Critical-Chains

Collaborative Project

Project Start Date 1st July 2019 Duration 36 Months

Deliverable D2.2

Technology & Watch Update

Published by the Critical-Chains Consortium

Version 2.0 Date 13-01-2021

Project Coordinator: Professor Atta Badii (University of Reading)

Dissemination Level: Public

Work Package Task: WP2

Document Responsible: JR

Contributors: All Partners

Status: Final

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 D2.2 (Technology & Watch Update) is an update of D2.1 to provide a further analysis of the evolving techniques and advances in FinTech applications. A detailed analysis of the evolutionary history for the financial and insurance sector is given and current technologies are presented. Nowadays, 89% of customers are using mobile phone payment systems and FinTech applications for bank transfers. As for the insurance sector, InsurTech shows strong growth with many customers linking smart devices and buying products such as micro-insurance or peer-to-peer insurance. FinTech and Banks are heavily regulated, with new European directives such as for example the Payment Service Directive 2, several cloud service regulations, Blockchain regulations and artificial intelligence regulations. Moreover, a detailed analysis of the current pull and push factors for FinTech trends are presented. As Critical-Chains aims to improve the cyber security of current solutions, a detailed analysis of the current cyber-attacks on financial infrastructures is presented and analysed. Finally, some insights are given for artificial intelligence and machine learning based algorithms that the consortium of Critical-Chains will use to improve the cyber security of FinTech application, by using anomaly detection, blacklisting and flow modelling.

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

Deliverable D2.2 Document History

Versioning			
Version Number	**Date**	**Contributors' name and organisation**	**Changes**
V0.1	19-08-2020	JR	Initial Draft
V0.2	05-10-2020	JR	Defined new chapters
V0.3	30-11-2020	All partners	Provided new insights and updates for corresponding sections, in relation to last year project work
V1.0	17-12-2020	JR	Merging all updates, end-to-end proofs reading and pre-final review
V2.0	13-01-2021	JR	All reviewers' suggestions and comments are addressed.
V2.0	24-01-2021	UREAD	Review and minor edits as needed

Internal Review History

Internal Reviewers	Date	Comments
ERARGE	11-01-2021	A few minor corrections, including style and references are required.
RINA-C	11-01-2021	Critical-Chains relevance should be emphasized throughout document. A few minor corrections within document are required.

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

Deliverable D2.2 Document History 3

Table of Contents 4

1. Executive Summary 9

2. Introduction 11

2.1. Background 11

2.2. Scope of this Deliverable 11

3. Methodology 13

4. Evolutionary History of Information and Telecommunication Technology (ICT) Support for the Financial and Insurance Sector 14

4.1. Legacy systems in financial infrastructures 14

4.1.1. Mainframes 14

4.1.2. COBOL Software Systems 15

4.1.3. Excel Sheets 15

4.1.4. ATMs running outdated operating systems 15

4.2. FinTech Support for Intra-bank Operation 16

4.3. Front Desk to Back-Office Operations 17

4.4. Financial processes that are supported by ICT technologies 18

4.4.1. Clearing 18

4.4.2. Settlement 19

4.4.3. Loans 19

4.4.4. Self-audit 25

5. Fintech Support for Inter-Bank Operations 27

5.1. Audit & Compliance 28

5.2. Advanced Analytics and Audit – 2020 insights 30

5.3. Blockchain and Audit – 2020 insights 31

6. European Banking Regulatory Mechanisms Evolution and Current Banking Processes Transformation Responsive to European Directives 32

6.1. European Banking Regulatory Mechanisms 32

6.1.1. PSD1 e 2 32

6.1.2. GDPR 34

6.1.3. CRR 35

6.2. Current regulatory picture in Europe and present and future obligations for Banks 36

6.2.1. Payment Services Directive 2 (PSD2) 36

6.2.2. Cloud service regulation in Europe 37

6.2.3. Blockchain Regulation in Europe 37

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

6.2.4. Artificial Intelligence Regulation in Europe 38
7. FinTech Market Push and Pull Forces Responsive to the Regulatory and Market Demands 40
7.1. What are Push and Pull Factors in Business 40
7.1.1. Pull/ Proactive Forces- Attractiveness of the Foreign Markets: 40
7.1.2. Push/ Reactive Forces- Compulsion of the Domestic Market: 41
7.2. Push-Pull Forces in terms of Fintech 41
7.2.1. Blockchain in Fintech 43
7.2.2. Security Aspects of Fintech 43
7.2.3. European Market Demands 43
8. Financial Sector Transformative Responses to Distributed Ledger Technology trends 46
8.1. Definition of DLT 46
8.2. Commercialisation of Blockchain/DLT 47
8.3. Customer Service through Chatbots 47
8.4. The Last Mile in Digitizing Financial Services 47
8.5. Biometric-Based Fraud Prevention 48
8.6. FinTech's and Financial Institutions Playing Cat and Mouse 48
8.7. Benefits from Using DLTs in Financial Sector 48
8.8. Benefits for using DLTs in the Securities market 49
8.8.1. Settlement cycle 49
8.8.2. Near-real-time Operations and Access to the market 49
8.8.3. Automation 49
8.8.4. Compliance and Reporting 50
8.9. Let's stay grounded when talking about financial processes 50
9. FinTech Market Analysis 51
9.1. Changing Consumer Priorities 51
9.2. Rise of non-financial services companies and the growth of ecosystems 53
9.3. SMEs Fintech users 54
9.4. European Market 55
9.5. Technological excursus 57
9.6. SWOT Analysis 59
9.7. Porter's Five Forces Analysis 59
9.8. State-of-the Art in FinTech and Trends 60
9.9. Current Authentication schemes in online banking 64
9.10. Audit & Compliance Technology 65
9.10.1. IT Governance, Risk, and Compliance Management and Software Solutions 65
9.10.2. RegTech 65

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

9.10.1. Audit & Compliance SW Platform – 2020 insights 66
9.11. Use of HSMs and TRNGs in Blockchain- and IoT-enabled Fintech Industry 67
9.11.1. Recent status of HSMs and TRNGs 67
9.11.2. HSMs, TRNGs, CPS and Blockchain 68
9.12. Recent Status of Authentication Schemes in Identity Management 75
10. Cyber-Attacks against Financial Infrastructures 82
10.1. Cyber-attacks against financial infrastructures between 2005 and 2019 82
10.2. Cyber-attacks against financial infrastructures in 2020 83
10.3. Cyber Incidents on Financial Infrastructures 85
10.3.1. EasyJet data breach 85
10.3.2. Capital One data breach 86
10.3.3. Desjardins data breach 86
10.3.4. First American data breach 87
10.3.5. Westpac data breach 88
10.3.6. Bank of Montreal and Simplii Financial data breach 88
10.3.7. Equifax data breach 89
10.3.8. Coast Central Credit Union data breach 90
10.3.9. Scottrade data breach 91
10.3.10. European Central Bank (ECB) data breach 91
10.3.11. JPMorgan Chase data breach 92
10.3.12. Korea Credit Bureau data breach 92
11. AI, Machine Learning Technologies, Blacklisting, Anomaly Detection, Flow Modelling 94
11.1. System decomposition – flow modelling process 95
11.2. Intrusion detection 96
11.3. Related Work 97
12. Ontological Domain State-of-the-Art – 2020 insights 100
12.1. Analysis of the Emerging Needs of the Fintech 100
12.1.1. Stakeholder Gaps 100
12.1.2. Consumer Gaps 102
12.1.3. Fintech Metrics 102
12.2. Cyber-Physical Privacy-Security Ontology Semantic Modelling Framework State-of-the-art 103
12.2.1. Data Representation Model 103
12.2.2. Domain Representation Ontology 104
12.2.3. The Critical-Chains Privacy-Security Protection Data Modelling (Entities, Attributes and Relations) 104
12.2.4. Data Representation Formats 105

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

12.2.5. Overview of Most Common Ontology Development Errors explained by examples 109

13. Privacy and Security Threat Analysis & Modelling Tools & Frameworks State-of-the-Art – 2020 insights 111

13.1. STRIDE 111

13.2. PASTA 112

13.3. LINDDUN 113

13.4. CVSS 114

13.5. Attack Trees 115

13.6. Persona non Grata 115

13.7. Security Cards 116

13.8. hTMM 116

13.9. Quantitative Threat Modelling Method 116

13.10. Trike 117

13.11. VAST Modelling 117

13.12. OCTAVE 117

13.13. TREsPASS 118

13.14. DREAD 119

14. Conclusions 120

References 122

Appendices 130

Appendix 1 – Fintech Cyber Incidents 2013-2019. 130

Appendix 2 – Fintech Cyber Incidents 2020. 132

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 Figures

Figure 1. Example of CPMS Platform 23
Figure 2. EY (2019), "Blockchain use cases in financial sector" 49
Figure 3. EY (2019), “Fintech Adoption Index” 52
Figure 4. EY (2019), "Fintech Adoption Index" 53
Figure 5. EY (2019) "Fintech Adoption Index" 54
Figure 6. EY (2019) "Fintech Adoption Index" 55
Figure 7. EY (2019) "Fintech Adoption Index", Including: banking & payments, Insurtech, proptech, enabling Fintech platforms (es. r3) 56
Figure 8. EY internal Analysis 58
Figure 9. EY internal Analysis 59
Figure 10. EY internal analysis 59
Figure 11. EY internal analysis "Porter's five forces - FinTech considerations" 60
Figure 12. EY (2019) " Fintech Adoption Index " 61
Figure 13. EY (2019) "Fintech Adoption Index" 62
Figure 14. EY (2019) "Fintech Adoption Index" 63
Figure 15. BCG Matrix for HSM and TRNG market 70
Figure 16. U2F standard in FIDO 75
Figure 17. IDMS usage frequency in various fields 77
Figure 18. BCG digital identity survey related to online financial services 77
Figure 19. BCG matrix for authentication schemes in IDMSs 79
Figure 20 The Forrester Wave™: Identity-As-A-Service (IDaaS) For Enterprise, Q2 2019 81
Figure 21. Taxonomy of cyber-attacks against financial infrastructures between 2005 and 2019 82
Figure 22 The countries affected from cyber incidents in Finance domain since 2007 (image: Carnagie Endowment for International Peace) 83
Figure 23 The statistics about high-impact cyber attacks against financial institutions in Jan-Jul-2020 (Ref: Carnagie Endowment for International Peace) 84
Figure 24: Illustrating domain ontology and an example of entity classes relationships 106
Figure 225: 7 stages of PASTA and their sub steps (Velez 2017) 113
Figure 226: LINNDUN methodology and its required system-specific knowledge (Wuyts, et al. 2019) 114
Figure 227: CVSS Metric Groups (FiRST n.d.) 114
Figure 228: An Attack tree with the goal of opening a safe. Showing costs and denoting the feasibility of each way of achieving the goal (Schneier 1999) 115
Figure 29: Security card topics and activities (Shevchenko, et al. 2018) 116
Figure 30: The 3 OCTAVE Phases (Mayer 2009) 118
Figure 31: An example of an Attack Cloud (TREsPASS Project 2016) 118
Figure 32: Table showing DREAD rating for two threats (INFOSEC 2014) 119

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 D2.2 (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 FinTech applications and distributed ledger technologies. Moreover, it gives insights into the evolving techniques and advances in technology within the financial domain. It is an update of D2.1, covering additional aspects that arise from project work, and SoA, SoM and SoP updates over the past year (2020). This deliverable provides new insights in 11 chapters covering topics of interest identified in D2.1, and two additional chapters covering newly identified topics of interest in Critical-Chains – Ontological Domain State-of-the-Art and Privacy and Security Threat Analysis & Modelling Tools & Frameworks State-of-the-Art.

The deliverable is split into 15 chapters as outlined in the following:

Chapter 2 gives insights into background of presented work and scope of this deliverable.

Chapter 3 provides a brief explanation of methodology used for the work presented in this deliverable.

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

- 2020 update: This chapter includes additional analysis of legacy systems in financial infrastructures.

Chapter 5 provides technology trends for FinTech support for Inter-Bank operations, and determines audit and compliance procedures.

- 2020 update: This chapter includes updates according to insights during 2020 year, including advanced analytics and audit, and blockchain and audit.

Chapter 6 focuses on the European Banking Regulatory Mechanisms Evolution and 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.

- 2020 update: This chapter includes new insights originating from project work during 2020 year, especially considering PSD and GDPR.

Chapter 7 provides information on the Pull and Push forces in the FinTech Market responsive for the regulatory and Market Demands.

- 2020 update: This chapter includes new insights in Fintech push-pull forces in 2020, especially considering COVID-19 situation.

Chapter 8 gives information about the transformative responses to Distributed Ledger Technology trends within the financial sector.

Chapter 9 covers Fintech market analysis, including various aspects like consumer priorities, European market, SWOT and Porter's five forces analysis, authentication schemes, audit & compliance technology, use of TRNGs and HSMs in Fintech, etc.

- 2020 update: This chapter includes new insights in Fintech market analysis in 2020; special focus is on authentication schemes in online banking and audit & compliance technology; new insights include also update on latest TRNGs and HSMs in the market and the rise of Identity-as-a-Service (IDaaS).

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

Chapter 10 gives details about the cyber security issues and cyber-attacks against financial infrastructures. It lists and analyses the most critical attacks on financial infrastructures.

- 2020 update: This chapter includes an update on recent cyber incidents in Fintech in 2020, including general cybersecurity statistics and COVID19 related statistics, and the details of the EasyJet2020 cyberattack.

Chapter 11 provides information about current technology trends in Artificial Intelligence, Machine Learning Technologies, Blacklisting, Anomaly Detection, and Flow modelling.

- 2020 update: This chapter includes an update on related work within this field, including additional methods categorisation.

Chapter 12 provides an ontological domain analysis and state-of-the-art of cyber-physical privacy-security ontology semantic modelling framework.

- 2020 update: This chapter is added to D2.2 presenting the additional insights obtained during project work in the last year.

Chapter 13 provides the state-of-the-art of privacy and security threat analysis & modelling tools & frameworks.

- 2020 update: this chapter is added to D2.2 presenting the additional insights obtained during project work in the last year.

Chapter 14 concludes this deliverable.

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

2. Introduction

This document, D2.2, is an update of D2.1 – Technology & Watch Update, covering additional aspects that arise from project work, and SoA, SoM and SoP updates from the year 2020. This deliverable provides new insights in 11 chapters covering topics of interest identified in D2.1, and two additional chapters covering newly identified topics of interest in Critical-Chains – Ontological Domain State-of-the-Art and Privacy and Security Threat Analysis & Modelling Tools & Frameworks State-of-the-Art.

New insights are linked with project work in the last year and current COVID-19 situation and its influence on cyber-security in Fintech domain. New tables are added at the beginning of every chapter as the introduction of the chapter, explaining relevance of selected topic to Critical-Chains project, and providing a brief overview of the 2020-updates provided in that chapter.

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.

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.

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.

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.

2.2. Scope of this Deliverable

The scope of this deliverable is to specify evolving techniques and advances in the State-of-the-Art (SoA), State-of-the-Market (SoM) and the outputs of other emerging projects (H2020, international and national). Critical-

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

Chains is closely following the UI-REF methodology that defines to filter the requirements by applicable pull and push factors. These consists of user/practitioner/market-initiated as well as technology-initiated factors that influence the State-of-the-Market (SoM), State-of-the-Art (SoA) and State-of-the-practice (SoP).

This deliverable provides insights into the latest updates on the relevant products that are available in the market; it highlights the relevant gaps in the market that offer synergies with the offered functionalities that will be provided within the Critical-Chains Framework. Additionally, it provides an overview of the regulatory mechanisms and gives an overview of recent attacks on financial infrastructures.

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

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). In the scope of this deliverable, the UI-REF methodology suggests a market-technology-watch task to keep up with the market and technology evolution. The overall aim of this task (and therefore of this document), is to report any filtering/modification suggestions, that need to be integrated during iterations of a prototype. Hence, it should provide the required update of the re-engineered requirements and refinements between the prototype and the prototype of the next iteration.

While this deliverable provides an update of the State-of-the-Market (SoM), that keeps track of the recent developments and trends in the FinTech industry, it also defines the relationships between the technologies of the State-of-the-Art (SoA) and the proposed technologies within the Critical-Chains framework. Therefore, these influential pull & push factors can be seen as additional requirements to the Critical-Chains framework, to keep up to date with recent developments. Moreover, as the financial sector is highly regulated, this deliverable furthermore lists the relevant European banking regulations, such as PSD2, GDPR and CRR. Additional requirements arise, to be compliant to these regulations.

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

Intro

This section describes evolutionary history of legacy systems in financial infrastructures, ICT and Fintech support for intra-bank, front-desk and back-office operations, and details of financial processes that are supported by ICT technologies.

Critical-Chains relevance

Critical-Chains platform will implement the financial process described in this chapter.

2020 update

This chapter includes additional analysis of legacy systems in financial infrastructures.

4.1. Legacy systems in financial infrastructures

All products and services offered by financial institutions are usually backed by technology. Different transactions, including simple bank transactions or ATM withdrawals, require the interconnection and interaction between various different components. The reason for this lies in the fact that financial infrastructures are complex systems that have often been built on monolithic architectures (Lhuer, et al. 2019). One of obstacles that hold back innovation efforts and cripple the agility of financial institutions are legacy core banking systems at the heart of financial infrastructures. Technology used in such a systems, sometimes dates back more than 50 years, where the complexity of those systems makes it impossible to manage risks (Pogson 2019).

The main challenges with these monolithic architectures most commonly lies in the fact that customer-facing services and applications must evolve rapidly, while at the same time they have data dependencies on core banking systems running on outdated technology standards. The example of that are mobile apps, analytics based on machine learning, open banking, while the backend systems of current banks heavily rely on legacy systems such as mainframes from the 1980s, COBOL based software systems from the 1960s, excel, batch systems and ATMs with Windows XP.

This section provides an overview of the main legacy components used in the backend of financial institutions, including core banking components. These systems include **mainframes**, **software systems based on COBOL** and **Excel Sheets**. In addition to that a brief description of customer-facing components such as **ATMs running outdated operating systems** is also provided.

4.1.1. Mainframes

Mainframes are computer systems used for critical applications, usually in large organisations. They can be compared to supercomputers – optimised for high performance computing, and designed to ensure high reliability, security, high throughput and the ability for hot-swapping of hardware and offloading to separate computer systems.

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 a financial domain, mainframes are built to be reliable for various transaction processing. The main advantages of mainframes are *reliability* – they are robust against errors, *availability* around the clock, *security* – they have built in cryptographic hardware acceleration and secure operating systems, very high *analytical speed* and *high throughput* – large number of transactions.

Although mainframes evolved with time, they often do not fit the nowadays needs of bank customers anymore. Nowadays the banks are processing huge amounts of data. Open banking also needs to provide APIs to core banking functions. The solutions that are better suited for those requirements are cloud-based solutions that work as Software-as-a-Service and microservices (Kashyap, et al. 2017). Mainframes in this context are not flexible enough, they are expensive and out of date to cope with quickly changing requirements.

4.1.2. COBOL Software Systems

Common business-oriented language (COBOL), originated in the 1960s, is a computer programming language designed for business use. In the finance domain, COBOL is widely used in legacy applications that are deployed on mainframes. It is most commonly used for batch and transaction processing.

A recent study by Reuters (Mitchell, Cobol: Not Dead Yet 2017) showed that a significant share of major US banking systems still use COBOL - 43% of banking systems were built in COBOL, 80% of all in-person transactions used COBOL, and 95% of all ATM swipe transactions rely on COBOL. The same study claims that until these days there are still more than 220 billion lines of COBOL in use during the use of every day financial services.

There are numerous reasons why COBOL is considered outdated. COBOL programs are infamous for being monolithic and lack modularisation. It was also impossible to restrict access to data in older versions, so any procedure could modify any data item. Furthermore there were also compatibility issues, leading to many dialects that have been created. Moreover, an issue worth mentioning is that this programming language is not offered at universities anymore and there is a lack of available developers with this proficiency.

Required software stack is constantly adapting and evolving with new technologies. Programming languages are often designed directly for these new technologies and architectures, and COBOL simply cannot cope with this rapid growth and changing of technologies. The most of programming in COBOL nowadays is purely done to maintain existing applications (Mitchell, Cobol: Not Dead Yet 2006).

4.1.3. Excel Sheets

Another legacy tool that is widely used in the finance domain is Excel, or huge Excel sheets. Those Excel sheets are used for accounting and financial services, and Excel is also used as an analytical tool in this sector.

However, Excel is prone to various security issues, including manipulation. It is also error-prone due to manual data entry and manipulation, and formula errors that provide scope for perpetrators with criminal intent. Another important issue is the inability to trace the data user identity and the lack of audit trails. All these issues make Excel a risky and manipulative tool.

4.1.4. ATMs running outdated operating systems

Automated Teller Machines (ATM) are widely used all over the world to dispense cash. An ATM consists of two main parts, a cabinet that contains the ATM computer, and a safe that contains the money. The computer usually runs an embedded version of Windows, and up until 2014 the vast majority of ATM machines, almost 95%, were running Windows XP (Goldsmith 2014). While Microsoft stopped support for Windows XP in 2014, still in 2020 there are numerous ATMs still running on this legacy operating system. This opens a plenty of security holes within ATMs (Security 2019), as there is no continuous support, and vulnerability patching. The reason why ATMs have not updated their operating systems vary from huge operational costs, considering the number of ATMs in use, but also a lack of alternatives as newer versions of Windows also do not offer long-term support.

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

4.2. FinTech Support for Intra-bank Operation

The term "FinTech" 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 Fintech deals (FINCH CAPITAL 2019).

While the term "FinTech" 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 globalisation 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. However, greater use of telegraph or telephone facilities also resulted in both internal and public price related information becoming homogeneous.

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 FinTech 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 organisation 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 generalised, structured and integrated body of data that could be read and updated in a controlled, efficient, and reliable way.

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.

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 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. tokenisation 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, impacting also 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 FinTech 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 FinTech industry, that offers advantages such as economies of scale, flexibility, operational efficiencies and cost effectiveness (FSB – Financial Stability Board 2019). Cloud technology is characterised 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.

4.3. 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 organised into front, middle and back offices, each of which perform different tasks (Retail Banking Academy 2014):

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 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 task 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.

4.4. Financial processes that are supported by ICT technologies

4.4.1. 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.

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 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.

4.4.2. 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 2020).

4.4.3. 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 standardised);
- 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 securitisation 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).

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

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 specialised version of new account opening for financial services organisations, with certain people and organisations getting increasingly specialised in loan origination (e.g. mortgage brokers).

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 summarised 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 more risky). 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

Once the loan for the bank is disbursed it is difficult to know if the borrower have had, or has, opportunistic behaviours (ex. finance a project more risky 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

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

costs associated with the transaction; Management and monitoring (i.e. control and periodic review of relationships);
- Portfolio management

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 securitisation 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 from:

- 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 realised for the contractors, among which the most important are the stabilisation 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 organisational structure of the bank, and to the characteristics of the credit demand expressed by the markets in which the bank operates.

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

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

  - 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 characterised 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

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 (Business Process Modelling) standards, allowing configuration of both processes as well as all the credit product parameters.

This kind of system are based upon a SOA (Service Oriented Architecture) 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 (Customer Relationship Management) 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.

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

Big player, such us traditional big banks, which are slowly approaching to the FinTech 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 FinTech services providers, is already estimated to be around 267 Million US Dollars.

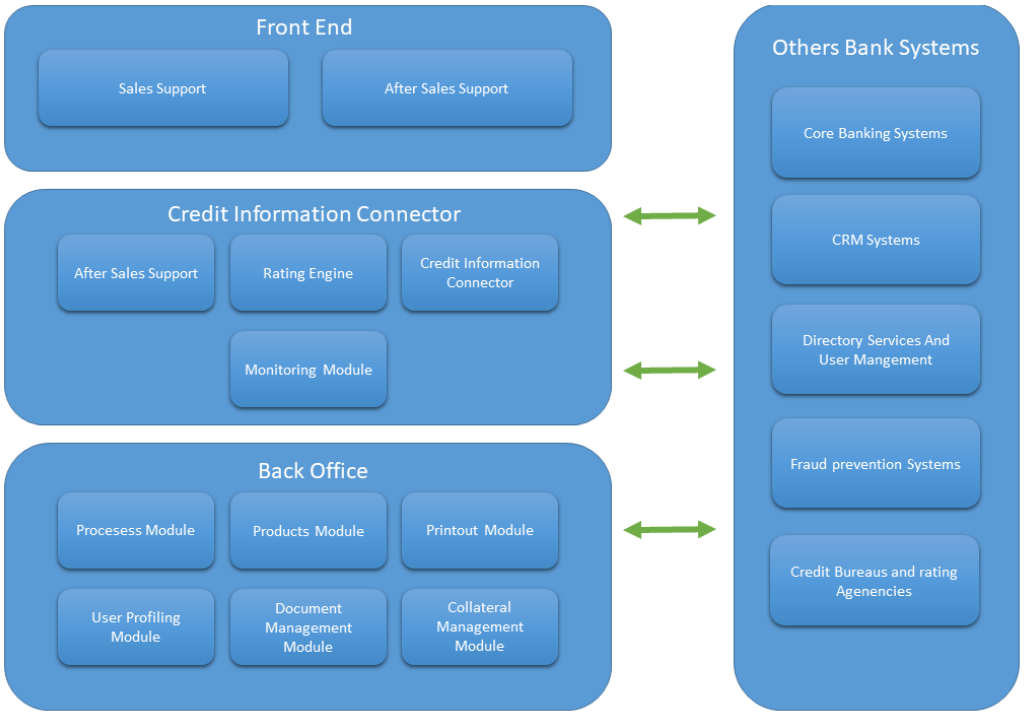

Figure 1. Example of CPMS Platform

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 digitalised 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

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

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 customised by each client. Customisation 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 exist 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, decision making, credit analysis, and approvals.

The strong points of CLS are the fact that it's 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 decision making 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's 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's functionality are: lending campaign creation and management, loan application collection, review, decision making 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 customisation, 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

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

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's 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.

4.4.4. 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

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

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 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 organisation, 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 needs 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 2020):

- 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. Fintech Support for Inter-Bank Operations

Intro

This chapter describes Fintech support for inter-bank operations, including audit & compliance, especially considering advanced analytics and blockchain.

Critical-Chains relevance

This chapter defines guidelines for the Blockchain-as-a-Service Critical-Chains building block to support Audit activities in interbank operations.

2020 update

This chapter includes updates according to insights during 2020 year, including advanced analytics and audit, and blockchain and audit.

New technologies and business models make it possible for auditors to analyse large amounts of a company's financial data and test 100% of a 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

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

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 organisations should use in order to reach a continuously productivity improvement in their organisation. The definition is:

A set of actions and procedures to control an organisation. 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.

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 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 finalised. 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 organisations 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 organisation'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 of 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):

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

- **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.

5.2. Advanced Analytics and Audit – 2020 insights

There is a double type of relation between audit and advanced data analytics: audit can control advanced analytics algorithms and data analytics can enhance audit performance. This relation has been addressed by European Banking Authority (EBA) [1] and KPMG[2] in two reports. In particular, EBA decided to pursue a 'deep dive' review on the use of big data and Advanced Analytics (BD&AA) in the banking sector. The report focuses on BD&AA techniques and tools, such as machine learning (ML), that go beyond traditional business intelligence to gain deeper insights, make predictions or generate recommendations using various types of data from various sources. EBA highlights that ML is certainly one of the most prominent AI technologies at the moment, often used in advanced analytics due to its ability to deliver enhanced predictive capabilities. A key constraint for the integration of BD&AA into existing business processes is the introduction of trust elements such as **traceability and auditability** i.e. the use of traceable solutions that assists in tracking all the steps, criteria and choices throughout the process, which enables the repetition of the processes resulting in the decisions made by the ML model and helps to ensure the auditability of the system. In fact all the steps and choices made throughout the entire data analytics process need to be clear, transparent and traceable to enable its oversight. In addition, it is important to track and document carefully the criteria followed when using the model in a way that is easily understood (e.g. including a clear indication of when a model should be retired), the alternatives (e.g. model choices) and all the relevant information on each step throughout the process.

