# Scenario Analysis of Secure Multi-party Computation implementation in EU-based multinational banks

Master thesis submitted to Delft University of Technology

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

in Management of Technology

Faculty of Technology, Policy and Management

by

Julia Lam

Student number: 4885732

To be defended in public on September 30, 2020

## Graduation committee

| | |
|---|---|
| First Supervisor | : Dr. ir. G.A. Reuver, Information Communication Technology |
| Second Supervisor | : Dr. R.M. Verburg, Economics of Technology and Innovation |
| External Supervisor | : R. Steenbergen, Rabobank Netherlands |

# Preface

This thesis is my final graduation project for the Management of Technology Master's program at the Delft University of Technology. This thesis was also written as part of my internship with the Tech Labs team at Rabobank, Netherlands in the Digital Transformation Strategy & Innovation department. I would like to express my gratitude to those who have helped me in this project and those who have provided their support during my master's program.

First and foremost, I would like to thank my first supervisor, Professor Mark de Reuver, for his incredible and critical feedback and his empathic support during moments of uncertainty. His supervision and involvement contributed greatly to the quality and completion of my thesis. I would also like to thank my second supervisor, Professor Robert Verburg for connecting me to Rabobank for my internship. His feedback, kind support, and motivation helped immensely with addressing the theoretical components of my thesis. Thirdly, my appreciation goes out to my supervisor at Rabobank, Roel Steenbergen, for being present, patient and helpful during the writing process. I am grateful for the opportunity to work with the Tech Labs team and for the creative freedom that I was granted to manage my own project. Furthermore, I am thankful to my manager Chris Huls and the entire Tech Labs team for kindly supporting me throughout my internship and for making it a fun and exciting experience.

As for the content and data for this project, I am really appreciative to each person who participated in interviews for my thesis. Every discussion gave me a new perspective and it contributed significantly to the subject matter of my report. I hope this thesis will be useful information in return. To my best friend at TU Delft, thanks for being a dependable group member since the beginning and reassuring me throughout the way. Lastly, to my friends and family (especially my sister), thank you for your advice on varying matters about school and the curveballs that came during these past two years. To everyone, words cannot express how truly grateful I am.

Julia Lam
September, 2020

# Executive Summary

Data has become a source of competitive advantage for many enterprises seeking to leverage customer and market insights. However, data privacy and ownership are becoming an increasing concern in society and among policy makers and regulators. Moreover, inter-organizational data sharing and collaboration between competitive firms are risky due to the precariousness of leaking confidential data that may threaten their competitive standing. This presents a challenge to balance data sharing and accessibility whilst safeguarding sensitive information. Innovative methods such as Secure Multiparty Computation may be a viable solution for enterprises facing this issue. Secure multi-party computation, "SMPC" or "MPC" can potentially solve this issue by enabling competing businesses to perform data analytics on shared data whilst maintaining the privacy of their data.

In this thesis, secure multi-party computation (hereafter MPC), is the subject of investigation. MPC has gained interest and traction among researchers and businesses as a novel method for secure and private data sharing and analytics. In particular, businesses in collaboration may want to use MPC in order to compute functions or extrapolate meaning from their combined datasets without requiring a trusted third party to do so. In principle, data cannot be leaked via a third party since MPC allows these computations to occur without a trusted entity.

These key characteristics of MPC addresses the security and privacy issues among people and organizations with regards to data sharing and analytics. This has implications in improving collaboration between different organizations and empowering firms to maintain the secrecy their data. It may also change how businesses operate and participate in co-creation of new business solutions and innovations which can ultimately lead to value creation. However, there is little observed or empirical evidence on these potential effects which requires more exploration.

Additionally, there are gaps in prescriptive and descriptive knowledge of business value creation and capture from MPC in extant literature. Moreover, there are limited empirical studies of MPC applications in real-world settings that can inform businesses about their decisions with regards to implementing. Hence, it is difficult for firms to leverage MPC without understanding the full scope of MPC capabilities and what the possible outcomes are. Aside from MPC technicalities and algorithms, there is little scientific literature that addresses and connects MPC to business model concepts such as business model ontologies and business model components. Without this knowledge, it becomes difficult for managers and decision makers to effectively assess and strategize how MPC can be implemented and leveraged for their organizations.

In order to further understand MPC's business value, MPC was contextualized from a business perspective as opposed to a technical perspective. Given that there is little academic literature on MPC implementation and its outcomes, this thesis investigated MPC from a future studies assessment via scenario analysis. The potential and perceived benefits and outcomes of MPC are attractive to firms seeking to find secure ways to share data and derive insights from that aggregated data. This knowledge and insight can help inform decision making with regards to MPC implementation for their organizations.

*Therefore, the research objective was to determine plausible MPC implementation scenarios within banks via scenario analysis over time horizon of five years (2020-2025). Scenario analysis methods are used to elucidate possible future outcomes of MPC implementation since current MPC implementations in banks do not yet exist. Scenarios in this study will target two core bank functions that are unequivocally important to all banks and that is protecting the bank by some form of financial risk mitigation and*

*enabling new or improved business opportunities. Furthermore, the findings of this study may provide insights for practitioners to improve decision making within banks concerning potential MPC business models. The implications of this study can serve as a foundation for linking MPC to business model concepts and inter-organizational systems which are the fields of research used in the literature review for this study.*

Thus, the main research question that was investigated in order to address the research objective is:
**What are the future scenarios of MPC implementation in banks in the context of financial risk mitigation and business model concepts?**

The research of the main research question is facilitated by the following **sub-questions** and based on the selected scenario analysis method for this study:

1. **How does value creation theories explain the relationship between MPC implementation outcomes and business model innovation?**
2. **What are the future trends for a data-driven economy in the context of banking and finance?**
3. **What are the critical uncertainties of MPC implementation in banking environments?**
4. **Which business model components could be affected by MPC implementation and use?**

The research method proposed in this thesis followed an intuitive logics scenario analysis methodology whereby data was collected from three incumbent banks in the EU via semi-structured interviews. In total, eight interviews were conducted between three multinational banks and one non-bank entity. Furthermore, qualitative data analysis methods such as content analysis and general comparative analysis were coupled with scenario analysis methodology to extrapolate insights that address the proposed research questions. Both of these approaches are qualitative and descriptive in nature.

The main deliverable of the thesis and answer to the main research question which was to develop plausible future outcomes of MPC implementation in EU-based banks. The four main scenarios to consider over a time horizon of five years (2020-2025) are:

1. MPC improves the internal efficiency of bank operations with regards to risk frameworks: cybersecurity threat detection and prevention, sharing security related information with other banks, and fraud detection among banks. One example being inter-bank data sharing of fraud indicators or risk profiles for improved risk/security monitoring.
2. Enhance existing bank products, services, and offerings with MPC enabled data sharing and analytics. In this scenario banks can adopt industry platform business models and target B2B and B2C segments. Data-driven enhancements can either enable novel processes for existing offerings or improve services and business models due to improved data-driven insights and decision making. Credit and loan risks are ubiquitous among banks and therefore, sharing credit profiles between other banks or financial institutions can improve interest rates for the customer and loan defaults for the bank.
3. MPC implementation can also create new products and services resulting in new data-driven business models or business model innovation. These generally take the form of integrity validation services, benchmarking services, and co-created new product and market segments between banks and other non-bank industry incumbents. For instance, MPC can enable banks to sell computations as a service whereby bank data is used in analytic transactions but never revealed to external parties.
4. MPC is implemented in order to support open policy and supervisory bodies/government authorities in fighting financial misconduct and money laundering. The scenario forsakes revenue building and profit generating opportunities. As such, this scenario entails that banks must

implement MPC to assist and comply with government mandates rather than for economic benefits. In order to monitor and create oversight of banks, the scenario most likely entails the sharing of data between banks and government authorities about crimes committed in financial fraud and money laundering.

The development and analysis of these scenarios are found in Chapter 7. The full range of possible combinations of outcomes are also found in chapter 7, whereas a full description of the aforementioned decision scenarios is detailed in Chapter 8. In general, these scenarios indicate that MPC is positioned to serve in defense operations of the bank and also in new business opportunities. This indirectly or directly helps improve risk and profitability by saving costs or creating revenue.

Scenario analysis and qualitative data analyses indicate that MPC is a preferable method chosen by experts to be used in data sharing applications compared to conventional data sharing structures that require a trusted third party. However, MPC must guarantee that data is not at risk and that outputs are correct. This is insured partly by technical capabilities and design requirements of MPC protocols and partly by legal contractual arrangements between the parties themselves for each MPC use-case.

The decision to implement MPC is justified by the specific use-case and application. Therefore, experts note that preferred MPC network partners should transpire between other homogeneous actors such as major banks. These MPC computations would serve to enrich and/or extend existing data owned by the bank. Whereas, sharing information with the government would be more beneficial for the authorities rather than banks. However, the underlying incentive for MPC arrangements is to access information that would improve the risk profiles and mitigation structures of the banks and improve the integrity of the financial system.

On the other hand, the inclusion of heterogeneous parties within the computation such as tech incumbents, other leading industry firms i.e. telecom companies or insurance companies attribute more to creating business value for customer facing offerings. These arrangements enable more differentiation potential because banks would be able to access new and external data that they do not already have such as trends or customer profiles from other industries. Subsequently, banks can leverage this information for the creation or co-creation of new products and services. In some cases, MPC can also be used to enrich existing data. For instance, sharing fraud information between banks and insurance companies. Nonetheless, MPC is positioned to not only improve internal processes and operations of banks, it can also directly and indirectly enable new offerings for customers.

Ultimately, the investigation of the main and sub-research questions contributed research findings that have theoretical and practical significance. Firstly, MPC has been linked to interorganizational systems research and data driven business model concepts. A conceptual model was developed which consists of value creation outcomes of MPC implementation. This presents a starting theoretical basis to be tested and used in future MPC business research. This thesis also provides evidence that MPC can be identified or considered as a type of interorganizational system. By linking MPC to data driven business model components, new business model components have been identified in the context of MPC. These new components can extend data driven business model research. Secondly, this master thesis extends MPC literature and knowledge by conducting a scenario analysis for MPC implementation in EU banks.

As for practical contributions, this thesis can provide insights for managers seeking to learn more about MPC and its potential business value. Firstly, this study can inform decision making and strategy for managers interested in MPC or aim to implement MPC within their organizations. Descriptive knowledge of MPC's business potential in banking from a business model and data persepective. Secondly,

descriptive knowledge of the range of possible combinations of future outcomes can help manage expectations for future decisions. MPC is contextualized within a business environment as it relates to the future of EU banking and the data ecosystem. Thirdly, insights into data driven business model choices and components in the context of MPC may have implications on business model innovation for banks. Fourthly, descriptions of MPC use-case examples can generate ideas and challenge conventional thinking within organizations, but it is most useful for incumbent organizations such as multinational banks which have the resources and capital to invest in MPC. Lastly, this report can increase awareness of the business environment and drivers that affect the future of MPC in the EU banking and the data ecosystem.

In conclusion, MPC is a viable and plausible option for leveraging anonymous data sharing and analytics to support banks' business opportunities. MPC can seemingly also enable banks to adopt or improve business models in the data-driven economy, enhance banks' risk management frameworks in security, and allow banks to contribute to responsible banking environments by fighting financial and organized crime. The most useful chapters for managers and practitioners who want to understand the project outcomes of this study are the results discussion chapter (7) and the findings chapter (8).

## Table of Contents


**Preface** **2**

**Executive Summary** **3**

**1. Introduction** **13**

*1.1 Problem Description* *13*

*1.2 Research Objective* *14*

*1.3 Research Questions* *15*

*1.4 Knowledge Gap and Research Contributions* *17*

*1.5 Thesis Structure* *18*

**2. Research Design** **21**

*2.1. Research Approach* *21*

*2.2 Research Methodology – Scenario Analysis* *24*
2.2.1 Intuitive Logics Model for Scenario Analysis 25
2.2.2 Scenario Analysis Phases and Outcomes 25
2.2.3 Criteria for scenarios 27

*2.4 Data Collection* *28*

*2.5 Data Analysis* *29*

**3. Literature Review** **31**

*3.1. Research Domains* *31*
3.1.1 MPC Definition 31
3.1.2 Historical Background of MPC 31
3.1.3 Current state of MPC technology 32
3.1.4 MPC Applications in Banks 33
3.1.5 Business Models in the EU Bank Sector 34

*3.2 Theoretical Background* *34*
3.2.1 Digital Business Models 35
3.2.2 Inter-organizational Systems (IOS) 36
3.2.3 Value Creation Theories 38
3.2.4 Data Driven Business Models (DDBM) 40
3.2.5 Business Model Innovation 42

*3.3 Conclusion* *46*

**4. Scenario Preparation and Scenario Exploration (Phase 1 & 2)** **48**

*4.1 Scenario Preparation* *48*

*4.2 Scenario Exploration* *49*
4.2.1 PESTLE Method and Approach 49
4.2.1 Data Ecosystem Analysis 50
4.2.2 EU Banking Ecosystem Analysis 55
4.2.3 Conclusion 61

*4.3 Approach to identifying trends and uncertainties* *63*

*4.4.Data Ecosystem Trends and Uncertainties* *64*
4.4.1 Data Ecosystem Trends 64
4.4.2 Data Ecosystem Uncertainties 66
4.4.3 Conclusion 68

*4.5 Bank Ecosystem Trends and Uncertainties* *69*
4.5.1 Bank Ecosystem Trends 69
4.5.2 Bank Specific Uncertainties 71
4.5.3 Conclusion 72

**5. Scenario Development (Phase 3)** **73**

*5.1 MPC Uncertainties* *73*

*5.2 Initial Learning Scenarios* *75*

**6. Interview Protocol** **79**

*6.1 Interviewee Selection* *79*

*6.2 Rationale for Interviews* *81*
6.2.1 Conducting Interviews 81
6.2.2 Interview Questions 82
6.2.3 Interview Presentation and Information Dissemination 83

**7. Results & Analysis** **85**

*7.1 Research Sample* *85*

*7.2 Data analysis approach* *86*

*7.3 Coding & Data Analysis* *88*

*7.4 Data Comparison* *90*

*7.5 Determining Critical Uncertainties* *93*
1. Legal and Governance Structure 94
2. Technology Ownership 96
3. Incentives 97
4. Data Requirements 99
5. Business Models 100
7.5.1 Summary 102

*7.6 Interview feedback for learning scenarios* *104*
Scenario 1: MPC improves processes and operations 104
Scenario 2: Enhances existing products, services, and technologies 105
Scenario 3: Enables new products/services 105
Scenario 4: Assists government and supervisory authorities 106

*7.7 Data Analysis for Scenarios* *107*
7.7.1 Morphological Analysis 107

*7.8 Conclusion* *115*

**8. Discussion & Conclusion** **117**

*8.1 Interpretation of Findings* *117*
Decision Scenario 1: Improving internal efficiency of the bank. 117
Decision Scenario 2: Enhancing existing product/services/offerings with MPC. 117
Decision Scenario 3: MPC enables new products and services (use-case driven MPC) 118

Decision Scenario 4: Assisting government and supervisory authorities. 118
*8.2 Theoretical contributions* *119*
*8.3 Practical contributions* *122*
*8.4 Recommendations for banks in the EU* *123*
*8.5 Evaluation of Limitations* *124*
*8.6 Areas for Future Research* *125*
**References** **128**
**Appendix A: Literature Review Method** **138**
*MPC Selection and Search Criteria* *138*
*Business Models Selection and Search Criteria* *138*
*Interorganizational Systems Selection and Search Criteria* *139*
*Value Creation Selection and Search Criteria* *139*
**Appendix B: Extended Literature Review** **141**
*Value creation drivers in the context of IOS and MPC data sharing mechanisms* *141*
*Comparison of traditional and network model of RBV theory* *144*
*List of business model frameworks* *146*
*List of DDBM in extant literature* *148*
**Appendix C: Interview Protocol – Presentation slides** **149**
*Main presentation slides* *149*
*Presentation Slides for Bank C:* *152*
**Appendix D: Informed Consent Form for Interview Participants** **157**
**Appendix E: Coding List Exported from Atlas.ti** **159**
**Appendix F: Atlas.ti network reports filtered by uncertainty code group** **162**
*Legal and Governance Structure* *162*
*Technology Ownershi* *163*
*Incentives* *163*
*Data Requirements* *164*
*Business Models* *164*
*Technological Maturity and Computational Ability* *165*
*Customer Acceptance* *166*
**Appendix G: Atlas.ti network reports filtered by scenario code groups** **167**
*Scenario 1* *167*
*Scenario 2* *167*

*Scenario 3* *168*

*Scenario 4* *168*

**Appendix H: DDBM Framework (Hartmann et al., 2014, p. 6)** **169**

**Appendix I: Summary of Interview Reponses concerning business models** **170**

## List of Tables

*Table 1: Scenario analysis methodology for research study based on critical realist approach and intuitive logics model.* 26
*Table 2: List of DDBM definitions* 40
*Table 3: Comparison of different outcomes and activities of traditional versus data-driven business model innovation.* 44
*Table 4: Conceptual and practical knowledge inputs for initial learning scenarios.* 76
*Table 5: Interviewee participant selection* 80
*Table 6: Rationale and approach for interview questions.* 83
*Table 7: Description of interviewees by organization.* 86
*Table 8: Comparison of interviewees in this study.* 92
*Table 9: Interview responses (Yes/No/No Answer) to the plausibility and relevancy of uncertainties in legal and governance structure of MPC implementations.* 95
*Table 10: Interview responses (Yes/No/No Answer) to the plausibility and relevancy of uncertainties in MPC technology ownership.* 97
*Table 11: Summary of Interview responses (Yes/No/No Answer) to the plausibility and relevancy of uncertainties in MPC implementation incentives.* 99
*Table 12: Summary of interview responses (Yes/No/No Answer) to the plausibility and relevancy of MPC implementation data type requirements.* 100
*Table 13: Overview of interview responses (Yes/No/No Answer) to the plausibility and relevancy of MPC enabled business models.* 101
*Table 14: Summary of all critical uncertainties and plausible and relevant outcomes. Decision rationale for crossed out values are highlighted in red.* 102
*Table 15: Summary of interview responses to plausibility and relevancy of MPC implementation scenarios.* 104
*Table 16: Morphological box or field of the problem space (constructions of all possible solutions).* 108
*Table 17: Pair-wise comparison and justification of inconsistent value pairs for uncertainties.* 110
*Table 18: Actual MPC enabled business model components versus new plausible components based on (Hartmann et al., 2014)* 121
*Table 19: MPC business model components and practical examples in the context of EU bank sector.* 123
*Table 20: Business Model Definitions (2000 – present)* 147
*Table 21: Descriptions of DDBM Literature* 148

## List of Figures

*Figure 1: Thesis structure flow diagram.* 19
*Figure 2: Decision tree for research approaches constructed from research philosophies and paradigms in business and management research (Kersti, 2014; Saunders et al., 2019; Sekaran & Bougie, 2016).* 22
*Figure 3: Critical realist layered /stratified ontology adapted from (Bhaskar, 2008; Saunders et al., 2019).* 24
*Figure 4: Overview of Research Design Framework* 30
*Figure 5: Components of business model affinity diagram (Shafer et al., 2005, p. 202).* 35
*Figure 6: Relationships investigated in organizational consequences of IOS implementation (Robey et al., 2008, p. 505).* 38
*Figure 7: RBV theory underpins the academic disciplines that are used to contextualize MPC.* 39
*Figure 8: Overview of data-driven value creation in business models.* 42
*Figure 9: Abductively derived conceptual framework for MPC implementation outcomes and consequences.* 45
*Figure 10: The bank in its business environment. Adapted from Van Der Heijden, (1996, p.155).* 50
*Figure 11: Single Supervisory Mechanism (SSM) Risk Map for 2020 sourced from the European Central Bank (2019b).* 56
*Figure 12: Flow diagram for developing trends and uncertainties* 63
*Figure 13: Survey results for obstacles to B2B data sharing sourced from Arnaut et al. (2018).* 67
*Figure 14: Concept map for potential business model outcomes in banks.* 89
*Figure 15:Concept map for business model outcomes for third party MPC vendors.* 89

*Figure 16: Cross-consistency matrix which includes stakeholder feedback regarding MPC uncertainties and requirements for implementation and use. X = inconsistent pairs; black spaces are duplicate/redundant pairings.* _____ *111*
*Figure 17:Theoretical framework for MPC implementation and scenario applications.*_____ *120*
*Figure 18: Inter-organizational relationship motive definitions.* _____ *143*

# 1. Introduction

## 1.1 Problem Description

Major EU-based multinational banks have a dual obligation to generate and protect assets as a due diligence for their customers, their business longevity and in accordance with the European Central Bank. These incumbent banks must sustain their business models in order to remain competitive but also implement cost saving measures and risk frameworks. However, these core activities of banks with regards to maintaining or increasing overall profit must assume integrity in all aspects.

In 2011, the United Nations estimated 2-5% of the global GDP ($2.1 trillion) is accredited to illicit and organized crime whereby $1.6 trillion of these financial flows was available for money laundering (United Nations Office on Drugs and Crime (UNODC), 2011, p. 99). The total net financial flow of illicit money through Europe was reported to be $11.94 billion (United Nations Office on Drugs and Crime (UNODC), 2011, p. 98). In 2019, the Dutch National Banking Association estimates that €16 billion euros is laundered through the Netherlands annually (NVB, 2019). These reported statistics in 2011 and 2019 suggest a clear rise in organized crime and financial corruption across the EU. As such, this implies that banks are still at risk for issuing financial services to criminals that could hurt the banks' reputation.

Financial crime is also a threat to banks' integrity and assets because banks are subject to sanctions and fines for permitting unlawful transactions. For instance, the Dutch bank, ING was fined for $900 million for failing to meet regulatory standards with regards to financial crime whereas, Deutsche Bank was fined for $150 million for admitting a convicted sex trafficker to make corrupt transactions through the bank (ING, 2018; Stempel et al., 2020). There are many other examples whereby banks have paid fines for similar offenses. Thus, banks must take the necessary precautions and steps to comply with regulation and to prevent organized crime from growing via bank financing.

On the other hand, banks are also challenged by rising competition from start-ups and novel financial services deployed by fintech companies and technology incumbents. Banks need to find innovative ways to maintain or improve their market position for sustained competitive advantage. Data can be used on both ends to not only inform banks on improving their due diligence to government and society, but also to expand their business offerings. For instance, banks can derive insights from data analytics in order to make better business decisions and to safeguard the integrity of their business operations such as risk frameworks in security or credit monitoring.

The effective use of data presents opportunities for banks to meet their obligations in securing the integrity and trust of the bank and also providing business growth and continuity in their offerings. For these reasons, there is value in acquiring and using mixed or aggregated data sets from external sources as a means to extrapolate and gain the most information and knowledge. However, the sophistication of data analytics techniques can extrapolate sensitive information which may threaten and violate data privacy regulations, and thus ruin the integrity of bank operations. Sharing sensitive data between organizations can either be illegal or discouraged due to the privacy concerns of their customers and clients. Moreover, inter-organizational data sharing and collaboration between banks and other firms are risky due to regulatory compliance and the precariousness of leaking confidential data which may threaten their competitive standing.

Secure Multi-party Computation or MPC, is a unique configuration of encryption schemes and computational algorithms that enables data privacy in data sharing arrangements. Data privacy in this study refers to maintaining the secrecy of data inputs in MPC arrangements. In other words, a contributing

party's input data is not revealed to anyone within this particular arrangement. In the case of bad or malicious actors, data needs to be shared securely so no other party can steal information. Data security is enabled by specific cryptographic protocols, e.g. homomorphic encryption, that are used in MPC arrangements. These protocols are dependent on the use-case and design requirements of the stakeholders themselves (Archer et al., 2018). This thesis will focus less on the backend technical requirements and specific configurations of the protocols. Nonetheless, it is important to establish that MPC can have multiple protocols that protects data so that it can be used in computational and algorithmic functions for private and secure data sharing and analytics.

The balance between data privacy and data use remains a challenge for banks which impedes on their ability to proficiently and resourcefully generate and protect their assets. Given the increasing interconnectedness of people via electronic devices, the need for effective digital security is also becoming progressively important among practitioners, researchers, and consumers. Especially with the inception of EU privacy regulations like the General Data Protection Regulation (hereafter GDPR), there is a greater demand for privacy preserving technologies and cryptography to enable data sharing, data use, and collaboration in a competitive economy.

MPC can potentially solve this issue by enabling privacy-preserving data sharing without the need of a trusted third party (Lindell & Pinkas, 2009). MPC protects participants' input data while enabling participants to perform computations on that shared data (Lindell & Pinkas, 2009). MPC can protect the privacy of customer or commercial data of the firms participating in a multi-party computation. This presents opportunities for banks to utilize MPC for benchmarking competition, anonymous voting, fraud detection between banks, anti-money laundering, securities trading, and threat detection intelligence applications (Archer et al., 2018; Bogdanov et al., n.d., 2012; Du & Atallah, 2001; Sangers et al., 2019; Volgushev et al., 2016; Watanabe & Koseki, 2014). In this thesis, MPC will be generally defined as an emerging technology that enables anonymous data sharing without a trusted third-party.

However, MPC is an emerging technology in which barriers to deployment are apparent given the lack of knowledge regarding the tangible and realized business value (Kanger & Pruulmann-Vengerfeldt, 2015). Although MPC is versatile in a number of applications and industries, there are prescriptive and descriptive knowledge gaps in how MPC generates realized business value and economic profit. Therefore, the business potential of MPC for firms remains unclear. Furthermore, empirical evidence of MPC uses or applications in business models are unfounded in academic literature. Hence, the impact of MPC systems on business models is the central focus of this thesis. The investigation of this problem takes place in banking environments that are interested in using MPC for future business objectives in the context of financial risk mitigation and business models.

## 1.2 Research Objective

The research objective is to determine plausible MPC implementation scenarios within banks via scenario analysis over time horizon of five years (2020-2025). Scenario analysis methods are used to elucidate possible future outcomes of MPC implementation since current MPC implementations in banks do not yet exist. Studies support the notion that MPC can be implemented in risk mitigation frameworks for banks such as sharing data regarding threat detection and security monitoring. Scenarios in this study will target two core bank functions that are unequivocally important to all banks and that is protecting the bank by some form of financial risk mitigation and enabling new or improved business opportunities.

Therefore, MPC implementation scenarios will be scoped to encompass financial risk mitigation schemes and any implications this may have on business models for banks. A future studies assessment via scenario analysis is adopted as the research method and data will be collected via semi-structured interviews. The chosen methodology is the *intuitive logics* scenario analysis which is governed by three main outcomes:

1. enhancing understanding of sequence of events;
2. challenge conventional thinking and existing mental models of stakeholders;
3. and improve decision making (Van Der Heijden, 1996; Wayland, 2019; Wright et al., 2013).

Accordingly, the implications of this study aim to manage expectations for MPC implementation and to find potential MPC application areas that could bolster banks' core businesses. Moreover, correlations between the underlying structures that result in or affect MPC implementation is necessary in order to develop a logical sequence of events. Secondly, developing scenarios should expand the possible future outcomes for MPC applications within banks by interviewing multiple stakeholders from different EU banks. Thirdly, the findings of this study may provide insights for practitioners to improve decision making within banks concerning potential MPC use-cases in financial risk mitigation and any potential MPC enabled business models.

Preliminary background research will partially entail concepts from business model and inter-organizational systems literature to build a foundation of knowledge that will be used to guide the scenario analysis process. Business model concepts are well documented in literature which is useful for understanding how technology enables value creation and capture for organizations. Since MPC business literature is relatively unexplored, it is necessary to understand how conventional business model concepts can be applied for MPC contexts and purposes. Moreover, interorganizational systems, hereafter IOS, are defined as information systems that allow organizations to link business processes, pool information resources, and share data (Robey et al., 2008). IOS coincides with MPC in this aspect whereby MPC is also used to facilitate data sharing and ultimately, knowledge sharing between organizations. Background research in IOS literature will be scoped to IOS implementation within organizations. Hence, the implications of this study could result in findings that links MPC to business model concepts such as data driven business models and/or business model components. Thesis findings may also link IOS literature to MPC such that MPC implementation scenarios can be understood from an IOS perspective and conceptual lens.

Ultimately, the main deliverable of the research objective is the development of decision scenarios for MPC implementation in banks whereby 'decision scenarios' are finalized scenarios that can be used for decision making. The research approach and scenario methodology of this study will result in descriptive decision scenarios. The implications of this research deliverable have scholarly and practical significance which is discussed in the next section.

## 1.3 Research Questions

This section discusses the formulation and rationale for the research questions in this study. Firstly, the main research question (RQ) that will be investigated in order to address the research purpose is formulated as follows:

**What are the future scenarios of MPC implementation in banks in the context of financial risk mitigation and business model concepts?**

The main research question will be facilitated by the following **sub-questions (SQ)** which are explained thereafter:

1. **How does value creation theory correlate MPC implementation and business model concepts?**
2. **What are the future trends for a data-driven economy in the context of finance?**
3. **What are the critical uncertainties of MPC implementation in banking environments?**
4. **Which business model components could be affected by MPC implementation and use?**

Generally, SQ1 serves to address and understand MPC implementation outcomes using existing research and theory in business model literature and IOS literature. SQ2 and SQ3 are formulated according to scenario analysis steps that aid in eventually developing the main scenarios and deliverable of this study. SQ4 aims to address the connections between MPC implementation and business model components to ultimately, understand more about MPC business models. The rationale for each sub-question will be explained chronologically.

In order to deliver scenarios accordingly, research sub-questions are developed to guide the research process towards answering the main RQ. Firstly, the relationships between MPC, value creation outcomes and business models should be established. Since these relationships have yet to be observed, theories will be utilized from the field of IOS which can explain the outcomes of B2B data sharing and implementation of information systems that share and link resources and data between organizations (Robey et al., 2008). In this thesis, MPC is considered as an information system in the field of IOS. Then, the relationship between IOS outcomes and business model concepts can be translated to MPC as a starting point for building knowledge. Hence, **SQ1** theoretically explains the variables and factors that might give rise to MPC implementation in banks. It is formulated as a 'how' question because it is meant to understand the relationships between value creation, MPC implementation and business model innovation. However, the purpose of this study does not entail proving causality between variables or validating the conceptual framework which would require a longer study.

In the scenario analysis method, a macro-environmental analysis is necessary to establish the external drivers that organizations may react to during decision making and strategic management. External drivers can be future trends of banking or known factors that are expected to persist within the time horizon of five years that have an impact on banks. These finance and data related external drivers may also affect or influence the plausibility of future outcomes and therefore, the development of scenarios. Consequently, **SQ2** is formulated as a 'what' question to determine the external drivers which serves as input for developing descriptive scenarios.

External drivers has to be linked to the internal drivers that affect the organization; otherwise, it has less value in the development of effective scenarios for organizations (Burt et al., 2006). External and internal drivers are inputs for determining the uncertainties that can also affect MPC implementation. These uncertainties must be confirmed by stakeholders to be relevant and plausible to banks which ultimately, produce critical uncertainties. Critical uncertainties can be defined in this study as the confirmed internal drivers that have an effect on MPC implementation in banks and the stakeholders involved. Stakeholders relying solely on external or internal drivers may not be informed or fully equipped to make an accurate decision regarding MPC use. For instance, using generic MPC implementation scenarios that are not contextualized to banking environments does not truly have managerial significance in banks. Therefore, **SQ3** addresses the uncertainties of MPC implementation as it directly relates to banks whereby, stakeholders can react to these drivers but also influence them. This question is similarly descriptive.

The scenario outcomes and stakeholder interview responses may or may not provide evidence or explanation as to whether banks' business models will be affected by MPC. Therefore, **SQ4** ensures that MPC's impact on business models is analyzed and evaluated from the data collected. In order to align with the time-fame and exploratory approach to this thesis, this question is intended to be descriptive and correlational. Therefore, answering **SQ4** aims to understand and explore what the underlying mechanisms are in MPC implementation and business model components, but not test or explain the causal relationships.

## 1.4 Knowledge Gap and Research Contributions

This section discusses the scientific knowledge gap in MPC business literature and the academic and practical significance for conducting this research.

For this thesis, a survey of academic sources in MPC business literature was conducted. Based on the literature selection criteria (See Appendix A: Literature Review Method and literature review (Chapter

3. Literature Review), it is apparent that there is limited knowledge of MPC from a business perspective within academic literature. The findings from academic literature indicate that most research studies focus on validating and producing secure MPC protocols and algorithms (Ankele et al., 2016; Archer et al., 2018; Du & Atallah, 2001; Kanger & Pruulmann-Vengerfeldt, 2015; Lindell & Pinkas, 2009). A limited number of real-life MPC implementations also indicate that more research is needed in specific industries and applications such as banks.

Although MPC is considered to be versatile in a number of applications and industries, specific knowledge pertaining to algorithms and protocols of these computations depends on the parties involved, the type of data used, and the output requirements of the participants involved. These requirements have implications on the contexts of use of MPC and what type of data is used and extracted from in the process. Given the lack of MPC implementation in research, it is difficult to understand the realized business impact and value of MPC as well as the prescriptive knowledge on how to leverage MPC in business settings. There is also little research that directly links business concepts to MPC. Therefore, understanding particular business model concepts in the context of MPC implementation will be the subject of academic investigation in this thesis.

It is unknown whether pre-existing business model tools or methods can be used for MPC or if MPC enables new business models. Hence, this explorative study aims to contribute descriptive knowledge towards MPC business models and furthering the body of MPC literature. This study also aims to contribute practical knowledge to banks and potentially other firms regarding their data sharing decisions via MPC. For example, by understanding the (dis)advantages of MPC, it can influence or change how businesses operate and participate in co-creation of new business solutions and innovations which can ultimately lead to value creation.

Moreover, there are few and underdeveloped guiding principles for technological development such as the use of standards or formal definitions, legal requirements for interorganizational data collaboration via MPC, and governance of fairness and robustness of semi-honest MPC protocols. This early investigation of MPC implementation may influence technological development and protocol requirements before it is used by banks. Although this could be tied into the research findings of this study, it is not the main focal research purpose or objective.

The next section outlines the structure of the thesis and where each sub-question is addressed accordingly.

## 1.5 Thesis Structure

This thesis is structured into four main parts: **research strategy, background research, data collection and analysis,** and **evaluation.** These sections are outlined in the flowchart below and delineated by process steps, chapters, and sub research questions.

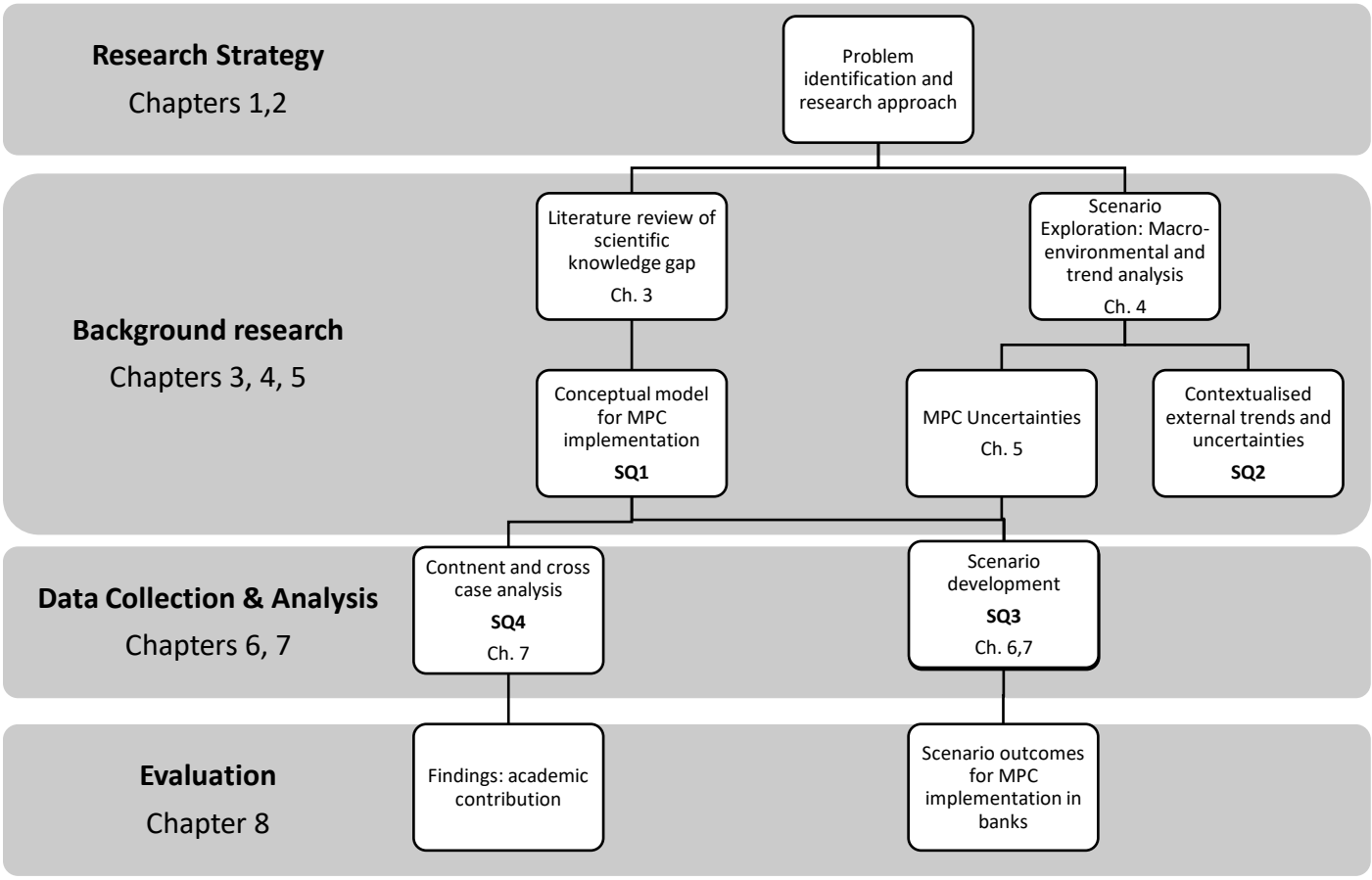



*Figure 1: Thesis structure flow diagram.*

The first phase, **research strategy**, establishes the research approach and deign choices for investigating the problem description and corresponding knowledge gaps. The main output of this phase is the formulation of the research question(s) and research design.

The second phase, **background research**, entails a literature review for theory development and for trends analysis in order to develop theoretical knowledge and practical knowledge. One of the outcomes of this theory development is a conceptual framework that describes the relationship between MPC implementation and business models, subsequently answering SQ1. The other output of this phase is obtaining practical information and knowledge about the external contextual environment of the EU banking sector and data ecosystem in order to start the scenario analysis method. The background research will be used as input for the next phase in scenario development and qualitative analysis.

**Data collection and analysis** is the third part of this thesis whereby, data is collected via semi-structured interviews to be analyzed via scenario analysis method and the qualitative case study methods. In the scenario analysis, validated uncertainties and initial scenarios will progress towards decision scenarios as the main deliverable of this thesis. In the case study methods, interviewee responses will be analyzed to further elucidate the link between MPC implementation and the business model concept.

In the last stage, **evaluation**, the scientific and managerial significance of this thesis will be evaluated based on the study's findings. Future areas of research and a descriptive recommendation for banks will be discussed.

The first sub question (SQ1) will be answered via a literature review (Chapter 3) in order to address the lack of theory and research for MPC business models. SQ2 is determined through desk research via micro-environmental analyses and trend analyses in Chapter 4. These analyses aim to be the foundation for determining the uncertainties in MPC implementation. SQ3 will require data collection from experts in the banking sector who can validate and identify the critical uncertainties of MPC implementation. SQ2 and SQ3 will contribute to the development of future scenarios for MPC implementation (Chapter 7). Lastly, SQ4 will be addressed via data analysis in Chapter 7. The answer to the main RQ will ultimately be answered in the findings chapter (8).

# 2. Research Design

There are numerous approaches within business research and social sciences that can be used to develop new knowledge for the research problem and academic disciplines considered in this thesis. The assumptions of the researcher as well as the cognitive and social dispositions of the sample study has implications on the manner in which the conceptual and practical knowledge is defined throughout the research process and presented at the end of this study (Kersti, 2014; Saunders et al., 2019; Sekaran & Bougie, 2016). Thus, this chapter aims to explain the justification for the research approach and methods used for addressing the research objective and research questions.

Firstly, the research philosophy and assumptions of this report are discussed to justify research approach. Secondly, the scenario analysis methodology is explained with accompanying objectives and criteria. Thereafter, the chosen data collection and analysis methods for the research design is outlined.

## 2.1. Research Approach

In the problem description, banks are challenged by leveraging data sharing and analytics for business model sustainability and risk frameworks. In order to investigate this problem, a qualitative research strategy is chosen to address the use of MPC that has yet to produce facts and figures about the economic and business value of its utility in banks. Due to the absence of empirical evidence of MPC in business contexts, scenario analysis and planning will be used to establish the current banking environment and what are the future possibilities to use MPC within this setting.

Business research is supposed to guide or seek solutions for managers to use or address the issues that the organization is facing (Sekaran & Bougie, 2016). Since the problem specification of this research encapsulates exploration of a social phenomenon within a business setting, the disposition of the researcher and the phenomenon to be studied should inform the research approach and methods (Saunders et al., 2019; Sekaran & Bougie, 2016). Research paradigms and philosophical perspectives has implications on how knowledge is developed and thus, contributed at the end of the research study (Saunders et al., 2019). However, there are multiple ways and perspectives to understand the problem and to investigate it. The research approach should take on a scientific approach so as to establish the reliability and generalizability of the findings for multiple organizations or in this case, EU banks (Sekaran & Bougie, 2016).

As a discipline, business and management research is underpinned by multiple philosophies, paradigms, and sciences (Saunders et al., 2019). Firstly, the ontological and epistemological views will direct and influence the research design, questions, and methods (Sekaran & Bougie, 2016). Ontology is the philosophy of what exists or the assumptions made about the nature of reality (Saunders et al., 2019; Sekaran & Bougie, 2016). Epistemology relates to the theory of how knowledge is established and generally the assumptions made about the nature of knowledge (Saunders et al., 2019; Sekaran & Bougie, 2016). The perspective or stance of these views in business and management research can range from positivism, critical realism, constructionism, pragmatism (Sekaran & Bougie, 2016), interpretivism, postmodernism (Saunders et al., 2019) and constructivism (Kersti, 2014) which infers the types of methodology used. Furthermore, the degree of objectivity and subjectivity with regards to studying organizations shapes the meaning and knowledge that this research project should deliver.

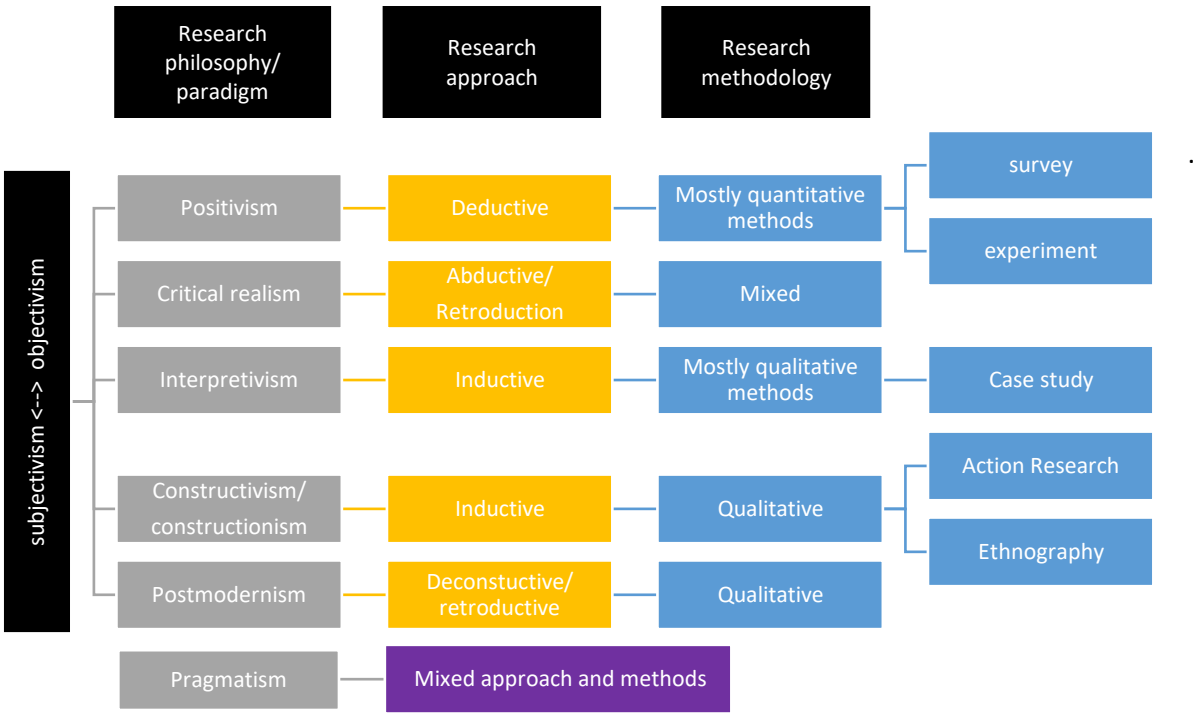



*Figure 2: Decision tree for research approaches constructed from research philosophies and paradigms in business and management research (Kersti, 2014; Saunders et al., 2019; Sekaran & Bougie, 2016).*

Figure 2 is a constructed decision tree for research approaches to theory development and methodology based on the philosophical frame of reference for business and management research. The complexity and diversity of business and management research design choices are not fully shown, but it can be used as a guide for a basic research strategy. The extremity or degree of objectivist and subjectivist dispositions inform the research philosophy or paradigm in grey. Typical approaches to theory development (yellow) follow from the philosophical assumptions of the researcher and problem to be studied. Consequently, these ontological assumptions can inform the epistemological assumptions of how research and knowledge should be carried out (blue). The justification for adopting a critical realist paradigm for this thesis is discussed below.

From an ontological viewpoint, this research entails studying banks within the EU and their current state of affairs for using MPC to enable banks to improve profit margins by some form of value creation and capture. Furthermore, what is not known is whether MPC can be used for improving risk management and monitoring and/or enable new business models. By definition, business research should be objective (Sekaran & Bougie, 2016). The extremity of objectivism and subjectivism can also vary in business research of organizations due to the diversity of social actors involved (Saunders et al., 2019). However, the proposed research objective cannot be espoused by an entirely objective and scientific approach such as that of an objectivist researcher. In the most extreme sense, 'an objectivist researcher wants to establish universal facts and laws governing social behavior by using assumptions from natural sciences' (Saunders

et al., 2019, p. 135). Since business research should be objective, a positivist standpoint would be suitable compared to subjectivist paradigms such as constructivism and interpretivism. However, MPC's contexts of use for achieving business value in banks cannot be observed or measured directly yet since MPC enabled risk frameworks or business models are not yet observable. Moreover, the business model concept is not entirely objective because it is shaped by shared realities and perceptions of what is valuable by actors in the organizations and by the target customers.

On the other hand, critical realism is less objective than positivist views by considering the subjectivist philosophy that some aspects of reality can be shaped by social actors and their mental processes and personal experiences (Saunders et al., 2019; Sekaran & Bougie, 2016). In order to consider the subjective perceptions of what is useful and valuable for MPC in a bank setting and business context, a critical realist philosophy is adopted for this thesis. Additionally, other views that try to bridge or reconcile objective and subjective aspects in research such as postmodernism and pragmatism are not suitable for the scope and purpose of the research objective. Postmodernism aims to deconstruct existing realities and interpret historical views and data in order to provide alternative worldviews (Saunders et al., 2019). Pragmatism searches for practical solutions to business issues with the consideration that some organizational function can be improved (Saunders et al., 2019). These research paradigms are complex in the sense that qualitative and quantitative methods are typically used; longitudinal data is necessary; and it assumes that there is already an existing and observable phenomena that can be changed (Saunders et al., 2019; Sekaran & Bougie, 2016). For these reasons, postmodernist and pragmatists dispositions cannot be applied for the research problem of this thesis.

However, ontologically speaking, there are drawbacks to what can be research or studied because MPC use and implementation in banks have not occurred yet. In critical realism ontology, there is a distinction between what is or can be observable, which is referred to as 'the actual' domain, and what is actually observed or experienced, which is referred to as 'the empirical' domain (Bhaskar, 2008; Wynn Jr. & Williams, 2012). Critical realism is also focused on causality and explanatory mechanisms which is referred to as 'the real' (Bhaskar, 2008; Wynn Jr. & Williams, 2012). The 'empirical' or the events and experiences such as MPC implementation by banks cannot be 'empirically' studied since this has yet to occur. Subsequently, 'real' or causal mechanisms such as social and physical structures that explain how MPC is used can also not be directly observed or measured yet, but can be theoretically investigated. Thus, this thesis will focus predominantly on 'the actual' or what can be observed or possible for MPC use in banks which will be further explored via **scenario analysis**. The critical realist ontology domains in the context of this study is illustrated in Figure 3. Each layer is a subset of the other whereby the 'real' and the 'actual' are minimally understood phenomenon for MPC implementation in organizations. Since these ontological domains are subsets of each other, the research approach requires the exploration of the real domain to understand the 'actual' domain. The empirical domain is not yet possible to investigate given the maturity stage of MPC technology.

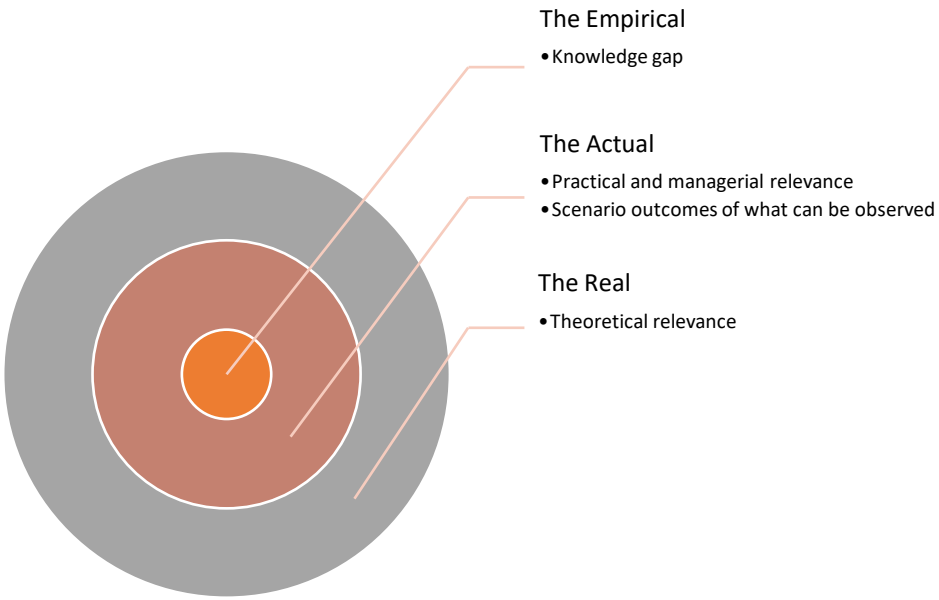



*Figure 3: Critical realist layered /stratified ontology adapted from* (Bhaskar, 2008; Saunders et al., 2019).

After establishing what can be studied ontologically, a critical realist position from an epistemological perspective informs how theory and knowledge is obtained and interpreted throughout the research process. Critical realist research approaches can bridge and combine methods and data from objective and subjective research strategies (Saunders et al., 2019). Hence, critical realism paradigms are underpinned by abductive approaches to theory development, meaning that the research process can include both inductive and deductive tactics in order to develop or modify theory (Saunders et al., 2019).

For new and emerging topics such as MPC, developing new theory for MPC business models would usually use inductive methods but due to the available time for this research thesis, a conceptual framework will be abductively derived instead. Furthermore, this study will be qualitative in order to account for bias and subjectivity of the research data which is more feasible to interpret from qualitative data. Additionally, mixed method approaches or triangulation is necessary in critical realist perspectives to account for flawed or inconsistent data, methods, and biases throughout the research process (Sekaran & Bougie, 2016). Thus, a qualitative research approach is chosen for the abovementioned concerns in dealing with the subjectivity of socially constructed business models and perception of MPC's utility and value in banks. Wynn Jr. & Williams (2012) identifies that critical realist approaches suppport the study of socio-technical phenomenons such as the implementation or use of information systems (p. 795).

The main deliverable of the research objective is conducted via scenario analysis. The social phenomenon is to understand the implications of MPC implementation and use within banks, with a focus on contexts of use in financial risk mitigation and enabling new business models. However, there are limitations to what is directly and objectively measurable and observable. Thus, scenario analysis will be used to deliver possible future outcomes to determine what can be observed for MPC implementation in banks.

## 2.2 Research Methodology – Scenario Analysis

This section outlines the research methodology used to address the aforementioned research problem and to execute the research objective. Firstly, the intuitive logics model for scenario analysis is introduced

as a method that aligns with the epistemological and ontological assumptions of this study. Secondly, the specific steps of the scenario analysis method is outlined according to the research assumptions and intuitive logics model. Thirdly, four judgment criteria for scenarios is established in order to guide and validate the scenario development process throughout the study.

### 2.2.1 Intuitive Logics Model for Scenario Analysis

Scenario analysis is a method for developing possible future scenarios to guide an articulated business idea towards strategic decision making (Schoemaker, 1995; Van Der Heijden, 1996). There are three schools of scenario techniques in extant literature which are the Intuitive-Logics model, La Prospective Model, Probabilistic Modified Trend Models (Bradfield et al., 2005). In order to ontologically and epistemologically align with the critical realist outlook for this study, the intuitive logics technique will be used. The objective of La Prospective adopts a pragmatic approach for developing or improving solutions whereas the probabilistic method coincides with a positivist and postmodernism stance in how scenario outcomes are developed and the predictive power it has (Bradfield et al., 2005; Saunders et al., 2019). Furthermore, the intuitive logics approach uses qualitative data for scenario development whereas the latter techniques are quantitative (Bradfield et al., 2005).

