Japan	Mar. 2019	Ursnif, also known as Gozi ISFB, is a popular malware that steals information on infected Windows devices. The malware terminates itself on devices outside of the country. The campaign uses a distribution network of spam botnets and compromised web servers to deliver the Trojan.
Unknown	Bank of Valletta	Unknown (Disruption)	Malta	Feb. 2019	Bank shut down operations after an attempted theft of €13 million. Attackers made multiple transfer requests from the

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

					Maltese bank to accounts in the UK, United States, Czech Republic, and Hong Kong.
U.S. Credit Union Spear-Phishing	Multiple credit unions	Phishing	US	Feb. 2019	Multiple credit unions in the United States were hit by spear-phishing emails impersonating compliance officers from other credit unions. While it is believed that no employee clicked the link, there is speculation as to how the attackers obtained the email addresses of the compliance officers.
SBI Breach	UK-based Metro Bank	Disruption	UK	Feb. 2019	This is a cyber intrusion that intercepts text messages with two-factor authentication codes used to verify various customer transactions.
Chile ATM Attack	Chile's ATM interbank network, Redbanc	Espionage	Chile	Jan. 2019	Realised by tricking an employee into downloading a malicious program during a fake job interview over Skype. Redbanc claims the event had no impact on its business operations.
Fuze Cards	Banks	Theft	US	Jan. 2019	The U.S. Secret Service has identified a number of criminal rings turning to Fuze cards in an attempt to avoid detection by U.S. law enforcement.
Evercore Breach	global investment bank	Phishing (data breach)	Western Europe	Dec. 2018	The attackers used phishing tactics to gain access to an employee's inbox, enabling them to steal around 160,000 pieces of data including documents, diary invitations, and emails.
Government Payment Portals	local government services	Data breach	US	Dec. 2018	Threat intelligence firm Gemini Advisory discovered that several users' card details were sold on the dark web for approximately £10. Gemini identified 294,929 compromised payment records, resulting in at least $1.7 million in earnings for the criminals.
Brazilian Mobile Malware	Several banks	Malware (theft)	Brazil	Dec. 2018	Over 2,000 mobile banking users in Brazil downloaded an Android-based Trojan through Google Play applications. The malware also targeted apps such as Uber, Netflix, and Twitter using phishing tactics.
ThreadKit Exploit	unknown	Phishing (Espionage)	Unknown	Dec. 2018	In late 2018, security researchers uncovered that Cobalt, a state-sponsored threat group that specializes in attacks on financial institutions, had begun employing a new variant (evolved) of the ThreadKit exploit builder kit to execute phishing schemes utilizing Microsoft Office documents.
Insider Threat against banks	eight banks in Eastern Europe	Theft	Eastern Europe	Dec. 2018	Attackers connected electronic devices (such as netbooks, inexpensive laptops, USB tools, and other devices) directly to the banks' infrastructure. The attacks are believed to have caused tens of millions of dollars in damages.
Rapid Raids Jackpotting	ATMs	Malware (theft)	US	Dec. 2018	Two Venezuelan men were found guilty of jackpotting, where they installed malicious software or hardware on ATMs to force the machines to dispense huge volumes of cash on demand. The duo stole $125,000 from four ATMs in Indiana, Kentucky, Wisconsin, and most recently Michigan
Magecart Payments Breach	Lloyds Banking Group and other UK banks	Unknown (Theft)	UK	Nov. 2018	Lloyds Banking Group and other UK banks were forced to replace payment cards after the breach of numerous retail sites. Websites for retailers, including Ticketmaster and British Airways, were manipulated to skim card information from hundreds of thousands of customers using the Magecart toolset.

DDoS-for-Hire	Banks	DDoS (disruption)	UK	Apr. 2018	It was revealed that authorities in five countries worked together to take down Webstresser, a DDoS-for-hire site they said was behind up to 6 million attacks around the world over three years.
Mabna Iranian Hack on the United States	Financial firms	Password spraying (Data breach)	US	Mar. 2018	The actors are accused by the United States of stealing 31 terabytes of academic and commercial information in a campaign dating as far back as 2013.
Dutch DDoS Attack	ABN Amro, Rabobank, and ING	DDoS (Disruption)	Netherlands	Jan. 2018	ABN Amro, Rabobank, and ING suffered disruptions to online and mobile banking services, while the Dutch tax authority website was taken down for several minutes
Youbit Hacked	Youbit bitcoin exchange	Unknown(Theft)	South Korea	Dec. 2017	In a demonstration of cryptocurrency's growing role in online crime circles, the bitcoin exchange Youbit was hacked twice in 2017, forcing it to file for bankruptcy.
SEC Edgar Hack	Edgar database	Software vulnerability (Data breach)	US	Sept. 2017	Hackers might have accessed inside information from the Edgar database, which contains market-sensitive filings for companies listed on U.S. stock exchanges, and used it to make illegal profits on share trades.
Equifax Hack	Credit reporting agency Equifax	Web app vulnerability (Data breach)	US	Sept 2017	Equifax announced that more than 150 million customer records had been compromised, including some sensitive data such as birth dates and 12,000 U.S. social security numbers.
Metel Malware Attack	Russian Banks	Multiple: malware, phishing and browser vulnerabilities (Theft)	Russia	2011-2015	The Metel banking Trojan, which was discovered in 2011, was repurposed by a criminal gang in 2015 to steal directly from bank ATMs and even manipulate the Russian exchange rate. Metel had infected 250,000 devices and more than 100 financial institutions in 2015, according to researchers at Group IB.
JPMorgan Chase Data Breach	JPMorgan	Stolen password (Data breach)	US	Aug. 2014	Account information and home addresses for 83 million customers were exposed after attackers stole login credentials from a JPMorgan Chase employee.
South Korea Attacked	Banks	Diskwiping (Disruption)	Sç Korea	Mar. 2013	The Shinhan, Nonghyup, and Jeju banks were targeted by a Trojan that deleted data and disrupted ATMs, online banking, and mobile payments.

11.1. Cyber Incidents on Financial Infrastructures

In the following, a few of the prominent attacks are listed and explained in more details.

11.1.1. Capital One data breach:

Date reported: 29. July 2019

Date discovered: 19 July 2019

Date of incident: 22-23. March 2019

Links:

https://www.bbc.com/news/world-us-canada-49159859
https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html
https://www.ft.com/content/7c6c6d7a-b269-11e9-8cb2-799a3a8cf37b
https://www.cnet.com/news/capital-one-data-breach-involves-100-million-credit-card-applications/
http://press.capitalone.com/phoenix.zhtml?c=251626&p=irol-newsArticle&ID=2405043

Who was affected?

About 100 million individuals in the US and 6 million individuals in Canada.

What was compromised?

About 140 000 Social Security numbers of US based credit card customers. About 80 000 linked bank account numbers of US based secured credit card customers. About 1 million Social Insurance numbers of Canada-based credit card customers.

Costs of the breach?

Capital One estimates the costs with incremental costs of approximately $100 to $150 million in 2019.

How?

In a statement by Capital One they mention that a highly sophisticated individual was able to exploit a specific configuration vulnerability in Capital One's infrastructure. Capital One encrypts all data and tokenizes selected data fields. While the tokenized data remained protected, the encrypted data could be decrypted.

11.1.2. Desjardins data breach:

Date reported: 20. June 2019

Date discovered: 14. June 2019

Date of incident: unknown – 14. June 2019

Links:

https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-1.5183297
https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-protection-1.5212030
https://www.cbc.ca/news/canada/montreal/desjardins-data-breach-explain-1.5185163
https://www.cyberark.com/blog/data-breach-at-desjardins-bank-caused-by-malicious-insider/
https://montrealgazette.com/business/desjardins-rogue-employee-caused-data-breach-for-2-9-million-members

Who was affected?

According to Desjardins Group around 2.9 million of their Canada-based customers had been affected from the data breach.

What was compromised?

Desjardins Group reported that personal identifiable information including names, dates of birth, social insurance numbers, addresses and phone numbers of 2.7 million customers were compromised. Moreover, 173000 business customers had also been affected.

Costs of the breach?

Desjardins Group reported that they will pay for credit monitoring for every customer with a coverage of 5 years. Moreover, a class action has been field against Desjardins Group requesting $300 for each customer plus additional money for damages.

How?

Desjardins Group reported that an employee stole the data as the employee had already some privileged access, but further obtained credentials from other employees to access the data.

11.1.3. First American data breach:

Date reported: 24. May 2019

Date discovered: 24. May 2019

Date of incident: approximately March 2017 – 24. May 2019

Links:

https://www.wired.com/story/first-american-data-exposed/
https://bloom.co/blog/first-american-data-leak/
https://edition.cnn.com/2019/05/25/business/first-american-data-exposed/index.html
https://techcrunch.com/2019/05/24/first-american-millions-sensitive-records/
https://qz.com/1628542/first-american-data-leak-highlights-how-much-info-homebuyers-share/
https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

Who was affected?

Customers of the US-based insurance company First American were compromised, as 885 million sensitive financial records have been exposed.

What was compromised?

According to a security researcher, the exposed records included social security numbers, driver's license images, bank account numbers and statements, mortgage and tax documents and wire transaction receipts.

Costs of the breach?

A class action complaint had been filed against First American claiming for compensation for the massive data breach.

How?

First American has sent their customers emails containing a document URL that links to a document on a webserver. The URL itself consisted of a document record number (i.e. 000000075). However, it was possible to simple change the number that seems to be iteratively assigned for each new customer, without the need of any authentication. Therefore, anyone with access to a valid link could see the documents of any other customer, resulting in 885 million documents.

11.1.4. Westpac data breach:

Date reported: 3. June 2019

Date discovered: 22. May 2019

Date of incident: 7. April 2019 – 22. May 2019

Links:

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

https://www.smh.com.au/business/banking-and-finance/australians-private-details-exposed-in-attack-on-westpac-s-payid-20190603-p51u2u.html
https://7news.com.au/business/banking/westpac-cyber-attack-bank-under-fire-after-thousands-of-customers-details-exposed-c-147291
https://finfeed.com/features/westpac-breach-highlights-cyber-security-threat/
https://www.news.com.au/technology/online/hacking/westpacs-payid-breach-sees-almost-100000-users-personal-details-exposed/news-story/737d71b8a39dfb9f71799947dd852c9e

Who was affected?

The private details of almost 100000 Australian bank customers have been exposed on the real-time payment's platform PayID.

What was compromised?

According to Westpac around 98000 names of bank account holders associated with their telephone number had been compromised.

Costs of the breach?

Unknown.

How?

The real-time payments platform PayID operates like a telephone book, allowing anyone to type in a mobile phone number or email address, and have it confirmed the name of the corresponding bank account. Hackers simply iteratively tried around 600000 phone numbers and succeeded with around 98000 lookups revealing the names of the bank account holders.