Moreover, institutions could keep a register of the evolution of the models. Having all the versions of a model registered enables an institution to compare different models or perform a roll-back if necessary. The steps involved in a decision made by a model can be tracked from data gathering (including from third-party data sources) to the moment when the decision is made and even beyond, as, when a model is retired, institutions could still be able to explain how its results were produced and why its decisions were made. To enable the repetition of the process by which a decision was made, the correct version of the model and data could be used. Sometimes, the model and data will need be recovered from repositories with previous versions of models and data. Some institutions leverage an integrated platform to ensure the traceability of all the phases of a data science development process. These platforms usually include versioning features to keep track of the evolution of the model. A traceable solution, for which there are detailed audit logs for all phases of the process that can be used to identify 'who did what, when and why', facilitates oversight of the system, as it makes it possible to follow the whole process and gain better insights. KPMG highlights that for financial services organisations, the need of robust assurance processes has never been clearer. Over the past decade, vast amounts of new regulations have been handed down to financial services organisations of all types, demanding massive amounts of data across a wide range of operational areas. But the challenge is not necessarily the volume of data that is

[1] EBA Report on Big data and Advanced Analytics January 2020 EBA/REP/2020/01
[2] Financial Services, Data, Analytics and audit Getting ready for the era of data driven audit, KPMG

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

required but rather the quality of the data. Financial services organisations know the power of Data and Analytics (D&A). Many investment management houses either use or rely on sophisticated D&A algorithms for automated trading. Internal auditors also know the power of D&A. Indeed, at its simplest, audit is all about collecting massive amounts of data and correlating it against other internal and external sources to uncover new insights about the business. The introduction of modern D&A tools and approaches takes the audit to the next level. At the same time, the potential sources of data available for external audit have evolved dramatically. Today, huge pools of external data are being aggregated and companies are able to access it, providing auditors with an unprecedented ability to benchmark internal data against external sources.

5.3. Blockchain and Audit – 2020 insights

Blockchain (Liu, Wu and Xu 2019)offers a drastically new way to record, process, and store financial transactions and information, and has the potential to fundamentally change the landscape of the accounting profession and reshape the business ecosystem. At the application level, blockchain brings new business to auditors, such as reviewing certain transactions and verifying the existence of digital assets, and attesting to consistency between information on a blockchain and in the physical world. These new tasks could be challenging, particularly when there are no centralised authorities on the blockchain. Auditors need to leverage their expertise in IT system audits to invent novel methods to accomplish verification of ownership. As a complete record of transactions is stored on a blockchain, auditors will no longer need to request, and wait for trading parties to provide, data and documents. In addition, blockchain will surpass the traditional audit sampling process, and allow continuous audits for any ‘‘on-chain’’ transactions in any specific period. The adoption of blockchain will free up resources that were previously expended on evidence collection and verification. To prepare for the changes brought by this disruptive technology, auditing professionals should consider the following initial steps to adapt to the new environment:

- Acquire competency in blockchain technology and governance of blockchain. Auditors should be able to assess the costs and benefits of adopting specific blockchains, and provide advice on blockchain implementation for their clients. Audit firms could reach this goal by adjusting their hiring and training strategy.
- Actively participate in blockchain development with emphasis on risk control. Auditors should consider stepping forward to influence and lead implementation of blockchain. Audit firms should shift their focus to assess the effectiveness of risk management and advice on solutions and assurance for internal control. Rapidly growing technology brings enormous opportunities to auditors. In order to promote high-quality services, auditors should consider the following long-run prospects:
- Move to continuous auditing. Blockchain applications make it feasible to conduct continuous auditing due to real-time access to transaction records.
- Grow the advisory function. With resources freed from traditional evidence collecting and testing, audit firms should consider applying appropriate data analytics in blockchain, and expand advisory services such as control design, change management, and blockchain governance.

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

6. European Banking Regulatory Mechanisms Evolution and Current Banking Processes Transformation Responsive to European Directives

Intro

This chapter describes European regulatory mechanisms evolution, including PSD, GDPR and CRR, and current banking processes transformation responsive to European directives, including PSD2, cloud service, blockchain and artificial intelligence regulation.

Critical-Chains relevance

Within Critical-Chains project the compliance analysis will be carried out to verity that the Critical-Chains Platform satisfies the regulation described in this chapter.

2020 update

This chapter includes new insights originating from project work during 2020 year, especially considering PSD and GDPR.

6.1. European Banking Regulatory Mechanisms

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 (European Parliament 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).

6.1.1. 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

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

made available by authorised 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 authorised third parties. It is a set of formalised 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.

2020 Insights

PSD2 has enabled the emergence of new business models based on the sharing of payment account data (‘Open Banking'), such as payment initiation and account information services. It has also improved the general level of the security of payment transactions through the implementation of strong customer authentication. It is a worldwide reference for open banking and secure transactions. The experience gathered from the full implementation of PSD2 will inform the Commission's work on a broader framework for open finance, as set out in the Digital Finance Strategy.

The European Commission adopted on 24 September 2020 a digital finance package, including a digital finance strategy and legislative proposals on crypto-assets and digital resilience, for a competitive EU financial sector that gives consumers access to innovative financial products, while ensuring consumer protection and financial stability. The digital finance strategy sets out general lines on how European can support the digital transformation on finance in the coming years, while regulating its risks. The strategy sets out four main priorities: i) removing fragmentation in the Digital Single Market, ii) adapting the EU regulatory framework to facilitate digital innovation, iii) promoting a data-driven finance, and iv) addressing the challenges and risks with digital transformation, including enhancing the digital operational resilience of the financial system.

The Commission proposes a framework on crypto-assets to allow for innovation in a way that preserves financial stability and protects investors. The overall objective of the initiative is to provide clarity as regards the applicability of the EU financial regulation to crypto-assets (and related activities). The initiative should support innovation and fair competition by creating a framework for the issuance, and provision of services related to crypto-assets. It should ensure a high level of consumer and investor protection and market integrity in the crypto-asset markets. It should address financial stability and monetary policy risks that could arise from a wide use of crypto-assets and DLT-based solutions in financial markets. Crypto-assets are digital representations of values or rights, which are transferred and stored electronically Crypto-assets are inextricably linked to blockchains, as they are the blocks that make up the chains themselves. Crypto-assets come in many forms and with varying rights and functions. A crypto-asset can serve as an access key to a service (often referred to as “utility tokens”), can be designed to facilitate payments (often referred to as “payments tokens”) but can also be designed as financial instruments, such as transferable securities under the Markets in Financial Instruments Directive (MiFID II). The Commission differentiates between those crypto-assets already governed by EU legislation, and other crypto-assets. The former will remain subject to existing legislation but the Commission proposes a pilot regime for market infrastructures that wish to try to trade and settle transactions in financial instruments in crypto-asset form. This should enable market participants and regulators to gain experience with the use of DLTs exchanges that would trade or record shares or bonds on the digital ledger. For previously unregulated crypto-assets, including ‘stablecoins’, the Commission proposes a bespoke regime. The proposed

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

regulation sets strict requirements for issuers of crypto-assets in Europe and crypto-asset service providers wishing to apply for an authorisation to provide their services in the single market. Safeguards include capital requirements, custody of assets, a mandatory complaint holder procedure available to investors, and rights of the investor against the issuer. Issuers of significant asset-backed crypto-assets would be subject to more stringent capital requirements, liquidity management and interoperability requirements.

6.1.2. 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. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Personal data is any information relation to an identified or identifiable natural person. 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. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Personal Data is any information relating to an identified or identifiable natural person. The GDPR applies to all organisations, 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 and in relation to extraterritorial scope, the GDPR applies to organisations that are not established in the EU, but monitor the behaviour of individuals, as far their behaviour takes place in the EU. The GDPR provides that it should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data or which monitor the behaviour of EU citizens residing in the EU. This regulation is relevant at the banking level because it regulates large mass of data with a high content of sensitive data, which all banks and FinTech companies store and then extrapolate drawing economic benefits such as customer profiling (Famularo and Magazine 2018).

2020 Insights

The GDPR makes a substantial changes relating to processing of personal data. GDPR recognizes accountability as a fundamental privacy principle, states that the controller shall be responsible and able to demonstrate compliance with data protection laws. Also, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Data protection by design takes into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing the personal data. Data protection by default ensuring that only personal data which are necessary for each specific purpose of the processing are processed. The aim is to limit the use of personal data or at last make conditions of use as transparent as possible. The GDPR separates responsibilities and duties of data controllers and processors, obligating controllers to engage only those processors that provide “sufficient guarantees to implement appropriate technical and organisational measures” to meet the GDPR’s requirements and protect data subjects’ rights. Processors must also take all measures required by Article 32, which delineates the GDPR’s “security of processing” standards. Under Article 32, similarly to the Directive’s Article 17, controllers and processors are required to “implement appropriate

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

technical and organisational measures" taking into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons." Unlike the Directive, however, the GDPR provides specific suggestions for what kinds of security actions might be considered "appropriate to the risk.

Unlike the Directive, which was silent on the issue of data breach, the GDPR contains a definition of "personal data breach," and notification requirements to both the supervisory authority and affected data subjects. Under the GDPR, a "personal data breach" is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. In the event of a personal data breach, data controllers must notify the supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of it".

The GDPR introduce the concept of Data Protection Impact Assessment (DPIA), i.e. the assessment of the risk that the processing could involve on the freedoms and rights of data subjects. DPIA is a processes designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms to the rights and freedoms of natural person resulting from the processing of personal data by assessing them and determining the measure to address them. , as well as the new figure of the Data Protection Officer (DPO).

Also the GDPR introduce the new figure of the Data Protection, 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, 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.

The GDPR provides for two different levels of administrative penalties. The fines imposed by the GDPR are flexible and scale with the firm. Any organisation that is not GDPR compliant, faces a significant liability. Some violations to fines up to 10,000,000 EUR or up to two percent of global annual turnover, while for violations, those maximums are doubled to 20,000,000 EUR or 4 percent of global turnover of the rules around consent generally subject controllers to the higher level of fines of the rules concerning age of consent are subject to the lower level of penalties. The GDPR is stiff fines are aimed at ensuring the best practices for data security.

6.1.3. 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 (Blue Ocean Finance 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 more risky the assets are, the higher 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

amount of capital 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 (European Parliament 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 Bank 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.

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

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.

6.2.1. 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 require 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.

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

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.

6.2.2. 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) FinTech 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 localisation 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.

6.2.3. Blockchain Regulation in Europe

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

- **The European Commission (EC) FinTech 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. It is important to underline that

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

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, are realised 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.

6.2.4. 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 remains 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

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

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

7. FinTech Market Push and Pull Forces Responsive to the Regulatory and Market Demands

Intro

This chapter describes push and pull factors in business in general, and in more detail push-pull forces in Fintech.

Critical-Chains relevance

Analysis presented in this chapter is taken into account in Critical-Chains in producing different strategies and performance goals of project results exploitation.

2020 update

This chapter includes new insights in Fintech push-pull forces in 2020. In conclusion, the world is faced with COVID-19. Although COVID-19 dropped the deals over 2020, the virus created new opportunities across Europe. Companies almost doubled their investment in Fintech services since customer behaviours and points of view positively shifted to digital banking. Over the long term, the impact of the pandemic could be beneficial over the digital change amongst corporates.

7.1. 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 internationalisation 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 (UK Essays 2017).

7.1.1. 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

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

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 globalisation. 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 globalisation. The free trade regime, business across the globe has grown considerably. Goods, services, capital, and technology are moving across the nations significantly (Kirkwood 2009).

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

- **Saturation of domestic demand:** The market for the number of products tends to saturate or decline in the advanced countries. This often happens when the market potential has been almost fully tapped. For example, the fall in the birth rate implies a contraction of market for several baby products. Businesses undertake international operations in order to expand sales, acquire resources from foreign countries, or diversify their activities to discover lucrative opportunities in other countries.
- **Scale economies and technological revolution:** Economies of scale are reductions in unit production costs resulting from large-scale operations. The technological advances have increased the size of the optimum scale of operation substantially in many industries making it necessary to- have the foreign market, in addition to the domestic market, to take advantage of scale economies.
- **Technological revolution:** Revolution is the right word that can best describe the pace at which technology has changed in the recent past and is continuing to change. Significant developments are being witnessed in communication, transportation and information processing, including the emergence of the internet and the World Wide Web.
- **Domestic recession:** Domestic recession often provokes companies to explore foreign markets. One of the factors, which prompted the Hindustan Machine Ltd. (HMT) to take up exports very seriously, was the recession in the home market in the late 1960s.
- **Competition as a driving force:** Competition may become a driving force behind internationalisation. There might be intense competition in the home market but little in certain foreign countries. A protected market does not normally motivate companies to seek business outside the home market.
- **Government policies and regulations:** Government policies and regulations may also motivate internationalisation. There are both positive and negative factors that could cause internationalisation. Many governments offer the number of incentives and other positive support to domestic companies to export and to invest in foreign investment.
- **Improving the image of the companies:** International business has certain spin-offs too. It may help the company to improve its domestic business; international business helps to improve the image of the company. There may be the 'white-skin' advantage associated with exporting- when domestic consumers get to know that the company is selling a significant portion of the production abroad, they will be more inclined to buy from such a company.
- **Strategic vision:** The systematic and growing internationalisation of many companies is essentially a part of their business policy or strategic management. The stimulus for internationalisation comes from the urge to grow, the need to become more competitive, the need to diversify and to gain strategic advantages of internationalisation (Kirkwood 2009).

7.2. Push-Pull Forces in terms of Fintech

After a record-setting 2018, the first half of 2019 got off to a quiet start for FinTech investment globally which mirroring a trend seen in the broader VC (Venture Capital) market. The steep drop-off in investment reflected

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 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. Fintech 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, FinTech investment got off to a very strong start in Europe. While well off the pace required to match 2018's massive investment record, FinTech investment in the Americas was also very good during H1'19 (Pollari and Ruddenklau, The Pulse of Fintech 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 FinTech investors across most jurisdictions, H1'19 also saw the continued maturation of the FinTech industry as a whole and the broadening of its definition. Areas like wealth tech, PropTech, and RegTech also grew on the radar of investors (Pollari and Ruddenklau, The Pulse of Fintech 2019).

InsurTech continues to attract large funding rounds and had a banner year in 2018 in terms of funding, with 14 InsurTech 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. InsurTech 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, The Pulse of Fintech 2019).

Digital banking FinTech 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, The Pulse of Fintech 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, The Pulse of Fintech 2019).

2020 insights

In 2020 the world is faced with a pandemic issue because of a virus called Covid-19. This virus has made a lot of changes to every sector, especially to technology-based sectors. Almost every company has shifted to work-home policies. Within this mind, It is undeniable that COVID-19 has an impact on the Fintech deal activity in H1'20 as well. However, new deals activities ground almost to a halt with many of the completed deals in H1'20. Although the world faces a pandemic issue, H1'20 highlights that Fintech trends are unaffected. During H1'20 a number of governments decided to push their Fintech plans forward. The UK announced a review plan according to how governments can support Fintech growth (Nicole 2020). In March, Australia re-opened Select Committee on Financial Technology and Regulatory Technology to clarify how Covid-19 has affected the sector (Australia 2020). In the meantime, Hong Kong SAR and Singapore introduced a licensing program for Digital Asset Exchanges and platforms.

Remarkable tech and platform providers such as Gojek which its digital payment services raised $3 billion in H1'20 from investors including Google. During the time, Tencent, Facebook, and Paypal also made their Fintech

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

investments (PYMNTS 2020). Due to the COVID-19 popularity of digital platforms, digital banking, and no-touch payments, and other Fintech services has been remarkably increased. Therefore, in almost every region of the world, many financial service companies have doubled down their Fintech investments. Nevertheless, COVID-19 will likely remain an active factor for Fintech investments heading into H2'20. In the meantime, Regtech companies will focus on credit-related solutions while data analytics for financial services will focus on cybersecurity, fraud prevention, and digital identity management.

7.2.1. Blockchain in Fintech

Last year FinTech 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's 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).

2020 insights

Along the H1'20 blockchain proceed to shift homogenous approach toward a focus on bringing partners to develop sector-specific, integrated use cases. Complexity of supply chain, lack of trust from customers to blockchain, and the increasing availability of data, blockchain will focus on the enablement in the upcoming quarters. Heading into H2'20 VC investments in the blockchain and cryptocurrency fell during the H1'20 because of the COVID-19. Looking forward to H2'20, COVID-19 has helped governments to focus on digital currencies. It is expected to see common data taxonomies or common languages to support Blockchain along with 2020. (Pollari ve Ruddenklau, The Pulse of Fintech 2019)

7.2.2. Security Aspects of Fintech

Analyses in FinTech intersection with other key arenas have produced intriguing insights, particularly the overlap between FinTech 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 FinTech 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 FinTech sector.

2020 insights

In H1'20 there was a focus on privacy and consumer fraud prevention. Along with the rapid rise in remote access to online services, it is expected that the investment in Security subjects such as password-less technologies, biometrics, and behaviour monitoring solutions will increase. In the upcoming months, cybersecurity is expected to be a popular area of investment such as cloud security and governance. Apart from cloud security and governance areas access and identity management will also constitute big priorities given the increasing focus on fraud prevention and detection. (Pollari ve Ruddenklau, The Pulse of Fintech 2019)

7.2.3. European Market Demands

While overall FinTech investment in Europe dropped in H1'19 Strength of the UK's FinTech sector provides resilience. Despite ongoing concerns related to Brexit and a government leadership election, the UK continued to attract a significant amount of FinTech funding during H1'19. UK-based firms accounted for six of the top ten FinTech deals in Europe at mid-year, including an $800 million investment by the SoftBank Vision Fund into

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

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 FinTech in Europe (Shanghai Diarong Financial Information Services 2019).

On the other side European challenger banks targeting global growth and the FinTech 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, The Pulse of Fintech 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 FinTech companies that are emerging as category leaders.

2020 insights

COVID-19 has been a major factor for Fintech across Europe. New entrepreneurs and start-ups are facing challenges given the typical avenues. Europe investment down in H1'20. However, the pandemic has created new opportunities due to it is effect on digital behaviours. Demand for digital tools, products, and services increased during the COVID-19. Those who able to respond quickly to customer demands in terms of digital tools, products, and services saw strong growth. During H1'20 European Commission held a new digital finance strategy and Fintech action plan over the next 5 years (European Commission 2020). Traditional banks began to shift the digital banking point o view and started to invest in Fintech to grow and enter new markets.

France's Fintech gained attractiveness in Europe with government support. France remained strong in H1'20 due to the COVID-19 although the deals activities dropped. Challenger business bank Qonto raised $115 million Series C funding round led by Tencent and DST Global but the big banks are also becoming more focused on this next generation of Banks (Societe Generale acquired freelance challenger bank Shine). The French government has identified Fintech as a key industry to support the economic stimulus plan and the state will continue to invest companies for Fintech about €1, 2 billion (Pollari ve Ruddenklau, Pulse of Fintech H1 2020 2020).

Apart from France, Germany is also resilient overall in H1'20, led by US$570 million by N26, a US$73 million raised by the Trade Republic, and a US$65 million raise by Solarisbank. COVID-19 led companies to shift digital banking services as people also changed their point of view to digital banking as a positive driver. As an outcome, these shifts could help Fintech to improve profitability.

The UK saw the amount of Fintech funding in H1'20 with US$100 million deals which comprise Revolut,Checkout.com, Starling Bank, and Currency Cloud. Since the UK government has support on Fintech services, corporate investment is expected to become more focussed on the market due to COVID-19. In addition to the UK, H1'20 was alive for Ireland too. Ireland continued to gain transaction from UK-based Fintech companies such as Starling Bank and Revolut looking to create a Brexit-Hedge until January 2021. Ireland is expected to remain alive into H2'20 as the UK and global Fintech work to ensure they provide their customers across Europe (Pollari ve Ruddenklau, Pulse of Fintech H1 2020 2020).

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 conclusion, the world is faced with COVID-19. Although COVID-19 dropped the deals over 2020, the virus created new opportunities across Europe. Companies almost doubled their investment in Fintech services since customer behaviours and points of view positively shifted to digital banking. Over the long term, the impact of the pandemic could be beneficial over the digital change amongst corporates.

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. Financial Sector Transformative Responses to Distributed Ledger Technology trends

Intro

This chapter describes financial sector transformative responses to distributed ledger technology trends, including different business and technical aspects.

Critical-Chains relevance

Analysis presented in this chapter is taken into account in Critical-Chains in producing deployment and exploitation strategies.

8.1. 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 in 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 authorised to take up certain roles. For instance, a ledger could restrict the validators to a predefined set of authorised nodes but let any node to locally verify the correctness of the ledger.

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

Smart Contracts bring ground-breaking innovation to the DLT world. Rather than using DLTs' decentralised trust model for offering just an immutable decentralised append-only data store, they exploit the mechanisms to provide a tamper-proof decentralised "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 centralised trusted third party.

8.2. Commercialisation 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 FinTech'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 Fintech's and financial institutions continue to experiment but in a way that's 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.

8.3. Customer Service through Chatbots

The application of artificial intelligence is a FinTech 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 FinTech'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.

8.4. The Last Mile in Digitizing Financial Services

Nearly all FinTech'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 digitisation 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 digitisation of customer-facing activities and live and die by their UX.

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 last mile digitisation 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.

8.5. 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, standardisation 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 today's or tomorrow's challenges.

The market, which has pushed back on biometrics for reasons of privacy, is becoming desensitised 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 FinTech's and financial institutions can avoid.

8.6. FinTech'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 FinTech's and moving quickly on strategic acquisitions to enhance their capabilities. FinTech's with solid vision, backed by great execution, will be rewarded. FinTech's without a viable value proposition or poor execution will continue to burn cash (Gengler 2018).

8.7. 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.

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

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

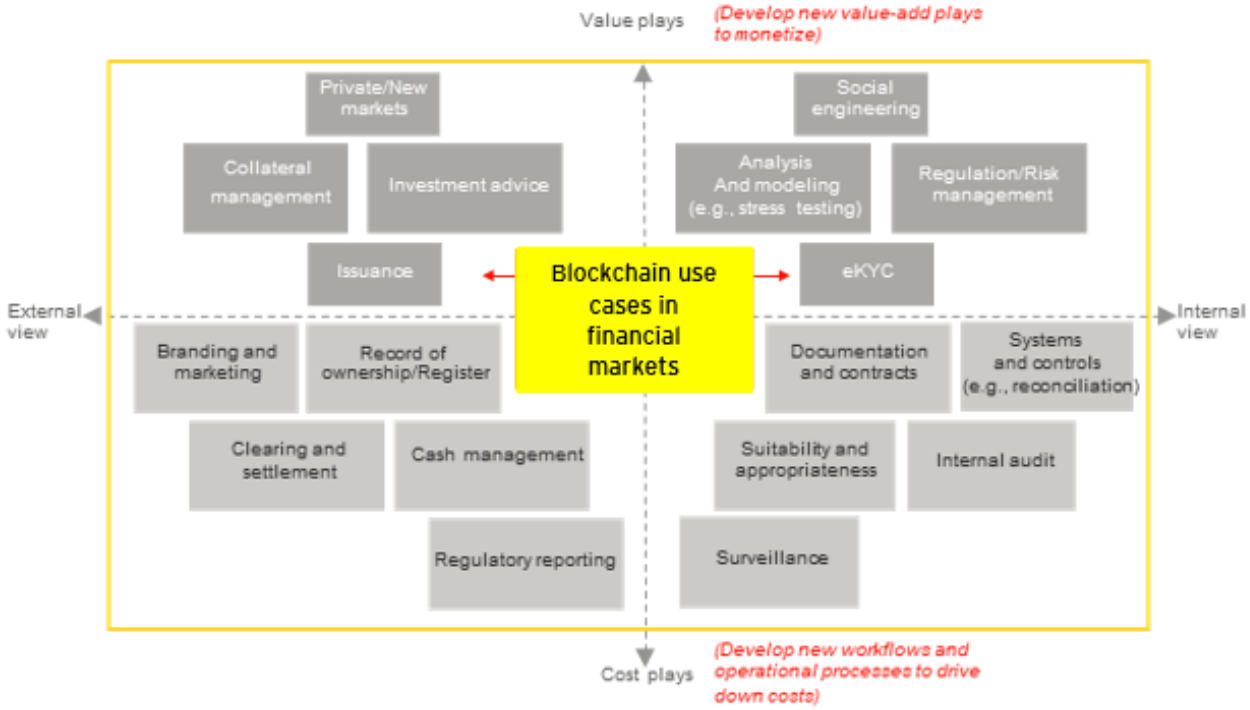

Figure 2. EY (2019), "Blockchain use cases in financial sector"

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.

8.8. 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:

8.8.1. 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 amount 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.

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

DLTs somehow introduce a standardised and easier way to integrate operators worldwide and working around the clock, could push the globalisation 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.

8.8.3. Automation

Once involved parties agree upon a set of rules and validate a Smart Contract, which enforces it, operations on distributed ledgers could be fully automated in a high-trust context, reducing operational costs and mitigating

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 risk that potential disputes arises. These considerations strongly apply to Reconciliation processes, which requires accuracy, non-repudiation, repeatability, certification of data and full transparency on operations.

8.8.4. 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 evidences" 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.

8.9. Let's 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

9. FinTech Market Analysis

Intro

This chapter covers Fintech market analysis, including various aspects like consumer priorities, European market, SWOT and Porter's five forces analysis, authentication schemes, audit & compliance technology, use of TRNGs and HSMs in Fintech, etc.

Critical-Chains relevance

Analysis presented in this chapter is taken into account in Critical-Chains in producing different strategies for technology selection, market positioning and exploitation of project results.

2020 update

This chapter includes new insights in Fintech market analysis in 2020. Special focus is on authentication schemes in online banking and audit & compliance technology. New insights include also update on latest TRNGs and HSMs in the market and the rise of Identity-as-a-Service (IDaaS).

9.1. Changing Consumer Priorities

Digital transformation is reshaping financial services with incumbent and challengers 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 FinTech services that are accessible, personalised, transparent and cost-effective. On the other side, incumbents are most responsive with a tendency to disrupt their own proposition by offering comparable FinTech services, either through partnerships, acquisitions or in house development. In recent years, incumbents have brought their FinTech versions of services such as online foreign exchange, online investments advice and management or peer to peer payments.

In effect, FinTech 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 FinTech adopters want. 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[3]. Overall, despite their security concerns, adopters are comfortable with online aggregator sites and all-digital branchless financial services.

[3] European Commission (2018), "Fintech Action Plan"

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

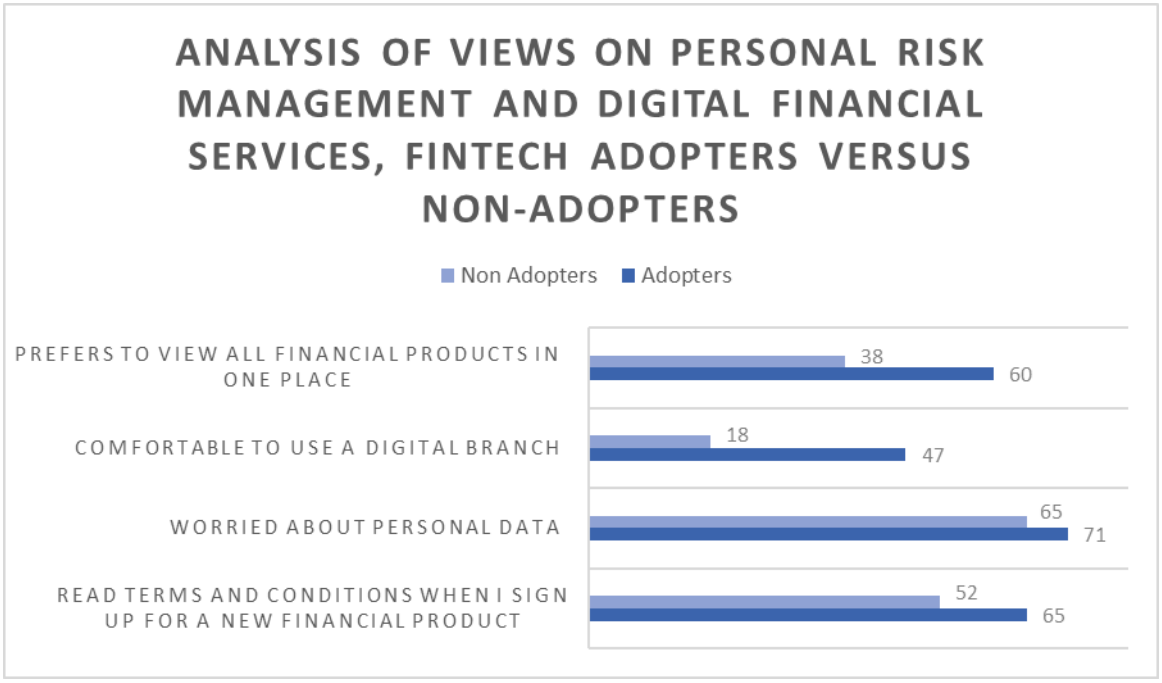

Figure 3. EY (2019), "Fintech Adoption Index"

One of the maturation sign of FinTech industry is the evolution in consumer priorities when they look for a provider. In 2018[4], 30% of adopters ranked the ease of opening an account as their top priority when selecting a FinTech 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 FinTech challenger, perhaps indicating the increasing comparability and competitiveness of FinTech 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.