The intuitive logics model is described by Bradfield et al. (2005) as scenarios that are qualitative, slightly subjective to stakeholders' opinions, used for adaptive organizational learning and rely on 'disciplined intuition' (Bradfield et al., 2005, p. 807). The purpose and attributes of these scenarios are the most consistent with critical realism philosophy. Ontologically, it coincides with the integration of subjective views of social actors and the causality mechanisms of the business and contextual settings on socially constructed future outcomes. Epistemologically, it supports qualitative methods for data collection and analysis for delivering possible future scenarios. Moreover, inductive and deductive methods can be used for the intuitive logics technique which is also consistent with critical realist approach (Frith & Tapinos, 2020; Van Der Heijden, 1996).

### 2.2.2 Scenario Analysis Phases and Outcomes

In order to stay consistent with the research paradigms and philosophical assumptions, the chosen methodology will follow methods from the intuitive logics model. According to Frith & Tapinos, (2020), there are four phases for scenario analysis which are preparation, scenario exploration, scenario development and scenario utilization. Table 1 summarizes the main phases and chosen process steps for each phase in this research study. The fourth phase, scenario utilization, is out of the scope of this research because it entails testing the utility and effectiveness of scenarios within the organizations itself which is not feasible between the time of scenario development and future implementation of MPC.

| Scenario Analysis Phases | Process specification | Process and project outcomes | Reasoning/ justification | Reference(s) |
|---|---|---|---|---|
| **1. Preparation (Chapter 4)** | Define scope and determine time horizon of scenarios | Set up for macro-environmental analysis | Consistent with intuitive logics model (ILM); contextualized method for disruptive technologies | (Schoemaker, 1995; Schoemaker & Mavaddat, 2000) |
| | Determine validation criteria for scenarios | Judgment criteria for scenario development | Establish effectiveness and usefulness of scenarios | (Amer et al., 2013; Schoemaker & Mavaddat, 2000; Van Der Heijden, 1996) |
| **2. Scenario Exploration (Chapter 4)** | External (macro)environmental analysis analysis via STEEP or PESTLE analysis | Identification and selection of key drivers (predetermined factors or elements) and trends; examining contextual and contingent conditions for effective scenarios | Consistent with ILM; contextualize MPC in a business and bank setting; | (Bouwman, De Vos, et al., 2008; Bradfield et al., 2005; O'Brien & Meadows, 2013; Schoemaker, 1995; Schoemaker & Mavaddat, 2000) |
| | Determine macro-environment uncertainties according to plausibility and relevancy | Input for MPC uncertainties | Establishing utility of scenarios to stakeholders in banks | (Schoemaker, 1995; Schoemaker & Mavaddat, 2000) |
| **3. Scenario Development (Chapter 5, 6, 7, 8)** | Determine organization-specific uncertainties according to plausibility and relevancy via qualitative cluster analysis | Input for initial learning scenarios | Establishing utility of scenarios to stakeholders in banks | (Schoemaker, 1995; Schoemaker & Mavaddat, 2000) |
| | Inductively develop learning scenarios and validate with stakeholders according to plausibility, relevancy, novelty | Scenario narratives to challenge mental models | Challenge conventional thinking and existing mental models; transition from macro-environmental to organization specific environmental analysis | (Amer et al., 2013; Schoemaker & Mavaddat, 2000; Van Der Heijden, 1996; Wayland, 2019; Wright et al., 2013) |
| | Check for internal consistency and Morphological Analysis | Develop internally consistent scenarios | Meet judgment criteria for scenarios | (Amer et al., 2013; Schoemaker & Mavaddat, 2000; Van Der Heijden, 1996) |
| | Evolve towards decision scenarios | Decision scenarios for organizational learning | Improve decision making for MPC implementation within banks | (Schoemaker, 1995; Schoemaker & Mavaddat, 2000) |

*Table 1: Scenario analysis methodology for research study based on critical realist approach and intuitive logics model.*

Scenario analysis simplifies large amounts of data in order to map multiple uncertainties and several changing variables into a limited number of possible future states (Schoemaker, 1995). The development of possible future scenarios or states can be based on other frameworks in futures research such as trends

analysis and the PESTLE framework to account for environmental factors from multiple perspectives (Bouwman, De Vos, et al., 2008; Haaker et al., 2017). Scenario analysis goes beyond prediction and objective analyses such as computer simulations by coupling objective situations with subjective interpretations (Schoemaker, 1995). It can also include elements such as new regulations, value shifts, and innovations which help organizations to perceive their business environment for more robust decision making (Schoemaker, 1995; Van Der Heijden, 1996). This is relevant due to the changing landscape of financial services in the banking and finance sector. Scenario analysis has also been used as a tool to systematically process and assess the impact and robustness of business model choices (Bouwman et al., 2018; Bouwman, Zhengjia, et al., 2008; Gnatzy & Moser, 2012; Haaker et al., 2017).

As with the case of MPC, technological developments, legal implications and the socio-economic environment are uncertain. Due to the current maturity level of MPC technologies, proof of concepts and early pilots have yet to capture the economic and business potential in its irrespective potential use-cases. Therefore, technological uncertainties in its socio-technical environment need to be elucidated via the scenario analysis method. Furthermore, business models in the finance sector will experience a paradigm shift due to the growth of fintech, value shifts in customer empowerment, and rising developments in regulation (Rym; Ayadi et al., 2012). Therefore, scenario analysis should be applied in this study to facilitate in the conceptual evaluation for MPC enabled business models.

### 2.2.3 Criteria for scenarios

The criteria for scenarios in this study will guide the development of scenarios. The following criteria align with the intuitive logics model so that the criteria are also consistent with the research approach of this study.

In order to ensure that scenarios are valid, useful and effective, the judgment criteria for scenarios should be determined. The most important criteria of this study should be the plausibility of scenarios to ensure that the results of the study have meaningful use for researchers and practitioners. Secondly, scenarios should be consistent so that the logic of a scenario are not contradicted by the factors and scope that were selected for analysis. Furthermore, establishing consistency in scenarios allows for more accurate decision making. Thirdly, scenarios should be relevant to the stakeholders and interview participants in order to gather meaningful answers and prospects to base future research on. Relevancy is established by contextualizing interview questions and scenarios to a banking setting. Lastly, novelty ensures that scenarios challenge the organization's conventional perception about the future (Amer et al., 2013). Banks should inherently review and/or change their business models in order to remain competitive (Petralia et al., 2019). Therefore, creativity or novelty aspect should be a criterion in the initial scenario narratives and developed scenarios.

Utility/relevance is characterized by scenarios that 'contribute specific insights into the future that help to make the decision' (Amer et al., 2013, p. 36). Inherently, the purpose of most methods is to find plausible future scenarios. Furthermore, for most conceptual scenario analysis methods, the purpose is to trigger new thought processes and create new discussion for better strategizing and decision-making as characterized by the intuitive logics model (Amer et al., 2013; Wright et al., 2013). Therefore, scenario criteria such as relevance and novelty are not mutually exclusive and can be implied by the method.

Schoemaker's (1995; 2000) framework and the aforementioned four validation criteria are consistent with the characteristics of an intuitive logics model. Hence, Schoemaker's (1995; 2000) framework can be predominately used for this study but abiding by Van Der Heijden's (1996) recommended validation criteria: **plausibility, consistency, novelty, and relevance**.

The most suitable method used to select and validate raw scenarios in the third phase of scenario analysis is the (General) **Morphological Analysis,** referred to as GMA, because it accounts for more scenarios and uncertainties compared to the most common minimalist approach which uses two uncertainties for scenario development (Amer et al., 2013). The Morphological approaches are more suitable for this study compared to common methods such as the cross-impact analysis and the Wilson matrix. The cross-impact analysis helps determine the probability of trends occurring and thus, requires some form of a survey that records stakeholders' opinions on a rating scale (Amer et al., 2013). Since this study will gather answers from experts via semi-structured interviews, a cross-impact analysis will not be a suitable analysis method.

The Wilson matrix involves evaluating and prioritizing the impact and uncertainty of each scenario driver or factor (Amer et al., 2013). It ranks all drivers/factors against two dimensions: potential impact and probability that the trend/factor will develop into a significant issue (Amer et al., 2013). However, this coincides with the probabilistic model rather than intuitive logics model whereby the latter is the most suitable for the philosophical assumptions of this thesis. For further justification, GMA can explore all possible solutions in a multidimensional and qualitative manner whereby incompatible combinations of factors are eliminated and possible combinations are increased (Amer et al., 2013). GMA is an additional analysis method to formulate more accurate scenarios to account for subjective elements within the scenario analysis process.

The purpose of the study is to determine the plausible scenarios for MPC implementation within banks as well as evaluate the different business models that can arise based on these scenarios. Hence, research requires a more qualitative and introspective investigation rather than just determining the likely occurrence of a trend or uncertainty. In other words, cross-impact analysis and the Wilson matrix requires some form of quantitative measurement, scoring or rating of trends and uncertainties by stakeholders. However, this does not align with qualitatively addressing and evaluating the subjective nature of socially constructed realities due to the disparities of mental models across social actors. Therefore, the GMA is chosen as a suitable method for this study.

## 2.4 Data Collection

This investigation of MPC implementation among EU banks has not been conducted previously. There is no theory on the impact of MPC on business models and therefore, building the conceptual knowledge will take an exploratory and abductive approach. Abductive reasoning or thinking is used to *"explore a phenomenon, identify themes and explain patterns to generate a new or modify an existing theory"* (Saunders et al., 2019, p. 160). Therefore, abduction will be used to formulate an initial conceptual model in order to link two fields of research, IOS and business models, to MPC implementation in banks.

Additionally, conducting semi-structured interviews is the most suitable method for balancing an exploratory approach to investigation while gaining structured responses that abide by the criteria for scenario analysis. As such, conducting interviews is also required for gaining stakeholder input for scenario analysis (Van Der Heijden, 1996). The sampling of interviewees is based on access and availability to experts within the EU banking ecosystem. This is characteristic of judgment sampling which is defined as "*a purposive, nonprobability sampling design in which the sample subject is chosen on the basis of the individual's ability to provide the type of special information needed by the researcher*" (Sekaran & Bougie, 2016, p. 393).

Semi-structured interviews will be conducted with relevant stakeholders and experts who can provide valuable input in determining the possible outcomes of MPC implementation within their organizations. The main targets for interviews are experts within major EU banks who have technical knowledge or ability to understand MPC so that they can provide more qualitative feedback. Since MPC might be a new topic to some people, the MPC concepts can be explained to interviewees with technical knowledge or backgrounds who can apply and translate those ideas into business opportunities.

Interviews will be the main source for primary data and analysis in this thesis. Secondary data from desk research and academic literature will be utilized for guiding the main principles of the research question and sub-questions as well as the conceptual evaluation of MPC implementation scenarios. Given that there are constraints to gaining data for such a new topic, data analysis methods are necessary to make a more formalized and structured interpretation of the available data.

## 2.5 Data Analysis

Data analysis in this study involves the evaluation and interpretation of stakeholder input to produce useful scenarios. Additionally, a completely objective truth is implausible since MPC implementation in banks have yet to occur. Therefore, the subjectivity in possible scenario outcomes need to be analyzed. Scenario outcomes are a product of socially constructed answers which can be subjective in nature depending on the interviewee's background and interpretation of the interview questions. Subjectivity can undermine the effectiveness of scenarios as well as the validity of the findings. Therefore, data analysis is used to judge scenarios against a set of criteria. Furthermore, analysis and interpretation of data is necessary to understand the limitations that exist in researching a new topic such that areas of improvement and open problems can be identified for future research.

The data collection and analysis approach is not sufficient enough to conduct an extensive case study. However, some case study methods are useful in gaining in-depth contextual insights into the research problem (Yin, 2018). In case study research, Yin (2018) states that the purpose of the analytic strategy is to link collected data to theoretical concepts of interest and to have those concepts guide the data analytic process. Thus, the implications of this research may serve as a basis for theory building in MPC business models and future experiments and so some elements of a case study analytic strategy will be adopted in this thesis. The research design aims to use a mixed method approach to data analysis in order to account for some of the limitations in relying mostly on interview responses which can threaten the validity of research findings.  On overview of the research design framework is shown in Figure 4.

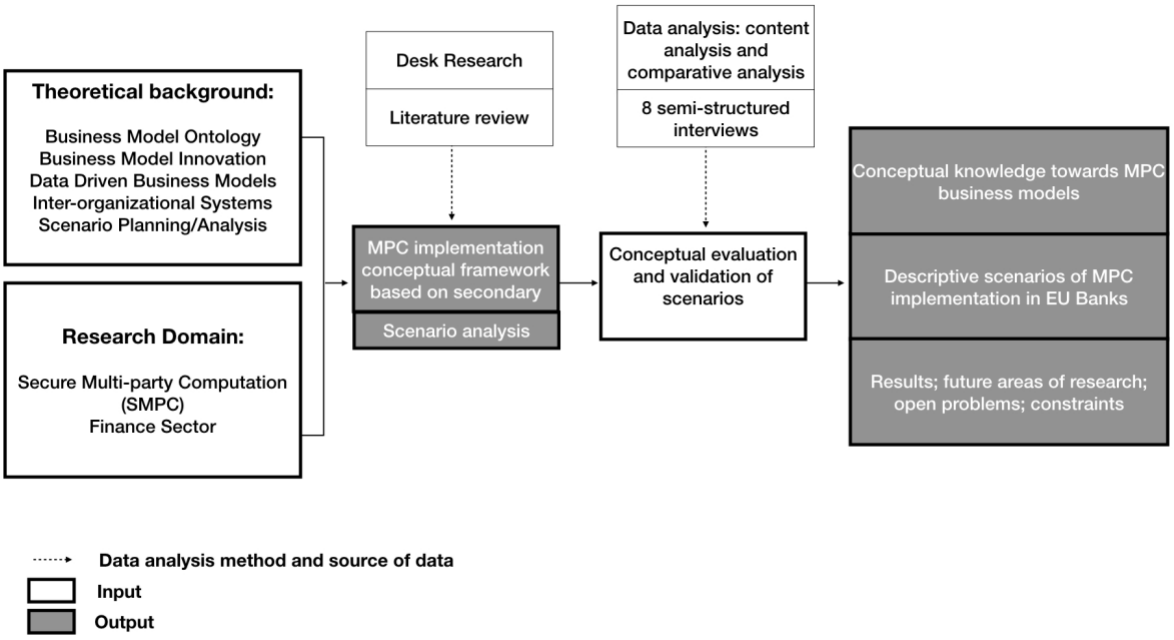



*Figure 4: Overview of Research Design Framework*

Firstly, one method for qualitative data analysis in this study is content analysis. A content analysis can be a qualitative and deductive analytic approach that aims to extend concepts and theory (Hsieh & Shannon, 2005). In this approach, the coding of interview transcriptions is used to identify concepts that connect MPC to business models and to understand some of the correlations in MPC implementation scenarios. Moreover, computer assisted qualitative data analysis (CAQDA) tools may be used to assist with the coding of data and to maintain a case study database or chain of evidence (Yin, 2018). The Atlas.ti software program will be used to keep track of codes and coding cycles or iterations as a means to increase the reliability of the research design.

Secondly, there can be differences between interview responses depending on the bank and expertise of the interviewee. These differences can weaken the reliability of scenarios. On the other hand, collecting data from different banks versus one bank may provide alternative interpretations that may strengthen the validity of the research. A cross-case analysis is typically used to evaluate differences between organizations in a multiple-case study design (Yin, 2018). Given the limitations in this study, a general comparative analysis of banks and their interview responses is used to identify and interpret these differences and how it might influence research validity. Unlike coding and data analysis, differences and similarities will be cited and evaluated by organization.

The following chapters in this thesis entails background research (Chapter 3 – 5), data collection & analysis (Chapters 6 – 7), and evaluation of the research findings (Chapter 8).

# 3. Literature Review

The purpose of this chapter is to determine the underlying theories that can be used as a frame of reference for understanding MPC in a business context. The findings from this literature review will be used to formulate a general conceptual model that may indicate whether the potential outcomes of MPC implementation and use have implications on business models of firms. Furthermore, by the end of this review, SQ1 of this study should be answered:

**How does value creation theory correlate MPC implementation and business model concepts?**

The first subchapter (3.1) is a literature review of the research domains in MPC and finance. In this chapter the historical view of MPC to the current state of MPC is discussed, predominately from a business research perspective. Further review of MPC applications and business models in banking serves as a foundation of information for readers in these topics. The second subchapter (3.2) focuses on the theoretical components of this thesis and the development of a conceptual model for MPC implementation. In the last subchapter (3.3), SQ1 is answered. The literature review method can be found in Appendix A.

## 3.1. Research Domains

The purpose of this subchapter is to discuss MPC and business model concepts in order to contextualize MPC from a business model perspective. Firstly, MPC and its potential applications will be defined in order to understand MPC contexts of use in banking (Section 3.1.1 – 3.1.3). Secondly, the current state of MPC technology and barriers are discussed (Section 3.1.4). Thirdly, background research into the current and future state of banking business models are outlined (Section 3.1.5).

### 3.1.1 MPC Definition

MPC must be defined in order to order to understand its contexts of use. Secure MPC is a type of cryptography that enables distributed parties to carry out a joint computation on shared data in a secure manner whereby each party's dataset is not revealed (Ankele et al., 2016; Lindell & Pinkas, 2009). More specifically, MPC uses mathematical algorithms in which the *"computation problem is defined by a set of parties* $P_1 \ldots P_n$*, each with their private inputs* $X_1 \ldots X_n$*, jointly computing a function* $f(X_1, \ldots, X_n) = y$*"* (Ankele et al., 2016, p. 1). In other words, it can enable competing businesses ($P_1 \ldots P_n$) to perform data analytics ($f(X_1, \ldots, X_n) = y$) on shared data whilst keeping their individual datasets ($X_1 \ldots X_n$) private from each other. Every party $P_n$, will not have their data input $X_n$ revealed when the function $f(X)$ *is perfomed via MPC.* According to Lindell & Pinkas (2009), the requirements for secure computation protocols are *privacy*, *correctness*, *independence of inputs*, *gauranteed output delivery*, and *fairness* (p. 5). These requirements stipulate that all honest parties should be entitled to receiving a correct computed output regardless of the presence of dishonest parties whereby the secrecy of their independent raw data is preserved.

### 3.1.2 Historical Background of MPC

The origins of MPC was developed by Andrew Yao in the 1980s where he created a secure computation protocol among two parties (Yao, 1982). His protocol was developed under the premise that there are two people who want to know which one of them is richer, but neither of them want to disclose their wealth to each other or to a third party (Yao, 1982). This is now referred as Yao's Millionaire problem within MPC literature. The two key aspects of his algorithm are to safeguard against saboteurs or adversaries who may threaten the security of the computation and to ensure privacy of the millionaires' data inputs (Yao, 1982).

Yao's two-party computation protocol was further developed by Goldreich, Micali, & Wigderson (1987) into a multi-party computation protocol. Both of these protocols utilize a cryptographic technique called *Oblivious Transfer* (Evans et al., 2018). A simplified notion of Oblivious Transfer is that Party A has secret inputs and Party B can select one of these secret inputs, whereby the function of the protocol does not reveal which secret input was selected by Party B and what the other secret inputs were (Evans et al., 2018). Oblivious transfer protocols can involve two or more parties and are the building blocks of MPC (Evans et al., 2018). Subsequent protocols by Beaver, Micali, & Rogaway (1990) and Ben-Or, Goldwasser, & Wigderson (1988) utilize secret sharing. *Secret sharing* or verifiable secret sharing is a cryptography scheme in which multiple parties hold a private share of a value that can ultimately be recovered by the participants involved in the computation using their encryption keys (Beaver et al., 1990; Ben-Or et al., 1988; Haaften et al., 2020). Moreover, it is important to note that these methods protect against bad actors from making unauthorized operations or obtaining the secret value from its output values. Thus, being more *secure* than two-party computation. These initial methods and schemes have developed into the modern notion of (secure) multiparty computation or privacy preserving computation. Contemporary MPC protocols can use the properties of additive homomorphic encryption, fully homomorphic encryption, and different secret sharing schemes which are already established cryptographic techniques (Evans et al., 2018; Haaften et al., 2020).

### 3.1.3 Current state of MPC technology

The current state of MPC technology is discussed in this section as a means to form an understanding of how MPC might be implemented in the future. MPC applications are promising to many industries seeking to secretively and securely share data, but implementing MPC depends on the use-case.

Ankele et al. (2016) state that the limitations in large scale MPC applications stem from a large communication overhead between players involved in the exchange, the computational power necessary for implementation, storage needs for enormous key sizes, and the investment needed to implement cryptographic operations against malicious adversaries. Kanger & Pruulmann-Vengerfeldt (2015) note that developers also lack the knowledge and resources to fully realize application potential of the technology. Additionally, articulated user preferences are either absent or not clearly defined (Kanger & Pruulmann-Vengerfeldt, 2015). User preferences may also be unique to every use-case or group of parties and this can make it difficult to establish a comprehensive framework for user and technical requirements. Moreover, given the transition from theoretical models to proof of concepts and pilots, MPC has evolved from a single protocol to a growing class of protocols for specific use-cases.

In order to generalize MPC operations, Archer et al. (2018) defines three generic roles in MPC applications:

1. Input Parties who are responsible for delivering private input data for the computation;
2. Result Parties who receive the results of the computation;
3. Computing Parties who jointly participate in the computation (Archer et al., 2018, p.2).

Furthermore, Archer et al. (2018) state that despite the differences in properties across various MPC protocols, all MPC protocols should share the concept of "no single point of trust" (Archer et al., 2018, p. 2). This entails that none of the involved computing parties can individually gain access to the encrypted input (Archer et al., 2018). If all parties agree on a set of rules to follow in order to maintain integrity and equality in the system, then each MPC operation and algorithm may be a specialized case. Hence, scalability may be a barrier in commercializing this technology. Scalability issues suggests that there could be higher costs to use MPC which narrows its users to larger organizations and corporations.

In conclusion, despite the absence of a business framework for MPC implementation, some of these early MPC requirements and properties can be expanded upon over the course of this study. It is apparent that

full system capabilities of MPC is not fully understood. In turn, design requirements and system capabilities can still be changed and structured depending on researchers and early adopters. Since there is an inability to foresee deployment and implementation issues during the technical development phases, the social and business implications of MPC are still unfounded and speculative. It is expected that scenarios will expand and elaborate on the technical requirements and socio-technical concerns for MPC.

### 3.1.4 MPC Applications in Banks

MPC has evolved from a single protocol to a growing class of protocols for specific use-cases (Archer et al., 2018). Secure multiparty computation can be used for many computational problems that requires cryptography (Lindell & Pinkas, 2009). According to Lindell & Pinkas (2009), applications of MPC include *"electronic auctions and bidding, electronic voting, or privacy-preserving data mining*" (Lindell & Pinkas, 2009, p. 4). On the other hand, confidential benchmarking has been used to aggregate data from multiple parties such as financial institutions to improve credit checking and reports while safeguarding sensitive data (Archer et al., 2018; Damgård et al., 2017; Frikken, Atallah, & Zhang, 2005). Furthermore, data privacy regulations such as the GDPR is causing organizations in the public and private sectors to shift to more efficient privacy methods and/or become more cognizant of the consequences of sharing data. MPC can benefit organizations by enabling them to share and leverage data without violating regulations especially in the financial and healthcare industry wherein data is extremely sensitive.

The aforementioned applications for benchmarking credit scores and reports may also lead to the development of MPC based fraud detection schemes (Sangers et al., 2019). MPC can enable secure integration of financial data from multiple companies which can improve fraud detection of dishonest borrowers (Bogdanov et al., n.d.; Sangers et al., 2019). This can translate into multiple fraud detection schemes such as company tax fraud, health insurance fraud, and anti-money laundering (Bogdanov et al., n.d.; Rabobank, 2020).

MPC can facilitate secure sharing of financial portfolios for better decision-making in mitigating financial risk (Watanabe & Koseki, 2014). Lastly, benchmarking competition with other financial institutions or determining bank stress tests with financial regulators have been demoed and identified as viable use-cases (Volgushev et al., 2016).

Furthermore, there are potential applications and use-cases for intrusion detection that could be valuable to banks (Du & Atallah, 2001). Scenarios wherein companies share metrics of intrusion behavior and data patterns of hackers can improve their intrusion detection systems (Du & Atallah, 2001). Another potential application involves sharing data about an adversary's behavior during a break-in and using that data to query multiple profile databases (Du & Atallah, 2001).

In conclusion, MPC can have wide scale applications in any data analytics scenario whereby data sharing is precarious or illegal. Secure MPC can be developed and adapted for very specific use-cases. Data sharing via secure inter-party collaboration of the public and private sectors can potentially change the landscape of many facets of society wherein knowledge and information sharing is no readily accessible or possible. Some examples could entail cross-sector or cross-industry data sharing and collaboration as well as private-public sector partnerships. However, empirical evidence of these applications and use cases are lacking in academic literature. Nonetheless, MPC is positioned to provide value for businesses to improve the quality of their data analytics for better insights as well as improve coopetition and collaboration in B2B environments.

After a comprehensive review of MPC applications in banks, it is clear that trust should be guaranteed by the design requirements of the protocol as well as enforced by the participating parties. MPC values and characteristics are related to MPC implementation decisions. It can partly inform what the use-case requirements should be and the what the implications might be.

### 3.1.5 Business Models in the EU Bank Sector

European banks have seen a transformation and restructuring of their business models after the 2008 financial crisis which also resulted in new regulations for banks requiring financially stable and less risky business models (Rym; Ayadi et al., 2012, 2017; Kok et al., 2016). Contemporary financial services and banks are being disrupted by the coined term, 'fintech', which will further shift the paradigm of banking business models in the financial sector (Gomber et al., 2018, 2017; Lee & Shin, 2018).

According to Ayadi et al. (2017), the financial crisis emphasized the importance of business models to monitor and manage risk in evolving market structures and regulations. This led to a need for more supervision and regulation in order to establish more transparency in bank activities (Rym; Ayadi et al., 2012; Rym Ayadi et al., 2012). However, the rise of fintech also has implications on financial risk and transparency much like the financial crisis did because fintechs are not bound by the same transparency rules and regulations (Petralia et al., 2019). The changes in financial service technologies are changing faster than regulation. However, regulations will eventually have to change in order to warrant further trust and transparency of novel financial systems and services. In order to prevent incidents like the financial crisis, effective and transparent risk frameworks and innovations will have to be managed by the banks itself and by higher supervisory entities. The undertaking of new forms of risk due to new technologies ultimately has implications on banks' business models.

Moreover, business models are essential for the survival of banks. Business model transformation and innovation are also necessary to keep up with fintech start-ups that are competing and overtaking product lines and customer segments from larger banks. Business model sustainability is preferred and becoming more required by regulators (Lueg et al., 2019, p. 102). However, banking business models are not entirely data-driven. Brownlow, Zaki, Neely, & Urmetzer (2015) report from a random sample of four established businesses in the finance sector that the dominant offerings were non-data products or services. Furthermore, B2B customer targeting was lower compared to other sectors in insurance, publishing, retail and telecom (Brownlow et al., 2015). This suggests that banks are not well-positioned to strategically implement new data driven business models for B2B environments. Therefore, banks may lack the knowledge and experience to leverage data-driven technologies such as MPC for their business models.

## 3.2 Theoretical Background

This subchapter aims to clarify business model concepts and IOS theories that can be applied to MPC. Firstly, reviewing different business model concepts will provide a conceptual basis for underlying business model theories that can be linked to IOS. Secondly, the theoretical foundation of inter-organizational systems will be the starting point for abductively using the historical view of data sharing via information systems to gather insights on plausible MPC characteristics. Thirdly, value creation and IOS theories are reviewed to further analyze and conceptualize data sharing mechanisms in inter-organizational environments. Fourthly, extant literature in data-driven business model research is reviewed as a means to formulate a comprehensive view of business model concepts that addresses the data aspects in MPC applications. Lastly, business model innovation is discussed as well to build a conceptual framework that links IOS implementation outcomes to value creation business outcomes.

Based on an abductive approach, the underlying theories in business models and IOS fields is used to derive a conceptual model for MPC implementation outcomes.

### 3.2.1 Digital Business Models

In order to understand how business model concepts can be applied within this thesis, a review of extant literature is needed to define and outline business models and its components. There is no standard business model framework in academic literature (El Sawy & Pereira, 2013; Osterwalder, 2004; Osterwalder, Pigneur, & Tucci, 2005).

The review of business model definitions and concepts in literature have an underlying theme in constructs that either explain or describe business models as a tool for value creation (El Sawy & Pereira, 2013; Osterwalder et al., 2005; Ritter & Lettl, 2018; Shafer et al., 2005). Business models are used as a guiding principle to create and capture value which ultimately results in economic value and profit (Shafer et al., 2005). Ritter & Lettl (2018) interprets business models as an explanation of *"how an actor is positioned within a value network or supply chain, and how a business turns inputs into outputs while fulfilling its goals"* (Ritter & Lettl, 2018, p. 1). More widely cited authors such as Chesbrough & Rosenbloom (2002) describe successful business models to link the potential of technology with the realization of economic value. Furthermore, the conceptualization and definitions for value creation, value capture, and value propositions vary in extant literature reviews.

The components of a business model, summarized in Figure 6 should provide an indication of which business model is best suited for an organization's purpose. However, this creates challenges in establishing a formal definition and unified framework for business models. This notion is reinforced by Shafer et al. (2005) who argues that business models can fail due to flawed assumptions and misunderstandings about the underlying core logic of business models. Consequently, this can derail the practicality of business models in real business settings wherein practitioners are not fully aware of which business model to use and how to use them optimally.

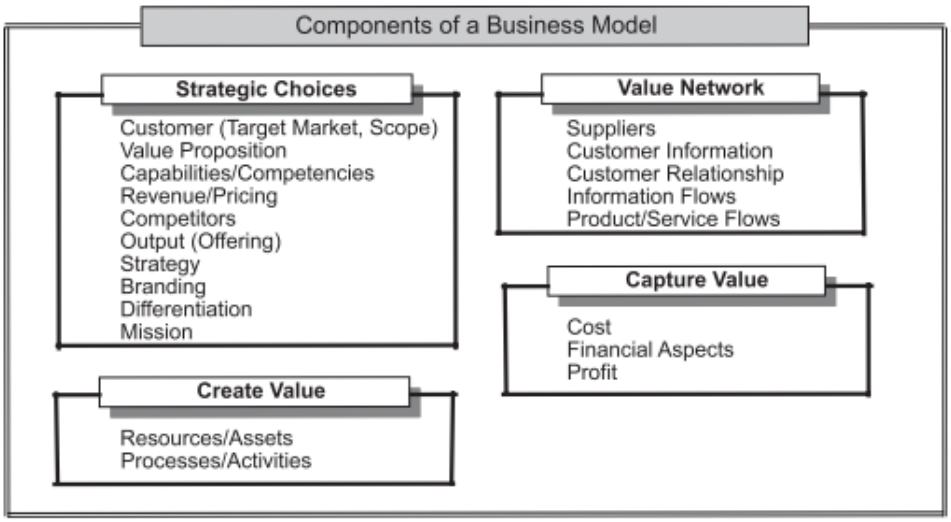



*Figure 5: Components of business model affinity diagram* (Shafer et al., 2005, p. 202).

A list of business model frameworks and definitions can be found in Appendix B: List of business model frameworks. According to Wirtz, Pistoia, Ullrich, & Göttel (2016), modern business model research and concepts for the new economy includes business models from 2000s to present. Business models within

this time period and the number of citations in academic literature are the selection criteria for that list. Academic papers that were also cross-referenced in data driven business model research and comprehensive business model literature reviews was the third selection criteria.

The diverse definitions and conceptualizations of business models show that the premise of **a business model is essentially a prescriptive and descriptive representation of how a firm creates and appropriates value.** According to DaSilva & Trkman (2014), the use of the 'business model' term was scarce until the inception of information and communication technologies and the world wide web in the 1990s. Thereafter, the use of business model terminology grew and diversified due to digitalization and technology- and internet-based companies (DaSilva & Trkman, 2014). There are a multitude of definitions of business models due to a lack of formal definition as well as endeavors to build upon theories of prior business model concepts. As such, business models seem to develop and evolve with technologies which suggest that technology and business model concepts are interrelated to some extent.

Business model definitions and concepts vary depending on the context, scope and theoretical perspective of the authors (Lambert & Davidson, 2013). Furthermore, bank business models are becoming more varied and specific to the organization, shifting away from a 'one size fit all' approach (Lueg et al., 2019). In MPC applications, it is unknown what the business model components will be and therefore, it is difficult to justify which business model tool, method, or other frameworks is the most suitable. For instance, the output of MPC is some form of data and how this data will be used to create value for banks is mainly speculative. Perhaps, it can be sold, or it can be used to improve internal processes, or it can enable new products and services. A quantitative study of 63 EU and U.S. banks even suggest that managers within banks inaccurately choose business models based on biases rather than performance indicators (Lueg et al., 2019).

Adopting an existing business model framework for this study would require more descriptive knowledge about MPC business components which is still undocumented in literature and therefore, this investigation is part of the research objective (SQ4). There is not enough evidence to support that the general business model frameworks reviewed for this study are suitable for MPC applications. Instead of unjustifiably, and hence inaccurately, selecting a general business model framework, a more useful approach is to use the underlying theories within these frameworks as a foundation of knowledge. The underlying theories for value systems in digital business models are transaction cost economics and resourced based view (DaSilva & Trkman, 2014; Zott & Amit, 2010). In the next section, IOS is reviewed to determine underlying theories that may coincide with business model logic.

### 3.2.2 Inter-organizational Systems (IOS)

Inter-organizational systems or IOS is defined as information systems that allow organizations to link business processes, pool information resources, and share data (Robey et al., 2008). IOS research is relevant to this study because it discusses why organizations collaborate in B2B data sharing (Elgarah et al., 2005; Narayanan et al., 2009; Robey et al., 2008), the dynamics of interorganizational relationships which can influence data sharing (Elgarah et al., 2005), and the derived benefits and outcomes of IOS implementation (Narayanan et al., 2009; Robey et al., 2008). MPC systems also serves the same purpose as IOS where organizations can aggregate and share data in cooperation.

IOS paradigms also integrates theoretical concepts and frameworks to link the variables of technology implementation to social, organizational, and strategic outcomes (Narayanan et al., 2009; Robey et al., 2008). Therefore, IOS literature can lend itself useful in contextualizing MPC according to Saunders' et al. (2019) definition of abduction in business and management research. Hence, this academic field will also

prove useful in informing scenario development. Moreover, IOS research can help conceptualize the social context of interorganizational data sharing and the social values (e.g. institutional trust) that influence implementation decisions (Robey et al., 2008) and interorganizational relationship motives (Elgarah et al., 2005). This aligns with critical realist assumptions that the reality of interorganizational data sharing is not mutually exclusive from social values of the organization and people in those organizations. Given these similar properties, MPC will be considered a type of IOS technology in this study. Therefore, IOS theories will be used to derive an MPC conceptual framework.

There are three main aspects of IOS: (1) factors influencing organizational adoption of IOS; (2) the impact of IOS on governance over economic transactions; and (3) the organizational consequences of IOS (Robey, Im, & Wareham, 2008, p. 498). It can be assumed that banks who agree to be interviewed for this study intend or want to adopt MPC. For the purposes of focusing solely on the research objective which is the implications of MPC use, antecedents to MPC implementation will be out of scope for this thesis. The scope of this research will focus on the organizational consequences of IOS because these have **operational, social, and strategic outcomes** that may have a contingency on business model innovation.

Firstly, operational outcomes refer to more efficient operations and processes within the organization which is a likely benefit of IOS implementation (Robey et al., 2008). Transaction efficiency is one of the most common and observed consequences of IOS technology use (Elgarah et al., 2005; Robey et al., 2008). Transaction efficiency is supported by reduced transaction costs within business processes which impact operational outcomes (Robey et al., 2008). Secondly, social outcomes include organizational change in the form of process innovation as well as interorganizational relationship dynamics and structure (Robey et al., 2008). Organizational change relates to transforming ways of working as well as implementing novel processes. According to Robey et al. (2008), IOS enabled business process change result in superior business outcomes. Thirdly, the strategic impact of implementing IOS technologies can produce competitive advantage and result in new product and service innovations. IOS technologies can broaden a firm's network and bring added benefits and value (Robey et al., 2008). However, these added benefits are contingent on the interfirm relationships within the network that should be governed by trust. These concepts are illustrated in Figure 6 to describe the relationships between IOS implementation and organizational outcomes. The conceptual framework is adopted from Robey et al. (2008) and will be used as a starting point and foundation for contextualizing MPC in a business environment.

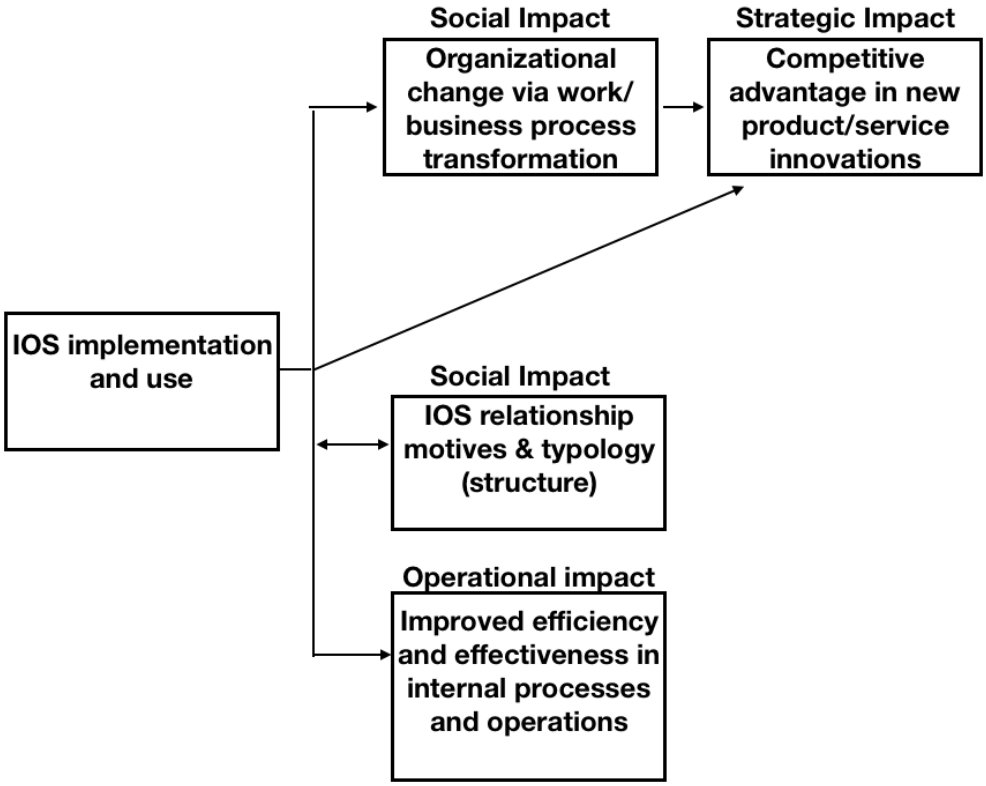



*Figure 6: Relationships investigated in organizational consequences of IOS implementation (Robey et al., 2008, p. 505).*

This figure expresses and contextualizes IOS in an organizational setting which can expand the understanding of MPC in a similar fashion, with the assumption that MPC is an emerging technology in the IOS field. However, in order to use this framework to address the main RQ, it needs to be further developed by integrating business model concepts. According to Robey et al. (2008), establishing theoretical foundations is important for IOS research and emerging technologies in this landscape. Thus, value creation theories will be used for this purpose since it is an underlying theory in strategic outcomes of IOS implementation (Robey et al., 2008). Furthermore, value creation is also important in business model concepts. Then, a conceptual framework for MPC implementation outcomes in the sense of business model opportunities can be developed by linking business model concepts and MPC via value creation theories. In subsequent sections, different disciplines of business model literature are assessed for this reason.

### 3.2.3 Value Creation Theories

Value creation concepts are related to business model concepts because business models are generally used as a tool for value creation among firms (Section 3.2.1). Underlying value creation constructs will be used to link concepts from business model, IOS and MPC research. By considering the value creation theory from different fields, it can provide insight into the potential value activities of inter-organizational data sharing and its implications on business models. The aim is to translate and link these ideas to MPC applications.

Amit & Zott (2001) are widely cited authors for their studies in e-business value creation and business models. They define 'value' as *"the total value created in e-business transactions regardless of whether it is the firm, the customer, or any other participant in the transaction who appropriates that value"* (Amit

& Zott, 2001, p. 503). Furthermore, value drivers are considered to be factors that enhance the total value creation and capture by an organization (Amit & Zott, 2001).

In some instances, value creation can dictate business model design choices and innovation. Hence, value creation drivers can also be used to determine value drivers for business model innovation (Amit & Zott, 2012). In the context of virtual markets, Amit & Zott (2001) argues that the drivers for value creation are contingent on the interdependencies between four factors which are: **efficiency, complementarities, lock-in,** and **novelty**. This value creation framework is used due to its grounded theory in organizational theory such as resource based view and transaction cost economics which also underpins IOS organizational outcomes and business model frameworks (Amit & Zott, 2001; DaSilva & Trkman, 2014; Robey et al., 2008; Wirtz et al., 2016). The four main drivers of value creation are discussed in order to elucidate how value may be created in data-sharing environments which can be found in *Appendix B*.

From this review, it can be concluded that all four value drivers can be applied to MPC scenarios with the assumption that MPC is classified as an IOS. MPC is also use-case dependent and thus, the value drivers in MPC systems align with Amit & Zott's(2001) notion that drivers are interdependent. Moreover, the importance of each driver is contingent on the use-case as well for MPC systems. For instance, there may be more efficiency in the type of MPC collaboration as opposed to the system capabilities of MPC and vice versa. Since these value drivers are heavily use-case specific, these concepts cannot be generalized and condensed into a single conceptual framework for MPC implementation.

Transaction cost economics is also embedded in value creation and IOS theory but it is more focused on the governance structures of IOS which precedes IOS implementation (Robey et al., 2008). Thus, it is more important to focus on RBV theory for building a conceptual framework for MPC implementation. Resource based view is one of the main theories that are used to understand business models, value creation and IOS implementation as depicted in Figure 7 (Amit & Zott, 2001; Robey et al., 2008). However, value creation and IOS implementation is also influenced by network theory (Amit & Zott, 2001; Robey et al., 2008). Therefore, Lavie's (2006) extension of RBV from a network perspective is better suited to utilize for the development of a conceptual framework. In Appendix B, traditional and networked RBV is further discussed and compared.

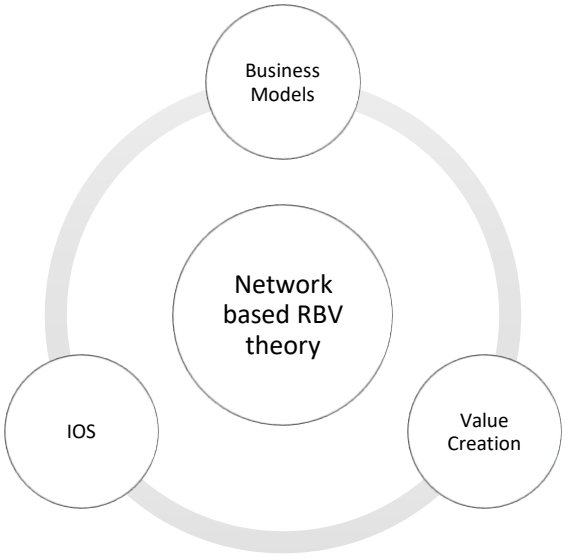



*Figure 7: RBV theory underpins the academic disciplines that are used to contextualize MPC.*

Within networked RBV theory, value-creating resources are also based on the resources of the firm's collaborators and partners via interorganizational alliances (Lavie, 2006). Pooling alliances share resources of a similar type that is more characteristic of a reciprocal interorganizational relationship (Lavie, 2006). Whereas, complementary alliances are indicative of enabling power dynamics since distinctive resources are shared for synergies effects (Lavie, 2006). Thus, value creation and capture is enabled by the dynamics of sharing and collaborating in order to gain either: heterogenous resources or homogenous/complementary resources (Lavie, 2006). The extent of value capture by each firm may differ due to bargaining power, opportunistic behavior, and competitive position that a firm may undertake (Lavie, 2006). These notions from RBV theory support that a bank can create value from using MPC for interbank and non-bank collaboration, data sharing, and leveraging non-shared and shared resources synchronously.

### 3.2.4 Data Driven Business Models (DDBM)

The aforementioned business models consider the aspects of technology and digitalization. However, these business models do not focus on how data is leveraged for businesses and to what extent that it influences business models among firms. Academic and scientific research on data driven business models (hereafter DDBMs) are limited. DDBM frameworks are mostly extensions or adaptations of Osterwalder's (2004) theories for value proposition and his business model canvas (Benta et al., 2017; Kühne & Böhmann, 2018; Mathis & Köbler, 2016; Schuritz & Satzger, 2016). Evidently, there is no widely accepted formal or scholarly definition of DDBMs (Benta et al., 2017; Hartmann et al., 2014; Kühne & Böhmann, 2018; Mathis & Köbler, 2016; Schuritz & Satzger, 2016).

From a selection of 30 papers of data-driven business model research, only a few papers explicitly define a DDBM. Most authors adopt Hartmann's et al. (2014) definition of a DDBM which is expressed as *"a business model relying on data as a key resource"* (p.4). In essence, data-driven business models utilize, exploit, or capitalize on data as a main or key resource (Hunke et al., 2017; Kühne & Böhmann, 2018; Schuritz & Satzger, 2016). Other variations of DDBM definitions in literature are listed in Table 2 below.

| Author | DDBM Definition |
|---|---|
| **(Hartmann et al., 2014, p. 4)** | "…a business model relying on data as a key resource." |
| **(Zolnowski et al., 2016, p. 2)** | "When data are exploited as main resource for innovative service business models, they are called data-driven business models" |
| **(Benta et al., 2017, p. 350)** | "…Data- driven business model shows the potential of implementing collected user data from the companies' products and services as well as the needed data resources for offering data-driven value proposition." |
| **(Kühne & Böhmann, 2019, p. 4)** | "...we define data-driven business models as business models which use data as a key resource to create new insights for a value proposition for customers." |

*Table 2: List of DDBM definitions*

Moreover, existing DDBM literature which is partially summarized in Appendix B consists of taxonomies, frameworks and process models that bolster the understanding of the utility and capitalization of data-based products and services. These papers have varying methodologies, contributions, and perspectives in evaluating and conceptualizing DDBMs. In all papers, there is a commonality that researchers present or state the challenges with utilizing (big) data and that the perception of big data and its definition can differ in academia and industry which requires more validation and empirical research. These challenges

are most notable in papers from Bulger et al. (2014); Kühne et al. (2019); Schroeder (2016). However, most papers either reference or adopt Hartmann's et al. (2014) taxonomy for DDBMs and therefore, this framework will be used in this study to address the data aspect for MPC enabled business models.

As previously mentioned, there are obstacles in leveraging (big) data and analytics as a main resource for business models. However, there are many context specific unknowns with regards to using data as a resource. Data quality, provenance, privacy, accessibility, collection, governance, preparation, processing, storing, and sharing can impede and sometimes inhibit the use of data within organizations and between other firms (Bulger et al., 2014; Schroeder, 2016). Essentially, data needs to be reliable in order to be efficiently and effectively used in business processes and operations. Hence, the complexity and dynamics of utilizing data contributes to some of the knowledge gaps in empirical studies with regards to how data produces value for firms, how firms capture that value, and the business model opportunities for data-driven processes. Thus, DDBM literature will be used to understand value creation processes and concepts in data-driven contexts rather than used as prescriptive tool for data-driven business models.

The monetization of data can occur by improving the effectiveness or efficiency of internal processes or operations, data-driven product or service enhancement, or completely new data-based product or service such as DaaS or AaaS or selling data (Schüritz et al., 2017; Wixom & Ross, 2017). The terms data enrichment, data enhancement, data infusion is used interchangeably across literature to describe the DDBM typology or patterns in which data complements an existing product or service in order to create and appropriate value.

Data enhancement can also be conceptualized from a value creation perspective. Schuritz & Satzger's (2016) data-infusion framework identifies the patterns of data-driven value activities that extends the traditional view of value creation in business models. Schuritz & Satzger's (2016) names six data-infusion patterns that are either singular or coupled data-infused value creation, capture, and proposition. The framework postulates that new business models are enabled when data is leveraged to its full potential resulting in novel value creation, capture, and propositions (Schuritz & Satzger, 2016). This logic is reinforced by Sorescu's (2017) view that data can either support business processes or products or change the value proposition of the firm in which the latter requires business model innovation. Furthermore, Hilbig et al. (2018) has a similar interpretation that coincides with the notion that the extent of data exploitation within a construct of the business has implications on the DDBM type or design. These notions for different value creation patterns in DDBMs are illustrated in Figure 8.

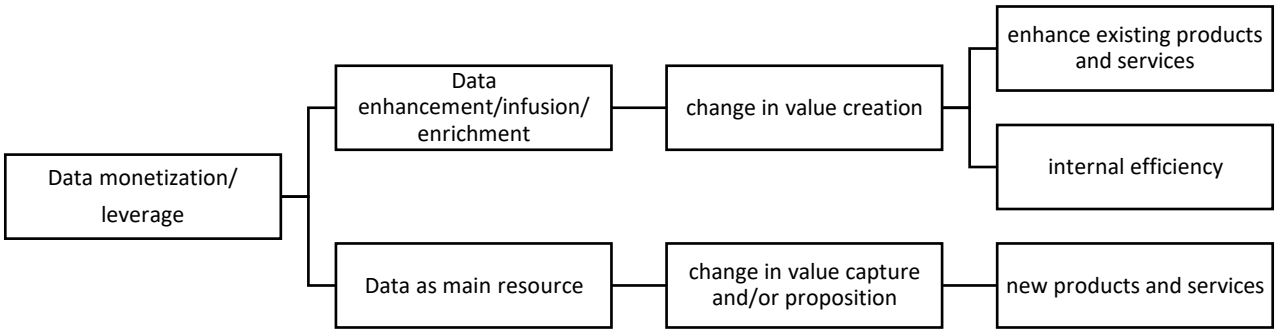



*Figure 8: Overview of data-driven value creation in business models.*

In conclusion, DDBMs are more suitable frameworks for MPC enabled business models because data is the focal point and feature of the technology and value creation system. There are differences in how DDBMs are defined, but the general theme among researchers is that data can indirectly and directly influence business models. What constitutes as a data driven business model depends on how the value systems is defined and the type of value mechanisms that contribute to it. For direct DDBMs, data is used as a main resource whereas, indirect DDBMs entails the use of data to enhance some component of the business model. Data can directly produce new products and services and inextricably affecting the entire value system leading to the creation of new value proposition(s). For indirect models, data contributes or enhances some business model component(s) that supports value creation, capture or proposition. This results in an indirect improvement of an existing product or service offering and/or indirect creation of new products and services. These high-level abstractions coincide with implementation outcomes of IOS with regards to: improved internal efficiency of organizational operations, process innovations, and new product or service innovations. The commonalities suggest that DDBM literature can be connected to IOS theories.

Next, underlying theories between business model, value creation and IOS fields will be further assessed in order to build a proper framework for investigating MPC's potential business value. Closely related topics and themes that were discussed in DDBM literature are the notions of value creation and business model innovation which are the subjects of review in the following subsections of this chapter.

### 3.2.5 Business Model Innovation

Business model innovation (BMI) is perceived as a means to maintain competitive advantage in a hostile environment by either creating new business models or changing existing business models (Amit & Zott, 2001; Hunke & Engel, 2018; Schuritz & Satzger, 2016; Schüritz et al., 2017; Sorescu, 2017; Voelpel et al., 2004). Business model sustainability is important in the banking sector due to rising competition and

important for regulators to manage risk (Lueg et al., 2019). Hence, incorporating business model innovation within the conceptual evaluation of MPC is warranted. In doing so, the utility of this research is more substantiated for practitioners.

Firstly, business model innovation will be defined from an RBV perspective. Secondly, BMI will be defined according to data-driven business model literature. Thirdly, the definition for BMI used in this study will be presented with its assumptions. Lastly, BMI concepts will be linked back IOS to further develop the MPC implementation conceptual framework for this thesis.

Business model innovation and value creation is underpinned by a resource based view (RBV) theory (Amit & Zott, 2001). Resource-based view postulates that enterprises can gain sustainable competitive advantage through their business model innovations (Barney, 1991; Lavie, 2006). Whereby, Barney's (1991) framework for sustainable competitive advantage stipulates that a firm's resources must be valuable, rare, imperfectly imitable, and non-substitutable to remain competitive. This has managerial significance in banks intending to implement technologies such as MPC for sustained value creation.

Business model innovation allows organizations to create value, uniquely and strategically adapt to changing competition and market forces, and make it difficult for other firms to imitate their business models (Amit & Zott, 2012; Pohle & Chapman, 2006). Similarly, to the business model concept, there is not one standard definition or interpretation for business model innovation as a concept. Business model innovation is described as either creating entirely new business models (Schüritz et al., 2017; Sorescu, 2017; Voelpel et al., 2004), or modifying existing business models (Schuritz & Satzger, 2016; Sorescu, 2017) or exploiting new ways to create and capture value (Amit & Zott, 2012) or generate a change in value activities and value proposition (Sorescu, 2017).

More specifically, business model innovation can result in reaching new markets (Schuritz & Satzger, 2016), exploit new opportunities in existing markets (Amit & Zott, 2012), a change in the structure or financial model of the firm (Pohle & Chapman, 2006), or involve revolutionary or disruptive innovation (Voelpel et al., 2004). Moreover, business model innovations do not have to be disruptive or designed around product innovation (Sorescu, 2017). It can also be operational wherein processes and core functions are improved for efficiency or services are enhanced in quality (Pohle & Chapman, 2006).