11.1.5. Bank of Montreal and Simplii Financial data breach:

Date reported: 28. May 2018

Date discovered: 27. May 2018

Date of incident: January 2018 – 27. May 2018

Links:

https://www.csoonline.com/article/3276275/2-canadian-banks-hacked-90000-customers-data-stolen.html
https://www.cbc.ca/news/business/bank-hack-tuesday-1.4682018
https://www.zdnet.com/article/bank-of-montreal-cibcs-simplii-financial-confirm-customer-data-breaches/
https://newsroom.bmo.com/index.php?s=2429&item=129367
https://business.financialpost.com/news/fp-street/cibcs-simplii-says-fraudsters-may-have-accessed-data-of-40000-clients

Who was affected?

The Bank of Montreal confirmed that less than 50000 customers based in Canada have been compromised. Simplii Financial, a subsidiary of the Canadian Imperial Bank of Commerce, confirmed that 40000 of their customers have been compromised.

What was compromised?

Both financial institutions confirmed that names, dates of birth, Social insurance numbers and account balances of in total 90000 customers had been compromised.

Costs of the breach?

Both financial institutions claimed that they will fully compensate any losses of their customers. News articles indicate that civil law actions have been filed, but no details are given about any further costs of the breach.

How?

The hacker wrote in details how he compromised the websites of the financial institutions. Initially, he used a mathematical algorithm (Luhn algorithm) to verify randomly generated account numbers. Furthermore, he seemed to have access to some account numbers that helped to understand the numbering system of the bank accounts. Next, the hacker used the password reset page of the financial institution that just required the previously generated account number, some security questions and to verify the email. However, the website generated an authentication cookie, that allowed the hacker full access without authentication. With that cookie, the attack could change the security questions to known answers and also change the email address, giving him full access to a user's bank account.

11.1.6. Equifax data breach:

Date reported: 07. September 2017

Date discovered: 29 July 2017

Date of incident: 13. May – 30. July 2017

Links:

https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/
https://www.forbes.com/sites/leemathews/2017/09/07/equifax-data-breach-impacts-143-million-americans/#edc164e356f8
https://www.lifelock.com/learn-data-breaches-equifax-data-breach-2017.html
https://www.bbc.com/news/business-41192163
https://www.theverge.com/2019/7/22/20703497/equifax-ftc-fine-settlement-2017-data-breach-compensation-fund

Who was affected?

Equifax identified that the identity theft affected approximately 145.5 million US based costumers. Moreover, Equifax estimated that between 400 000 and 44 million UK based customers and 8000 Canada based customers were compromised.

What was compromised?

In total, the breach exposed 147 million people's names and dates of birth, 145.5 million Social Security numbers and in some instance driving license numbers. 209 000 credit card numbers of US based customers were compromised, and documents with personal information of 182 000 customers was stolen.

Costs of the breach?

On 22. July 2019 Equifax agreed to a settlement in the amount of $575 million, including $300 million for victim compensation, $175 million to the state and territories in the agreement, and $100 million to the Consumer Financial Protection Bureau (CFPB).

How?

Equifax reported that a flaw in Apache Struts (CVE-2017-5638) facilitated the breach. A patch for the flaw was released on 7. March 2017, however, Equifax failed to apply the security patch until 30. July 2017. The flaw in

Apache Struts was not a single point of failure, as also an insecure network design that lacked sufficient segmentation, inadequate encryption of personal identifiable information and an ineffective breach detection mechanism was used.

11.1.7. Coast Central Credit Union data breach:

Date reported: 25. February 2016

Date discovered: 23. February 2016

Date of incident: 23. February 2016 – 26. February 2016

Links:

https://krebsonsecurity.com/2016/02/breached-credit-union-comes-out-of-its-shell/
https://lostcoastoutpost.com/2016/feb/26/coast-central-credit-union-website-hacked-manageme/
https://techtalk.pcpitstop.com/2016/02/29/52744-coast-central-credit-union-hacked/
https://www.cuinsight.com/coast-central-credit-union-website-hacked.html
https://www.cutimes.com/2016/02/26/coast-central-credit-union-website-hacked/?slreturn=20190706090123

Who was affected?

About 60000 customers of the Coastal Central Credit Union had been affected, as the website of the financial institution had to be taken down for maintenance for one entire day.

What was compromised?

While the website of Coast Central Credit Union was replaced by a shell website for several days and had to be taken offline and maintained for one day, Coast Central Credit Union reported that no personal data of any customer was stolen. Moreover, the Coast Central Credit Union faced criticism from cyber security experts regarding the way it handled the event.

Costs of the breach?

Unknown.

How?

A security researcher suggests that the website might have been hacked by using an outdated version of Akeeba Backup, a Joomla component that manages backups of Joomla-based websites. Exploiting this vulnerability allowed the hackers to upload a web shell, which further allowed the hackers to access and modify files on the webserver of Coast Central Credit Union.

11.1.8. Scottrade data breach:

Date reported: 2. October 2015

Date discovered: August 2015

Date of incident: late 2013 – early 2014

Links:

http://web.archive.org/web/20151106034905/https://about.scottrade.com/updates/cybersecurity.html
https://www.wired.com/2015/10/scottrade-alerts-4-6-million-brokerage-customers-breach/
https://www.cnbc.com/2015/10/02/scottrade-data-breach-affects-up-to-4m-customers.html

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

https://money.cnn.com/2015/10/02/technology/scottrrade-hack/
https://www.bankinfosecurity.com/scottrade-a-8565

Who was affected?

According to Scottrade about 4.6 million clients between late 2013 and early 2014 have been affected.

What was compromised?

According to Scottrade, the compromised database contained names, addresses, email addresses and social security numbers of customers. However, the company indicated that the hackers appeared to exfiltrated only names and addresses of customers.

Costs of the breach?

Scottrade announced that all customers get a free year of identity theft services through a security company.

How?

No details of the attack have been disclosed, apart from that the known intrusion point was secured and Scottrade conducted an internal data forensics investigation with assistance of a leading computer security firm. Moreover, they report that appropriate steps to further strengthen their network defences have been taken.

11.1.9. European Central Bank (ECB) data breach:

Date reported: 24. July 2014

Date discovered: 21. July 2014

Date of incident: unknown

Links:

https://www.cnbc.com/2014/07/24/ecb-announces-data-theft.html
https://www.ecb.europa.eu/press/pr/date/2014/html/pr140724.en.html
https://www.zdnet.com/article/european-central-bank-suffers-security-breach-personal-data-stolen/
https://www.bbc.com/news/business-28458323
https://www.ft.com/content/67b32a28-1317-11e4-925a-00144feabdc0

Who was affected?

According to the ECB data from a database of a public website for events was stolen, affecting around 20000 users.

What was compromised?

The European Central Bank reported that 20000 email addresses and a much smaller number of phone numbers and street addresses have been stolen. While most of the data were encrypted, parts of the database, including the email addresses, street addresses and phone numbers was not encrypted. No internal systems or market sensitive data were compromised.

Costs of the breach?

Unknown.

How?

The European Central Bank declined to offer technical details, including which application was hacked or how data was being encrypted.

11.1.10. JPMorgan Chase data breach:

Date reported: 02. October 2014

Date discovered: late July 2014

Date of incident: late June – mid August 2014

Links:

https://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach
https://www.reuters.com/article/us-jpmorgan-cybersecurity/jpmorgan-data-breach-entry-point-identified-nyt-idUSKBN0K105R20141223
https://www.businessinsider.de/jpmorgan-hacked-bank-breach-2015-11?r=US&IR=T
https://www.bankinfosecurity.com/chase-breach-affects-76-million-households-a-7395

Who was affected?

According to JPMorgan Chase 76 million US based households and 7 million small businesses, including 83 million accounts, have been compromised.

What was compromised?

JPMorgan reported that names, addresses, phone numbers and email addresses were stolen. However, they said that there was no evidence that account numbers, passwords, user IDs, birth dates and Social Security numbers had been stolen.

Costs of the breach?

Not disclosed by JPMorgan Chase. However, they announced that they are spending $250 million on cyber security per year.

How?

According to JPMorgan a government sponsored hacker stole the credentials of an IT specialist of JPMorgan. As one of the network servers at JPMorgan did not require two-factor authentication, or multi-factor authentication, the hackers could access the data and trigger further attacks against more sensitive systems from the unsecured network server.

11.1.11. Korea Credit Bureau data breach:

Date reported: 20. January 2014

Date discovered: unknown

Date of incident: October 2012 – December 2013

Links:

https://www.businessinsider.com/south-korea-data-leak-2014-1?IR=T
https://phys.org/news/2014-02-korean-credit-card-firms-leak.html
https://securityaffairs.co/wordpress/21431/hacking/south-korea-20-million-credit-card-data-leaked.html
https://www.telegraph.co.uk/technology/internet-security/10584348/Credit-card-details-of-20m-South-Koreans-leaked.html
https://www.bbc.com/news/technology-25808189

Who was affected?

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

According to the Korea Credit Bureau the personal data of 20 million bank and credit card users in South Korea has been leaked.

<u>What was compromised?</u>

According to the Financial Supervisory Service (FSS) personal data, including customer names, social security numbers, phone numbers, credit card numbers and expiration dates have been stolen.

<u>Costs of the breach?</u>

The companies involved have been forced to suspend all their new business for three months, which is estimated to cost them $100 million in operating revenue. Moreover, the companies involved have to cover any financial losses of their customers.

<u>How?</u>

An employee of the personal credit rating firm Korea Credit Bureau, that worked as a temporary consultant stole the data by copying it to an USB stick. Later the contractor sold the data to phone marketing companies.

12. AI, machine learning technologies, blacklisting, anomaly detection, flow modelling

Fintechs – Financial Technology, refers to the financial technology sectors in a wide range of operations for enterprises or organizations, which mainly addresses the improvement of the service quality by using Information Technology (IT) applications (Gai, Qiu and Sun 2018).

In contrast to conventional financial services, Fintechs services reveal the following non-conventional characteristics – diversity in transaction models, evolvability of transaction models, customer-centric transaction models, simplified and speedy transaction processing, mobile/wireless network-based dataflow, etc. (La and Kim 2018).

Therefore, a continuous growth of the investment has been powering the development of Fintechs to advance on technologies breakthroughs in general, such as mobile networks, cloud computing, trust management, big data, image processing, and data analytic techniques (Gai, Qiu and Sun 2018).

However, massive adoption of Fintechs services leads to very significant challenges in security and privacy domain, mainly due to the inter-crossed realms, complicated integrated systems, and distinctive demands (Gai, Qiu and Sun 2018).

Often, traditional research in the field of security and privacy focuses either on the physical security domain, e.g. protection against intruders or physical damage, or on the cybersecurity domain, e.g. data theft, malware infection or shutdowns. Fintechs services, as any IT service, can be target for different types of random cyberattacks.

Additionally, due to its nature, Fintechs services are especially targeted by Advanced Persistent Threats (APT) – targeted malicious attacks aimed at a specific individual, company, system or software, based on some specific knowledge regarding the target. Classic IDS – Intrusion Detection Systems, have many limitations when it comes to detection of advanced threats. Therefore, this field presents an open research area of very high importance, where combination of advanced technologies, like artificial intelligence (AI), machine learning, blacklisting, anomaly detection and flow modelling are strongly considered as part of the possible solution.