[4] 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

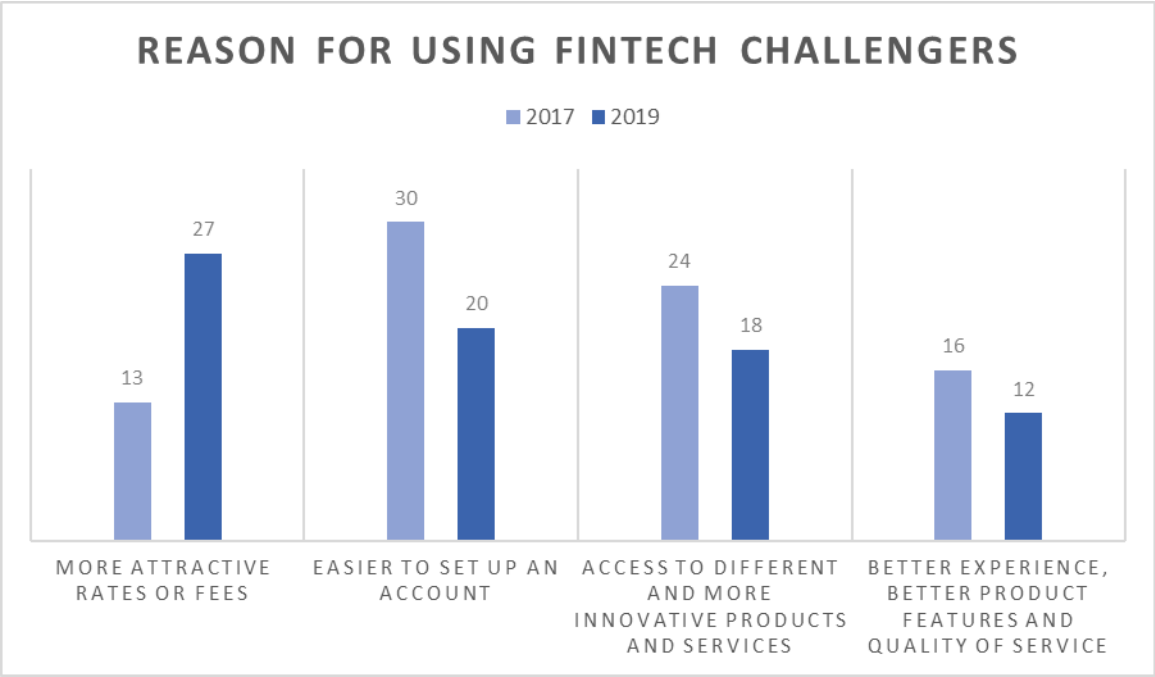

Figure 4. EY (2019), "Fintech Adoption Index"

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 FinTech challenger and the reason is clear: non-adopters choose to remain with incumbent providers because they trust them more than FinTech challengers. Trust is the top barrier to using a FinTech challenger in markets such as Italy or France. As more incumbents offer their own FinTech services, their ability to build on pre-existing trust takes on new significance.

9.2. 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 organisations 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%[5]) as service providers, and most willing to use money and transfer payment FinTech services such as digital only banking and multi merchant eWallets.

[5] EY internal analysis

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

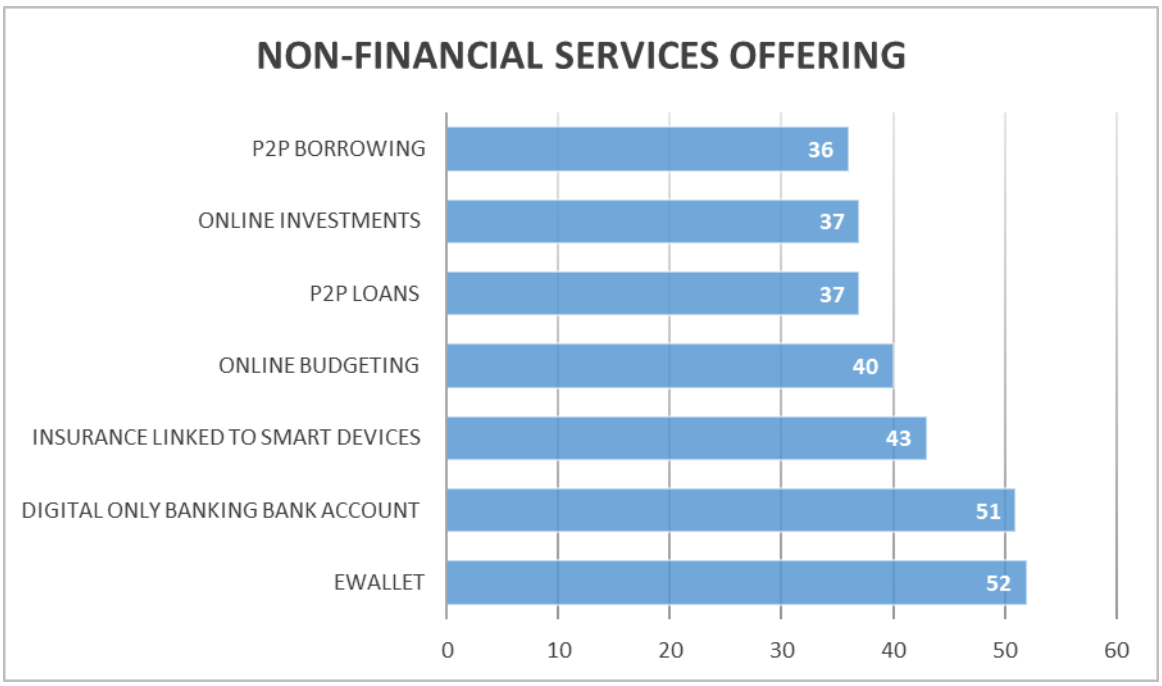

Figure 5. EY (2019) "Fintech Adoption Index"

Fintech 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 FinTech proposition depend on the easy portability of data, such as during onboarding or in enabling real time account access. However, 46% of FinTech adopters are willing to share their banking data with other organisations in exchange for better offers but they are hesitant when it comes to sharing data with non-financial services companies.

9.3. SMEs Fintech users

Across different markets, European SMEs seems to be more restrictive on FinTech services compared to China ones, that displays the highest adoption rate at 61%, followed by the US at 23%. When SMEs use a FinTech. Because SMEs commit resources and personnel to select their vendors, the decision to use a FinTech is deliberate and made in a professional context. SMEs adopt FinTech 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.

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

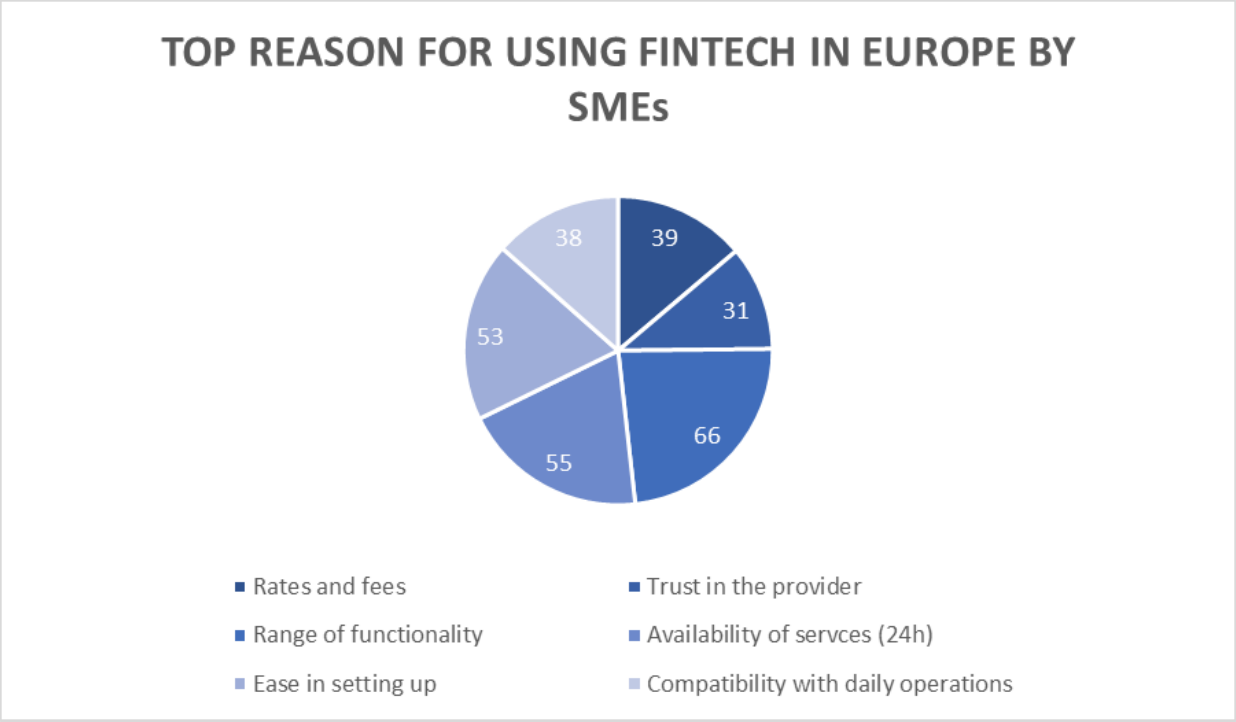

Figure 6. EY (2019) "Fintech Adoption Index"

9.4. European Market[6]

Most EU Fintech operates in the areas of payment and alternative finance and Europe has five Fintech 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 Fintech in the B2B market, but it is also attracting most of the funding. Fintech 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, Fintech was seen as a "threat" if not as "the end of traditional banking". The rise of Fintech 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 Fintech 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.

[6] EY (2018), "Fintech Ecosystem Playbook"

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

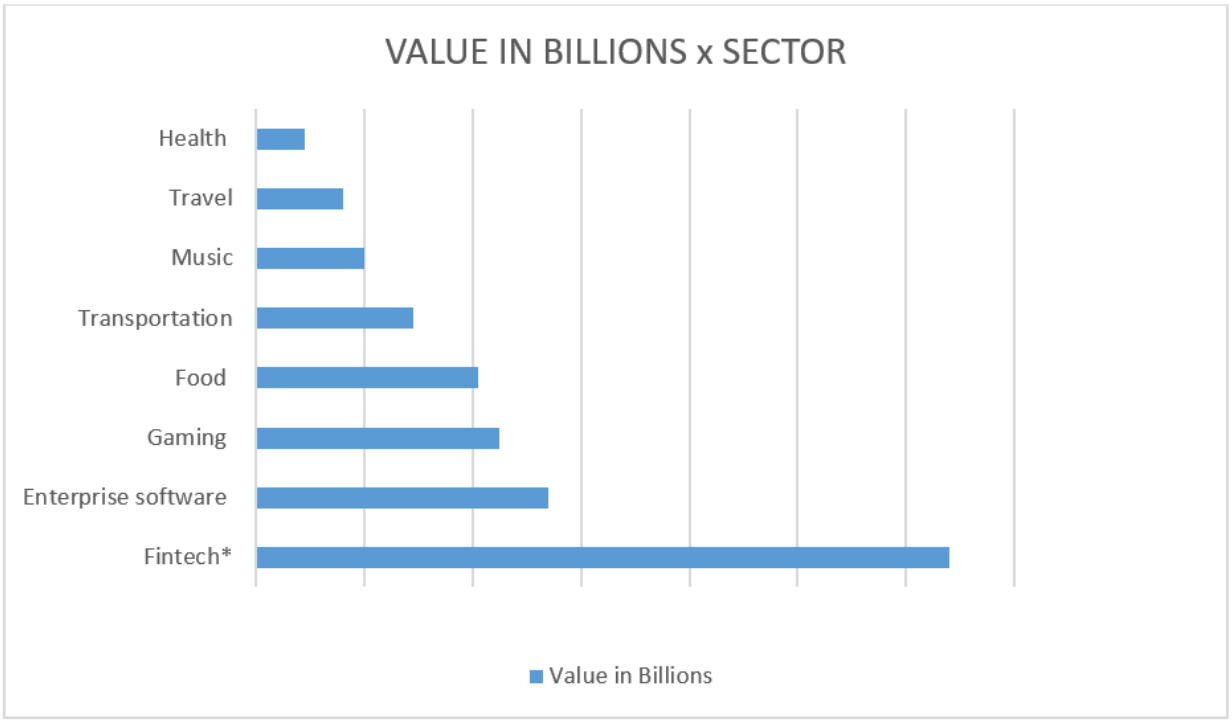

Figure 7. EY (2019) "Fintech Adoption Index", Including: banking & payments, Insurtech, proptech, enabling Fintech platforms (es. r3)

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 Fintech market, with the highest number of Fintech companies as well as the highest Fintech 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 Fintech 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 Fintech ecosystem. However, after Brexit, Fintech companies face uncertainty about the future of market access because of issues around passporting rules and the regulatory framework[7].

The German Fintech 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 Fintech sector. If Brexit results in London will be positive, it is likely that Germany will be a draw for many Fintech companies in future28. In terms of overall investment in Fintech, Germany currently lags behind the UK[8].

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[9].

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

[7] Deloitte (2016), "Driving Fintech innovation in financial services"
[8] Gogardless, "What you did not know about the German Fintech"
[9] Investstockholm (2015), "Stockholm – Europe's No.2 Fintech city"

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

IFS Strategy, the Irish Government's strategy for developing Ireland's financial services sector[10]. Ireland post-Brexit will serve as the EU's only native English speaking country.

In Netherlands the Fintech sector is growing fast but it is still small compared to the UK and Germany. The Fintech sector is crucial for the Netherlands given that the contribution of the financial services sector to GDP is around 7%. The Fintech sector is hindered by gaps in the rigidity of regulation and legal framework, regulatory execution/supervision and collaboration[11].

In France, investment in Fintech 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[12]. France has the potential to concentrate a large number of Fintech 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[13].

Estonia and Lithuania constitute interesting examples as they offers many digitised 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 FinTech 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[14].

Despite Europe, FinTech 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 (Fintech District) to attract this ecosystem becoming a city phenomenon, particularly in Europe[15]:

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

9.5. 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. Advanced analytics is one of the technologies that is already impacting all the financial services providing advantages such as better risk management and product

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

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

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, RegTech 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 personalised products.

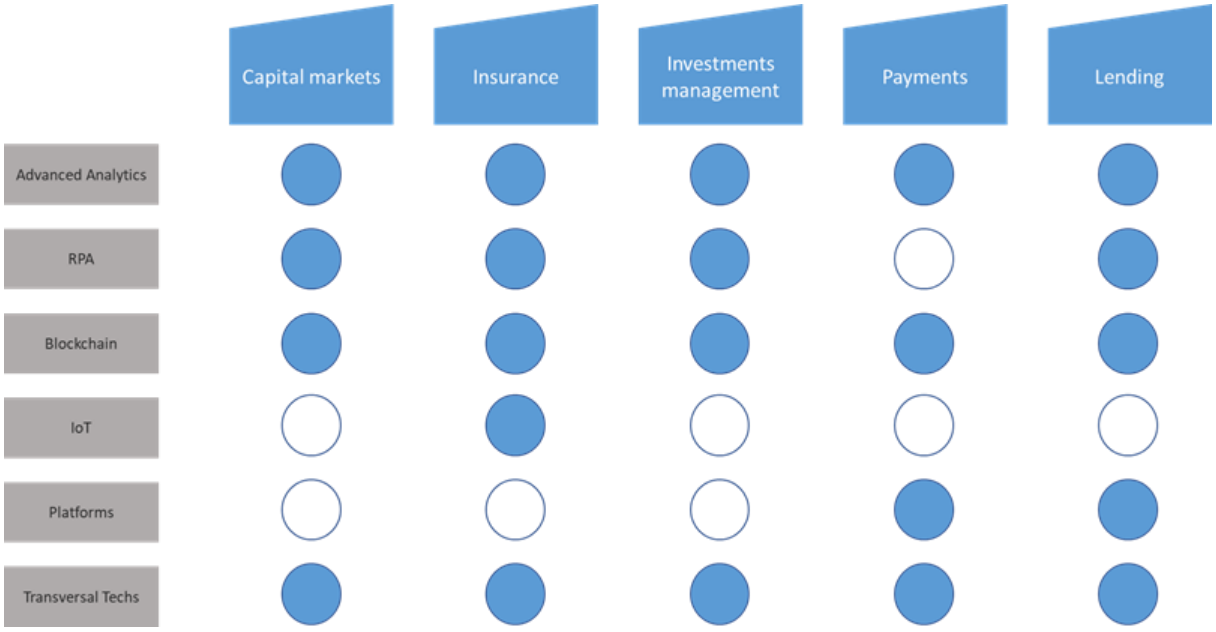

Figure 8. EY internal Analysis

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

9.6. SWOT Analysis

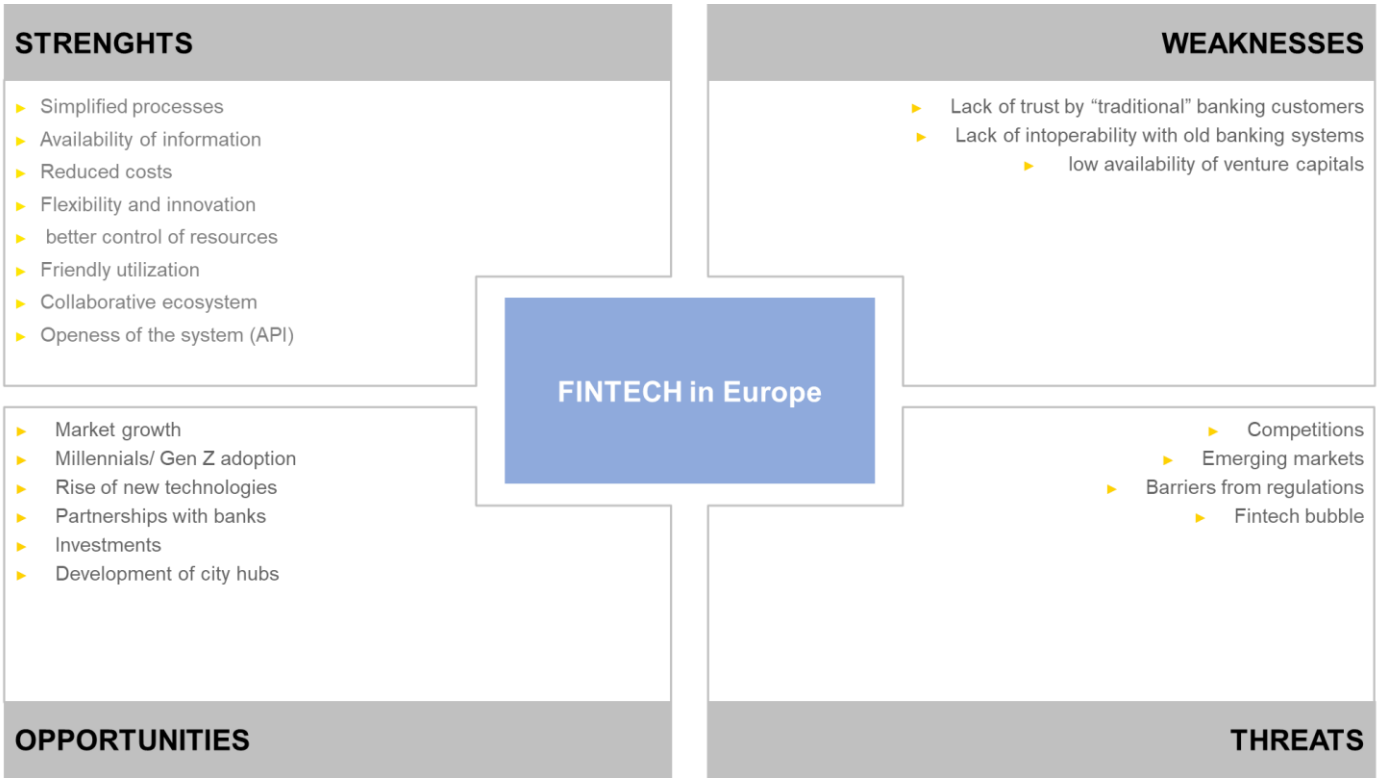

Figure 9. EY internal Analysis

9.7. Porter's Five Forces Analysis

Porter's five forces allows you to determine how profitable the market really is and how profitable will be in the future. By evaluating the impact and power of customers, competitors and the landscape of the market it helps you plan where you can be successful and avoid more challenging markets.

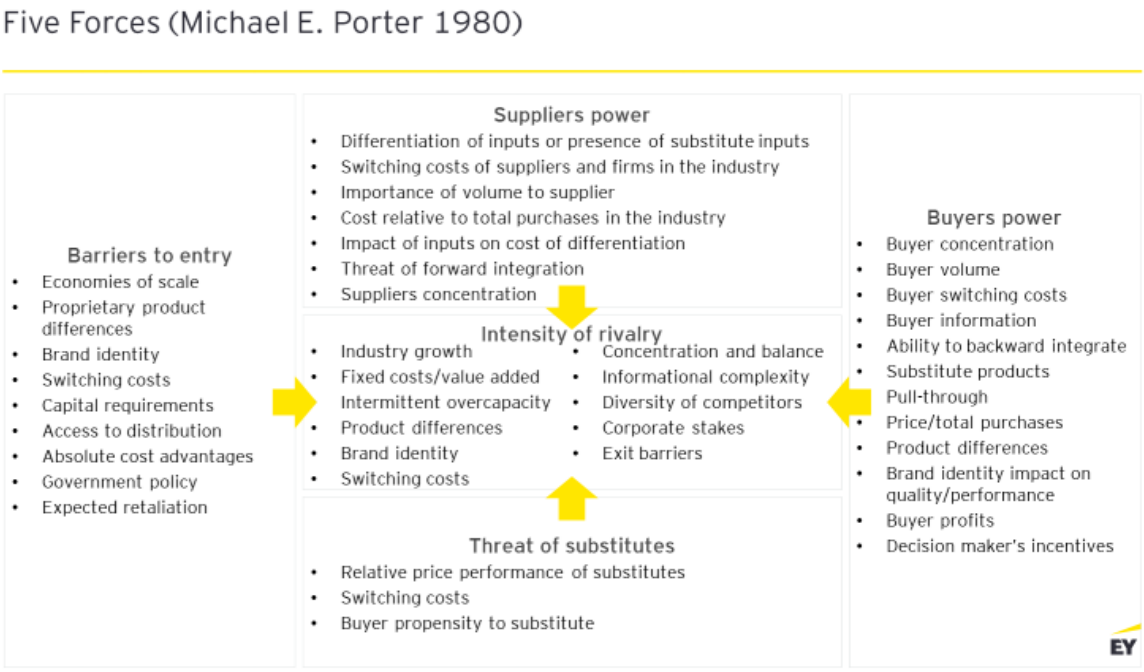

Figure 10. EY internal analysis

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

When we take the traditional financial industry as a focal industry, you'll find that all five forces have low power, thus leading to low overall rivalry:

- It is hard to obtain a banking license (barriers to entry)
- Customers cannot exert influence on financial products (buyers power)
- Banks use very little (asset) suppliers and are not fully dependent on them (suppliers power)
- Everybody is dependent on fiat currencies (threat of substitutes)
- There are only a few major players that hold majority of power (intensity of rivalry)

Now let's consider Porter's 5 forces again, but this time with Blockchain, crypto-currencies and the overall rise of FinTech and peer-to-peer decentralised financial solutions use cases:

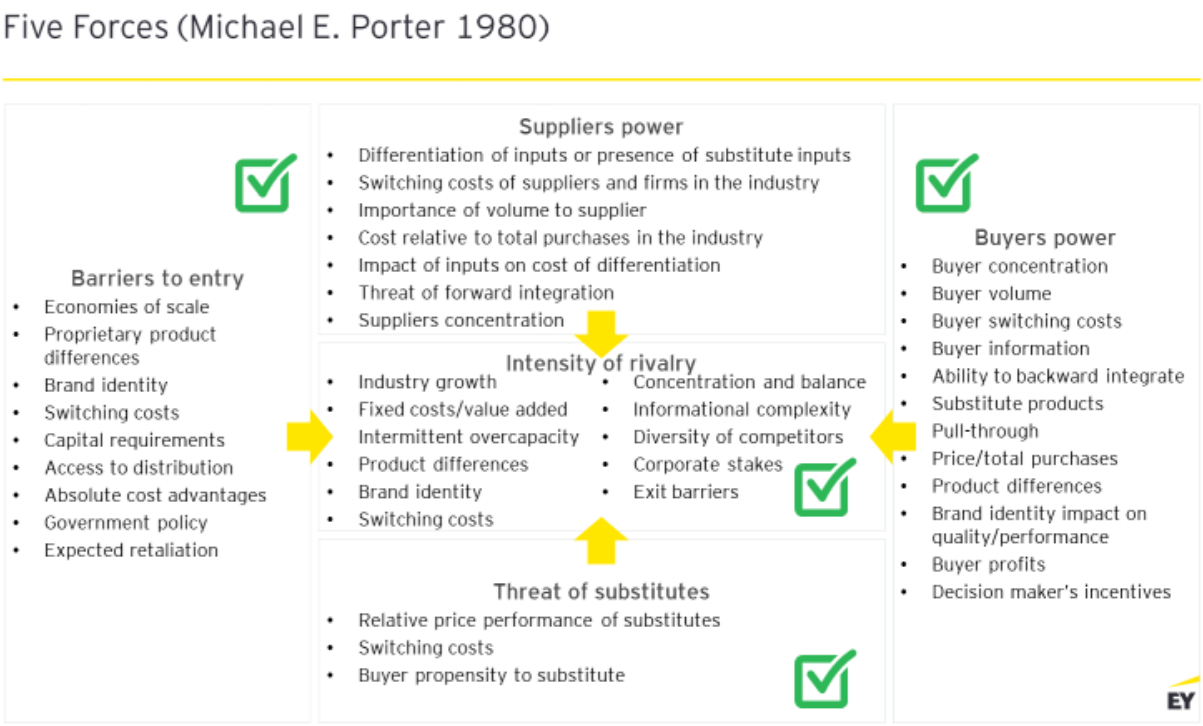

Figure 11. EY internal analysis "Porter's five forces - FinTech considerations"

By taking a closer look, we'll see that 4 out of 5 forces now have a HIGH power and thus exhibit an increased level of rivalry:

- Everyone can join (just look at the amount of ICOs launched every day) and obtaining a banking license is easier than ever (at least in the US, EU and the UK) (barriers to entry)
- Customers are in control and decide which currency to buy and pay with – without any middlemen activity. Look, for example, at the amount of wallet providers out there (buyers power)
- Direct payment solutions and crypto currencies are the substitute for traditional banking solutions and FIAT currencies (threat of substitutes)
- Because of all above mentioned reasons, rivalry is bigger than ever, allowing for a healthy market place of supply and demand (intensity of rivalry).

9.8. State-of-the Art in FinTech 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

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

up and fostering the enlargement of the financial services' market, promoting interoperability and exploitation of data and information for creation of services as Fintech and InsurTech.

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

According to EY Fintech Adoption Index (Ernst & Young 2019) 96% of global consumers are aware of at least one money transfer and payment through Fintech service and 3 out of 4 customers use one of these services. In addition, according to this research, 48% of global consumers use an InsurTech service. Therefore, we can presume that awareness of these new services is now very high.