In the perspective of a data ecosystem, data sharing and analytics are driving competition with emerging markets and hence, pushing firms to redesign their business models. Chen, Kreulen, Campbell, & Abrams (2011) describes the shift of analytics business models *"from a closed, proprietary, and business-directed model to a much more open, collaborative, and value co-creation model"* (p.16). Business model innovation in this context has evolved in six phases by leveraging:

1. internal proprietary data;
2. shared data;
3. shared data analytics;
4. shared and co-created value between customers and businesses;
5. the co-development and collaboration of data analytics solutions between industry partners;
6. and the generation of entirely new businesses (Chen et al., 2011).

Schuritz & Satzger (2016) argues that eventually every firm needs to have data-based products and services to remain competitive and ultimately incorporate data and analytics into the core business model. Their framework postulates that new business models are formed when data is leveraged to its full potential changing its value mechanisms (Schuritz & Satzger, 2016). Whereas, Sorescu (2017) makes

the distinction among business models wherein data can support product innovation or it can also change process innovation. However, this does not necessarily require business model innovation if these product or process innovations do not change the entire value proposition of the firm according to Sorescu (2017). Furthermore, Hilbig's et al. (2018) argues that BMI potential is contingent on the degree of digitization that can exploit data and not on the value mechanisms or structure. The possible BMI activities and outcomes are summarized in Table 3 below.

| | Possible outcomes/activities of BMI | Possible outcomes/activities of data-driven BMI |
|---|---|---|
| **1.** | New Market Entry (Schuritz & Satzger, 2016) | New businesses e.g. co-creation with customers or business partners (Chen et al., 2011). |
| **2.** | Adapt to/exploit existing markets (Amit & Zott, 2012) | Degree of digitization/exploitation of data (Hilbig et al., 2018) |
| **3.** | Improved processes/internal efficiency (Pohle & Chapman, 2006) | Process innovation (Sorescu, 2017); incorporation of data and analytics (Schuritz & Satzger, 2016) |
| **4.** | Change in business model component(s) e.g. financial model (Pohle & Chapman, 2006) | Change in value proposition (Sorescu, 2017) |
| **5.** | Disruptive innovation (Voelpel et al., 2004) | Product innovation (Sorescu, 2017) |
| **6.** | | data-based products or services (Schuritz & Satzger, 2016) |

*Table 3: Comparison of different outcomes and activities of traditional versus data-driven business model innovation.*

The activities in the table shows that some activities coincide or are similar. However, in order to reconcile these slightly opposing views for data driven BMI, the definition of DDBM from Hartmann et al. (2014)will be applied to make the assumption that new business models or business model innovation is plausible when data is used as a key resource, regardless if it changes the value proposition or not. In terms of using data to improve internal processes within a firm, it can be assumed that these processes may not be mainly data-driven and rather assisted by data. Moreover, using data to improve internal processes and boost decision making quality is the most immediate but not the most effective profitable approach to capitalizing on data (Wixom & Ross, 2017). Hence, if data is not used as a main resource in internal processes then it does not *directly* lead to data-driven business model innovation.

**This study will incorporate both traditional and data-driven BMI activities that overlap or are similar:**

1. **New market entry or creation of new businesses via data-based products and services or data-based product innovation;**
2. **Exploitation or adaption of existing markets by using data or analytics;**
3. **Using data or analytics to improve process innovation and/or internal efficiency.**

It can be assumed that any of these three points can result in some change in business model components and therefore, it is redundant to add 'change in business model components' to this list. For the same reason, incorporating rows 5 and 6 (Table 3) as a separate point would be superfluous.

Business model innovation is required for practitioners aiming to monetize data in the bank sector as well as the growing data economy for sustained competitive advantage. Business model innovation can be considered a type of value capture in which a business aims to appropriate revenue from data. Business model innovation can also occur via some enhancement or change in business model components. Across IOS, DDBM, and business model innovation research, common value creation logic refers to an

improvement in some process of the organization and or the creation of new products and services. These notions will be carried over to the overall conceptual framework which is illustrated in Figure 9.

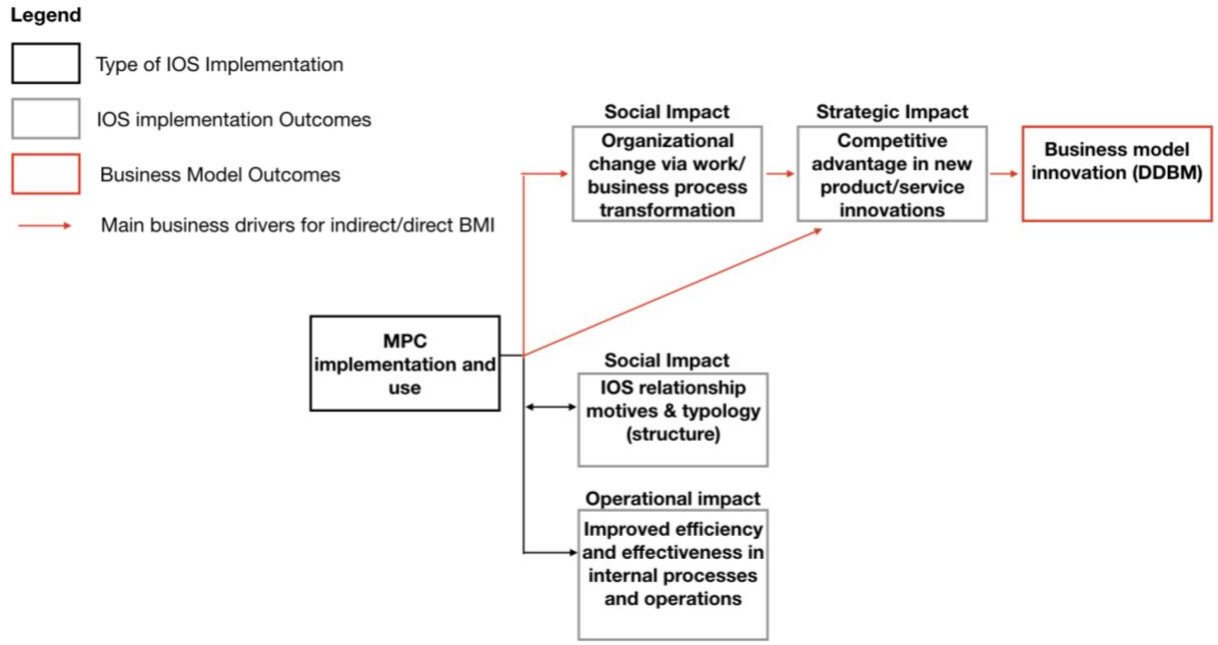



*Figure 9: Abductively derived conceptual framework for MPC implementation outcomes and consequences.*

Data sharing and analytics is a key feature of MPC and consequently, data driven business model innovation is correlated with MPC value creation outcomes. The lines in red show the managerial and practical importance of implementing MPC for business growth and sustainable competitive advantage and represent the main business drivers for MPC implementation. The arrows point towards implementation outcomes. It was established in Section 3.2.2 that social values are interdependent on organization outcomes and technology implementation. Moreover, the arrows also illustrate that MPC implementation can indirectly and directly affect business model innovation based on Hartmann's et al. (2014) definition of DDBM. In section 3.2.3, it was also asserted that there is not enough evidence that would justify adding conventional digital business model components to the conceptual framework. Furthermore, MPC business model components are very use-case specific and still unknown. Thus, components could not be represented in a general conceptual framework. The relationships in this conceptual model is supported and linked by networked RBV theory.

The social and strategic impacts are linked to business model innovation which was supported by resource-based view theory from DDBM and value creation literature. In this model, when data is used as a main resource for new offerings, e.g. selling data, then *direct* data driven business model innovation occurs which coincides with Hartmann's et al. (2014) definition of a DDBM. When data is not used as main resource, e.g. data analytics improving some operation or process, then *indirect* business model innovation could be an outcome. This coincides with DDBM literature wherein enriching existing products, services, and processes with data substantiate better offerings. However, this may not always lead to business model innovation unless the efficiency and efficacy of these processes are so superior, that new business models can be created or multiple value activities change.

Alternatively, using data to improve internal efficiency of an organization may be beneficial in cost saving measures. However, this type of data leverage within organizations is typically not maximizing the use of data or profit (Wixom & Ross, 2017). This coincides with data-driven business model typologies and concepts which denotes that data-enhanced internal processes may not require or necessitate business model innovation (Hilbig et al., 2018; Sorescu, 2017). Thus, the operational impacts of MPC implementation may hold less managerial significance and less bearing on MPC enabled business models.

Lastly, the social impact from MPC collaborations can either enable efficiency structures or influence the implementation decisions relative to MPC use. As previously noted in section 3.2.2, efficiency can be evaluated from a system capabilities perspective and from a governance perspective in IOS (Amit & Zott, 2001; Elgarah et al., 2005). From a system capabilities perspective, MPC can drive value in organizational operations. From a governance and social structure perspective, MPC systems might enable value creation in facilitating collaboration that was previously difficult or inconvenient. IOS relationship structures may not have a direct link on new data-based products for business models, but there is a correlation between interfirm alliances and the extent of value creation and capture for a focal firm, based on networked RBV theory.

## 3.3 Conclusion

Academic literature defines business model concepts as either constructs or tools for value creation whereby definitions, scope, and perspectives vary. Therefore, the theoretical perspectives and foundations of business model concepts depends on the conceptual lens and context. In order to develop a framework and understanding for a business model concept in the context of MPC, theoretical foundations from relevant research fields were reviewed. The purpose of this chapter is also to answer SQ1 of this research study.

Since value creation theories were used to connect IOS, MPC, and business models concepts for the development of a general conceptual framework, an explanation of this framework will be used to answer SQ1: **How does value creation theory correlate MPC implementation and business model concepts?** In short, MPC implementation and use by an organization can result in three types of value creation outcomes: *operational*, *social, and strategic outcomes.* Subsequently, these three outcomes can directly or indirectly lead to data driven business model innovation. These relationships are represented in the conceptual model (Figure 9) adapted from the theoretical model of Robey et al. (2008).

Firstly, value creation from operational outcomes entail the use of data sharing and analytics to increase the internal efficiency of an organization which was established by the chosen IOS and DDBM frameworks (Hartmann et al., 2014; Robey et al., 2008). Secondly, value creation from social outcomes utilizes data sharing and analytics more readily by contributing to business process innovation and transformation or enhancing existing customer offerings. Social outcomes also entail changes in collaboration due to the use of data sharing and analytics. Collaborations with other organizations has a contingency on whether the focal firm implements MPC, the type of value creating activity is pursued (use-case), and the extent of value appropriation. Thirdly, the strategic outcomes are the main business drivers for value creation because this entails using data as a main resource to create new offerings and markets. Subsequently, the social and strategic outcomes can indirectly or directly lead to data driven business model innovation, respectively.

Transaction cost economics, network theory and resource-based view are the underlying theories in business models, value creation, and IOS. Thus, themes and insights from these theories started as the basis for conceptualizing MPC in a business framework. These theories were narrowed down to networked RBV to focus solely on MPC implementation from an IOS conceptual lens. Networked RBV was used to evaluate MPC and then used to develop a general conceptual framework for MPC implementation value creation outcomes.

Moreover, some theoretical assumptions were made in order to justify how these theories would be used to link MPC implementation to value creation outcomes. The stated assumptions in this review include:

- MPC is a type of emerging information system within the IOS field;
- an IOS implementation theoretical framework from Robey et al. (2008) was adapted for this thesis;
- Transaction cost economics are more suitable to describe MPC implementation antecedents rather than outcomes;
- Value creation drivers are use-case specific for MPC;
- A DDBM definition from Hartmann et al. (2014) was applied towards MPC implementation and business model contexts;
- MPC systems and banking business models are use-case specific.

These assumptions and conceptual evaluation in this review were inputs for the MPC implementation conceptual model. Only value creation outcomes were included in the model because value creation drivers are essentially use-case specific and interdependent. The importance of each value creation driver (efficiency, novelty, complementarities, and lock-in) are also contingent on external factors such as market and competition or governance structure, for instance. Therefore, in this thesis, value creation drivers are treated as moderating variables whereby MPC implementation and use is the independent variable and value outcomes are the dependent variables. These relationships will not be tested in this study, but used to understand the correlation between MPC implementation and plausible scenario outcomes.

In theory, it can be inferred that MPC enabled data sharing and analytics can create value and new business models for organizations, but MPC is context specific wherein the technology requires special engineering for its use-cases and participants or data owners. However, there are regulatory, legal, governance and social challenges in utilizing and monetizing data (Bulger et al., 2014; Schroeder, 2016). These challenges can also affect MPC systems as well and the extent of MPC implementation and use by banks. Moreover, the interdependencies of the social and strategic impacts and benefits may change whether MPC enables new business models or not. Therefore, it cannot be predicted from this conceptual model alone whether MPC creates new business models in banks, especially in such highly regulated industries such as finance and banking.

Thus, understanding external and contextual factors of MPC is necessary to logically understand how MPC implementation outcomes could develop. The next chapters will commence with the scenario analysis method that will help further understand MPC use within a bank setting. The conceptual model from this chapter will be used as a basis for guiding the abductive reasoning and analysis for the development of scenario outcomes as well.

# 4. Scenario Preparation and Scenario Exploration (Phase 1 & 2)

The purpose of this chapter serves as the starting point for developing scenarios. The first phase of the scenario analysis method entails setting up the scene and scope of scenarios (section 4.1). The second phase of scenario analysis will use the PESTLE framework to determine which external drivers can influence MPC technology and banks in the next five years (Section 4.2 – 4.5).

Scenarios are judged by four criteria: plausibility, relevancy, consistency, and novelty. The research objective aims to produce useful outcomes that ultimately improve decision making in banks. Thus, the two most important criteria are plausibility and relevancy and these two criteria should be considered throughout the entire scenario analysis process. Phase 1 ensures that scenarios are scoped to the relevant time scale, geographical location and industry of the research sample. Phase 2 ensures that external drivers of MPC are relevant to the data ecosystem and the banking ecosystem in the EU. Phase 3 entails the development of organization and context specific scenarios which is in this thesis is MPC implementation scenarios in EU banks.

## 4.1 Scenario Preparation

The initial steps of scenario analysis requires defining the scope of analysis with regards to the *time frame or horizon, sectors and geographical location* (Schoemaker, 1995). In regards to analyzing MPC, trends within the **data ecosystem** should be outlined because the main value and output of MPC is derived from data. However, there are many challenges, especially with regulatory and privacy concerns, that may inhibit how MPC technology is developed and used. According to scenario analysis methods for emerging technologies, the scope of analysis should be broader than the units of analysis and the technology itself (Schoemaker & Mavaddat, 2000).

Thus, the drivers in the European data and bank ecosystem will be determined via a macro-environmental analysis. The most important drivers as it relates to the barriers and enablers for MPC technology will be evaluated. Then the trends will be delineated according to the important factors and drivers that are identified in the environmental analyses. The environmental and trend analyses will be used for input in building scenarios. Hence, the scope of the data trends should include important factors that extend beyond data sharing and analytics since interorganizational data sharing is interrelated to data security, privacy, use, compliance, and other factors that may inhibit or accelerate the use of MPC. Risk and profitability trends in the **bank sector** should also be evaluated since it will have an effect on business models and the role of fraud detection for banks.

According to Gartner, MPC will take 5-10 years to reach the plateau of productivity or widescale adoption (Mizrahi, 2018). The **time horizon for analysis will be five years from 2020 to 2025**, given that the current maturity stage of MPC is in the proof of concept and pilot stage for some researchers and organizations and undoubtedly, too early for any observable implementations in banks. Therefore, there is no legal and regulatory framework that governs the use of MPC in banks. The main insights from the data ecosystem and bank ecosystem will be used to understand:

- how data will be used and the potential of data in banks' business operations, functions, lines;
- the barriers and enablers of data-driven activities in banks;
- and the potential of data in the future of banks' business models.

Since banks are highly regulated, PESTLE analyses will also focus on relevant regulations that are or will be implemented according to reports and publications from the European Commission. The analyses in the next section will be evaluated from a broad lens as recommended by Schoemaker & Mavaddat (2000)

and then converged to consider the factors and drivers that are the most important in relation to using data for fraud schemes and bank business models. Following the PESTLE analyses, trends and uncertainties will be sorted throughout Chapter 4 & 5 according to main themes that were derived.

## 4.2 Scenario Exploration

This chapter aims to understand the main external driving forces that can shape the future of MPC technology within the banking sector. The **PESTLE** framework will be used for the macro-environmental analysis which covers the **P**olitical, **E**conomic, **S**ocial, **T**echnological, **L**egal, **E**nvironmental drivers in data and finance ecosystems. PESTLE framework has also been used in scenario analysis case studies and referenced as the most common macro-environmental framework for intuitive logics scenario methods (Burt et al., 2006; Gnatzy & Moser, 2012; Schoemaker, 1995). The PESTLE framework is chosen in order to stay consistent with the most common practice for intuitive logics model. Additionally, PESTLE factors can affect the variables established in the conceptual model developed in Chapter 3. These external factors are context specific and interrelated to the value creation activities of MPC systems and thus, should be considered to determine what is plausible and relevant to data use and banking in the EU.

### 4.2.1 PESTLE Method and Approach

In order to align with the time horizon and scope of scenarios, the search criteria for information related to trend reports for the EU data ecosystems and banking sector was facilitated in Google Scholar and Google. Search results surmounted to journal articles, white papers, published papers from government, legislative documents, and consultancy reports. Given that scenarios have to be internally consistent with the time horizon of 5 years, documents were selected based on trend reports and documents that were published in the year 2020 or had information related to trend projections in the years 2020-2025. Therefore, search criteria needed to be broadened to include information from multiple sources other than journal articles. PESTLE analysis and trend analysis relied predominately on documents published by government and supervisory bodies such as the European Commission and European Central Bank as an alternative for reliable sources, in the case that peer reviewed journal articles were not sufficient sources of information.

Other than searching for trend analyses and reports, document search criteria were facilitated by the PESTLE analysis taxonomy to find specific information. For example, to understand the legal implications of EU data laws, a Google scholar and Google search was facilitated to find formal legal documents and legislations by the European Commission. This was executed for every environmental factor of the PESTLE framework and selected according to consistency with time horizon (2020-2025), geographical location (EU), and industry/sector (banking and EU data ecosystem).

PESTLE analysis is meant to serve as a generic methodology to find potential drivers of change (Burt et al., 2006). Since the macro-environment is outside the internal contextual environment of banks, PESTLE analysis should be considered as generic information, which is most likely already known to experts, and used as a starting point for identifying areas or concern or interest (Burt et al., 2006). After appropriate sources of information and documents were obtained that addressed every environmental driver in the PESTLE framework in both macro-environments (banking and data), texts and information were copy-pasted and listed under each category according to the PESTLE framework.

After relevant information was categorized accordingly, common patterns and themes were combined and any factors that banks would react to or that could affect their business were also noted. It was an iterative process of rewriting, reading and searching to find the most relevant and up-to-date drivers. This

process is known as qualitative clustering analysis which can used over the course of multiple steps in the scenario analysis process for intuitive logics (Van Der Heijden, 1996). Clustering analysis is a systematic approach to intuitively combining elements that are governed by some rule or criteria of association (Van Der Heijden, 1996). However, according to Van Der Heijden (1996), there is no set or standard criteria for clustering and therefore, the PESTLE framework was used to govern this process. Ultimately, this information was analyzed and used to converge towards developing trends and uncertainties.

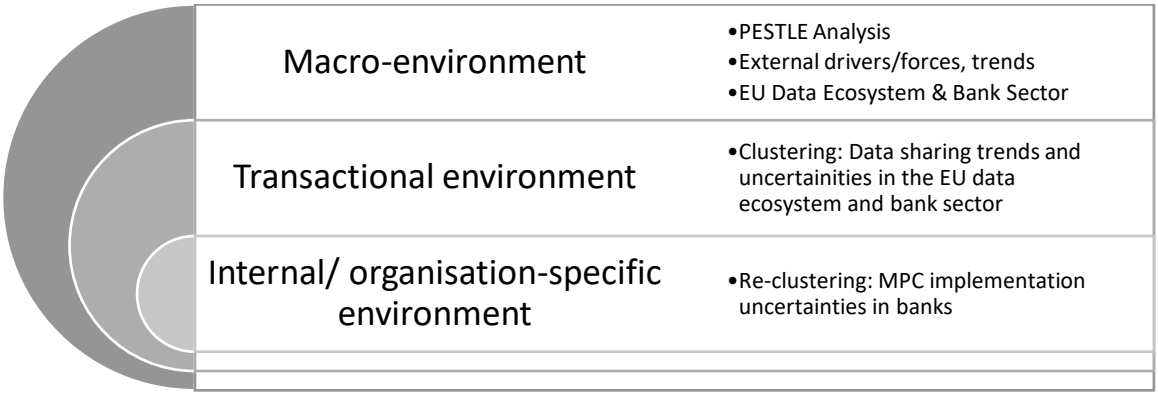



*Figure 10: The bank in its business environment. Adapted from* Van Der Heijden, (1996, p.155).

Figure 10 above shows the relationship between the different contextual environments and the analyses that is needed to derive internally context-specific scenarios. Following the intuitive logics model, qualitative inductive and deductive clustering analysis is used to reduce the number of drivers, elements, or ideas down to high level concepts (Van Der Heijden, 1996). In this scenario exploration phase, cluster analysis was specifically used to inductively derive trends and uncertainties to a manageable set of categories that will be used as input for the scenario development in the third phase (Chapter 5).

### 4.2.1 Data Ecosystem Analysis

This section aims to understand the main driving forces in the data ecosystem. However, the challenges to leveraging data for new business models are the practical complications in obtaining reliable and quality data (Bulger et al., 2014; Schroeder, 2016). Another barrier is the regulatory and legal framework, or lack thereof, for processing data correctly in different use-cases (Bulger et al., 2014; Schroeder, 2016). Companies lack incentive to participate in B2B data sharing because of the risk with compliance issues (Arnaut et al., 2018). Thus, a focus on existing regulation will be discussed throughout this section in order to understand the legal and governance framework that will apply to MPC.

Personal data is protected under the General Data Protection Regulation or GDPR. The GDPR mandates that all organizations and companies must abide by obtaining consent from consumers to use their data and provide the option to delete their data from any database. The European Commission describes the GDPR as the most common framework for digital trust (European Commission, 2020a). However, the complexity of data usage and the ethical considerations of using data are not completely addressed by the GDPR (Arnaut et al., 2018; European Commission, 2018b, 2020a).

Due to emerging technologies and increasing amount of data that will be produced, EU regulation and legislation is expected to change in order to safeguard data privacy and security in society (European Commission, 2020a). The right to access, use, and own data need to be clearly and explicitly defined within

legal frameworks (Arnaut et al., 2018; European Commission, 2020a, 2020f). Other regulations that the EU has developed are the free flow of nonpersonal data (FFD), the Open Data Directive and the Cyber Security Act (CSA) (European Commission, 2020a). These directives relate to the use of open data or public sector information and complies with the GDPR (European Commission, 2020a; Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019).

On the other hand, there are also legislations on proprietary data access for certain sectors such as the payment services directives, PSD1 and PSD2 in finance (European Commission, 2020a). Given that data provides value for the economy and public policy, the European Commission plans to further develop and implement their strategy for developing a single open data market as a means to support the data ecosystem within the EU (European Commission, 2020a). These developments provide indications of how the data-driven economy may develop in the coming years and how changes to the regulation and governance of data is expected to change.

**Political.** The executive branch of the European Union, the European Commission, has the responsibility to create and govern the mandates for economic and public policy. According to the Commission, they intend to create a longer-term goal of establishing a policy environment for the data economy by 2030 (European Commission, 2020a). Generally, their vision is to leverage the data that is stored, processed, and used for value creation and monetization (European Commission, 2020a). This entails creating a single common data space or more specifically, a single market for data which contains personal and nonpersonal data, proprietary data, and industrial data to boost growth for the economy (European Commission, 2020e). Industrial and commercial data is expected to be the main drivers for a data economy (European Commission, 2020e).

Given the highly regulated environment in the finance sector, especially for incumbent banks, sector and country specific legislation with regards to data may be necessary to support the data ecosystem (European Commission, 2020a). The PSD2 and anti-money laundering/terrorist financing initiatives are examples of mandates that affect how proprietary data is used, shared and if it remains secret to the proprietary company. According to the *High-level Expert Group for business to government (B2G) data sharing*, which was independently set up by the Commission, reports that it is likely for member states to set up conditions to 'facilitate access to private sector data for public interest purposes' (European Commission, 2020c, p. 36).

The prospect and uncertainty of fragmented legal frameworks across member states is possible which will result in higher compliance costs and technical requirements (European Commission, 2020f). Compliance and legal obligations can hinder data sharing because these costs may outweigh the benefits or there may be a lack of incentive or value in data sharing practices (European Commission, 2020f). Hence, the rules and procedures governing data across borders and sectors must be defined (European Commission, 2020f). According to the *High-level Expert Group,* member states could provide some form of government incentive such as tax incentives or investment of public funds in order to free up commercial data for public use (European Commission, 2020f).

However, the *High-level Expert Group* also notes that it may not be possible to create an overarching EU tax incentive given that taxes differ on a national level (European Commission, 2020f). Therefore, there is an uncertainty whether the data sharing market will be stimulated by B2G, B2B, or G2B data sharing. G2B (government to business) data sharing is defined by the Commission as using public sector data by businesses (European Commission, 2020a). B2B data sharing is the use of proprietary or commercial data between companies and it has the most economic potential but is inhibited by barriers such as lack of

trust and economic incentives, imbalances of power, lack of governance and legal frameworks, and contractual agreements (Arnaut et al., 2018; European Commission, 2020a). B2G data sharing is defined as the use of privately held data by government authorities but there is not enough data or data sharing activities to support government and civil agendas (European Commission, 2020a, 2020f).

**Economic.** According to Micheletti & Pepato (2019), the expected growth of the data economy may surmount to €829 billion (5.8% EU GDP) in 2025, almost triple the amount reported in 2018 (€301 billion euros; 2.4% EU GDP) (p.11). However, this forecast is contingent upon having the proper legal frameworks and policies in place by 2025 as described by Micheletti & Pepato (2019). Whereas, the Commission assesses that the economic impact of public sector data is expected to reach EUR 194 billion in 2030 (European Commission, 2020c). Data is a value driver for society as well as businesses, predominately SMEs (European Commission, 2020f).

Moreover, big data is expected to grow and become the main driver for the EU data ecosystem whereas, industrial data will reap the most economic benefit (Arnaut et al., 2018; European Commission, 2020g). However, big data and analytics are on the top of the list for critical skills shortages across the EU (European Commission, 2020a). In order to stimulate the data economy, thousands of data professionals are expected to be employed in the workforce and investment efforts to increase data literacy across the board will be supported by the government (European Commission, 2020a). Data should be pooled across key sectors and interoperable between sectors and member states (European Commission, 2020a).The estimated financial commitment from the government for these initiatives in stimulating and preparing for a data-driven economy is €4-6 billion (European Commission, 2020e).

**Social.** The standard EU regulation, the General Data Protection Regulation (GDPR), ensures and safeguards the use of data for citizens but most companies do not go beyond the minimum compliance standards (European Commission, 2020a). One of the most important factors with regards to using data, is the dichotomy between data producers/owners and data users (European Commission, 2020a). The EU lacks a standard legal and governance framework for data produced by multiple parties that may inhibit the use of data and data sharing (Arnaut et al., 2018). The EU aims to have regulation and rules place that will stimulate cross-border and cross-sector data sharing (European Commission, 2020a). However, cross-border data sharing and data re(use) is impeded by data localization rules, according to Arnaut et al. (2018), which requires data to be stored in the country where it has originated from. The Commission has implemented the EU Regulation 2018/1807 or FFD which has guidelines about how non-personal data may be used by private companies and if it is subject to data localization and GDPR rules so that personal privacy is protected whilst private companies can still benefit from data use (Arnaut et al., 2018; REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018).

The European Commission's strategy for the data driven economy aims to primarily balance the socioeconomic benefits of the general public and companies and protecting the interests of individual consumers (European Commission, 2020a). Therefore, technological products and services should be based more on accessible and open data (European Commission, 2020a). Open data is defined In the EU Directive 2019/1024 as "data in an open format that can be freely used, re-used and shared by anyone for any purpose" (European Parliament, 2019, p. 58). It is the Commission's mission to support B2G legal frameworks and strive for an open data space (European Commission, 2020a).This may conflict with B2B use of private and commercial data in the private sector which has implications on how private data markets will develop or possibly decelerate by regulations and compliance.

Furthermore, there is a value shift with regards to data control and customer empowerment. According to the Commission, the tension between data producers or suppliers and users should be alleviated by allowing users the rights, tools, and skills to be in control of their data (European Commission, 2020e). In the context of finance, the Commission expects the following benefits from PSD2 in opening banking initiatives: data decision rights on a granular level, health and wellness, better personal finances, reduced environmental footprint, access to public and private services and transparency of personal data (European Commission, 2020a, p. 10). Overall, the Commission intends for an **attractive**, **secure**, and **dynamic** single data market with *fair, practical* and *clear* rules for data access and re-use (European Commission, 2020d, p. 1-2).

According to the EU Directive 2019/1024 for open data, data is expected to enhance public interests and tasks, research and science, innovation, education and eventually benefit citizens in the long run (Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). However, the exploitation of open data by private companies and the competition rules between member states are still not addressed and the fragmented rules across member states are in fact, barriers to fair, non-discriminatory and transparent use of data (Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). Additionally, the EU is predominately dependent on third country cloud service providers which entails that personal data processed and stored in the cloud is vulnerable to threats and not completely protected under European law (European Commission, 2020a).

**Legal.** The aforementioned legislations such as the free flow of non-personal data, FFD (EU Regulation 2018/1807), and the Open Data Directive (EU Regulation 2019/1024) are standardized EU legal frameworks for using different types of data (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018; Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). These regulations also meet the compliance requirements of the GDPR (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018; Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). The FFD makes it permissible to ease restrictions that formerly may have inhibited the use of data that does not have any personally identifiable information or violate the GDPR (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018). The FFD serves as a framework for fostering competition whilst protecting natural persons with regards to mixed data sets that contain (non)personal data as well (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018).

The FFD is applied to processing non-personal data whereas the GDPR is applied to processing personal data (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018). It is made clear that mixed data sets with inextricably linked personal and non-personal data will abide by the GDPR (European Parliament, 2018, p. 65). This includes big data and aggregated data that becomes or contains personal data even if it was formerly anonymized to start with (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018). However, data is vaguely defined in this regulation wherein data is encapsulates all data other than personal data (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018). It can include big data, data produced or obtained

from technologies and devices but it does not specifically address co-created or shared data between companies. It can be assumed that shared data falls under the FFD jurisdictions but the FFD mainly ensures the free flow of data across borders within the EU, requiring the repeal of data localization laws (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018). However, it does not address how private companies can maintain or protect their proprietary data when shared or processed between organizations in different member states. This may imply that shared data and contractual agreements for B2B data sharing is up to the discretion of the organizations themselves.

The Open Data Directive is a revision of the Public Sector Information (PSI) Directive and it essentially establishes a governance framework and standardized law for open data held by public authorities (Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). The purpose is to stimulate the use of open data for innovation and provision of services (European Parliament, 2019, p. 68). The Open Data Directive is set to be implemented by the member states in 2021 (Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). It sets forth the principles and conditions for data re-use, fees, transparency, data formats, legal arrangements, and high-value data sets (Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). High value data sets will be made available for free use according to the EU's assessment on the following criteria:

- ability to generate socioeconomic, environmental, innovation benefits;
- benefit a high number of users and SMEs;
- generate revenues;
- and can be combined with other datasets (European Parliament, 2019, p. 75).

Generally, data re-use should be unrestricted as possible, free of charge or not charged above minimum requirements to prepare and keep the data, and be machine readable (Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). However, there is also a lack of specification on how companies can maintain their competitive standing and protect their commercial data in instances that publication of high value datasets is required by the EU.

**Technological.** The volume of data is expected to grow by a yearly average of 20%, reaching 175 zettabytes by 2025 (European Commission, 2020e). The rise of data calls for better infrastructure and technologies to handle the demand (European Commission, 2020a). Most processing and storage of data takes place in the cloud, data centers and centralized computing facilities (European Commission, 2020a, p. 2). This comprises 80% of current processing analysis of data the other 20% is comprised of IoT and edge computing (European Commission, 2020a, p. 2). By 2025, there will be a shift in greater data processing in edge computing due to the lack of bandwidth in the cloud (European Commission, 2020a). Additionally, other projects and investments will be allocated to architectures and governance mechanisms for data sharing in AI ecosystems (European Commission, 2020a). As a means to increase technological sovereignty, infrastructures for the data economy should support big data, data aggregation, and AI and machine learning purposes (European Commission, 2020a).

The Open Data Directive explains that APIs will be the main facilitators and enablers for data re-use, accessibility, exchange, and availability (Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). APIs or Application Programming Interfaces is defined as a "technique that enables organizations to share their business processes, data, services, and applications with partners and internal and external developers" (Premchand & Choudhry, 2019, p. 25). Open APIs should be used as frequently as possible to ensure uniformity of protocols via international standards with regards to open data made available by the EU (European Parliament, 2019, p. 62). This also includes dynamic data

or changing (real-time) data that can be produced by specific sectors and technologies such as smart devices and high-value data-sets (Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019).

**Environmental.** Climate change is at the top of the agenda for most regulators and governments (European Commission, 2020a). With this single European data space, the EU aims to minimize carbon emissions and the environmental footprint (European Commission, 2020a). There could be regulation and legislation that demands companies to decrease their energy consumption and carbon emissions which is a factor in using computing power and technologies (European Commission, 2020a). The ICT sector is estimated to comprise of 5-9% of the world's total electricity use in more than 2% of all emissions due to cloud services, data centers, and connectivity (European Commission, 2020a, p. 3). Given the current environmental initiatives such as the European Green Deal and the effort to become climate neutral by 2030, environmental legislation calls for limiting services and data centers and investing in more environmental technologies (European Commission, 2020a, 2020d).

From this analysis, it can be concluded that the main drivers that may impact the use of MPC enabled data sharing is balancing the legal and compliance requirements for data regulations and in a similar vein remaining competitive but also ensuring that the social and personal interests of people are protected. Technological and economic drivers also have implications on the use of MPC wherein APIs will be the main facilitators and enablers for data enabled services and activities. Digitalization and IT infrastructure introduces practical considerations and barriers for leveraging data. Since the newly implemented FFD and Open Data Directive regulations do not place rules to commercial matters, organizations still need to navigate the governance and legal uncertainty of B2B data sharing arrangements. Environmental drivers may be less of a concern for banks in terms of their implementation decisions for new technologies and business model choices.

### 4.2.2 EU Banking Ecosystem Analysis

The aim the of this analysis is to provide a frame of reference for the business environment, but moving towards the transactional environment for banks whereby, decision makers have a degree of control and influence (refer to section 4.2.1 for method). Schoemaker (1995) recommends assessing past trends as indicators for which trends and drivers that will likely persist or change in the future. Therefore, in order to provide further context to this analysis and to form a foundation of knowledge by which to judge future trends, a review of bank profitability will be discussed prior to PESTLE analysis. The search criteria for PESTLE analysis will be mainly used to evaluate future trends in the time horizon of five years.

The macro-economic environment for European banks is characterized by mainly low profitability due to zero-negative interest rates (European Central Bank, 2018; Srinivas et al., 2019). Currently within the EU, banks have high nonperforming loans for households and businesses resulting in total banks assets to remain lower than 2008 levels (European Central Bank, 2018, p. 8). Nonperforming loans surmounted to €1 trillion euros for European banks at the end of 2016 (European Central Bank, 2019e; Srinivas et al., 2019). These nonperforming loans in the EU are much higher compared to the UK and US (more than 5% higher) (European Central Bank, 2018). In 2019, **nonperforming loans** have decreased by 3.7% (€543 billion) but it still remains as one of the two, top supervisory priorities of the ECB (European Central Bank, 2019a, 2019e). The second priority of the banking supervision is **risk assessment** in relation to banks' strategies for non-performing loans and key risk drivers (European Central Bank, 2019a).

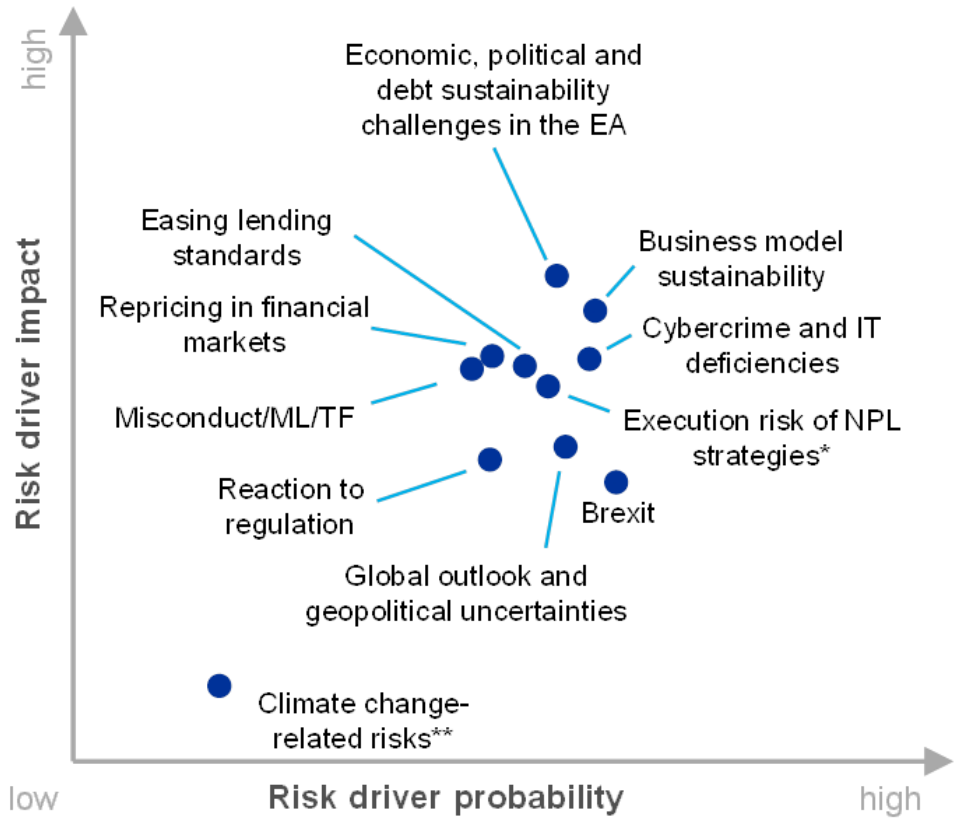



*Figure 11: Single Supervisory Mechanism (SSM) Risk Map for 2020 sourced from the European Central Bank (2019b).*

The **highest risks to the euro banking ecosystems** with a time horizon of three years are economic, political, and debt sustainability challenges; business model sustainability; and IT & cyber risk as shown in Figure 11 above (European Central Bank, 2019b). Hence, these risk drivers will most likely be pervasive and interrelated in future outcomes of MPC implementation since these drivers are located in the transactional environment. Credit risk will remain ubiquitous in banks' challenges, however, the ratio of nonperforming loans have decreased from 3.81% of Q1 to 3.22% in Q4 of 2019 (European Central Bank, 2019d). Whereas there is an increasing attention on money-laundering and/or terrorist financing which is reported to be subject to insufficient governance and risk controls (European Central Bank, 2019b). Despite being lower on the list of risk drivers, the ECB Banking Supervision intends to 'examine laundering cases more critically and closely because it can increase the risk of losses for banks' (European Central Bank, 2019b).

However, unprecedented risks such as the Coronavirus or COVID-19 could either accelerate and exacerbate some of these issues such as higher loans for those unable to support their businesses as well as repricing in financial markets as a result of economic downturn. For the purposes of this study, the current pandemic will be mentioned where necessary but it cannot be exhaustively covered or analyzed due to the ongoing and simultaneous changes within the duration of this research project. Furthermore, the assumption will be made that the coronavirus or COVID-19 pandemic will not affect financial markets and loans for the long term (years) given the mitigation efforts of banks and the European Banking Authority. Nonetheless, current trends indicate that financial markets and nonperforming loans are not in the top three main risk drivers for banks in the upcoming years.

**Political.** It is uncertain how Brexit will affect banks in five years and what the repercussions are for EU banks that are in business or depend on UK banks (European Central Bank, 2019b). It is expected that markets and GDP growth will be impacted (European Central Bank, 2019b). The UK left the EU in January 2020 and negotiations and agreements still need to take place between the UK and the European Commission (on the behalf of 27 EU member states) (Government of the Netherlands, n.d.). Until there is an agreement, EU rules and regulations will continue to apply to the UK during the transition period due to end in 2022 (Government of the Netherlands, n.d.).

Other political drivers are also under the jurisdiction of the European Banking Authority or EBA which is an independent EU authority whose main tasks is to ensure and maintain effective regulation and supervision across the European banking sector (European Banking Authority, n.d.). The EBA must provide an overarching and harmonized set of rules for financial institutions in the EU called the 'European Single Rulebook in Banking' (European Banking Authority, n.d.). They are also responsible of supervising risk assessments with regards to the financial stability and sustainability of EU banks (European Banking Authority, n.d.). The EBA also reports and advises the European Parliament, the Council, and the Commission on specific legal and supervisory matters in the finance sector (European Banking Authority, n.d.).

The EBA has taken efforts to combat the impact of the COVID-19 pandemic which has caused market volatility and risk within the economy (European Banking Authority, 2020). The EBA has proposed to adjust the capital impacts by amending its standards on valuation, allow flexibility with supervisory reporting, and delay reporting on account of increased operational challenges faced by banks (European Banking Authority, 2020). Along with recovery planning activities, the EBA emphasizes the importance of digital operational resilience to ensure business continuity, ICT capacity, and security risk management (European Banking Authority, 2020). They will form a new EBA ICT and security risk management guidelines as a result of these measures (European Banking Authority, 2020).

The Commission also wants to create an integrated *single market* for payment services which enables easy and safe cross-border payments (European Commission, n.d.-b). The goals of the EU for an efficient payments market are: uniform rules across the EU, transparency on payment information, fast payments, consumer protection, a wide choice of payment services (European Commission, n.d.-b). In an effort to establish EU rules on payment services, the payment services directives (PSD1/2) was created (European Commission, n.d.-b). PSD1 covers non-cash and e-payments, disseminates the information that payment services providers are obliged to give to their consumers, and the rules for the use of payment services (European Commission, n.d.-b). The PSD2 includes provisions that mainly strengthen and protect consumer rights (European Commission, n.d.-b). It is supposed to ensure easier and safer e-payments, protect against financial fraud and abuse, promote innovation in the payments market, and strengthen the role of the EBA in supervising and drafting technical standards (European Commission, n.d.-b). The PSD2 also imposes that transaction fees are limited and retailers are banned from imposing surcharges on debit/credit cards (European Commission, n.d.-b).

**Economic.** As mentioned previously, European banks continue to experience near zero to negative interest rates and low growth (European Central Bank, 2018; Srinivas et al., 2019). The ECB recommends that banks need to be profitable by improving their cost reduction programs, impact on control environment and income generation to circumvent business model challenges and external forces in the macro-environment (European Central Bank, 2018). The 22 top-performing EU banks profit from either being very cost-efficient or generating higher revenues than their competitors (European Central Bank,

2018). Therefore, the most important trends to consider are those related to risk management functions for cost reduction and sources of revenue in business models.

Competition with fintechs and large technology firms are expected to continue where there will be more activity in market entry from big tech players (European Central Bank, 2018; European Commission, 2020f; Srinivas et al., 2019). Trends indicate that the competition will likely change whereby fintechs become more mainstream in the market and incumbents will have to change their strategies in order to compete (Srinivas et al., 2019). PSD2 opens the payments markets to third party providers such as fintechs and incumbents outside of the banking/financial industry by allowing these third parties access to data from banks in order to provide new services to the consumer (European Commission, 2019c). Consumers can provide consent to these third parties to access, use and process their data for these services (European Commission, 2019c). Personal data is protected under the GDPR and PSD2 wherein the processing of data requires informed consent (European Commission, 2019c).

Within the payment space of financial services, incumbents are increasingly challenged by startups with their innovative platforms and digital payment options. In order to gain an edge, competition and market demand is pushing for enhanced customer experiences with regards to banking and payments. According to Srinivas et al. (2019), open and platform banking may also open opportunities for entrants from insurance companies, private equity firms, and traditional asset managers, and fintechs. Some banks implement merger and acquisition strategies to obtain complementarities in the payments market and also partnerships to gain revenue from network effects (Petralia et al., 2019; Srinivas et al., 2019). Overall, enhancing the customer experience can entail faster payments, easier processes for the customer, transparent pricing, digital protection, more services, and more accurate information for example (Petralia et al., 2019; Premchand & Choudhry, 2019; Srinivas et al., 2019). Or provision of services can provide greater flexibility and options for consumers in a pay per use model, similar to tech firms like Uber and Airbnb (Kobler et al., 2016; Sorescu, 2017). This is contingent upon how well corporate banks can modernize their IT infrastructures, leverage different types of data and data sources, improve data collection measures so that new technologies and business models can be implemented more readily (Bulger et al., 2014; Petralia et al., 2019; Srinivas et al., 2019).

**Social.** The intended social benefits for open banking as a result of PSD2 is empowering consumers in terms of enhanced transparency and control of their data (European Commission, 2019c). PSD2 delineates the security requirements to protect consumer financial data and fraud with regards to e-payments (European Commission, 2019c). Furthermore, these security and privacy requirements should be respected by all banks and third party service providers in the provision of financial services and products (European Commission, 2019c). Moreover, payment service providers must use a strong customer authentication or SCA to abide by PSD2 security requirements in order to lower the risk of fraud and to protect financial and personal data for the benefit of consumers (European Commission, 2019c). Consumer rights also extend to the reducing liability for unauthorized payments, flexible debit refunds, and the ban of surcharges for credit and debit cards (European Commission, 2019c).

The COVID-19 pandemic may also change customer expectations for banking in the future. Banks are making efforts to manage and maintain security and trust with their customers during the pandemic. However, in retrospect of the pandemic, customers may be unsatisfied with regulation as well as banks' measures to safeguard and protect their customers. In general, there could be customer dissatisfaction that has arisen from unforeseen circumstances due to the pandemic which may lead to changes in regulation, supervision, and banks' protocols. There is an increasing social responsibility for banks to not

only protect their customers but help and enable authorities to better prevent money laundering and terrorist financing (NVB, 2019).

On the other hand, work cultures and hiring requirements will change as a result of increasing digitalization and automation for front and back office operations in banks (Srinivas et al., 2019). The skills and specialists needed to drive big data and analytics within the industry is severely lacking (European Commission, 2020a). Consequently, banks will redefine and redesign jobs to accommodate changes in the workforce, reduction of routine and administrative tasks, and need for specialized skills and professionals (Srinivas et al., 2019).

The impact of Corona has also affected workers in their ability to commute, travel, engage, and collaborate in person. This poses a question on whether the pandemic will reinforce the need to stay home or create a new work culture in which workers prefer to stay home and whether there is a need for extensive travel and commuting. Moreover, there is an uncertainty on whether the pandemic will result in an increase or decrease of workers working from home and or traveling more infrequently or frequently. This can result in cost improvements for the bank and/or more efficient and happier employees.

**Technological.** The financial crisis in 2008 reinforced the ubiquitous need to manage and mitigate risk for financial stability (Rym Ayadi et al., 2012). Hence, technologies play an important role in banks' core competences and business operations. According to Deloitte reports, high quality and accessible data are needed for product innovations that connects lending, payments and wealth management services (Srinivas et al., 2019). There remains a challenge in monetizing data and analytics to fuel core business activities and operations, especially for banks who are less flexible in changing business models, adopting new technologies, and renewing their legacy systems (Petralia et al., 2019; Srinivas et al., 2019). The ECB notes that banks that have better strategic steering capability in their business models are more successful and perform better in the EU bank ecosystem (European Central Bank, 2018). Incumbent banks also face challenges with IT and technology investments that could affect their profitability and returns in the long run (Srinivas et al., 2019). Given the rising importance of data in the economy and efforts to continually digitalize processes, technical investment is necessary.

Cybersecurity is also important in not only protecting the bank but also securing trust with their customers (Petralia et al., 2019; Premchand & Choudhry, 2019). Deloitte estimates that the financial services sector is four times more likely to be victims of hackers and therefore, cyber security measures is the utmost importance to managing risk (Srinivas et al., 2019). Due to open banking, incumbent banks must compete with other entrants and therefore, sustaining that trust should be a priority for banks. Moreover, increased digitalization of banking as well as the opening of digital channels via APIs may introduce more vulnerabilities and threats to customers. Novel innovations and sophisticated technologies may also enable criminals and/or weaken existing cybersecurity measures and technologies. For instance, quantum computing is believed to break encryption and cryptography schemes (European Commission, 2018b; Srinivas et al., 2019).

According to Srinivas et al. (2019), that many banks do not have the proper risk controls for APIs, the opening of architectures and platforms, or the reliance on third parties for technologies. Furthermore, preventing money laundering and terrorist financing still needs significant improvement on the banks' end as well as increased efforts from governmental and supervisory authorities (European Commission, 2019b). Overcoming legacy systems, data management, and cyber security issues are extremely costly for

banks but it is necessary for competitive advantage and maintaining customer relationships (Srinivas et al., 2019). Hence, risk management in cyber security and fraud enables and constrains banks' profitability.

Financial risks are closely related to fighting financial crime such as money laundering and terrorist financing that is increasingly being conducted in cyberspace (NVB, 2019). Know Your Client or KYC policies entail validating customer identification and assessing their risk profiles which has consequently resulted in the proliferation of e-identity technologies (European Commission, n.d.-a). This heavily impacts the technical standards and compliance rules for payment service providers and electronic money issuers (COMMISSION DELEGATED REGULATION (EU) 2018/1108, 2018). Other lines of business impacted by fraud include wealth management and thus, it requires more risk management and compliance with KYC and AML regulations (Srinivas et al., 2019). Advising in this area has become more digitalized and changes in managing cybersecurity and fraud with new technologies will become increasingly important (PwC, 2016b, 2016a; Srinivas et al., 2019).

With regards to technology changes as a result of the PSD2, banks must configure communication channels that allows third-party providers to access their data (European Commission, 2019c). It should also enable banks and third-party providers to identify and securely communicate to each other when accessing customer data (European Commission, 2019c). Due to the PSD2, bank data is opened to third parties with APIs which could allow the development of banking platforms (Al-Ajlouni & Al-Hakim, 2019; Premchand & Choudhry, 2019). Banking platforms can enable faster payments and online banking for consumers. As previously mentioned, banks can either acquire other companies offering financial services or collaborate with them. However, there are risks with depending on third party providers because there could be technological and legal complications or failures in instances such as loss of data or different sectoral and country jurisdictions that complicates liabilities and compliance rules (European Commission, 2020a; Petralia et al., 2019; Srinivas et al., 2019).

Other technologies such as AI, ML, and IoT also play in role the future of banking which require in some shape or form, the use of data. Although blockchain and quantum computing are emerging technologies that are expected to disrupt financial services, these technologies are longer term and past the time horizon of reaching maturity within 5 years. Therefore, these emerging technologies will be excluded from the scope of these scenarios.

**Legal.** The bank ecosystem is highly regulated in terms of how data is shared, reporting activities to higher powers and authorities, as well as rules for economic policy (European Central Bank, 2019e; Petralia et al., 2019). It can vary on an EU and national level. For instance, in the Netherlands, banks are prohibited by the NVB, or Dutch Banking Association, from using customer transaction data to provide customers with personalized advertising (find source).

The aforementioned FFD regulation, frees up some barriers to processing non-personal data by removing data localisation rules within the EU (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018). This allows increased cross-border data movements and broadens cross-border collaborations as well. However, data within specific commercial concerns are not addressed or have rules in place according to the FFD regulation (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018). The Open Data Directive also mirrors the PSD2 in the notion that data should be opened in order to foster fair competition and to benefit society with data (European Commission, 2019d; Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019).

The general theme of an open data environment also has a contingency on the regulation for privacy, governance of data, on legal frameworks regarding data ownership, and use of co-generated data and aggregated datasets for businesses (Arnaut et al., 2018; Bulger et al., 2014). However, rules and standards that need to be followed can inhibit or slow down the development of data-driven technologies and innovations. As mentioned by the European Commission there should be an existing legal framework for data driven technologies and processes (European Commission, 2020a). However, there could be tailored approaches to regulations depending on the context, region or country, and industry/sector (European Commission, 2020a). Legal matters can dampen innovative liberty but is also necessary to ensure that organizations and innovators are not burdened with high legal, compliance, and regulatory costs which is already a significant financial commitment for banks given the highly regulated environment (Petralia et al., 2019).

Whereas, other instances support and require data sharing of banking and transaction data in order to fight financial crime. Banks must report to the Financial Intelligence Unit of their member state regarding money laundering and terrorist financing (European Commission, 2018a, 2019b). These Financial Intelligence Units are supervisory bodies in each member state responsible for governing the criminal activity in the financial industry and sharing data amongst each other and reporting to higher government authorities (European Commission, 2018a, 2019b).

**Environmental.** Banks will also have a greater responsibility for socioeconomic issues including environmental and climate change and empowering civil society (Srinivas et al., 2019). The environmental footprint of carbon emissions due to ICT is increasing and therefore regulations are making efforts to combat this climate change (European Commission, 2020a). There is a push for decreasing ICT sector carbon emissions and for the EU to become climate neutral by 2030 (European Commission, 2020d). Managing risk for climate change are also important for financial institutions to consider in their prevention and risk management plans (European Central Bank, 2019b; Srinivas et al., 2019).