Advanced cyber threats detection usually requires a systematic analysis of the system and the assets to protect, the intentions of potential attackers, and the likely attack vectors. Various methodologies for performing such an analysis do exist, as the ones described in (A. Shostack 2014), (UcedaVelez and Morana 2015) and (Howard and Lipner 2006). Steps common to most methodologies are (i) system decomposition, (ii) attack identification, and (iii) risk analysis and intrusion detection.

The typical tools for **system decomposition** are the data flow diagram (Abi-Antoun, Wang and Torr 2007), attack graphs (Swiler and Phillips 1998), (Lippmann, et al. 2006) and weaknesses tools such as Mitre CWRAF[17].

For **attack identifications**, semantic models have been used to apply automated reasoning to leverage the potential of machine learning and classifiers to carry out advanced cybersecurity analytical reasoning (Bromander, Jøsang and Eian 2016), Existing taxonomies like Mitre's Common Weakness Enumeration (CWE) or ATT&CK[18] taxonomy can serve as a basis. Formal methods or the "Correct by Construction" principle can prove – or disprove – the absence of weaknesses in a system (Degabriele, Paterson and Watson 2010).

[17] https://cwe.mitre.org/cwraf/

[18] https://attack.mitre.org

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Risk analysis and intrusion detection for modern communication networks, in particular by means of detection primitives relying on machine learning offer promising results (e.g., (Potluri and Diedrich 2016), (Yousefi-Azar, et al. 2017), (Liu and Zhang 2016)).

12.1. System decomposition – flow modelling process

This follows normally a typical six steps process:

- Understanding Problem Definition,
- Understanding the Data,
- Preparing the Data,
- Building the Model,
- Evaluating the Model, and
- Deploying and Monitoring the Model

The process starts with understanding the problem. The first step is to define the objective or to determine the business requirements that need to be met. Once this has been determined, a plan can be formulated on how to proceed. In the Critical Chains project, the following questions arise:

1. Is this Blockchain message typical?
2. Is this Blockchain activity part of an attack?
3. How likely is this node to be an insider security threat?
4. Can this financial transaction be fraudulent transaction?
5. Is this Blockchain charge fraudulent?
6. What are the abnormal conditions that involve fraudulent traders?
7. How can suspicious user behaviour and transaction sets be detected?

The next step is to plan and understand the data. Critical Chains deals with two types of data. First, user and transaction data such as average in-transaction, average out-transaction, average time interval between in-transactions, average time interval between out-transactions. The second data type contains data in smart contracts.

Step three is to prepare the data contained within it for use. This includes data that has errors, perhaps missing data, outdated, or data that is redundant, will reduce confidence in the analysis and hinder accurate decision-making.

Step four is determining the model and then building it. This is where deep technical knowledge is required to determine the best model to use, as well as the tools used to achieve this.

In step five, test cases will be built and run against the testing data set, with results interpreted to provide a basis for validating the models and their success.

In a final step, when a model has been found, it can then be **deployed to a production environment** where the data and output is applied.

12.2. Intrusion detection

Artificial Intelligence in general, and specifically machine learning and anomaly detection, are considered as promising techniques for intrusion detection in Fintechs domain.

Machine learning technologies have shown their effectiveness in solving such tasks as spam detection, image recognition, product recommendation, predictive analytics etc. For example, in fraud management, Machine Learning can be used to predict fraud in a large volume of transactions by applying cognitive computing technologies to raw data (Magomedov, et al. 2018).

Table 3 shows an example of questions of interest in Critical Chains, and a technology type that can potentially be used as a solution.

Table 3. Example Questions for Critical Chains

No.	Question	Technology
1.	Is this message typical?	Anomaly detection, classification
2.	Is this activity part of an attack?	Classification, regression
3.	How likely is this node to be an insider security threat?	Regression
4.	Can this financial transaction be fraudulent transaction?	Anomaly detection

According to the question types, three different ML approaches are prominent.

- Classification
- Regression
- Anomaly (outlier) detection

Regression and classification are both categorized as supervised machine learning. The main difference between them is that the output variable in regression is continuous (numerical) while that for classification is discrete (categorical).

Regression analysis tends to become more sophisticated when applied to fraud detection due to the number of variables and size of the data sets. It can provide value by assessing the predictive power of individual variables or combinations of variables as part of a larger fraud strategy. According to this technique, the authentic transactions are compared with the fraud ones to create an algorithm, which will then predict whether a new transaction is fraudulent or not (Magomedov, et al. 2018). Examples of the common regression algorithms include linear regression, Support Vector Regression (SVR), and regression trees.

Classification can be two-class classification and multi-class classification, according to number of expected data classes. Some of the methods commonly used for binary classification are: Decision trees, Random forests, Bayesian networks, Support vector machines, Neural networks, logistic regression. Additionally, several algorithms have been developed based on neural networks, decision trees, k-nearest neighbours, naive Bayes, support vector machines and Extreme Learning Machines to address multi-class classification problems.

Anomaly detection main objective is to identify anomalous or unusual data from a given dataset. It involves automatically discovering interesting and rare patterns from datasets. It is also known as outlier detection, deviation detection, novelty detection, and exception mining. Anomalies are important because they indicate significant but rare events, and they can prompt critical actions to be taken in a wide range of application domains (Ahmed, Mahmood and Islam 2016). For example, abnormal behaviour in a credit card transaction could indicate fraudulent activities, an unusual traffic pattern in a network could mean that a computer is hacked or under attack. Several anomaly detection techniques have been proposed in literature. Some of the popular techniques are: Density-based techniques (k-nearest neighbour, local outlier factor, isolation forests, and many more variations of this concept); Subspace-, correlation-based and tensor-based outlier detection for high-dimensional data; One-class support vector machines; Replicator neural networks., Auto encoders, Long short-term memory neural networks; Bayesian Networks; Hidden Markov models (HMMs); Cluster analysis-based outlier detection; Deviations from association rules and frequent item sets; Fuzzy logic-based outlier detection; Ensemble techniques, using feature bagging, score normalization and different sources of diversity.

12.3. Related Work

There are several survey papers covering this topic and providing very good insight into current trends. **Ahmed et al.** (Ahmed, Mahmood and Islam 2016) survey provides an overview of anomaly detection methods, specifically clustering algorithms, in financial domain. Proposed paper defines assumptions on how to detect anomalies and summaries works applying partition-based and hierarchical-based clustering algorithms. **Abdallah et al.** (Abdallah, Maarof and Zainal 2016) proposed a survey on fraud detection systems. **Gai et al.** (Gai, Qiu and Sun 2018) proposed very comprehensive survey on Fintechs technology in general.

West and Bhattacharya (West and Bhattacharya 2016) present survey results of applying classification algorithms to financial fraud detection. Proposed work analyses strengths and limitations of classification-based approach to financial fraud detection, and classifies existing works in terms of performance, applied algorithms, and fraud types.

Bhattacharyya et al. (Bhattacharyya, et al. 2011) propose comparison results of applying SVM, random forest, and logistic regressions to a credit card fraud detection.

La and Kim (La and Kim 2018) proposed a comprehensive framework for managing Fintechs transactions, which utilizes machine learning-based intelligence in deriving anomaly detection models and adaptive Fintechs security provision.

Mogomedov et al. (Magomedov, et al. 2018) proposed anomaly detection method in fraud management based on machine learning and graph databases.

Le Khac and Kechadi (Le Khac and Kechadi 2010) work apply k-means algorithms to detect money laundering while **Chang and Chang** (Chang and Chang 2010) work apply k-means algorithms to detect online auction frauds.

Glancy and Yadav (Glancy and Yadav 2011) and **Torgo and Lopes** (Torgo and Lopes 2011) utilize hierarchical clustering to detect anomalies in financial transactions.

Chang and Chang (Chang and Chang 2012) proposed a method for early fraud detection in online auctions. They reduce attributes used for generating learned models through principal analysis and utilize the last 20% of the transaction histories in building the models to maximize detection rates while minimizing efforts.

Some authors utilize hybrid approaches to maximize the fraud detection performance. **Behara and Panigrahi** (Behera and Panigrahi 2015) propose method for utilizing fuzzy c-means clustering algorithm and neural network algorithm to detect credit card frauds. **Sahin and Dauman** (Sahin and Duman 2011) utilize artificial neural network and logistic regressions to detect credit card frauds, while **Yaram** (Yaram 2016) proposes document clustering and classification algorithms for identifying frauds in insurance claims.

Existing works focus on selecting an optimal set of features for detecting frauds, identifying frauds from the proposed models, and evaluating performance of the models. Very important aspect in all approaches is the fact that the effectiveness of the proposed methods largely depends on the data used for learning models.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

13. The future of financial intermediation, disruption and re (evolution)

In this section we focus on examining the disruptive and re-evolutionary forces that have been unleashed on the financial services as a new emerging eco-system within which banks and other financial services providers e.g. non-bank lenders, Small-Loan providers, Venture Capitalists etc. will have to re-examine and radically or to some extent re-invent their form of intermediation.

The latest regulatory directives affecting the banking sector, in particular those related to open banking and the trend towards mobile banking and payments supported by emergent payment services have led to a fast evolving Fintechs landscape. Apple, through the introduction of Apple Pay has been instrumental in the evolution of the easy payment market which has been further extended through a similar easy-pay service called “K Pay” from Korea (Kim 2016). Overall the indications are that the following factors are amongst the key correlates of the evolution of payment-type Fintechs services

- Usefulness, cost and convenience
- Security and privacy protection
- De-regulation

Mobile payment services are embraced by a sector of the market who value easy-to-use payment services without having security concerns and not needing to use active X. However it is important to note the extent to which, beyond the so-called digital divide, concerns for privacy, security and mis-use continue to influence the take-up of mobile banking services by the majority of users who could otherwise join the mobile payment services trend.

13.1. The Challenges & Needs posed by the new forms of financial intermediation

The future of financial intermediation is not solely influenced by jus Blockchain but also new decentralisation trends and democratisation trends such as in fund-raising e.g. Crowdsourcing and also by other Fintechs innovations such as Mobile Money. Fintechs innovations are seen as capable of disrupting existing financial industry structures and blurring industry boundaries (Cai 2018). The raison d'être for traditional banks is evolving and some old banking service workflows may be entirely disintermediated.

For instance, in the past, traditional financial intermediaries have gained considerable economies of scale due to their size and the volume of business transacted. They also have obtained cost advantages through effective knowledge management and the accumulation of financial, economic and legal expertise. Powerful intermediaries have often imposed monopoly power and obtained excessive profits for themselves. Such monopolistic status has acted as a barrier system constraining products enhancement and New Product Development and has contributed to inefficiency and poor consumer experience.

However for over 100 years the banking has been regarded as providing reliable effective and efficient financial intermediation for transaction processing and other services such as business loans etc. Such Intermediation has been a fundamental component of finance as services and many critical interrelated purposes such as asset aggregation, market making, risk management and information clearing (Lin 2016). However the banking crisis in 2008, the need to bypass traditional financial markets to obtain lower costs, fewer restrictions and more efficiency and the trend towards decentralisation and network-centric citizen engagement and the new regulatory environment have set the financial services sector on a transformative course towards decentralisation of services new forms of (dis) intermediation such as crowdsourcing, Blockchain and Fintechs innovations.