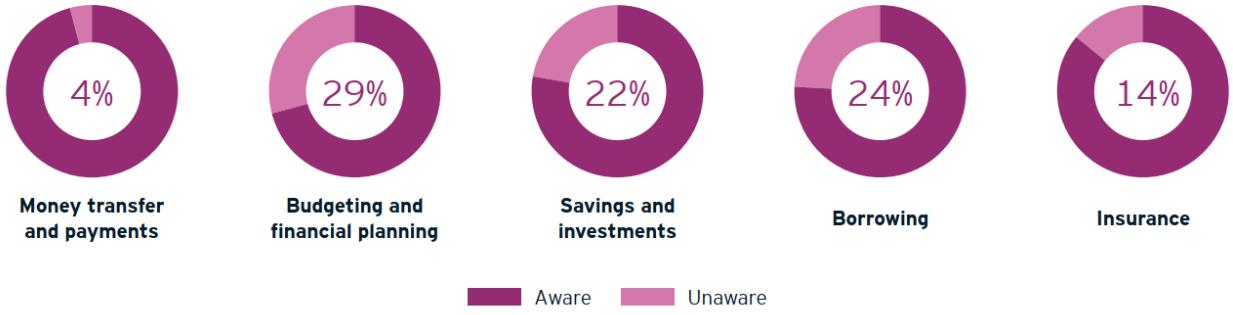

Figure 12. EY (2019) " Fintech Adoption Index "

We tend to define a Fintech 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 Fintech propositions: "disrupted" and "invented". A disrupted service is one that has historically been offered by incumbents, such as automotive insurance or foreign exchange trading. FinTech 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 Fintech 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" FinTech services [quoted FinTech 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 Fintech. 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.

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

InsurTech 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 organisations often facilitate consumer FinTech 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).

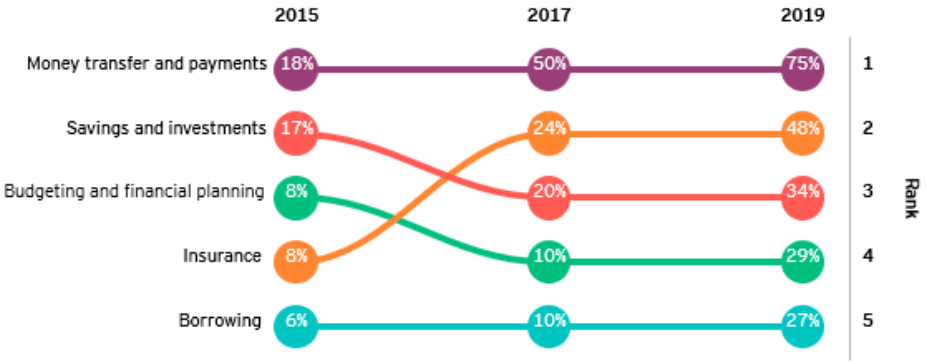

Figure 13. EY (2019) "Fintech Adoption Index"

37 privately held Fintech unicorns have a combined valuation of approximately 142.17 Billion US-Dollars. Several startups 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 startups driving trends listed below:

- **Banks, AI and machine learning powered platforms** to manage core processes, either paper or data sensitive, to analyze 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 FinTech 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, startups and especially regulators.
- **Lending platforms powered by data analytics** to reduce lending process time.
- **Personalised 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 FinTech 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

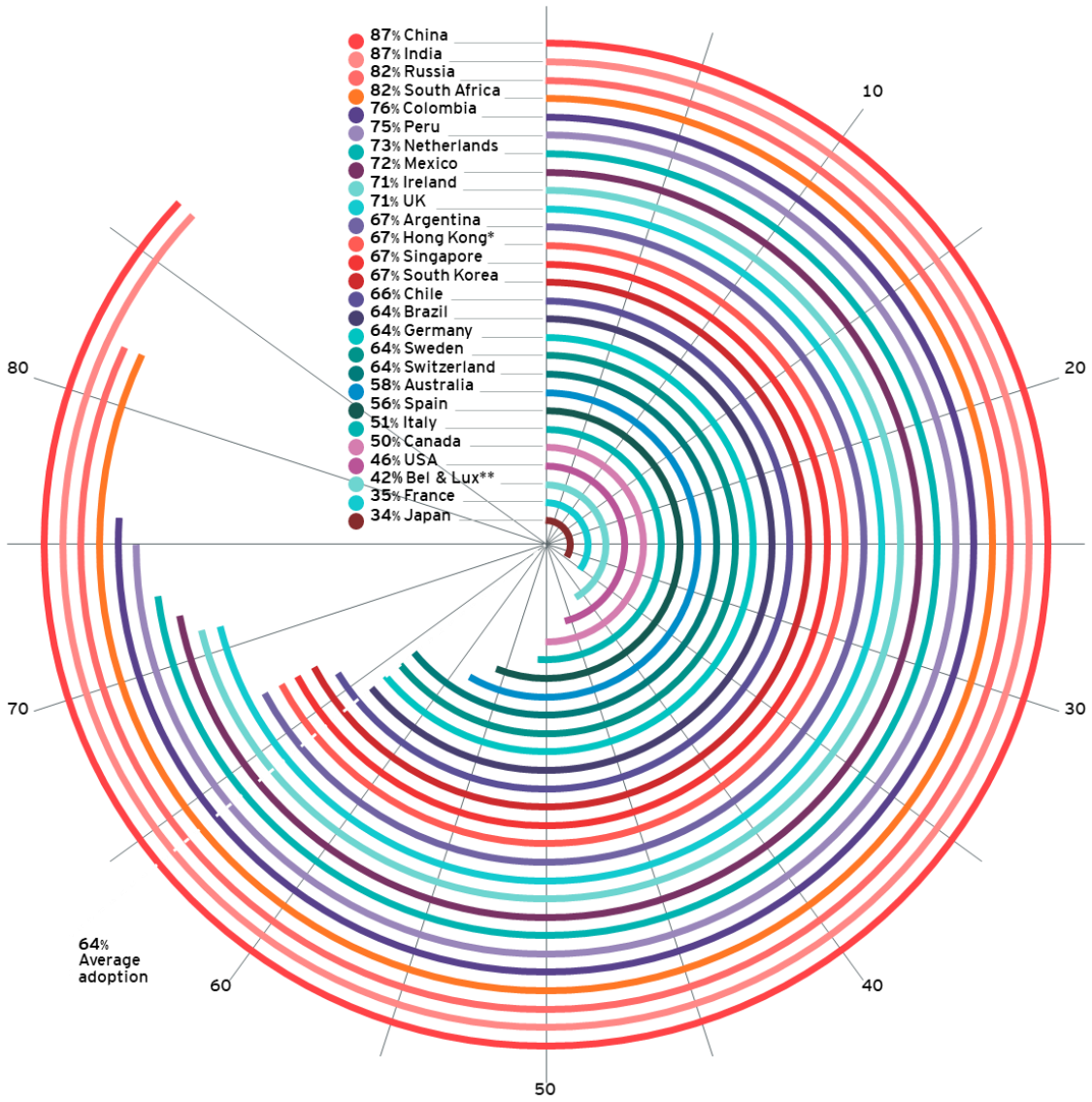

Figure 14. EY (2019) "Fintech Adoption Index"

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 Fintech is iterating on product quickly by offering alternative financing sources and more. Consumers preferences of course will 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 Fintech 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.

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

Some of the core security related issues for which Fintech 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.

9.9. 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 authorised 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 Fintech 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 initialisation 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).

2020 Insights

Recently, 30 international banks were analysed w.r.t the multi-factor authentication protocols they provide (Sinigaglia, et al. 2020). One of the findings of this study is that, while there exist some attempts for a standardisation like FIDO and OATH Authentication, there is no consensus about what kind of multi-factor authentication schemes should be used in online banking. The protocols use different combinations of OTP and operational identifiers together with data channels like inter-process communication, optical code scan, network packet, etc. Further differences can be seen for the enrolment and binding of new customers where in some cases the process can be completed in a remote session while in other cases users have to go to a local branch.

The investigated institutions follow their national or EU guidelines but the resulting authentication frameworks vary greatly and also contain insecure practices like the use of look-up secrets. Especially when it comes to enrolling and binding new customers best practices are widely ignored. As a result, the vulnerability against attacks is higher than expected.

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

9.10. Audit & Compliance Technology

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

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

To manage the many growing and changing needs of IT compliance, many organisations 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 organisation 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.

9.10.2. RegTech

In the recent years, the regulatory compliance in FinTech is supported by RegTech (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 RegTech solutions may help Financial Institution in meeting compliance adherence in an "agile way". The RegTech realities collaborate with financial institutions and regulatory entities and use cloud computing and big data to share information.

Deloitte (Deloitte 2019) classifies the RegTech 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

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

"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 analyze 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).

9.10.1. Audit & Compliance SW Platform – 2020 insights

GRC and RegTech technologies have been adopted in a set of Compliance Audit software such as:

- **ADAudit Plus**[16] is a top on-premise auditing solution developed by ManageEngine. It is built to detect and report the changes done in a company's Windows Active Directory. This enables users to analyze the changes while ensuring that they remain compliant with current IT regulations. Moreover, with ADAudit Plus, organisations can make sure that crucial resources like Domain Controllers are timely audited, monitored, and reported. Besides, they can also track the user logon activity on Domain Controller with the help of email alerts and pre-configured audit reports to determine the reasons behind login failures.
- **iAuditor**[17] is a compliance audit software that fosters positive accountability in user compliance measures. This cloud-based compliance software enables the user to perform regular audits and easily manage the document compliance tasks right from user handheld devices. Moreover, it allows process owners to work together and develop compliance checklists so that they can take the required actions to meet the regulatory compliance standards. iAuditor ensures that user compliance tasks are done timely and correctly. Further, it also tracks task completion across multiple locations and gives a red flag in case of any issues so that you can make better decisions.
- **LexComply**[18] is one of India's leading GRC technology solutions providers. It dominates the industry with its 13 SaaS-based risk and compliance management solutions. As it comes integrated with a legal library, it enables the user to identify, assess, monitor, manage, and report regulatory compliances effectively. Right from connecting the entire risk ecosystem to capturing information on crucial parameters, LexComply strengthens company's internal controls. Moreover, it plays a crucial role in combining the analytics and visualisation areas of an organisation; thus, bringing all the departments and stakeholders of the company on a single platform.
- **Symbiant**[19] is a set of varied tools for managing activities related to risk, audit, and compliance. It aids companies in predicting, measuring, and managing the associated risks. It caters to its service across verticals such as banks, charities, public sectors, PLCs, and more. Symbiant's compliance management solution is deemed ideal for all types of regulations and compliances. Owing to its dominance in the industry, it has been ranked among the top 20 risk management solutions across the globe. Besides being flexible, intuitive, and powerful, Symbiant is the most affordable yet advanced compliance software available on the market.

[16] https://www.manageengine.com/products/active-directory-audit/
[17] https://safetyculture.com/app/compliance-software/
[18] https://www.samaaudit.com/software/lexcomply-corp/index.html
[19] https://www.symbiant.co.uk/

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

- **VComply**[20] is a compliance audit software by VComply can help the user to build a robust internal control framework. It facilitates the user to set mandatory requirements for assigning tasks, uploading evidence or proofs of work, and escalating requests upon delay or failure. Built on EVAS (Entrust, Verify, Analyse, Sustain) framework, this GRC platform enables the user to manage compliance, assess and mitigate risks, and strengthen the governance within your organisation. You can thus induce accountability and increase transparency in the processes and workflows.
- **Hexanica**[21] is a data management and reporting solution for financial institutions. Their software uses an algorithm that can source and ingest data in multiple formats to normalize datasets. The Saas is powered by Hadoop. This Regtech startup is helping banks cut regulatory costs and skirt hefty fines for noncompliance
- **MindBridge**[22] is a Platform that uses Artificial Intelligence and Machine Learning to detect anomalous patterns of activities, unintentional errors and intentional financial misstatement in financial datasets. The auditing software automates ingestion and analysis of data and help accountants identify risks.
- **Alessa**[23] Offers integrated real-time due diligence, transaction monitoring, sanctions screening/watchlist filtering and regulatory reporting capabilities to comply with AML and CTF regulations
- **AQMetrics**[24] is a platform that gives asset service providers and their customers access to a premium on-demand, cloud-based software solution for multi-jurisdictional risk and regulatory reporting.

9.11. Use of HSMs and TRNGs in Blockchain- and IoT-enabled Fintech Industry

The IoT and cyber-physical systems are merging with new trends like Blockchain in Fintech 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 Fintech 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.

9.11.1. 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 (360 Research Reports 2018). According 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

[20] https://www.v-comply.com/
[21] http://hexanika.com/
[22] https://www.mindbridge.ai/
[23] https://www.caseware.com/alessa/
[24] https://www.aqmetrics.com

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

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.

9.11.2. 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 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 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

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

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 brings 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 Fintech 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 155 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 Fintech 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.

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

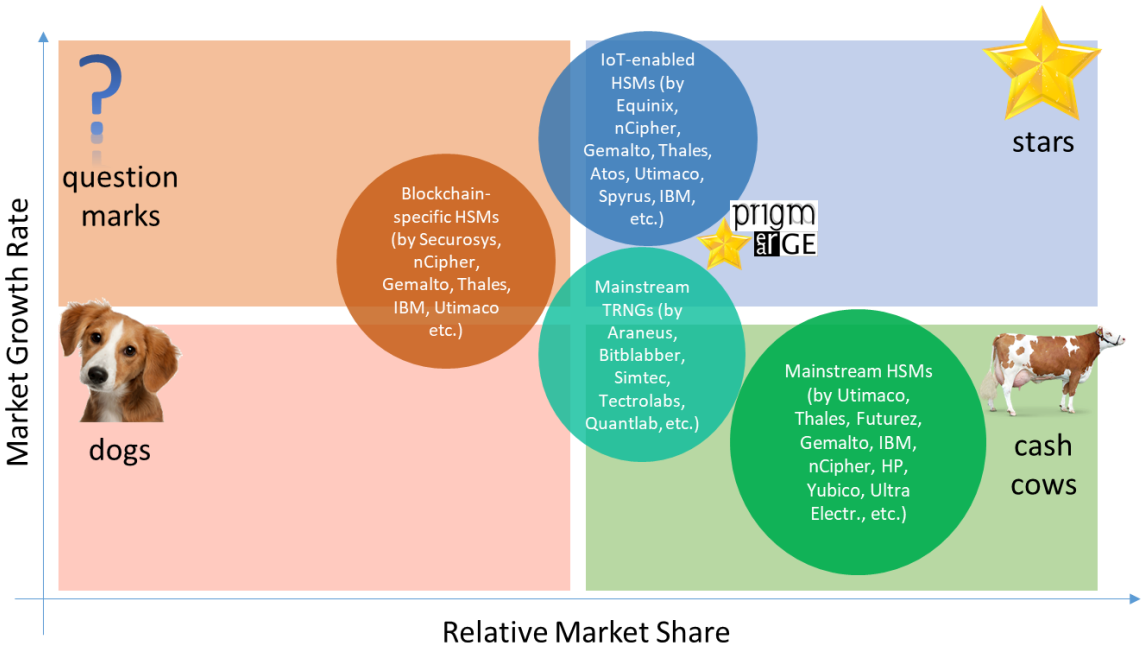

Figure 15. BCG Matrix for HSM and TRNG market

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 High Growth, Low Share	Stars High Growth, High Share
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're worth investing in to increase market share. Consider investing for market penetration, market development, or product development; or divesting.	These products have a high market share and are in a fast-growing industry. They bring in good profits and 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	Cash Cows Low Growth, High Share

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

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 defense against competitors. Suggested action: Consider eliminating these products by retrenching, divesting, or liquidating. Maintain (in special circumstances)	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.

2020 update on Recent TRNGs and HSMs in the market

The improved knowledge in information theory, numerical methods, signal analysis and electronics have turned into advancements in marketable TRNGs and HSMs. Especially in the last decade, the foremost products have been introduced. According to a recent market research[25], the global Hardware Security Modules (HSM) market size is expected to gain market growth in the forecast period of 2020 to 2025, with a CAGR of 10.3% in the forecast period of 2020 to 2025 and will expected to reach USD 2036.2 million by 2025, from USD 1373.9 million in 2019. TRNGs play a crucial role in HSM as the recent trends on the wider exploitation of blockchain, especially cryptocurrencies, forge the Fintech industry to deserve faster and more unique key generators. Big companies like Thales, Gemalto, IBM, Utimaco, Atos, and Synopsis are still leading the HSM market. The other companies like FutureX, Yubico, Ultra Electronics, HUB and Fortanix are penetrating the market as they are revising their vision to meet the requirements of blockchain infrastructures and the needs of new normal since the first days of the COVID -19 outbreak. COVID-19 can affect the global economy in three main ways: i) by directly affecting production and demand, ii) by creating supply chain and market disruption, and iii) by its financial impact on firms and financial markets. HSMs, and generally crypto-as-a-service solutions will take the lead in near future. Aligned with this trend, IBM has invested more on their CloudHSM and lowered its price to 1250-1500 USD/month.

In Table 2, some well-known and recent TRNGs and their prices are presented.

Table 2 Some recent TRNGs in the market

Manufacturer	Model	Interface	OS	Price	Throughput
Araneus	Alea I	USB	Windows/Linux/BSD[2]	159€[3]	100 kbit/s[2]
TectroLabs	TL200	USB	Windows/Linux/Mac	$249[4]	2.0 Mbit/s[5]
Quant-Lab	QRBG121	USB	Windows/Linux	2700€	12 Mbit/s[6]
ID Quantique SA	Quantis-USB	USB	Windows/Linux	990€	4 Mbit/s[7]
ID Quantique SA	Quantis-PCI-4	PCI	Windows/Linux	2,230€	16 Mbit/s[7]
Comscire	PQ4000KU	USB	Linux/Windows/Mac	$895	4 Mbit/s[8]
Comscire	PQ32MU	USB	Linux/Windows/Mac	$1,495	32 Mbit/s[9]

[25] http://www.industryresearch.biz/global-hardware-security-modules-hsm-market-2020-by-manufacturers-regions-type-and-application-forecast-to-2025-16118608

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

LETech	GRANG (various devices)	PCI/USB3/SATA	Linux/Windows	N/A	400 Mbit/s[10]
TRNG98	TRNG9803	SERIAL	Linux/Windows/Solaris/BSD	109€[11]	72 kbit/s[12]
TRNG98	TRNG9815	USB	Linux/Windows/Solaris/BSD	620€	550 kbit/s[13]
Flying Stone Technology	FST-01 (includes NeuG 1.0)	USB	GNU	$35[14]	0.6 Mbit/s[15]
ubld.it	TrueRNG	USB	Linux/Windows/Mac/Pi	$49.95	>350 kbit/s[16]
WaywardGeek	Infinite Noise TRNG	USB	Linux/Windows/Pi	$15.00	300 kbit/s[17]

Similarly, in Table 3 the foremost HSMs and regarding price information are presented.

Table 3 Some recent HSMs in the market

			Price (USD)	
Vendor	Model	Description	Lowest Config.	Highest Config.
Thales	Luna G5 HSM for Government	A small form factor HSM that is widely used by government agencies for data, applications and digital identities to reduce risk and ensure regulatory compliance	5289	13029
	PayShield/nShield	Remote administration license for Thales and nCipher HSMs	2967	41280
	ProtectServer External 2 (and 2+)	Security hardened network crypto servers designed to protect cryptographic keys against compromise, while providing encryption, signing and authentication services to security sensitive applications. Rapid processing of cryptographic commands. Specialised cryptographic electronics — including a dedicated data cipher micro-processor, memory, and a true Random Number Generator (RNG)	8449,5	17028
	SafeNet ProtectServer A Series PCIe HSM	Tamper-protected hardware security for server systems and applications that require high-performance symmetric and asymmetric cryptographic operations.	7107,9	15996
	SafeNet ProtectServer S Series PCIe HSM	Tamper-protected hardware security for server systems and applications that require high-performance symmetric and asymmetric cryptographic operations.	13674	94686
	Thales Luna A700 Series	Network attached Hardware Security Module (HSM) designed for high performance non-payments cryptographic processing, message authentication, comprehensive key management, and general-purpose cryptographic processing.	21414	40893
	SafeNet Luna Backup HSM 7	secure backup of high value cryptographic key material	3508,8	9352,5
	Thales Luna S700 Series	Multi-factor (PED) Authentication for high assurance use cases	29670	49149

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

HUB	FireVault HSM	Dedicated hardware server and 24/7 always online, key management solution for safely storing and using all of a company's sensitive data	175440	175440
	Security FireWallet	Hardware Wallet with an embedded Firewall.	2193	13545
nCipher	nShield Connect	FIPS-certified appliances that deliver cryptographic services to applications across the network. These tamper-resistant platforms perform such functions as encryption, digital signing and key generation and protection over an extensive range of applications,	3225	27090
	nShield Edge	Full-featured, FIPS-certified, USB-connected devices that deliver encryption, key generation and key protection along with convenience and economy.	1806	6450
	nShield Solo	FIPS-certified, low-profile PCI-Express cards that deliver cryptographic services to applications hosted on a server or appliance. These tamper resistant cards perform such functions as encryption, digital signing and key generation and protection over an extensive range of applications,	16125	27090
Utimaco	Atalla AT1000	A payment HSM that enables interbanking business	13416	33669
	Utimaco Block/Quantum -safe	Protecting sensitive data and associated keys for blockchain systems using distributed ledger technology (DLT) and wallets	19479	36765
	ESKM-Enterprise Secure Key Manager	Protect sensitive information such as payment cardholder data, customer and employee records, electronic health records, intellectual property, cloud-hosted data, and national security and defence information with strong encryption key management.	35088	35088
	SecurityServer CSe-Series	Tamper-responsive technology to secure cryptographic key material for servers and applications. It is ideally suited for applications and market segments with high physical security requirements, e.g. government authorities or banking environments.	21801	28767
	SecurityServer CSe PCIe	FIPS Level 4 security of cryptographic key material for servers and applications. It includes integration software that supports the industry standard PKCS#11, Microsoft CSP/CNG/SQLEKM and JCE interfaces.	10320	16254
	SecurityServer Se Gen2	Security of cryptographic key material for servers and applications. It includes integration software that supports the industry standard PKCS#11, Microsoft CSP/CNG/SQLEKM and JCE interfaces.	14319	31605
FutureX	Excrypt Series	Processing speed and robust security are staples of the Excrypt Series	20575,5	32895
	Excrypt SSP Enterprise v.2	General purpose HSM	38377,5	38377,5
	Excrypt Touch	A portable tablet that incorporates a FIPS 140-2 Level 3 compliant HSM	2580	3225

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

	Guardian Series 3	Allows authorised users to centralise management of Futurex devices, physical and virtual, pool resources and commands through synchronous peering and remote configuration, making in-person physical management of cryptographic infrastructure virtually obsolete	19350	38700
	Vectera Series	FIPS 140-2 Level 3-validated technology to general purpose cryptography, ensuring security at a level reserved for the most sensitive data.	16125	30637,5
Fortanix	FX2200 Series II	Fortanix Self-Defending Key Management Service ™ (SDKMS) in a private cloud or as a managed service. With SDKMS, you can securely generate, store, and use cryptographic keys and certificates, as well as secrets, such as passwords, API keys, tokens, or any blob of data.	47988	47988
IBM	Cloud HSM	HSM-as-a-Service over cloud	1250-1500 USD/month	1250-1500 USD/month
Ultra Electronics	APE KeyperPLUS	FIPS 140-2, Level 4 general purpose HSM	15000	18000

Findings:

- The recent trends in hardware-based security have shown that hardware-based cryptographic solutions are still indispensable.
- The COVID-19 outbreak has proven that the faster cryptographic tools will gain more popularity. Recent solutions are evolving by transforming into X-as-a-Service mode where the customers are not asked to pay huge amounts for the hardware but relatively smaller amounts for online or on-demand solutions for their actual needs.
- The blockchain-supported HSMs are getting more popular although they are not offering very novel features. The use of the magical word “blockchain” has been seen as a good tactic for promoting the HSMs. This seems like a “star” (a.k.a. BCG matrix methodology) but has the risk to become either a “question mark” or a “dog” if the customers do not see any innovation behind the blockchain-supported HSMs.
- The recent research activities are also aligned with the exploitation of blockchain-based IoT infrastructures. For instance, in a recent study Mohanty et al. (Mohanty 2020). presented the PUFchain, which is a Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE). They applied physical unclonable functions as the secret for Hardware-Assisted Proof-of-Authentication (HA-PoAh). In another study, Bao et al. (Bao, et al. 2018) presented IoTChain: A Three-Tier Blockchain-based IoT Security Architecture, which is composed of three layers: an authentication layer, a blockchain layer and an application layer which is very similar to the Critical-Chains architecture. Finally, in (Singh and Meher 2020) major security issues were addressed that are essential to be overcome before blockchain adopts the mainstream. Here, HSMs were proposed as strong tools to assist the holistic security of blockchain infrastructures.
- The recent security schemes usually rely on PUF-based secret as tamper-proof countermeasures. However, PUFs provide tamper-resistance after they are manufactured. There is no guarantee for preventing any injection before they are produced. TRNGs may provide a better security at this stage as they enable dynamic secret generation (e.g. one-time passwords). TRNG, for sure brings more security as compared to the static PUF-based solutions (for more details see D5.5 and D5.9 and the published papers by ERARGE in (Ergün and Tanriseven, Random Number Generators Based on Discrete-time Chaotic Maps 2019) (Ergün, Attack on a Microcomputer-Based Random Number Generator Using Auto-

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

synchronisation 2019) (Ergün, Revealing the Unknown Parameters of a Microcomputer-Based Random Number Generator 2019) (Demir and Ergun 2019) in Critical-Chains).

9.12. Recent Status of Authentication Schemes in Identity Management

Identity solutions play a crucial role in Fintech 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[26], 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 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 166 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.

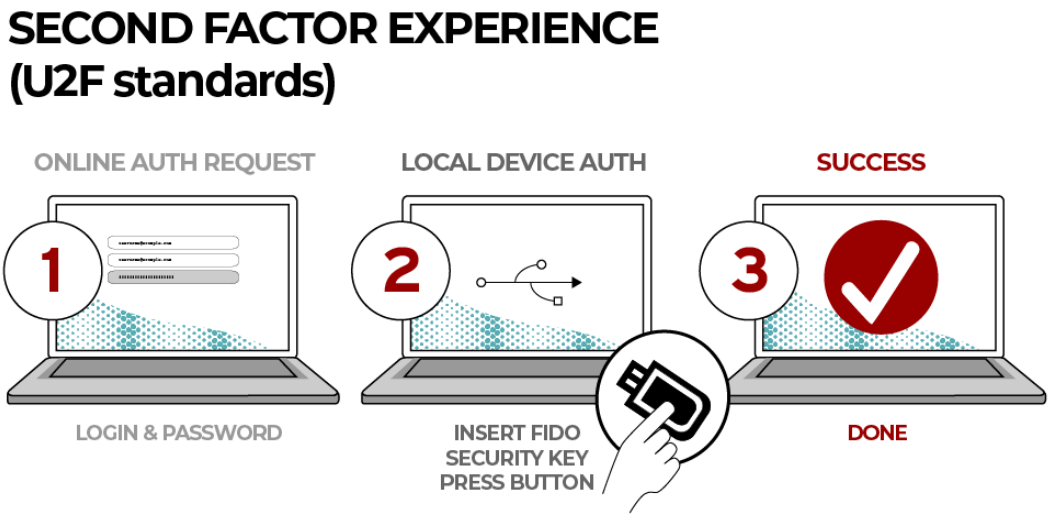

Figure 16. U2F standard in FIDO

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,

[26] https://fidoalliance.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

published in Australia, summarises the actual use of IDMS in these fields of operation[27]. 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 recognised by public bodies across the EU. From the banking perspective, EU banks seriously invest in seeking the optimised 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:

- 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[28] 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.