Climate change related risks can have significant direct and indirect impacts on banks (European Central Bank, 2019b). It could affect the continuity of operations and the risk profile of their assets (European Central Bank, 2019b). Climate change related risks are expected to intensify over the horizon of more than three years which reaffirms that banks should incorporate this environmental driver into their risk management practices (European Central Bank, 2019b).

The coronavirus pandemic only highlights this importance and how drastically external natural causes can affect the economy, business, and profitability without the proper risk management and prevention protocols. According to Srinivas et al. (2019), environmental threats is causing central banks around the world such as the Fed, the ECB and the Bank of England to examine monetary policies that are more robust and resilient during economic distractions caused by extreme weather (p. 38). Similar scale of threats in global health such as viruses can have the same implications as exemplified by COVID–19.

### 4.2.3 Conclusion

To summarize, a general and coinciding theme in the paradigm shift for business models and banking is openness and transparency enabled and driven by data (Rym; Ayadi et al., 2012; European Commission, 2020a; Srinivas et al., 2019). Banks will experience increased competition in the payments market due to the provision of PSD2 and also increased risks in cybersecurity and fraud as result of digitalization. Trust and data are the key differentiators for banks that should be leveraged in open banking and in the payments markets (Petralia et al., 2019; Srinivas et al., 2019). This environmental analysis highlighted the

most important functions for banks' success which are new business models, gaining market share in open banking and payment services, and managing risk effectively to reduce costs and prevent losses. Therefore, scenarios will be scoped to MPC implementation in the areas of fraud mitigation as means to manage risks for banks as well as MPC for new business models with regards to payments and open banking. Another important core banking activity to consider is improving credit risk and lending assessments and strategy as delegated by the ECB.

Furthermore, the measures to prevent money-laundering (ML) and terrorist financing (TF) has remained crucial in banks' risks drivers and also heightened during the coronavirus pandemic which started in 2019 (European Banking Authority, 2020; NVB, 2019). Financial institutions are supported by the EBA and competent authorities to share information on emerging ML/TF risks (European Banking Authority, 2020). The regulatory expectations and supervisory tools used during this time may generate a framework and guideline for future ML/TF scenarios or change existing frameworks within banks. The initiatives within this area may accelerate the need for interorganizational data sharing and therefore, become a priority for regulators and lawmakers in the upcoming years.

COVID–19 has also affected economic activity and it is expected to continue throughout 2020 due to social distancing and quarantine protocols. Essential processes, operations, and workers such as IT have to remain working despite the new rules and measures in place which affects the normal and daily business operations of banks. There is also either a standstill or temporary hold on hires, projects, changes within some banks, and other business activities that may slow down operations. It is uncertain how long isolation and quarantine measures will last and to what extent the impact will be for banks. However, banks can use this as an example and learning scenario to create modus operandi for future instances of global change in unprecedented crises. Financial institutions may have incurred more costs in order to manage organizational change, risk, operations, and increased IT needs to support workers from home and to maintain some normalcy to business. This may also highlight or underline the importance of investing in social responsibility efforts not just as a corporate marketing strategy but as a means to manage future risk challenges and situations.

## 4.3 Approach to identifying trends and uncertainties

The next step of the scenario exploration phase is determining the trends and uncertainties of interest in the external and internal environment of banks. Trends and uncertainties are essentially derived from the PESTLE analysis. In order to develop scenarios, trends and uncertainties should be established and contextualized to MPC implementation. However, MPC trends in EU banking and data ecosystems are yet to be defined in literature. The identification of relevant areas of concern and studying of trends and uncertainties should be an iterative process (Schoemaker & Mavaddat, 2000). Therefore, general information from the PESTLE analyses are analyzed again via cluster analysis to formulate trends and uncertainties that may influence banks and data sharing in the future. Furthermore, uncertainties were identified by using combined resources from the PESTLE analysis and the literature review (Chapter 3) in order to further address unknowns that are also relevant to internal organizations. Deriving uncertainties across these two domains should be the input for developing MPC uncertainties whereby the latter will be used as a starting point for scenario development (Phase 3).

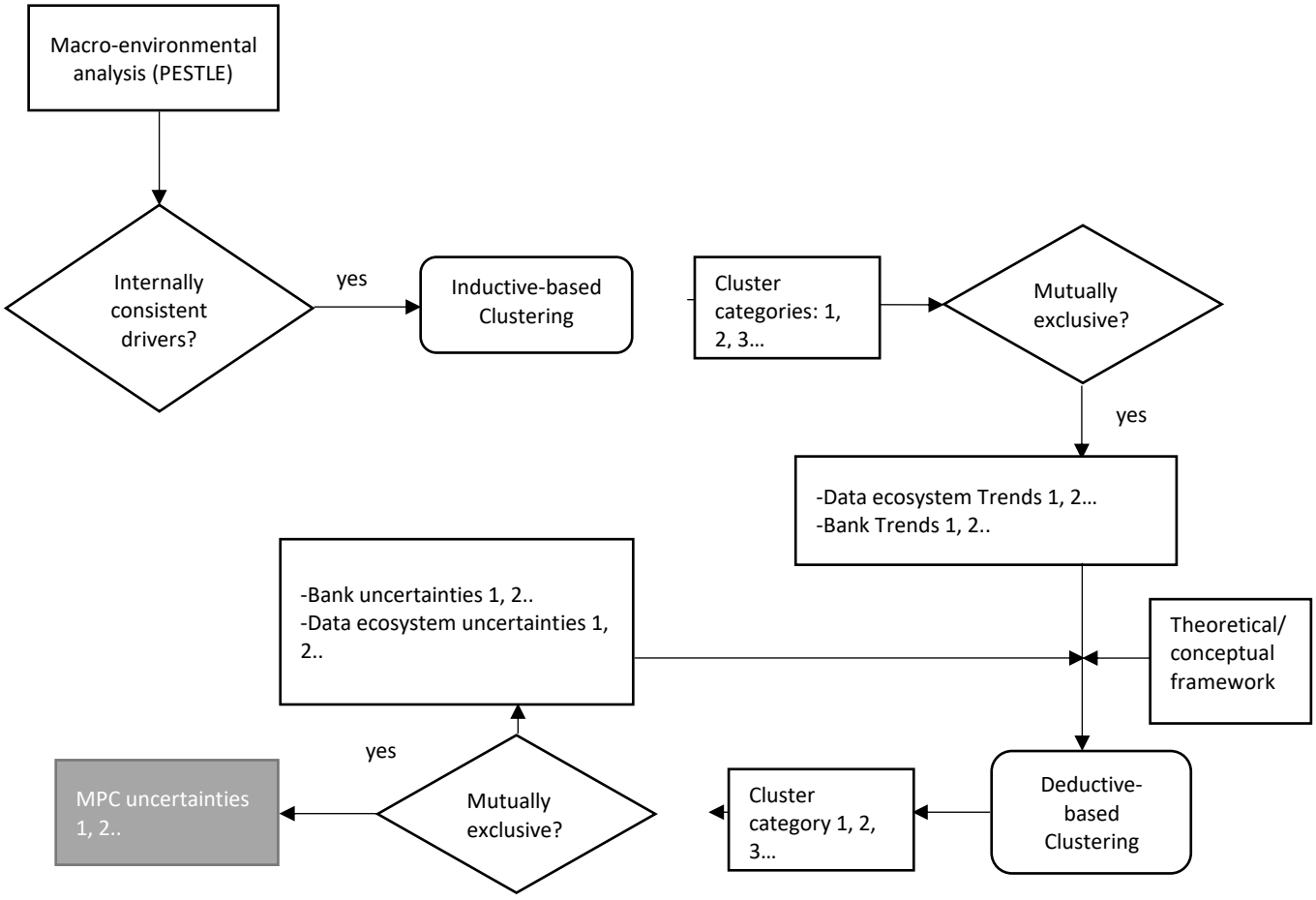



*Figure 12: Flow diagram for developing trends and uncertainties*

The flow diagram above depicts the clustering process and criteria for developing trends and uncertainties. External trends will be derived inductively whereas, uncertainties are derived deductively and sometimes abductively/retroductively which aligns with the philosophical and epistemological

assumptions of this thesis. Van Der Heijden (1996) suggests that there are no rules for developing cluster criteria, but categories or clusters should be mutually independent whereby the category can be labelled with a clear and short title (p. 189). Furthermore, uncertainties should be kept to a maximum of 5 categories to ensure manageable complexity of future scenarios. Therefore, this rule was applied for deriving uncertainties in the next sections.

## 4.4.Data Ecosystem Trends and Uncertainties

The following sections delineates data and financial ecosystem trends that are relevant to consider in scenarios for MPC implementation in banks. Uncertainties or risk drivers in the macro-environment will be discussed to determine hindrances that may impede MPC implementation or affect the plausibility of possible future scenarios.

### 4.4.1 Data Ecosystem Trends

Trends analysis builds upon the PESTLE analysis but restructured via cluster analysis. Overall, the government and most private industries are increasingly focused on how to fully maximize the potential of their data and data from other businesses in order to derive more accurate insights for decision making. Hence, data markets and the data economy are expected to grow concomitantly with the use of data in the public and private sectors.

1. **Cross-border data sharing**. There will be an increase in cross-border data sharing due to globalization and the incentives for acquiring better datasets from other parties. This will be partially supported by the government on an EU level and also stimulated by competition and market forces. However, the government and private sector may have diverging interests for the usage of data. The European Commission aims to develop a single open data market that allows the free flow of data between public and private sectors and between EU member states (European Commission, 2020a).
2. **Cross-sector data sharing.** From a market competition perspective, cross-sector data sharing will allow companies to derive better customer insights with aggregated data from multiple companies and industries. Cross-sector and interorganizational data sharing is an attractive incentive for companies to gain access to data that is not readily available. However, access to private data requires collaborative or coopetitive partnerships and/or legal contracts in order to sustain these data sharing relationships. Whereas, data sharing for public use and research purposes are also expected to grow. According to the Commission, a data sharing market that supports data driven public policy and research is absent (European Commission, 2020f). Therefore, national or multinational governments may foster an environment wherein researchers can share data securely or police authorities can obtain data from private companies more readily (European Commission, 2020a, 2020f).
3. **Big data and analytics.** There are varying opinions among researchers and practitioners about the potential of big data, what it means, and how it can be leveraged. Some researchers describe big data according to four of five characteristics, referred to as the four V's or five V's: *volume, veracity, variety, velocity, and/or value* (European Parliament, 2017; Schroeder, 2016). These dimensions can generally describe big data in terms of how much data is produced or used, the variety of datasets, the velocity of data use or computing power, and how reliable the data is (European Parliament, 2017; Schroeder, 2016). Government and companies will continue to struggle utilizing big data because of their lack of knowledge in the consequences of use and legal frameworks surrounding the concept. Furthermore, business will also encounter challenges with fully monetizing their (big) data and analytics as opposed to partially enhancing their product, services and customer relationships and experiences (Schroeder, 2016).

4. **Cloud storage and services.** According to the European Commission, EU companies are heavily dependent on third party service providers from companies such as Amazon and Microsoft which may have different jurisdictions than that of the EU with regards to standards for privacy and security (European Commission, 2020a). The demand for cloud storage and bandwidth to support the data and digital economy is rising. This is expected to be offset with emerging technologies such as edge computing and IoT whereby data is stored and computed on local devices. The Commission plans to develop cloud services to obtain a share of the cloud provider market that will benefit the EU and their open data market strategy (European Commission, 2020a).
5. **Cyber-security.** The growing digital economy and rise of new technologies will be vulnerable to cybersecurity attacks and meanwhile subject to improvements against threats. Cybersecurity will continue to be a main concern for any stakeholder and actor in the digital economy because it can have serious consequences and risks for misuse and/or loss of data and assets. Emerging technologies such as quantum computing has yet to reach maturation, but it is expected that quantum computing is powerful enough to break encryption schemes. Although quantum computing is a long-term technology that will take more than five years to develop, and hence out of scope for the scenarios of this study, it highlights the importance for developers to continue creating new and better cybersecurity innovations and solutions.
6. **Compliance and Regulation.** As mentioned previously in cross-sector data sharing, there is either an absent or small data sharing market due to compliance issues (European Commission, 2020f). Regulation can either hinder data sharing for private companies who will be subject to sanctions regarding the sharing of personal and proprietary data. Regulation can also encourage the sharing of data for governmental and public purposes. There are many legal and ethical considerations to consider when companies share data because data can be reused, but the ownership and authoritative right to use this data especially shared or co-created data is not explicitly defined in EU regulation (European Commission, 2020a). Interorganizational data sharing is mostly dependent on contractual agreements between companies themselves. The rising complexity of data sharing may result in a standardized EU level regulation like the GDPR for data sharing between governments and companies. There will also be regulatory changes for enhanced data security, privacy, and openness of data to support open data market within the EU (European Commission, 2020a).
7. **Governance and Legal Frameworks.** Similarly, to compliance and regulations, there will be rising complexities and developments in determining how data is shared by governments on the EU level or member state level. Currently, there are barriers to full data access and use on account of different entities and organizations having different permissions and rights to use data. Data sharing exacerbates this issue because data shared between different parties have to agree on who has access to the data, who owns the data, how the data is used, and any liabilities that may arise from sharing data. Therefore, governance and legal frameworks that define how data is used, owned, stored, and should be used in B2B, G2B, or B2G environments are on the EU's agenda as well as on a sector specific level (European Commission, 2020a).
8. **Climate Change.** Climate change will be a pervasive challenge and global trend for governments, corporations, businesses and people. The use of technologies and computing power to support the use of data has an impact on the environment and carbon emissions (European Commission, 2020a). Therefore, different environmental initiatives will attempt to reduce carbon emissions and that may lead to mandates for limiting services in the general technology and data landscape (European Commission, 2020a, 2020f). Moreover, environmental concerns will have greater importance for corporations as a due diligence for social responsibility and rising customer expectations who support green businesses.

### 4.4.2 Data Ecosystem Uncertainties

Scenario analysis also calls for determining the uncertainties and challenges that may affect future scenarios. The method and approach for derivation of these uncertainties is discussed in sections 4.2.1 and 4.3. Uncertainties are defined as branching questions about a concern or trend or forces that are important but cannot be predicted (Schoemaker & Mavaddat, 2000; Van Der Heijden, 1996). Uncertainties can be articulated into three forms: risks, structural uncertainties, and unknowns (Van Der Heijden, 1996).

**1. Growth of different data markets.** Researchers and practitioners have noted the challenges with data accessibility, data provenance, data quality, and data sharing. These obstacles also exacerbate tension and complexities between data producers and data owners. Therefore, on the European Commission's strategic agenda, data accessibility and availability and reuse are important issues to consider (European Commission, 2020a). The EU plans to have a B2G open data directive as a means to increase interorganizational data sharing for governmental use (European Commission, 2020a). However, the Commission also notes that the main drivers for the data economy are sourced from commercial and industrial data (European Commission, 2020; European Commission, 2020c). Thus, it is uncertain whether the data economy will be stimulated by sharing proprietary data between businesses in B2B environments or whether government investment will increase or accelerate the market for B2G data sharing. Whereas, the G2B market has already been fostered via the Open Data Directive within the EU (European Commission, 2020a).

There are other uncertainties in how specific data markets will develop to support the data economy such as big data versus data analytics which also depends on the balance between regulatory bodies and market demand. Moreover, the value of data is difficult to quantify in these different environments and instances. Therefore, how data is valued and used has implications on market and technology developments as well. From a market pull and technology push perspective, different data markets can be enabled or accelerated due to new technologies such as MPC. Conversely, the complexity of ethics and consumer needs for data control can also shape the market and regulation accordingly, whereby open data for public value is supported rather than the commercial value of data.

**2. Data Governance.** As mentioned previously, interorganizational data sharing is inhibited due to a lack of formal governance frameworks. The impediments to data sharing include imbalances in power, an ambiguous legal framework for data ownership and use, and the lack of incentive to share private data with competitors (European Commission, 2020a; Robey et al., 2008). Other data sharing obstacles in the B2B segment are summarized in Figure 13 below, sourced from Arnaut, Pont, Scaria, Berghmans, & Leconte (2018) study on data sharing between companies. According to this study, the most common barriers to B2B data sharing that companies face are technical, legal, and governance of data. However, some of these barriers may not be as important or relevant to MPC conditions such as localization rules and reputation. The Free Flow Data Directive and MPC privacy preserving functions may be able to alleviate any concerns for malpractice with regards to data use and cross-border/sector transactions.

On account of developing the proper governance models and contractual agreements for IOS relationships, rules and legal requirements can be standardized on a national or EU level, created on a sector-specific level or vary between each group of companies who enter into data sharing agreements. It is difficult to standardize governance frameworks because data is so diverse. Data uses can vary and thus, the value will vary depending on its use as well as the perception of stakeholders and actors (European Commission, 2020a). It is likely that companies will be protective of their assets, including data and it has implications on how governance models will develop and to what extent.

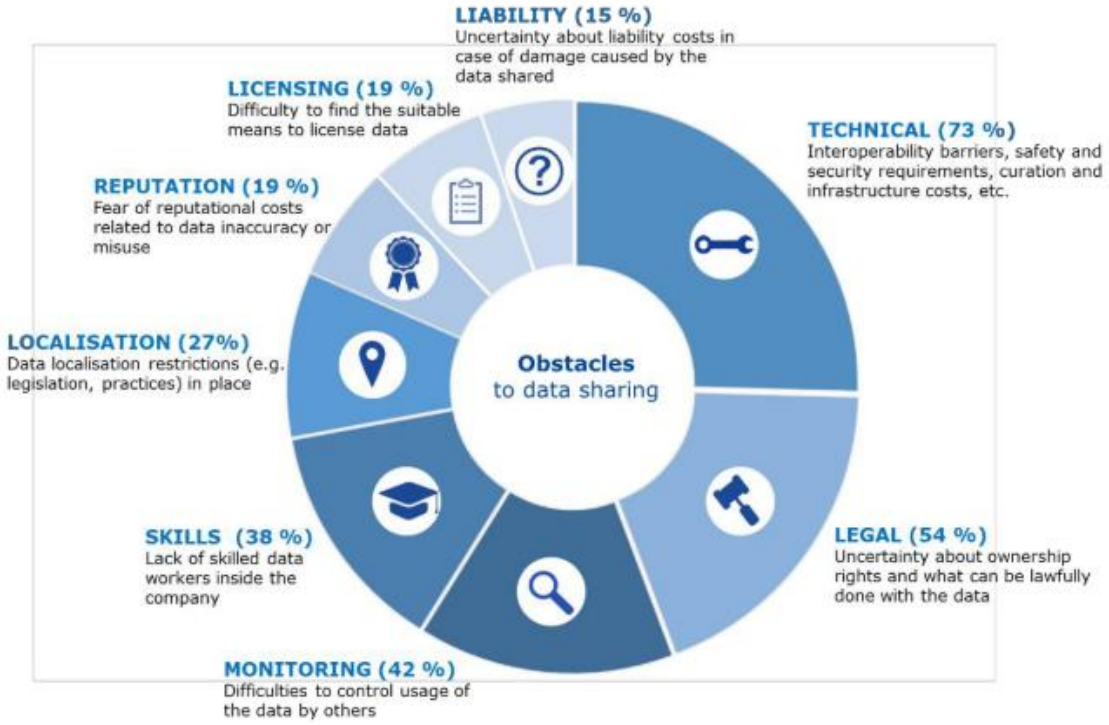



*Figure 13: Survey results for obstacles to B2B data sharing sourced from Arnaut et al. (2018).*

According to van den Broek & van Veenstra (2018), there are four inter-organizational governance arrangements: market, bazaar, hierarchy, networks. Data sharing collaborations are more aligned with a *network governance* arrangement. Van den Broek & van Veenstra (2018), describe the *network governance* arrangement to have the following characteristics:

- trust incentives;
- moderate control: reciprocity and social contracts;
- reasons for adoption: low cost access to resources and joint solutions;
- moderate flexibility of the collaboration;
- long-term duration;
- social contract is informal, focused on common objectives;
- and the network relationships are interdependent (van den Broek & van Veenstra, 2018, p. 332).

Some of these features also coincides with interorganizational theory and characteristics of banks which depend and benefit from networks effects and externalities (Petralia et al., 2019; Robey et al., 2008). However, MPC may have an effect on these governance mechanisms such as improving trust and limiting legal developments in this regard. Or it can increase the difficulty of data sharing arrangements because stakeholders may not know how data is processed or computed in MPC, where the data is sourced, if the data is reliable, and who owns the MPC outputs and what they are allowed to do with it. This may result in more formal contracts, requiring legal entities and powers.

**3. Compliance with big data and analytics.** The main framework for protecting personal data is the GDPR. However, big data and new technologies for data analytics may make it easier to find personally identifiable information in datasets (van den Broek & van Veenstra, 2018). This issue is described by van den Broek & van Veenstra (2018), whereby the concept of big data aims to extrapolate information from

aggregated data and large datasets which can lead to non-personally identifiable information becoming identifiable if it is combined with other data. Whereas, Petralia et al. (2019) note that technology incumbents disagree with this notion and deem it implausible that anonymised data can have personal attributes when it is aggregated with so many data points (p.21). The mixing of anonymised and nonpersonal data may have unforeseen consequences that violate the protection laws of the GDPR, especially for financial services (Petralia et al., 2019; van den Broek & van Veenstra, 2018).

### 4.4.3 Conclusion

Predetermined factors and elements and trends were identified using the PESTLE framework. However, macro-environmental analysis is limited in structuring the environment from an organizational approach (Burt et al., 2006). Therefore, it has limited utility for banks and little effectiveness for strategic decision making in MPC implementation decisions. It was established in the scenario analysis method that one of the main objectives is to improve decision making for banks. Therefore, uncertainties that are used in the first step of scenario development needs to be relevant and important to the organizations. In order to meet this objective, uncertainties were examined according to the contextual and contingent conditions that are relevant to the organisation itself and MPC related activities.

The extent to which these uncertainties are interrelated or interdependent to MPC implementation and business models are not fully understood. However, establishing the importance of uncertainties based on historical precedents can be useful to establish a correlation and insight into the probabilities of outcomes (Schoemaker & Mavaddat, 2000; Van Der Heijden, 1996). The most important risks should be accelerators or inhibitors to MPC implementation which is partly informed by sustainable competitive advantage as established in Chapter 3, and the historical view of bank stability and business models (Section 3.1.5). Furthermore, the predetermined barriers to data monetization and leverage also pose risks to MPC implementation in banks.

Due to the financial crisis, more regulation and supervision was placed on EU banks to institute more transparency in banking activities and in the sustainability of their business models. Therefore, data regulations like the GDPR ensure transparency and integrity in these operations should be an important variable in how banks decide to use their data. The high regulatory environment demands that banks are compliant with these regulations and therefore, remains an important concern to stakeholders. It can be inferred that MPC will need to be compliant with GDPR, but the development of new data laws over the coming years may inhibit or decelerate use of MPC.

In the historical view of barriers and challenges to data sharing, regulation can also affect who banks are allowed to share data with and by what means. However, it is uncertain if this is the main driver or if the growth of different data markets will be the driver for MPC implementation in banks. Nonetheless, market segments will dictate who banks compete with and who they share data with via MPC. Moreover, regulation and the market can lead to multiple uncertainties in the development of data driven technologies, its use, and how business model components are affected.

Banks' sources of competitive advantage includes trust with their customers and their data (Petralia et al., 2019). Therefore, in order to continue using leverage points, MPC needs to ensure that the trust of banks' clientele and the secrecy of their data is maintained. Theoretical notions of sustainable competitive advantage for banks indicate that MPC will be applied from a network perspective, leading to the unpredictability in the degree to which organizations share, use, and protect their data. There seems to be a logical relationship between data governance and the strategic decisions regarding outcomes or adoption of data-driven business models.

The high-level objective of identifying and correlating uncertainties is to eventually improve decision making for MPC adopters. In order to improve decision making:

- manage the focus of the organisation has to be managed
- make the organisation more preceptive of its environment and therefore, more adaptive (Van Der Heijden, 1996, p. 132).

Therefore, these principles in scenario analysis leading up to decision-making needs to be pervasive throughout. The trends in this section are data related and are inherently relevant to MPC, but could be still too generic for developing effective scenarios for a specific organisation. Nonetheless, uncertainties are derived from trends while maintaining the conceptual lens of data sharing in organizations via MPC. In the domain of data ecosystems and data sharing, the main uncertainties that are relevant to organizational use of MPC were outlined. The next section will repeat the cluster analysis as a means to evolve towards bank-specific uncertainties for MPC implementation.

## 4.5 Bank Ecosystem Trends and Uncertainties

This section narrows the scope of trends that are relative to the EU bank sector and their position in the financial ecosystem. Similarly, these inputs provide value to developing possible future outcomes for MPC implementation and use in European banks.

### 4.5.1 Bank Ecosystem Trends

**1. Profitability.** Generally**,** profitability and risk are the utmost essential drivers for success in banks because it entails how banks generate revenue, prevents losses, and ensures cost savings. European banks' profitability compared to other nations like the US and UK, have comparatively low interest rates, high non-performing loans which contributes to their overall low profitability (Deloitte, 2020; Srinivas et al., 2019). Although, the ratio of nonperforming loans have decreased from 3.81% in Q1 to 3.22% in Q4 of 2019, non-performing loans and credit risk will remain ubiquitous in banks' challenges (European Central Bank, 2019d). European banks have still not recovered completely from the financial crisis in 2008 wherein some banks have rate of returns (ROI, ROA, ROE) that have been persistently low (European Central Bank, 2018). Hence, remains a high-risk driver for banks and a priority of supervision for the EU (European Central Bank, 2019a). As mentioned previously, European banks continue to experience near zero to negative interest rates due to the interest rates set by the European Central Bank (Srinivas et al., 2019). If banks cannot pay interest to the ECB, then bank customers and clients will receive higher fees as result which may deter customers away from large banks (European Central Bank, 2018; Srinivas et al., 2019; Viorica, 2013). Since profitability remains an issue for incumbent banks, new business models are required in order to increase revenues, become more cost-efficient, reduce losses, and increase returns.

**2. Competition with fintechs and technology incumbents.** The banking sector will also continue to be challenged by fintech and technology companies. Banks have difficulty in balancing technology adoption and digital transformation due to rising compliance and regulatory costs, low interest rates, and competition (European Central Bank, 2018; Petralia et al., 2019; Srinivas et al., 2019). This gives fintechs and other market entrants a competitive edge because these companies are more readily able to adopt emerging technologies as well as change or enhance their business models (Rym; Ayadi et al., 2012; Petralia et al., 2019). The rise of start-ups and investments into fintechs will continue and either force banks to collaborate with fintechs or buy them out (European Central Bank, 2018; Petralia et al., 2019; Srinivas et al., 2019).

Petralia et al. (2019) compares the (dis)advantages between banks, fintechs, and big technology firms and argues that banks have an advantage over their competitors in terms of funding, network effects, and abiding by data privacy and protection regulation. However, banks have a disadvantage in implementing new technologies due to legacy systems that affect interoperability between systems and leveraging data (Petralia et al., 2019; Srinivas et al., 2019). However, they can be fluid in terms of managing the customer experience and prudential regulation (Petralia et al., 2019). Hence, banks can gain a competitive advantage by either overcoming their weakness with regards to legacy systems and using new innovations and/or improving customer experience.

**3. Growth in payments market and mobile services.** Increased competition is also encouraged by the EU due to the implementation of the PSD2 (Premchand & Choudhry, 2019). This requires banks to provide data access via digital channels in order to grow the financial services market (European Commission, 2019d). The PSD2 enables open banking that allows fintechs and big tech to access banks' customer data, most likely via APIs, so that they can provide more products and services to customers (Premchand & Choudhry, 2019).

There will be a push on the consumer side and industry side for faster payments and seamless transactions. Thus, the payments services market is one of the fastest growing markets in finance. PSD2 empowers third party providers (TPPs) to create applications for mobile services and empowers consumers to be in control of how their data is used for these third party applications (European Commission, 2019d; Premchand & Choudhry, 2019). The increased competition and growing market will allow companies and new technologies to shape the payments market in the coming years (Petralia et al., 2019).

**4. Rising customer expectations.** There will be less face-to-face interactions between customers and banks, especially in retail banking (European Central Bank, 2018; Srinivas et al., 2019). There will be rising expectations in the options to control and manage their banking activities from mobile and digital interfaces. Banks have competitive advantage in terms of customer data that they have amassed as well as the trust that consumers have in managing their assets (Petralia et al., 2019). Since open banking can jeopardize the value of their customer data, banks should leverage the value of trust in new products and services. Premchand & Choudhry (2019) argue that customers will expect the same security and trust in these new financial services in open banking in terms of protecting their personal data and assets.

There will also be increased market demand for cross-border transactions and lending. Cross-border e-payments are supported by the EU and the PSD2 because it protects consumers rights, ensures security in transactions, protects against fraud and lowers or bans surcharges across borders (European Commission, n.d.-b). Moreover, banks are expected to increase customer engagement via faster interbank payments and e-payments, real-time information flows, and better service offerings in communication and advisory services (Premchand & Choudhry, 2019; Srinivas et al., 2019).

**5. Cybersecurity and Risks.** Similarly, to data ecosystems trends, cybersecurity will be ubiquitous in all banking activities. The opening of digital channels to third parties increases risks for banks and vulnerability to bad actors (Petralia et al., 2019). As a result, Petralia et al. (2019) describes that the consequences include loss of data, identity theft, and fraud. Furthermore, the dependency on third parties for technologies and outsourced services increases the risks to cybersecurity threats and any form of system failures.

**6. Increasing risk/importance of AML/CTF.** Closely related to cyber security are the risks associated with money laundering and terrorist financing. The Commission reports that 0.7-1.28% of the EU's GDP is involved in suspicious financial activity (European Commission, 2019b). The European Central Bank and the European Commission are increasing their focus and supervision on anti-money laundering (AML) and counter terrorist financing (CTF) initiatives and risk mitigation frameworks (European Central Bank, 2019b; Petralia et al., 2019). Moreover, the rise of e-identity or digital identity authentication products and services are a result of maintaining integrity in the financial system and digitalizing Know Your Client/Customer (KYC) processes. Petralia et al. (2019) notes that banks and stakeholders have 'raised the value of data in compliance and risk management in order to enhance AML and financial crime prevention and to improve fraud mitigation and detection' (p. 32).

On the regulatory side, the EU has failed to deliver adequate supervisory practices and frameworks in order to improve AML/CTF across EU member states (European Commission, 2019b). Due to developments in technologies and criminal activity and lack of proper informational sharing between the financial supervisory entities for each EU state, the Commission plans to apply new rules for sharing data (European Commission, 2019a, p. 1-2).

**7. Rising compliance and technical costs.** Given that the risks and security requirements are high for incumbent banks, technical and compliance costs are increasing alongside changing markets and regulations. In particular, legacy systems hinders banks from creating new business models, adopting new technologies, and maintaining cost-efficiencies with regards to IT infrastructure and interoperability (Srinivas et al., 2019). It also affects banks' ability to compete with new fintech startups and technologically advanced companies.

### 4.5.2 Bank Specific Uncertainties

**1. Legacy systems.** There are uncertainties in how banks will overcome barriers with legacy systems that prevent banks from fully leveraging their data and adopting new business and technologies (Schroeder, 2016; Srinivas et al., 2019). It also is a huge factor in costs and losses from technology investments and IT costs (Srinivas et al., 2019). Petralia et al. (2019) argues that banks can utilize cloud computing to overcome issues with legacy systems and interoperability in order to leverage customer data more readily. However, one of the challenges is that the European commission faces is that most companies are dependent on third party cloud service providers that are not in the jurisdiction of the EU (European Commission, 2020a). Other technologies that banks can benefit from is AI and machine learning which can both improve efficiencies in certain processes but also lead to new products and services for the bank (Petralia et al., 2019). Lastly, Petralia et al. (2019) highlights the transformative power of blockchain and distributed ledger technologies for data storage, data collection, and record keeping because it will be quicker and cheaper for meeting compliance standards (Petralia et al., 2019). However, one of the disadvantages of blockchain is the storage capacity required to keep all of that data including the storage requirements for public and private keys.

Legacy systems also pose uncertainties and barriers to MPC implementation because quality data as well as proper data collection and processing mechanisms need to be in place in order to derive value from MPC. Legacy systems also introduce barriers to the combination of MPC with other technologies such as AI and ML. MPC may not be implemented as a standalone technology but it can be potentially used to enhance other data-driven operations and technologies. However, this is dependent on how well banks can utilize new technologies or update their legacy systems.

**2. Regulations.** There may be new compliance and regulations that banks need to abide by within the next five years. There is a possibility that the Commission will be revising the payment services directives or changing the directives for AML/CTF which has been revised six times to date (COMMISSION DELEGATED REGULATION (EU) 2018/1108, 2018). Furthermore, the aforementioned compliance and ethical standards for data sharing will also apply to the finance sector. The importance of governance and legal frameworks and contractual agreements in data sharing are heightened and need special attention because transaction and customer data are subject to risks.

Given that banks are highly regulated and have to abide by laws with regards to data and services/products, banks are less flexible with regards to competing with fintechs and big techs because these third party companies are under different jurisdictions (Petralia et al., 2019). This provides third party providers with an edge in the competition because they may be able to circumvent policies or adhere to different rules that do not or cannot apply to banks (Petralia et al., 2019). On the other hand, if the EU and national governments increase regulation and governance over these companies then it may open opportunities for banks to create and sell innovative solutions to help them navigate compliance rules and standards.

To summarize, banks can improve their competitive advantage if they cut costs in their business operations and processes which leads to higher profits for the bank and possibly more legroom to invest in better technologies and innovative solutions (European Central Bank, 2018; Srinivas et al., 2019). Banks can also improve costs in areas related to risk management in credit lending, money laundering and terrorist financing, and cyber security (European Central Bank, 2019a, 2020; Srinivas et al., 2019). Digitalization and automation also play a role in improving organizational processes that can directly or indirectly lead to better customer experience and relationships such as robotic process automation (RPA) in advisory services (Petralia et al., 2019; Srinivas et al., 2019). Data can facilitate or enable these technologies which positions MPC as a disruptive technology to mediate processes in risk management such as credit lending and financial crime or providing better data input for AI and RPA technologies.

### 4.5.3 Conclusion

In conclusion, there are parallels with the uncertainties in the banking environment and in the data-driven environment with regulation. It was established in the preceding sections that most data-specific uncertainties involved risks to MPC implementation and the uncertainty of how these risks will play out in the future. However, bank-specific risks are more predictable and manageable because banks are already adept to handling market risks to a certain extent. However, interventions in regulation are difficult for banks to effectively manage since they have less power and flexibility. For the same reason, legacy systems are always a main concern for banks because it is not easily solvable and may produce more issues for banks over time when they seek other ways to operate. Thus far, the main uncertainties take the form of risks which is defined as known unpredictability on the basis of historical contexts or events (Van Der Heijden, 1996). The underlying theme in these threats to MPC implementation involve structures and mechanisms that restrict banks to act or narrow the options for strategic positioning and decision making. This theme is further explored in the next chapter, the start of the scenario development phase.

# 5. Scenario Development (Phase 3)

The purpose of this chapter is to initiate the third phase of the scenario analysis method by deriving uncertainties for MPC and then develop initial learning scenarios. In order to create effective scenarios, MPC implementation uncertainties should establish utility of scenarios to stakeholders in banks and then validated via semi-structured interviews. The next step is to create initial learning scenario narratives in order to challenge the existing mental models of stakeholders (Amer et al., 2013; Schoemaker & Mavaddat, 2000; Van Der Heijden, 1996; Wayland, 2019; Wright et al., 2013). After discussing these scenarios with stakeholders, qualitative feedback and input from interviews will be used to generate more accurate scenarios.

## 5.1 MPC Uncertainties

MPC implementation should help banks with improving profitability. Hence, uncertainties and scenarios will be contextualized from a risk and revenue perspective since these are some of main drivers for success in banks. Main risk drivers for banks are credit lending and financial crime management whereas, the fastest growing market in the finance sector are payments (European Central Bank, 2019c; Premchand & Choudhry, 2019). By understanding the macro-environment and trends that have implications on MPC implementation, the uncertainties for MPC can be determined so as to move towards more context and organization specific scenarios.

**1. Legal and Governance frameworks for MPC datasets and collaborations.**

The possibility of mistrust in the reliability and quality of data from other parties requires a legal and governance framework to maintain control, trust, and liability in MPC settings. However, data regulation and governance can vary on different levels (Arnaut et al., 2018). Contractual agreements on an organizational level will require investment and time to produce between multiple parties and it may also vary according to different use-cases. MPC involving transaction data can have different legal arrangements than sharing fraud indicators, for example due to the fact that different data is involved which may have implications for different type of risks. Similarly, to data re(use) barriers, there are unknowns regarding how MPC outputs will be owned and (re)used. It also ambiguous as to who will be liable for instances when MPC outputs are incorrect due to incorrect or unreliable data inputs. Moreover, MPC provides value because a trusted third party is not required to facilitate data sharing (Archer et al., 2018). However, there may be required entities or mechanisms, legal or not, in order to ensure proper and ethical practices among MPC participants such as those related to data collection or preventing abuse of power.

Information sharing and data regulations on a national and EU level can also have implications that either foster or inhibit the use of MPC. The minimum compliance requirements that MPC should follow with regards to personal data are mandated by the GDPR. Since cross-border and cross-sector data sharing is a growing market and stimulated by government investment, it is unknown how future EU or national regulations will develop over the horizon of five years (European Commission, 2020d). The aforementioned newly implemented data regulations such as the Free Flow Data Directive and the Open Data Directive can be the overarching regulatory frameworks that also apply for MPC applications. However, these regulations do not replace or override the GDPR and they do not specifically apply to MPC or contractual arrangements between private organizations. Furthermore, the Open Data Directive may require some organizations to provide their data under an open data policy in order to promote competition for SMEs and less so for incumbent banks (Directive (EU) on open data and the re-use of public sector information, 2019/1024, 2019). Therefore, these regulations can either foster the

implementation of MPC or make it more difficult for organizations to use MPC. This could further complicate MPC collaborations, make it less scalable, and deter banks from implementing it.

In the aforementioned data trends, there was a discrepancy in the perception of big data and personal data privacy. One MPC research study, tested their MPC protocol by anonymizing personal data prior to MPC computations (Haaften et al., 2020). However, there is a possibility that anonymized data points can become personally identifiable when aggregated with other datasets (Petralia et al., 2019; van den Broek & van Veenstra, 2018). There may also be instances for certain business use cases whereby criminals must be identified in order to combat cyber security threats and or financial crime related to anti-money laundering or terrorist financing. If MPC outputs provide enough personally identifiable data points that can expose or pinpoint individuals or make them vulnerable to other data computation techniques such as data mining, then it would violate the GDPR and ethical rules for data privacy. Lastly, although MPC protects the privacy of individual data sets, it is unknown whether companies are still obliged to provide informed consent to clients and customers when their data will be used for MPC applications.

**2. MPC implementation and use/participation incentives.**

In order to use or implement MPC, there needs to be data sharing between at least three parties otherwise, MPC becomes obsolete and risky with two-party computation protocols (Evans et al., 2018). However, investing and adopting new technologies are costly for banks because there are legacy systems and interoperability issues to overcome (Petralia et al., 2019; Srinivas et al., 2019). However, there are likely to be increased partnerships and collaborations in the payments services market (European Commission, 2019d; Premchand & Choudhry, 2019). In order to add value to their existing customer data, additional external data from other banks or third parties must be enough incentive for banks to participate and/or invest in MPC. Furthermore, this is difficult to determine given that the value of data is hard to quantify. The premise of MPC is to maintain the privacy of individual datasets and therefore, this can also introduce a lack of trust in partnerships because each party cannot evaluate or determine the value and quality of data inputs of the other parties. Otherwise, processing or checking for data quality goes against the purpose of MPC. Therefore, legal and compliance frameworks are necessary to govern these partnerships.

**3. Technology ownership of MPC**

Alongside the unknowns about the legal risks of MPC, there are uncertainties related to the ownership of MPC technology. Banks are known to rely on third party providers for new technologies but this introduces risks in loss of data and system failures (European Commission, 2020a; Petralia et al., 2019; Srinivas et al., 2019). Therefore, the risks might outweigh the benefits if banks choose to rely on MPC providers. On the other hand, if banks develop their own MPC technologies then there could be heavy investment and interoperability issues with other MPC systems. Furthermore, this may also introduce another layer of legal uncertainty because any system failures may be under the fault or jurisdiction of the company who owns the technology.

**4. MPC (meta)data requirements**

The ambiguity with regards to how data is sourced, how reliable it is, and what type of data can be used or not used, is a barrier for MPC implementation and use. Long standing banks have accumulated customer data via different IT systems and therefore, interoperability and variety of data can be quite diverse. Raw, processed, structured and unstructured data have implications on the correctness of MPC outputs because data formats should be somewhat similar in order to derive value in data analytic computations. However, processing data for MPC can violate the rules and regulations of data privacy.

**5. Business Models**

The aforementioned uncertainties and barriers to implementation are mostly related to legal risks, governance frameworks for data and collaboration, and practical investment and technical considerations. However, the aims of this study is to also understand how MPC may enable new business models. Scenarios should postulate sources of revenue or revenue models for MPC enabled business models. Value capture from data is also another concern because shared data may be governed by the network and re(use) of MPC outputs may be legally bounded or inhibited. Value capture is contingent upon regulation, compliance, and governance frameworks. Moreover, the future role and intervention of supervisory and regulatory powers such as the European Commission and the European Central Bank are also unknown.

Petralia et al. (2019) describes the value of data in the following examples of bank operations (p.32-33). Combined data sets from different sources can improve the success rate for detecting and preventing fraud which raises the value of data in compliance and risk management processes. The importance of data is also underpinned in improving credit decisions via risk monitoring and reducing information asymmetry. Moreover, better data and algorithms are perceived to improve risk monitoring of customers, digitalizing the screening process, and preventing financial fraud. However, interviews with banks in Petralia's et al. (2019) study note that data collection and protection would affect the pricing of products and services and can change revenue models in order to access more customer data.

## 5.2 Initial Learning Scenarios

The following scenarios are developed using inputs from the environmental and trend analyses of the data and financial ecosystems. According to Bradfield, Wright, Burt, Cairns, & Van Der Heijden (2005), intuitive logics scenarios can be derived deductively. Thus, scenarios will also include inputs from theoretical foundations of IOS and business model concepts that were discussed in Chapter 3 of the literature review section. Scenarios can be developed intuitively or with a more structured approach with matrices Schoemaker & Mavaddat (2000). Given that building scenarios is an iterative process, initial scenarios will be developed intuitively. Then the most important uncertainties and scenarios will be verified by stakeholders via semi-structured interviews. This will provide further effort and consistency for scenario development using a more structured approach such as morphological analysis, later in this study. This list of scenarios is not meant to exhaust all the possible future outcomes, but rather to include scenarios that are plausible, consistent, relevant to banks, and are novel to businesses in order to challenge conventional thinking. Therefore, it is not particularly useful to include a scenario wherein MPC is not implemented or used at all by banks or worst-case scenarios since it does not satisfy two criteria: relevancy and novelty.

As such, scenarios will encompass outcomes that are value creating. From the general conceptual model developed in Chapter 3, there are three main value creation outcomes for MPC implementation: operational, social, and strategic. Therefore, initial scenarios can follow this model whereby MPC implementation can result in the following generic outcomes:

- operational: improve banks' internal efficiency by some processes or operations;
- social: innovate or transform an existing process or customer offering in banks;
- strategic: enable new products and services.

These generic outcomes can formulate into more specific narratives by incorporating banking and data trends (subchapters 4.4 & 4.5) as well as documented MPC applications in banking (Section 3.1.4). The

theoretical and practical knowledge inputs for these scenarios are listed in Table 4 according to the four scenarios developed.

| Initial learning scenario | Value creation outcomes (Chapter 3) | MPC application in banks (Section 3.1.4) | Data Trends (Subchapter 4.4) | Bank Trends (Subchapter 4.5) |
|---|---|---|---|---|
| **1** | Operational | Data sharing for risk mitigation: cybersecurity, fraud, credit and loan risk | 2, 3, 5, 6, 7 | 1 |
| **2** | Social | Data sharing/benchmarking in credit and loan financing profiles | 1, 2, 3 | 2, 4 |
| **3** | Strategic | -Undocumented/unknown in banking<br>-overcome data sharing barriers | 1, 2, 3 | 1, 2, 3, 4, 5 |
| **4** | Social | Data sharing related to financial crime: AML/CTF | 1, 2, 3, 5, 6, 7 | 4, 5, 6, 7 |

*Table 4: Conceptual and practical knowledge inputs for initial learning scenarios.*

In general, initial learning scenarios can become more specific by coupling general value creation outcomes from the conceptual model with MPC applications and industry trends that fall under those outcome categories. Then more specific scenario narratives can be developed with these several inputs. Each learning scenario is listed separately and explained below. Furthermore, informal discussions with bank professionals about fraud detection and compliance helped with generating initial scenarios 2 and 4.

1) One of the outcomes of IOS involves improved efficiency across organizational processes that has cost saving and productivity benefits (Robey et al., 2008). Known MPC applications in literature coincides with this purpose to support defense and risk mitigation efforts in banks. These applications include information sharing in cybersecurity, fraud detection, credit checking, and anonymous voting and data sharing. The aforementioned risk functions can help banks save money or prevent them from losing money, if risk is lowered. Thus, for cybersecurity and fraud detection operations, MPC can be applied in helping banks to achieve a social outcome or operational outcome.

***MPC improves banks' processes and operations (operational outcome).***
*This scenario will most likely be supported by government and supervisory bodies because banks must improve their strategies for nonperforming loans as delegated by the European Central Bank, report to Financial Intelligence Units with regards to anti-money laundering and terrorist financing, and also properly screen their customers to abide by Know Your Client/Customer rules (European Central Bank, 2019a; European Commission, 2019a; Srinivas et al., 2019). However, MPC will only be used as a matter of necessity in compliance and risk management by the private sector in this scenario.*

2) Improving credit and loan risk intel is cost saving for a bank, but it is also a ubiquitous core offering for all banks. Based on trends and risk targets for banks and regulators (See subchapter 4.5), improving credit and loan risk is one of the top priorities in the industry. Therefore, MPC enhanced credit risk functions can also have a social outcome that may indirectly lead to new business models in the credit financing market.

Other trends in existing markets such as financial advisory services and e-banking can result in other value creation activities for social outcomes.

***MPC enhances existing products, services, and technologies (social outcome).***
*If the aforementioned scenario is successful, the data driven improvements in credit monitoring, fraud detection and cybersecurity processes can lead to enhancements in products and services. The data produced from MPC collaborations can provide input for other data-driven technologies such as AI or ML which can enhance automated and digitalized financial advisory services. It can also open new opportunities and partnerships with third party providers. If banks outsource these services to other companies or use their technologies that help manage credit lending, AML/TF monitoring, or cybersecurity needs then banks can collaborate with them by providing their data that will improve TPPs' products and services. In this scenario, banks may be able to benefit from network effects and receive revenues from these TPPs.*

3) New MPC driven customer offerings in banking are not documented in academic literature. Therefore, this scenario is less transparent and predominately informed by market trends in banking in order to determine potential business opportunities. With the rise of e-banking and PSD2 regulations, new collaborations with non-bank partners and new products for this market are possible. Furthermore, considering that banks have leverage in terms of data and compliance, these factors should be considered valuable in competing in the open banking space. Based on these trends in banking and data ecosystems, MPC enabled new offerings and collaborations can lead to strategic value creation outcomes.

***MPC enables new products and services (strategic outcome).***
*If MPC outputs are permitted by the network partners for re(use) and that the data is reliable, then it can enable banks to create new products and services. Banks have a competitive advantage over TTPs with regards to the trust of their customers, the customer data they hold, and their fluency in regulatory compliance for financial services (Petralia et al., 2019; Premchand & Choudhry, 2019). Hence, if MPC implementation results in better outcomes in compliance and risk management, it can enable banks to produce innovative solutions for other new entrants in the financial services market who are not well versed in ensuring security and privacy standards that meet regulatory compliance. In this scenario, banks can receive revenue directly from sales and also network effects if multiple developers incorporate algorithms or data into their APIs or applications.*

4) The rationale for scenario 4 is similar to scenario 1 whereby data sharing for security and risk purposes inadvertently helps banks' internal processes. However, scenario 4 is distinguished separately from scenario 1 to consider situations in which banks are pressured by government and policy rather than business incentives to combat financial crime. Moreover, this scenario is also modelled after an on-going proof-of-concept in MPC fraud detection schemes with other banks and governing bodies.

***MPC assists supervisory bodies and governmental agencies (operational outcome).***
*A fourth scenario is similar to the first scenario listed, but is characterized by more data sharing between public and private sectors to support financial policy and an open data economy. The European Union intends to invest in a single open data market as well as improve frameworks for AML/TF (European Commission, 2019b, 2020a). In this regard, regulators may require that banks open up their data or provide their data for free. MPC may be a solution to incentivize banks to share their data for public policy without revealing their proprietary data and risking their competitive advantage. On the other hand, this implies that MPC will be utilized by government more so than the private sector. Banks will only use MPC*

*as a requirement to comply to AML/TF initiatives, report to supervisory entities such as the ECB, and provide data for governmental purposes.*

These four scenarios slightly mirror the conceptual model in the perspective that MPC produced data analytics or computations can (in)directly improve or create a new activity or function within the bank. The next chapter will detail how these uncertainties (subchapter 5.1) and scenarios (5.2) will be validated with experts via semi-structured interviews.

# 6. Interview Protocol

The main objective of interviews is to continue through the scenario development process (Phase 3) by confirming uncertainties and initial learning scenario narratives with stakeholder experts. Expert feedback helps with ascertaining whether the information presented from Chapter 5 is plausible and relevant. Interviews serves as a checkpoint and justification for proceeding to the next phase of scenario analysis. Moreover, the intended project outcomes for intuitive logics model includes challenging existing mental models of stakeholders with scenario narratives which may take place during interview proceedings.

Data collection via semi-structured interviews with industry experts and stakeholders is necessary in order to answer the third research sub-question which is, 'What are the critical uncertainties of MPC implementation in banking environments?'. Questions within the interviews will also be structured around business models and opportunities with the objective of answering SQ4 which is, "Which business model components could be affected by MPC implementation and use?". Expert input and data will be further analyzed in Chapter 7 to fully address these sub-questions.

## 6.1 Interviewee Selection

Interviewee selection criteria was based on knowledge and understanding of MPC or at least its purpose and value as a data sharing technology for privacy preserving data analytics. Since MPC is new technology and unbeknownst to some experts and professionals in the banks, security experts in cryptography, fraud, and cybersecurity were also selected due to their technical knowledge and the business areas that they work in where MPC can be applied. Furthermore, the high regulatory environment of the bank sector requires input from a stakeholder or professional with a compliance or legal background/expertise. Schoemaker (1995) recommends to involve managers or individuals with decision making power for validation input and scenario development. Moreover, the exploratory nature of the research design was not limited to selecting interviewees with some managerial or decision-making role within the bank who could provide qualitative feedback with regards to the business opportunities and strategies of their respective banks.

Most interviews were held internally via connections through the internship organization. Experts working on MPC projects at the internship organization was formally asked first. Furthermore, the research advisor and internship supervisor provided contact details or connections to other individuals who would be knowledgeable in MPC or evaluating new business opportunities for the bank. The research advisor of this thesis also provided contacts from his TRUSTS network which is a consortium focused on enabling secure and private data exchanges across the EU. The internship company advisor recommended internal experts to invite for interviews as well as ask for further contacts in their network. These interviewees were asked at the end of the interviews whether they could recommend person(s) to contact either internally or externally as potential interview participants in the research study. Mostly security experts were recommended. Interview availability and willingness to participate was dependent on network connections because these industry experts could recommend or vouch for a particular individual with MPC knowledge or expertise.

The following table summarizes the interviewees who rejected, accepted, or did not correspond to the interview invitation and why they were chosen to partake in the research study. Van Der Heijden (1996) recommends to conduct 10-15 interviews or until new information or insights approaches an apex. Therefore, more than 15 potential participants were contacted. The table rows highlighted in green indicate the interviewees who participated in formal interviews.

| | Organization Type | Role/Title/Expertise | Agreed to Interview | Selection Rationale |
|---|---|---|---|---|
| 1 | Independent Network Organization | Security & Innovation | Yes | Expert security knowledge and network collaborations with organizations in the public and private sector |
| 2 | National Bank Association | N/A | No | Legal and governance input for MPC and banks |
| 3 | Bank A | Security | Yes | Expert in security and interests in technical solutions for the bank |
| 4 | | Technical/innovation, management | Yes | Technical expert and knowledge of MPC; works in MPC projects |
| 5 | | Compliance | Yes | Expert in compliance, legal and governance issues at the bank |
| 6 | | AI, innovation, monitoring and detection | Yes | Technical knowledge of MPC; Researched MPC for 5 years, published paper in MPC research for fraud detection |
| 7 | | Computer fraud, security | Yes | Expert in fraud and security; interests in technical solutions for the bank |
| 8 | | Security expert | No; agreed to informal discussion | specializes in applying cryptography solutions |
| 9 | | Customer onboarding | Scheduled but meeting was cancelled | Digital transforming, maximizing data capabilities |
| 10 | | Lead Products Strategy & innovation | Undetermined sick leave | MPC knowledge and senior bank professional |
| 11 | Bank B | Data science, information security | Yes | Technical knowledge of MPC; published paper in MPC research for fraud detection |
| 12 | | Information security, business development | Yes | Cryptographic expert and business expertise |
| 13 | | Cryptography | Yes | Cryptography expert |
| 14 | | Senior Data Scientist; AML | Schedule conflict and no response | Works in AML initiative and research areas in MPC |
| 15 | Bank C | Innovation; digital business | Yes | Knowledge of data market and trends; expert knowledge in digital business |
| 16 | Bank D | Data science; fraud; cybersecurity | No response | Co-author of published paper on fraud detection via MPC |
| 17 | Bank E | CTO | Agreed but ceased responses to schedule | Technical expertise and executive/managerial role |

*Table 5: Interviewee participant selection*

Out of a total of 17 potential interview participants, only 8 interviews were conducted with a total of 11 respondents. One of those respondents did not agree to a formal interview, but agreed to an informal discussion whereby the points of discussion was consented by the interviewee to be used and included in

this study. The lack of response from the National Bank Association rejected requests for an interview due to lack of MPC knowledge and availability. This organization was approached by a compliance officer on behalf of the researcher. This compliance officer noted that they cannot comment or communicate on behalf of all banks on an unfamiliar topic that is still early in research and development.