The unit cost of financial intermediation has declined only marginally since the 2008 global financial crisis (Bazot 2017) (Philippon 2016).

As mentioned, cost and convenience have motivated the emergence and growth of the following innovations with disruptive impacts on the financial intermediation environment as a whole:

A. Blockchain
B. Crowdfunding and Blockchain Technology (ICOs, Tokenomics)
C. Fintechs (Fintechs Innovations)
D. Small Loans ("Micro loans" Microfinance and inclusive finance
E. Mobile Payments/e-Wallets
F. X-as-a-Service (XaaS): Artificial intelligence (AI), Machine Learnings and Robot-Advisor

We now present the Disruption, Challenges & Needs analysis with respect to each of the above innovations impacting the evolution of future forms of financial intermediation.

13.1.1. The Challenges & Needs posed by Blockchain

The essential Blockchain offering is to enable trustless consensus re validity of transactions to be achieved in a decentralised manner. In this way whilst Blockchain eliminates one of the roles that the banks have traditionally played namely as "trusted third parties" it does not eliminate other roles that the banks could play.

Challenges & Needs

i. Blockchain introduces other forms of intermediation.
ii. Proof-of-Stake in itself involves intermediation.
iii. It should not however be concluded that the new forms of intermediation have all the answers. Firstly these are not as yet well-regulated and secondly the traditional banking services will still be needed in some form because although, for example crowd sourcing require lower transaction costs, it does not necessarily offer aggregation and rea-allocation of funds raised in a way that is more efficient than the traditional banking system which any how ultimately provides the aggregation and reallocation services to support crowdsourcing platforms.
iv. Miners in essence perform an intermediary layer similar to the role played by the banks. Bitcoin payment settlements are provided by the miners with their costs and rewards; the future role of miners and their strategic behaviour in mining competition is still evolving.
v. Bitcoin or any token ultimately would need to be converted and without an intermediary it is not possible to exchange bit coin for other currencies.
vi. The financial institutions including mist banks are already exploring ways to use Blockchain to new integrative services leveraging their incumbency in various financial services by thus minimising the layers of intermediaries and therefore the transaction costs. Some of the old financial intermediaries can be thus more efficient and more transparent, in this way re-inventing themselves to become more competitive and therefore having an enduring business model into the future. An example is using Blockchain to help banks reduce their layers of intermediaries (e.g. other banks involved and custodial services) to accelerate the payment process making it faster than the 3-day period it currently takes for a payment to be settled and the actual balance finally reconciled through a network of financial intermediaries. By using an inter-bank Blockchain, the distributed ledger showing the transactions history transparent to all relevant entities' banks could achieve the settlement and reconciliation without a third party, faster and at lower cost. It is estimated that the associated saving for a sizeable bank could be of the order of $20 per annum (Anthemis 2015).
vii. In an exceedingly niche product-focused market, banks have to move towards specialization; some are already re-positioning themselves to become leaders in customer experience, cost-competitive or product / service -specific excellence. For example, some banks are re-structuring their services to become specialize in new product innovation, aggregators, distribution, market segment leaders, or banking X-as-a-service providers. This includes Robotic PA technology, which is a software robot (bots)

enabled business process automation, based on AI (Machine Learning, Recommender Systems, Advanced Personalization, and AI-as-a-service). For instance, as early as 2015 10 major world stock exchanges including London Stock Exchange, CME, Deutsche Beors, NYSE and Nasdaq had already been working towards the application of Blockchain technology in payments systems (Rizzo 2016) and, 80 % of banks had declared the willingness to initiate Blockchain technology projects by the end of 2017 (World Economic Forum 2016).

13.1.2. The Challenges & Needs posed by Crowdfunding and Blockchain Technology

An example of a joint application of crowdfunding and Blockchain innovations is the ICO ('Initial Coin Offering', also known as a token sale) that has led to disruption, and elimination or re-shaping of the old financial intermediaries in the fund-raising process. ICOs emerged in 2017 an ICO can be regarded as a kind of crowdfunding that uses the Blockchain technology to verify transactions.

ICOs work similarly to IPOs but without a linked share ownership; instead, the firm offers to the ICO buyers a digital unit of value called 'tokens' which can be traded in Bitcoins or other cryptocurrencies or a token can be created on top of a Blockchain and governed by a smart contract . Tokens are thus linked to a particular venture (project) in which the ICO buyer as an investor invests funds and the rise/fall in the market value of the tokens is linked to the success of the venture. With the familiar Venture Capitalist (VC) the exit strategy for the investor would be a possible successful IPO, an acquisition or merger of the firm which would allow the VC to recover the returns on their investment.

In this way investors can choose when to exit on companies through token trading thus bypassing the traditional VCs. Moreover, Blockchain tokens are scarce, global, liquid and tradable, making them especially appealing to global investors (Coinbase 2016) (R Massey 2017). ICOs trading showed a very high growth rate initially from less than $100 M in 2015 to 10s of Billions over a couple of years by the end of 2017 and then stabilized with a significant share of the market relative to the VC volumes which by then had also started to hold their ground (Statisa 2019).

Challenges & Needs

i. The challenges relevant to this type of disruption of traditional intermediaries namely crowdfunding bypassing the traditional VCs existing whether and to what extent peer-to-peer platforms can really differentiate themselves from traditional funding channels.
ii. In any case the abiding issue with the peer-to-peer platforms is information asymmetry and the challenge here lie in how Blockchain may be adapted to resolve the issues arising from such information asymmetry.

13.1.3. The Challenges & Needs posed by Fintechs Innovations

Fintechs covers digital innovations and technology-enabled business model innovations in the financial sector.

As alluded to in the introduction to this section although traditional intermediaries are being disrupted by Fintechs, they look set to hold their own essentially by seeking to exploit the new Fintechs to achieve efficiencies and re-shape their offerings. In a rapidly evolving Fintechs innovations landscape new patterns and cooperation competition and tensions are emerging amongst incumbents, new entrants (Porter 2008) and the Regulators.

According to the European Investment fund (H Kraemer-Eis 2018), the following represent the salient European trends in Fintechs

- In the past year, investment volumes in the global Fintechs market have been subject to large fluctuations.
- The sharp decrease in global Fintechs investment volumes between Q1/2018 and Q3/2018 occurred despite relative strength on the US market, while European and Asian investment declined significantly.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

- The dominant position of the US and the EU on the global Fintechs market has been under threat in recent years. Their combined market share has dropped from 90% over the 2010-2012 period to 70% over 2016 to 2018, mostly driven by an expanding Asian market at the expense of the EU.
- The European Fintechs VC ecosystem differs structurally from the other global markets, and is mainly driven by Late Stage VC investment, although this does not translate to higher than average investment sizes.
- The European VC Fintechs market experienced an exceptionally strong year in 2017, with record volumes in the final quarter for both the Late Stage (EUR 507m) and Early Stage (EUR 369M) segments. Preliminary data for the year 2018 indicate a possible market set back.

Challenges & Needs

i. Intermediary essentially are to help support the balancing of money supply and demand i.e. productive capital investment/loans and savings are the two sides of the marketplace and in this context, the intermediaries operate to deliver **a)** Economies of scale, **b)** Risk management, **c)** Asset aggregation and information clearing.

ii. It is important to assess the impact of the Fintechs innovations on the above important roles of the players in the emerging intermediation sector.

iii. As financial markets have become more competitive than ever, it is expected that more efficiency gains to customers in the form of reduced interest margins and fees – particularly so by the incumbents.

iv. To what extent will the Fintechs new entrants will continue to exert competitive advantage based on unit cost of financial intermediation and how would the traditional intermediaries respond to such challenges.

v. Most Fintechs innovations appear to be led by technology companies rather than by banks. Such new entrants, some of them Fintechs start-ups, are not bound by existing systems and are less regulated or not at all.

13.1.4. The Challenges & Needs posed by the Small Loans, Microfinance and Inclusive Finance

Small financial contributions for innovation projects, small loans (“micro loans”, “payday loans”) are also another source of disruption of traditional financial intermediaries and the evolution or reshaping of intermediation in this sector which involves equity finance, guarantees, securitisation, microfinance often for Small and Medium Enterprises (SMEs) , start-ups/ micro-enterprises. As per the June update of the 2018 of the European Small Business Finance Outlook (ESBFO) the following indicates the salient trends of the small loan market with the caveat that a significant part of the market (e.g. unrated bilateral transaction type) is not visible in the statistical data.

- SMEs borrowing costs continue to vary greatly within Europe, with Greek, Irish and Slovakian SMEs operating in the most expensive lending environment. In Spain, the interest rate charged on small loans continued to decline.
- While banks have eased their credit standards, they grew more cautious about the future, possibly indicating a pending reversal in their accommodating lending policies.
- While on average, the external financing market improved for Euro area SMEs, 1 in 4 still report severe difficulties in accessing external finance sources. For Greece, this number rises to nearly 1 in 2.
- SMEs continue to report a lack of public support to external financing markets.

According to According to the European Investment Fund Report (H Kraemer-Eis 2018), the following indicates the salient trends of the Microfinance and inclusive finance market:

- Microenterprises and social enterprises are important contributors to employment and social value, especially in countries with high unemployment rates.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

- According to the data from the latest ECB SAFE survey, microenterprises have perceived a decrease in the external financing gap indicator. However, the share of enterprises which see access to finance as their most important problem remained higher among microenterprises than among their larger peers.
- Microenterprises, in general, use less bank loans than their larger peers, as they are more likely to be rejected if they decide to apply for a bank loan. Often not apply for a bank loan due to fear of rejection, but also because of insufficient collateral, high interest rates and excessive paperwork.
- Customers, as they get rejected by or discouraged from banks, often apply for a microcredit from Microfinance institutions (MFI). MFIs do not always charge lower interest rates than banks, but they are less demanding in terms of collateral and guarantee requirements. MFIs offer their clients more personal, tailor-made and simple products; MFIs “know their customers”.
- Digitalization of microfinance operations is efficient for both lenders and borrowers, but yet suppliers are only partially digitalized and poor customers often have no access to digital payments.
- Access to finance is crucial not only for existing microenterprises, but also for those who are eager to
- create a business in order to escape poverty or unemployment and contribute to job creation. In addition to financial support, unemployed people are often in need of acquiring the necessary skills for success through coaching and mentoring.
- MFIs, especially non-bank MFIs face challenges in securing funding to support growth. They also are in need of additional investment in technologies in order to stay competitive with Fintechs.

The International Finance Corporation (IFC), (World Bank Group 2010), published the findings of their research on factors relating to the availability of Small Loans, for SMEs in Indonesia, seeking loans though the traditional banks. This research included a mystery shopper type of experiments with the same request for a hypothetical loan being put to various banks by someone posing as an SME and the results which may be the shared experience of most SMEs, revealed that:

- Banks, as institutions, vary substantially in products offered and loan requirements.
- Most individual bank branches offered just one type of loan.
- Although there is product variation in the overall small-medium business loan market, businesses can only find out about that variation by shopping around themselves.
- Bank officers’ service quality is often quite poor, very little cross-selling of other products is done even when a client is in the office.