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

[28] 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

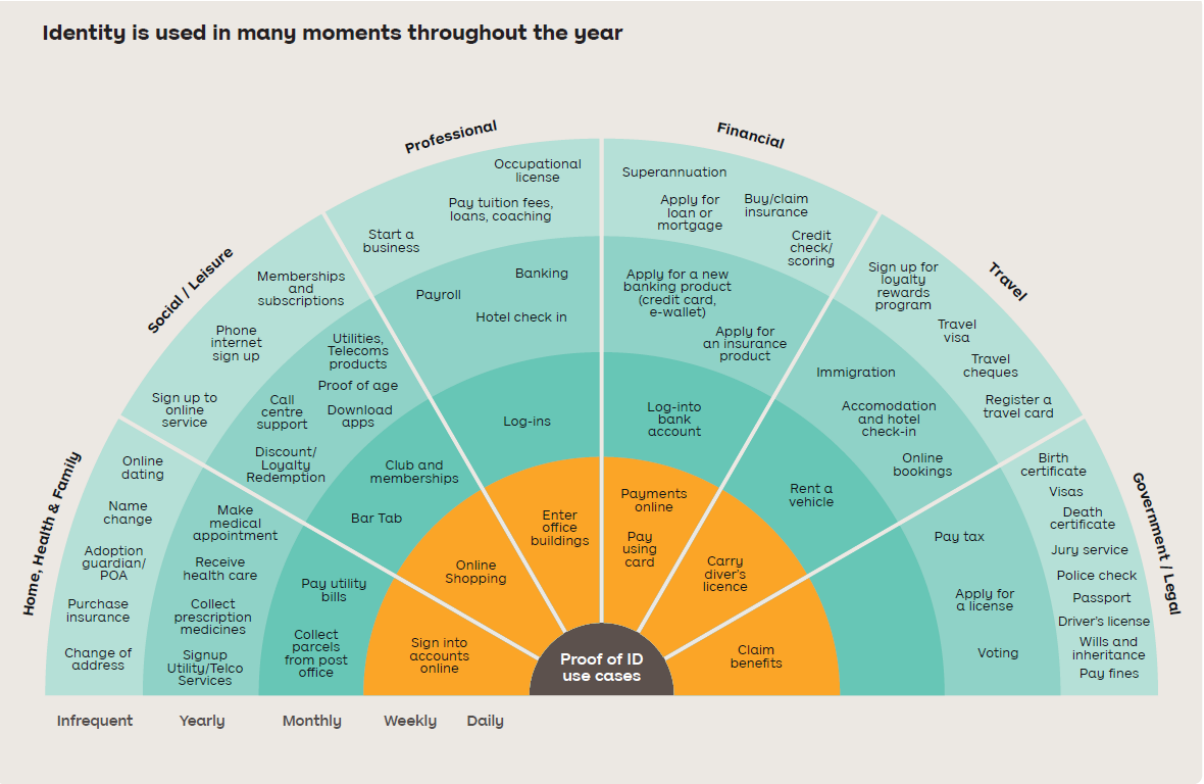

Figure 17. IDMS usage frequency in various fields

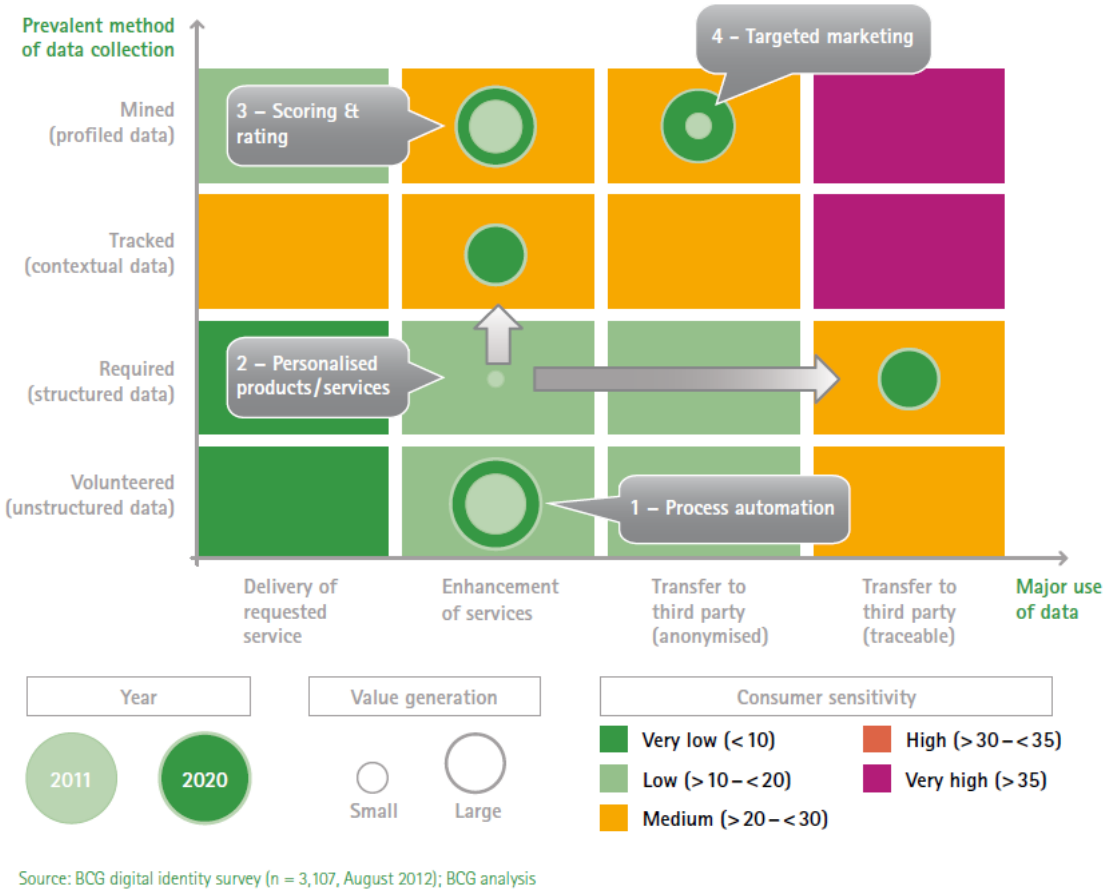

Figure 18. BCG digital identity survey related to online financial services

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 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”.
- **Who 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 indicates 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

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

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".

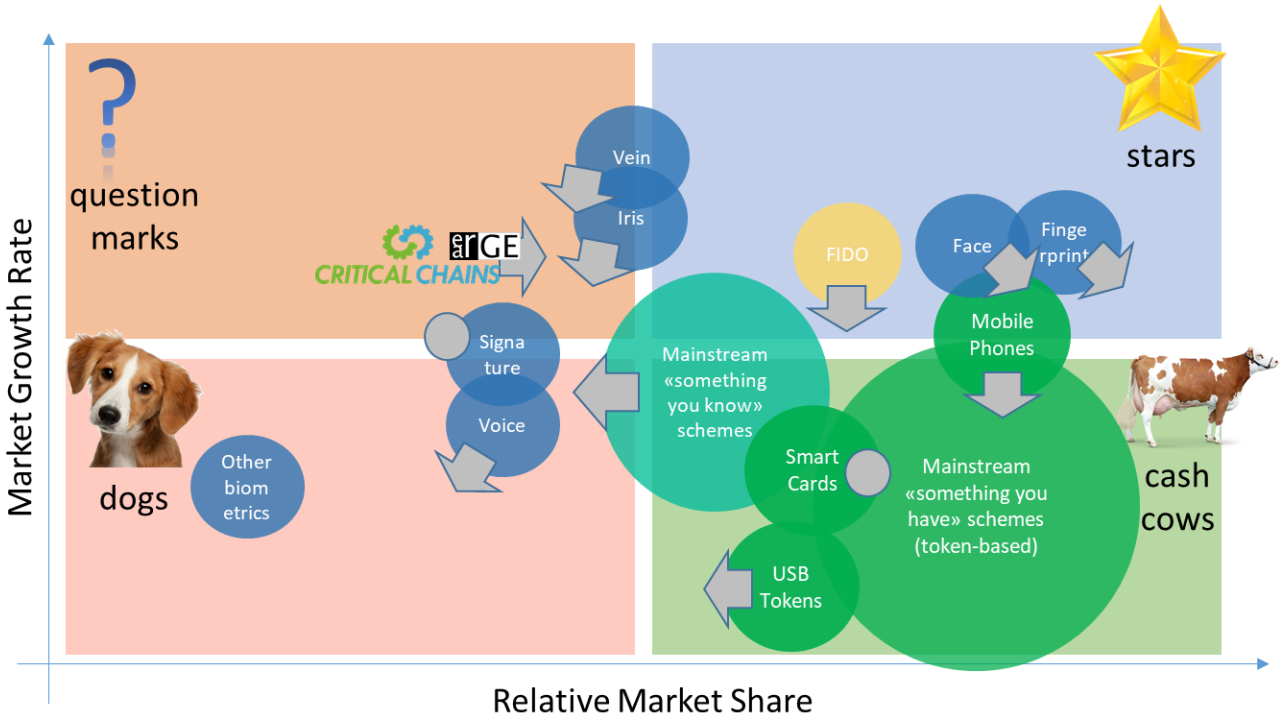

Figure 19. BCG matrix for authentication schemes in IDMSs

2020 insights – The Rise of Identity-as-a-Service (IDaaS)

Enterprises are embracing cloud and mobile technologies. As they do, they're moving beyond traditional network boundaries and the capabilities of their legacy identity and access management (IAM) solutions or generally Identity Management Systems (IDMS). Identity as a service (IDaaS) is a SaaS-based IAM that allows organisations to use single sign-on, authentication and access controls to provide secure access to their growing number of software and SaaS applications. With the recent trends, especially after the COVID-19 outbreak, IDaaS has become a new business model for all online services, including the Fintech industry.

The enterprise IDaaS solutions have gained a momentum as they tend to provide the following capabilities:

- Single Sign-on (SSO): Single sign-on obtains easy, fast and secure access to all SaaS, mobile and enterprise applications with a single authentication using corporate credentials. SSO works based upon a trust relationship set up between an application, known as the service provider, and an identity provider, very similar to the protocol proposed in Critical-Chains.
- Multi-factor Authentication (MFA): MFA typically includes adaptive authentication methods that incorporates the regular login-password scheme but also more advanced techniques like authentication tokens (SecureStick in Critical-Chains) and biometrics (face verification in Critical-Chains).
- Access Security: Access security is policy-based access management for applications and APIs to enhance security beyond SSO.

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

- Directory: While most enterprises prefer to integrate IDaaS with their existing user stores, they may use a cloud directory, especially to support customers and/or partners. The Critical-Chains main framework addresses the need of a cloud-based directory for identity management.

According to a recent research published by Forrester[29], the foremost ten IDaaS providers were evaluated across their current offering, strategy, and market presence. As seen is Figure 20, Okta (2000+ employees) and Idaptive (a spin off from Centrify with about 300 employees) have become the leaders in IDaaS in the last 5 years. These two US-based companies had highest ranking in both the "current offering" and "strategy" categories and also they earned the highest possible score in twenty of the evaluation criteria, including "access management policy administration," "API security and solution APIs," and "certifications". Idaptive has become now part of CyberArk, the global leader in privileged access management. The giants like Microsoft and Google come after as the strong performers. OneLogin, Ping and the others are penetrating right top corner in Forrester Wave as promising performers, contenders or challengers.

[29] https://www.forrester.com/report/The+Forrester+Wave+IdentityAsAService+IDaaS+For+Enterprise+Q2+2019/-/E-RES144405

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

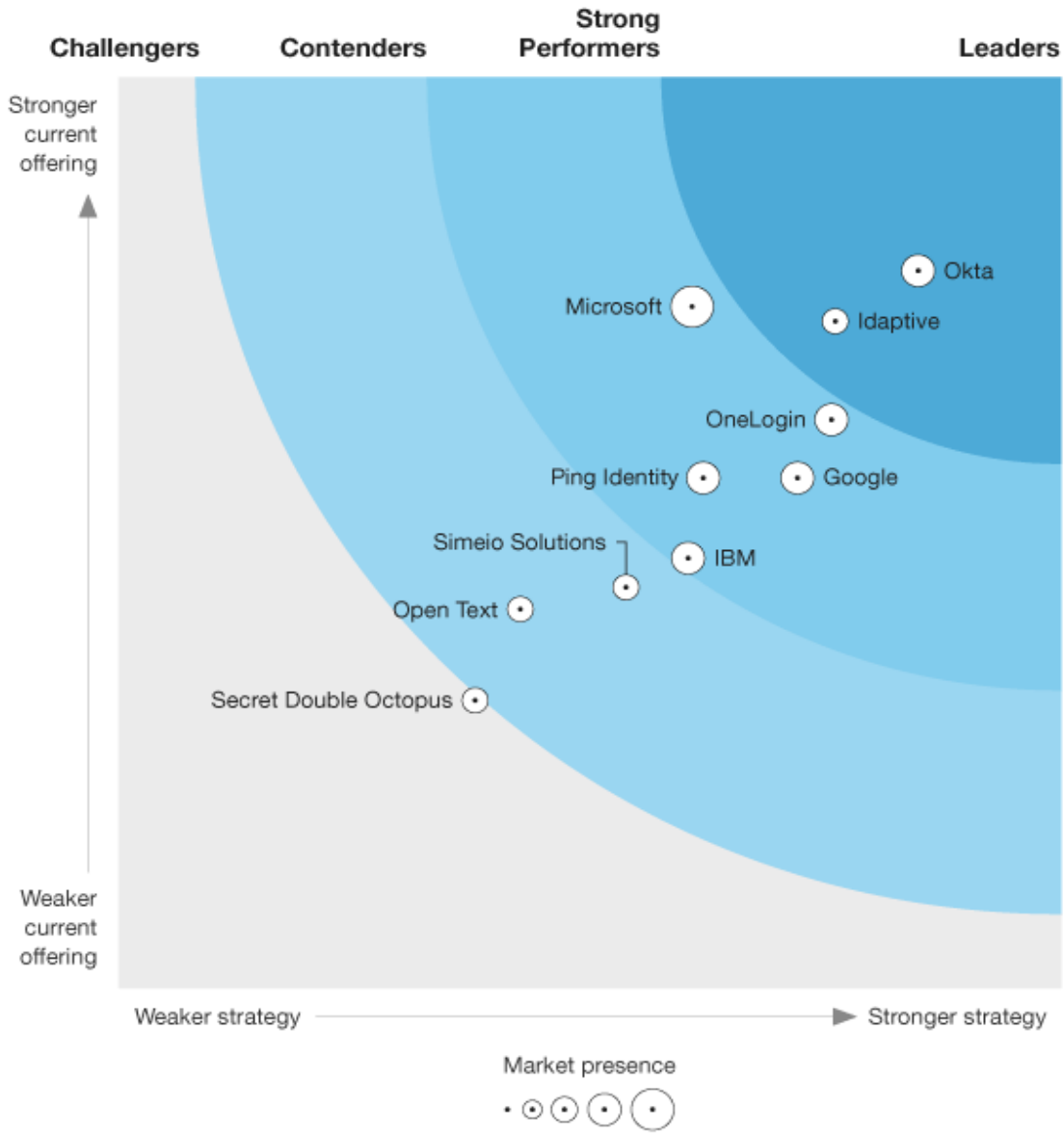

Figure 20 The Forrester Wave™: Identity-As-A-Service (IDaaS) For Enterprise, Q2 2019

Findings:

- The current market for IDaaS is highly aligned with the XaaS notion behind the Critical-Chains, as the consortium has already started develop and integrate HwSaaS, Crypto-as-a-Service and Authentication-as-a-Service.
- The pricing strategy of the leaders relies on win-from-offtake which is based on selling the services with relatively cheap prices abut win from huge amount of sells in a monthly basis. For instance, Okta's per-user/per-month prices for SSO, MFA and universal director are 2USD, 3USD and 2USD, respectively.
- The FIDO-compliant authentication mechanisms are getting popular. Google is behind the FIDO alliance as the main notion behind this scheme is that the authentication should be easy-to-use and browser-friendly (interoperable for wider uptake)
- The open-source access management solutions are getting popular in the market. For instance, KeyCloak an open source identity and access management library, is being used in many solutions.

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. Cyber-Attacks against Financial Infrastructures

Intro

This chapter lists details of the most important cyber-attacks in Fintech domain.

Critical-Chains relevance

Analysis presented in this chapter is taken into account in Critical-Chains in framework design phase and technology selection, with the goal to optimize and increase to the highest possible level cyber-attacks defence capabilities.

2020 update

This chapter includes an update on recent cyber incidents in Fintech in 2020, including general cybersecurity statistics and COVID-19 related statistics, and the details of EasyJet2020 cyberattack.

10.1. Cyber-attacks against financial infrastructures between 2005 and 2019

Cyber incidents involving financial institutions have been dramatically increasing in recent years. According to a 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 21 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.

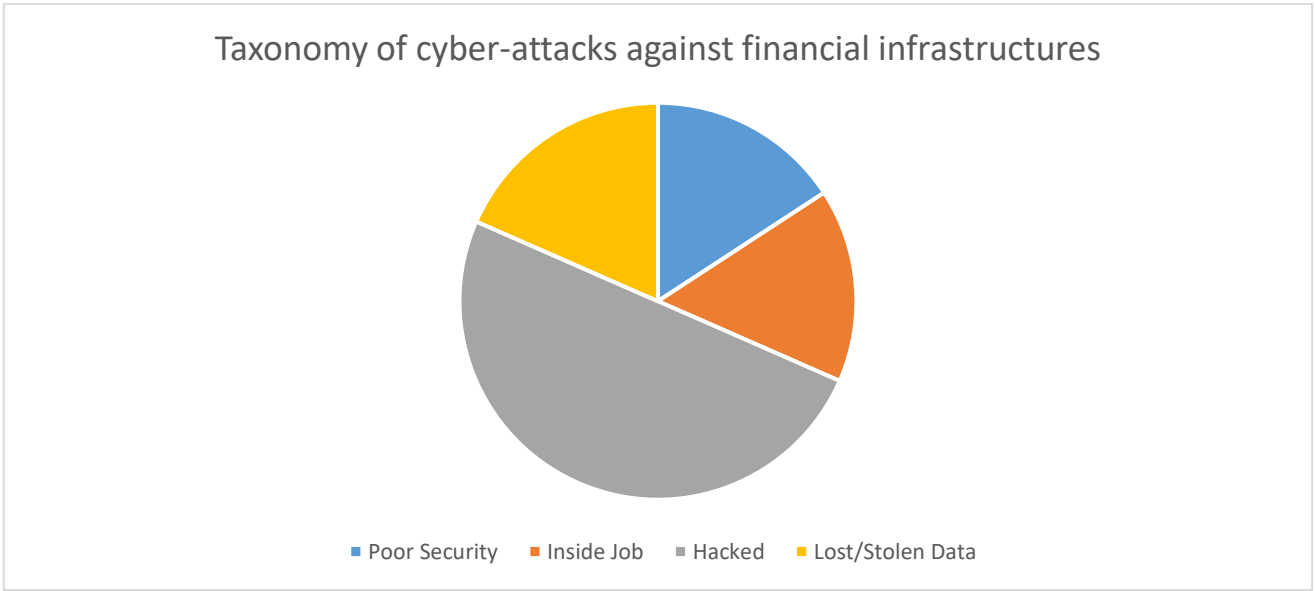

Figure 21. Taxonomy of cyber-attacks against financial infrastructures between 2005 and 2019

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

Appendix 1 – Fintech Cyber Incidents 2013-2019. 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.

10.2. Cyber-attacks against financial infrastructures in 2020

Cyber Incidents Involving Financial Institutions are getting world-widespread with a significant increase in quantity and in terms of their cascading effects covering the loss of money and reputation. According to the timeline of cyber incidents involving financial institutes, published by Carnagie Endowment for International Peace[30], the number of attacked countries has significantly increased since 2007. As seen in Figure 22, entire Europe and also other well-developed, developing or less-developed countries have become the targets and usually victims of attackers.

Figure 22 The countries affected from cyber incidents in Finance domain since 2007 (image: Carnagie Endowment for International Peace)

As a follow-up study, Critical-Chains consortium has surveyed the recent attacks to financial institutions in the period of January-July 2020 which are listed in Appendix 2 – Fintech Cyber Incidents 2020. The list contains the high-impact attacks which are presented in the timeline of Carnagie Endowment for International Peace. We mainly focused on the analysis of these attack, their causes and cascading effects. We identified 29 serious cyber-attacks to financial institutions in this 7-month period resulting mostly with theft but also data breach and disruption. The majority of incidents had been realised by malware but DDoS and ransomware were the other preferred methods. Nearly in all incidents actors and their attribution were unknown. Only a few of them was realised by either non-state or state-sponsored actors. The banks and cryptocurrency infrastructures had been the most attacked organisations in general, but financial firms, insurance companies and governmental organisations (e.g. tax office) were also hit by the hackers. Europe and USA had been the most active geographies that were subject to cyber-attacks. In general, 25 out of 37 affected countries (known) are known as well-developed countries. The reason is obvious as these countries are also leader in finance, trade, commerce and banking worldwide.

The fact figures are summarised in the following pie diagrams (Figure 23):

[30] https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline#click-hide

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

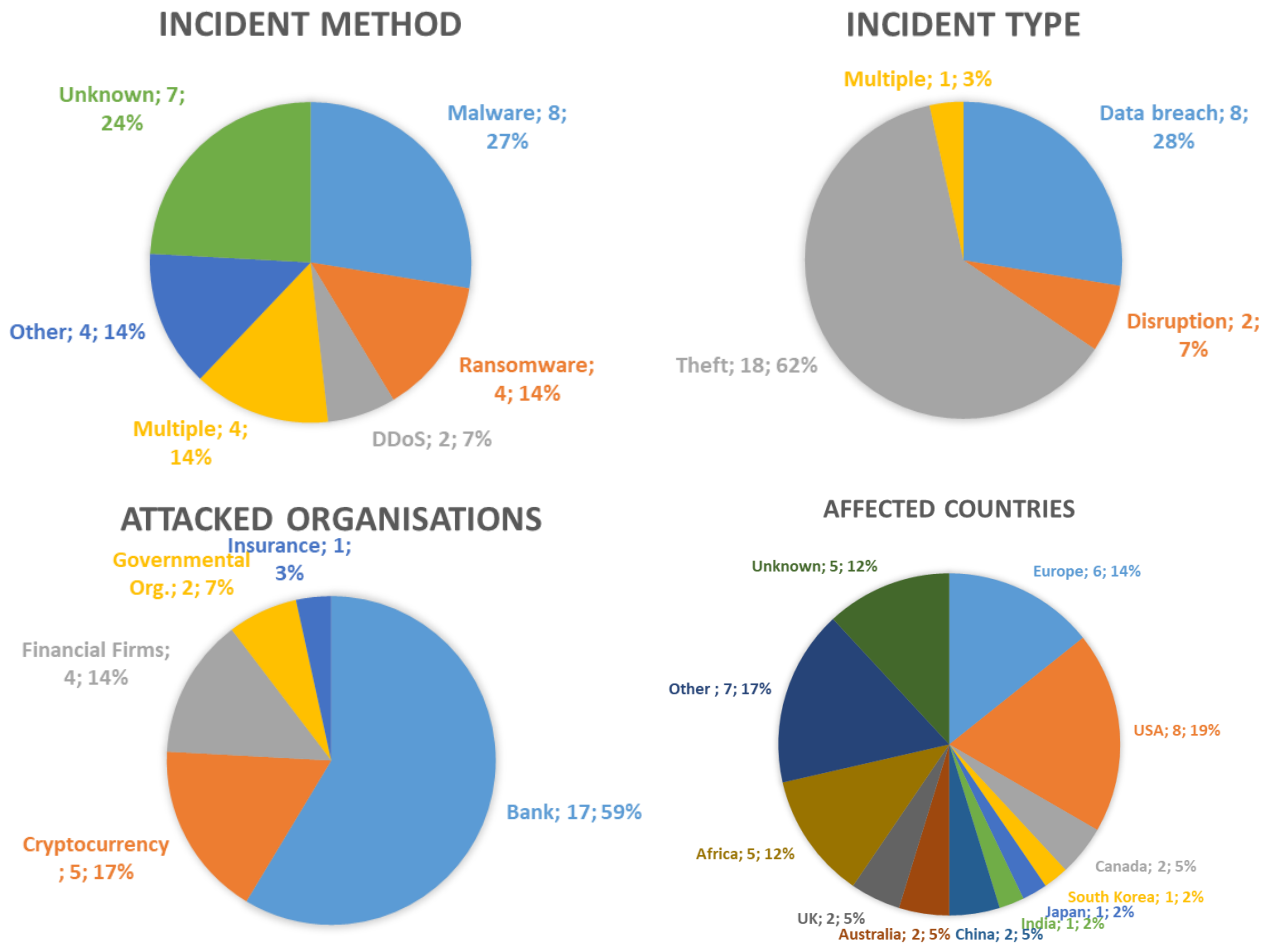

Figure 23 The statistics about high-impact cyber attacks against financial institutions in Jan-Jul-2020 (Ref: Carnagie Endowment for International Peace)

Cybersecurity statistics for 2020[31]:

- 85% of people posting puppy photos are trying to scam you
- 43% of data breaches are cloud based web applications
- 67% of data breaches resulted from credential theft, human error or social attacks
- 70% of breaches are caused by external actors
- Organised crime gangs account for 55% of attacks
- 37% of credential theft breaches used stolen or weak credentials
- 25% involved phishing
- Human error accounts for 22%
- Ransomware is found in 27% of malware incidents – up from 24% in 2019
- 18% of organisations reported a ransomware attack
- 41% of customers would stop buying from a business victim of a ransomware attack
- 9 million EasyJet customers had their data hacked
- Hacker leaks 40 million user records from Wishbone app
- There is a cyberattack every 39 seconds
- 75% of cyberattacks start with an email

[31] https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know

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

- 21% of online users are victims of hacking
- 11% of online users have been victims of data theft
- 72% of breaches target large firms
- 10% of organisations receive cryptocurrency mining malware

COVID19 and cyberattack stats[32]

- Coronavirus blamed for 238% rise in attacks on banks
- 80% of firms have seen an increase in cyberattacks
- 27% of attacks target banks or healthcare
- Cloud based attacks rose 630% between January and April 2020
- Phishing attempts rose 600% since the end of February
- Ransomware attacks rose 148% in March
- Attacks targeting home workers rose five-fold in six weeks since lockdown
- 5% of coronavirus-related domains deemed suspicious
- Visits to hacker websites and forums rose 66% in March
- Average ransomware payment rose 33% to $111,605, compared to Q4 2019
- EventBot, identified in March, has targeted 200 banking and money transfer apps

10.3. Cyber Incidents on Financial Infrastructures

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

10.3.1. EasyJet data breach

Date reported: May 2020

Date discovered: May 2020

Date of incident: April 2020

Links:

https://www.theguardian.com/business/2020/may/19/easyjet-cyber-attack-customers-details-credit-card

https://www.cybersecurity-insiders.com/cyber-attack-on-easyjet-will-fetch-18-billion-compensation-to-customers/

https://www.independent.co.uk/travel/news-and-advice/easyjet-data-hack-news-cyber-attack-passengers-personal-information-a9522241.html

https://www.bbc.com/news/technology-52722626

Who was affected?

Approximately nine million customers.

What was compromised?

It said email addresses and travel details had been stolen and that 2,208 customers had also had their credit and debit card details "accessed".

Costs of the breach?

[32] https://www.fintechnews.org/the-2020-cybersecurity-stats-you-need-to-know

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

It is estimated that cyberattack on EasyJet will fetch £18 Billion compensation to customers.

How?

In a statement by EasyJet they said "This was a highly sophisticated attacker. It took time to understand the scope of the attack and to identify who had been impacted".

10.3.2. 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 tokenised data remained protected, the encrypted data could be decrypted.

10.3.3. 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

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

Who was affected?

According to Desjardins Group around 2.9 millions 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.

10.3.4. 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?

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

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.

10.3.5. Westpac data breach

Date reported: 3. June 2019

Date discovered: 22. May 2019

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

Links:

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 confirm 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.

10.3.6. 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/

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://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.

10.3.7. 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?

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 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.

10.3.8. 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.

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

10.3.9. 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
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.

10.3.10. 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?

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 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.

10.3.11. 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.

10.3.12. Korea Credit Bureau data breach

Date reported: 20. January 2014

Date discovered: unknown

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

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?

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

What was compromised?

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.

Costs of the breach?

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.

How?

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.

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. AI, Machine Learning Technologies, Blacklisting, Anomaly Detection, Flow Modelling

Intro

This chapter lists state-of-the-art of artificial intelligence and machine learning technologies, and their application blacklisting, anomaly detection and flow modelling in Fintech domain.

Critical-Chains relevance

Analysis presented in this chapter is taken into account in Critical-Chains in preselecting optimal techniques for fraud detection in FMaaS component.

2020 update

This chapter includes an update on related work within this field, including additional methods categorisation.

FinTech – Financial Technology, refers to the financial technology sectors in a wide range of operations for enterprises or organisations, 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, FinTech 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 FinTech 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 FinTech 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. FinTech services, as any IT service, can be target for different types of random cyberattacks.

Additionally, due to its nature, FinTech services are especially targeted by various fraudulent activities, that often originates from legitimate or legitimate-like sources. Classic IDS – Intrusion Detection Systems, have a lot of limitations when it comes to detection of these types of 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

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

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[33].

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[34] 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).

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)).

11.1. 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.

[33] https://cwe.mitre.org/cwraf/
[34] 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

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.

11.2. Intrusion detection

Artificial Intelligence in general, and specifically machine learning and anomaly detection, are considered as promising techniques for intrusion detection in FinTech 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 4 shows an example of questions of interest in Critical-Chains, and a technology type that can potentially be used as a solution.

Table 4. 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 categorised 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

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

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, A survey of anomaly detection techniques in financial domain 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 normalisation and different sources of diversity.