The individual at Bank D was contacted via LinkedIn and not directly via email which may be the reason for lack of response. The individual may have not seen the message request, forgot to respond, or was not interested or available to partake in an interview. However, this person is or was directly involved in MPC research and projects and has MPC knowledge. Moreover, from informal discussions, Bank D was delaying the joint AML project between Banks A and B for undetermined reasons.

The Bank E interviewee (CTO) was procured via a network partner and therefore, there was indirect communication between the researcher and CTO. It was made aware that this individual did not have technical knowledge of MPC but was willing to answer questions about MPC in a business context. However, the facilitator and point of contact between the researcher and Bank E had issues with finding availability. After a few attempts, this point of contact stopped responding to schedule requests.

## 6.2 Rationale for Interviews

The goal of conducting semi-structured interviews is to validate the uncertainties and initial scenarios with stakeholders in order to develop learning scenario narratives. In literature, there are four recommended criteria in which to judge and develop scenarios for. These criteria are 1) consistency, 2) plausibility, 3) relevance or utility and 4) creativity/novelty (Amer et al., 2013; Schoemaker, 1995; Van Der Heijden, 1996). There is also a possibility that some trends and scenarios or aspects of scenarios may not be plausible in terms of MPC implementation and applications in banks. Therefore, input is needed from different stakeholders to first verify that uncertainties are plausible and relevant to banks and to gain further perspectives about MPC implementation.

### 6.2.1 Conducting Interviews

In any case study research with human research subjects, the researcher needs to act ethically and respect the boundaries of the interview participants (Yin, 2018). Thus, interviews require informed consent from participants about the agreement to the interview conditions, the use of their responses and data in research publishing, and the standards for privacy and confidentiality. Each interview participant was sent an informed consent form prior to the interview date and the form was dictated to the participant before starting the recording of interviews. The consent form also provides a brief summary and description of the research case to inform participants about what information they will be exposed to and the topic of research questions. Furthermore, participants also received information about the research context and study and were able to ask questions about the study when they were contacted and approached for interviews.

Conducting interviews for validation of uncertainties and scenarios requires the researcher to record the responses and maintain a natural, on-going and non-directive conversation with experts (Van Der Heijden, 1996). The research presentation and questions were structured for 30-60 minutes according to the time availability of the respondent. The duration of all interviews within banks were at least 45 minutes and with most culminating to 60 minutes. The interview was structured to chronologically address the most important topics to least important in order to warrant that the objective and criteria for plausibility and relevancy was met and also to ensure that an ongoing conversation was maintained with additional questions. Van Der Heijden (1996) recommends that note taking and recording is important after

conducting interviews and therefore, interviews were transcribed manually in order to maintain a fresh perspective on responses.

### 6.2.2 Interview Questions

The following seven questions outlines the general structure of the interview question list.

1. What judgment can you make about the plausibility and relevance of the uncertainties in MPC implementation?
2. What judgment can you make about the plausibility and relevance of the MPC scenarios for banks?
3. What other aspects of risk management that were not mentioned can be resolved by MPC? You can consider activities outside the scope of credit lending and fraud mitigation/detection.
4. What other opportunities in open banking and payments that were not mentioned can be resolved or enabled by MPC?
5. If you consider new business models enabled by data-driven technologies such as MPC, what are the plausible revenue models that banks should adopt?
6. Given increased competition from fintechs and tech incumbents, how will MPC help banks to manage or improve customer engagement and relationships?
7. Has or will the COVID-19 pandemic affect future banking operations in risk management frameworks? If so, in what capacity and to what extent?

The purpose of **question 1-2** is collect stakeholder input about the plausibility and relevance of uncertainties and initial scenarios **questions 2 and 3**. After stakeholder input is provided, it will allow to develop more accurate scenarios which is one of the deliverables of this study. Since scenarios will revolve around MPC implementation in banks, it may not necessarily answer or show how new business models may arise. Hence, **Question 4-7** aims to understand the value of MPC mechanisms in fraud and payments systems. It is also generally used to establish relevancy for banks in the scenarios which is the third criteria for scenario development. Banks face issues with legacy systems, risk management, compliance and competition which could affect their profitability (European Central Bank, 2018; Srinivas et al., 2019). As a means to understand data-based value activities for enabling new business models, questions with regards to the opportunities and barriers that banks may have in leveraging or monetizing data in fraud management/detection schemes should be included.

Questions 4 and 5 aim to understand stakeholders' perspective with regards to barriers in using data such as legacy systems, organizational structure, lack of data professionals, etc. Questions 6 and 7 is targeting stakeholders' opinions about new business opportunities enabled by data sharing and analytics. Moreover, the payments services market is one of the highest growth segments in financial services (European Central Bank, 2018; Srinivas et al., 2019). Therefore, question 7 aims to gain insights into if and how MPC can be used in other banking competencies besides risk functions and fraud schemes.

**Question 7** aims to identify how the Coronavirus/COVID-19 will impact banks and their risk, security and/or fraud management protocols. The pandemic could potentially change plans for government and banks in the future and therefore, it may affect future scenarios as well. Lastly, questions 4-7 aim to establish novelty and creativity which is the fourth criteria for scenario development chosen in this study. By challenging stakeholders about possible future states based on new technologies or current global events such as COVID-19, it can provide some novelty to scenarios and also challenge preconceived notions and conventional thinking as proposed by the intuitive logics model for scenarios.

Table 6 summarizes the corresponding sub-question, rationale and method for each interview question.

| Interview Question | Research sub-question to be answered | Input or Rationale | Method |
|---|---|---|---|
| 1 | **SQ3**: What are the critical uncertainties of MPC implementation in banking environments? | Uncertainties were derived from PESTLE and trend analyses. See 4.3 Approach to identifying trends and uncertainties | Validate uncertainties with stakeholders; satisfy validation criteria (plausibility, relevance). See 2.2 Scenario Analysis |
| 2 | **SQ3** | Initial scenarios were based on intuitive logics method, uncertainties, and value creation theories *(3.2.3 Value Creation Theories)* | Validate initial scenarios with stakeholders; satisfy validation criteria (plausibility, relevance). |
| 3 | **SQ4**: Which business model components could be affected by MPC implementation and use? | MPC has utility in prevention mechanisms for banks as well as possibly creating value for banks business lines/offerings. This question aims to understand how MPC creates value for banks in relevant risk management functions. | Contextualize scenarios to business model concept to build effective scenarios that are relevant to stakeholders so as to improve effectiveness of final scenarios |
| 4 | **SQ4** | Whereas, this question aims to understand how MPC creates value for banks in payments, the fastest growing market in finance according to trend analysis | |
| 5 | **SQ4** | Understanding other components of MPC enabled data-driven business models. | |
| 6 | **SQ4** | Customer engagement was noted as an essential factor in sustaining competitive advantage in open banking, therefore this question aims to bring insight to how banks should meet or leverage rising customer expectations in their business models. | |
| 7 | Practical question to evaluate plausibility of scenarios | COVID-19 may affect the time horizon, plausibility, and internal consistency of scenarios. | Judgement criteria for scenario analysis method |

*Table 6: Rationale and approach for interview questions.*

### 6.2.3 Interview Presentation and Information Dissemination

The interviews will start with a review of the informed consent form sent to the interviewees prior to the interview. The research objective and purpose and rights for partaking in the interview will be read aloud to the interviewee. Interviewees will be asked if audio recording can start before commencing with Q&A.

A brief explanation of MPC will be explained as well as providing an example for context of use such as Yao's Millionaire Problem. The first question of the interview entails validating MPC uncertainties which will be described as well as shown on a shared screen via Microsoft Teams. Interviewees will be asked to comment on the plausibility and relevance of each uncertainty after each explanation.

Some characteristics or aspects of each uncertainty had slight variations in description and explanation according to the interviewee's role and expertise. For example, aspects regarding the bank's incentives for investing in IT development for MPC use will take precedence while interviewing a security officer as

opposed to details about law and compliance that they may be not so familiar with. The interview process requires these minor adjustments in order to create a conversation that is relevant and useful for both the researcher and the interviewees. This will effectively help carry out scenario analysis objectives in understanding and challenging existing mental models of the firm and create more useful decision scenarios. After discussing the last uncertainty about business models, the dialogue segued into discussing possible outcomes of MPC implementation in the context of open banking and risk/fraud frameworks.

The main six slides show the four elements of the interview presentation which are:

1) Defining MPC and providing an example and MPC application area (slide 1);
2) Explaining the research scope, purpose, and context to the interviewee (slide 2-3);
3) Reviewing uncertainties and validating the plausibility and relevancy of those uncertainties with stakeholders (slides 4-5);
4) Reviewing learning scenarios and validating the plausibility and relevancy of those uncertainties with stakeholders (slide 6).

See Appendix C for presentation slides.

Slide 5 contains definitions of some B2B data sharing business models sourced from Arnaut et al's study on B2B data sharing and re-use in the EEA (2018, p. viii). These definitions were explained to the interviewee in order to evaluate the possibilities of the different types of business models in banks. The actual results of this protocol are reported in the next chapter.

# 7. Results & Analysis

The purpose of this chapter is to present the interview results regarding the validation of initial uncertainties and scenarios as well as responses to MPC enabled business model archetypes. After analyzing interview data, SQ3 (what are the critical uncertainties of MPC implementation) and SQ4 (what business model components can be affected by MPC implementation). This chapter will be used contribute to scenario building in subchapter 7.7. Then the data and results will be analyzed to develop internally consistent scenario outcomes via morphological analysis.

Firstly, the actual research sample is documented (7.1). Secondly, the data analysis approach is outlined (7.2). Thirdly, the coding and data analysis for interviews is described and the results of the concept map are shown (7.3). Fourthly, the uncertainties and scenarios from Chapter 5 are revised according to interview responses whereby analysis was assisted by Atlas.ti (7.4 - 7.5). Afterwards, a general comparative analysis in subchapter 7.6 is conducted to develop more insights from interview data. Lastly, morphological analysis of scenarios is undertaken to develop decision scenarios which are analyzed for plausibility, relevancy, and consistency. To conclude the results and analysis section, SQ3 and SQ4 of this thesis is answered in subchapter 7.8.

## 7.1 Research Sample

There were three sample groups representing three incumbent banks within the EU. These banks were chosen based on availability to collect data and managerial or organizational interest in MPC functions. Table 7 summarizes the units of analysis by organization type and indicates the level of knowledge and understanding of MPC. Knowledge of MPC is indicated by their awareness of MPC and its benefits to enable privacy preserving data sharing and analytics. Understanding of MPC denotes the level of technical understanding of how MPC works and how it can be applied. High is representative of individuals who possess knowledge of MPC because they are involved in researching MPC for their organizations or involved in MPC projects.

| Nr. | Organization Type | Expertise | Selection Rationale | Level of understanding/ awareness of MPC functions | Level of MPC technical knowledge |
|---|---|---|---|---|---|
| **1** | Independent Network Organization | Security & Innovation | Expert security knowledge and network collaborations with organizations in the public and private sector | Low | Low |
| **2** | Bank A | Security | Expert in security and interests in technical solutions for the bank | Low | Medium |
| **3** | | Technical/innovation, management | Technical expert and knowledge of MPC; works in MPC projects | High | High |
| **4** | | Compliance | Expert in compliance, legal and governance issues at the bank | High | Medium |
| **5** | | AI, innovation, monitoring and detection | Technical knowledge of MPC; Researched MPC for 5 years, published paper in MPC research for fraud detection | High | High |
| **6** | | Computer fraud, security | Expert in fraud and security; interests in technical solutions for the bank | Low | Medium |
| **7** | Bank B | Data science, information security | Technical knowledge of MPC; published paper in MPC research for fraud detection | High | High |
| **8** | | Information security, business development | Cryptographic expert and business professional | High | Medium |
| **9** | | Cryptography | Cryptography expert | High | Medium |
| **10** | Bank C | Innovation, digital business | Knowledge of data market and trends; expert knowledge in digital business | Medium | Low |

*Table 7: Description of interviewees by organization.*

## 7.2 Data analysis approach

According to the research approach (Chapter 2), a mixed method approach to data analysis is used to produce a higher qualitative data analysis and to link data to the business model concepts derived in Chapter 3. The data analysis approach for this chapter includes content analysis of interview transcriptions and a general comparative analysis of the banks in the research sample.

Firstly, interviews needed to be transcribed in a manner that abides by the GDPR and ensures the least risk for interview subjects per the signed confidentiality agreements. All interviews were transcribed manually. Cloud storage services and third-party transcription services were not used in order to prevent any data risks and localization rules in the future. Audio recording, playback and transcription was executed locally on a MacBook laptop and via Microsoft Word.

After interviews were transcribed, Atlas.ti coding software was used to facilitate the coding and data analysis process. The purpose of coding and data analysis is to use another method in order to answer SQ4 which was partially answered by semi-structured interviews. Saldaña's (2013) coding manual for qualitative research was used for reference as recommended by Yin (2018) as well as Hsieh & Shannon's (2005) approach to qualitative content analysis. The interview transcriptions were codified using a computer software tool, Atlas.ti, in order to maintain a chain of evidence as recommended by Yin (2018) for qualitative data analysis and establishing reliability.

Secondly, a directed content analysis is a qualitative and deductive analytic approach that aims to extend concepts and theory (Hsieh & Shannon, 2005). This analytic procedure entails the use of predetermined coding categories for initial key concepts and is also referred to as hypothesis coding (Hsieh & Shannon, 2005; Saldaña, 2013). The predetermined codes are scenarios and business model concepts that were initially derived. According to Hsieh & Shannon (2005), any text that cannot be coded into the predetermined categories should be given a new code and any data that cannot be coded will either follow this procedure or be further analyzed to fit into a new category or subcategory of codes (p. 1282). Given that new information was provided in the interviews, exploratory and inductive approaches to coding also included holistic coding, descriptive coding, and In Vivo coding.

The coding scheme is an iterative process that can be executed inductively and deductively. The first cycle of coding entailed holistic coding to review and formulate a comprehensive understanding of the interview data. In Vivo coding also assigned codes that matched key words and terms that interviewees used. These initial codes helped to analyze data that stayed true to the original wording and perceptions of the interviewees so as to minimize researcher bias to some extent about the content of scenarios. Descriptive coding was also used for the purposes of documenting similar responses in the first cycle, for instance mentions about ‘customer perception’.

The second cycle of coding emerged into a mixture of axial coding, pattern coding and hypothesis coding. These methods were used to condense similar codes and categorize codes under scenarios, uncertainties and business model concepts that were formerly derived. Furthermore, these methods attribute to developing the interrelationships between themed data and concepts for logic models (Saldaña, 2013). Therefore, this approach is suitable for carrying out one of the main objectives of scenarios which is to understand the correlations between MPC implementation variables and business model concepts.

Thirdly, the second data analysis approach in this chapter is comparing interview responses between different banks. This second analysis coupled with coding is meant to obtain more in-depth and reliable findings as recommended in qualitative research by Saldaña (2013) and Yin (2018). An extensive cross-case analysis is not possible due to the information asymmetry between banks and due to confidentiality concerns of MPC projects. Therefore, a more general approach to comparing banks and interview responses is chosen. Lastly, memos and notes functions in Atlas.ti were informally used throughout the process to summarize interview responses and keep track of longer excerpts related to SQ3 and SQ4 of this thesis.

Lastly, the coding, categorizing, and documenting of interview responses assists with the analysis of progressing scenarios from intuitively derived to justifiably plausible and relevant. Hence, the final analysis method in this chapter is morphological analysis to counterbalance limitations with research bias and research sample biases in scenario development. Morphological analysis will judge scenarios by the consistency criteria to finally produce the main deliverable of this thesis which are decision scenarios.

## 7.3 Coding & Data Analysis

The first and second iterations of coding resulted in 301 codes. The first cycle was partially conducted manually before transferring the codes to Atlas.ti. The third cycle of coding aimed to combine and categorize codes by similarity in meaning, concepts, and themes. Generally, code groups were predetermined and created for each scenario, each uncertainty and one code group for grouping business model concepts and constructs. This method follows a directed content analysis as mentioned in chapter 2, whereby concepts deducted from theories are used and any new codes or categories will be analyzed and determined in the coding process. For example, two groups for new uncertainties: Uncertainty of 'Customer Acceptance' of MPC and the uncertainty of 'Technological maturity and Computational Capabilities' was added during code analysis iterations.

The process of merging codes involved removing codes that were redundant and marginal as instructed by coding methodologies for qualitative data from Saldaña (2013). Codes that were attributed to 1-2 quotations were first examined to determine their importance relative to other codes with 5-10 quotations assigned. Most of these codes were redundant codes and subsets of a larger meaning in the transcriptions. Redundant codes were merged and/or renamed under a more accurate concept or theme. Codes that were not as significant upon second and third examination were discarded. This process resulted in 110 codes that were distributed amongst 12 code groups and 27 codes unattributed to a group (Appendix E). After manual examination and evaluation of redundant and trivial codes, the 'Find Redundant Codings' tool in Atlas.ti was used to further determine duplicate coding entries. With this tool, redundant quotations assigned to the same code were accounted for. Each duplicate quotation of the code was either merged to one quotation or unlinked.

Network or causation/logic models are used to depict the causal relationships between variables in explanatory research (Saldaña, 2013; Yin, 2018). Although, this study is predominately exploratory, logic models are analytic techniques in qualitative research and scenario analysis used to portray the flow of events, outcomes and theoretically derived events (Saldaña, 2013; Schoemaker & Mavaddat, 2000; Yin, 2018). Concept mapping coincides with multiple facets of the research design as well as improving validity of the research. Therefore, the network groups function in Atlas.ti was used to formulate an initial logic model to represent possible outcomes of business model scenarios in order to gain further insight in determining which business model components could be affected by MPC use by banks. Figure 14 and Figure 15 show business model plausible outcomes for bank and non-bank entities.

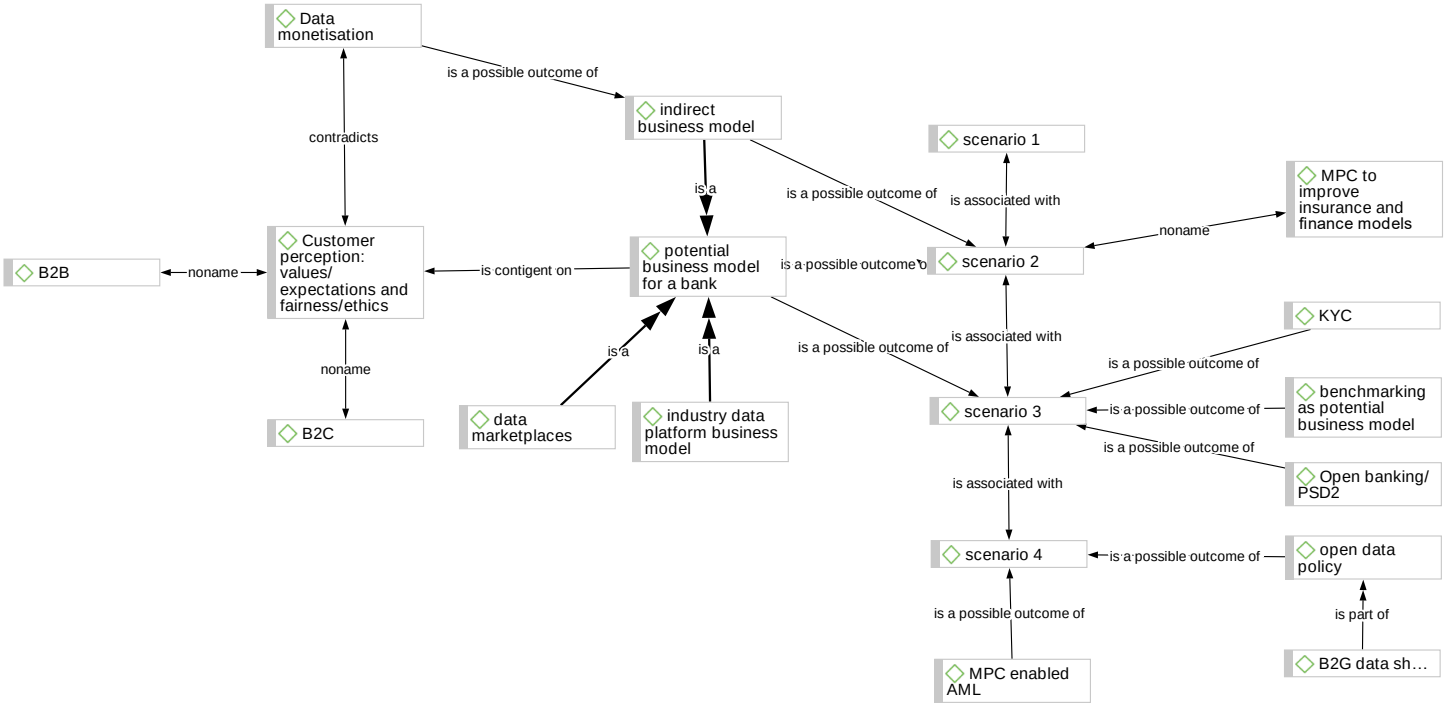



*Figure 14: Concept map for potential business model outcomes in banks.*

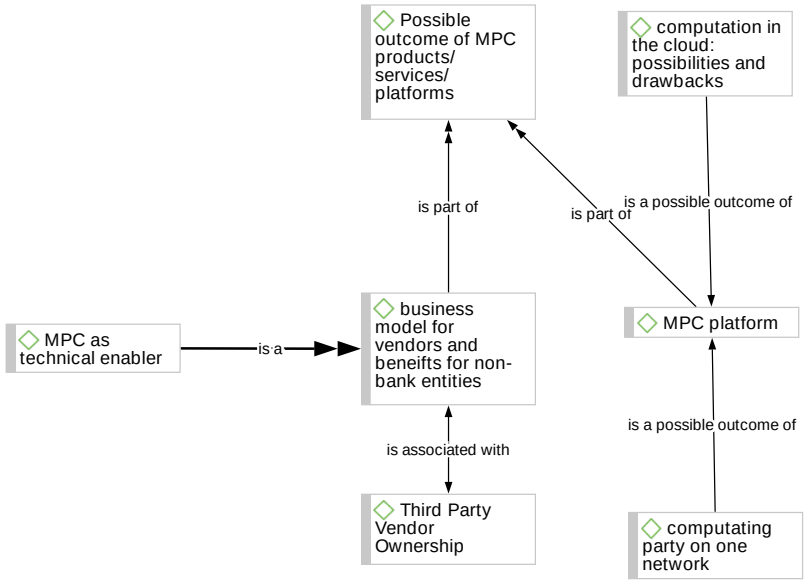



*Figure 15:Concept map for business model outcomes for third party MPC vendors.*

The inclusion of data requirements and use-cases can increase complexity of the interrelationships between possible outcomes of MPC implementation and business models. Although Yin (2018) recommends to include or address contextual conditions to improve the effectiveness of logic models,

every condition would make the map too complex since all business models are use-case dependent. It would generally result in more or less 768 configurations if each possibility were mapped.

These diagrams express the interrelationships and interdependencies of scenarios and potential business model outcomes. On a higher abstract level, it also confirms some of the aforementioned business model components that are affected such as the target customers, new sources of data, and offering. These concept maps also coincide with the scenario archetypes whereby a technical enabler business model is not likely to be adopted by banks, but by third party vendors who may offer an MPC platform or service. In conclusion, coding and data analysis results validated the scenario archetypes that were developed as well as supported that data-driven business model components that would be affected by MPC implementation. Ultimately, it also shows the correlations between business model outcomes and scenarios.

## 7.4 Data Comparison

A cross-case analysis is used in multiple-case studies to determine patterns and differences across each individual case (Yin, 2018, p. 350). This helps determine possible rival explanations that increase the internal validity of the research study (Yin, 2018). Cross-case analysis should critically examine any differences that undermine the findings of this study. This section will mainly distinguish differences and note similarities among the banks by backgrounds and what can be inferred about their thinking logic from their statements. Atlas.ti assisted with this process by grouping documents by each bank and utilizing memos for note taking.

**Organization-specific comparison**

Three banks were the units of analysis in this study which are all considered large commercial banks within their respective countries in the EU. Bank A and Bank B notably have similarities in research efforts and projects concerning MPC for AML and fraud detection. One author from Bank A and B were co-authors for research into MPC enabled fraud detection. Both respondent authors agreed that MPC may be more suitable for AML efforts rather fraud detection which also coincides with fraud security experts. Furthermore, both banks are located in the same country which guarantees that Bank A and B are subject to the same laws, restrictions and jurisdiction of the respective national banking association of that country. Therefore, there are similarities in the approach in abiding by those rules and regulations such as steering clear from business models that sells customer data or using it to provide personalized marketing to their customers.

The greatest differences among the research sample are between Bank A & B and Bank C. Bank C differs by geographical location, investment and research into MPC technology, and jurisdictional differences in that country compared to Bank A & B. Bank A and B are both involved in similar research projects for fraud detection. The national banking association for Bank A and B stimulate the collaboration and sharing of data to collectively work with police and governmental authorities to combat AML and CTF. Therefore, the technological approaches to AML/CTF for Bank A and B are similar. Moreover, interviewees from Bank A and B are connected via MPC projects or AML projects and these interviewees also have similar expertise in security, data science, and cryptography.

**Comparisons of experts**

Money laundering and financial crime is a pervasive risk to all banks in the EU (European Central Bank, 2019b). Bank C only mentioned once in the interviews about the importance of combatting these criminal issues within banks, but the interview was focused predominately on business opportunities rather than

prevention use-cases for fraud or AML. Furthermore, most correspondents from Bank A and B are involved in improving some aspect of security of the bank whereas correspondent from Bank C is focused on digital business and innovation.

Bank A & B interviewees are more knowledgeable in MPC functions and technical aspects whereas, Bank C's interviewee is more knowledgeable in business, market, and data trends of the banking and data ecosystem. Therefore, Bank A and B have more exposure and experience with attempting to use MPC in banks whereas, Bank C has not.

Furthermore, respondent from Bank C requested interview questions prior to the interview taking place which could have introduced some bias in the correspondent's answers to MPC uncertainties, scenarios and business opportunities. However, Bank C confirmed the plausibility and relevancy of trends in the bank ecosystems from Chapter 4 which were not shared beforehand. This suggests that Bank C could have similar logic to Bank A & B since scenarios were abductively derived from the trends, despite receiving questions beforehand.

Another difference in data collection was the group interview conducted with Bank B due to their preference and availability. There were three participants in the group interview but not every participant answered every single question. Therefore, it cannot be speculated whether a particular person did not have an answer, did not want to answer, or (dis)agreed with their colleagues and chose not to speak. Given that some preferred to have their cameras off, verbal confirmation was necessary in order to use the data for analysis. Moreover, sacial expressions and eye contact were sometimes absent which could also introduce interview bias wherein it is not completely certain whether participants were engaged, attentive, multi-tasking etc.

Interview questions also slightly differed between different types of professionals and experts. Therefore, this decreases the internal validity of research findings. Furthermore, casual relationships and explanatory knowledge cannot be established in this study due to selection bias of the interview participants, the inconsistency in interview questions across stakeholders, and the diversity and number of interviewees per bank.

Due to the majority of stakeholder's expertise in security, most suggested MPC use-cases from Bank A and Bank B involved security solutions for fraud, cybersecurity and financial crime. Whereas, a compliance stakeholder stated there was business value in MPC enabled integrity detection such as developing KYC products and services. Hence, it is possible that not all plausible scenarios were evaluated or considered due lack of expertise in other departments of their banks. There could also be bias in only seeing business value in their respective fields.

Furthermore, the comparison table below shows the differences between the participant's backgrounds and degree of knowledge of MPC on a high level and technical level. Most project members in Bank A and B who are involved in MPC projects are experts in security whereas Bank C is an outlier in that regard. Across different banks, there was at least one non-security expert who could provide some diversity in interpretation and opinion. Additionally, Bank A and Bank B have the most knowledge experts and experience with MPC.

| Nr. | Organization Type | Expertise | Awareness of MPC | Understanding of MPC functions | Remarks |
|---|---|---|---|---|---|
| **1** | Independent Network Organization | Security & Innovation | Low | Low | -contributed information and perspective on the social repercussions of emerging security technology<br>-can be used as an unbiased opinion that social perception (e.g. customer perception) greatly affects the implementation decisions of a technology and its acceptance by actors |
| **2** | Bank A | Security | Low | Medium | -answered the greatest number of questions and therefore, interviews were more comprehensive<br>-larger representative sample in research results and findings, suggests bias towards Bank A<br>-only bank to develop legal and governance requirements for MPC<br>-proof of concepts and pilots in MPC with heterogenous organizations<br>-proofing of scalability and MPC over a network of three parties<br>-more diverse sample of respondents<br>-more clear direction of how MPC can be leveraged<br>-fraud experts rejected the use of MPC in fraud detection but have little technical knowledge of MPC |
| **3** | | Technical/innovation, management | High | High | |
| **4** | | Compliance | High | Medium | |
| **5** | | AI, innovation, monitoring and detection | High | High | |
| **6** | | Computer fraud, security | Low | Medium | |
| **7** | Bank B | Data science, information security | High | High | -focused on proofing and developing MPC technology rather than legal and governance mechanisms<br>-all respondents were security professionals which could infer a lack of diversity of MPC project members in the bank |
| **8** | | Information security, business development | High | Medium-high | |
| **9** | | Cryptography | High | Medium-high | |
| **10** | Bank C | Innovation, digital business | Medium | Low | -decision-making is more involved from an EU data and banking ecosystems perspective<br>-confirmed banking trends to be accurate<br>-involved in EU level research projects regarding secure sharing of data |

*Table 8: Comparison of interviewees in this study.*

However, due to some an uneven representation of answers from mostly Bank A, findings in this study can be biased towards Bank A whereby developed scenarios are mentally constructed from mostly one organization. Generalizability be threatened here, but both banks have two experts who have the same expertise and high-level knowledge of MPC and the number of high-level experts from each bank are also similar. This suggests that data collection from Bank A and B might be more accurate and consistent than at first glance. Furthermore, Bank A was clearer and more concise with their statements about how to leverage MPC and what applications areas it had outside of security, fraud and AML. Furthermore, they were heavily focused on legal and governance issues and value sensitive design e.g. compliance by design. This suggests that Bank A experts has developed more knowledge and research with regards to MPC and have an advantage in understanding business cases. Bank B was less concise from an MPC-business perspective whereas Bank C's respondent was less knowledgeable about MPC but had developed ideas on how to utilize MPC in current projects.

In conclusion, based on prior analysis of interview data and the comparison of the banks from a case-based approach, there is evidence of inconsistencies that threaten validity and there is an indication that existing mental models can socially construct future scenarios or reality. The higher degree of knowledge of MPC, the more use-cases and examples will be provided for MPC scenarios. Creativity seems to be a factor in decision-making because fraud experts did not see the utility of MPC to improve fraud detection whereas other professionals within technical innovation at the same bank found ways to use fraud indicators in an MPC proof of concept project. This discrepancy in answers may be a result of industry professionals not being able to see outside of their normal ways of working or due to the lack of knowledge of MPC. Nonetheless, these are variables within the bank and whereas, conclusions should be drawn from comparisons of each case.

Bank B seemed more technology driven in terms of advancing technical advancement due to the lack of knowledge about requirements for MPC legal and governance structures. This could be due to a number of reasons, organizational culture, individual expertise and preference for MPC topics, or unknown reasons that are apparent to the researcher. Bank C contributed more business knowledge and agreed to the correctness of business trends in the banking sector. This is an indication that despite the subjectivity in deriving trends and uncertainties, the scenarios remain plausible and relevant. It also confirmed that respondents are normally less interested and less focused on generic information like trend analysis. Therefore, scenarios need to be really context and organization specific to the interviewee. Lastly, it validates existing scenario methods research that in order to improve decision making, managers and experts need to have knowledge of the context and environment to better adapt to external driving forces and instances of discontinuity (Van Der Heijden, 1996; Wayland, 2019).

An exploratory approach was intended for the research design and thus, research availability, access to internal data and interview participants varied. Information asymmetry across organizations and interview participants and differences across interview questions, participant engagement, interest and communication channels make it difficult to establish any cause and effect relationships between variables and scenario outcomes.

## 7.5 Determining Critical Uncertainties

The purpose of this section is to document the results from formal interviews and informal discussions with industry experts in banking, innovation, security, cryptography, compliance, and fraud. Interview participant answers are supposed to contribute to the confirmation or rejection of uncertainties and initial scenarios. The goal is to formulate critical uncertainties, or confirmed factors that affect MPC implementation in banks, and more accurate scenarios. Consequently, SQ3 can be answered which is, “what are the critical uncertainties of MPC implementation in banking environments?”.

In subchapter 5.1, MPC uncertainties were abductively derived. These uncertainties are discussed and revised according to the interview data hereafter. Each uncertainty is accompanied by a table representing the overview of interview feedback to questions about the plausibility and relevancy of each uncertainty. Atlas.ti assisted with the analysis whereby the responses were coded and categorized by each uncertainty group. A full coding list and coding network reports by uncertainty can be found in Appendices E & F, respectively. The codes and categories assisted with organizing and filtering by uncertainty, common themes, and specific interviewee scripts.

## 1. Legal and Governance Structure

According to expert inputs, the most agreed upon plausible legal and governance structure for MPC implementations are contractual agreements. Interviewees agreed that due to the case specificity of MPC implementations, the application and use-case can have different implications for the legal context and rules of the MPC arrangement. Three interviewees mentioned that it is difficult to create a standardized legal framework or to have regulation of MPC on an EU level due to the contingency of the MPC use-case. Standardization is most likely needed on the technical front where a common understanding of what MPC is, what it can and cannot do, how computations occur would be required for the legal and governance framework. Furthermore, trust mechanisms need to be established where either the technology itself or aspects of the technology such as algorithms can be checked by other parties, audited. It also somehow needs to be proven or assured in the legal framework that data is private, cannot be leaked, and that only functions are being computed on the data but the data in essence is not shared with other parties.

Other plausible but less agreed upon legal and governance frameworks are established or separate legal entity to be the computing party or to make agreed upon rules and actions for MPC collaborations. Moreover, the maturity of MPC and its current understanding is too early to be considered in national or EU level regulations. However, Interviewee 5 who works on compliance issues with new technologies, mentioned that in some circumstances the latter is possible but only to set guidelines for implementing MPC, not rules on MPC implementation itself. Interviewee 5 also notes that with overarching legal and governance frameworks, there has to be absolute certainty of the technology that data cannot be leaked.

Interviewee 4, a compliance officer, discusses that compliance by design is important as well as the use-case in MPC implementations. Within MPC implementations, there are a few compliance and legal risk subjects that were mentioned: data privacy, conflict of interest, party corruption, fraud, market abuse, market misconduct or abuse, sanctions, money laundering, terrorist financing, customer fairness and record keeping. These subjects could be potential points to address in legal and governance frameworks for MPC implementations for at least one unit of analysis. Interviewee 4 also added that the main themes within compliance for MPC applications are customer fairness, data privacy, and record keeping.

An underlying issue with contracts to support MPC arrangements is the notion of 'explainability'. The complexity and communication of how MPC works needs to be discussed from a technical standpoint and to other departmental stakeholders such as those in legal and compliance. Interviewees noted that it is imperative that there is a common or mutual understanding of MPC between all communications regarding MPC implementations and involvement. Interviewee 3 specifically mentions that contracts have a lot of gray areas due to MPC's technological maturity and therefore, MPC technology needs to be standardized as much as possible and explained clearly as much as possible. He/she mentions that one possible solution to improving understanding of MPC, explainability and these grey areas is to have a validated decision tree which allows one to understand the legal and compliance risks for different types of MPC use-cases, problems, and implementations.

The table below is a general overview of the possible outcomes of legal and governance structures or frameworks for MPC implementation according to the interviewee's responses to questions about plausibility and relevancy of uncertainty.

**Y** denotes that the interviewee has affirmed that this particular outcome is possible and relevant, whereas **N** denotes that the interviewee has rejected the plausibility and relevancy of this outcome. Lastly, the diagonal lines represent that the interviewee did not reject or affirm the plausibility and relevancy of the possible outcomes or was not asked due to lack of expertise and knowledge of MPC on the topic.

| Outcomes / Interviewee | Contracts | Overarching legal framework (National) | Standardized legal framework (EU) | Creation of separate legal entity | Use-case specific |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | Y | | | | Y |
| 3 | Y | N | N | | Y |
| 4 | Y | | | Y | Y |
| 5 | Y | Y | Y | Y | Y |
| 6 | N | N | N | N | Y |
| 7 | Y | | N | | |
| 8 | | | | | |
| 9 | Y | | | | |
| 10 | | | | | |

*Table 9: Interview responses (Yes/No/No Answer) to the plausibility and relevancy of uncertainties in legal and governance structure of MPC implementations.*

In short, the usage and processing of data requires legal and governance structures within organizations that own and use personal data. However, there are several layers of legal and governance structure requirements that are necessary in MPC applications. There needs to be a legal framework for the procurement and use of data, both personal and commercial. Customers and clients need to be assured that their personal data is safe and secure with the bank whereas, the privacy of commercial data is most likely essential to protect the bank and their competitive standing.

MPC is an enabling technology that needs to maintain the privacy and security of commercial and customer data. The processing and use of personal data within the EU is regulated by the GDPR and thus, it is certain that banks implementing or using MPC must abide by the GDPR, at minimum. However, input data and output data are more than likely to contain mixed datasets that can become personally identifiable after multiparty computations. The Free Flow Data Directive is meant to coincide with the GDPR concerning the processing of mixed datasets that contain personal and non-personal data (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018). However, this regulatory framework does not require businesses to adopt this framework for non-personal data usage nor does it mention or concede contractual arrangements between organizations that are sharing and computing data (REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, 2018). Therefore, banks implementing MPC have no current legal or governance framework that they must abide by, besides the GDPR for personal data.

There are multiple facets when using mixed data or aggregated datasets which has implications on the technology itself, its use, and if MPC can be implemented by the banks. Legal and governance frameworks are necessary to demarcate what type of data is used; how it is used; to what extent it is procured, processed, and validated; data ownership; and data usage rights. Moreover, there is an uncertainty whether these legal and governance frameworks should be held accountable by the parties themselves or a higher legal entity or authority such as the ECB or a national banking association. Experts note that the most plausible scenario is to implement contracts on an organizational level so that the sensitivity of data can be addressed between all parties, the specificity of the use-case is properly outlined, liability of data is clear, the computations and algorithms are transparent, and there is some form of proof, checks and balances or auditing allowed.

### 2. Technology Ownership

Technology ownership adds more layers to legal and governance matters and uncertainty because there are liability risks, technology failures, and data ownership rights to consider. Technology ownership is also dependent on the degree of trust in the technology, the ability to prove and check that the technology works, assurance and auditing of algorithms, and to a lesser extent the business incentives. According to stakeholder input, MPC technology ownership can be configured or owned in a number of ways: open source, commercial or third-party vendor, by internal bank, external bank, government, trusted organizations, consultancies, or mixed ownership. The main themes and requirements across the board for MPC implementation are complete certainty in the technology itself, ability to review and check the code and algorithms, and technical and social trust.

7 out of 10 respondents agreed that it is plausible that MPC technology can be open source/code and open standard. On the other hand, four interviewees think that MPC technology should be open source compared to other options that were mentioned or discussed. According to expert interviews, open source or code is beneficial because it can be reviewed by everyone; vulnerabilities can be found if any; enables more trust and transparency in the technology; it's more generic and compatible with standardized or open source encryption techniques such as public key generation. On the other hand, some noted the drawbacks to open source, are liability risks if the source or code is wrong, vulnerabilities that appear later which have compliant risks, security risks, and risks to continuity of the process or service.

According to Interviewee 3, there could be a mixed technology ownership scenario with open source wherein a third party can offer and MPC framework and implementations. In order to generate monetary value, this third-party vendor or provider would need to implement business or use-cases, solutions, and consult about these cases. This is observed by the interviewee to be happening with research organizations such as TNO who enable, develop, or consult MPC users about MPC solutions.

Interviewee 5 argues that open source is preferable compared to a third party offering an MPC platform or MPC service in the cloud. Moreover, he/she mentions that the general technology such as encryptions should be generic and open source but the "technology ownership for the task should be by the banks or by the contributors to the platform, the consortium". Although, MPC in the cloud is plausible, it is too early in order to produce or standardize within the near future or in the time span of five years. Furthermore, he/she notes that the vulnerabilities are possible with a cloud solution because there can be a security breach, shortcuts could be implemented for performance improvements, and a lack of transparency. On the other hand, being dependent on a third-party vendor makes It probable that open source is less likely to use generic or open source such as key generation for example.

Stakeholder input from interviewees (1 &6) who are less familiar with MPC, but who are experts in security solutions, advocate for owning the technology as a bank, third-party or trusting the technology itself as with case with bitcoin (Interviewee 6). On the other hand, Interviewee 1 discusses the importance of trust in security solutions. He/she notes that government are big purchasers of private sector security solutions because they don't have the resources to develop solutions themselves. Customer perception plays a role where people may be more likely to trust government owned MPC versus private sector owned MPC technology. There is also a risk in depending on private sector solutions because these companies can be acquired or merged with larger organizations or foreign institutions that lead to different jurisdictions and less transparency of the technological environment. Other technology ownership possibilities are enabling a trusted organization and having it open source. He/she recommends that perhaps, government ownership is preferable over a trusted organization and open source would be the third option.

Interviewee 8 remarked that banks could have it open source or have it as intellectual property that could be sold as a service. Lastly, interviewee 10 does not have the technical expertise to comment on technology ownership, but argued similarly to all interviewees that the technology ownership has to be checked, completely or 100% trusted, and proof that the technology works as expected. The table below is a general overview of the possible outcomes of MPC technology ownership situations according to the interviewee's response to those questions. **Y** denotes that the interviewee has affirmed that this particular outcome is possible, whereas **N** denotes that the interviewee has rejected the plausibility of this outcome. Lastly, the diagonal lines represent that the interviewee did not reject or affirm the plausibility relevancy of the possible outcomes or was not asked due to lack of expertise and knowledge of MPC on the topic.

| outcomes / Interviewee | Open source or open standard | Bank owns the technology | External bank owns the technology | Third party vendor or commercial vendor | Government /authoritative body | Mixed ownership | Trusted organization |
|---|---|---|---|---|---|---|---|
| 1 | Y | | | | Y | | Y |
| 2 | Y | N | N | N | N | | |
| 3 | Y | N | | Y | | Y | |
| 4 | Y | Y | | Y | | | |
| 5 | Y | | | | | | |
| 6 | | Y | Y | Y | | | |
| 7 | | | | Y | | | |
| 8 | Y | Y | | | | | |
| 9 | Y | | | | | | |
| 10 | | | | | | | |

*Table 10: Interview responses (Yes/No/No Answer) to the plausibility and relevancy of uncertainties in MPC technology ownership.*

## 3. Incentives

The incentives for MPC implementation and use vary among stakeholders. Generally, it can depend on the value of data; the type of organizations within the MPC network; use-case such as AML, fraud or cybersecurity; privacy and security of proprietary data; and improved efficiency. Moreover, all interviewees perceived an incentive to implement MPC in some manner. However, one interviewee and

one informal discussion with fraud and security experts and advisors from Bank A, were not convinced that MPC would be useful in fraud detection. The primary reason is the fraud detection and analyses require the decryption of data and therefore, they would need to apply that to MPC outputs as well which conflicts with the GDPR, if they are dealing with personal data.

Furthermore, they mentioned that there has to be in some way to correlate the MPC output back to the fraudster. Eventually, the end goal is to prosecute a fraudster or criminal or be able to explain to a client why their account is being investigated or why there is an issue with transactions. Informal talks with other Bank A employees working with MPC, conclude that MPC outputs cannot be used as legal proof for fraud detection or pinpoint criminals but rather to form a prioritization scheme for fraud investigations of bank clients. Another correspondent from Bank B, similarly mentioned that personal data and account numbers cannot be used or traced to the individual so MPC is more useful in AML use-cases. Within fraud use-cases, the banks already share fraud figures and cybersecurity attacks information with other banks and the supervisory authorities such as the ECB, respective national bank associations. The advantage of MPC in these data sharing situations is that they can do so anonymously without jeopardizing their reputation or power positions. However, three security experts mention that the level of details of information that can be exchanged has implications on how useful and valuable the data is which is not always the case with fraud.

Other common use-cases that were mentioned among interviewees was money laundering detection and cybersecurity threat detection. Interviewee 9 mentioned that improving this process by having better data would help the bank internally and also benefit the bank's customers. Interviewee 9 also mentions that there can be instances wherein data needs to be shared in order to mitigate cybersecurity attacks. He/she states, 'eventually if we find ourselves in a situation where criminals organizations are attacking all banks for instance, then there would be a need for us to share other kinds of data that would not be customer data, maybe it would be technical data or technical logs in our system that we would not be comfortable sacrificing our confidentiality in order to share that data'.

Other incentives mentioned were about efficiency. Banks are required to share AML or fraud information to supervisory entities and authorities but according to interview feedback, this requires a trusted third party and sharing all or complete set of data and transactions. Interviewee 4 and 2, mention that this presents a risk to the security and privacy of data with a trusted third party. However, interviewee 2 and other security experts want to be able to share personal details like names and account numbers to improve fraud detection. Whereas, interviewee 4 prefers to have a higher number of parties join so that it requires less data input and more private for the bank itself. Moreover, there is also more efficiency and incentive for banks to use MPC as a means to circumvent a highly regulated environment by proving that they're "not using any external data or transporting any specific use of the data but still use it". Interviewee 4 also mentions the benefit of benchmarking use-cases among other banks and perhaps, with performance or sales information according to Interviewee 2.

| outcomes / Interviewee | Interbank data sharing | Inter-organizational data sharing (incumbents) | Collaboration with third parties/fintech/ SME | B2G data sharing | Forego the need for trusted third party/entity/ gov | Data related | Privacy | Use-case dependent | Efficiency |
|---|---|---|---|---|---|---|---|---|---|
| 1 | | Y | | | N | Y | | Y | Y |
| 2 | Y | | | | Y | | | Y | |
| 3 | Y | Y | | | | Y | | Y | |
| 4 | | | | | | Y | Y | | Y |
| 5 | Y | | Y | | | Y | Y | Y | |
| 6 | | | | | | N | | | Y |
| 7 | Y | | | Y | | | | | |
| 8 | | | | | | | | | Y |
| 9 | Y | | | | | | | | |
| 10 | Y | Y | | Y | | | | | |

*Table 11: Summary of Interview responses (Yes/No/No Answer) to the plausibility and relevancy of uncertainties in MPC implementation incentives.*

To summarize, it is plausible to use MPC to gain access to external data from other banks or other big organizations to be used in products, internal functions, or for AML and fraud. Some barriers to MPC implementation are that all data must be stored in the format to be used in MPC or complying with the GDPR. It also provides opportunities to gain insight for benchmarking or performance, cybersecurity threats across banks without being directly linked to this data that could hurt the reputation of the bank. Stakeholder input also mentioned that incentives can vary and also conflict between different type of organizations. The perception of the public and customers have an influence on collaboration incentives because they might not trust the government with their data as opposed to private companies and vice versa.

## 4. Data Requirements

There are ambiguities with the technical aspects of data requirements such as the format and reliability of data since all parties have to procure their data for MPC. However, these technical requirements are less relevant to stakeholders. The type of data or meaning of data that is required or metadata is a factor in how MPC will derive or create value for banks. It can be assumed that accuracy and reliability of data is assumed by all honest parties who use MPC, otherwise the output of data would not be valuable/useful or correct. There are technical, legal, governance, and compliance issues to consider for data that were mentioned in all interviews. However, this uncertainty revolves around the scope of understanding how or what type of data creates value within MPC applications in banks.

As shown in the table below of responses to data requirements uncertainties, most interviewees work in or know of use-cases in fraud, AML, and threat detection as well as benchmarking and customer related data. As mentioned in the 'incentives' sections above, within fraud detection use cases, it is not as useful

to security advisors in Bank A because they want to be able to use encrypted data without decrypting it. Decryption is required to detect or convict criminals or fraudsters but MPC use in this context would have issues with customer fairness and compliance with GDPR. The metadata or meaning of data is important to consider as well as how it is defined. According to interviewee 3, performance margins can be useful to determine via MPC but all banks have different definitions of their performance margins so new metadata has to be created in order to derive value from the MPC outputs.

In contrast to most answers related to use-cases in combatting financial crime, interviewee 10 mentions example use cases in which MPC enables data sharing between banks and telecom companies in order to provide better products and services to their customers. It was mentioned in interviews and informal talks about the strict regulations of the ECB and national banking associations regarding use or selling of customer data. Generally, customer data should not be used by banks or shared with other organizations to provide special advertising for products and services to their customers. Therefore, interviewee 10 mentions that creating profile trends from aggregated data from different industries might be possible in the future in order to avoid this issue. Another example of monetizing data is to share anonymized customer data to telecom companies wherein e-banking can facilitate transactions for customers uploading more data or minutes into their phones.

| outcomes / Interviewee | Personal data | Fraud related data | Performance indicators | Threat/security related data | AML/CTF | Product or customer related data |
|---|---|---|---|---|---|---|
| 1 | | | | Y | | |
| 2 | Y | Y | Y | | Y | |
| 3 | | Y | Y | Y | Y | |
| 4 | N | Y | | | Y | |
| 5 | | Y | | | Y | |
| 6 | Y | N | | | | |
| 7 | | Y | | | Y | |
| 8 | | | | Y | | |
| 9 | | | | Y | | |
| 10 | | Y | | | Y | Y |

*Table 12: Summary of interview responses (Yes/No/No Answer) to the plausibility and relevancy of MPC implementation data type requirements.*

## 5. Business Models

Interviewees were asked about the plausibility and relevancy of uncertainties concerning business models. Definitions of B2B data sharing models were sourced from Arnaut et al's study on B2B data sharing and re-use in the EEA (2018, p. viii) and reviewed with 4 interviewees. Interviewees 1, 2, 6, 7-9 were not shown these definitions due to either lack of time in the interview; it was irrelevant to ask according to interviewee's expertise or interest; or they declined to answer. Others were also asked about business models outside of the scope of these definitions in terms of example use-cases and in general bank contexts in fraud detection, AML, compliance and risk monitoring, open banking/PSD2 and payments.

| Possible outcomes / Interviewee | Data monetization (DaaS, AaaS) | Data marketplace | Industry data platforms | Technical enabler | Open data policy | B2C |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | Y |
| 3 | Y; indirectly | Y; indirectly | Y | N | Y; indirectly | |
| 4 | N | N | N | Y | N; due to current regulatory environment | |
| 5 | N for B2B, Y for B2C | Y | Y; but strict parameters | Y | N; not necessary with MPC | Y |
| 6 | | | | | | |
| 7 | | | | | | |
| 8 | | | | | | |
| 9 | | | | | | |
| 10 | N for DaaS<br>Y for AaaS | N | Maybe | N | N | Y |

*Table 13: Overview of interview responses (Yes/No/No Answer) to the plausibility and relevancy of MPC enabled business models.*

Most of the responses denied the adoption of DaaS business model because it is too risky to sell customer data. This is prohibited by the ECB and in most cases and discouraged by customers themselves. However, analytics as a service (AaaS) that does not directly include personally identifiable information can constitute as a plausible business model. Although, some stakeholders are still cautious about this model due to negative response from the public. Generally, data marketplaces, industry data platforms, technical enabler and open data policy are plausible business models but it depends on the use-case, information that is to be shared, and rules and guidelines in place to ensure customer data is secure or not being sold.

Otherwise, responses for other business models varied because most interviewees conceptualized and explained business models through business case examples. A summary of specific examples of use-cases can be found in Appendix I. Interviewees also had remarks to the plausibility of business models depending on MPC computational capability, customer perception, the level of detail of the data that can be shared, regulation and the extent of privacy and security in transactions. Despite the enabling properties of MPC, interviewees judgement of appropriate business models seemed to be clouded or affected by regulation, customer perception of data use by banks, and the security of data.

However, of the responses received, indirect MPC business models seemed to be more likely supported by stakeholders. MPC is more useful to protect the bank's private data in data sharing situations than for sharing customer and transaction data. Moreover, it is difficult for stakeholders to foresee new business opportunities with MPC's current technological maturity since experts need to be aware of the exact capabilities of MPC to avoid liabilities and risks that are inherent in technological implementation. Additionally, interviewees need technical and legal assurance about the security of their data before pursuing business opportunities with MPC. Furthermore, the data outputs need to be on a somewhat high-level such as analytics so as to avoid strict data regulations.