In the USA, the limitations facing the SMEs in securing loans led to the following request by a Congress sub-committee. The US 113 Congress, (US 113 Congress, House Sub-Committee Hearing 2014 2014) urged Congress to “support legislation to revisit the business lending cap to make it easier for credit unions to meet the business lending needs of their members and to expand participation in SBA” (Strategic Business Administration) programmes.

Challenges & Needs

i. The traditional banks small loan sector in so far as it mainly intended to have a focus for serving the SMEs is expected to provide a portfolio of services including equity finance, guarantees, securitisation, and microfinance, the new forms of intermediaries in the Small Loans sector mainly operate in the small loans market.

ii. Clearly the banks do not appear to serve the small loans and microfinance market well since it is widely reported that both in Europe and worldwide the SMEs a whole, and in some European countries particularly, face difficulties securing small loans through the banks.

iii. Micro-enterprise face even more difficulties than SMEs in securing loans through the banks, so much so that they mostly do not apply to the banks but to MFIs instead.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

iv. Such difficulties are expected to even more severely affect unemployed persons seeking funding for re-training.
v. MFIs in contrast to the banks tend to care to provide tailor-made loans to their SME clients.
vi. MFIs rates are comparable to the banks than the banks.
vii. MFIs pose less stringent lending pre-conditions than banks in terms of security etc.
viii. MFIs themselves suffer from lack of investment to support their growth and uptake of new Fintechs technology.
ix. Some MFIs are only partially digitalized and some customers not at all and so have no access to digital payments.
x. Bank officers' service quality is often quite poor, very little cross-selling of other products is done even when a client is in the office.

13.1.5. The Challenges & Needs posed by Mobile Money, Mobile Payments, E-Wallets

Increasing mobile consumer and P2P payments are fuelling the global growth of mobile international payment services. A variety of mobile payment options exist, the most common being, mobile POS mobile payments, apps for shopping online and mobile wallets. However Mobile Payments in our analysis here is to be distinguished from that using a mobile phone for money transfers or online shopping using a payment pre-processor (e.g. PayPal, using credit card details). Mobile payment here is that which uses:

i. an electronic wallet (e-wallet) service which stores, sends and receives money, using:
ii. the user's mobile phone device, and,
iii. technology such as near-field communication (NFC) payments as Apple pay uses, Magnetic secure transmission (MST) payments as deployed by Samsung Pay or Sound waves-based /signal-based payments to make an in-store or point of sale payments using mobile wallets.

This kind of Mobile Money usage is a trend with potentially significantly disruptive impacts on the banking sector developments as the move towards cashless transactions has taken a firm hold particularly in emerging markets such as parts of Africa e.g. Kenya, Tanzania and Uganda) and become increasingly popular in China, Korea and Japan. Analysis of data on the rapid increase of mobile money in Africa has shown that mobile money systems offer new opportunities for distributing cash transfers and can affect economic outcomes in developing countries (Aker 2010) (Empirical evidence based on similar data from Kenya has shown that mobile money has had a significant impact on risk sharing attributable to the reduction in transaction costs (the costs of transferring resources between individuals (Jack 2014). The reduction in transaction costs and convenience are amongst the main drivers responsible for the mass scale mobile payment market adoption that has become disruptive of the banking sector revenue streams from credit and debit cards as can be seen in Figure 21. below:

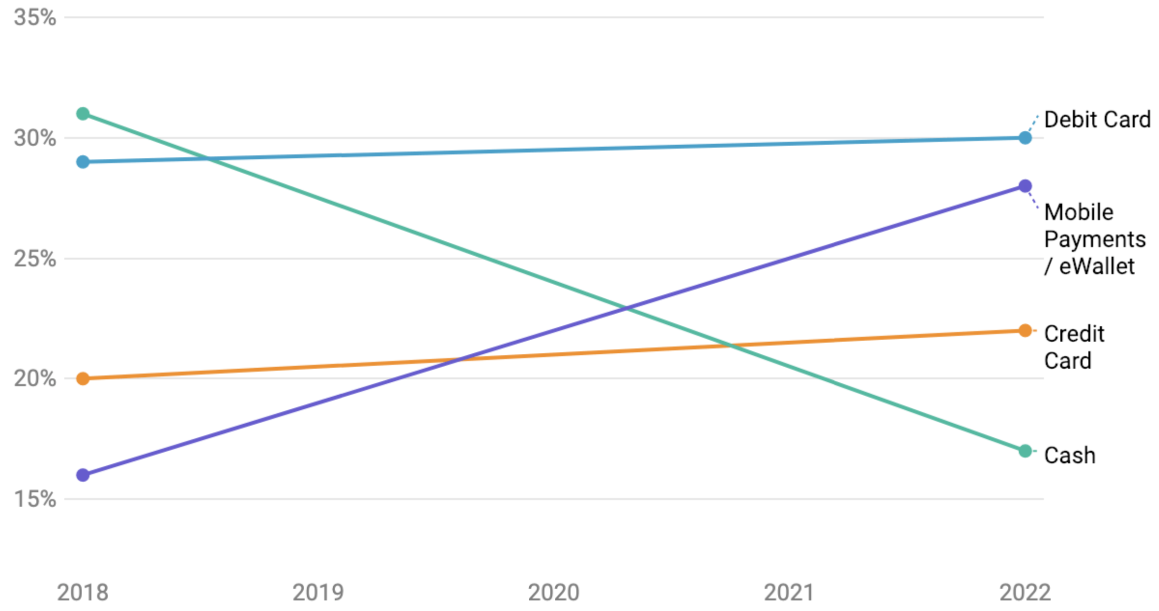


Figure 21. Trend in growth of traditional payment methods compared to e-wallets, (Global Mobile Payment Stats, Trends & Forecasts 2019)[19]

The worldwide mobile payment revenue in 2015 was 450 billion U.S. dollars and is expected to surpass 1 trillion U.S. dollars in 2019 (Payment Industry Intelligence 2019).

By 2023, it is estimated that there will be 1.31 billion proximity mobile payment transaction users worldwide, up from 950 million users in 2019 (Payment Industry Intelligence 2019).

In most countries, Mobile phones are still in early evolutionary stages. Across the world, approximately 2.07 billion people used mobile wallets to make a purchase in 2019; an increase of around 30% over the 1.6 billion mobile payment users recorded as of the end of 2017.

The Figure 22 below shows the relative volumes of mobile payment usage in various countries which shows China as the leader in growing Mobile payment adoption with Alipay and WeChat, with QR codes supporting the growth of this growth; in contrast as it is NFC, rather than QR that is predominantly used for mobile payments across the western world, the lack of QR acceptance points has restricted the take-up.

By early 2019, Wechat, AliPay and Samsung Pay who had been amongst the leading mobile payment providers, each had over 1 billion active users already; ApplePay, Paypal, Amazon, Google Pay have been trailing far behind but have seen their market share increase steadily consistent with the growth of mobile payments overall.

[19] https://www.merchantsavvy.co.uk/mobile-payment-stats-trends/

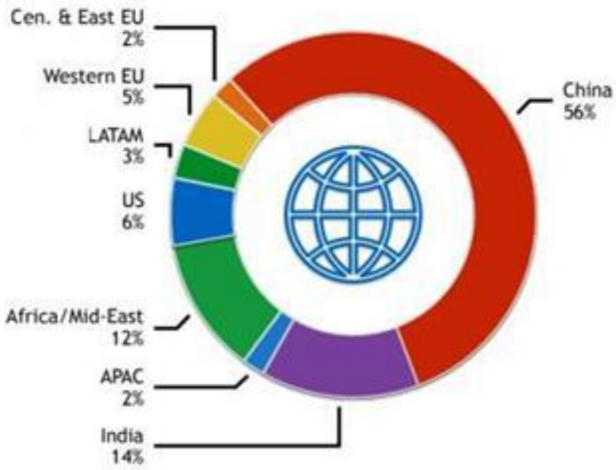


Figure 22. Relative volumes of mobile payments across the world (Mobile Wallet Trends Annual Report 2019, Payment Industry Intelligence)[20]

With the proliferation of smartphones and tablets in developing countries, the mobile payment technologies revenues around the globe are expected to increase at a CAGR of 20.5% between the years of 2016 and 2024. From $338.72 billion in 2015 to $1,773.17 billion in 2024 (Payments Market 2019).

Mobile payment use across Europe has significantly increased last year, jumping 200% from 2015 (18%) to 2016 (54%) (Rolfe 2017). In Europe, the British are leading adoption of mobile payment, with 74% of UK citizens using a mobile device to make payments and manage their finances. Swedes are expected to use cash for barely 0.5% of all payments made in 2020 (Henley 2016). Denmark is another European country with a relatively high uptake of mobile payment; as high as around 60% back in 2016 and expected to have substantially increased by 2020 (Henley 2016). In the U.S., mobile wallets are expected to surpass the use of both credit and debit cards by 2020 (Bradley 2016).

The results of a survey amongst cybersecurity professionals have shown that they are not convinced of the security of mobile payments; only 23% are confident that the personal information used in association with mobile payments is safe. Eighty-nine percent agree that cash is the most secure payment method available, but only 9% prefer to use it (Bradley 2016). The highest security vulnerability associated with mobile payments is public Wi-Fi (26%), followed closely by lost or stolen devices (21%) (ISACA 2015).

Challenges & Needs

i. **Growth Opportunities:** generational differences greatly influence payment mechanisms, as well as the availability of technology (Mobile Wallet Trends 2019).
ii. **Online Merchant Needs:** fraud reduction and compliance regulations, which vary from country to country, play a role in the creation of new payment mechanisms (Mobile Wallet Trends 2019).
iii. **Offline Merchant Needs:** increased efficiency, cost savings to the merchant and increased customer loyalty are all benefits to entering the mobile payment space (Mobile Wallet Trends 2019).
iv. **Lack of access to a traditional bank account but access to a mobile phone/tablet:** Over 1.7 billion adults (21% of the world's total population) do not have access to a traditional bank account. Of these over a billion would be mobile phone users and thus potentially e-wallet users.
v. **Lock-in:** in terms of proprietary Hardware and contracts.
vi. **User Experience, therefore, User Loyalty**: Continuous customer engagement is correlated with high potential success, evidenced by companies with outstanding user experiences, such as Uber.

[20] https://www.paymentscardsandmobile.com/mobile-wallet-trends-annual-report-2019/

vii. **Cross- Generational Factors:** the uptake of mobile payments is prevalently due to Gen Y and Gen Z (Mamonova 2019). This observation has been supported by a study conducted by the Pew Charitable Trusts which concluded that around 70% percent of millennials used mobile payments and identified rewards and/or discounts as the most compelling motivational factors motivating their choice.

viii. **Security:** this is a significant barrier to mobile payment uptake, with 70% of the U.S. population regarding it as such.

ix. **Excellent UX**: Mobile Payments may still be in their early uptake phase in many countries, but the deployment of technology and applications that can maintain improved user experience will support higher adoption and engagement.