11.3. Related Work

The literature analysis presented in this section is to support the mapping of the potential research directions and open issues.

In general, one of the greatest challenges for fraud detection represents the fact that it requires real-time processing. In general, the accuracy of manual fraud detection techniques is relatively low. Also, it requires many resources with regard to time and resources to identify common fraud patterns. Another challenge represents the fact that profiles of common and fraudulent behaviours are subject to constant changes. In addition to that, existing information about frauds is often skewed and cannot be relied on. Therefore, the performance of fraud detection depends, among others, on the sampling approach and selection of the dataset, as well as the applied detection techniques.

There are several survey papers covering this topic and providing very good insight into current trends. Ahmed et al. (Ahmed, Mahmood and Islam, A survey of anomaly detection techniques in financial domain 2016) survey provides an overview of anomaly detection methods, specifically clustering algorithms, in financial domain, and a review of anomaly detection methods application on big data in financial markets (Ahmed, Choudhury and Uddin, Anomaly detection on big data in financial markets 2017). 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 FinTech 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.

Various ML methods are proposed in literature, and they can be categorised to - general ML methods, graph-based methods, outlier detection methods and deep learning methods.

General ML methods and graph-based methods are proposed in numerous publications. 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. Bhattacharyya et al. (Bhattacharyya, et al. 2011) propose a comparison results of applying SVM, random forest, and logistic regressions to a credit card fraud detection. Glancy and Yadav (Glancy and Yadav 2011) and Torgo and Lopes

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

(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. Pham and Lee (Lee 2016) apply ML techniques to detect suspicious users and transactions in financial networks. Specifically, they apply k-means clustering, Mahalanobis distance as well as unsupervised Support Vector Machine (SVM). The approach is demonstrated on two case studies from a Bitcoin framework with promising initial results.

Another paper that discusses calibrated probabilities is described by Bahnsen et al. (Bahnsen, Aouada und Ottersten 2014). In this case, two different methods for calibrating probabilities are evaluated and analyzed in the context of credit card fraud detection. The goal of the approach is to find a model that minimizes fraud-caused impact. After calibrating probabilities, the authors apply Bayes minimum risk classifier to reduce the risk of such impacts. Finally, they claim that this method outperforms traditional ML techniques, which often rely on raw probabilities and fixed thresholds.

Mogomedov et al. (Magomedov, et al. 2018) proposed anomaly detection method in fraud management based on machine learning and graph databases. Huang, et al. (Huang, et al. 2018) address fraud detection in financial transactions with focus on money laundering. They introduce a detection framework, called CoDetect, that analyses a network, i.e. its entities and transactions, and subsequently detects frauds and feature patterns. CoDetect applies a Graph mining approach for different real-world fraud scenarios.

Ostapowicz and Zbikowski (Żbikowski 2019) apply supervised learning techniques to detect fraudulent accounts on blockchain. The authors compare models like Random Forests, SVM and XGBoost classifiers to identify suspicious accounts. Monamo, Marivate and Twala (Monamo, Marivate und Twala 2016) use a trimmed k-means unsupervised learning mechanism for anomaly detection in a bitcoin network. This method is able of simultaneous object clustering, thus achieving positive results for fraud detection in such transactions. Other general discussions about the use of ML for fraud detection in financial transactions are described by Amarasinghe et al. (Amarasinghe, Aponso und Krishnarajah 2018) and Awoyemi et al. (Awoyemi, Adetunmbi und Oluwadare 2017), respectively.

Dal Pozzolo et al. (Dal Pozzolo, et al. 2015) analyze how undersampling affects the posterior probability of a ML model. They elaborate their experiment on a real-world dataset composed of credit card transactions. It contains, among others, online transactions as a highly unbalanced dataset. The applied technique can produce well-calibrated classifiers that play an important role for fraud detection. The same group of authors published several papers within this domain, and tested application of different ML and DL techniques for fraud credit-card fraud detection (Dal Pozzolo, Boracchi, et al., Credit card fraud detection and concept-drift adaptation with delayed supervised information 2015) (Dal Pozzolo, Boracchi, et al., Credit card fraud detection: a realistic modeling and a novel learning strategy 2017) (Carcillo, Dal Pozzolo, et al. 2018) (Carcillo, Le Borgne, et al. 2018) (Lebichot, et al. 2019).

More recent approaches focus mostly on outlier detection methods and deep learning. La and Kim (La and Kim 2018) proposed a comprehensive framework for managing FinTech transactions which utilizes machine learning-based intelligence in deriving anomaly detection models and adaptive FinTech security provision. The paper from Chalapathy and Chawla (Chawla 2019) discusses Deep Learning for inspection of credit card transactions. In fact, the lack of consistent patterns represents the biggest challenge for this type of fraud. For this sake, techniques from Deep Anomaly Detection (DAD) are used to track the user's profiles and behavior for deviations.

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

Anomalous behavior in data flows is investigated by applying Group anomaly detection (GAD). GAD puts an emphasis on irregular group distributions by investigating collections of individual data points.

Podgorelec et al. (Podgorelec, Turkanović und Karakatič 2020) focus on frauds in blockchain transactions by introducing ML-based signing and information monitoring. For this sake, they apply Isolation Forest, an unsupervised anomaly detection method. The technique simplifies the digital signing process by automatically executing the process. An anomaly detection model is created, which is used further to evaluate transactions for anomalies. Subsequently, this personalised anomaly detection process tracks transactions for individual user profiles. Local Outlier Factor was proposed for credit card fraud detection by Tripathi et al. (Tripathi, et al. 2018) and by Mishra and Chawla (Mishra and Chawla 2019). In addition to LOF John and Naaz (John and Naaz 2019) propose Isolation Forest for credit card fraud detection.

Different types of AutoEncoders (Chandradeva, Jayasooriya and Aponso 2019) (Misra, et al. 2020) were also extensively researched in literature. Vynokurova et al. (Vynokurova, et al. 2020) proposes Wavelet-Neuro AutoEncoder for fraud detection, Li et al. (Li, et al. 2019) proposes spectral AutoEncoder, and Schreyer et al. proposes Vector Quantised Autoencoder Neural Networks.

LSTM is also one of most recently studied methods within FinTech domain. (Alghofaili, Albattah and Rassam 2020) (Bao, Yue and Rao 2017) (Heryadi and Warnars 2017) (A. Singh 2017)

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.

Table 5 Related work overview

Category	Methods	References
General ML	SVM Random Forest k-means ANN Logistic regression	(Le Khac and Kechadi 2010) (Chang and Chang 2010) (Bhattacharyya, et al. 2011) (Torgo and Lopes 2011) (Glancy and Yadav 2011) (Behera and Panigrahi 2015) (Sahin and Duman 2011) (Yaram 2016) (Lee 2016) (Monamo, Marivate und Twala 2016) (Awoyemi, Adetunmbi und Oluwadare 2017) (Żbikowski 2019) (Dal Pozzolo, et al. 2015)…
Outlier detection	LOF Isolation Forest	(Podgorelec, Turkanović und Karakatič 2020) (Tripathi, et al. 2018) (Mishra and Chawla 2019) (John and Naaz 2019)
Deep Learning	Autoencoders LSTM	(Chawla 2019) (Chandradeva, Jayasooriya and Aponso 2019) (Misra, et al. 2020) (Vynokurova, et al. 2020) (Li, et al. 2019) (Bao, Yue and Rao 2017) (Heryadi and Warnars 2017) (A. Singh 2017) (Alghofaili, Albattah and Rassam 2020)

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

12. Ontological Domain State-of-the-Art – 2020 insights

Intro

This chapter provides an ontological domain analysis and state-of-the-art of cyber-physical privacy-security ontology semantic modelling framework.

Critical-Chains relevance

Analysis presented in this chapter is taken into account in Critical-Chains in defining methodology and KPI assessment framework, and in security/privacy threat semantic modelling.

2020 update

This chapter is added to D2.2 presenting the additional insights obtained during project work in the last year.

12.1. Analysis of the Emerging Needs of the Fintech

12.1.1. Stakeholder Gaps

The Fintech has experienced a deep transformation with new services that are taking place on a global scale. There is a big gap in the Fintech market from Stakeholder's point of view. The services that are available in the Fintech market do not provide a neutral environment with the user's multiple financial services. Many stakeholders need is to see all their financial products in a unique frame to analyse their customer's behaviour together and track their company's financial status. This unique speciality could adapt stakeholders to new Fintech services easier and it will lower the marketing barrier to small service providers as well.

The research study carried out by an antivirus firm called Bitdefender indicates that financial sector companies face 300 times more cyber-attacks compared to other industries. Sometimes, a new technology comes with risks in terms of ease of use. Particularly the financial services involve storing customers' data and regulators are very concerned about the security in this topic. Therefore, Fintech companies should handle these kinds of attacks in order to provide the needed security to protect this critical information. Cyber-attacks not only endanger banks, but it is also putting in risk any other sector companies. As a result, new security approaches are needed, and the current ones need to be updated.

Although Fintech services usage has recently risen, there is another data privacy issue that concerns stakeholders, sharing customer's data with non-financial companies. It is very hard for financial authorities to develop regulatory responses to assist innovation and provide safe financial systems. Many policymakers examine closely Fintech developments and their impacts on markets. To assist this process, Centre for Latin American Monetary Studies (CEMLA) established the Fintech Forum made of 18 Latin American and Caribbean (LAC) Central Banks that launched a stream of work to analyse Fintech regulatory aspects in the region and created a task force, known as the REG WG.

Even though there are no Fintech laws that define the different aspects of operating as a Fintech company, there are many regulations that affect Fintech companies. For example, there is a regulation that defines Payment Services that is applied for Fintech companies to focus on payments. However, for analysing the market and regulations, regulators need access to actual transactional need. For instance, in Turkey, there is a Law 6493 which focus on Payment Services indicated below.

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

Law no. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions Article 12 as:

> 1. All the transactions required for operating a payment account including the services enabling cash to be placed on and withdrawn from a payment account,
>
> 2. Execution of payment transactions, including the transfer of funds on a payment account with the user's payment service provider, direct debits, including one-off direct debits, payment transactions through a payment card or a similar device, credit transfers including standing orders,
>
> 3. Issuing or acquiring payment instruments,
>
> 4. Money remittance,
>
> 5. Execution of payment transaction, where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT devise and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services,
>
> 6. Corresponding services enabling bill payments.

If any operation of the Fintech Company falls into any of these explanations, the license from BRSA (Banking Regulation and Supervision Agency) will be required. Since many Fintech companies do not fit in any of the categories that are mentioned above, Fintech services and the risks and benefits associated with them.

Moreover, as traditional banks are heavily regulated, most of the new Fintech companies start without all the licenses, they acquire them in later phases. Acquiring licenses is a high cost for a young company and regulations can be changed at any time.

Central banks need to balance the money supply and demand in more challenging situations than before. More transactional data is needed for this and Fintech companies can provide it. Blockchain-based currencies and services can provide visibility to central banks.

Large financial institutions have had strong trust between them. With small competitive Fintech companies, we must discover new trust-building tools, environments and motivations. Much more trust is needed to operate the markets tomorrow.

Most of the Fintech operations are based on cloud environments that bring the needed flexibility and cost-effectiveness. Cloud services require you to trust a cloud service provider (CSP). The data is only as secure as the CSP – and cloud service providers do not always give all the levers needed to understand and manage the security (confidentiality and integrity) of data and processes. Cloud services are also exposed to insider threats from CSP's employees and contractors. Furthermore, commercial CSPs can be a subject to extraterritorial legal mandates (e.g. law enforcement data access requests from foreign countries) or conflicting commercial incentives (to monetize data in other ways or gain competitive insight into how your business functions).

Cloud services have unique security vulnerabilities, such as multi-tenancy issues and malicious hypervisor attacks and suffer from the same security issues as self-provisioned IT services. Major cloud services pose an attractive target for attackers – a security exploit can give global access to many high-value customers – and both nation-state and criminal hackers are paying growing attention to commercial cloud services. Even when cloud services are secure, misconfigurations and administrative errors frequently create security holes. With the growing complexity and virtualisation of cloud architectures, this problem is getting worse.

A growing list of horizontal and sectoral regulations means compliance, certification, auditing and reporting to a growing list of different government and private bodies that means an immense cost. Governments are risk-

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

averse when it comes to information security. They need to ensure absolute sovereignty over their data. Failing this mandate is not just a business risk but a failure of one of its main tasks as a government. Data protection law alone is not enough fall back – e.g. there are exceptions for national security, which is precisely the area that every government must address. For public services, government bodies have an extra layer of administrative law that often imposes further restrictions on how data can be processed. Guidelines on individual information systems are often written into law. Governments' agencies also face transparency and oversight mandates that need third-party auditing. "Government" is not one enterprise, but a series of agencies and bodies with their own mandates and sometimes conflicting agendas. Making a single whole-of-government approach to IT systems is difficult. Governments also need to take particular care to avoid lock-in or dependence on a single source of cloud services. Governments must provide "universal service", which means they face additional difficulties in jettisoning old legacy systems or standardizing processes on a single platform.

Over the last decade, the paradigm for cybersecurity has been largely perimeter control, signature-based heuristics and AI probabilistically making assertions of potential compromise. This approach breaks down in the era of cloud and edge/IoT – services are running on someone else's infrastructure, so there is no perimeter to protect. Security and audit costs have also skyrocketed, especially in the log ingestion and analysis space. Vendors typically charge by the number of logs stored, which means escalating costs with growing data volumes. Log analysis cannot be fully automated, which means expensive security teams in the private sector and – frequently – nothing at all in the public sector. And breaches are detected weeks or months after they occur, leaving it too late to act. Regulators have supported new cloud security standards and certifications, but these are static check-boxing exercises that confirm the compliance of cloud service at the point of audit (e.g. once a year), but do not provide ongoing compliance for platforms and services that are constantly renewing and updating.

12.1.2. Consumer Gaps

Incumbents of Fintech have realised that existing and emerging enabling technologies, mobile and cloud are importantly changing customer's expectations. However, Fintech is not taking advantage of these customer's expectations because it is difficult to adapt legacy systems. Therefore, there is new kind of services that Fintech provides such as transactional offerings payments, loans and investments.

Many Fintech incumbents face with trust issues from the consumers perfective. Interviews show that customers do not trust Fintech operations to take loans or transactional operations as they trust payments. Fintech companies have been developing services to provide great value to customers. These services are mainly based on electronic services such as e-invoice, e-payments and e-government services. These new services' purposes raise awareness and gain customer trust by providing campaigns according to their monthly behaviours' analyses.

Not all companies are aware of Fintech technologies. They are called non-adapters; non-adapters lack of awareness that decreases consumer awareness as well. These types of companies believe that traditional methods work, and they believe they are more secure compared to Fintech services or products. However, with regulations, policies, and actions taken that companies from different sectors' awareness increased. The customer has begun to realize that Fintech services and products are secure and friendly and non-adapter companies have begun to shift new technology areas. As the gaps in the Fintech area are met, non-adapter companies started to use new products, so the customer awareness has risen. To completely have the full achievement of these gaps in the banking Fintech sector customer side should be concerned. Consumers need transparent platforms for benchmarking and comparison.

12.1.3. Fintech Metrics

The SWOT (Strengths, Weakness, Opportunities and Threats) of Fintech from Customer and Stakeholders perfectives is presented below. As seen, there are many strengths and opportunities for the Fintech sector.

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

However, weaknesses and threats are very important as well. Innovations like Critical-Chains project will try to fulfil the gaps in the Fintech sector in order to reduce weaknesses and threats.

Trust in the digital domain needs specific tools and education to expand its impact. Trustful institutions can lend it to start benchmarking Fintech services. Digital services can support the processes. Transparency and comparison between the different security options will build more trust. It is good to know how new Fintech services are compared to traditional bank services. Knowledgeable risk-taking can be a much better alternative than monopoly offering.

When Fintech companies are organised and use similar technologies, they can achieve better results regarding regulation changes. It is easy to argue against a small company from status quo point, but it is much more demanding to do it against an important amount of companies who can offer more to consumers. Life changes and our tools must change with it. The next steps will define specific success metrics to achieve the business models that can be more sustainable in the Fintech domain.

These are examples of metrics: Fintech company rating (1-10); process descriptions available (n); data leaks per year (n); capital (EUR); turnover growth (EUR); customers per year (n); regulations adapted (y/n).

Figure 21: SWOT Analysis of Fintech

12.2. Cyber-Physical Privacy-Security Ontology Semantic Modelling Framework State-of-the-art

12.2.1. Data Representation Model

Triple-based data representation models have received significant attention in research and development communities and triple-based models in particular have been deployed in real-world systems. Triple-based representation models organise data in the form of triplets, each consisting of subject, predicate and object. Commonly used triple representation models combine such subject-predicate-object associations and unique identifiers for each element participating in a triple aspect data representation. Triple representations have seen significant adoption as part of data exchange formats such as the Resource Description Framework (RDF) as is

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

described in this chapter. This representation model differs somewhat from the tuple model of representation used in relational databases such as SQL databases. Fundamentally, such databases describe information about a uniquely identified element by means of a tuple, which is a uniquely identified row in a table with a set of attribute values defined by the columns of the table. Relationships between multiple tables are defined by referencing unique tuple identifiers.

12.2.2. Domain Representation Ontology

A decision to use a simple and flexible model for the representation of information such as triples makes even more important the general requirement to formally represent the domain under consideration. Ontological representations are well-suited for this task in the case of Critical-Chains. A frequently cited basic definition of an ontology is that an ontology is a "formal, explicit specification of a shared conceptualisation" (Gruber 1993). An ontology for Critical-Chains should describe the relevant concepts for the domain and the relevant relationships between the identified concepts. The concepts and relationships that are used in the data that is ingested into the data representation subsystem should be contained in the ontology so that the domain knowledge encoded in the ontology can be utilised when interacting with the data representation subsystems.

12.2.3. The Critical-Chains Privacy-Security Protection Data Modelling (Entities, Attributes and Relations)

This model has to describe the key entities and relationship types relevant to the data flows and the privacy-security threats analysis to support a threat-driven risk-based privacy-security-by design approach. This begins with a top-down identification of relevant entities in the domain. The identified entities should be general to the extent that they can be used as top-level entities for the domain ontologies. As a next phase real-world example data and data extracted from usage scenarios are used together with available documentation of the relevant terminologies and processes to create an ontology that is populated with the elements identified in the Critical-Chains prototypical data sources such as financial transaction data. Once this process is completed, the extended ontology is examined and may be restructured to improve the overall representation; this process should involve data that was not used to create the ontology instance in order to identify problems with the ontology elements and their organisation.

Entity Types

The initial definition of entity types for Critical-Chains is based upon two main concepts that need to be captured and represented in the system: events and actor-actor relationships. Events Data such as transactions data will represent the bulk amount of information input to the data analytics. Actor-Actor relationships are the relationships of interest for analysis and audit of financial flows and access control policies. It is envisaged that mediated actor-actor relationships can also be of interest whereby actors can be connected via elements which may themselves be represented as nodes in a network, or as connections between actors as in cascaded flows that are variously correlated and prime facie co-implicated in orchestrated financial transactions which may be anomalous or indeed fraudulent as in any form of trafficking including money laundering

Actor

An actor is a human or a group of humans; a group actor is composed of a set of actors, which themselves may be groups of actors. Basic subtypes of actor to be modelled in the data model include e.g. account holder, funds-sender, funds-receiver, Properties include person names, account history, funds transfer profile, etc.

Object

An object is a non-human entity that can be uniquely identified either in the physical or virtual sphere and that itself can be characterised via properties. Relevant objects include a mobile client device and properties may be biometric sensor type, OS type, available encryption etc.

Place

A place is a real-world or virtual location that can be uniquely identified and bounded by soft or hard boundaries in the respective space, e.g. a trust boundary where a financial transaction is initiated such as the we-page (place)

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

within a certain open bank portal (space) and an example of property may be any relevant security –privacy context qualifier of a place e.g. the communication channel that the place has available and the abstraction in turn of the security and privacy safeguards of such communication channel (data transmission modalities, wireless/wired, protocols, encryption etc.

Event

An event is an observable activity that can be observed at a specific point in time or over a specific period of time. This would include the classes of events that will be identified by the data analysis components to be developed within Critical-Chains e.g. Data transaction events of which a regular and normal transaction is one type and an (ir)regular or anomalous transaction would be the other type; event properties would be e.g. Time , location (place, space)

Context

Context is an ancillary condition or property that cannot feasibly be modelled as bound to one of the other defined basic entity types. Context classes will include conditions such as a particular set of conditions being co-present or co-absent relating to groups entities and/or persons who may or may not be directly involved in an activity e.g. a particular topology of relationships between co-implicated individuals and/or any funds transfer that they were involved in.

Relations

Relations in the Critical-Chain Data Model connect entities and are generally directional including multi-valued directionality as in bi-directional or star they thus create a directed graph.

Properties

Property relations more closely describe an entity. This can include permanent properties such as the geo-location of a bank hosting a customer account as well as transient properties such as the volumes or periodicity of fund transfer events in general and/or in relation to any co-respondents

Activities

Activities are usually carried out by actors. Activity relationships connect entities in a subject-proposition-object relationship that does not indicate a subordinate property of the subject entity.

Roles/Responsibilities

Roles connect entities with other entities in a relatively time-stable manner. Roles identify functional relationships of actors and objects usually with respect to an event.

12.2.4. Data Representation Formats

This section briefly discusses candidate data representation formats for

- the exchange of data between the data representation subsystem and the other subsystems within Critical-Chains
- the ontological representation of ingested data,
- querying the data representation subsystem and
- creating rules that can be processed within the data representation subsystem.

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

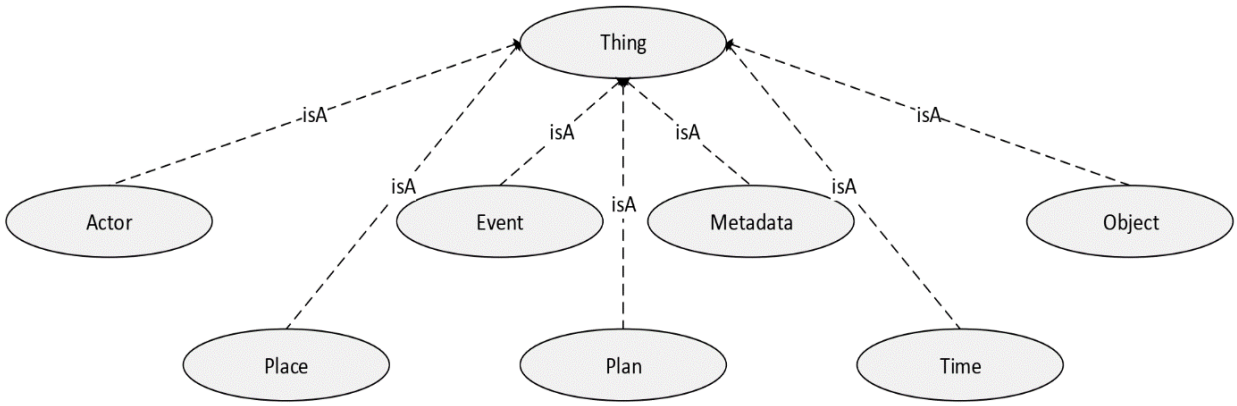

Figure 24: Data Representation Formats

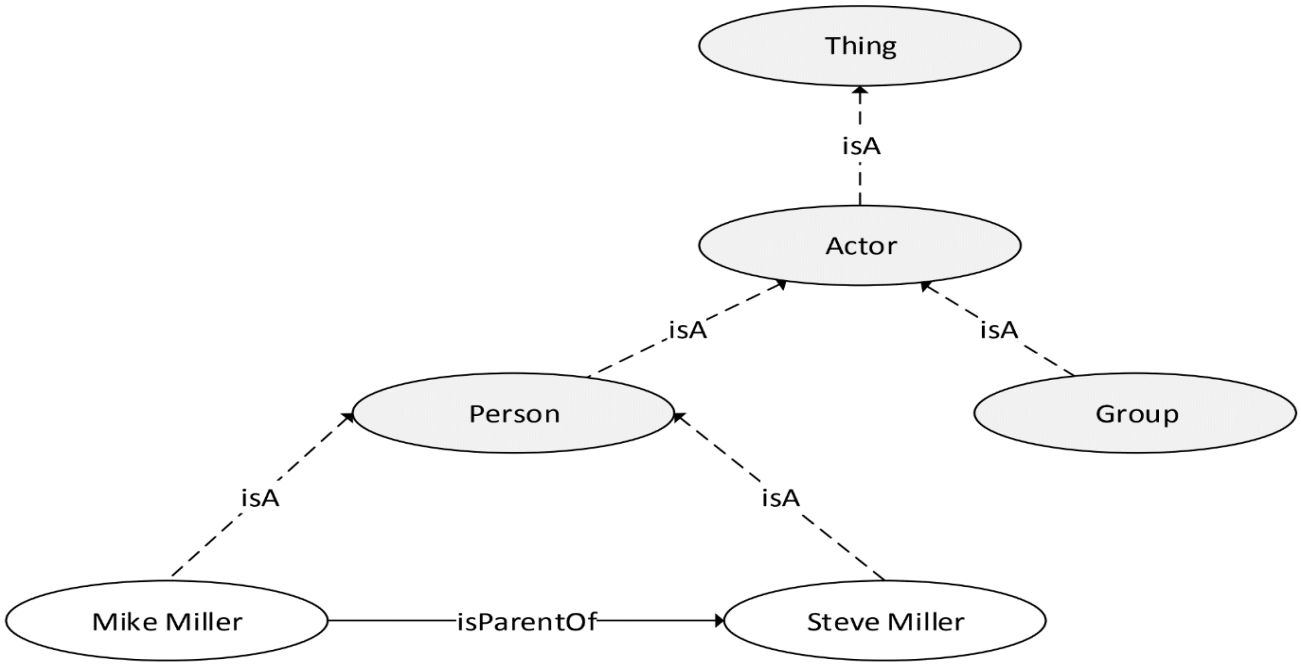

Figure 24: Illustrating domain ontology and an example of entity classes relationships

Resource Description Framework

The Resource Description Framework (RDF) (RDF Working Group 2010) is a group of specifications for the representation and description of entities and relationships between entities. RDF representations are intended to be machine-processable and as such require a minimum degree of formal specificity. RDF is based around the concept of triples that describe a subject, an object and a (typed) predicate/relation between the two. It is frequently referred to as one of the key formats used for describing concepts and relationships in the Semantic Web. RDF generally describes data in the form of triples and a set of RDF triples with partially overlapping subjects and/or objects forms a multi-graph with directed and labelled edges as shown in Figure above. Since RDF is usually used on the World Wide Web, unique identifiers that may be required for instances described in RDF are commonly defined in the form of URIs/URLs (or “web addresses”), but it is not required in all instances to provide unique identifiers for RDF subjects, predicates or objects in the form of URIs, when constant values, or “literals” in RDF terminology, are used.

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 RDF specifications are not strictly bound to a specific notation format. Representation formats of RDF data include RDF/XML (the recommended RDF XML serialisation format), Turtle notation, RDF/a notation and N3 notation. The example below, adopted from (Manola and Miller 2004), provides information on the unique identifier for the creator, a literal creation date and a literal for the language of a Web resource in RDF/XML

```
<?xml version="1.0"?>

<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:dc="http://purl.org/dc/elements/1.1/"
         xmlns:exterms="http://www.example.org/terms/">

<rdf:Description rdf:about="http://www.example.org/index.html"> <exterms:creation-date>August 16,
         1999</exterms:creation-date> <dc:language>en</dc:language>
```

format:

The RDF specifications describe the format in considerable detail and the specification contain a range of formalisms that can be used to reduce the complexity of RDF. It will be necessary to adapt and integrate an appropriate name space for data description consistent with RDF. Further information on RDF can be found under RDF Working Group (RDF Working Group 2010); and a tutorial on the principles and representation formats for RDF under Manola et al (Manola and Miller 2004).

RDF Vocabulary Description Language

The RDF Vocabulary Description Language (or RDF Schema, RDFS) provides a means for defining vocabularies and ontologies for RDF instances in an RDF format. RDFS defines the fundamental elements that are required for RDF vocabularies and for the description of ontologies (Brickley and Guha n.d.). Effectively, RDFS is used to define a format to be applied in RDF resources that reference that specific RDF schema. As the name RDF Schema implies, RDFS aims to fulfil a similar role relative to RDF as XML Schema does for XML documents – to define types and elements that can be used in document instances that are created based on a defined schema definition.