### 7.5.1 Summary

Table 14 below summarizes the plausible and relevant outcomes of the critical uncertainties. Each outcome in this table was verified, at the very least, by one stakeholder in a bank. These outcomes will be reanalyzed for consistency which is the third judgment criteria for scenarios in later sections. The rationale and decisions for the table values are discussed hereafter.

| **Legal & Governance Structure** | **Technology Ownership** | **Incentives** | **Metadata Requirements** | **Business Models** | **Customer Perception** | **Tech Development** |
|---|---|---|---|---|---|---|
| Contractual arrangements | Open Source | Interbank collab | Personal data | Data monetization for AaaS | Customer disapproves of MPC | ~~Scalable (user preference rather than requirement)~~ |
| Standardized | Banks | Collab with big organizations | Fraud related data | ~~Data monetization for DaaS (not plausible)~~ | Customer approves of MPC | Secure/private Data analytics |
| ~~Creation of Separate legal entity (not relevant)~~ | Third party provider/vendor | Collaborations with smaller companies | Performance indicators | Data marketplaces | Customer cannot validate MPC | ~~Cryptographic protocol (user preference rather than requirement)~~ |
| Use-case specific | Gov/supervisory | B2G data sharing | Threat/cybersecurity data | Industry data platforms | | ~~Fast (user preference rather than requirement)~~ |
| | Mixed ownership | Don't want a trusted third party | AML/CTF related data | Technical enabler | | ~~Computational algorithm (user preference rather than requirement)~~ |
| | Trusted organization | Access to external data | Product or customer data | Open Data policy | | |
| | | Privacy | | B2C | | |
| | | Use-case dependent | | | | |
| | | Efficiency | | | | |

*Table 14: Summary of all critical uncertainties and plausible and relevant outcomes. Decision rationale for crossed out values are highlighted in red.*

In order to use these results to develop scenario narratives or decision-based scenarios, the plausibility and relevancy of each value must be considered again before moving forward with scenario development. Scenarios in this study is based on four judgment criteria: plausibility, relevancy, consistency and novelty. These criteria were previously defined in the methods chapter for the scenario analysis method. The purpose of scenarios analysis is to not find the most likely future scenarios but rather, to determine the possible future outcomes as a learning and decision making tool within organizations (Schoemaker, 1995; Schoemaker & Mavaddat, 2000). Therefore, not all values for each uncertainty were ruled out by probability of occurring.

Based on stakeholder input, it was made clear that **data monetization of customer data or sharing customer data as a service (DaaS) will be prohibited by law**. Hence, DaaS is implausible and ruled out. Additionally, MPC enabled fraud detection and analysis can only be viable on a high or abstract level such as analytics of fraud indicators and scores. In cannot be used for fraud analysis, legal proof or explainability for customers who are being investigated, and it does not help police authorities or banks to convict or single out individual criminals for prosecution. Moreover, **the creation of a legal separate identity to share data *does not* meet the criteria of relevancy** to stakeholders because the purpose is to understand different types of MPC implementation scenarios for data sharing; both conditions should not coexist within the scenarios. Furthermore, use-case dependent or contingent incentives were added as a possible outcome. Use-cases were important in identifying potential application areas and possible future outcomes because MPC can only be leveraged and create value in a specific context. It depends on the type of data being shared, how reliable and secure the algorithms are, the liability and risks in data and security, and knowing what can be achieved with MPC.

Two interviewees mention that customer perception and technological requirements are important uncertainties or factors to add to the list. Customer perception was added to the matrix based on the underlying importance of bank reputation, regulation, and customer preferences for new banking services and innovation. There was a past incident with a few major Dutch banks who had planned an innovative solution to use customer data to provide them with more accurate service and product offerings/advertising. Due to customer opinion on personal data privacy, the NVB (Dutch banking Association) placed strict rules to prevent any bank from selling their customer data or using it to provide personal advertising. This incident shows that customer opinion matters greatly in new innovations and business models used by the banks. However, customers will not be able to validate whether MPC is protecting their data and therefore, this should not be the only factor in implementing MPC.

Technological development uncertainties are an important uncertainty to consider because the algorithmic and computational capabilities have an implication on the application and utility for banks. Stakeholder opinions throughout interviews care more about how reliable MPC is, if it can be trusted, how secure it is, and can it do the computations that they need or what it promises. However, some technological uncertainties were not added to the matrix such as technical reliability, secure and trusted technology. If MPC was not reliable, secure, trustworthy then banks would not implement MPC and therefore, these values should be already assumed and disregarded from the matrix.

There are a range of potential MPC computations in data mining, data query, data analysis as well as a range of cryptographic methods. The end goal of MPC outputs is to extrapolate meaning from shared data in the form of secure and privacy preserving data analytics which will inputted into the matrix. There are multiple encryption and cryptography schemes that can be used for MPC functions and analytics, so these use-case and stakeholder specific preferences will not be included in the matrix. However, technological development uncertainties need to at least be able to provide function output or analytics on the data in some form.

Scalability is also a technical uncertainty but it is more of a preference rather than requirement. It is also dependent on the use-case and how often the MPC parties plan to run computations. For instance, some problems require many parties within the computation in order to derive a valuable output. How fast the technology may not a major concern with stakeholders because MPC is an enabler to make a data sharing process easier, not faster. Furthermore, Bank A made a proof of concept and tested the scalability of MPC between three or more parties. They have established that the speed of computations with multiple parties is already faster than trying to get the same data analytics output manually or via current

processes. Therefore, technical scalability is not as relevant because it can be assumed that if MPC cannot handle computing functions on data from multiple parties then the technology would not be useful or relevant for banks. Scalability in terms of how many parties are able to use and implement MPC themselves or adopt an MPC platform is more significant.

The next section will re-evaluate the conditions and values for each uncertainty in subsequent sections for consistency. These conditions will then be used as input for learning scenarios that were also validated by stakeholders.

## 7.6 Interview feedback for learning scenarios

Interviewees were asked to comment or provide their opinion on the plausibility and relevancy of the four learning initial scenarios described in subchapter 5.2. The responses were coded and categorized by scenario; a full coding list and scenario network reports can be found in Appendices E & G respectively. These reports list the codes and code groups (scenario 1-4). The coding was used to keep track of responses related to the four scenarios in each transcription document. In order to revise scenarios, these codes and interviewee groups were referred to and used as a search and filter function to re-read and re-evaluate interviewee responses. Responses were also tallied in Table 15 below which represents a simplified overview of these responses.

| Scenario / Interviewee | 1. Improving Processes and Operations | 2. Enhancing existing products and services, technologies | 3. enabling new products and services | 4. Assisting Supervisor and Government Authorities | Comments |
|---|---|---|---|---|---|
| 1 | | | | | |
| 2 | Y | Y | Y | Y | |
| 3 | Y | Y | Y | Y | |
| 4 | Y; fully agree and can start right away | Y; maybe not within 5 years | Y; but for benchmarking | Y | |
| 5 | Y; interbank level | Y for AML but expensive | Y; but with blockchain or use case for sharing personal data | Y | Inter-bank data sharing is most relevant |
| 6 | Y; but N for fraud detection and credit and risk monitoring | N | N | N | |
| 7 | Y | N | Y | Y; but not the most relevant | |
| 8 | Y | Y | Y | Y | |
| 9 | Y; fraud detection has most value for banks | | | Y | |
| 10 | Y | N | Y | Y | |

*Table 15: Summary of interview responses to plausibility and relevancy of MPC implementation scenarios.*

### Scenario 1: MPC improves processes and operations

All stakeholders expressed that improving current processes and operations for fraud detection, cybersecurity threat detection, and credit and risk monitoring are plausible, relevant and most feasible among the four scenarios. There was an important distinction from both banks that MPC can improve better fraud detection by having aggregate data from other banks and improving products for their customers. However, fraud detection via MPC can only improve the prevention and modus operandi of

fraud detection rather than the full scope of fraud detection analysis and prosecution of criminals. The computational outputs can be personally identifiable if the algorithm aims to extrapolate data points from the shared data in that manner. However, in order to abide by the GDPR, MPC enabled fraud detection should have computational outputs that cannot be correlated back to the identified potential criminal or fraudster. This conflicts with security protocols in banks because banks are required to report financial crime related incidents to the prosecution authorities and financial intelligence units with the end goal of enforcing law on criminals/fraudsters (European Commission, 2019a). Hence, banks can only use MPC in fraud detection with computational outputs containing higher or abstract levels of data such as calculating risk profiles, tends, or data analytics on the data.

MPC enabled preserving data analytics in fraud detection decreases the utility for security departments in banks who need to administer fraud analysis on their customers as well as the overall value chain of fraud detection. Privacy preserving analytics can results in more accurate fraud indicators, risk scores, and even facilitate creating a class system of customers based on the likelihood to commit fraud. This works in the interest of compliance for banks because they can prevent fraud with using less internal data and more external data from other banks. Furthermore, sharing data without revealing personally identifiable information benefits the banks' customers and their rights to data privacy.

### Scenario 2: Enhances existing products, services, and technologies

Both AI experts that were interviewed did not see the plausibility or relevancy of MPC aiding or enhancing technologies such as AI or ML. However, MPC coupled with AI/ML could be feasible. Interviewee 4 sees the plausibility and relevancy of MPC solutions and products but the explainability of MPC to the public needs to happen before MPC based solutions can be implemented by the banks. Interviewee 5 also comments that MPC to enhance data aggregation and privacy preserving data analytics for technology in AML contexts could be done, but it is not necessary to use MPC and it would require too many resources and computing power to do this via MPC. Moreover, personal data should not be used in AI (it is unnecessary) but to leverage MPC on an inter-bank level, personal data needs to be shared. About five interviewees work directly in a security function for the bank so feedback was generally focused on security solutions or their expertise rather than products in other functions of the bank such as marketing or lending.

On the other hand, MPC would be more useful in financing and insurance because these business lines can derive value from having different types of data from multiple parties as input for calculating better risk scores or interest rates for customers. Using MPC to enhance or contribute in a bank's offering introduces an uncertainty of customer perception of MPC and the ability of banks to explain how MPC works. Technically, customer data is safeguarded or not revealed within the computation which allows banks to abide by and circumvent strict data regulations. With MPC, the benefits for the bank is to use less internal data and access external data.

### Scenario 3: Enables new products/services

Interviewee 3 rejected the idea that MPC could be directly applicable in the payments sector. However, an alternative in the payments market that would be a potential business case is to incorporate KYC into the payment products or services to verify or validate the customer before the transaction occurs. Currently, some companies do this with a centralized database to run the checks and verifications. However, the caveats are that it requires extreme regulation and MPC would need to be fast enough in order to facilitate that. Interviewee 6 also agrees that a nice application would be to find a way to share

data with a third party who has a different product or service than that of the bank and provide a KYC validation service to them.

Interviewee 4 remarks that this option may be beyond the scope of five years like scenario 2. However, using MPC for benchmarking services might benefit companies to know where they stand on a certain criteria or performance indicator. They could share their data privately and receive output on how their company is performing. Interviewee 5 mentions that using MPC in combination with other technologies makes it a difficult business case wherein the use-case should be looked at first such as sharing private data in areas that cannot be shared. In open banking, the combination of MPC and blockchain might be an application area whereby data needs to remain private.

### Scenario 4: Assists government and supervisory authorities

This scenario is the most plausible since it is stimulated by some banking associations. Within the Netherlands, major Dutch banks have joined an AML project that researches the utility of MPC in combatting financial and terrorist crime. Interviewees from Bank B, agreed that the fourth scenario is the most concrete and plausible but not necessarily the most relevant because by law, banks have to share data for combatting money laundering and counter terrorist financing. However, better fraud detection has a direct financial benefit if they can provide better products and gives the bank more of an advantage in this context.

## 7.7 Data Analysis for Scenarios

This chapter aims to analyze scenarios based on the criteria of internally consistent scenarios. After scenarios are analyzed for consistency, intuitively derived scenarios can evolve towards more accurate scenarios. These final scenarios would then be useful for decision making in banks and thus, resulting in decision-based scenarios that can be used for strategy and planning in banks.

### 7.7.1 Morphological Analysis

General Morphological Analysis (GMA) is suited for complex and exploratory problems within a range of environments such as those in an organization (Tom Ritchey, 2015). The GMA is a non-linear and iterative process for problems that have a range of possible outcomes with non-linear relationships (Johansen, 2018; Tom Ritchey, 2015). The GMA is not meant for explanatory purposes or establishing causal relationships between variables because scenarios are created for systems governed or subject to human behavior (Johansen, 2018, p. 117). Therefore, this method to assess the consistency of scenarios is suitable to address the critical uncertainties and scenarios for exploratory research in plausible MPC implementation outcomes.

The table below is described as a morphological field which demarcates the entire problem field according to Johansen's (2018) method for morphological analysis in scenario modelling. Each possible state for each uncertainty (columns) should be mutually exclusive (Eriksson & Ritchey, 2002). Those that are eliminated according to this rule will be indicated by a diagonal line in Table 16. For instance, **use-case specificity** should apply to all legal and governance structures and frameworks and it is more of a criterion rather than regulatory framework. Therefore, it is inconsistent with the other values within the column. The decision rationale for mutually exclusive values are explained sequentially, according to the column order in Table 16.

**Legal and Governance:** Contractual arrangements and standardized EU legal framework can coexist. Given that contractual arrangements are more plausible in regulatory environment such as banking and that developing an EU regulatory framework for MPC is highly improbable within the next five years (technological maturity is too early), standardized legal framework can be eliminated.

**Technology Ownership**: Aspects of open source can apply to algorithms and encryption schemes which can coincide with any MPC framework that a company or organization owns. Therefore, it must be defined as entirely open source. Moreover, mixed ownership in itself is not mutually exclusive and can be eliminated. Also, having a trusted organization to only own MPC technology is also not likely.

**Implementation Incentives:** Theoretically, different type of collaborations with homogeneous and heterogeneous organizations can occur within one MPC use-case and therefore, four types of interorganizational data sharing incentives will be condensed under the umbrella term ‘interorganizational data sharing’. Within the same vein, by definition, MPC enabled privacy, access to external data, and foregoing a trusted third party is not mutually exclusive from MPC enabled data sharing. Also, it can be assumed that MPC will maintain the privacy of data.

**Data Requirements:** It is assumed that MPC will contain mixed datasets configured of personal and non-personal or commercial data such as transaction data for fraud detection. Thus, personal data can be eliminated from the field. Customer data is also in the same category and can be deleted.

**Business Models:** In theory, banks can adopt multiple business models but the type of business model for a specific use-case are mutually exclusive.

**Customer perception:** If customers disapprove of MPC and any other product or service related to a bank's implementation of MPC, then that garners the technology irrelevant to banks. Hence, banks will not implement MPC which makes the outcome or scenario irrelevant to banks and contradictory to the utility/relevancy judgement criteria for banks. Furthermore, customer approval and disapproval are not mutually exclusive. Therefore, it is only relevant and internally consist to accept scenarios wherein customers approve of MPC.

| | **Legal & Governance Structure** | **Technology Ownership** | **Implementation Incentives** | **Data Type Requirements** | **Business Models** | **Customer Perception** | **Tech Capability** |
|---|---|---|---|---|---|---|---|
| 1 | Contractual arrangements | Open Source | Interbank collaboration | Personal data | Data monetization (AaaS) | Customer disapproves of MPC | Secure/private Data analytics |
| 2 | Standardized EU legal framework | Banks | Collaborations with big organizations | Fraud related data | Data marketplaces | Customer approves of MPC | |
| 3 | Creation of Separate legal entity to share data | Third party provider/vendor | Collaborations with smaller companies | Performance indicators | Industry data platforms | Customer cannot validate MPC | |
| 4 | Use-case specific | Gov/supervisory authorities | B2G data sharing | Threat/cybersecurity data | Technical enabler | | |
| 5 | | Mixed ownership | Don't want a trusted third party for data sharing | AML/CTF related data | Open Data policy | | |
| 6 | | Trusted organization | Access to external data | Product or customer data | B2C | | |
| 7 | | | Privacy e.g. secret bidding | | | | |
| 8 | | | Algorithmic capability/use-case dependent | | | | |
| 9 | | | Efficiency/improvement in data sharing process; circumvent strict data regulations | | | | |
| 10 | | | Interorganizational collaboration via MPC (external data) | | | | |

*Table 16: Morphological box or field of the problem space (constructions of all possible solutions).*

This morphological field now represents 768 possible configurations (1 x 4 x 4 x 4 x 6 x 2 x 1 = 768) as indicated by the GMA method.

Afterwards, each condition or option in each column is compared to each option in the adjacent columns according to Eriksson & Ritchey's (2002) method for non-quantified morphological analysis. A solution space must be created by eliminating impossible or inconsistent solutions via a cross consistency matrix (Eriksson & Ritchey, 2002; Johansen, 2018; T. Ritchey, 2006; Tom Ritchey, 2015). Internal consistency will be analyzed via a cross-consistency analysis to determine the critical uncertainties in order to answer SQ3. Values or possible states will be compared pair-wise in order to eliminate unlikely pairs. According to Johansen's (2018) method , consistency is assessed on two criteria:

- **logical consistency**, or "the internal relationships of the concepts involved cannot be mutually contradictory" and

- **empirical consistency** or "solution cannot rest on empirically impossible or highly improbable assumptions" (Johansen, 2018, p. 118).

For example, if banks use an open source model, then they cannot have a data monetization business model whereby algorithms or analytics are sold as a service. This is a logical inconsistency demarcated by a red X in Figure 16 below and coincides with the first row in Table 17 which is also highlighted red. The inconsistency rationale for each pair is listed in Table 17. Consequently, the unlikely pairs or solutions will be marked in the cross-impact matrix below (Figure 16).

| Condition | Condition | Inconsistency | Remarks |
|---|---|---|---|
| Open source | Algorithms as a Service business model | Logical | Open source algorithms cannot be monetized as a service but how it is used can be proprietary. |
| 1. Contractual Arrangements | B2C business model | Logical | Customer data will be governed by GDPR |
| 1. Contractual arrangements | Customer approves of MPC | Logical | Customer data will be governed by GDPR |
| 1. Contractual arrangements | Data monetization (AaaS) | Empirical | Improbable that banks adopt a data monetization model that uses data from other parties unless there is shared ownership of revenues. The latter would be more representative of industry data platform. |
| 1. Contractual arrangements | Open data policy | Empirical | Contractual arrangements between parties is unlikely in the scenario that government requires banks to freely provide their data. Furthermore, freely supplying data would threaten competitive advantage. |
| 3. Customer cannot validate MPC | Secure privacy preserving analytics | Empirical | It is unlikely that if the customer cannot validate or understand the value of MPC in safeguarding their data then banks most likely will not use MPC (high investment and legal overhead). |
| 3. Customer cannot validate MPC | All | Empirical | Technology ownership will most likely not be fully transparent to customers and there is no way for them to entirely validate it. |
| 4. Privacy preserving data analytics | Technical enabler business model | Logical | Offering technical solutions for data sharing is inconsistent with the end goal of supplying privacy preserving data analytics |
| 8. Tech owned by government | All business models except for open data policy and data marketplaces | Empirical | Banks will be required by government to release their data which will unlikely be used for monetization in a business model |
| 8. Tech owned by government | All business and implementation incentives | Logical | Banks will be required by government for social/public interest rather than for business/functional opportunities |
| 8. Tech owned by government | Performance indicators | Empirical | Investment into MPC platforms and security solutions are improbable for determining performance indicators between banks/organizations |
| 11. Efficiency | Business Models | Empirical | Efficiency in data sharing will most likely be used to share data between or |
| 11. Efficiency | Performance indicators | Empirical | It is less probable that the incentive for companies to benchmark their performance indicators is due to wanting a more efficient process for data sharing such as in the AML cases. |
| 14. Performance indicators | Data monetization, technical enabler | Empirical/logical | Performance indicators will most likely be shared to improve internal efficiency of the |

| | | | |
|---|---|---|---|
| | | | banks themselves or offer a benchmarking service of some sort. Improbable or unlikely to use performance indicators for other business models. |
| 15. cybersecurity data | Data marketplaces | Empirical | Exchanging security information for revenue is prohibited because it can lead to cartel forming and banks are not allowed to compete on security in some EU countries (e.g. NL) |
| 16. AML/CTF related data | Business Models | Logical | Sharing this type of data is more relevant and consistent for public and social interests rather data monetization |
| 16. AML/CTF related data | Incentives | Logical | Sharing this type of data is more relevant and consistent for public and social interests rather than for data driven business models |
| 16. AML/CTF related data | Customer perception (disapproval and validation) | Logical | AML/CTF use-cases are typically required and governed by authorities/law rather than customers of the bank. Customers have less input and opinion on these concerted efforts by banks/gov. |
| 17. Data Monetization business model (Analytics and/or Algorithms as a service) | Efficiency | Logical | To sell analytics or algorithms as a service, there is a higher value in the data itself than the efficiency of procuring data from different parties. It Is probably more inefficient and costlier to facilitate via MPC |
| 20. Technical enabler | Open source | Empirical/logical | It is not likely that MPC technology will be entirely open source if a bank plans to use a technical enabler business model (difficult to monetize/create value). |
| 20. Technical enabler | Types of data | Logical | Selling data sharing solutions is more focused on the technical requirements rather than data requirements |
| 22. B2C | AML/CTF | Empirical/logical | Unlikely to adopt B2C business model if the main purpose is to combat financial crime |
| 22. B2C | Efficiency | Logical | Out of the four business incentives, exchanging data for B2C business models requires differentiation potential of the data rather than for efficiency in the process of sharing data |

*Table 17: Pair-wise comparison and justification of inconsistent value pairs for uncertainties.*

| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1. | Contractual Arrangements | | | | | | | | | | | | | | | | | | | | | | |
| 2. | Customer approves of MPC | X | | | | | | | | | | | | | | | | | | | | | |
| 3. | Customer cannot validate MPC | | | | | | | | | | | | | | | | | | | | | | |
| 4. | Secure & privacy preserving analytics | | | X | | | | | | | | | | | | | | | | | | | |
| 5. | Open Source | | | X | | | | | | | | | | | | | | | | | | | |
| 6. | Banks | | | X | | | | | | | | | | | | | | | | | | | |
| 7. | Third party provider/vendor | | | X | | | | | | | | | | | | | | | | | | | |
| 8. | Gov/supervisory | | | X | | | | | | | | | | | | | | | | | | | |
| 9. | Privacy e.g. secret voting/sharing | | | X | | | | | X | | | | | | | | | | | | | | |
| 10. | Algorithmic capability/ Use-case dependent | | | X | | | | | X | | | | | | | | | | | | | | |
| 11. | Efficiency in data sharing process | | | X | | | | | X | | | | | | | | | | | | | | |
| 12. | Interorganizational collaboration via MPC | | | X | | | | | X | | | | | | | | | | | | | | |
| 13. | Fraud related data | | | X | | | | | | | | | | | | | | | | | | | |
| 14. | Performance indicators | | | X | | | | | X | | X | | | | | | | | | | | | |
| 15. | Threat/cybersecurity data | | | X | | | | | | | | | | | | | | | | | | | |
| 16. | AML/CTF related data | | | X | | | | | | X | X | X | X | | | | | | | | | | |
| 17. | Data monetization (AaaS) | X | | X | | X | | | X | X | | X | | | X | | X | | | | | | |
| 18. | Data marketplaces | | | X | | | | | | | | | | | | X | X | | | | | | |
| 19. | Industry data platforms | | | X | | | | | X | | | | | | | | X | | | | | | |
| 20. | Technical enabler | | | X | X | X | X | | X | | | | | X | X | X | X | | | | | | |
| 21. | Open Data policy | X | | X | | | | | | | | | | | | | | | | | | | |
| 22. | B2C | X | | X | | | | | X | | | X | X | | | | X | | | | | | |

*Figure 16: Cross-consistency matrix which includes stakeholder feedback regarding MPC uncertainties and requirements for implementation and use. X = inconsistent pairs; black spaces are duplicate/redundant pairings.*[1]

This matrix shows a full range of possible scenario choices that are plausible, relevant, and consistent to banks. For this study, initial learning scenarios were abductively derived based on a conceptual model. Thus, the consistent values from the matrix will be reclassified according to the previously derived scenario archetypes.

[1] The 22 conditions or possible outcomes are numbered to reflect the same conditions in the first row and in the first column.

The following scenario classes shown in the tables below are highlighted with the possible outcomes for the respective scenario. Based on the consistent pairs from the cross-impact matrix, consistent solutions can be used to re-formulate scenarios. Learning scenarios were already framed and justified by stakeholder input, but evaluating for consistency produces more accurate scenarios for decision making in organizations.

Tables representing each scenario class was developed according to inputs from the cross-impact matrix and MPC application areas confirmed by interviewees (see section 7.6). MPC applications are listed in the first column of every table. Subsequent columns are reiterations of the possible outcomes for each uncertainty (refer to Table 16 and/or Figure 16). By color coding consistent pairings with scenario applications in each class, decision makers can identify and develop use-case stories or narratives based on different combinations that they deem useful.

Legend: Each MPC implementation scenario outcome is color coded to show the consistent groupings of outcomes. ***Each color (yellow, orange, red, blue)*** differentiates a different scenario application listed in the first column. Like colors in the represent consistent pairing with the scenario application. Whereas ***green*** denotes that the particular value is consistent with multiple scenario applications for that class. Moreover, the green cells are further denoted by numbers in parenthesis that correspond to the scenario application that it is consistent with. ***No color*** means that it does not apply for that particular scenario class. Scenario classes II and III have an additional column with business model outcomes since these scenario types are the main business drivers in business model innovation which is based on the conceptual model of this study.

### *Scenario Class I: Improving internal processes and operations with regards to fraud detection, cybersecurity threat detection, and credit and risk monitoring.*

| | Scenario Application | Legal & Governance Structure | Technology Ownership | Implementation Incentives | Data Type Requirements | Customer Perception | Tech Capability |
|---|---|---|---|---|---|---|---|
| 1 | Fraud Detection | Contractual arrangements **(1-4)** | Open Source **(1-4)** | Privacy e.g. secret bidding | Fraud related data | Customer approves of MPC **(1-4)** | Secure/private Data analytics **(1-4)** |
| 2 | Cybersecurity Threat Detection | | Banks **(1-4)** | Algorithmic capability/use-case dependent **(1-4)** | Performance indicators | Customer cannot validate MPC **(1-4)** | |
| 3 | Credit and Risk Monitoring | | Third party provider/vendor **(1-4)** | Efficiency/improvement in data sharing process; circumvent strict data regulations | Threat/cybersecurity Data **(2,4)** | | |
| 4 | Interbank live monitoring in security | | Gov/supervisory authorities | Interorganizational collaboration via MPC (external data) | AML/CTF related data | | |

*Scenario Class II: Enhancing existing products and services in banks by using MPC enabled data analytics or data aggregation.*

| | Scenario Application | Legal & Governance Structure | Technology Ownership | Implementation Incentives | Data Type Requirements | Business Models | Customer Perception | Tech Development |
|---|---|---|---|---|---|---|---|---|
| 1 | More accurate insurance and finance models | Contractual arrangements **(1-4)** | Open Source **(1-4)** | Privacy e.g. secret bidding | Fraud related data | Data monetization (computations/Analytics as a Service) | Customer approves of MPC **(1-4)** | Secure/private Data analytics**(1-4)** |
| 2 | Security | | Banks **(1-4)** | Algorithmic capability/use-case dependent **(1-4)** | Performance indicators of customers or banks **(2,3)** | Data marketplaces | Customer cannot validate MPC **(1-4)** | |
| 3 | Calculating rates and risks in lending for customers | | Third party provider/vendor **(1-4)** | Efficiency/improvement in data sharing process; circumvent strict data regulations | Threat/cybersecurity data | Industry data platforms | | |
| 4 | Recommend better products to customers | | Gov/supervisory authorities **(1-4)** | Interorganizational collaboration via MPC (external data) | AML/CTF related data | Technical enabler | | |
| 5 | | | | | | Open Data policy | | |
| 6 | | | | | | B2C **(3,4)** | | |

*Scenario Class III: Enabling new products and services with MPC.*

| | Scenario Application | Legal & Governance Structure | Technology Ownership | Implementation Incentives | Data Type Requirements | Business Models | Customer Perception | Tech Development |
|---|---|---|---|---|---|---|---|---|
| 1 | KYC validation products and services | Contractual arrangements **(2,3)** | Open Source **(1-4)** | Privacy e.g. secret bidding, sharing | Fraud related data | Data monetization | Customer approves of MPC **(1-4)** | Secure/private Data analytics **(1-4)** |
| 2 | Benchmarking services | | Banks **(1-4)** | Algorithmic capability/use-case dependent **(1,2)** | Performance indicators | Data marketplaces | Customer cannot validate MPC **(1-4)** | |
| 3 | Coupling of bank offerings with other non-bank incumbent(s) | | Third party provider/vendor **(1-4)** | Efficiency/improvement in data sharing process; circumvent strict data regulations | Threat/cybersecurity data | Industry data platforms | | |
| 4 | | | Gov/supervisory authorities | Interorganizational collaboration via MPC (external data) | AML/CTF related data | Technical enabler | | |
| 5 | | | | | | Open Data policy | | |
| 6 | | | | | | B2C | | |

*Scenario Class IV: Assisting government and/or supervisory authorities to combat financial crime.*

| | Scenario Application | Legal & Governance Structure | Technology Ownership | Implementation Incentives | Data Type Requirements | Customer Perception | Tech Development |
|---|---|---|---|---|---|---|---|
| 1 | AML/CTF detection | Contractual arrangements **(1-4)** | Open Source **(1-4)** | Privacy e.g. secret bidding, sharing **(1-4)** | Fraud related data | Customer approves of MPC **(1-4)** | Secure/private Data analytics **(1-4)** |
| 2 | Fraud detection | | Banks | Algorithmic capability/use-case dependent | Performance indicators | Customer cannot validate MPC **(1-4)** | |
| 3 | Real-time data flow/monitoring dashboard of fraud/credit risk | | Third party provider/vendor **(1-4)** | Efficiency/improvement in data sharing process; circumvent strict data regulations **(1-4)** | Threat/cybersecurity data | | |
| 4 | | | Gov/supervisory authorities **(1-4)** | Interorganizational collaboration via MPC (external data) **(1-4)** | AML/CTF related data | | |

These decision-based scenarios show that improving internal efficiency for financial risk mitigation or abiding by the government mandates to assist with financial crime do not really change the value proposition of banks sine these are already existing processes and protocols within the bank. Hence, new business models or business model innovation are not consistent with Scenario Class I and IV. However, enhancing or enabling *business* processes, products or services can lead to new business models for banks.

As discussed in earlier chapters for data driven business models and data monetization, data can complement an existing product or service, lead to process innovation, or enable entirely new data d-driven products and services (Schüritz et al., 2017; Sorescu, 2017; Wixom & Ross, 2017). Scenario class II and III are consistent with this logic whereby, MPC may be able to improve banks' existing offerings with more accurate data or privacy preserving data analytics and computations and/or completely innovate an existing service. Contrary to some DDBM literature that argues that data needs to be fully leveraged in the value creation, capture and proposition of the firm in order to create new business models, MPC can (in)directly enhance or enable financial risk mitigation functions that can lead to business model innovation or new business models as well. MPC can enable new KYC (Know Your Client) validation services and products for other businesses or provide benchmarking services to other businesses as well. In these scenarios, banks would use their internal data but leverage the computation functions of MPC to privately and securely provide a form of data analytics or function output to other businesses.

MPC data sharing and collaboration can also lead to new products and services from shared data. Heterogeneous partners in a network can share information from their respective industries to create a new offering or service targeting or creating a shared customer base. This requires the monetization and collaboration of shared data analytics in a co-created business model between MPC partners. This aligns with Chen's et al. (2011) description of data analytics business models that involves leveraging:

1. internal proprietary data;
2. shared data;
3. shared data analytics;
4. shared and co-created value between customers and businesses;
5. the co-development and collaboration of data analytics solutions between industry partners;
6. and the generation of entirely new businesses (Chen et al., 2011, p. 16).

This analysis also answers **SQ4** of which business model components are affected by MPC implementation and use. Based on more widely cited literature for DDBM research, Hartmann's et al. (2014) taxonomy for

DDBMs lists the components in his DDBM framework: data sources, key activities, offering, target customer, revenue model, and special cost advantage (p.6). For MPC use-cases and business models, the data sources that banks will leverage are internal and external as well as shared which is not listed in Hartmann's et al. (2014) framework (refer to Appendix F).

For internal data, banks will most likely use existing data that they have and procure or generate metadata specifically for MPC implementations. Banks will not obtain or acquire external data from other parties but gain access to shared datasets to compute functions with. From the seven data driven key activities, MPC will most likely enable predictive, prescriptive, and descriptive data analytics that banks will leverage for new business models. Predictive and prescriptive data analysis can be applied to money laundering prevention and real-time security monitoring uses, respectively, but this requires advancement of MPC technology computational techniques and abilities.

DDBM offerings include data, non-data product or service, information/knowledge (Hartmann et al., 2014). Banks cannot offer or sell data directly, but they can offer data analytics and computations for B2B models, data enhanced or non-data product or service for B2C models, and information/knowledge for B2B and B2G models. Target customers would be B2B or B2C. B2G is not listed in the DDBM framework, but if government stimulates or incentivizes banks to provide their data for AML and CTF purposes, then the government or supervisory bodies can become a target customer of the bank.

Lastly, the monetization and value capture aspect of MPC implementation such as revenue models needs more exploration and input from stakeholders. Due to the legal complexity of data ownership and usage rights of shared data outputs, the revenue model component of MPC enabled business models are unclear. Selling analytics or algorithms as a service is plausible but precarious due customer ethics, fairness, perception and rights to control their personal data. Value capture will most likely arise from the cost saving benefits of improved financial risk structures and models. However, it is undetermined yet if the cost of investment outweighs the benefits of MPC use.

## 7.8 Conclusion

The results of the data collection and data analysis answered SQ3 and SQ4. Expert opinions were collected across multiple stakeholders in security, technology management, innovation, business development, cryptography, and compliance. The purpose of data collection via semi-structured interviews was to validate uncertainties and learning scenarios with regards to MPC implementation in banks for financial risk mitigation. The data analysis methods aimed to elucidate plausible MPC enabled business models, establish decision scenarios for MPC implementation in banks, and establish validity and reliability in the research.

Interviews started with five uncertainties concerning MPC implementations that were validated by industry experts and stakeholders. These five implementation uncertainties broadly covered: legal & governance structure, business and collaboration incentives, MPC technology ownership, data requirements, and business models. Two interviewees provided feedback that customer perception or explainability and algorithm requirements should be added. Customer perception has a contingency on whether banks should use MPC because it is difficult to explain how MPC works to customers and to prove in non-technical terms that their data is secure. It was mentioned across all stakeholders that explainability is not only important to legal, compliance and management but also to customers. Furthermore, it is hard to speculate or imagine the plausibility of some scenarios or adopting certain applications and business models in the context of MPC due to lack of knowledge of what MPC is and the

technological maturity of MPC. **Hence, to briefly answer SQ3 of this research study, the critical uncertainties of MPC implementation in bank settings are:**

1. The legal and governance structure of MPC consortium/networks, liabilities, risks, usage and ownership of data;
2. Technology ownership of the MPC platform itself;
3. Business and collaboration incentives for MPC use;
4. Metadata requirements for MPC inputs and outputs;
5. MPC enabled business models;
6. Customer perception and acceptance of MPC as a technology;
7. Technology development and capability of MPC within a five-year horizon.

Possible outcomes for each uncertainty and learning scenarios needed to assessed by four criteria, listed by importance: plausibility, relevancy, consistency and novelty. Plausibility and relevancy were mostly validated and established by interview participants. The GMA method was used to systematically assess the consistency of each possible outcome. Each outcome was iteratively assessed pairwise to check for logical consistency and empirical consistency. A drawback to this assessment is that this iterative process can inconsistently change perceptions of what is logical and empirically possible.

Scenario development and codification of the interview transcripts provided insight into what type of business models are possible with MPC use, what kind of products and services banks can offer, the barriers to implementing and trusting MPC, and the challenges with fully monetizing data due to customer approval and a highly regulated environment. No scenario applications were rejected by stakeholders accept the utility of MPC to drive other technologies such as AI and ML. AI and ML would provide banks with predictive analytics whereas MPC would provide banks with more descriptive analytics such as trend profiles, risk scores and indicators, etc.

Although the morphological analysis and stakeholder input formed the foundation of scenario development for MPC implementation and use within banks. Further analysis was necessary to gain more in-depth understanding of MPC business model components. Hence, a concept map was created to further elucidate and evaluate MPC enabled business models as well as show the contingencies on business model scenarios. Ultimately, these analyses contributed to answering **SQ4**: **Which business model components could be affected by MPC implementation and use?** The main business components that can be affected by MPC implementation are the target customers (B2B, B2C, B2G), the data used, the key data activity (data analytics), and the offering (data analytics, algorithms, computations as a service, non-data product/service, and information.

# 8. Discussion & Conclusion

This chapter aims to evaluate and interpret the findings of the results and data analysis to answer the main research question. As well as to evaluate the research findings and future areas for researcher.

## 8.1 Interpretation of Findings

There are four archetypal MPC implementation scenarios in banks for financial risk mitigation. These scenarios are meant to be mutually exclusive and provide insight for decision makers within banks. The main research question is: **What are the possible future scenarios of MPC enabled business models for financial risk mitigation?** Out of the four scenarios derived, two scenarios (II, III) can lead to or result in new business models for banks within the EU. However, scenarios I and IV are the most plausible for banks but not the most relevant in terms of business opportunity and value creation. Enhancing existing products and services or enabling new ones with MPC depends on the capability and maturity of MPC computational algorithms, the use-case, and customer perception of MPC. Below are descriptions of the scenario archetypes.

### Decision Scenario 1: Improving internal efficiency of the bank.

MPC can result in more informed decisions with regards to tackling cybersecurity threats, financial crime, and credit monitoring. In cybersecurity, banks can inform other banks and supervisory bodies via interbank data sharing when a bank's cybersecurity has been attacked or threatened. The main incentive is being able to securely and anonymously share this data for the benefit of the network without compromising the banks' reputation and trust from their customers. In a similar vein, security related information can be shared more efficiently and faster depending on the future capability of providing real-time monitoring. This may allow more employees to work remotely if security across the organization is improved. Since banks are not allowed to compete on security, they can only share security related information with other banks to improve the internal efficiency of security monitoring. Within the domain of fraud detection, being able to share and produce risks scores, fraud indicators, and risk profiles with external banks adds value to the banks' internal fraud detection processes. The incentive is to improve their own databases and prevent fraud rather than analyzing and prosecuting fraudsters. Lastly, sharing external data to gain insight into credit scores and risk factors for defaults can improve banks' pervasive challenge with non-performing loans. These use-cases have cost saving benefits such as time and resources, but it does not create any additional value in revenue or value proposition because all banks receive the same output. There is no differentiation of outputs that can be leveraged among parties.

### Decision Scenario 2: Enhancing existing product/services/offerings with MPC.

If scenario 1 is successful, then data driven improvements in those areas can enhance the banks' offerings to their customers. More accurate insurance and finance models would require external data from non-bank entities such as health insurers. There would be differentiation potential since heterogenous organizations could leverage the data outputs strategically with the internal data that they have unlike scenario 1. Banks can adopt an MPC enabled industry platform business models whereby data analytics is exchanged to add value towards existing insurance or finance models from the bank. Data monetization and data marketplace business models would be risky due to the customer perception and ethics of indirectly using customer data analytic computations with external companies. They have no way of validating or checking if their data is secure and private so that can lead to skepticism from customers.

A B2C model data monetization business model can be adopted by enhancing interest rate offers for loans, insurance, etc. Banks can offer to calculate a customer's interest rate when they want to borrow

an asset by using their data without having insight into that data. It would provide fairer interest rate options for new and existing customers in the form of computation or analytics as a service. This would also indirectly improve financial oversight into banks' loan programs.

Sharing performance indicators in security for benchmarking can help banks improve their services. Banks offer and leverage trust and security for their customers. If banks determine how well they are doing in security compared to other organizations, they can make the necessary improvements to their security profiles. However, banks need to be careful that benchmarking remains anonymized so as to not violate the rule in competing in security. Lastly, exchanging information with other industries in the form of trend profiles can provide insight into banks' existing offers. In this scenario, banks can indirectly enhance their business models and value propositions with better or data enhanced offerings.

### Decision Scenario 3: MPC enables new products and services (use-case driven MPC)

There are three applications and three possible business models that banks can adopt. Validation of banks customers is important in business continuity and ensuring the integrity of the financial system. Banks can offer KYC validation services in open banking and PSD2 environments whereby, fintechs do not have the customer or transaction data to sufficiently validate their customers. Banks would be the data owner and the third-party providers would be the data users.

Benchmarking services from the bank can be monetized in the form of computations as a service whereby banks participate or supply their data to be used in MPC benchmarking calculations. This scenario allows banks to privately and securely provide their data without allowing competing and unauthorized parties to have insight into their data.

The third business model that can be implemented is a collaborative and competitive industry data platform enabled by MPC. Banks and non-bank industries exchange data such as customer personas or trend profiles that can produce new products and services in one or multiple organizations.

### Decision Scenario 4: Assisting government and supervisory authorities.

This scenario is characterized by data sharing between public and private sectors to support financial policy and protecting societal interests. In order to combat financial crime, banks will assist government and police authorities in supplying knowledge or information regarding fraudsters, money laundering transactions, money mule accounts, and other indicators of financial misconduct. Unless the government incentivizes banks to do this, there would be no direct monetary gain or business value in implementing MPC. Banks will indirectly benefit from the prosecution and increased knowledge on these types of crimes and individuals but there are no business models that would result from this scenario.

In conclusion, there is a possibility for combined scenarios or scenarios in which one scenario precedes another. However, according to the scenario analysis methodology scenarios were constructed to archetypal and independent of each other (Schoemaker & Mavaddat, 2000). The main objectives of developing these scenarios was to determine correlations between the underlying structures that result or affect MPC implementation, challenge existing mental models of banks and ultimately improve decision making regarding MPC use for financial risk management and new business ventures. This thesis was able to achieve the first two objectives to certain degree whereas, the last objective has a potential to do so given that there is no research on MPC implementation outcomes and combination ranges thus far. However, actual observation of an organization's strategic choices based on the scenarios is necessary in order to definitively say that this objective was met. Logic models and associations between variables

were established during the morphological analysis process and data analysis process. Moreover, it is assumed that new information that challenged interview participants in these organizations was warranted given that some had little understanding of MPC or some lacked the full organizational context of MPC that was presented during interviews. However, this was not validated verbally with interview participants.

Another main project outcome is making a scientific contribution to MPC business literature, the field of IOS, and business model disciplines which also upholds managerial significance to banks and possibly other organizations. Following from the identification of the knowledge gap, the purpose of research investigation was to understand the potential of MPC to be leveraged and used in banks and its possible observable outcomes that can manifest in the foreseeable future. This investigation was guided by the research sub-questions that was answered in previous sections (Chapter 3: SQ1, Chapter 4.4-4.5: SQ2, Chapter 7: SQ3, SQ4). The knowledge contributions are elaborated in the proceeding sections: theoretical and practical contributions.

## 8.2 Theoretical contributions

The main contribution from this study is a conceptual framework that links MPC implementation to organizational outcomes which was abductively derived from foundations of IOS theories and business model disciplines. Abduction usually results in a new theory being developed or a modification of an existing theory (Saunders et al., 2019). This conceptual model is illustrated below in Figure 17. This conceptual model is an adaptation of an IOS theoretical framework from Robey et al. (2008) which can be used as a foundation for future research in IOS and MPC business research. MPC can be interpreted as an IOS technology whereby the modified theory would be the relationship of value creation outcomes to data driven business model innovation.

Scenario 2

Scenario 3

Scenario 1,4

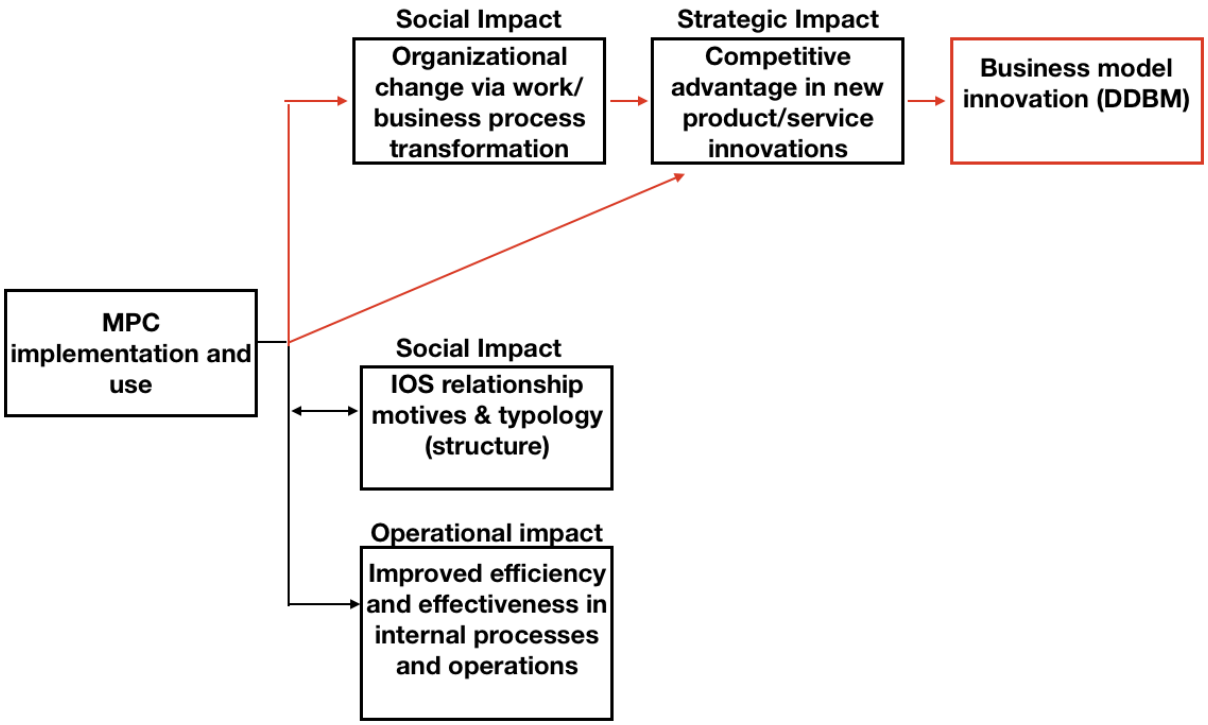



*Figure 17:Theoretical framework for MPC implementation and scenario applications.*

As depicted in the conceptual model, case study evidence supports a link or correlation between MPC implementation in theoretical and actual outcomes. Scenario 2 indicates that firms can use MPC to indirectly improve current offerings with data enhanced products and services. On the other hand, Scenario 3, suggests that firms can also strategically create new products and services driven by computational outputs and privacy preserving analytics. However, this would need to be further tested empirically in order to ascertain veracity to this claim.

The second contribution is conceptual knowledge towards data-driven business model concepts in two areas of research: business model innovation and business model components. Data-driven business model frameworks in extant literature are more comprehensive in addressing value creation logic for MPC applications as opposed to contemporary digital business model constructs. With value creation theories such a network theory and resourced based view, it was abductively derived that MPC implementation can indirectly and directly influence data-driven business models depending on the context of use. Hence, resulting in data driven business model innovation.

The chosen DDBM framework in this study was Hartmann's et al. (2014) taxonomy for data driven business models. This framework defined a taxonomy of business model components that can be used in data-driven contexts, predominately in big data applications. However, MPC has yet to scale to big data and thus, this required further research analysis and evaluation to determine MPC business model components (via case study and scenario analyses). Research findings indicate that business models for MPC data-driven contexts align with these pre-defined components from Hartmann's et al. (2014) taxonomy: data sources, key activities, offerings, and target customers. This is also listed in the left column of table 17 below.

However, it was evaluated based on content analysis and scenario development that new business model components are possible in the context of MPC. These new BM components (right column) were undefined and unlisted in Hartmann's et al. (2014) taxonomy. New MPC business model components are data sources from shared datasets, privacy preserving data analytics, and offerings such as privacy preserving algorithms as a service and computations as a service. Within bank settings, data monetization is perceived as unethical and therefore, banks are reluctant to adopt this business model such as DaaS. Therefore, banks need to leverage data so that is being indirectly used as an input for another service or offering. MPC may enable banks to offer the value of data analytics in a privacy preserving and integrity laden manner. Furthermore, data analytics is a different market than raw data because society is always trying to derive meaning from data for more informed views. Banks can position themselves to fill this need with the wealth of data that they own. The distinction here is that a firm can sell MPC based algorithms or offer to join or form a data analytic computation, whereby internal data is not given only the output.

Moreover, a potential target customer can be government entities but this is dependent on whether the government mandates an open data policy or incentivizes banks to share their data. This last point is speculative since most B2G data sharing is mandated rather than incentivized. Lastly, MPC revenue models require more exploratory investigation but based on the business model choices derived in this study, collaboration and newly co-created markets and offerings between heterogeneous sectors give rise to a different type of revenue model. Two-sided markets such as industry data platforms, allow the exchange of data whereby valuation of data is not equal with different industry partners. This was validated and confirmed by an interviewee in Bank A, wherein value is created when MPC outputs have a different value or meaning for every network partner that allows them to differentiate their business models.

| Existing DDBM Components for MPC | Plausible new MPC BM Components |
|---|---|
| Data sources: **internal, external data** | Shared datasets |
| Key activities: **Data analytics** | Privacy preserving data analytics |
| Offering: **Data (DaaS, AaaS), knowledge, non-data product/service** | Privacy preserving data algorithms, computations as a service |
| Target Customer: **B2B, B2C** | B2G |
| Revenue Model: | Two-sided markets |

*Table 18: Actual MPC enabled business model components versus new plausible components based on* (Hartmann et al., 2014)

Evidently, the revenue and monetization aspect of MPC enabled business models need more exploration and research and supported by more evidence. Due to the high regulatory environment of banking environments, banks need to be careful on how data is monetized without violating GDPR and remaining ethical and fair to customers. Nonetheless, this research links MPC case study evidence and research to two data driven business model disciplines.

The third contribution is conceptual knowledge towards business model innovation for inter-organizational systems data sharing. An MPC conceptual framework was deductively derived from IOS and business model innovation theory to understand the social, strategic, and operational consequences of MPC use. MPC can enable new products and services as well as business model innovation indirectly and directly. These scenarios are also highly dependent on the use-case.

The fourth contribution is adding MPC implementation scenarios to futures study and MPC literature in the context of banking and finance. possible future scenarios of MPC implementation in the banking sector, MPC literature and futures studies of emerging technologies.

## 8.3 Practical contributions

The practical implications are relevant to decision makers and managers who are evaluating whether to implement MPC. It will be more useful to banks, but can serve as a foundation for strategic choices in other firms and industries. There are five main practical contributions which are listed as follows:

1. Managerial implications for firms aiming to adopt or implement MPC and a step towards improving decision making in this regard;
2. Descriptive knowledge for actors looking for a range of possible combinations of future outcomes;
3. Insights into business model choices and components in the context of MPC as well as from a data perspective;
4. Descriptive knowledge of the business potential that MPC offers in banking from a business model and data perspective;
5. Awareness of the business environment and drivers that affect the future of EU banking and the data ecosystem.

Essentially, this study provides contextualized research and data regarding EU banks and their immediate and external business environments. Firstly, the most useful deliverable are the decision scenarios and scenario classes that show the ranges of possibilities in implementing and adopting MPC. Secondly, scenario possibilities started with 768 unique combinations which was aggregated and eliminated to a manageable set of four scenario archetypes. Thirdly, insights into business model choices and components in the context of MPC which is detailed in Table 18. Moreover, the theoretical contribution linked MPC to business model components and concepts, whereas the use-case examples in this study provide banks with practical knowledge and ideas for contextual business model components. These examples are listed in the left column of Table 18.

Fourthly, this research provides descriptive knowledge of the business potential that MPC can enable for banks which include integrity driven transactions and activities, secure and/or anonymous data sharing, and new business models. MPC can facilitate data enhanced value creation within banks, but also enable data-driven value creation and capture that would require business model innovation. Lastly, it equips decision makers with more knowledge about their environment and some of the contingent factors that underlie MPC implementation and consequences. For instance, data sharing with homogenous industry partners i.e. other banks is more likely to result in data-enhanced operations or internal efficiency. Conversely, collaboration with heterogeneous organizations can create new data driven business models such as industry data platforms.

| **DDBM Components** | **Plausible new MPC BM Components** | **Examples** |
|---|---|---|
| Data sources: **internal, external data** | Shared datasets | Use-case specific meta-data |
| Key activities: **Data analytics** | Privacy preserving data analytics | Data analytics (Benchmarking information, cybersecurity threat information, fraud |

| | | |
|---|---|---|
| | | indicators), anonymous data sharing and voting |
| Offering: **Data (DaaS, AaaS), knowledge, non-data product/service** | Privacy preserving data algorithms, computations as a service | Benchmarking as a service, credit risk calculations as a service, KYC validation as a service |
| Target Customer: **B2B, B2C** | B2G | ECB, Financial intelligence units, banking associations, other banks, prospective loan borrowers, |
| Revenue Model: | Two-sided market | Coopetition/co-creation with heterogenous main industry players (health insurers, telecom) |

*Table 19: MPC business model components and practical examples in the context of EU bank sector.*

As mentioned previously, descriptive scenarios are meant to establish causal modes of thinking by delineating a logical sequence of events which is inherently more intuitive for decision makers (Van Der Heijden, 1996). These scenarios and analysis also help managers adapt more readily to their environment via informed decision-making as a result of reviewing contextualized strategic options.

## 8.4 Recommendations for banks in the EU

The main output of this thesis is descriptive knowledge and therefore, the scenarios cannot prescribe to banks which scenario is most plausible or the most successful. All scenarios should be equally probable. However, scenarios can be used to guide strategic conversations that involve MPC implementation choices. A detailed reference for strategic management and adaptive organizational learning with scenarios can be found: **Scenarios: The Art of Strategic Conversation (Van Der Heijden, 1996)** and **Opening the 'black box' of scenario analysis through realist synthesis (Frith & Tapinos, 2020).** These sources provide systematic approaches to using scenarios and structuring workshops and exercises.