13.1.6. The Challenges & Needs posed by X-as-a-Service-based AI Support for the Financial Sector

Service-oriented intelligent systems and services on the XaaS model such as AI-as-Service will increasingly shape the value propositions from intermediaries and as such the enabling technology for new innovative products offerings in the financial markets, and new forms of financial (dis) intermediation including direct access to capital, small/micro loans and e.g. using AI agencies and robot-advisors and KYC supported regulatory compliance management, customer authentication and fraud detection.

Challenges & Needs

i. Despite and also because of continuing pressure on operational cost-efficiency, automation has to be pursued integratively including in particular for operational X-a-a-S enablement model to include intelligent/recommender and security support services.

ii. A network-centric, automated and thus efficient secure, deeply-personalised service delivery will have to feature amongst the key operational objectives of the intermediaries, old and new, and these will have to be underpinned by integrated automation.

iii. Integration of cognitive automation incorporating Robotic Process Automation, Domain Expert-Knowledge–Based Services and Machine/deep learning/ Data Analytics, Natural Language Processing (NLP), Visualization and Virtual Assistants (as illustrated in Figure 23 below) to include support for:

   a. **Operational Efficiency, Security Accountability:** e.g. fraud detection, risk management, regulatory compliance management, cybersecurity payments reconciliation and trade documents scrutiny, identity verification/user authentication such as smile to unlock and liveliness checking.

   b. **Customer Services:** e.g. the use of chat bots will show tangible gains in productivity and cost savings, deeply-personalised recommendations at scale on self-service channels based on data from the bank, third party channels, mobile usage patterns, and other sources.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

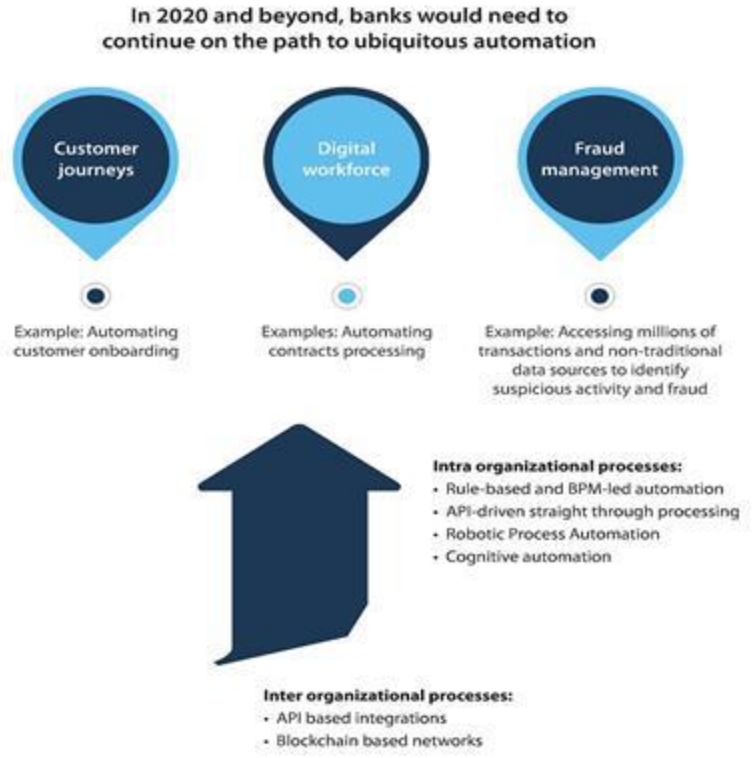

In 2020 and beyond, banks would need to continue on the path to ubiquitous automation
Customer journeys
Digital workforce
Fraud management
Example: Automating customer onboarding
Examples: Automating contracts processing
Example: Accessing millions of transactions and non-traditional data sources to identify suspicious activity and fraud
Intra organizational processes:
• Rule-based and BPM-led automation
• API-driven straight through processing
• Robotic Process Automation
• Cognitive automation
Inter organizational processes:
• API based integrations
• Blockchain based networks

Figure 23. AI Automation Needs for the Banking & Financial Services Sector (Rolfe2019). (Payments Cards and Mobile)[21]

13.2. Stakeholders' (SoA-SoM-SoP)-Gaps-Responsive Requirements

The disruptive influences of emergent forms of intervention have led to rapidly evolving forms of intermediation that have significantly impacted the shapes of the traditional financial sector products and prospects into the future. New paradigms for fund raising such as Crowdfunding and Blockchain-enabled Tokenomics (ICOs), Fintechs, emergent Small Loans trends and the unrelenting pace of automation in particular for workflow embedded cognitive Robotic Process Automation and AI advisory services on the X-as-a service model are being pursued for user-experienced–based differentiation, operational efficiency and cost-based competitive advantage.

Our analysis of the challenges, needs and thus the technological gaps in such an evolving landscape has to be itself evolving responsive to the developments and future trends as can be observed over the lifetime of the Critical-Chains project and thus to be updated in the subsequent deliverables.

However, it is already clear that the following market requirements should be considered amongst the priority candidates for Critical-Chains enabled support using Blockchain and X –as-a-Service Solution Stack to provide:

i. Block-Chain-enabled provision of a portfolio of services including
ii. Inclusive Small-Loans, Micro-finance
iii. Equity Finance
iv. Guarantees
v. Securitisation

[21] https://www.paymentscardsandmobile.com/9-trends-reshaping-banking-in-2020-3-automation-alive-and-well/

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

X-as-a Service Solution Stack to provide a portfolio of banking services support:

i. Blockchain-as-a-Service
ii. Cyber Security-as-a-Service
iii. Authentication as a Service
iv. Accountability-as-a-Service
v. FlowModelling-as-s Service
vi. Fraud detection-as-a Service

The use-cases supporting the above are set out in the Deliverable D2.1 (Specifications & Architectural Design) and will be re-visited following the first phase of usability evaluations and ongoing stakeholder-centred co-refection and revision of requirements; this will be updated in the subsequent version of the deliverable.

The business model ling and exploitation planning with respect to the above as candidate value propositions will be addressed within deliverable **D7.4** Report on business modelling, IPR and innovation modelling D7.8 (Business Modelling, IPR and innovation Management).

14. Conclusions

This deliverable, D2.1 (Technology & Watch Update), the has provided a systematic analysis of the evolving disruptive forces arising through the new Fintechs, intermediation innovations, the integration of Blockchain technology and Crowdfunding establishing tokenomics, the new mobile money payment industry based on e-wallets for mobile payments and the developing Small Loans and Microfinancing market. This methodologically-guided analysis has included the technology State-of-the-Art (SoA), State-of-the-Market (SoM) and State-of-Practice (SoP) and the Regulatory Environment. The perspective has factored in the Pull-Push market forces to examine the emergent competitive landscape.

Consistent with the central objective of this deliverable, the work has culminated in a Challenges & Needs Analysis perspective of the emergent Financial Services eco-system, factoring in the disruptive pressures that have impacted the Financial Intermediation and Payment Industries over the last decade. This has provided an initial indication of the Stakeholders' market-gaps-responsive requirements.

Accordingly the analysis has confirmed the need for an X-as-a-Service Solution Stack to provide a portfolio of banking services support for Blockchain, Authentication, Accountability, Transaction Flows Modelling, Anomaly/Fraud Detection, Cyber Security and Blacklisting. In particular the analysis of the current cyber-attacks on financial infrastructures has shown that there is a pressing need for more cyber security within the Fintechs applications domains. This has served to put in sharp focus the envisioned innovation objectives of Critical-Chains in aiming to provide a holistic and adaptable framework, including end-users and financial authorities who use new technologies beyond the State-of-the-Art. A novel "X-as-a-Service" (XaaS) platform is thus to be developed to protect financial infrastructures against illegal money trafficking and fraud on Fintechs operations. Furthermore, the framework shall be compliant with current regulations, such as the Payments Services Directive 2, Cloud service regulations, Blockchain regulations and Artificial Intelligence regulations.

It is also concluded that there is an opportunity for a Blockchain-enabled portfolio of services for Inclusive Small-Loans, Microfinance, Equity Finance, Guarantees, and Securitisation. This will support inclusive and transparent loan availability particularly for the SMEs, Micro-enterprises and re-training for unemployed persons.

The above conclusions have informed the prioritisation of use-cases within the iterative Critical-Chains design requirements as set out in Deliverable D2.3 (Specifications & Architectural Design) as well as suggesting possible exploitation opportunities as shall be explored within Deliverable D7.8 (Business Modelling, IPR and innovation Management).

****

1 References

360researchreports.com. 2018. *Hardware Security Module (HSM) Market 2019 Industry Size, Trends, Global Market Size & Growth, Insights and Forecast Research Report 2025.* 23 July. Accessed November 25, 2019. https://www.360researchreports.com/global-hardware-security-module-hsm-market-research-report-2019-12817574.

Abdallah, Aisha, Mohd Aizaini Maarof, and Anazida Zainal. 2016. "Fraud detection system: A survey." *Journal of Network and Computer Applications* (Elsevier) 68: 90-113.

Abi-Antoun, Marwan, Daniel Wang, and Peter Torr. 2007. "Checking threat modeling data flow diagrams for implementation conformance and security." *Proceedings of the twenty-second IEEE/ACM international conference on Automated software engineering.* 393-396.

Ahmed, Mohiuddin, Abdun Naser Mahmood, and Md Rafiqul Islam. 2016. "A survey of anomaly detection techniques in financial domain." *Future Generation Computer Systems* (Elsevier) 55: 278-288.

Aker, J C. 2010. "Information from Markets near and far: Mobile Phones and Agricultural Markets in Niger." *American Economic Journal: Applied Economics* 46-59.

Alberts, C, A Dorofee, J Stevens, and C Woody. 2003. *Introduction to the OCTAVE Approach.* Carnegie Mellon University.

Al-Matari, Yahya Ali, Sallahuddin Hassan, and Hassan Alaaraj. 2016. "Application of Basel Committee's New Standards of Internal Audit Function: A Road Map towards Banks' Performance." *International Journal of Economics and Financial Issues.*

Anthemis. 2015. *Fintech2.0.* Accessed April 2019. http://www.oliverwyman.com/our-expertise/insights/2015/jun/the-Fintech-2-0-paper.html.

Apache Software Foundation. 2012. *Apache Jena.* Apache Software Foundation. http://jena.apache.org/.

Arner, Douglas, Janos Barberis, and Ross Buckley. 2016. "The evolution of fintech: A new post-crisis paradigm?" *UNIVERSITY OF NEW SOUTH WALES LAW RESEARCH SERIES.*

Autonomous Research LLP. 2018. *#AUGMENTED FINANCE & MACHINE INTELLIGENCE.* Accessed November 21, 2019. https://next.autonomous.com/augmented-finance-machine-intelligence.

Badii, Atta. 2008. "User-intimate requirements hierarchy resolution framework (UI-REF)." *AmI-08: Second European Conference on Ambient Intelligence.*

Badii, Atta, David Fuschi, Ali Khan, and Adedayo Adetoye. 2009. "Accessibility-by-Design: A Framework for Delivery-Context-Aware Personalised Media Content Re-purposing." *HCI and Usability for e-Inclusion.*

Bani-Hani, Anoud, Munir Majdalweieh, and Aisha AlShamsi. 2019. "Online Authentication Methods Used in Banks and Attacks Against These Methods." *Procedia Computer Science, Volume 151.*

Bazot, G. 2017. "Financial Consumption and the Cost of Finance: Measuring Financial Efficiency in Europe." *Journal of the European Economic Association 16 (1)* 123-160.