RDFS can be used to simplify the description of resource relations for use in ontology and/or RDF vocabulary descriptions. Further information on RDFS can be found under Brickley and Guha (Brickley and Guha n.d.);

Tutorial information on RDFS is also contained in the general RDF tutorial available under Manola and Miller (Manola and Miller 2004). One of the advantages of using RDFS is that it can be queried easily when using the SPARQL query language as described in (W3C Consortium 2004) (Prdu'hommeaux and Seabone 2008) (McCarthy 2005).

Web Ontology Language

The Web Ontology Language (OWL) (Apache Software Foundation 2012) (Smith, Welty and McGuiness n.d.) refers to a group of language variants that are specifically designed for representing ontologies. To achieve this, OWL relies on RDF Schemas. When comparing OWL and RDFS, OWL variants permit developers to express more complex properties and relationships than basic RDFS is capable of (W3C Consortium 2004). The OWL 1 specification describes three variants of OWL (W3C OWL Working Group 2009): OWL Lite, OWL DL and OWL Full. OWL DL is an extension of the more basic OWL Lite, and OWL Full is an extension of the more specific OWL DL variant, so that ontologies defined in the "more basic" (W3C OWL Working Group 2009) variants are valid for the more complete or more general variants:

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

- OWL Lite provides limited expressiveness and is not widely used; hence it is unsuitable for use in the CRITICAL-CHAINS project.
- OWL DL, where the appended "DL" is intended to indicate a relation to "description logic", aims at providing expressiveness while maintaining completeness and decidability from a propositional logic perspective. OWL DL has been developed to offer a highly expressive language while at the same time remaining computationally complete and decidable with practically useable reasoning algorithms.
- OWL Full uses different semantics than OWL DL (and OWL Lite) and provides a degree of compatibility with RDF. It can also be used to augment predefined vocabularies.

OWL 2 profiles restrict how terms can be used and which types of inferences are to be expected.

The following profiles are currently defined (W3C Consortium 2004):

- OWL 2 EL aims to enable classification and instance queries that can be executed in polynomial type;
- OWL 2 QL aims to enable rewriting of queries to relation database query formats, in particular SQL;
- OWL 2 RL aims to enable reasoning with rule engines in polynomial type

The references to OWL in this document refer to the 2009 "OWL 2" specification unless explicitly stated otherwise. Restrictions defined in OWL 2 profiles each exclude a number of specific features of OWL DL and/or OWL Full to achieve their respective goals. A general strength of OWL representations is the support for sophisticated representation combined with the ability to apply well-known reasoning algorithms on the represented ontologies. Examples and basic definitions of several OWL syntax formats can be found in Hitzler et al (Herman 2012).

Rule Interchange Format

The Rule Interchange Format (RIF) (McGuiness and van Harmelen n.d.) (W3C Consortium 2004) has been proposed as a framework for using rules in the Semantic Web. RIF specifies an XML language for expressing rules and can interoperate with SPARQL to some extent and with RDF and OWL to a larger extent. RIF is not a specific rule language designed for use with a particular rule engine implementation. RIF would be useful desirable to carry out reasoning directly on the data representation subsystem database instead of first execution queries to retrieve data and then processing the retrieved data with rules in an external system.

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

12.2.5. Overview of Most Common Ontology Development Errors explained by examples

In setting out an ontology for a domain, given the objective, the motivation for an ontology must be to support standardisation, computational inferences and reasoning. Then the class structuring has to enable correct object-oriented abstraction, subsumption and therefore correct inheritance. Fundamental to ontological commitment is set-theoretic membership of data types so it is important to avoid mixing

- data of different types in subsumption lines
    - mixing up the ***Mention*** and ***Use*** of an entity
    - mixing type of an instance of which also should not happen in an ontology.

- An entity “play” is a data structure, taken as an OWL Thing; but then a person can (go) see a play which would be of a *period-in-history*, have a *location/space/price/cast/chorus/set/genre* etc.
- Anyhow here is the list of most common errors with more examples
- **Failure to distinguish** between *an instance-of relationship* and a *subclass-of relationship*. "John" is an instance of Mammal. Human is a subclass of Mammal.
- **Failure to distinguish** *part-of* from *subclass-of.* A wheel is a part of a car, not a more specific type of car. An opening argument by a trial lawyer is part of a criminal legal proceeding, not a specific type of criminal legal proceeding. This error is surprisingly common in OWL since it has a convenient "rdf:type" relationship, but not a corresponding one for part-of.
- **Modelling *events* as *relations:*** One can see this occasionally in the linguistics literature. (eats Joe CheeseSandwich) looks simple and convenient, but if one then wants to say when the eating happened, there is a problem. The typical solution is to say (occurs Monday (eats Joe CheeseSandwich)), However most languages that can permit some inferences, e.g. OWL, exclude statements as arguments to relations as this makes for reasoning difficulties
- **Ontological Liberalism** (No “Occam’s Razor”): Each term has to earn its rent in an ontology and not just be added liberally. Ontology elements must be distinctive from each other according to the principle of necessity and sufficiency and standardisation of expressiveness of the ontology.
- Modelling roles as classes. Manager is a role. Human is a class. If we define "Joe as a manager" or (instance Joe Manager), then what if Joe were to change his role over time?

Classified Description of Ontology Errors

1) **Synonyms as classes -** creating several classes whose identifiers are synonyms and in defining them as equivalent.
2) **Label vs. Comment and other annotations** - Interchanging the contents of the annotations of the types “label” and “comment” and in not including any annotation of the type “label” and “comment”.
3) **Inverse relationships that are not inverse -** defining two relationships as inverse when, in fact, they are not.
4) **Undefined inverse relationships** - having inverse relationships in the ontology, but they are not defined as such.
5) **Recursive definition** - an ontology element in its own definition.
6) **Multiple classes in domains and/or ranges of relationships and/or attributes** defining the ranges and/or domains of the relationships and/or attributes by intersecting several classes in cases in which they should be the union of such classes.

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

7) **Polysemy** - using an ontology element to represent concepts different from the domain under consideration.
8) **Same URI for different ontology elements** - Assigning the same URI to two different ontology elements.
9) **Relationship *"is"* -** Confusing the subclass relationship (*subclassOf*), the membership to a class (*instanceOf*), or the equality between instances *(sameIndividual*) with an ad hoc relation called "is".
10) **Class 2 in 1 -** Creating a class whose name is "Class1AndClass2".
11) **Classes vs. Instances -** Deepening into a hierarchy so that the more specific classes do not have instances since such classes become class instances of the upper level of the hierarchy.
12) **Relationship and/or attributes without domain or range -** Not specifying the domain or range in the relationships/attributes.
13) **Incomplete information -** Not representing all the knowledge that could be included in the ontology.
14) **Miscellaneous class -** Creating an artificial miscellaneous class to classify in a certain level the instances not belonging to any of the sibling classes of this level.

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. Privacy and Security Threat Analysis & Modelling Tools & Frameworks State-of-the-Art – 2020 insights

Intro
This chapter provides the state-of-the-art of privacy and security threat analysis & modelling tools & frameworks.

Critical-Chains relevance
Analysis presented in this chapter is taken into account in Critical-Chains in selecting the most suitable methods for security/privacy threat semantic modelling.

2020 update
This chapter is added to D2.2 presenting the additional insights obtained during project work in the last year.

Threat modelling allows discovery of potential threats and security mitigations that a given software system may be susceptible to. In essence, modelling tools and frameworks detail the ideas behind the system; which includes a catalogue of potential threats, alongside the parties that could exploit the threats, and their methods to do so.

Threats discovered during the lifecycle of a system can be very expensive to fix; so, threat modelling tools and frameworks are used to identify threats and minimize the cost to fix by discovering them early in the development cycle. Based on the needs of a project or software different modelling methods can be used. Each are somewhat specialised for each for different parts of the process and more than one method can be used to fully model all threats.

13.1. STRIDE

The STRIDE model was developed by Microsoft after it was invented by Loren Kohnfelder in 1999, making it the oldest method covered in this section. It is no longer in development or maintained anymore but is still available. While a model of the target system is being constructed, a STRIDE model can be constructed in parallel. It is the aim of this STRIDE model to provide a full breakdown of processes, trust boundaries data stores and data flows to discover potential threats.
STRIDE aims to group questions such as ‘how can an attacker change the authentication data’ and ‘what is the impact if an attacker can read the user profile data’ into six distinct threat categories (Microsoft 2009). These six categories are:

- Spoofing identity – which concerns authenticity; in particular the possibility of an attacker using stolen authentication information to gain unauthorised access to a system.

- Tampering with data – concerned with the possibility of data being tampered maliciously. Could include unauthorised changes made to data in a database, or a man in the middle attack to alter data between systems on the internet.

- Repudiation – is the concept that a user can reject the truth or an action they made as the accuser is unable to prove it. In the context of a system this could be a user making an illegal operation, which

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

admins are unable to trace. The concept of nonrepudiation is the idea of countering repudiation threats; for example, provide a receipt after a purchase or logging the actions of users.

- Information disclosure – this concerns the availability of information and the assurance that a user can only gain access to information if they have permission. Users without permission to read a file should not get access, and attackers should not be able to read confidentiality information between communicating systems.

- Denial of service- DoS attacks stop users being able to use a given service. This could be achieved by making a web server unavailable through a DDos attack.

- Elevation of privilege – this threat is concerned with the possibility of an unprivileged user gaining privileged access by an exploit or bug. As a result, the user could change, create and delete data on the system, posing a significant threat.

STRIDE models are built by detailing the system design. Data flow diagrams are built to model the proposed or current in-place system. The Data flow diagrams identify the entities, events and boundaries present in the system (Hernan, Lambert and Shostack 2006). Once modelled threats from the above mentioned 6 categories can be identified. This process can be aided by using checklists and tables that assist in explicitly describing the threats, violations, victims and attackers in a typical system (A. Shostack 2014). Once threats have been identified, mitigation strategies can be devised and then document and prioritised.

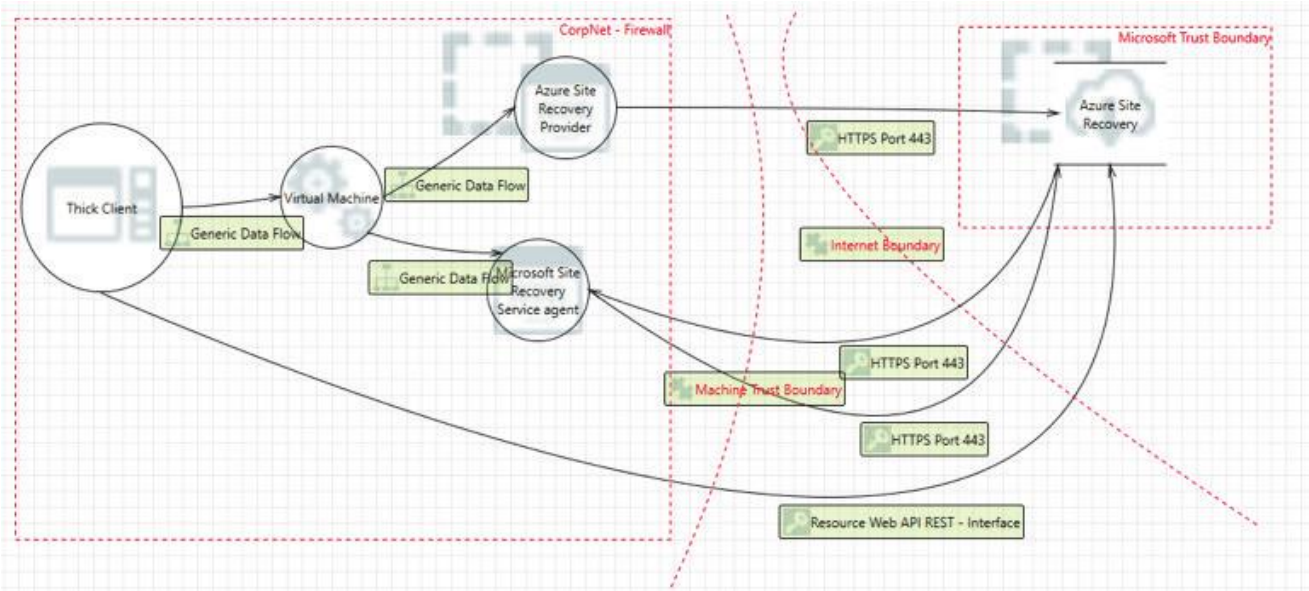

Figure 25: STRIDE model of a cloud backup service (Glowinski, Krawinkler and Gossmann 2018)

STRIDE is a relatively easy method to use however it comes at the cost of being time consuming. As a system grows in complexity the number of threats also grow rapidly too, making it an inefficient method for large systems. In addition to this it has been observed that STRIDE has a low rate of false positives in but a high rate in false negatives (Scandariato, Wuyts and Joosen 2015).

13.2. PASTA

PASTA or Process for Attack Simulation and Threat Analysis is a threat modelling framework developed in 2012. It is a risk-centric framework which aims to combine technical requirements and business objectives (Beyst 2016) that has 7 distinct stages where threats are identified, analysed and modelled; where each stage consists of multiple steps. Each stage employs different techniques to achieve their goals; such as using data flow diagrams in step 3 to decompose the application.

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

PASTA is considered a risk-centric framework as it considers input from many different key levels; such as operations, governance, architecture and development (Simeonova 2016). It provides dynamic threat identification and enumerates them to produce scores for each threat. It is the aim of this methodology to provide a view of a system from the attacker's perspective, such that an asset-centric mitigation strategy can be developed.

Figure 225: 7 stages of PASTA and their sub steps (Velez 2017)

Using PASTA has many advantages; by design it encourages stakeholders to collaboration as each step requires different stakeholders to contribute. It also contributes to the risk management of the system and also supplies built-in prioritisation of threats. However, it does require a lot of effort to fully model, but also has plenty of documentation to aid the effort.

13.3. LINDDUN

LINDDUN stands for link-ability, identifiability, non-repudiation, detectable, disclosure of information, unawareness, and non-compliance. It is focused on privacy threats surrounding data security and is analogous to STRIDE. LINDDUN intrusts the analyst on the issues that should be investigated, and where within the model those issues could appear. This is achieved first by defining a list of privacy threat types and then mapping them to elements in the system model (Wuyts, et al. 2019). The methodology consists of 6 main steps; the first three map problems to the domain of the problem space, and the final three to the domain of the solution space. These steps are defining the dataflow diagrams (DFD), mapping privacy threats to DFD elements, and identifying threat and misuse case scenarios in the problem space. Then in the solution space: prioritizing threats and risks,

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

eliciting privacy requirements and finally selecting privacy enhancing solutions. These steps are shown with their system-specific knowledge in the following figure.

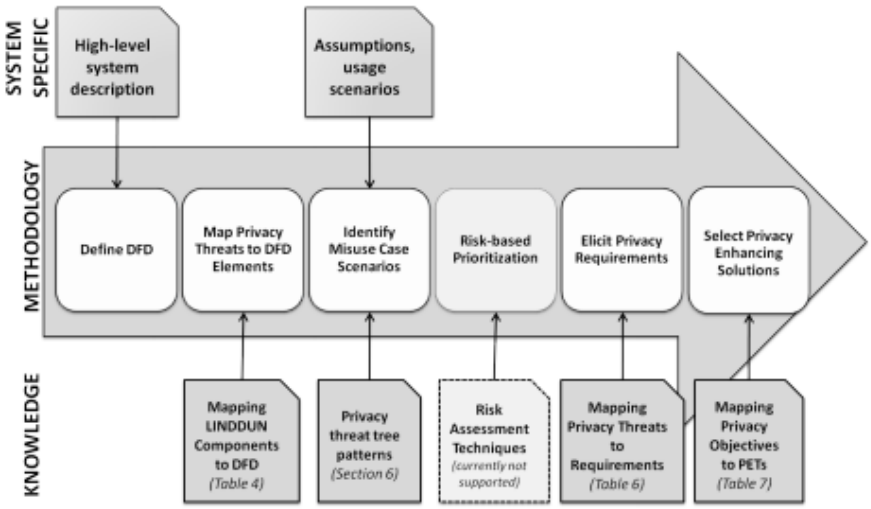

Figure 226: LINNDUN methodology and its required system-specific knowledge (Wuyts, et al. 2019)

LINNDUN is well documented and provides an extensive privacy knowledgebase although due to its similarities to STRIDE it also has the same threat scaling problem; as the complexity of a system increases the number of threats increases rapidly too. LINNDUN is quite labour intensive too, which in combination with a complex system results in a very time-consuming process to finish mapping LINDDUN. Generic applicable threats are also harmful to the efficiency and effectiveness of the method as they add more consideration to each step (Wuyts, et al. 2018).

13.4. CVSS

CVSS or Common Vulnerability Scoring System aims to 'capture the principle characteristics of a vulnerability, and produce a numerical score reflecting its severity' (FiRST n.d.). CVSS was originally invented by NIST and is now maintained by FIRST (Forum of Incident Response and Security Team). CVSS is an openly available framework that describes the characterises and severity of vulnerabilities found in software. It outputs numerical scores which indicate the severity of a vulnerability relative to others.

Vulnerabilities are scored over three metrics; base, temporal and environmental. The base score represents the severity of the vulnerability with respect to its characteristics in a worst case scenario and assume that these characteristics do not change over time. The temporal metric adjusts the base metric based on factors that change over time such as availability of the exploit or the speed at which it can be remedied. The environment metric adjusts the base and temporal metrics in regard to a specific computing environment. Factors that might change the environment metric include the presence of security controls that could mitigate the consequences of a successful attack.

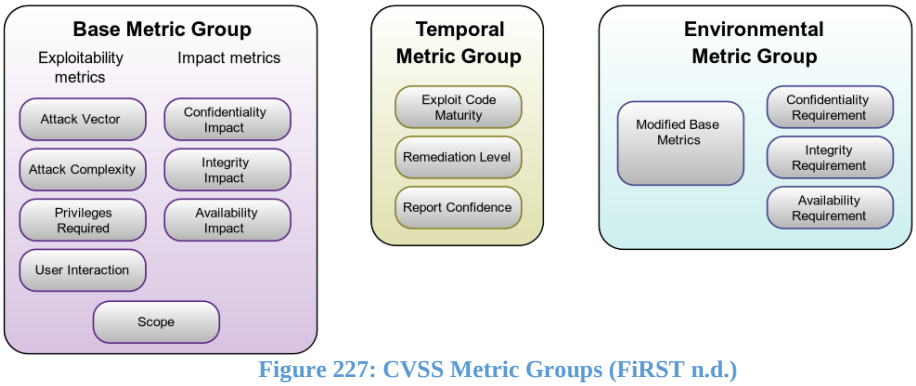

Figure 227: CVSS Metric Groups (FiRST n.d.)

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 CVSS calculator is available online, so a score can be easily computed. This makes CVSS a popular choice and is often used in conjunction with other models. However, some parties are concerned by the non-transparent score calculation process, alongside the inconsistencies that may be produced by differences in scores from different judges (Potteiger, Martins and Koutsoukos 2016).

13.5. Attack Trees

Attack trees are an old technique from 1999 but are still popular and can be applied to many types of systems. Essentially attacks are tree diagrams which depict attacks on a system. The root of the tree denotes the goal of an attack, and the leaves represent the ways in which that goal can be achieved. Each goal requires its own attack tree, so for a system to be fully represented by attack trees, many will have to be made.

An attack tree is built iteratively starting with the goal. Then leaves are added by identifying ways in which the given goal can be achieved. While adding the leaves the possibility of each attack should be considered and denoted on the leaf. It is also worth considering if special equipment is required to successfully execute an attack, as it reduces the number of potential attackers. The cost of each type of attack should also be denoted, and the low cost on a tree shows the minimum expense an attacker must pay to successfully attack the system.

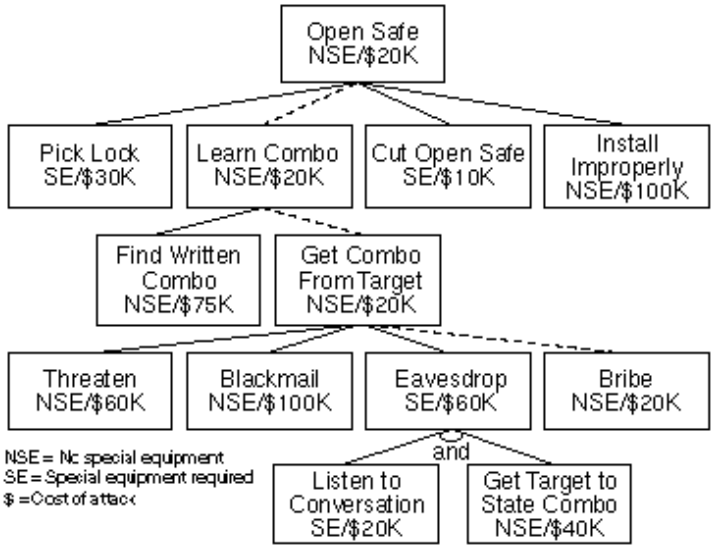

Figure 228: An Attack tree with the goal of opening a safe. Showing costs and denoting the feasibility of each way of achieving the goal (Schneier 1999)

Attack trees are commonly used in conjunction with other frameworks like STRIDE, CVSS and PASTA. They are easy to comprehend and use but require the system and its threats to already be well studied. It also assumes that the model analysts are very competent in the area of cybersecurity as it provides no additional guidelines to assess attacks and risks (Cheung 2016).

13.6. Persona non Grata

Persona non Grata or PnG is a modelling method that focuses on archetypal users who wish attack a system; by characterizing their motivations and skills. The model analysts should view and model the system from the point of view of the attackers by considering their goals and actions they may take (Cleland-Huang 2014). The output of using the PnG method is to produce multiple user profiles that detail an attacker's motivation, skills, and goals. Many different types of attackers can exist, and their goals, motivation and skills can vary; including other factors such as insider knowledge. The idea of PnG is to offer an agile approach to make attackers more traceable due to the focus on the attackers' motivations, abilities and persona while being easy to use and adopt. It has a high consistency and only produces a few false positives yet in practice PnG is barely used. This may be perhaps due to its affinity to only detect a distinct subset of threat types (Mead, Shull, et al. 2018).

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

13.7. Security Cards

Security cards is a creative method that utilises a deck of 42 cards, to help analysts brainstorm different questions and activities to identify unusual or complex attacks. The deck of cards in split into 4 archetypes of cards; human impact, adversary's motivations, adversary's resources and adversary's methods. Cards are picked from the deck and then discussion between stakeholders and analysts occurs to brainstorm new threats. These archetypes and their child cards are detailed in the below figure.

Human Impact	Adversary's Motivations	Adversary's Resources	Adversary's Methods
• the biosphere • emotional well-being • financial well-being • personal data • physical well-being • relationships • societal well-being • unusual impacts	• access or convenience • curiosity or boredom • desire or obsession • diplomacy or warfare • malice or revenge • money • politics • protection • religion • self-promotion • world view • unusual motivations	• expertise • a future world • impunity • inside capabilities • inside knowledge • money • power and influence • time • tools • unusual resources	• attack cover-up • indirect attack • manipulation or coercion • multi-phase attack • physical attack • processes • technological attack • unusual methods

Figure 29: Security card topics and activities (Shevchenko, et al. 2018)

The benefits of security cards include the increase in collaboration in stakeholders by encouraging them to brainstorm, the variety of threat types identified and identification of unusual threats that may not normally be considered. However, it comes at the cost of leading to many false positives and may be better suited to non-industrial uses as it is rarely used (Mead, Shull, et al. 2018).

13.8. hTMM

hTMM or Hybrid Threat Modelling Method was recently developed in 2018 by the Software Engineering Institute. It combines a mix of other methods including PnG and Security cards and another method called SQUARE (Security Quality Requirements Engineering Method) (Mead, Hough and Stehney, Security Quality Requirements Engineering Technical Report 2005).
The steps of hTMM can be summarised to:

- Choosing the system that should be threat-modelled
- Use security cards to identify many threat types and attack profiles
- Remove unlikely attack profiles or threats (false positives) from previous steps
- Summarize results using a tool
- Apply a formal risk assessment method

The advantages of using hTMM include no missed threats, no false positives, cost-effectiveness and consistent results independent of the individual undertaking the threat modelling given it is repeated.

13.9. Quantitative Threat Modelling Method

Quantitative Threat Modelling (QTMM) is another hybrid method that combines attack trees, STRIDE and CVSS. It was introduced in 2016 and aimed to tackle threat modelling issues caused by systems that have complex interdependences between their components. In the first step of Quantitative Threat Modelling a component attack tree is built for each threat type present in STRIDE. This results in 6 attack trees concerning spoofing, tampering, repudiation, information disclosure, DoS and privilege elevation. In each attack tree the dependencies and low-level component attributes are detailed for the given threat. In the next step the CVSS scores are calculated for components present in each attack tree (Potteiger, Martins and Koutsoukos 2016).

It can be another aim of QTMM to generate attack ports for individual components. The attack ports illustrate the activities that pass risk to the components. Once this risk is scored by CVSS the amount of risk that

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

components pass onto other dependant components can be visualised. The Quantitative Threat Modelling method is relatively complete and provides built-in method to prioritize threats and ways to mitigate them. It has automated components so it is not overly laborious and if repeated offers consistent results. Adding attack ports to components also helps model threats on complex interdependent systems with communicating components.

13.10. Trike

Trike is a security audit framework invented in 2005 with the aim to model threats from a defensive and risk management perspective (Saitta, Larcom and Eddington 2005). It begins by building a requirement model that enumerates over the system users, assets, actions and rules to create an actor-asset-action matrix. In this matrix assets are represented by the columns and actors by rows. The cells in the actor-asset-action matrix consist of four action parts; one part creating, one reading, one updating, and the last deleting (CRUD). A value and rule tree should also be assigned to each cell, where the value assigned comes from a selection of three distinct values; these being allowed action, disallowed action and action with rules.

Once requirements are defined a dataflow diagram is built to map actors and assets. The dataflow diagram is then iterated through to identify threats which are categorised as privilege elevations or denials of service. Then discovered threats are assigned as the root nodes in an attack tree. In the final step the risk of attacks that impact assets are assessed through the CRUD actions present in the matrix prior. This is achieved by rating the actors for the risks they pose to each asset. They are rated on a five-point scale where a lower rating represents higher risk. In addition, the actors are also rated on another scale based on the likelihood they perform an action on an asset (always, sometimes, never). Despite offering many positives such as built-in prioritisation methods, automated components and contributing to risk management; Trike is not very well maintained, and the lack of available documentation means it is too vague to formally represent as a method.

13.11. VAST Modelling

VAST Modelling or The Visual, Agile and Simple Threat Modelling method is an automated threat modelling platform based on ThreatModeler (Threat Modeler n.d.). Manually models such as stride often struggle when systems grow in complexity, making it harder to implement efficient threat modelling. VAST modelling aims to be relevant for the entire software development life cycle of a system (Threat Modeler n.d.). As a result, VAST Modelling aims to be scalable and usable for large companies while producing reliable results. VAST requires creation of two models; an application threat model and an operation threat model. The application model utilises process flow diagrams to represent the architectural view of the system. While the operational model is created from the attacker's point of view using dataflow diagrams. One flaw with VAST Modelling is the lack of publicly available documentation due to the fact it is a product for purchase.

13.12. OCTAVE

OCTAVE or Operationally Critical Threat, Asset, and Vulnerability Evaluation applies a risk-based strategic assessment and planning method towards cybersecurity (Alberts, et al. 2003). OCTAVE concentrates on assessing organisational risks and does not assess technological risks whatsoever.
Building an OCTAVE model is achieved in three phases:

- Building an organisation view of asset-based threat profiles
- Identifying the vulnerabilities present in the infrastructure
- Developing a security strategy and plans

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

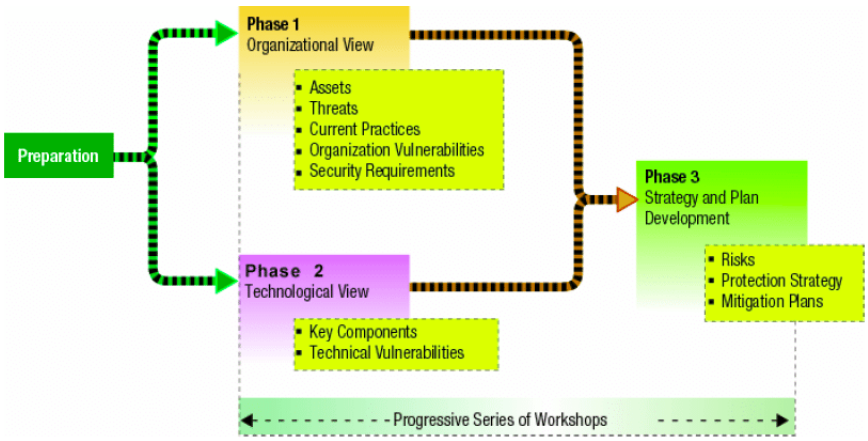

Figure 30: The 3 OCTAVE Phases (Mayer 2009)

OCTAVE has plenty of advantages which include; offering aid to identify relevant threat mitigation techniques, contributing to risk management, built-in prioritisation of threat mitigation, encourages collaboration, designed to be scalable and offers consistent results when repeated. However, it has a lot of vague documentation and is time consuming to implement.