Every MPC implementation requires a specific legal and governance structure in order to establish data ownership and liability, address the security, privacy and reliability risks in MPC algorithms, and definition of what the purpose of the MPC implementation is. Furthermore, MPC enabled business models are dependent on the use-case since data and MPC network partners have to be procured. Therefore, the decision to implement or use MPC must start from the use-case and agreed upon by contracts with external parties before MPC implementation can occur. Since MPC implementation is very contingent on the context and use-case, technological maturity and research developments need to occur on the technical aspects of MPC before it can be used in banking operations and applications. Trust, security and data are sources of competitive advantage for banks and these can be compromised in MPC implementations if the technology is not secure, auditable, and proven. Therefore, MPC implementation decisions may require research and proofing from the banks themselves or external consultancy from experts.

For more in-depth knowledge of possible MPC outcomes, chapter 7 records all the possible, relevant, and internally consistent combinations of events. Additionally, a full range of possible combinations are classified to four categories of scenarios that align with the conceptual model that was derived. For more detailed and contextual information, Appendix I discusses the record of interview responses which include

specific MPC use case examples that can be used for generating new ideas and challenging conventional thinking for MPC opportunities.

## 8.5 Evaluation of Limitations

There are several limitations to this study in data collection, interview bias, and subjectivity in scenario analysis. The interview selection was chosen based on judgment sampling, availability, and convenience given that researching MPC implementation within banks is not easily conducted or previously researched. Banks are competitive and do not always market or publicly announce new innovative projects that they are involved in. Thus, there is difficulty in gaining access to internal documents regarding these projects as well as the individuals involved. Due to this, there are inconsistencies and discrepancies in how data was collected from the banks as well as interview participants. This undermines the research findings and introduces interviewee bias and subjectivity. Furthermore, the scenario analysis method is also vulnerable to inconsistencies with stakeholder opinions, judgements, and various levels of MPC understanding, knowledge and interests. This threatens the internal validity of the research and hence, a mixed method data analysis approach was used to account for this.

There were also differences between the bank samples with regards to the number of participants per case and the information asymmetry in MPC knowledge which also threatens the generalizability of the research. The varying degrees of expertise and research of MPC between stakeholders have implications on bias towards their specialist fields and accuracy of MPC scenarios. MPC technology is quite new and therefore, it is difficult for stakeholders to speculate how MPC can be used in banks, within their specialist fields and in other core banking activities of the banks. Therefore, this can affect the accuracy and plausibility of scenarios.

Furthermore, COVID-19 can exacerbate this issue and affect the research and development of MPC projects within banks. Therefore, some participants were asked whether COVID-19 affects the plausibility and relevancy of scenarios. The general consensus was that it did not affect the scenarios or the security of banks which infers that security frameworks within banks is consistent with scenario analysis. However, COVID-19 can increase the risk drivers of money laundering, counter terrorist financing, cybercrime and financial fraud since more bank networks are vulnerable with the rise in employees working remotely. This can either accelerate the need to combat financial crime and stimulate the development of MPC or slow down banking operations and initiatives in MPC enabled fraud detection. Therefore, these scenarios can be slightly inconsistent and/or implausible within the time horizon of five years.

Lastly, the judgment criteria of scenarios used in this study can be subjective depending on the interview participant's behavior, social values and disposition. Perhaps not all plausible scenarios were determined based on the limited number of participants and between different banks. Moreover, the novelty criteria could not be assessed entirely for each participant. The 'novelty' criterion is supposed to introduce creativity and innovativeness which can also contradict the plausibility of scenarios to some extent. In other words, creative and novel scenarios may not always be plausible. Therefore, the novelty aspect can be deemed as an additional judgment criterion for scenarios as opposed to the required criteria: plausibility, relevancy, and consistency. Furthermore, novelty was not validated with all participants. However, two participants commented after the interview that they were able to learn more about MPC and think about MPC in a new way. One of these participants also has a high level of MPC knowledge and proofing of technical concepts in MPC which can suggest that these scenarios are also novel. Whereas, the other stakeholder is leading in compliance by design for MPC systems which also suggests that to

some degree, the mental models of participants were affected. Therefore, one of the main objectives of scenario analysis was executed in this study.

## 8.6 Areas for Future Research

In order to determine future areas of research, revisiting the research approach is necessary to determine the logical next steps. The purpose of future studies is to attend to rival explanations and/or pursue different interpretations in order to elevate findings, concepts and generate more objective truths about MPC implementation. Essentially, an exploratory and qualitative research was undertaken from a critical realist stance. Therefore, future studies can generally comprise of the following targets:

- Apply the same research methods in order to collect more data for more generalizable findings;
- Build upon this research by adding new findings;
- And use different research methodologies to explore and investigate a different perspective to the research problem;
- change the scope of the research by time horizon, geography, and industry sector.

The possible avenues for these targets are detailed sequentially.

Firstly, similar studies can be conducted methodologically to compare studies as a means to identify any differences, similarities, or validation and rejection of any of the findings of this study. In doing so, findings will be more generalizable and more data collection can present new findings and/or validate or invalidate the findings of this research. For instance, collecting data from a wider and more diverse sample of interviews within banks. Or the theoretical framework developed in this study can be (in)validated in a different industry or organization.

Secondly, the research findings of this thesis are principally descriptive and it presents the first investigation and insights into MPC implementation in banks. Building upon this study to test causal relationships or provide prescriptive knowledge for implementing MPC. This research study undertook an intuitive logics approach to scenario analysis whereas, La Prospective and Probabilistic Modified Trend Models to scenario analysis and analysis requires a more quantitative and explanatory approach. If done successfully, these methods will be able to inform the probability and likelihood of scenarios and/or prescribe the ranking of best to worst case scenarios. Within the intuitive logics model, there is a fourth and last phase of scenario analysis, called scenario utilization. This last phase entails testing causal relationships of plausible futures to actual enactment of those scenarios in real world settings. Essentially, it calls for a case study of using these scenarios for actual implementation and strategic decision making in the organization itself. Or in other words, testing the extent to which decision making is improved as a result of scenarios.

Thirdly, adopting different methodologies and philosophical worldviews presents opportunities to further understand MPC implementation outcomes. For example, adopting a positivist philosophy to determine the actual implementation of MPC via an explanatory case study could be viable. In terms of building upon this research study, it was initially proposed to investigate the two critical realist domains, whereas the empirical domain in the stratified ontology of critical realism was left unexplored. Therefore, a critical realist perspective can also be adopted for future studies to test these scenario outcomes against actual outcomes of MPC implementation. However, both options require the time progression and/or development of MPC technology towards a more mature stage. Moreover, in order to be objective as possible for this study, axiological assumptions were not entirely considered in the research design choices. Axiological assumptions goes beyond social science and management research to include humanities and arts sciences (Saunders et al., 2019). Axiological assumptions refer to the understanding

and interpretation of certain phenomenon from the perspective of values and ethics. This inherently requires a more subjectivist approach to understanding the underlying structures and mechanisms that constitute a person's logic and choices from their experiences, values, etc. This may be particularly useful due to absence of standard rules and ethics for MPC use.

As an example, customer empowerment and digital sovereignty are rising in the digital society. Society is pushing to create ethical and regulated technologies that protect the interests of people's values. Ethical data analytic algorithms such as those used in AI are now being examined by the EU (European Commission, 2020h). Therefore, ethical requirements for MPC should also be a concern among stakeholders, especially in bank settings, since MPC utilizes data analytic algorithms as well. Algorithmic bias in customer profiling and analytics could be particularly problematic in MPC as well as jeopardize the reputation of MPC adopters. On the other hand, cryptographic and privacy preserving technologies such as blockchain, for example, can be used for organized crime. Similarly, MPC could potentially enable organized crime by enabling secret transactions between criminals themselves or keeping nefarious information secret from the public. Furthermore, privacy preserving transactions between fraudsters and banks can alternatively, reduce the transparency of clients and KYC related matters since it would be more difficult to access a customers' data that was procured via MPC.

In this same line of reasoning, future areas of research should explore the causal relationships of customer perception on banks' business model choices. A common understanding among stakeholders involved in MPC arrangements and implementation is required, especially among non-technical people. Moreover, banks' customers need to understand how MPC works, how their data is being used in computations but not revealed. Customers will have a hard time understanding MPC and banks will have difficulty explaining MPC. Furthermore, customers will not be able to validate entirely the security and privacy of their data in MPC computations so there is a link between customer opinion, MPC acceptance and use, and ethics. Trust is also a social value that is important for bank customers and also the non-technical experts/stakeholders of the bank. Hence, another research area can explore the normative and social values that may affect the implementation or development of MPC technology.

Moreover, the limitations of the researching findings did not entirely elucidate revenue models for MPC in banks which requires more exploratory research. Stakeholders in this study sample were overwhelmingly concerned about the reliability of the algorithms with regards to security and privacy of data and the risks such as data leakage. However, algorithmic capability and output correctness can be two separate mutually exclusive aspects of MPC. Furthermore, MPC needs to have the correct output in order to derive value or be used for decision making. However, the accuracy of outputs is also important to inquire for further inspection. Most use cases will utilize data analytics such as risk scores or fraud indicators. If banks utilize these scores and create a class system of risk profiles on correctness of outputs then it can have dire consequences on the business. For example, MPC can detect fraudsters correctly in a dataset and they are grouped or classified as fraudsters. However, this class system needs to be accurate because they could have all committed fraud but some have more egregious crimes than others within the same grouping or class. If these criminals are handled by the authorities and prosecution office, inaccurate fraud or risk profiles can result in unfair punishments and misinformation that is liable to the bank. Therefore, decision making on different type of outputs and the extent of output correctness/accuracy should be explored.

Generally, this study explored the plausibility of MPC to create and capture value for banks in the form of improved business operations or enabled business model innovation. However, the degree to which value is created needs more investigation. This may entail the extent to which data is used for MPC, the

valuation of data types and activities for MPC, and/or empirically evaluating MPC business use-cases to compare B2B, B2C, and B2G models and markets.

# References


Al-Ajlouni, A., & Al-Hakim, D. M. S. (2019). Financial Technology in Banking Industry: Challenges and Opportunities. *SSRN Electronic Journal*, *February*. https://doi.org/10.2139/ssrn.3340363

Al-Debei, M. M., & Avison, D. (2010). Developing a unified framework of the business model concept. *European Journal of Information Systems*, *19*(3), 359–376. https://doi.org/10.1057/ejis.2010.21

Amer, M., Daim, T. U., & Jetter, A. (2013). A review of scenario planning. *Futures*, *46*, 23–40. https://doi.org/10.1016/j.futures.2012.10.003

Amit, R., & Zott, C. (2001). Value creation in e-business. *Strategic Management Journal*, *22*(6–7), 493–520. https://doi.org/10.1002/smj.187

Amit, R., & Zott, C. (2012). Creating Value Through Business Model Innovation. *MIT Sloan Management Review*, *53*(3), 40–49.

Ankele, R., Küç, K. A., Küçük, K., Martin, A., Simpson, A., & Paverd, A. (2016). Applying the Trustworthy Remote Entity to Privacy-Preserving Multiparty Computation: Requirements and Criteria for Large-Scale Applications. *2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld)*. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0077

Archer, D. W., Bogdanov, D., Kamm, L., Lindell, Y., Nielsen, K., Pagter, J. I., Smart, N. P., & Wright, R. N. (2018). From Keys to Databases-Real-World Applications of Secure Multi-Party Computation. *The Computer Journal*, *61*(12), 1749–1771.

Arnaut, C., Pont, M., Scaria, E., Berghmans, A., & Leconte, S. (2018). *Study on data sharing between companies in Europe*. https://doi.org/10.2759/354943

Athanasopoulou, A., de Reuver, M., Nikou, S., & Bouwman, H. (2019). What technology enabled services impact business models in the automotive industry? An exploratory study. *Futures*, *109*(March), 73–83. https://doi.org/10.1016/j.futures.2019.04.001

Ayadi, Rym;, Arbak, E., & De Groen, W. P. (2012). REGULATION OF EUROPEAN BANKS AND BUSINESS MODELS: TOWARDS A NEW PARADIGM? In *Centre for European Policy Studies CEPS*.

Ayadi, Rym;, De Groen, W. P., Sassi, I., Mathlouthi, W., Rey, H., & Aubry, O. (2017). Banking Business Models Monitor 2015 Europe. In *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2784334

Ayadi, Rym, Arbak, E., & Pieter De Groen, W. (2012). Business Models in European Banking: A Pre-and Post-Crisis Screening. In *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.1945779

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. In *Journal of Management* (Vol. 17, Issue 1, pp. 99–120). https://doi.org/10.1177/014920639101700108

Beaver, D., Micali, S., & Rogaway, P. (1990). *The Round Complexity of Secure Protocols*.

Ben-Or, M., Goldwasser, S., & Wigderson, A. (1988). Completeness theorems for non-cryptographic fault-tolerant distributed computation. *Proceedings of the Annual ACM*

*Symposium on Theory of Computing*, *January*, 1–10. https://doi.org/10.1145/62212.62213
Benta, C., Wilberg, J., Hollauer, C., & Omer, M. (2017). Process model for data-driven business model generation. *Proceedings of the International Conference on Engineering Design, ICED*, *2*(DS87-2), 347–356.
Bhaskar, R. (2008). A Realist Theory of Science. In *Noûs* (Vol. 24, Issue 5). https://doi.org/10.2307/2215817
Bogdanov, D., Jõemets, M., Siim, S., & Vaht, M. (n.d.). *How the Estonian Tax and Customs Board Evaluated a Tax Fraud Detection System Based on Secure Multi-party Computation (Short Paper)*.
Bogdanov, D., Talviste, R., & Willemson, J. (2012). Deploying secure multi-party computation for financial data analysis. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7397 LNCS*(8124), 57–64. https://doi.org/10.1007/978-3-642-32946-3_5
Böhmecke-schwafert, M., & Niebel, C. (2018). The General Data Protection's (GDPR) Impact on Data-Driven Business Models: The Case of the Right to Data Portability and Facebook. *ITU Journal: ICT Discoveries*, *9*(2), 0–7.
Bouwman, H., De Vos, H., Haaker, T., & Reuver, M. De. (2008). Mobile service innovation and business models. In *Mobile Service Innovation and Business Models*. https://doi.org/10.1007/978-3-540-79238-3
Bouwman, H., Nikou, S., Molina-Castillo, F. J., & de Reuver, M. (2018). The impact of digitalization on business models. *Digital Policy, Regulation and Governance* , *20*(2), 105–124. https://doi.org/10.1108/DPRG-07-2017-0039
Bouwman, H., Zhengjia, M., van der Duin, P., & Limonard, S. (2008). A business model for IPTV service: A dynamic framework. *Info*, *10*(3), 22–38. https://doi.org/10.1108/14636690810874377
Bradfield, R., Wright, G., Burt, G., Cairns, G., & Van Der Heijden, K. (2005). The origins and evolution of scenario techniques in long range business planning. *Futures*, *37*(8), 795–812. https://doi.org/10.1016/j.futures.2005.01.003
Brownlow, J., Zaki, M., Neely, A., & Urmetzer, F. (2015). Data and Analytics - Data-Driven Business Models : A Blueprint for Innovation. In *University of Cambridge Service Alliance*.
Bulger, M., Taylor, G., & Schroeder, R. (2014). Data-Driven Business Models: Challenges and Opportunities of Big Data. In *Oxford Internet Institute: Vol. Engaging C*. NEMODE. http://www.nemode.ac.uk/wp-content/uploads/2014/09/nemode_business_models_for_bigdata_2014_oxford.pdf
Burt, G., Wright, G., Bradfield, R., Cairns, G., & van der Heijden, K. (2006). The Role of Scenario Planning in Exploring the Environment in View of the Limitations of PEST and Its Derivatives. *International Studies of Management & Organization*, *36*(3), 50–76. https://doi.org/10.2753/imo0020-8825360303
Chen, Y., Kreulen, J., Campbell, M., & Abrams, C. (2011). Analytics ecosystem transformation: A force for business model innovation. *Proceedings - 2011 Annual SRII Global Conference, SRII 2011*, 11–20. https://doi.org/10.1109/SRII.2011.12
Chesbrough, H., & Rosenbloom, R. S. (2002). The role of the business model in capturing value from innovation: evidence from Xerox Corporation's technology spin-off companies. *Industrial and Corporate Change*, *11*(3), 529–555. https://doi.org/10.1093/icc/11.3.529

Damgård, I., Damgård, K., Nielsen, K., Nordholt, P. S., & Toft, T. (2017). Confidential benchmarking based on multiparty computation. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *9603 LNCS*, 169–187. https://doi.org/10.1007/978-3-662-54970-4_10

DaSilva, C. M., & Trkman, P. (2014). Business model: What it is and what it is not. *Long Range Planning*, *47*(6), 379–389. https://doi.org/10.1016/j.lrp.2013.08.004

Deloitte. (2020). *Banking regulatory outlook 2020 (USA)*.

Du, W., & Atallah, M. J. (2001). Secure multi-party computation problems and their applications: A review and open problems. *Proceedings New Security Paradigms Workshop*, 13–22. https://doi.org/10.1145/508172.508174

El Sawy, O. A., & Pereira, F. (2013). Business Modelling in the Dynamic Digital Space: An Ecosystem Approach. In *Springer, Berlin, Heidelberg*. Springer Briefs Series in Digital Spaces. https://doi.org/10.1007/978-3-642-31765-1

Elgarah, W., Falaleeva, N., Saunders, C. S., Ilie, V., Shim, J. T., & Courtney, J. F. (2005). Data Exchange in Interorganizational Relationships: Review Through Multiple Conceptual Lenses. *Data Base for Advances in Information Systems*, *36*(1), 8–29. https://doi.org/10.1145/1047070.1047073

Eriksson, T., & Ritchey, T. (2002). Scenario development using computerised morphological analysis. *Winchester International OR Conference, Winchester, England.*, 211–218.

European Banking Authority. (n.d.). *European Banking Authority*. Retrieved April 30, 2020, from https://eba.europa.eu/

European Banking Authority. (2020). *Our response to Coronavirus (Covid-19)*. https://eba.europa.eu/coronavirus

European Central Bank. (2018). *SSM thematic review on profitability and business models* (Issue September).

European Central Bank. (2019a). *ECB Banking Supervision : SSM supervisory priorities 2020*.

European Central Bank. (2019b). *ECB Banking Supervision: Risk assessment for 2020*. https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2020~a9164196cc.en.html#toc3

European Central Bank. (2019c). *ECB Banking Supervision: Risk assessment for 2020*. https://www.bankingsupervision.europa.eu/ecb/pub/ra/html/ssm.ra2020~a9164196cc.en.html#toc3

European Central Bank. (2019d). *Supervisory banking statistics*. https://www.bankingsupervision.europa.eu/banking/statistics/html/index.en.html

European Central Bank. (2019e). *Supervisory review (SREP) - Aggregate SREP outcome for 2019*. https://www.bankingsupervision.europa.eu/banking/srep/srep_2019/html/aggregate_results_2019.en.html#toc20

European Central Bank. (2020). *Non-performing loans*. https://www.bankingsupervision.europa.eu/banking/priorities/npl/html/index.en.html

European Commission. (n.d.-a). *Anti-money laundering and counter terrorist financing | European Commission*. Retrieved May 6, 2020, from https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en

European Commission. (n.d.-b). *Payment services | European Commission*. Retrieved April 30,

2020, from https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en
COMMISSION DELEGATED REGULATION (EU) 2018/1108, L 203 Official Journal of the European Union 2 (2018).
European Commission. (2018a). *Preventing money laundering and terrorist financing across the EU*. https://ec.europa.eu/info/sites/info/files/diagram_aml_2018.07_ok.pdf
European Commission. (2018b). *Rolling Plan for ICT Standardisation*.
European Commission. (2019a). *Assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*.
European Commission. (2019b). *Communication from the commission to the European parliament towards better implementation of the EU's anti-money laundering and countering the financing of terrorism framework: Vol. COM(2019)*. https://doi.org/10.1017/CBO9781107415324.004
European Commission. (2019c). *Frequently Asked Questions: Making electronic payments and online banking safer and easier for consumers*. European Commission Homepage. https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_5555
European Commission. (2019d). *Frequently Asked Questions: PSD2*. https://ec.europa.eu/commission/presscorner/detail/en/qanda_19_5555
European Commission. (2020a). *A European strategy for data: Vol. COM(2020)* (Issue 66 final). https://doi.org/10.1017/CBO9781107415324.004
European Commission. (2020b). *A New Industrial Strategy for Europe*. 1–16. https://ec.europa.eu/info/sites/info/files/communication-eu-industrial-strategy-march-2020_en.pdf
European Commission. (2020c). *Open data | Shaping Europe's digital future*. https://ec.europa.eu/digital-single-market/en/open-data
European Commission. (2020d). *Shaping Europe's digital future*. 9. https://doi.org/10.2759/48191
European Commission. (2020e). *The European Data Strategy: Shaping Europe's Digital Future* (Issue February). https://doi.org/10.2775/987881
European Commission. (2020f). *Towards a European strategy on data sharing for the public interest*. https://doi.org/10.2759/406717
European Commission. (2020g). *What's in it for Businesses - Shaping Europe's Digital Future*. https://doi.org/10.2775/653913
European Commission. (2020h). White Paper on Artificial Intelligence - A European approach to excellence and trust. *COM(2020) 65 Final*. https://www.cambridge.org/core/product/identifier/CBO9781107415324A009/type/book_part
European Parliament. (2017). *Data Flows - Future Scenarios*. http://files/15936/IPOL_IDA(2017)607362_EN.pdf
REGULATION (EU) 2018/1807 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, L 303/59 Official Journal of the European Union 59 (2018). http://europa.eu/rapid/press-release_IP-17-3190_en.htm
Directive (EU) on open data and the re-use of public sector information, 2019/1024, L 172

Official Journal of the European Union 56 (2019). http://data.europa.eu/eli/dir/2019/1024/oj

Evans, D., Kolesnikov, V., & Rosulek, M. (2018). A Pragmatic Introduction to Secure Multi-Party Computation. *Foundations and Trends® in Privacy and Security*, *2*(2–3), 70–246. https://doi.org/10.1561/3300000019

Fielt, E., Westerveld, P., Desouza, K., & Gable, G. (2018). Business model innovation and strategic transformation when confronting digital disruption: The case of data-driven business models for professional services. *ACIS 2018 - 29th Australasian Conference on Information Systems*. https://doi.org/10.5130/acis2018.ay

Frikken, K., Atallah, M., & Zhang, C. (2005). Privacy-preserving credit checking. *Proceedings of the ACM Conference on Electronic Commerce*, 147–154. https://doi.org/10.1145/1064009.1064025

Frith, D., & Tapinos, E. (2020). Opening the 'black box' of scenario planning through realist synthesis. *Technological Forecasting and Social Change*, *151*(October 2019), 1–12. https://doi.org/10.1016/j.techfore.2019.119801

Gnatzy, T., & Moser, R. (2012). Scenario development for an evolving health insurance industry in rural India: INPUT for business model innovation. *Technological Forecasting and Social Change*, *79*(4), 688–699. https://doi.org/10.1016/j.techfore.2011.08.001

Goldreich, O., Micali, S., & Wigderson, A. (1987). How to Plan any Mental Game or A Completeness Theorem for Protocols with Honest Majority. *Networks*.

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220–265. https://doi.org/10.1080/07421222.2018.1440766

Gomber, P., Koch, J. A., & Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. *Journal of Business Economics*, *87*(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x

Government of the Netherlands. (n.d.). *Brexit: where do we stand? | Brexit | Government.nl*. Retrieved April 29, 2020, from https://www.government.nl/topics/brexit/brexit-where-do-we-stand

Günther, W. A., Rezazade Mehrizi, M. H., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. *Journal of Strategic Information Systems*, *26*(3), 191–209. https://doi.org/10.1016/j.jsis.2017.07.003

Haaften, W. Van, Sangers, A., Engers, T. Van, & Djafari, S. (2020). *COPING WITH THE GENERAL DATA PROTECTION REGULATION ; ANONYMIZATION THROUGH MULTI-PARTY COMPUTATION TECHNOLOGY*. 1–10.

Haaker, T., Bouwman, H., Janssen, W., & de Reuver, M. (2017). Business model stress testing: A practical approach to test the robustness of a business model. *Futures*, *89*(August 2018), 14–25. https://doi.org/10.1016/j.futures.2017.04.003

Hartmann, P. M., Zaki, M., Feldmann, N., & Neely, A. (2014). Capturing Value from Big Data - A Taxonomy of Data-Driven Business Models Used by Start-Up. *International Journal of Operations and Production Management*.

Hilbig, R., Etsiwah, B., & Hecht, S. (2018). Berlin Start-ups – The Rise of Data-Driven Business Models. *Proceedings of ISPIM Conferences*, *December*, 1–19.

http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=134157647&site=ehost-live

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, *15*(9), 1277–1288. https://doi.org/10.1177/1049732305276687

Hunke, F., & Engel, C. (2018). Utilizing Data and Analytics to Advance Service: Towards Enabling Organizations to Successfully Ride the Next Wave of Servitization. *Exploring Service Science, 9th International Conference, IESS 2018 (Vol. 331)*, *July*. https://doi.org/10.1007/978-3-030-00713-3

Hunke, F., Seebacher, S., Schuritz, R., & Illi, A. (2017). Towards a process model for data-driven business model innovation. *Proceedings - 2017 IEEE 19th Conference on Business Informatics, CBI 2017*, *1*, 150–157. https://doi.org/10.1109/CBI.2017.43

Hunke, F., & Wambsganß, T. (2017). Turning Data into Value: Towards an Ideation Tool for Key Activities of Data-Driven Business Models. *3rd Karlsruhe Service Summit Research Workshop*, *September*, 0–6. https://publikationen.bibliothek.kit.edu/1000077554

ING. (2018). *ING reaches settlement agreement with Dutch authorities on regulatory issues in the ING Netherlands business | ING*. https://www.ing.com/Newsroom/News/Press-releases/ING-reaches-settlement-agreement-with-Dutch-authorities-on-regulatory-issues-in-the-ING-Netherlands-business.htm

Johansen, I. (2018). Scenario modelling with morphological analysis. *Technological Forecasting and Social Change*, *126*(February 2017), 116–125. https://doi.org/10.1016/j.techfore.2017.05.016

Kanger, L., & Pruulmann-Vengerfeldt, P. (2015). Social need for secure multiparty computation. *Applications of Secure Multiparty Computation*, *13*, 43–57. https://doi.org/10.3233/978-1-61499-532-6-43

Kersti, N. (2014). Research Strategy Development for Dummies : Define a Framework of Research Options and then Use It Research Strategy. *6th European Conference on Research Methodology for Business and Management Studies*, *February*, 1–12.

Kobler, D., Bucherer, S., & Schlotmann, J. (2016). Banking business models of the future. *Deloitte*, *Gennaio*(20), 1–8. https://www2.deloitte.com/lu/en/pages/investment-management/articles/banking-business-models-of-the-future.html

Kok, C., Móré, C., & Petrescu, M. (2016). *Recent trends in euro area banks' business models and implications for banking sector stability* (Vol. 33, Issue 2).

Kühne, B., & Böhmann, T. (2019). Data-Driven Business Models - Building the Bridge Between Data and Value. *ECIS 2019 Proceedings*, *April*, 1–16. https://aisel.aisnet.org/ecis2019_rp/167

Kühne, B., & Böhmann, T. (2018). Requirements for Representing Data-Driven Business Models - Towards Extending the Business Model Canvas. *Americas Conference on Information Systems 2018: Digital Disruption, AMCIS 2018*, *Zolnowski 2015*, 1–10.

Kühne, B., Zolnowski, A., Bornholt, J., & Böhmann, T. (2019). Making Data Tangible for Data-driven Innovations in a Business Model Context. *25th Americas Conference on Information Systems, AMCIS 2019*, *August*.

Lambert, S. C., & Davidson, R. A. (2013). Applications of the business model in studies of enterprise success, innovation and classification: An analysis of empirical research from

1996 to 2010. *European Management Journal*, *31*(6), 668–681. https://doi.org/10.1016/j.emj.2012.07.007
Lavie, D. (2006). The competitive advantage of interconnected firms: An extension of the resource-based view. *Academy of Management Review*, *31*(3), 638–658. https://doi.org/10.5465/AMR.2006.21318922
Lee, I., & Shin, Y. J. (2018). Fintech: Ecosystem, business models, investment decisions, and challenges. *Business Horizons*, *61*(1), 35–46. https://doi.org/10.1016/j.bushor.2017.09.003
Lindell, Y., & Pinkas, B. (2009). Secure Multiparty Computation for Privacy-Preserving Data Mining. *Journal of Privacy and Confidentiality*, *1*(1), 59–98.
Lueg, R., Schmaltz, C., & Tomkus, M. (2019). BUSINESS MODELS IN BANKING : A CLUSTER ANALYSIS USING ARCHIVAL DATA. *TRAMES*, *23(73/68)*(1), 79–107.
Mathis, K., & Köbler, F. (2016). Data-Need Fit-Towards data-driven business model innovation. *Proceedings of the 5th Service Design and Innovation Conference*, 458–467. http://www.ep.liu.se/ecp/article.asp?issue=125&article=037%0Ahttps://www.excell-mobility.de/wp-content/uploads/2017/11/ecp16125037.pdf
Micheletti, G., & Pepato, C. (2019). D2.6 Second interim report The European data market monitoring tool: key facts & figures, first policy conclusions, data landscape and quantified stories. In *European Commission – DG Connect* (Issue June).
Mizrahi, T. (n.d.). *Unbound Listed in 5 Gartner Hype Cycle Reports, 2nd Year in A Row | Unbound*. Retrieved April 23, 2020, from https://www.unboundtech.com/unbound-listed-5-gartner-hype-cycle-reports-2nd-year-row/
Narayanan, S., Marucheck, A. S., & Handfield, R. B. (2009). Electronic data interchange: Research review and future directions. *Decision Sciences*, *40*(1), 121–163. https://doi.org/10.1111/j.1540-5915.2008.00218.x
NVB. (2019). *Dutch banks join forces to combat money laundering*. https://www.nvb.nl/english/dutch-banks-join-forces-to-combat-money-laundering/
O'Brien, F. A., & Meadows, M. (2013). Scenario orientation and use to support strategy development. *Technological Forecasting and Social Change*, *80*(4), 643–656. https://doi.org/10.1016/j.techfore.2012.06.006
Oliver, C. (1990). Determinants of Interorganizational Relationships: Integration and Future Directions. *Academy of Management Review*, *15*(2), 241–265. https://doi.org/10.5465/amr.1990.4308156
Osterwalder, A. (2004). *The Business Model Ontology - a proposition in a design science approach.*
Osterwalder, A., Pigneur, Y., & Tucci, C. L. (2005). Clarifying Business Models: Origins, Present, and Future of the Concept. *Communications of the Association for Information Systems*, *15*(1).
Petralia, K., Philippon, T., Rice, T., & Véron, N. (2019). Banking disrupted?: Financial intermediation in an era of transformational technology. In *Geneva Reports on the World Economy* (Vol. 2019, Issue 22).
Pohle, G., & Chapman, M. (2006). IBM's global CEO report 2006: Business model innovation matters. *Strategy and Leadership*, *34*(5), 34–40. https://doi.org/10.1108/10878570610701531
Premchand, A., & Choudhry, A. (2019). Open banking and APIs for transformation in banking.

*Proceedings of the 2018 International Conference On Communication, Computing and Internet of Things, IC3IoT 2018*, 25–29. https://doi.org/10.1109/IC3IoT.2018.8668107
PwC. (2016a). *Financial Services Risk and Regulation FSRR Hot Topic*.
PwC. (2016b). *Financial Services Technology 2020 and Beyond: Embracing Disruption*. https://doi.org/10.1061/ciegag.0001345
Rabobank Tech Labs. (2020). *Technology Trend Report 2020 Tech Lab*.
Ritchey, T. (2006). Problem structuring using computer-aided morphological analysis. *Journal of the Operational Research Society*, *57*(7), 792–801. https://doi.org/10.1057/palgrave.jors.2602177
Ritchey, Tom. (2015). Principles of Cross-Consistency Assessment in General Morphological Modelling. *Acta Morphologica Generalis*, *4*(2), 1–20. http://www.amg.swemorph.com/pdf/amg-4-2-2015.pdf
Ritter, T., & Lettl, C. (2018). The wider implications of business-model research. *Long Range Planning*, *51*(1), 1–8. https://doi.org/10.1016/j.lrp.2017.07.005
Robey, D., Im, G., & Wareham, J. D. (2008). Theoretical foundations of empirical research on interorganizational systems: Assessing past contributions and guiding future directions. *Journal of the Association for Information Systems*, *9*(9), 497–518. https://doi.org/10.17705/1jais.00171
Sadovskyi, O., Engel, T., Heininger, R., Böhm, M., & Krcmar, H. (2014). Analysis of big data enabled business models using a value chain perspective. *Tagungsband Multikonferenz Wirtschaftsinformatik 2014, MKWI 2014*, 1125–1137.
Saldaña, J. (2013). The Coding Manual for Qualitative Researchers. In *International Journal*. https://doi.org/10.1017/CBO9781107415324.004
Sangers, A., Heesch, M. Van, Attema, T., & Veugen, T. (2019). *Secure Multiparty PageRank Algorithm for Collaborative Fraud Detection*. *1*, 605–623. https://doi.org/10.1007/978-3-030-32101-7
Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). Research Methods for Business Students Eighth Edition. In *Qualitative Market Research: An International Journal* (Vol. 3, Issue 4). https://doi.org/10.1108/qmr.2000.3.4.215.2
Schilling, M. A. (2017). *Strategic Management of Technological Innovation* (Fifth). Mcgraw-Hill Education.
Schmidt, J., Drews, P., & Schirmer, I. (2018). Charting the emerging business ecosystem of fintechs and banks: Seven types of collaborative business models. *26th European Conference on Information Systems: Beyond Digitization - Facets of Socio-Technical Change, ECIS 2018*.
Schoemaker, P. J. H. (1995). Scenario planning: a tool for strategic thinking. *Long Range Planning*, *28*(3), 117. https://doi.org/10.1016/0024-6301(95)91604-0
Schoemaker, P. J. H., & Mavaddat, V. M. (2000). Scenario planning for disruptive technologies. *Wharton on Managing Emerging Technologies*, *January 2000*, 206–241.
Schroeder, R. (2016). Big data business models: Challenges and opportunities. *Cogent Social Sciences*, *2*(1), 1–15. https://doi.org/10.1080/23311886.2016.1166924
Schuritz, R., & Satzger, G. (2016). Patterns of Data-Infused Business Model Innovation. *Proceedings - CBI 2016: 18th IEEE Conference on Business Informatics*, *1*(November 2017), 133–142. https://doi.org/10.1109/CBI.2016.23

Schüritz, R., Seebacher, S., & Dorner, R. (2017). Capturing Value from Data: Revenue Models for Data-Driven Services. *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*, 5348–5357. https://doi.org/10.24251/hicss.2017.648

Sekaran, U., & Bougie, R. (2016). Research Methods for Business: A Skill-building Approach. In *Wiley* (Seventh). John Wiley & Sons.

Shafer, S. M., Smith, H. J., & Linder, J. C. (2005). The power of business models. *Business Horizons*, *48*(3), 199–207. https://doi.org/10.1016/j.bushor.2004.10.014

Sorescu, A. (2017). Data-Driven Business Model Innovation. *Journal of Product Innovation Management*, *34*(5), 691–696. https://doi.org/10.1111/jpim.12398

Srinivas, V., Schoeps, J.-T., Ramsay, T., Wadhwani, R., Hazuria, S., & Jain, A. (2019). *2020 Banking and Capital Markets Outlook: Fortifying the core for the next wave of disruption*. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/banking-industry-outlook.html

Stempel, J., Sims, T., & O'Donnell, J. (2020). *Epstein red flags, Russian models land Deutsche Bank $150 million fine - Reuters*. https://www.reuters.com/article/us-deutsche-bank-settlement/epstein-red-flags-russian-models-land-deutsche-bank-150-million-fine-idUSKBN2481WB

Teece, D. J. (2010). Business models, business strategy and innovation. *Long Range Planning*, *43*(2–3), 172–194. https://doi.org/10.1016/j.lrp.2009.07.003

United Nations Office on Drugs and Crime (UNODC). (2011). Estimating Illicit Financial Flows Resulting from Drug Trafficking and other Transnational Organized Crimes. *Research Report (Final Drfat)*, *October*, 1–140. http://www.google.co.uk/url?sa=t&rct=j&q=estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes&source=web&cd=1&cad=rja&ved=0CDIQFjAA&url=http%3A%2F%2Fwww.unodc.org%2Fdocuments%2Fdata-and-analysis%2FStu

van den Broek, T., & van Veenstra, A. F. (2018). Governance of big data collaborations: How to balance regulatory compliance and disruptive innovation. *Technological Forecasting and Social Change*, *129*(November 2016), 330–338. https://doi.org/10.1016/j.techfore.2017.09.040

Van Der Heijden, K. (1996). *Scenarios: The Art of Strategic Conversation*. John Wiley & Sons.

Viorica, I. (2013). Recent Evolution and Predictable Trends of the Banking Industry's Future Inside the European Space. *Procedia - Social and Behavioral Sciences*, *93*, 842–846. https://doi.org/10.1016/j.sbspro.2013.09.290

Voelpel, S. C., Leibold, M., & Tekie, E. B. (2004). The wheel of business model reinvention: how to reshape your business model to leapfrog competitors. *Journal of Change Management*, *4*(3), 259–276. https://doi.org/10.1080/1469701042000212669

Volgushev, N., Schwarzkopf, M., Lapets, A., & Varia, M. (2016). *DEMO: Integrating MPC in Big Data Workflows*. https://doi.org/10.1145/2976749.2989034

Watanabe, Y., & Koseki, A. (2014). A financial risk evaluation service for integrating private portfolios securely. *Proceedings of 2014 IEEE International Conference on Service Operations and Logistics, and Informatics, SOLI 2014*, 59–64. https://doi.org/10.1109/SOLI.2014.6960694

Wayland, R. (2019). Three senses of paradigm in scenario methodology: A preliminary

framework and systematic approach for using intuitive logics scenarios to change mental models and improve strategic decision-making in situations of discontinuity. *Technological Forecasting and Social Change*, *146*(March 2016), 504–516. https://doi.org/10.1016/j.techfore.2017.09.005

Wirtz, B. W., Pistoia, A., Ullrich, S., & Göttel, V. (2016). Business Models: Origin, Development and Future Research Perspectives. *Long Range Planning*, *49*(1), 36–54. https://doi.org/10.1016/j.lrp.2015.04.001

Wixom, B. H., & Ross, J. W. (2017). How to monetize your data. *MIT Sloan Management Review*, *58*(3), 10–13. https://doi.org/10.7551/mitpress/11633.003.0009

Wright, G., Cairns, G., & Bradfield, R. (2013). Scenario methodology: New developments in theory and practice. Introduction to the Special Issue. *Technological Forecasting and Social Change*, *80*(4), 561–565. https://doi.org/10.1016/j.techfore.2012.11.011

Wynn Jr., D., & Williams, C. K. (2012). Principles for Conducting Critical Realist Case Study Research in Information Systems. *MIS Quarterly: Management Information Systems*, *36*(3), 787–810. https://doi.org/10.1016/j.ijproman.2012.11.012

Yao, A. C. (1982). Protocols for Secure Computations. *Annual Symposium on Foundations of Computer Science - Proceedings*, 160–164. https://doi.org/10.1109/sfcs.1982.38

Yin, R. K. (2018). Case study research and applications: Design and methods 6th ed. In *SAGE*.

Zolnowski, A., Anke, J., & Gudat, J. (2017). Towards a Cost-Benefit-Analysis of Data-Driven Business Models. *13th International Conference on Wirtschaftsinformatik (WI 2017)*, 181–195.

Zolnowski, A., Christiansen, T., Gudat, J., & Zolnowski, R. (2016). BUSINESS MODEL TRANSFORMATION PATTERNS OF DATA-DRIVEN INNOVATIONS. *Association for Information Systems AIS Electronic Library (AISeL)*, *Research Papers*. http://aisel.aisnet.org/ecis2016_rphttp://aisel.aisnet.org/ecis2016_rp/146

Zott, C., & Amit, R. (2010). Business model design: An activity system perspective. *Long Range Planning*, *43*(2–3), 216–226. https://doi.org/10.1016/j.lrp.2009.07.004

# Appendix A: Literature Review Method

## MPC Selection and Search Criteria

An exploratory Scopus review was used to ensure that populated results were relevant and hard coded to my search criteria as opposed to Google Scholar. Firstly, on account of secure MPC or MPC as being an emerging topic, I started my search very broadly with "Multi-party computation". 2,247 results populated which ensured me that I could narrow down my search criteria. Secondly, I limited my search to conference papers, conference reviews, and articles which populated with 2,189 sources. Thirdly, I limited all sources to English. Fourthly, I applied requirements whereby keywords should contain "secure M-PC", "MPC", and "Secure MPC". This narrowed the papers down to 1548. Many early theories and frameworks of MPC are based in the context of computer science and mathematics. In order to focus on business issues from a management perspective, the papers were filtered to the subject area of Business Management and Accounting. The end result was 24 papers in which I stopped refining results in general search terms for MPC. Every abstract was carefully considered and evaluated to determine relevancy and utility in the research domain and objective. Moreover, duplicate articles were also discarded. The number of citations or hits that a paper received were not considered as a factor in the search criteria with the assumption that MPC is a new and emerging topic that has not been fully realized and adopted to date. Conference reviews and papers were included in the search to gain the most updated industry knowledge from researchers and practitioners in MPC.

Many of these papers mention the applications of MPC and its technological viability in today's societal needs. On the other hand, the majority of these papers focused on validating mathematical algorithms and proofing the concept of MPC. These papers are more useful for practitioners and researchers whose main objective and focus is to develop their own MPC protocol or demo (Lindell & Pinkas, 2009). However, that is not the objective of this literature review or the aim for this research thesis. Thus, business related bibliographic sources that were referenced in relevant papers were also considered and evaluated by their abstract. The relevancy and utility of the bibliographic sources within these papers have also contributed 10 useful papers which have increased over the course of the iterative research and writing process.

## Business Models Selection and Search Criteria

In order to contextualize MPC from a business perspective and to investigate the business potential of MPC, business models were added as a subject of literature review. Peer-reviewed journal articles regarding business models were firstly selected from prior coursework from the Management of Technology master program, in particular Osterwalder's (2004) Business Model Canvas and the STOF model from Bouwman, De Vos, Haaker & De Reuver (2008). Given the extensive academic literature on business models, literature reviews of business models were used a foundation for bibliographic sources. The most commonly cited sources within other peer-reviewed literature reviews were considered according to relevancy in the abstract towards e-business and innovation and then selected according to paper content. Moreover, an exploratory study about the impact of technology enabled services on business models in the automotive industry by Athanasopoulou, De Reuver, Nikou, & Bouwman (2019) was used as a bibliographic reference. This article was chosen as a cross-reference for sources due to its similarity in research interest to understand the implications of technology X on business models in industry Y. These articles were chosen for practical relevance with the assumption that most organizations and firms adopt the more commonly known business models. Since data-sharing and data analytics are also key characteristics of MPC, data-driven business models were also selected as a part of the scope for this review.

Firstly, I applied a broad Scopus search with “data driven business models”. Secondly, I narrowed these results by limiting the selection criteria to “business management”, “English”, and “Innovation” in order to derive business models grounded in data and innovation. This produced a populated search result of 24 articles. Thirdly, I reviewed the abstracts of these papers but only selected two relevant papers according to the research scope. Fourthly, I used Google Scholar as a secondary search engine in which I applied an advanced search. In order to ensure that the focus of the article or research was solely focused on data driven business models, I selected my search to ensure that the title must contain “data driven business models”. Conference papers and reports were considered as well given that the present state of academic research in this domain is limited. In total, 40 papers were considered for this review of data driven business models.

A Scopus search was repeated to find business models in the finance or banking industry by search words “bank business models”, “business models in banks”, “business models in finance industry”, and “banking business models”. In order to narrow the populated search results, ‘banking business models in the EU or Euro area’ and combinations of this phrase were used. Furthermore, recent and up-to-date documents were needed since data-driven business models is a new concept in in itself. Therefore, finding evidence of data related impacts or changes to banking business models were unfounded. Therefore, a Google Scholar and Google Search were used to find articles and documents related to the future of banking and future of business models in banks. Overall, this search resulted in peer reviewed articles, consultancy reports, and reports and webpages from the European Central Bank.

### Interorganizational Systems Selection and Search Criteria

A literature list for interorganizational systems was obtained from a prior research study involving MPC conducted by a PhD student at the Delft University of Technology and the academic supervisor of this thesis. Peer reviewed articles that discussed the theories and concepts that comprised or underpinned the IOS field of study were used. Three papers were the main source for establishing the original concepts and theories for the conceptual framework. These included: Elgarah et al., (2005); Narayanan et al., (2009); Robey et al., (2008). From these papers, referenced sources were also used which produced a total of 9 papers related to IOS.

### Value Creation Selection and Search Criteria

Research for value creation needed to be placed within the frame and context of IOS and business models. Therefore, papers related to this topic were pulled from references and bibliographies from the abovementioned domains. The papers and authors that were referenced most frequently across these domains in business models, DDBM, and IOS were selected as a starting point for knowledge and research. Upon further reading about value creation, papers from this reference section were used as well; most notably from authors Christoph Zott, Raphael Amit, David J. Teece, and Jay Barney. These papers were also checked for number of hits or citations as a means to find the most reputable sources. Papers discussing value creation from a data-driven perspective were not selected by number of citations given that it is an emerging academic field and discipline. In total, 18 papers were considered for this section of the literature review.

Google Scholar was used to obtain papers that were selected from bibliographies of other authors in the MPC or business model domains in the instances that these articles were not immediately visible in

Scopus. Evidently, articles that could not be accessed via Scopus, Google Scholar and Google searches were not included in this review.

# Appendix B: Extended Literature Review

## Value creation drivers in the context of IOS and MPC data sharing mechanisms

**Efficiency**

Firstly, efficiency is based on transaction costs economics theory and it can be characterized by enhanced ability to execute the transaction and reduce transaction costs (Amit & Zott, 2001). Whereas, transaction cost theory is concerned with the type of governance that enables these transactions (Amit & Zott, 2001). These types of governance can either be hierarchical or market-based or a hybrid of these governance mechanisms (Amit & Zott, 2001; Elgarah et al., 2005). Hierarchical based transactions are governed by managerial decisions and internalized within the firm (Amit & Zott, 2001; Elgarah et al., 2005). Conversely, a market governance structure is characterized by transactions that occur within the market. These governance decisions are determined by the transaction costs that will either decrease or increase coordination costs for the organization and therefore, inform how value is extracted.

In e-businesses and virtual markets, strategic networks and hybrid governance modes provide a greater range of possibilities to create value. In the context of IOS, transaction cost economics is used to describe the economic efficiency of data exchange between firms by either transaction efficiency or reduced transaction costs (Elgarah et al., 2005). IOS supports either hybrid structures or market-based mechanisms for data exchange rather than hierarchical structures because it affords a higher degree of transactions for lower costs enabled by system capabilities and information technologies (Elgarah et al., 2005; Robey et al., 2008). Although transaction efficiency can be a value driver for IOS and e-businesses, these theoretical constructs are more directly linked to the governance of IOS. Therefore, the efficiency construct may have less weight and bearing on value creation that can explain the strategic and social outcomes of MPC implementation.

Moreover, the governance structure can impact the social outcomes of IOS and cooperation based on perceptions of trust and relationship quality (Robey et al., 2008). However, the key characteristic of MPC allow firms to secretly share data which can enable trust and improved cooperation. Hence, other value drivers from Amit & Zott's (2001) value creation framework, may take precedence in influencing the strategic outcomes that may lead to business model innovation for MPC systems.

**Complementarities**

Secondly, another source of value creation is complementarities or complementary goods which are additional goods and/or services that create more value when combined or coupled with another good (Schilling, 2017). When a particular good has a higher number of users or installed base, then complementarities can increase the value of the product for users (Schilling, 2017). Complementarities also holds importance in business model innovation whereby the interdependencies of business model activities can also enhance value (Amit & Zott, 2012).

The complementarities construct is grounded in resource-based view (RBV) theory and network theory (Amit & Zott, 2001). The historical view of RBV theory explains the link between the strategic use of a firm's resources to achieve sustainable competitive advantage (Barney, 1991). However, firm resources such as data can be used by other firms to create value. Moreover, data may not always be controlled or owned by the focal firm. These notions go against traditional RBV theory which postulates that in order to have sustainable competitive advantage, resources should not be mobile. Lavie (2006) extends RBV theory to consider the value of network resources of interconnected firms. This network perspective reassesses the manner in which alliances can enable the mobility of resources to create shared resources and synergies within the network (Lavie, 2006). However, Lavie's (2006) extended model does not inform

how to implement strategies that will create and capture the most value in terms of the degree to which resources are shared or non-shared.

In MPC settings, computational outputs would be considered the good which will increase in value with a higher number of participants or installed base. With the assumption that the correctness and quality of input data is present, then the computations on the pooled data should increase in value with number of participants in the MPC system. In other words, more accurate data should typically result in more informed decision-making which translates to higher value creation. However, complementarities from MPC, if any, depends on the specific use-case which partly informs the degree to which data is shared among network partners.

**Lock-in**

Thirdly, lock-in generally refers to the value-creating attributes that enhance incentives for customers and suppliers to stay and/or increase transactions within the activity system (Amit & Zott, 2001, 2012). The aforementioned theoretical foundations such as transaction cost economics and network theory describe how customer retention and managing customer relationships can provide value through higher transactions. However, this notion is based on the traditional view of exchange of goods between buyers and customers or suppliers. Moreover, network externalities in conventional transactions have positive effects when the value of a good increases with the number of users of that good (Amit & Zott, 2001; Schilling, 2017).

However, participants within MPC settings are not necessarily buying data from other participants or need to manage customer relationships if MPC is used to indirectly improve a bank's internal processes, for example. Network externalities may be only considered within the context of a specific MPC use-case or application and the perspective of the users. For use-cases in secret bidding or auctioning, there may be network externalities that benefit the auctioneer when more users (or bidders) are present which allows the auctioneer to set a higher asking price. However, bidders would have less bargaining power.

There are other potential scenarios in which a high number of MPC users or participants do not result in positive network externalities. For instance, in semi-honest MPC protocols, there is a threshold for the number of dishonest parties within the computation (Archer et al., 2018). An increase in MPC users may result in a shift from having an honest majority in the computation to a dishonest majority which could have implications on the utility and value of the computed output. Moreover, the parameters for MPC environments with dishonest majority of participants results in slower computation speeds which will lower the efficiency benefits for MPC systems (Archer et al., 2018). Lock-in can also include values such as trust, but in some MPC scenarios wherein correctness of output and fairness are compromised can lower the lock-in effect and consequently, value for users.

Therefore, the lock-in concept for MPC needs to be formulated from a data perspective and from the perspective of relationship structures of the participating parties and their roles. Lavie's (2006) resourced based view of interconnected firms places importance on the resource endowments of firms within its network. Whereas in IOS literature, inter-organizational relationship motives or IOR have been used to examine the strategic reasons that motivate firms to participate in data exchange. Oliver's (1990) six different types of relationship motives are summarized in the figure below, adopted from Elgarah et al. (2005, p. 12).

| | |
|---|---|
| Necessity | IORs are established to meet legal or regulatory requirements. |
| Asymmetry | IORs are established in response to power or control of another organization. |
| Reciprocity | IORs are based on cooperation, collaboration and coordination among organizations |
| Efficiency | IORs are prompted to improve the internal input/output ratio of an organization and internal efficiency. |
| Stability | IORs formation is an adaptive response to environmental uncertainty (generated by resource scarcity or lack of perfect knowledge). |
| Legitimacy | IORs are established to appear in agreement with the prevailing norms, rules or expectations of external constituents and/or to improve the image, reputation, prestige. |

*Figure 18: Inter-organizational relationship motive definitions.*

Hence, the potential value from lock-in effects of MPC can only be evaluated from specific contexts of use and the type of relationships within the network environment. The caveats to the conceptual lenses of RBV and IOR may be that it only describes strategic intent of firms and not the actual strategic outcomes of MPC implementation.

**Novelty**

The fourth driver of value creation is novelty which refers to the value creation potential of new transactions structures, new ways of linking business model activities, or novel ways of conducting business (Amit & Zott, 2001, 2012). The extent of deriving value from novelty is interdependent on the aforementioned factors or sources of value creation (Amit & Zott, 2001). Novelty alone cannot be the single source of value creation that will result in business model innovation. Therefore, the effectiveness of efficiency, lock-in, and complementarities are linked and contingent on the extent of novelty and vice-versa.

Efficiency can be evaluated from a system capabilities perspective and from a governance perspective in IOS (Amit & Zott, 2001; Elgarah et al., 2005). Efficiency for MPC systems might be useful in terms of governance structures that enable more efficient and convenient ways of collaborating. Meanwhile, efficiency may be partly constrained due to system capabilities such as the scalability and speed of computations, especially with a high number of participants in one computation. Efficiency is also interdependent on value creation via complementarities for MPC, because more data from different parties will result in more accurate data outputs. However, this depends on the system capabilities and threshold of computing a function as well as the threshold for input parties and dishonest parties. In a dishonest and imperfect MPC system, it constrains the value creation for lock-in effects due to value-laden motives for using MPC i.e. power, trust. Lastly, value creation from novelty is use-case dependent and contingent upon whether MPC can enable new products, services and market entry.

On the other hand, the novelty of MPC can enable firms to collaborate with firms that were previously not possible, perform shared data analytics in a new manner, and/or access data that was formerly inaccessible. Collaboration with new firms can enable incentivized data sharing and increased trust which provide lock-in benefits for MPC use. Access to new data and the ability to use potentially more accurate data analytics can drive value in the form of complementarities. The efficiency of MPC as a new data sharing method cannot be fully assessed since there is a lack of empirical evidence and pilots. However, the benefits from these value drivers are speculative, depending on the context of use, and assuming that MPC has high system capabilities for secure data sharing and analytics.