Bedri, Bia. 2019. "The Pulse of Fintech." *KPMG*, 31 July.

Behera, Tanmay Kumar, and Suvasini Panigrahi. 2015. "Credit card fraud detection: a hybrid approach using fuzzy clustering & neural network." *2015 Second International Conference on Advances in Computing and Communication Engineering.* 494-499.

Beyst, B. 2016. *Which Threat Modelling.* ThreatModeller. 15 April. https://threatmodeler.com/2016/04/15/threat-modeling-method/ .

Bhattacharyya, Siddhartha, Sanjeev Jha, Kurian Tharakunnel, and J. Christopher Westland. 2011. “Data mining for credit card fraud: A comparative study.” *Decision Support Systems* (Elsevier) 50: 602-613.

Blueoceanfinance. 2019. Accessed 12 12, 2019. https://www.blueoceanfinance.it/gestione-aziendale/accordi-di-basilea/.

Board, FSB – Financial Stability. 2019. “Fintech and market structure in financial services: Market developments and potential financial stability implications.”

Bradley, B. 2016. *Millenials and Mobile Payments: What is the price of convenience? Business2Community.* https;//www.business2commmunity.com/obile-apps/millennials-mobile-payments-price-convenience-01558204.

Bragg, Steven. 2018. *Types of audits.* 07 May. Accessed November 21, 2019. https://www.accountingtools.com/articles/types-of-audits.html.

Brickley, Dan, and R.V Guha. n.d. “RDF Vocabulary Description Language 1.0: RDF Schema.”

Bromander, Siri, Audun Jøsang, and Martin Eian. 2016. “Semantic Cyberthreat Modelling.” *STIDS.* 74-78.

Cai, C W. 2018. “Disruption of Financial Intermediation of Fintech, a review on crowdfunding and Blockchain.” *Journal of Accounting and Finance.* https://doi.org/10/1111/acfi.12405.

Carnegi. 2017. *Timeline of Cyber Incidents Involving Financial Institutions.* Accessed November 21, 2019. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Chang, Jau-Shien, and Wen-Hsi Chang. 2012. “A cost-effective method for early fraud detection in online auctions.” *2012 Tenth International Conference on ICT and Knowledge Engineering.* 182-188.

Chang, Jenny. 2019. *What is Compliance Management Software? Analysis of Features, Benefits and Pricing.* Accessed November 21, 2019. https://financesonline.com/what-is-compliance-management-software-analysis-of-features-benefits-and-pricing/.

Chang, Wen-Hsi, and Jau-Shien Chang. 2010. “Using clustering techniques to analyze fraudulent behavior changes in online auctions.” *2010 International Conference on Networking and Information Technology.* 34-38.

Cheung, C.Y. 2016. *Threat Modeling Techniques .* Delft University of Technology.

Cleland-Huang, J. 2014. *How Well Do You Know Your Personae Non Gratae? .* IEEE Software.

Coinbase. 2016. *A securities law framework for Blockchain tokens.* Accessed April 2019. htttps://www.coinbase.com/legal/securities-law-framework.pdf.

Consilium.europa.eu. 2019. 12 03. Accessed 12 12, 2019. https://www.consilium.europa.eu/it/policies/banking-union/single-rulebook/capital-requirements/.

Cyberlaws. 2019. Accessed 12 12, 2019. https://www.cyberlaws.it/2017/articolo-25-gdpr-regolamento-generale-sulla-protezione-dei-dati-ue2016679/.

Degabriele, Jean Paul, Kenny Paterson, and Gaven Watson. 2010. “Provable security in the real world.” *IEEE Security & Privacy* (IEEE) 9: 33-41.

Deloitte. 2019. *RegTech Universe.* Accessed November 21, 2019. https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html.

Deutsche-bank. 2019. *PSD2.* Accessed 12 12, 2019. https://www.deutsche-bank.it/psd2.html.

EACH. 2019. *About clearing.* Accessed 12 12, 2019. https://www.eachccp.eu/about-clearing/.

ec.europa.eu. 2009. *ec.europa.eu.* Accessed 12 12, 2019. https://ec.europa.eu/economy_finance/bef2009/speakers/jacques-de-larosiere/.

European Central Bank. 2010. “The payment system.”

European Parliament. 2016. 27 04. Accessed 12 12, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

—. 2007. *Council of the European Union.* 13 11. Accessed 12 12, 2019. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32007L0064.

EY. 2019. *Global FinTech Adoption Index 2019.* Accessed November 21, 2019. https://assets.ey.com/content/dam/ey-sites/ey-com/en_gl/topics/banking-and-capital-markets/ey-global-fintech-adoption-index.pdf.

Famularo, Massimo, and Anne Magazine. 2018. 03 07. Accessed 12 12, 2019. https://it.blastingnews.com/economia/2018/07/fintech-il-futuro-delle-banche-e-nella-capacita-di-sfruttare-i-dati-002645843.html.

FINCH CAPITAL. 2019. “The state of European Fintech.” *DEALROOM.*

FIRST. n.d. *https://www.first.org/cvss/v3.0/specification-document.* FIRST. https://www.first.org/cvss/v3.0/specification-document.

Gai, Keke, Meikang Qiu, and Xiaotong Sun. 2018. “A survey on FinTech.” *Journal of Network and Computer Applications* (Elsevier) 103: 262-273.

Gengler, Emmy. 2018. *The 5 Top Fintech Trends for 2019.* 26 November. Accessed November 21, 2019. https://softjourn.com/blog/article/the-5-top-fintech-trends-for-2019.

Glancy, Fletcher H., and Surya B. Yadav. 2011. “A computational model for financial reporting fraud detection.” *Decision Support Systems* (Elsevier) 50: 595-601.

Glowinski, Kamil, Andreas Krawinkler, and Christian Gossmann. 2018. “Security analysis of a cloud backup service based on a smart site failover.”

Goldsmith, Jett. 2014. “95% of ATM machines still use Windows XP, and will be exposed to vulnerabilities after April 8.”

Group, W3C OWL Working. 2009. *OWL 2 Web Ontology Language Document Overview. W3C Recommendation 27 October 2009.* W3C Consortium. http://www.w3.org/TR/2009/REC-owl2-overview-20091027/.

Gruber, Thomas. 1993. “A Translation Approach to Portable Ontology Specifications.” *Knowledge Acquisition* 5 (2): 199.

H Kraemer-Eis, Botsari A, Gvetadze S, Lang F, Torfs W. 2018. “EIF Research & Market Analysis EIF VC Survey.” https?//www.eif.org > news_centre > publications > eif-wp-51.

Hammar, Mark. 2019. *Il modello 'Plan-Do-Check-Act' nella norma ISO 9001.* Accessed November 21, 2019. https://advisera.com/9001academy/it/knowledgebase/il-modello-plan-do-check-act-nella-norma-iso-9001/.

Haupert, Vincent, and Tilo Müller. 2018. "On App-based Matrix Code Authentication in Online Banking." *In Proceedings of the 4th International Conference on Information Systems Security and Privacy – Volume 1: ICISSP.*

Henley. 2016. "Sweden leads the race to become cashless society." *The Observer Banking Review, Guardian Group.*

Herman, Ivan. 2012. *Tutorial on Semantic Web.* W3C Consortium. http://www.w3.org/People/Ivan/CorePresentations/SWTutorial/Slides.pdf.

Hernan, S, S Lambert, and A Shostack. 2006. *Uncover Security Design Flaws Using the STRIDE Approach.* MSDN Magazine.

Hochstein, Marc. 2015. *Fintech (the Word, That Is) Evolves.* 5 October. Accessed November 21, 2019. http://www.americanbanker.com/bankthink/fintech-the-word-that-is-evolves-1077098-1.html.

Howard, Michael, and Steve Lipner. 2006. *The security development lifecycle.* Vol. 8. Microsoft Press Redmond.

hypo-alpe-adria.it. 2015. 31 12. Accessed 12 12, 2019. https://www.hypo-alpe-adria.it/files/informativa_al_pubblico_sulla_situazione_al_31122015.docx.pdf.

iAuditor. 2019. *The Best Compliance Audit Checklists.* Accessed November 21, 2019. https://safetyculture.com/checklists/compliance-audit/.

INFOSEC. 2014. *Qualitative Risk Analysis with the DREAD Model.* INFOSEC. 21 May. https://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model/.

Irwin, Luke. 2017. 03 11. Accessed 12 12, 2019. https://www.itgovernance.eu/blog/en/how-the-gdpr-will-protect-individuals.

ISACA. 2015. *ISACA Survey.* Accessed April 2019. http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015Pages/isaca-survey-mobile-payments-data-breaches.aspx.

J, Aker. 2010. "Information from Markets Near and Far: Mobile Phones and Agricultural Markets in Niger." *American Economic Journal: Applied Economics* 46-59.

Jack, W. 2014. "Risk Sharing and Transaction Costs: Evidence from Kenya's Mobile Money Revolution." *American Economic Review* 183-223.

Kapersky. 2018. *Financial Cyberthreats in 2018.* 07 March. Accessed November 11, 2019. https://securelist.com/financial-cyberthreats-in-2018/89788/.

Kashyap, Manoj, John Shipman, Haskell Garfinkel, Steve Davies, and Dean Nicolacakis. 2017. "Redrawing the lines:FinTech's growing influence on Financial Services."

Kim, Y, Park Y, Choi J, Yeon J. 2016. "The adoption of mobile payment services for Fintech." *International Journal of Applied Engineering Research.*

Kirkwood, Jodyanne. 2009. "Motivational Factors in a Push–Pull Theory of Entrepreneurship." *Gender in Management: An International Journal. 24. 346-364. 10.1108/17542410910968805.*

KPMG. 2016. "KPMG internal audit."

La, Hyun Jung, and Soo Dong Kim. 2018. “A Machine Learning Framework for Adaptive FinTech Security Provisioning.” *Journal of Internet Technology* 19: 1545-1553.

Laszlo, Peter. 2019. “The Pulse of Fintech.” *KPMG*, 31 July.

Le Khac, Nhien An, and M.-Tahar Kechadi. 2010. “Application of data mining for anti-money laundering detection: A case study.” *2010 IEEE International Conference on Data Mining Workshops.* 577-584.

Leblanc, D. 2007. *DREADful.* 14 August. https://blogs.msdn.microsoft.com/david_leblanc/2007/08/14/dreadful/ .

Lhuer, Xavier, Phil Tuddenham, Sandhosh Kumar, and Brian Ledbetter. 2019. “Next-generation core banking platforms: A golden ticket?”

Lin, T C W. 2016. “Infinite financial intermediation.” *Wake Forest Law Review 50* 543-669.

Lindros, Kim. 2017. *What is GRC and why do you need it?* 11 July. Accessed November 21, 2019. https://www.cio.com/article/3206607/what-is-grc-and-why-do-you-need-it.html.