13.13. TREsPASS

The TREsPASS project aims to analyse and visualise security risks in dynamic organisations, alongside possible countermeasures. It was published in 2013 by a consortium of members funded by the European Commission (TREsPASS Project 2016).It presents a concept called an 'Attack Navigator' to lead analysts model the attack risks that are possible and most pressing, and the countermeasures which will be most effective. It claims to achieve this by applying knowledge from technical sciences, social sciences and state-of-the-art industry processes and tools.

TREsPASS also developed a number of extensions to attack trees giving them benefits in certain situations. These extensions are as follows:

- ADTool – provides user friendly application to automate security analysis based on attack-defence trees
- ATCalc – extends classical attack trees with notion of time
- ATAnalyzer – performs quantitative attack tree analysis
- ATtop – obtains quantitative values using priced timed automata and Uppaal SMC
- ATEvaluator – calculate Pareto efficient solutions for the attack tree.

A concept known as an 'Attack Cloud' is also defined, which aims to represent very large attack trees with over 1000 nodes up to 500,000 nodes. The idea that attack trees should be linear is challenged as steps could be attempted in any order in an attack; and as a result, many nodes can exist. This attack cloud format shows the viewer which steps are involved in which attacks and allow them to understand the full context.

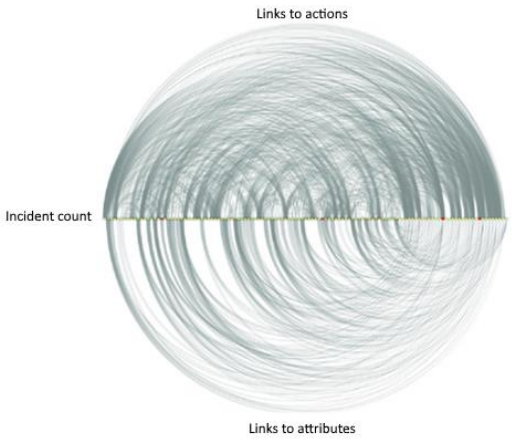

Figure 31: An example of an Attack Cloud (TREsPASS Project 2016)

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

Using a socio-technical risk model, human behaviour, technology and influencing policies can be considered to find threats. Within this model exist entities, interaction possibilities with associated quantitative properties. The quantitative properties have a difficulty, risk for attacker, reward for attacker and visibility attached. Given the social nature of this model it is also beneficial to brainstorm the characteristics of each context and scenario when building the model. This model consists of the following components:

- Spatial components – the geometric representation of the models shape in a space
- Social component – a human as an entity which interacts with the risk model, which can move and have relations with other entities
- Object component – set of all objects
- Digital component – programs or data that are present in objects
- Action – change of state in the socio-technical system/socio-technical security model
- Actor – object that executes actions

13.14. DREAD

DREAD is a modelling tool similar to STRIDE also developed by Microsoft. It takes a different approach to assessing threats. DREAD is a mnemonic standing for: Damage potential, Reproducibility, Exploitability, Affected Users and Discoverability. Threats found in a given system are evaluated by DREAD by assigning a value for each of the above categories for each respective threat. One of three values are assigned to Damage potential, Reproducibility, Exploitability and Affected Users for each threat, where the values are 1, 2 and 3; representing low, medium and high respectively. These values 'allow an average value to be calculated to represent the risk of the entire system' (Leblanc 2007). Once values for each threat have been derived, the risk rating can be obtained by summing the value of each DREAD component for the given threat. A rating from 5-7 is a low risk threat, a rating from 8-11 denotes a medium risk threat and finally a sum from 12-15 is a high-risk threat. The figure below gives an example of two high risk threats and how their scores are derived.

Threat	D	R	E	A	D	Total	Rating
Attacker obtains authentication credentials by monitoring the network.	3	3	2	2	2	12	High
SQL commands injected into application.	3	3	3	3	2	14	High

Figure 32: Table showing DREAD rating for two threats (INFOSEC 2014)

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

14. Conclusions

In this deliverable, D2.2 (Technology & Watch Update), the evolving techniques and advances in the State-of-the-Art of Fintech applications are analysed. An analysis of the current cyber-attacks on financial infrastructures shows that there is a need for more cyber security within the Fintech applications domain. The Critical-Chains consortium therefore, aims to provide a holistic and adaptable framework, including end-users and financial authorities that uses new technologies beyond the State-of-the-Art. A novel "as-a-service" (XaaS) platform will be delivered that is applicable to protect financial infrastructures against illegal money trafficking and fraud on Fintech operations. Furthermore, the framework is compliant with current regulations, such as the Payments Services Directive 2, cloud service regulations, Blockchain regulations and artificial intelligence regulations.

This deliverable includes new insights that arising from the research and development efforts within the Critical-Chains project over the last 12 months of Period I during which the COVID-19 pandemic has also had a significant effect on cyber-security in Fintech domain.

D2.2 covers new insights for a wide range of Fintech related technology and services, notably:

- Using mobile payment systems
- Blockchain in new arena (new applications, digital identity, contracts)
- New insights considering regulatory issues, such as those relating to PSD2 and GDPR
- The rise of Identity-as-a-Service (IDaaS):
    - Enterprises are embracing cloud and mobile technologies. As they do, they are moving beyond traditional network boundaries and the capabilities of their legacy identity and access management (IAM) solutions or generally Identity Management Systems (IDMS). Identity as a service (IDaaS) is a SaaS-based IAM that enables organisations to use single sign-on, authentication and access controls to provide secure access to their growing number of software and SaaS applications. With the recent trends, especially after the COVID-19 outbreak, IDaaS has become a new business model for all online services, including the Fintech industry.
    - The current market for IDaaS is highly aligned with the XaaS model of Critical-Chains and the consortium has already started to integrate HwSaaS for Crypto-as-a-Service and Authentication-as-a-Service.
    - The open-source access management solutions are increasingly popular in the market. For instance, KeyCloak an open source identity and access management library, is being used in many solutions.

- Recently, 30 international banks were analysed w.r.t the multi-factor authentication protocols that they provide. The investigated institutions follow their national or EU guidelines but the resulting authentication frameworks vary greatly and also contain insecure practices such as the use of look-up secrets. Especially when it comes to enrolling and on-boarding new customers, the best practices are widely ignored. As a result, the vulnerability against attacks remains higher than expected.

- Alarming statistics show the increased numbers and types of cyber-attacks in 2020:
    - Coronavirus blamed for 238% rise in attacks on banks
    - 80% of firms have seen an increase in cyberattacks
    - 27% of attacks target banks or healthcare
    - Cloud based attacks rose 630% between January and April 2020
    - Phishing attempts rose 600% since the end of February
    - Ransomware attacks rose 148% in March
    - Attacks targeting home workers rose five-fold within six weeks following the lockdown

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% of coronavirus-related domains could be reasonably deemed suspicious
- Visits to hacker websites and forums rose 66% in March
- Average ransomware payment rose 33% to $111,605, compared to Q4 2019
- EventBot, identified in March 2020, has targeted 200 banking and money transfer apps

****

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

References

360 Research Reports. 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.

Ahmed, Mohiuddin, Nazim Choudhury, and Shahadat Uddin. 2017. "Anomaly detection on big data in financial markets." *2017 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM).* 998-1001.

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

Alghofaili, Yara, Albatul Albattah, and Murad A. Rassam. 2020. "A Financial Fraud Detection Model Based on LSTM Deep Learning Technique." *Journal of Applied Security Research* (Taylor & Francis) 1-19.

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.*

Amarasinghe, T., A. Aponso, and N. Krishnarajah. 2018. "Critical Analysis of Machine Learning Based Approaches for Fraud Detection in Financial Transactions." *Proceedings of the 2018 International Conference on Machine Learning Technologies (ICMLT).* 12-17.

Apache Software Foundation. 2012. *Apache Jena.* Apache Software Foundation. Accessed November 10, 2020. 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.*

Australia, Parliament of. 2020. *Financial Technology and Regulatory Technology.* October. https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Financial_Technology_and_Regulatory_Technology/%20FinancialRegulatoryTech.

Autonomous Research LLP. 2018. *Augmented Finance & Machine Intelligence.* Accessed November 21, 2019. https://next.autonomous.com/augmented-finance-machine-intelligence.

Awoyemi, J.O., A.O. Adetunmbi, and S.A. Oluwadare. 2017. "Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis. In: Procee." *Proceedings of the 2017 International Conference on Computing Networking and Informatics (ICCNI).* IEEE. 1-9.

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.*

Bahnsen, A.C., Stojanovic, A., D. Aouada, and B. Ottersten. 2014. "Improving Credit Card Fraud Detection with Calibrated Probabilities." *Proceedings of the 2014 SIAM International Conference on Data Mining.* Society for Industrial and Applied Mathematics. 677-685.

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

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.*

Bao, Wei, Jun Yue, and Yulei Rao. 2017. “A deep learning framework for financial time series using stacked autoencoders and long-short term memory.” *PloS one* (Public Library of Science San Francisco, CA USA) 12: e0180944.

Bao, Z., W. Shi, D. He, and K.K.R. Chood. 2018. *IoTChain: A three-tier blockchain-based IoT security architecture.* arXiv:1806.02008, arXiv preprint.

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.

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

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.

Carcillo, Fabrizio, Andrea Dal Pozzolo, Yann-Aël Le Borgne, Olivier Caelen, Yannis Mazzer, and Gianluca Bontempi. 2018. “Scarff: a scalable framework for streaming credit card fraud detection with spark.” *Information fusion* (Elsevier) 41: 182-194.

Carcillo, Fabrizio, Yann-Aël Le Borgne, Olivier Caelen, and Gianluca Bontempi. 2018. “Streaming active learning strategies for real-life credit card fraud detection: assessment and visualization.” *International Journal of Data Science and Analytics* (Springer) 5: 285-300.

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

Chandradeva, Lakshika Sammani, Isuru Jayasooriya, and Achala Chathuranga Aponso. 2019. “Fraud Detection Solution for Monetary Transactions with Autoencoders.” *2019 National Information Technology Conference (NITC).* 31-34.

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.

Chawla, R. Chalapathy and S. 2019. “Deep Learning for Anomaly Detection: A Survey.” arXiv:1901.03407.

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.

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

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

Dal Pozzolo, A., O. Caelen, R.A. Johnson, and G. Bontempi. 2015. "Calibrating Probability with Undersampling for Unbalanced Classification." *2015 IEEE Symposium Series on Computational Intelligence.* IEEE. 159-166.

Dal Pozzolo, Andrea, Giacomo Boracchi, Olivier Caelen, Cesare Alippi, and Gianluca Bontempi. 2015. "Credit card fraud detection and concept-drift adaptation with delayed supervised information." *2015 international joint conference on Neural networks (IJCNN).* 1-8.

Dal Pozzolo, Andrea, Giacomo Boracchi, Olivier Caelen, Cesare Alippi, and Gianluca Bontempi. 2017. "Credit card fraud detection: a realistic modeling and a novel learning strategy." *IEEE transactions on neural networks and learning systems* (IEEE) 29: 3784-3797.

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.

Demir, K., and S. Ergun. 2019. "Random Number Generators Based on Irregular Sampling and Fibonacci–Galois Ring Oscillators." *IEEE Transactions on Circuits and Systems II: Express Briefs* 1718-1722.

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/.

Ergün, S. 2019. "Attack on a Microcomputer-Based Random Number Generator Using Auto-synchronisation." *2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST) .* 1-4.

—. 2019. "Revealing the Unknown Parameters of a Microcomputer-Based Random Number Generator." *2019 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS).* IEEE. 237-240.

Ergün, S., and S. Tanriseven. 2019. "Random Number Generators Based on Discrete-time Chaotic Maps." *IEEE EUROCON 2019-18th International Conference on Smart Technologies.* IEEE. 1-4.

Ernst & Young. 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.

European Central Bank. 2020. *The payment system.* Accessed December 12, 2020. https://www.ecb.europa.eu/paym/pol/activ/systems/html/index.en.html.

European Commission. 2020. *Consultation on a new digital finance strategy for Europe / FinTech action plan.* Accessed December 15, 2020. https://ec.europa.eu/info/consultations/finance-2020-digital-finance-strategy_en.

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

—. 2009. *Economic and Financial Affairs.* Accessed December 12, 2019. https://ec.europa.eu/economy_finance/bef2009/speakers/jacques-de-larosiere/.

—. 2016. *Official Journal of the European Union.* 27 04. Accessed 12 12, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

—. 2019. *Requisiti patrimoniali per il settore bancario.* 12 March. Accessed December 12, 2019. https://www.consilium.europa.eu/it/policies/banking-union/single-rulebook/capital-requirements/.

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

Famularo, Massimo, and Anne Magazine. 2018. *Fintech il futuro.* 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.* Report, dealroom.co.

FiRST. n.d. *Common Vulnerability Scoring System v3.0: Specification Document.* FIRST. Accessed October 23, 2020. https://www.first.org/cvss/v3.0/specification-document.

FSB – Financial Stability Board. 2019. *Fintech and market structure in financial services: Market developments and potential financial stability implications.* 14 February. Accessed October 15, 2020. https://www.fsb.org/2019/02/fintech-and-market-structure-in-financial-services-market-developments-and-potential-financial-stability-implications/.

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."

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

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.*

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.

Heryadi, Yaya, and Harco Leslie Hendric Spits Warnars. 2017. "Learning temporal representation of transaction amount for fraudulent transaction recognition using cnn, stacked lstm, and cnn-lstm." *2017 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom).* 84-89.

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.

Huang, D., D. Mu, L. Yang, and X. Cai. 2018. "CoDetect: Financial Fraud Detection With Anomaly Feature Detection." *IEEE Access* (IEEE Access, Vol. 6) 19161-19174.

Hypo Alpe Adria Bank. 2015. *Hypo Alpe Adria Informativa al pubblico.* 31 December. Accessed December 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. Accessed October 15, 2020. https://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model/.

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

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

John, Hyder, and Sameena Naaz. 2019. "Credit card fraud detection using local outlier factor and isolation forest." *Int. J. Comput. Sci. Eng.* 7: 1060-1064.

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."

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. 2020. *KPMG Internal Audit: Top10 in 2020; Considerations for impactful internal audit departments.* Internal Audit, Hong Kong: KPMG.

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.

Lebichot, Bertrand, Yann-Aël Le Borgne, Liyun He-Guelton, Frédéric Oblé, and Gianluca Bontempi. 2019. "Deep-learning domain adaptation techniques for credit cards fraud detection." *INNS Big Data and Deep Learning conference.* 78-88.

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

Lee, Thai T. Pham and Steven. 2016. "Anomaly Detection in Bitcoin Network Using Unsupervised Learning Methods." CoRR.

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

Li, Yuening, Xiao Huang, Jundong Li, Mengnan Du, and Na Zou. 2019. "SpecAE: Spectral AutoEncoder for Anomaly Detection in Attributed Networks." *Proceedings of the 28th ACM International Conference on Information and Knowledge Management.* 2233-2236.

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, M., K. Wu, and J.J. Xu. 2019. "How Will Blockchain Technology Impact Auditing and Accounting: Permissionless versus Permissioned Blockchain." *Current Issues in Auditing* A19-A29.

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.

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

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. *SVigilanza europea: per fare ordine il tempo stringe.* 29 February. Accessed December 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. Accessed November 25, 2020. https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN.

Mishra, Supriya, and Meenu Chawla. 2019. "A comparative study of local outlier factor algorithms for outliers detection in data streams." In *Emerging Technologies in Data Mining and Information Security*, 347-356. Springer.

Misra, Sumit, Soumyadeep Thakur, Manosij Ghosh, and Sanjoy Kumar Saha. 2020. "An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction." *Procedia Computer Science* (Elsevier) 167: 254-262.

Mitchell, Robert L. 2017. "Cobol: Not Dead Yet."

—. 2006. "Cobol: Not Dead Yet."

Mohanty, S.P., Yanambaka, V.P., Kougianos, E. and Puthal, D. 2020. "PUFchain: A Hardware-Assisted Blockchain for Sustainable Simultaneous Device and Data Security in the Internet of Everything (IoE)." *IEEE Consumer Electronics Magazine* 8-16.

Monamo, P., V. Marivate, and B. Twala. 2016. "Unsupervised Learning for Robust Bitcoin Fraud Detection." *Proceedings of the 2016 Information Security for South Africa (ISSA).* IEEE. 129-134.

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.

Nicole, Emily. 2020. *Budget 2020: Government to issue UK fintech sector review.* 11 March. Accessed 2020. https://www.cityam.com/budget-2020-government-to-issue-uk-fintech-sector-review/.

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

Podgorelec, B., M. Turkanović, and S. Karakatič. 2020. "A Machine Learning-Based Method for Automated Blockchain Transaction Signing Including Personalized Anomaly Detection." *Sensors 2020, 20(1)* 147.

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.

Pollari, Ian, and Anton Ruddenklau. 2020. *Pulse of Fintech H1 2020.* September.

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

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/.

PYMNTS. 2020. *PayPal, Facebook Take Stakes In Gojek.* 3 June. https://www.pymnts.com/news/investment-tracker/2020/paypal-facebook-invest-expand-with-gojek-in-southeast-asia.

RDF Working Group. 2010. *Resource Description Framework.* W3C Consortium. Accessed October 16, 2020. http://www.w3.org/RDF/.

Retail Banking Academy. 2014. “Course Code 108 - Operations.” *Retail Banking* 178-198.

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/ .

Singh, Akash. 2017. “Anomaly detection for temporal data using long short-term memory (lstm).”

Singh, L.D., and P. Meher. 2020. “A Novel Approach on Advancement of Blockchain Security Solution.” *Cognitive Informatics and Soft Computing* 449-456.

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.”

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

Threat Modeler. n.d. *ThreatModeler.* Accessed November 25, 2020. https://threatmodeler.com/.

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

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

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.

Tripathi, Diwakar, Y. Sharma, T. Lone, and Shubhra Dwivedi. 2018. “Credit card fraud detection using local outlier factor.” *International Journal of Pure and Applied Mathematics* 118: 229-234.

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

UK Essays. 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.

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/.

Vynokurova, Olena, Dmytro Peleshko, Polina Zhernova, Iryna Perova, and Andrii Kovalenko. 2020. “Solving Fraud Detection Tasks Based on Wavelet-Neuro Autoencoder.” *International Scientific Conference “Intellectual Systems of Decision Making and Problem of Computational Intelligence”.* 535-546.

W3C Consortium. 2004. *Guide. W3C Recommendation 10 February 2004.* W3C Consortium. 10 February. Accessed November 15, 2020. http://www.w3.org/TR/2004/REC-owl-guide-20040210/.

—. 2004. *W3C Recommendation.* W3C Consortium. 10 February. Accessed October 23, 2020. http://www.w3.org/TR/2004/REC-rdf-schema-20040210/.

—. 2004. *W3C Recommendation 10 February 2004.* W3C Consortium. Accessed October 23, 2020. http://www.w3.org/TR/2004/REC-owl-features-20040210/.

W3C OWL Working Group. 2009. *OWL 2 Web Ontology Language Document Overview. W3C Recommendation 27 October 2009.* W3C Consortium. Accessed October 16, 2020. http://www.w3.org/TR/2009/REC-owl2-overview-20091027/.

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.

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.

Wuyts, K., R. Scandariato, W. Joosen, M. Deng, and B. Preneel. 2019. *LINDDUN: a privacy threat analysis framework.* DistriNet Research Group, KU Leuven.

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.

Żbikowski, M. Ostapowicz and K. 2019. “Detecting Fraudulent Accounts on Blockchain: A Supervised Approach.” Proceedings of the International Conference on Web Information Systems Engineering (WISE).

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

Appendices

Appendix 1 – Fintech Cyber Incidents 2013-2019.

Table 6. 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 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

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

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)	Netherl ands	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(T heft)	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 vulnerabilit y (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 vulnerabilit y (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 vulnerabiliti es (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.

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

Appendix 2 – Fintech Cyber Incidents 2020.

Nr.	Cyber Incident	Target Location	Reported Date	Incident Method	Incident Type	Actor	Attribution	Attacked Entity	Description
1	**Scotiabank Data Breach**	Canada	7/21/20	Other	Data breach	Unknown	Unknown	Bank	On July 21, Scotiabank warned "a limited number" of customers of a data breach after Scotiabank bank an employee accessed client accounts without a valid business reason
2	**Emotet Spreading QakBot Banking Malware**	N/A	7/21/20	Malware	Theft	Non-state actor	Unknown	Bank	On July 21, observed Emotet, a known botnet, spreading the QakBot banking trojan at an unusually high rate. QakBot recently replaced the longtime TrickBot payload.
3	**Kattana Crypto App Malware**		7/16/20	Malware	Theft	Unknown	Unknown	Cryptocurrency	On July 16, researchers discovered GMERA malware embedded within Kattana, a cryptocurrency app, being used to steal wallet information.
4	**Famous Twitter Accounts Hijacked for Bitcoin**	USA	7/15/20	Multiple	Theft	Unknown	Unknown	Cryptocurrency	On July 15, several notable Twitter accounts including Joe Biden and Elon Musk were hacked to post a Bitcoin address purporting to double any contributions to the address.
5	**Argenta ATM Attack**	Belgium	7/13/20	Multiple	Theft	Unknown	Unknown	Bank	On July 13, Argenta, a Belgian savings bank shut down 143 cash machines after suffering a cyber-attack from Unknown criminals.
6	**Spanish Crypto App Malware**	N/A	7/12/20	Malware	Theft	Unknown	Unknown	Cryptocurrency	In July 2020, Avast found Cerberus malware hidden in a cryptocurrency converter app used to infect victims of Android devices.
7	**SEC Warning of Ransomware Attacks on US Banks**	USA	7/10/20	Ransomware	Theft	Unknown	Unknown	Financial firms	On July 10, the SEC issued a warning about a rise in ransomware attacks on U.S. financial firms.
8	**GoldenSpy Malware in Chinese Tax Software**	China	6/25/20	Multiple	Multiple	Speculated	Speculated	Government	On June 25, 2020, researchers identified a new backdoor trojan, dubbed 'GoldenSpy,' in Chinese tax software.
9	**IcedID Banking Trojan Using COVID-19 lures**	N/A	6/22/20	Multiple	Theft	Unknown	Unknown	Bank	On June 22, 2020, researchers identified a new variant of the IcedID banking trojan that uses COVID-19 related phishing lures.
10	**European Bank Targeted by Large DDoS Attack**	N/A	6/23/20	DDoS	Disruption	Unknown	Unknown	Bank	On June 21, 2020, a large unidentified European bank was the target of a massive DDoS attack that sent 809 million packets per second through its network.
11	**Coincheck Data Breach**	Japan	6/4/20	Other	Data breach	Unknown	Unknown	Cryptocurrency	On June 4, 2020 Coincheck, a Japanese digital currency exchange, paused remittances after Unknown attackers gained access to Coincheck's domain registry service and fraudulently obtained user email addresses as well as personal data.

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

12	**Banco BCR Data Breach**	Costa Rica	5/23/20	Ransomware	Theft	Non-state actor	Unknown	Bank	On May 21, 2020, the operators of the Maze Ransomware released 2GB of data, including credit card credentials, from Banco BCR, the state-owned Bank of Costa Rica.
13	**Indian Mobile Banking Apps Malware**	India	5/14/20	Malware	Theft	Unknown	Unknown	Bank	On May 14, CERT-In, India's national CERT, released a warning that a mobile banking malware called 'EventBot' that steals personal financial information was affecting Android users in India.
14	**Norfund Business Email Compromise**	Norway	5/14/20	Other	Theft	Unknown	Unknown	Government	On May 13, Norfund, Norway's state investment fund, was subject to a $10 million heist that involved business email compromise.
15	**Diebold Nixdorf Ransomware Attack**	USA	5/11/20	Other	Theft	Unknown	Unknown	Bank	On May 11, 2020, American ATM manfacturer Diebold Nixdorf was hit by a ransomware attack that caused 'a limited IT systems outage'.
16	**North Korean Web Skimming Attacks**	Serbia, Montenegro, Croatia, Slovenia, Bosnia and Herzegovina	4/23/20	Malware	Theft	State-sponsored actor	High confidence	Bank	On April 23, it was reported that North Korean hackers had been using webskimming malware to steal payment card details from online stores since at least May 2019.
17	**dForce Cryptocurrency Attack and Return**	China	4/21/20	Unknown	Theft	Unknown	Unknown	Cryptocurrency	On April 21, 2020 an attacker stole $25 million in Ethereum, a popular cryptocurrency, from the dForce platform, a cryptocurrency firm, only to return the funds two days later.
18	**Spanish Banks Attacked with Brazilian Trojan**	spain	4/13/20	Malware	Theft	Non-state actor	Unknown	Bank	On April 13, 2020, IBM researchers reported that Spanish banks had been the target of by a Brazilian banking Trojan, Grandoreiro, in a campaign lasting months.
19	**South Korean and US Payment Card Leak**	South Korea, USA	4/24/20	Unknown	Theft	Unknown	Unknown	Bank	On April 9, 2020, a cache of 400,000 payment card records from banks in South Korea and the U.S. were uploaded to a well-known underground marketplace.
20	**US, Canadian, Australian Banks Hit By Banking Trojan**	uSA, Canada, Australia	5/11/20	Malware	Theft	Unknown	Unknown	Bank	On March 30, researchers reported that U.S., Canadian, and Australian banks were being increasingly targeted by Zeus Sphinx, a banking trojan that had been dormant for three years.
21	**Monte de Paschi Bank Attack**	Italy	4/11/20	Unknown	Data breach	Unknown	Unknown	Bank	On March 30, 2020, attackers breached email accounts of employees at Monte dei Paschi bank, an Italian state-owned bank, and sent messages to clients with voice mail attachments.
22	**Chubb Ransomware Attack**	USA	3/26/20	Ransomware	Data breach	Unknown	Unknown	Insurance	On March 26, 2020, Insurer Chubb was targeted by Maze ransomware and the attackers claimed to have data stolen.
23	**Square Milner data breach**	USA	4/22/20	Unknown	Data breach	Unknown	Unknown	Financial firms	On March 25, 2020, Square Milner, one of the largest accountancy firms in the US, experienced a possible data breach.

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

24	**Finastra Ransomware Attack**	UK	3/20/20	Ransomware	Data breach	Unknown	Unknown	Financial firms	On March 20, 2020, Finastra, a large London-based financial technology company, stated they were the victim of a ransomware attack.
25	**Southeast Asian Banks Credit Card Breach**	Malaysia; Singapore; Philippines; Vietnam; Indonesia; Thailand	3/6/20	Unknown	Data breach	Unknown	Unknown	Bank	On March 6, 2020, it was reported that over 200,000 credit card details from top banks in Singapore, Malaysia, the Phillippines, Vietnam, Indonesia, and Thailand were stolen and published online.
26	**Australian Banks DDoS Extortion**	Australia	2/25/20	DDoS	Disruption	Unknown	Unknown	Bank	On February 25, 2020, it was reported that Australian banks and other financial institutions were being extorted by the Silence group with DDoS attacks unless they paid a ransom.
27	**PayPal Accounts Linked to Google Play Abused**	USA, Germany	2/25/20	Unknown	Theft	Unknown	Unknown	Bank	On February 21, 2020, hackers targeted PayPal accounts to carry out unauthorised purchases, estimated to be worth tens of thousands of euros, by exploiting PayPal's Google Pay integration.
28	**Loqbox Data Breach**	UK	3/2/20	Unknown	Data breach	Unknown	Unknown	Financial firms	On February 20, Loqbox, a UK-based credit score builder startup, was the victim of a data breach in which customer details were compromised.
29	**Sub-Saharan African Banks Targeted**	Africa	1/17/20	Malware	Theft	Non-state actor	Speculated	Bank	In the first week of January 2020, it was reported that major banks in sub-Saharan Africa were targeted by the Silence hacking group.

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