Lippmann, Richard, Kyle Ingols, Chris Scott, Keith Piwowarski, Kendra Kratkiewicz, Mike Artz, and Robert Cunningham. 2006. “Validating and restoring defense in depth using attack graphs.” *MILCOM 2006-2006 IEEE Military Communications conference.* 1-10.

Liu, Yajun, and Xuan Zhang. 2016. “Intrusion detection based on IDBM.” *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech).* 173-177.

Magomedov, Shamil, Sergei Pavelyev, Irina Ivanova, Alexey Dobrotvorsky, Marina Khrestina, and Timur Yusubaliev. 2018. “Anomaly Detection with Machine Learning and Graph Databases in Fraud Management.” *(IJACSA) International Journal of Advanced Computer Science and Applications* 9: 33.

Mamonova. 2019. *Trends for the Future of Payment Processing.* Accessed April 2019. http://ikajo.com'blog/digital-payment-trends.

Manola, Frank, and Eric Miller. 2004. *RDF Primer. W3C Recommendation 10 February 2004.* W3C Consortium. http://www.w3.org/TR/2004/REC-rdf-primer-20040210/.

Mayer, N. 2009. “Model-based Management of Information System Security Risk.”

McCarthy, Philip. 2005. *Search RDF data with SPARQL. SPARQL and the Jena Toolkit open up the semantic Web IBM DeveloperWorks Technical Library Series.* IBM DeveloperWorks. http://www.ibm.com/developerworks/xml/library/j-sparql/.

McGuiness, Deborah, and Frank van Harmelen. n.d. “OWL Web Ontology Language Overview.”

Mead, N, E Hough, and T Stehney. 2005. *Security Quality Requirements Engineering Technical Report.* Carnegie Mellon University.

Mead, N, F Shull, K Vemuru, and O Villadsen. 2018. *A Hybrid Threat Modeling Method.* Carnegie Mellon University.

Merli, Alessandro. 2009. *ilsole24ore.* 29 02. Accessed 12 12, 2019. https://st.ilsole24ore.com/art/SoleOnLine4/Speciali/2007/mercati_mercanti/mercati_mercanti_a_merli_250209.shtml?refresh_ce=1.

Microsoft. 2009. *The STRIDE Threat Model.* Microsoft. 11 November. https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN.

Mobile Wallet Trends. 2019. *Mobile Wallet Trends Annual Report 2019, Payment Industry Intelligence.* Accessed April 2019. https://www.paymentscardsandmobilecom/mobile-wallet-trends-annual-report-2019/.

Morrison, A., and R Wensley. 1991. “Boxing up or boxed in?: A short history of the Boston Consulting Group share/growth matrix.” *Journal of Marketing Management*, 105-129.

2019. *Payment Industry Intelligence.* Accessed 2019. https://www.paymentscardsandmobile.com/mobile-wallet-trends-annual-report-2019.

2019. *Payments Market.* Accessed April 2019. https://www.transparencymarketresearch.com/mobile-payments-market.html.

Philippon, T. 2016. “The Fintech Opportunity.” *The National Bureau of Economic Research Working Paper 22476.* http://www.nber.org/papers/w22476.

Piovan, Diego, David Pirondini, and Alessandro Vidussi. 2019. *RegTech: Get Onboarding The challenges of compliance.* 06 July. Accessed November 21, 2019. https://www.finriskalert.it/?p=7443.

—. 2019. *RegTechs: Get Onboarding The challenges of compliance.* 06 July. Accessed November 21, 2019. https://www.finriskalert.it/?p=7443.

Pogson, Keith. 2019. “Why banks can’t delay upgrading core legacy banking platforms.”

Pollari, Ian, and Anton Ruddenklau. 2019. “The Pulse of Fintech.” *KPMG*, 31 July.

Porter, M E. 2008. “The five competitive forces that shape strategy.” *Harvard Business Review, Leadership & Strategy.*

Potluri, Sasanka, and Christian Diedrich. 2016. “Accelerated deep neural networks for enhanced Intrusion Detection System.” *2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA).* 1-8.

Potteiger, B, G Martins, and X Koutsoukos. 2016. “Software and attack centric integrated threat modeling for quantitative risk assessment.” In *Proceeding of the Symposium and Bootcamp on the Science of Security*, 99-108.

Prdu’hommeaux, Eric, and Eric Seabone. 2008. *SPARQL Query Language for RDF.* W3C Consortium. 15 January. http://www.w3.org/TR/2008/REC-rdf-sparql-query-20080115/.

R Massey, Dalal D, Dakshinamoorthy A. 2017. *Initial coin offering a new paradigm.* Deloitte. https?//www2.deloitte.com/content/dam/Deloitte/us/documents/process-and-operations/us-cons-new-paradigm.pdf.

RDF Working Group. 2010. *Resource Description Framework.* W3C Consortium. http://www.w3.org/RDF/.

RETAIL BANKING ACADEMY. 2014. “Course Code 108 - Operations.”

Rizzo, P. 2016. *10 stock and commodities exchanges investigating blockchain tech.* http://www.coindesk.com/10-stock-exchanges-blockchain/.

Rolfe. 2017. *Mobile Payments are taking Off.* Accessed April 2019. https://www.mobilepaymentsworld.com/mobile-payments-are-taking-off.

This project has received funding from the European Union Horizon 2020 Programme for research, technological innovation and demonstration under Grant Agreement number 833326 H2020-SU-DS-2018

Russo, Nunzia. 2019. *RegTech: grande opportunità e primo passo verso una digital compliance.* Accessed November 21, 2019. http://www.riskcompliance.it/news/regtech-grande-opportunita-e-primo-passo-verso-una-digital-compliance/.

Sahin, Yusuf, and Ekrem Duman. 2011. "Detecting credit card fraud by ANN and logistic regression." *2011 International Symposium on Innovations in Intelligent Systems and Applications.* 315-319.

Saitta, P, B Larcom, and M Eddington. 2005. "Trike v.1 Methodology Document [Draft]."

Scandariato, R, K Wuyts, and W Joosen. 2015. "A descriptive study of Microsoft's threat modeling technique." *Requirements Engineering* 20 (2): 163-180.

Schneier, B. 1999. *Attack Trees.* Schneier. https://www.schneier.com/academic/archives/1999/12/attack_trees.html.

Security, Rewterz Information. 2019. "Outdated OS gets ATMs Hacked within minutes."

Shanghai Diarong Financial Information Services. 2019. "Shanghai Diarong Financial Information Services – $100M." *China Information Services Series F.*

Shevchenko, N, T.A Chick, P O'Riordan, T.P Scanlon, and C Woody. 2018. *THREAT MODELING: A SUMMARY OF AVAILABLE METHODS* . Carnegie Mellon University.

Shostack, A. 2014. "Threat Modeling: Designing for Security."

Shostack, Adam. 2014. *Threat modeling: Designing for security.* John Wiley & Sons.

Simeonova, S. 2016. *Threat Modelling in the Enterprise, Part 2: Understanding the Process: Security Intelligence.* 15 August. https://securityintelligence.com/threat-modeling-in-the-enterprise-part-2-understanding-the-process/ .

Smartsheet. 2019. *Maintain, Protect, and Diminish Risk with a Comprehensive IT Compliance Strategy.* Accessed November 21, 2019. https://www.smartsheet.com/understanding-it-compliance.

Smith, Michael, Chris Welty, and Deborah McGuiness. n.d. "OWL Web Ontology Language."

Statisa. 2019. *Global VC -vs-ICO funding by category Statisa Report 2019.* https://www.statista.com/statistics/863868/vc-vs-ico-funding-by-category/.

Swiler, Laura P., and Cynthia Phillips. 1998. "A graph-based system for network-vulnerability analysis." Tech. rep., Sandia National Labs., Albuquerque, NM (United States).

ThreatModeler. n.d. *Threat Modeling Methodologies: What is VAST?* https://threatmodeler.com/threat-modeling-methodologies-vast/.

—. n.d. *ThreatModeler.* https://threatmodeler.com/.

Torgo, Luis, and Elsa Lopes. 2011. "Utility-based fraud detection." *Twenty-Second International Joint Conference on Artificial Intelligence.*

TREsPASS Project. 2016. *TREsPASS, Picturing Risk.* Egham: Royal Holloway University of London.

UcedaVelez, Tony, and Marco M. Morana. 2015. *Risk centric threat modeling.* Wiley Online Library.

UKEssays.com. 2017. *Push and Pull Factors in Business.* 23 February. Accessed October 21, 2019. https://www.ukessays.com/essays/business-strategy/push-and-pull-factors-in-business.php.

University of Pittsburgh, Internal audit department. 2019. *Audit Process.* Accessed November 21, 2019. https://www.cfo.pitt.edu/intaudit/auditProcess.php.

US 113 Congress, House Sub-Committee Hearing 2014. 2014. *Examining the post-recession small business lending environment.* US Government Publishing Office. https://www.govinfo.gov/content/pkg/CHRG-113hhrg85743/html/CHRG-113hhrg85743.htm.

Velez, Uceda. 2017. *Threat Modeling w/PASTA: Risk Centric Threat Modeling Case Studies.* OWASP.

Veyrat, Pierre. 2019. *Audit Process: Definition, Objectives and Types.* 10 May. Accessed November 21, 2019. https://www.heflo.com/blog/business-management/what-is-an-audit-process/.

W3C Consortium. 2004. *Guide. W3C Recommendation 10 February 2004.* W3C Consortium. http://www.w3.org/TR/2004/REC-owl-guide-20040210/.

—. 2004. *W3C Recommendation.* W3C Consortium. 10 February. http://www.w3.org/TR/2004/REC-rdf-schema-20040210/.

—. 2004. *W3C Recommendation 10 February 2004.* W3C Consortium. http://www.w3.org/TR/2004/REC-owl-features-20040210/.

Wazid, Mohammad, Sherali Zeadally, and Ashok Kumar Das. 2019. "Mobile Banking: Evolution and Threats: Malware Threats and Security Solutions." *IEEE Consumer Electronics Magazine.*

West, Jarrod, and Maumita Bhattacharya. 2016. "Intelligent financial fraud detection: a comprehensive review." *Computers & security* (Elsevier) 57: 47-66.

World Bank Group. 2010. *Serving the Needs of Indonesian SMEs, International Finance Corporation.* Norc (University of Chicago. http://documents.worldbank.org/curated/en/556861495102658074/pdf/115101-WP-ID-SME-Banking-Study-Main-Findings-PUBLIC.pdf.

World Economic Forum. 2016. *A look at how Blockchain can reshape financial services.* Accessed April 2019. http://www3.weforum.org/docs/WEF_The future_of_financial_infrastructure.pdf.

Wuyts, K, D Van Landuyt, A Hovepeyan, and W Joosen. 2018. "Effective and efficient privacy threat modeling through domain refinements." In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 1175-1178.

Yaram, Suresh. 2016. "Machine learning algorithms for document clustering and fraud detection." *2016 International Conference on Data Science and Engineering (ICDSE).* 1-6.

Yousefi-Azar, Mahmood, Vijay Varadharajan, Len Hamey, and Uday Tupakula. 2017. "Autoencoder-based feature learning for cyber security applications." *2017 International joint conference on neural networks (IJCNN).* 3854-3861.