## Comparison of traditional and network model of RBV theory

The research approach for this thesis includes abducting reasoning. Hence, the approach to developing a conceptual model for MPC implementation will use underlying theories such as RBV.

The traditional resource-based view asserts that a firm's resources must be valuable, rare, imperfectly imitable, and non-substitutable for competitive advantage (Barney, 1991). Valuable is characterized by the exploitive opportunities and enables strategic implementation that neutralizes threats in a firm's environment (Barney, 1991). Rare is defined as having resources and capabilities that are not available to current and potential competition (Barney, 1991). The imperfectly Imitable or inimitable attribute asserts that these resources cannot be copied or implemented by other competitors (Barney, 1991). The non-substitutable attribute asserts that resources cannot be replaced by another firm. However, substitutability can be strategic by having very different firm resources as strategic substitutes or having similar resources that enables a firm to imitate and implement the of strategies competitors (Barney, 1991).

In order to sustain this competitive advantage, resources must be (1) heterogeneous or distinctive from the resources possessed by other firms and (2) immobile or not easily transferred, valued or obtained by other firms (Barney, 1991). However, value creation and IOS implementation is also influenced by network theory (Amit & Zott, 2001; Robey et al., 2008). Therefore, Lavie's (2006) extension of RBV from a network perspective is better suited to understand the value activity mechanisms for MPC. Traditional RBV is focused on the focal firm's inherent resources. These resources (assets, information, knowledge, capabilities) are controlled by the firm and enable the firm to implement strategies that improve its efficiency and effectiveness (Barney, 1991). Whereas Lavie (2006) argues that network resources in the firm's alliance network are significant in deriving strategic opportunities as well. Therefore, value-creating resources are also based on the resources of the firm's collaborators and partners via interfirm alliance (Lavie, 2006). Sustainable competitive advantage in a network context can still be enabled by heterogenous resources, but the mobility of resources across interfirm alliances can benefit new strategies in which resources were formerly inaccessible.

In an IOS context, mobilizing resources is more favorable than controlling resources because more value is derived when resources are configured to respond to competitive and market conditions (Robey et al., 2008). More specifically, "*IOS can be considered to be boundary-spanning capabilities that can be dynamically recombined with other resources to generate greater competitive value"* (Robey et al., 2008, p. 511). Lavie's (2006) extended RBV theory distinguishes between non-shared and shared resources and its role in the appropriation or capture of value within collaborative environments (Lavie, 2006). Lavie (2006) defines two types of interfirm alliances that garners increased competitive formidability and hence, enhanced value creation. Pooling alliances occurs when shared resource sets are substantial to achieve a greater scale of resources and competitive positioning (Lavie, 2006). Complementary alliances arise when firms seek to achieve synergies or complementarities by employing resources that are difficult to accumulate in combination by any given firm (Lavie, 2006). In contrast to pooling alliances, shared resources are minor and less similar to the resources of their partners (Lavie, 2006). However, value distribution and capture may not be equal among firms in the network. Within these alliances, the bargaining power, opportunistic behavior, and competitive position of the focal firm is important in appropriating relational rents or capturing value. If the focal firm has less power or competitive standing compared to other firms then their rents or appropriated value will spill over to other partners and their total rents may be reduced (Lavie, 2006).

IOS relationship motives can help explain or predict the level of appropriated value from MPC based on network and RBV theories. Collaborations that form in an asymmetric or reciprocal manner may be more likely to have better benefits for value creation and capture compared to other IOS relationship typologies. However, the type of innovations (process vs product) that result from MPC settings and the partner firms are interdependent and contextual. This can be explained by Lavie's (2006) notion of pooling alliances or complementary alliances. Furthermore, the degree of value creation can also depend on the scalability of MPC and how many participants can be involved in the joint computation. More participants should result in more value via combined resources in pooling and complementary alliances. However, the scalability of MPC is still lacking in research and development.

Notions from RBV theory provide an understanding of why organizations may choose to collaborate or participate in MPC and how value can be extrapolated and enhanced from an interconnected data sharing environment. The consequences of IOS implementation and interfirm alliances can create value but the implications of these outcomes on new business models need to be further connected to business model innovation research.

## List of business model frameworks

| Authors | BM Context and/or Scope | BM Definition | Contribution | Components/Elements & Characteristics | Citations |
|---|---|---|---|---|---|
| (Chesbrough & Rosenbloom, 2002) | -E-business -activity system perspective | "The business model provides a coherent framework that takes technological characteristics and potentials as inputs, and converts them through customers and markets into economic outputs. The business model is thus conceived as a focusing device that mediates between technology development and economic value creation." (p. 532) | -Framework -Mediating construct between technology and economic value | Value proposition, market segment, value chain, cost structure, profit potential, firm position and value network, competitive strategy | 5585 |
| (Osterwalder, 2004; Osterwalder et al., 2005) | -E-business -Enterprise and value creation perspective (Al-Debei & Avison, 2010) | "conceptual tool containing a set of objects, concepts and their relationships with the objective to express the business logic of a specific firm. It is a description of the value a company offers to one or several segments of customers and of the architecture of the firm and its network of partners for creating, marketing, and delivering this value and relationship capital, to generate profitable and sustainable revenue streams." (Osterwalder et al., 2005, p. 17) | -Business Model Canvas ontology | -Customer segments, value propositions, channels, customer relationships, revenue streams, key resources, key activities, key partnerships, cost structures | 4109 + 3097 |
| (Shafer et al., 2005) | Review and Classification | "a representation of a firm's underlying core logic and strategic choices for creating and capturing value within a value network" (p. 202) | -Comprehensive conceptual literature review | Strategic choices, the value network, creating value, and capturing value. | 2322 |
| (Bouwman et al., 2008) | Services | "blueprint for a service to be delivered, describing the service definition and the intended value for the target group, the sources of revenue, and providing an architecture for the service delivery, including a description of the resources required, and the organizational and financial arrangements between the involved business actors, including a description of their roles and the division of costs and revenues over the business actors" (p. 33) | -Ontology - **S**ervice, **T**echnology, **O**rganization **F**inance (STOF) | Creating value from technology-based services, predominately mobile services | 509 |
| (Al-Debei & Avison, 2010) | Conceptual review | "an abstract representation of an organization… of all core interrelated architectural, co-operational, and financial arrangements designed and developed by an organization presently and in the future, as well all core products and/or services the organization offers, or will offer, based on these arrangements that are needed to achieve its strategic goals and objectives" (p.372) | -Conceptual Framework | value proposition, value architecture, value finance, value network | 821 |
| (Zott & Amit, 2010) | -BM Design -Network and activity system perspective | "a system of interdependent activities that transcends the focal firm and spans its boundaries." | -Conceptual Framework | -grounded in Transaction Cost Economics (TCE) and Resource Based View (RBV) theories | 2798 |
| (Teece, 2010) | Business Model Design | "articulates the logic and provides data and other evidence that demonstrates how a business creates and delivers value to customers. It also outlines the architecture of revenues, costs, and profits associated with the business enterprise delivering that value." (p.173) | -Business Model framework | Business model component perspective | 7237 |
| (El Sawy & Pereira, 2013) | -Digital business -Network perspective | "A business model is a representation of the strategic choices that characterize a business venture…the business model can be seen as a communication or a planning tool" (p.15)<br><br>"VISOR defines how a firm responds to a customer need, latent or established, thus creating and delivering the greatest value to the customer, in a profitable and sustainable manner, and, as such, optimizes costs to value creation" (p. 24) | **V**alue proposition, **I**nterface, **S**ervice Platform, **O**rganizing model, and **R**evenue model (VISOR) | -considers the dynamics of digital business ecosystems in the conceptualization of the VISOR model | 176 |

| | | | | | |
|---|---|---|---|---|---|
| (DaSilva & Trkman, 2014) | -Review and theoretical grounding<br>-activity system perspective | "core of a business model is defined as a combination of resources which through transactions generate value for the company and its customers" (p 383) | -Theoretical framework<br>-conceptual evaluation | -grounded in TCE and RBV theory<br>-business processes and business process engineering | 592 |

*Table 20: Business Model Definitions (2000 – present)*

## List of DDBM in extant literature

| Author | Contribution | Scope; Characteristics |
|---|---|---|
| **(Hartmann et al., 2014)** | Taxonomy, DDBM framework | Data Sources, seven key data activities, offering, target customer, revenue model, specific cost advantage |
| (Sadovskyi et al., 2014) | Conceptual analysis | Value chain perspective for data-driven services |
| **(Bulger et al., 2014)** | Normative DDBM framework | Implications of DDBM |
| **(Brownlow et al., 2015)** | Prescriptive model/framework for BMI | Structural guidelines for constructing DDBMs – industry focused |
| **(Schroeder, 2016)** | DDBM typology | Types of business models and applications; challenges in data ecosystem |
| **(Zolnowski et al., 2016)** | Multiple case study of BMI | Transformation patterns: (1) cooperative value innovation, (2) customer-centric value innovation, (3) cooperative productivity improvement, and (4) company-centric productivity improvement |
| **(Mathis & Köbler, 2016)** | Method/Process Model for BMI | Data Canvas: method for collecting and documenting data<br>Data-Need fit: Process to match data with user needs |
| **(Schuritz & Satzger, 2016)** | Data-infusion framework | patterns of data infused value activities that determine type of BMI |
| **(Wixom & Ross, 2017)** | | Data monetization approaches |
| **(Hunke et al., 2017)** | Process Model DDBMI | Design principles for data-driven BMI |
| **(Hunke & Wambsganß, 2017)** | Tool for ideation of key activities | Key activities: Data collection, data organization, data selection, data preprocessing, data transformation, data mining and interpretation |
| **(Sorescu, 2017)** | Research agenda, conceptual framework | Data-driven value creation and BMI |
| (Schüritz et al., 2017) | Qualitative multi-case analysis | Revenue models for data-driven/based services; value capture |
| **(Benta et al., 2017)** | Process Model for data-driven BMI | Data-enhanced BMC; integration of product development and business model generation |
| (Günther et al., 2017) | Literature Review & integrated Model | Value creation/realization |
| (Zolnowski et al., 2017) | Service Business Model Canvas | Cost-benefit model for DDBM; identification of factors for cost benefit analysis |
| **(Hunke & Engel, 2018)** | Literature Review | Key characteristics of data-enhanced services |
| (Hilbig et al., 2018) | Taxonomy | Low data, data-enhanced, pure data-driven BMs |
| (Fielt et al., 2018) | Scenarios | BMI and strategic transformation; Data-driven professional services |
| **(Böhmecke-schwafert & Niebel, 2018)** | Case study | Applied Hartmann's taxonomy; data portability |
| (Schmidt et al., 2018) | Classification for data-driven fintech business models | Applied Hartmann's taxonomy; data processing model, information processing model, data aggregation model, data analytics model, data distribution model, data value chain model |
| **(Kühne & Böhmann, 2018)** | Literature review, research agenda | DDBM requirements |
| **(Kühne & Böhmann, 2019)** | DDBM Artefact | Value realization and capture; complementary artefact to BMC |
| **(Kühne et al., 2019)** | Extension of BMC and service-based business model | DDBM design principles, DDBM visualization/canvas |

*Table 21: Descriptions of DDBM Literature*

## Appendix C: Interview Protocol – Presentation slides

### Main presentation slides

# What is MPC?

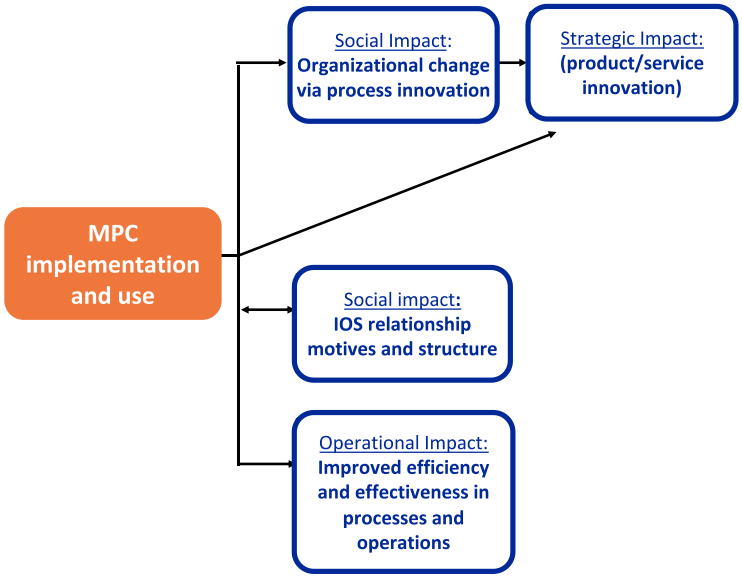
- Secure MPC is a field of cryptography that enables distributed parties to carry out a joint computation on shared data in a secure manner whereby each party's dataset is not revealed to any other party (Ankele et al., 2016; Lindell & Pinkas, 2009).

- In other words, it can enable competing businesses to perform data analytics on shared data whilst keeping their individual datasets private from each other → Privacy preserving data computation and analytics without a trusted third party

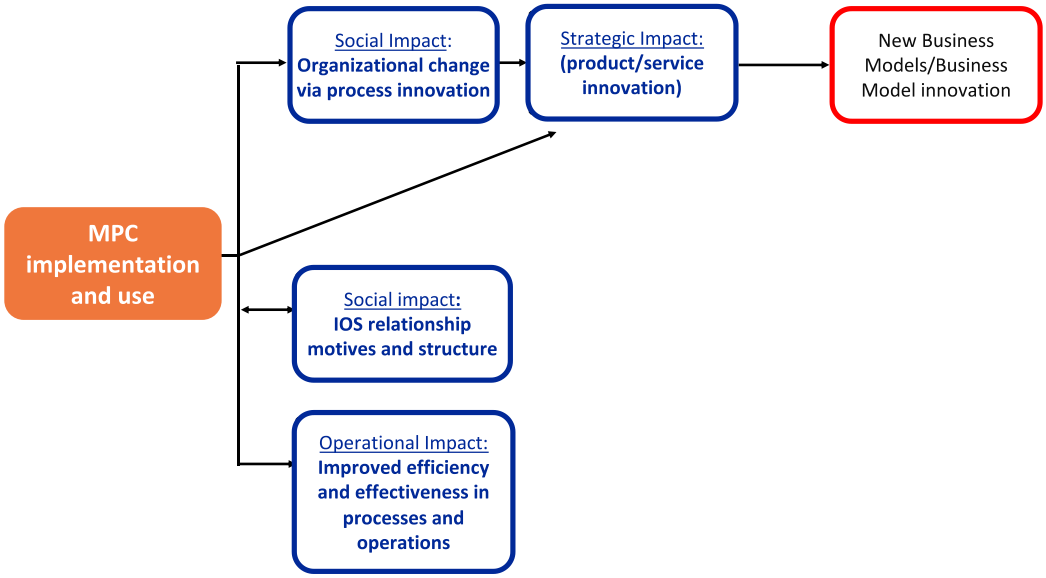
- Example: Andrew Yao's Millionaire Problem

- Use-cases: Fraud and cybersecurity detection

## MPC Organizational Context




## Does MPC enable new business models?



## Uncertainties in implementing MPC in banks

| | |
|---|---|
| Legal and governance structure | • Contractual arrangements: data ownership, re-use capabilities<br>• Risk of liability and data misuse<br>• Data regulation |
| Technology ownership | • Banks outsources MPC or depend on vendors<br>• Open source |
| Incentives | • Data sharing and collaboration incentive<br>• Data incentives (external data, data analytics) |
| Data Requirements | • Type, source, structure, format, etc.<br>• Reliability, correctness<br>• IT modernisation and interoperability |
| Business Models | • B2B/B2C<br>• Revenue models for monetising co-created or shared data |

## Uncertainties in implementing MPC in banks

| | |
|---|---|
| Business Models | • Types of B2B data sharing business models<br>• Revenue models for monetizing co-created or shared data |

- **Data monetization:** Additional revenue from shared data and provision of services e.g. DaaS, AaaS..
- **Data marketplaces:** Trusted intermediary to connect data suppliers and data users to exchange data
- **Industry data platforms:** collaborative and strategic approach to exchange data among a restricted group of companies.
- **Technical enablers:** Revenues gained from developing and offering technical solutions for data exchange
- **Open data:** companies that opt to share data for free to foster the development of new products and/or services.

Arnaut et al. (2018)

# MPC Implementation Scenarios in banks

| | |
|---|---|
| 1. Improves processes and operations | • Cybersecurity threat detection<br>• Better fraud detection<br>• Credit and risk monitoring |
| 2. Enhances existing products, services and technologies | • Privacy preserving data analytics and data aggregation for tech (AI,ML)<br>• Enhances cybersecurity products/services<br>• Enhances other data driven technologies |
| 3. Enables new products and services | • New products/solutions for risk management or security in open banking<br>• New compliance and regulatory solutions<br>• DaaS/AaaS for partnerships/collaboration |
| 4. Assists supervisory/government authorities | • Anti-money laundering/counter terrorist financing reporting<br>• Combating financial crime and fraud |

Presentation Slides for Bank C:

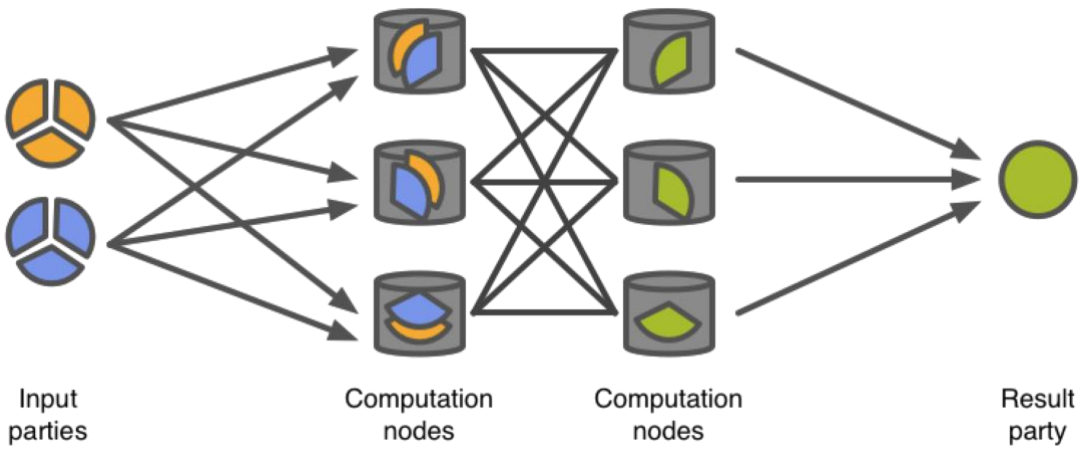
# What is MPC?

- Secure MPC is a collection of cryptographic protocols and computation alogirthms that enables distributed parties to carry out a joint computation on shared data in a secure manner whereby each party's dataset is not revealed to any other party (Ankele et al., 2016; Lindell & Pinkas, 2009).

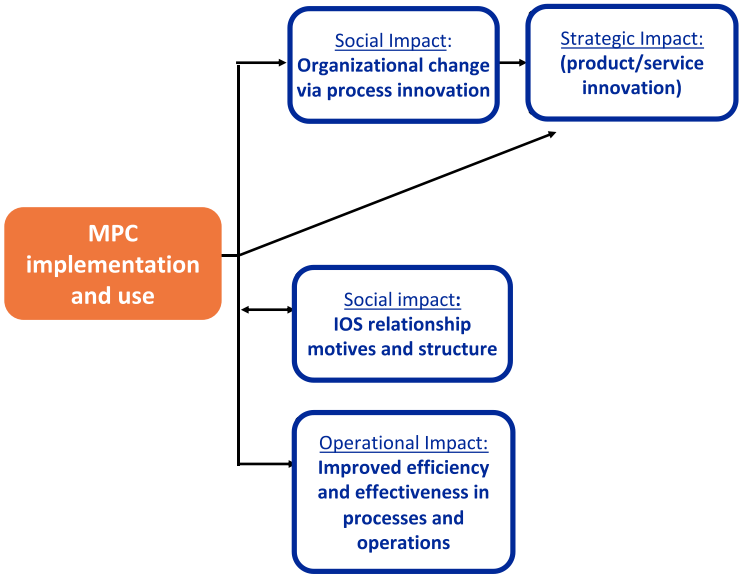
- In other words, it can enable competing businesses to perform data analytics on shared data whilst keeping their individual datasets private from each other

  → Privacy preserving data computation and analytics without a trusted third party

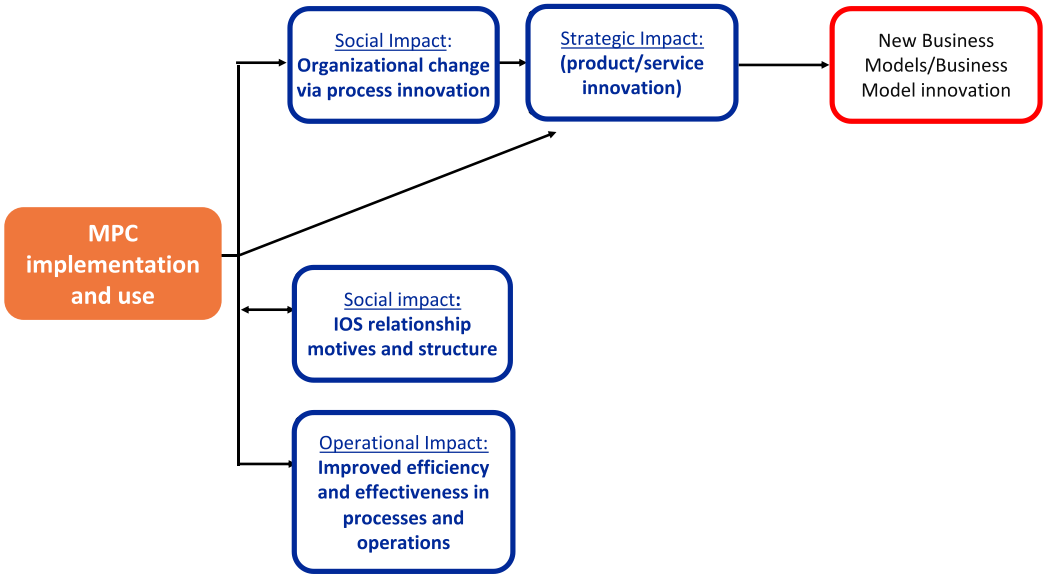
# Example: Andrew Yao's Millionaire Problem



## MPC Organizational Context




## Does MPC enable new business models?



## Business Trends – EU Data Ecosystem

| | |
|---|---|
| Cross-border/sector data sharing | • Access to external datasets for increased competitive advantage<br>• EU single open data market & coopetition |
| Big Data and Analytics | • Continued technical, legal and governance challenges with monetizing data |
| Cloud Storage and Services | • EU to develop cloud service provider market due to heavy dependence on third party service party providers<br>• Rise of edge computing & IoT |
| Cyber-security | • Cyber-security needs are increasing to combat emerging technologies i.e. quantum computing |
| Climate change | • Higher computing power to support increasing digitalization and data usage<br>• Corporate responsibility to reduce carbon emissions |

## Business Trends – EU Banking Ecosystem

| | |
|---|---|
| Low Profitability | • New business models (revenue) and risk mitigation (cost-efficiency) |
| Rising Competition | • Challenged by fintechs and big tech incumbents |
| Growth in payments & mobile services | • PSD2 & Open Banking push for faster and real-time services |
| Rising customer expectations | • Customer empowerment via mobile and digital interfaces<br>• Cross-border transactions |
| Cyber-security & Risk | • Ubiquitous in all banking activities<br>• Open banking creates vulnerabilities in digital channels |
| AML/CTF | • 0.7-1.28% of the EU's GDP is involved in suspicious financial activity<br>• rise of e-identity or digital identity authentication products (KYC) |
| Rising Costs | • Rising compliance and technical costs to compete and maintain trust, security and data |

# Uncertainties in implementing MPC in banks

| | |
|---|---|
| Legal and governance structure | • Contractual arrangements: data ownership, re-use capabilities<br>• Risk of liability and data misuse<br>• Data regulation |
| Incentives | • Data sharing and collaboration incentive<br>• Data incentives (external data, data analytics) |
| Technology ownership | • Banks outsources MPC or depend on vendors<br>• Open source |
| Data Requirements | • Type, source, structure, format, etc.<br>• Reliability, correctness<br>• IT modernisation and interoperability |
| Business Models | • Types of B2B data sharing business models: data monetization; data marketplaces; industry data platforms; technical enablers; open data<br>• Revenue models for monetising co-created or shared data |

# Uncertainties in implementing MPC in banks

| | |
|---|---|
| Business Models | • Types of B2B data sharing business models<br>• Revenue models for monetizing co-created or shared data |

- **Data monetization:** Additional revenue from shared data and provision of services e.g. DaaS, AaaS.
- **Data marketplaces:** Trusted intermediary to connect data suppliers and data users to exchange data
- **Industry data platforms:** collaborative and strategic approach to exchange data among a restricted group of companies.
- **Technical enablers:** Revenues gained from developing and offering technical solutions for data exchange
- **Open data:** companies that opt to share data for free to foster the development of new products and/or services.

# MPC Implementation Scenarios in banks

| | |
|---|---|
| 1. Improves processes and operations | • Cybersecurity threat detection<br>• Better fraud detection<br>• Credit and risk monitoring |
| 2. Enhances existing products, services and technologies | • Privacy preserving data analytics and data aggregation for tech (AI,ML)<br>• Enhances cybersecurity products/services<br>• Enhances other data driven technologies |
| 3. Enables new products and services | • New products/solutions for risk management or compliance in open banking<br>• New security and regulatory solutions<br>• DaaS/AaaS for partnerships/collaboration |
| 4. Assists supervisory/government authorities | • Anti-money laundering/counter terrorist financing reporting<br>• Combating financial crime and fraud |

# Appendix D: Informed Consent Form for Interview Participants

Consent Form for MPC Research Study at TU Delft:

Summary: Secure multi-party computation (MPC) enables secure and private interorganizational data sharing while forgoing the need for a trusted third party. MPC is positioned to enable the European data-driven economy by overcoming privacy, security, and trust issues with sharing confidential or personal data. However, MPC technologies are still in the testing and experimental phases of development. Hence, there is limited research and empirical studies on the implications of MPC implementation and its realized socioeconomic and business value. This study aims to contextualize MPC from a business perspective by evaluating the possible outcomes of MPC in its external and business environment via scenario analysis methods. The scope of the study will be to analyze how MPC can be implemented within banks and if it can enable new data enhanced/driven business models. The expected developments in EU policy and investments for data, value shifts in data privacy, as well as the anticipated paradigm shifts in banks' business models require a future studies assessment. Scenarios will encompass the political, economic, social, technological, legal and environmental driving forces in the data and financial ecosystems. The time and spatial scale for scenario development is short term (5 years) and focused within the EU. The trends and uncertainties derived from research and analysis will be used to evaluate the plausibility of MPC implementations as a technology for data sharing in European banks and whether MPC can be leveraged as means for enabling new business models.

Research Objective: The research objective is to contribute conceptual knowledge to the business model concept, more specifically to data-driven business model ontology, by investigating the future scenarios of MPC implementation and use in banks. This exploratory study aims to understand the implications of MPC on financial risk mitigation and to provide practical insights for banks about how MPC can affect their business models.

| ***Please tick the appropriate boxes (only if you agree)*** | **Yes** | **No** |
|---|---|---|
| **Taking part in the study** | | |
| I have read and understood the study information dated [DD/MM/2020], or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction. | ○ | ○ |
| I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason. | ○ | ○ |
| I understand that taking part in the study involves audio-recorded interviews which will be transcribed for analysis in this study. | ○ | ○ |
| **Use of the information in the study** | | |
| I understand that information I provide will be used for research purposes and published by the Delft University of Technology (Technische Universiteit Delft). Information may also be referenced or used in future research. Audio recordings will not be published or released to the public and will be deleted at the end of the project. | ○ | ○ |

| | | |
|---|---|---|
| I understand that personal information collected about me that can identify me, such as [e.g. my name or email], will not be shared beyond the study team. | ○ | ○ |

**Future use and reuse of the information by others**

| | | |
|---|---|---|
| I give permission for the anonymized interview transcripts and any additional anonymized company information that I provide to be archived in the 4TU Center for Research Data, managed by TU Delft, so it can be used for future research and learning. | ○ | ○ |
| I understand that only the research study team will have safeguarded access to the collected data for future research. | ○ | ○ |
| I understand that any contact information archived will only be used by the researcher(s) for information validation and to report research results. | ○ | ○ |

**Additional Permissions**

| | | |
|---|---|---|
| | ○ | ○ |
| I agree that my information can be quoted in research outputs | ○ | ○ |
| I agree that my real name can be used for quotes | | |

**Signatures**

_____ _____ _____

Name of participant [printed] and legal representative If applicable) Signature Date

*For participants unable to sign their name, mark the box instead of sign*

I have witnessed the accurate reading of the consent form with the potential participant and the individual has had the opportunity to ask questions. I confirm that the individual has given consent freely.

_____ _____ _____

Name of witness [printed] Signature Date

I have accurately read out the information sheet to the potential participant and, to the best of my ability, ensured that the participant understands to what they are freely consenting.

_____ _____ _____

Researcher name [printed] Signature Date

# Appendix E: Coding List Exported from Atlas.ti

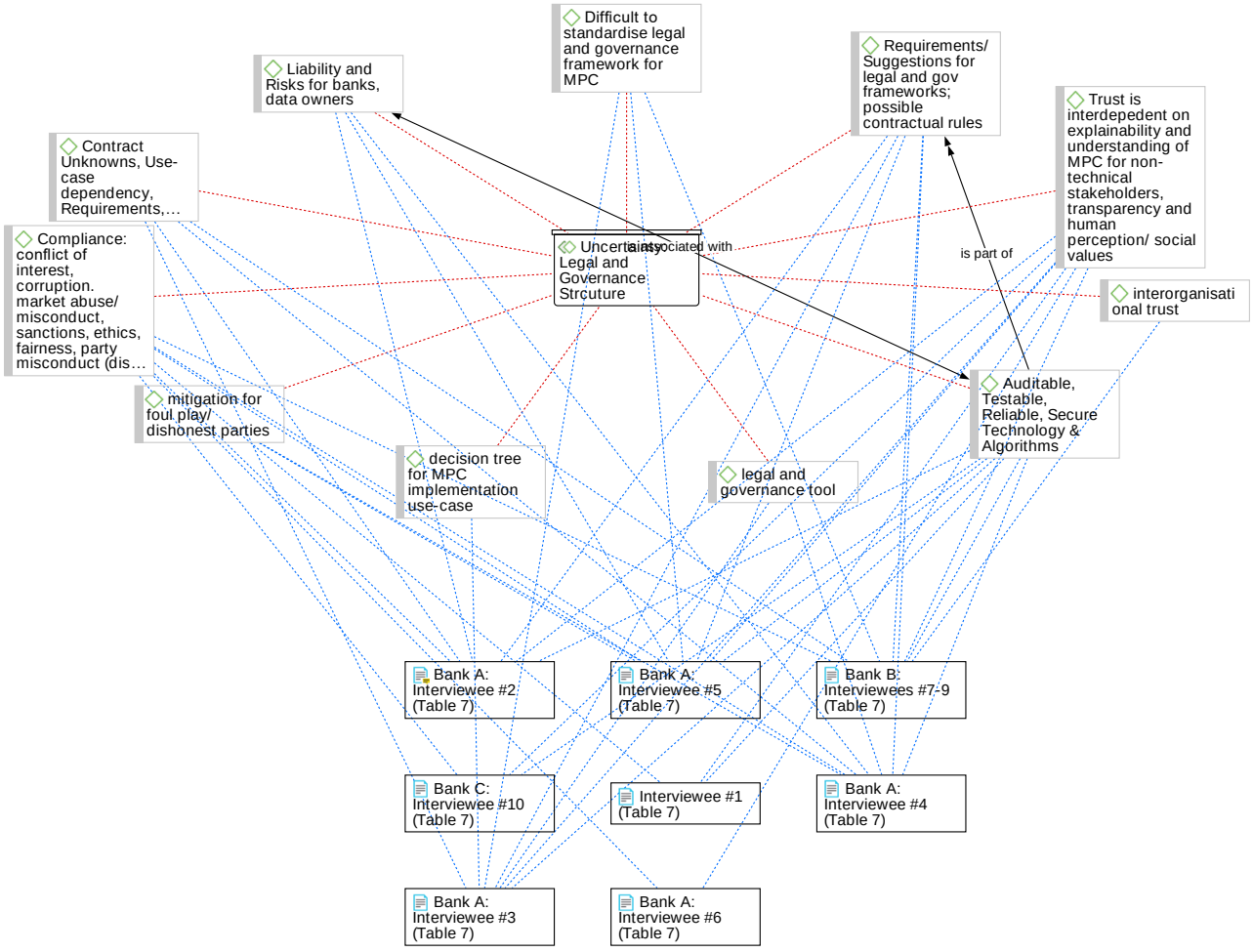
| | Code | Code Group 1 | Code Group 2 | Code Group 3 | Code Group 4 |
|---|---|---|---|---|---|
| 1. | Auditable, Testable, Reliable, Secure Technology & Algorithms | Uncertainty: Legal and Governance Structure | Uncertainty: Technology maturity and Computational ability | Uncertainty: Tech ownership | |
| 2. | B2B | Business Model Components and Characteristics | | | |
| 3. | B2C | Business Model Components and Characteristics | | | |
| 4. | B2G data sharing | Business Model Components and Characteristics | Scenario 4: assists gov/authority/supervisory | | |
| 5. | Bank B use-case project | | | | |
| 6. | benchmarking as potential business model | Uncertainty: Business Models | Scenario 3: enables new products/services | | |
| 7. | Business Incentives for data sharing, leveraging data, type of data shared | Uncertainty: Incentives | | | |
| 8. | business model for vendors and benefits for non-bank entities | Uncertainty: Business Models | Scenario 3: enables new products/services | | |
| 9. | business model, action/decision-making, and implementation is contingent on output | Uncertainty: Business Models | | | |
| 10 | circumvent strict data regulations | Uncertainty: Incentives | | | |
| 11 | Combination of scenario 1,4 | Scenario 4: assists gov/authority/supervisory | Scenario 1: improves processes and ops | | |
| 12 | Common Goal | Uncertainty: Incentives | | | |
| 13 | comparable market value of data | Uncertainty: Data Requirements | Uncertainty: Incentives | | |
| 14 | Competition mechanisms with fintechs/tech companies | Uncertainty: Incentives | | | |
| 15 | Compliance: conflict of interest, corruption. market abuse/misconduct, sanctions, ethics, fairness, party misconduct (dishonest parties) | Uncertainty: Legal and Governance Structure | Uncertainty: Data Requirements | | |
| 16 | computing party on one network | | | | |
| 17 | computation in the cloud: possibilities and drawbacks | | | | |
| 18 | Contract Unknowns, Use-case dependency, Requirements, and Explainability | Uncertainty: Legal and Governance Structure | | | |
| 19 | Corona/COVID implications for rival explanations | | | | |
| 20 | Credit monitoring & Risk Monitoring | Scenario 1: improves processes and ops | Scenario 3: enables new products/services | | |
| 21 | Current/existing product offerings | Uncertainty: Business Models | | | |
| 22 | Customer perception: values/expectations and fairness/ethics | Business Model Components and Characteristics | Uncertainty: Customer Acceptance | | |
| 23 | cybersecurity | Scenario 2: enhances existing products and services, tech | | | |
| 24 | data marketplaces | Uncertainty: Business Models | | | |
| 25 | Data monetization | Uncertainty: Business Models | | | |
| 26 | Data requirements | Uncertainty: Data Requirements | | | |
| 27 | data risk factor | Uncertainty: Customer Acceptance | | | |
| 28 | decision tree for MPC implementation use-case | Uncertainty: Legal and Governance Structure | | | |
| 29 | Details of the data matters in fraud detection/analysis/prosecution | Scenario 1: improves processes and ops | | | |
| 30 | difference between fraud detection and legal proof | Scenario 1: improves processes and ops | | | |
| 31 | differences between social and technical values | | | | |
| 32 | Difficult to standardize legal and governance framework for MPC | Uncertainty: Legal and Governance Structure | | | |
| 33 | EU regulation guidelines for implementation | | | | |
| 34 | Example use-cases /potential business case | Uncertainty: Business Models | Uncertainty: Technology maturity and Computational ability | Scenario 4: assists gov/authority/supervisory | |
| 35 | exchange data with third parties/collab with third parties | Uncertainty: Incentives | | | |
| 36 | explainability | Uncertainty: Customer Acceptance | | | |
| 37 | Fraud Detection/Mitigation/Prevention | Scenario 4: assists gov/authority/supervisory | Uncertainty: Incentives | Uncertainty: Data Requirements | Scenario 1: improves processes and ops |

| | | | | | |
|---|---|---|---|---|---|
| 3 | government ownership | Uncertainty: Tech ownership | | | |
| 3 | Hierarchical governance structure | Uncertainty: Tech ownership | | | |
| 4 | Implementation challenges and barriers: high risk, high investment, data analysis complexity, compliance risks, privacy concerns | | | | |
| 4 | improving fraud detection | Scenario 1: improves processes and ops | | | |
| 4 | incentive for bank customers | Uncertainty: Incentives | | | |
| 4 | incentive for banks | Uncertainty: Incentives | | | |
| 4 | Incentive for supervisory authorities | Scenario 4: assists gov/authority/supervisory | Uncertainty: Incentives | | |
| 4 | inconveniences/disadvantage of current processes | Uncertainty: Business Models | Uncertainty: Incentives | | |
| 4 | indirect business model | Uncertainty: Business Models | | | |
| 4 | industry data platform business model | Uncertainty: Business Models | | | |
| 4 | input data requirements | Uncertainty: Data Requirements | | | |
| 4 | insufficient capability or capacity to build MPC tech | Uncertainty: Tech ownership | | | |
| 5 | integrity detection | | | | |
| 5 | intellectual property | Uncertainty: Tech ownership | | | |
| 5 | interbank interest rate example | | | | |
| 5 | interdependent relationship between use-case, value in data and governance of data | | | | |
| 5 | Internal Efficiency; Improved Efficiency of current operations/processes | Scenario 1: improves processes and ops | | | |
| 5 | Interorganizational data sharing incentive for better results, accessibility to external data, number of parties | Business Model Components and Characteristics | Uncertainty: Incentives | | |
| 5 | interorganizational trust | Uncertainty: Legal and Governance Structure | | | |
| 5 | KYC | Scenario 3: enables new products/services | | | |
| 5 | Lack of Incentive | Uncertainty: Incentives | | | |
| 5 | lack of knowledge and expertise to understand MPC | | | | |
| 6 | legal and governance tool | Uncertainty: Legal and Governance Structure | | | |
| 6 | Lending | Uncertainty: Business Models | Scenario 2: enhances existing products and services, tech | | |
| 6 | Liability and Risks for banks, data owners | Uncertainty: Legal and Governance Structure | Uncertainty: Technology maturity and Computational ability | | |
| 6 | limitations due to data rules | | | | |
| 6 | mitigation for foul play/dishonest parties | Uncertainty: Legal and Governance Structure | | | |
| 6 | MPC as technical enabler | Uncertainty: Business Models | | | |
| 6 | MPC enabled AML | Scenario 4: assists gov/authority/supervisory | | | |
| 6 | MPC implementation contingent on other parties | | | | |
| 6 | MPC platform | Uncertainty: Tech ownership | | | |
| 6 | MPC Technological uncertainty and trust among technical stakeholders is interdependent on maturity, algorithmic security, computational ability | | | | |
| 7 | MPC to improve insurance and finance models | Scenario 2: enhances existing products and services, tech | | | |
| 7 | Mutual Benefit for banks and other parties | Scenario 4: assists gov/authority/supervisory | Uncertainty: Incentives | | |
| 7 | network analysis components | | | | |
| 7 | Non-competition Law | Uncertainty: Business Models | | | |
| 7 | Open banking/PSD2 | Uncertainty: Business Models | Scenario 3: enables new products/services | | |
| 7 | open data policy | Uncertainty: Business Models | | | |
| 7 | Open Source | | | | |
| 7 | output accuracy | Uncertainty: Data Requirements | Uncertainty: Technology maturity and Computational ability | | |
| 7 | output correctness | Uncertainty: Data Requirements | Uncertainty: Technology maturity and Computational ability | | |

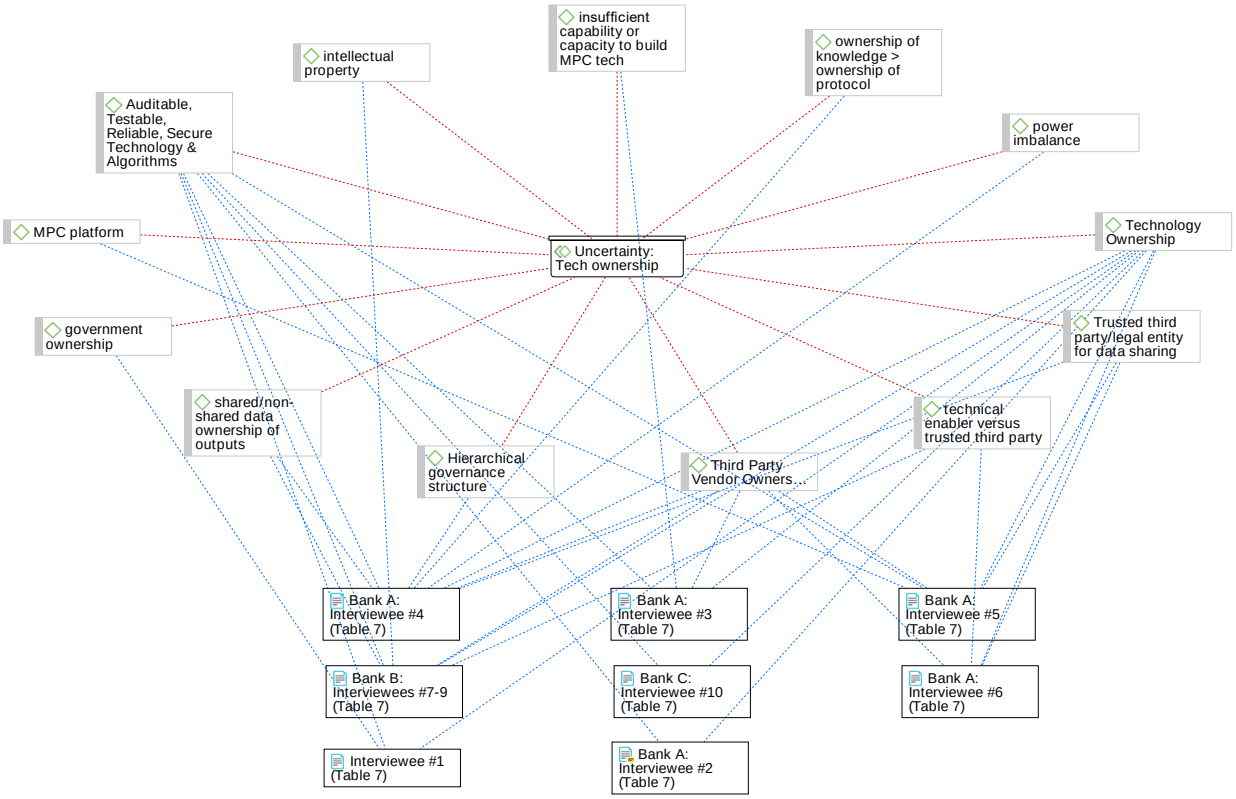
| | | | | | |
|---|---|---|---|---|---|
| 7 | overarching legal framework & extra EU regulation | | | | |
| 8 | ownership of knowledge > ownership of protocol | Uncertainty: Tech ownership | | | |
| 8 | Personal, transaction, customer data | | | | |
| 8 | Possible outcome of MPC products/services/platforms | Business Model Components and Characteristics | Uncertainty: Business Models | Scenario 3: enables new products/services | |
| 8 | potential business model for a bank | Business Model Components and Characteristics | Uncertainty: Business Models | | |
| 8 | Potential MPC enabled customer offering | Business Model Components and Characteristics | Scenario 3: enables new products/services | | |
| 8 | power imbalance | Uncertainty: Tech ownership | | | |
| 8 | prevention rather than prosecution | | | | |
| 8 | Privacy incentive: anonymization of personal/proprietary data and anonymous data sharing (untraceable/secret sharing); secret voting | Uncertainty: Incentives | | | |
| 8 | Privacy preserving data analytics: customer profiles, trend profiles | Business Model Components and Characteristics | | | |
| 8 | recommend better products | Scenario 2: enhances existing products and services, tech | | | |
| 9 | rejection of MPC in payments | Scenario 3: enables new products/services | | | |
| 9 | rejection of possible outcomes/implausibility due to time horizon, technological maturity | | | | |
| 9 | Requirements/Suggestions for legal and gov frameworks; possible contractual rules | Uncertainty: Legal and Governance Structure | | | |
| 9 | researcher assumptions | | | | |
| 9 | risk mitigation | | | | |
| 9 | role delineation of input/output parties | | | | |
| 9 | scenario 1 | Scenario 1: improves processes and ops | | | |
| 9 | scenario 2 | Scenario 2: enhances existing products and services, tech | | | |
| 9 | scenario 3 | | | | |
| 9 | scenario 4 | Scenario 4: assists gov/authority/supervisory | | | |
| 1 | Security Related Use-cases and Data | Uncertainty: Data Requirements | | | |
| 1 | Sensitive Commercial Data | | | | |
| 1 | shared/non-shared data ownership of outputs | Uncertainty: Tech ownership | | | |
| 1 | standardization of MPC technology | Uncertainty: Technology maturity and Computational ability | | | |
| 1 | technical enabler versus trusted third party | Uncertainty: Tech ownership | | | |
| 1 | Technology Ownership | Uncertainty: Tech ownership | | | |
| 1 | Third Party Vendor Ownership | Uncertainty: Tech ownership | | | |
| 1 | Trend validation: data, security, competition | | | | |
| 1 | Trust is interdependent on explainability and understanding of MPC for non-technical stakeholders, transparency and human perception/ social values | Uncertainty: Customer Acceptance | Uncertainty: Legal and Governance Structure | | |
| 1 | Trusted third party/legal entity for data sharing | Uncertainty: Tech ownership | | | |
| 1 | uncertainty about MPC use-case in payments opportunities | Scenario 3: enables new products/services | | | |
| | | | | | |

# Appendix F: Atlas.ti network reports filtered by uncertainty code group

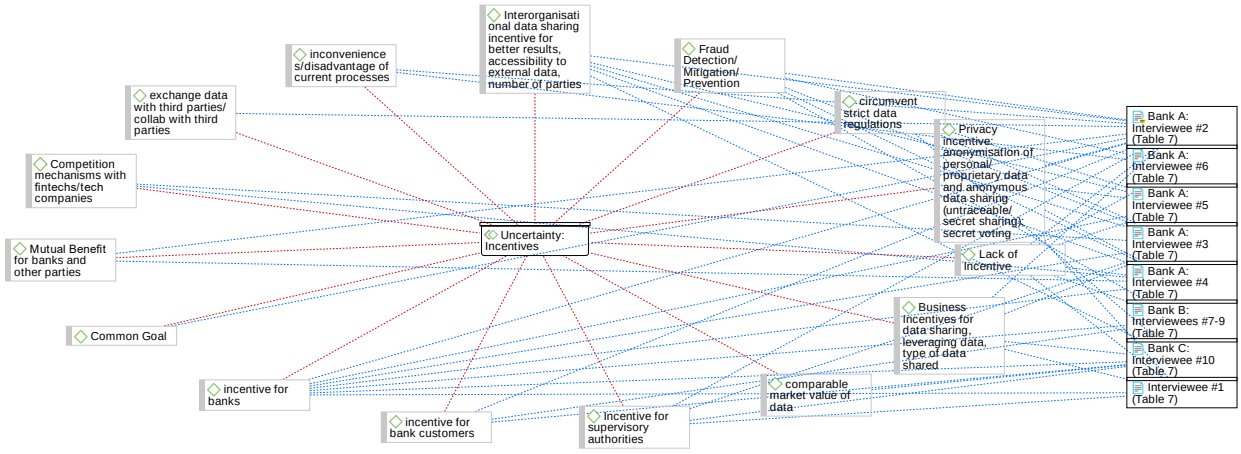
## Legal and Governance Structure



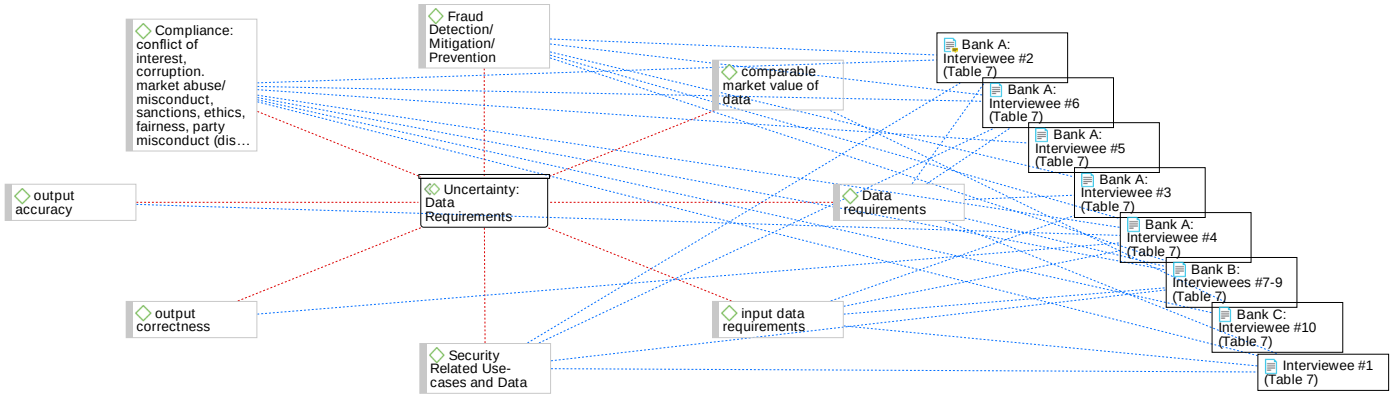
## Technology Ownership



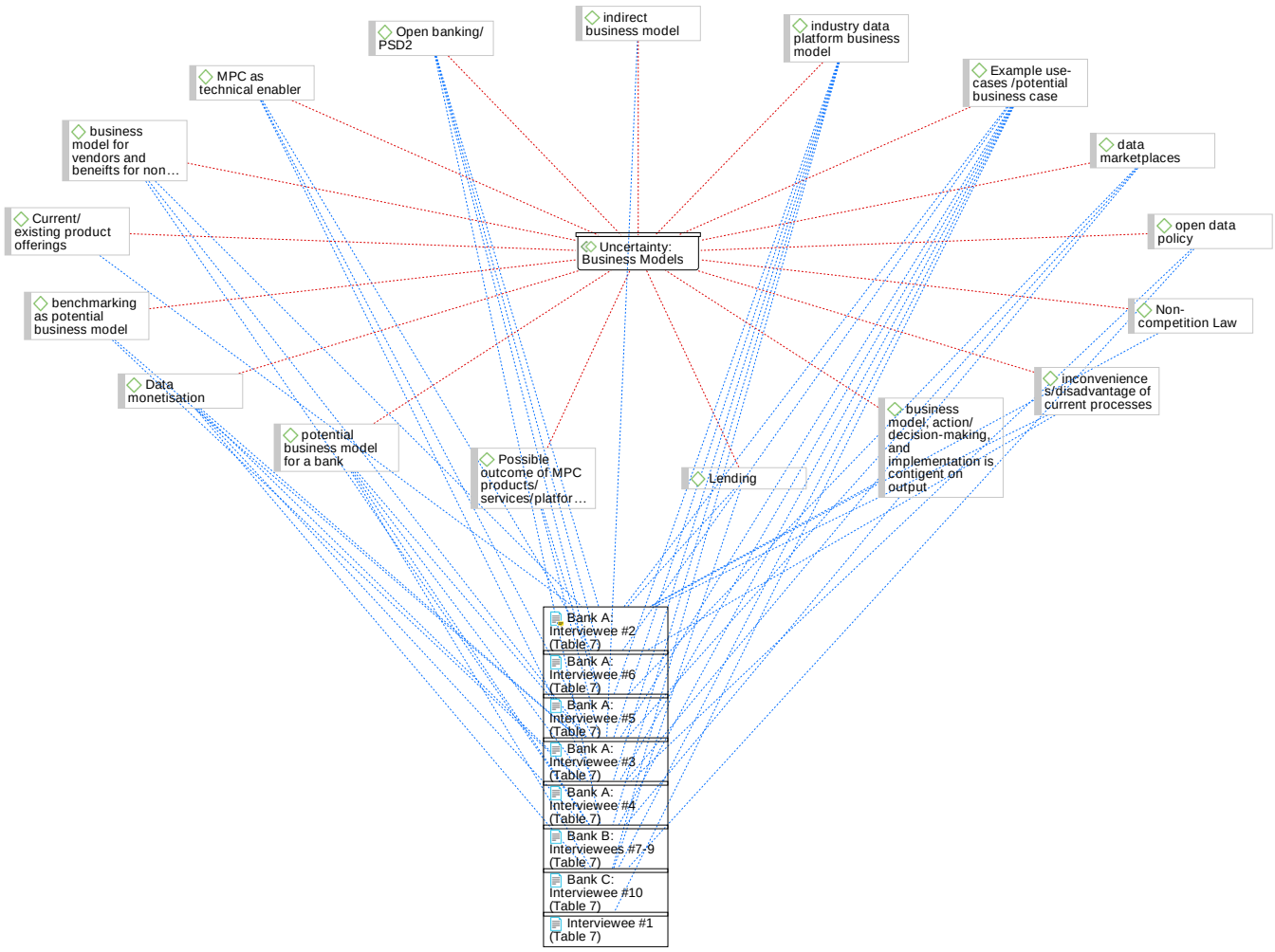

## Incentives



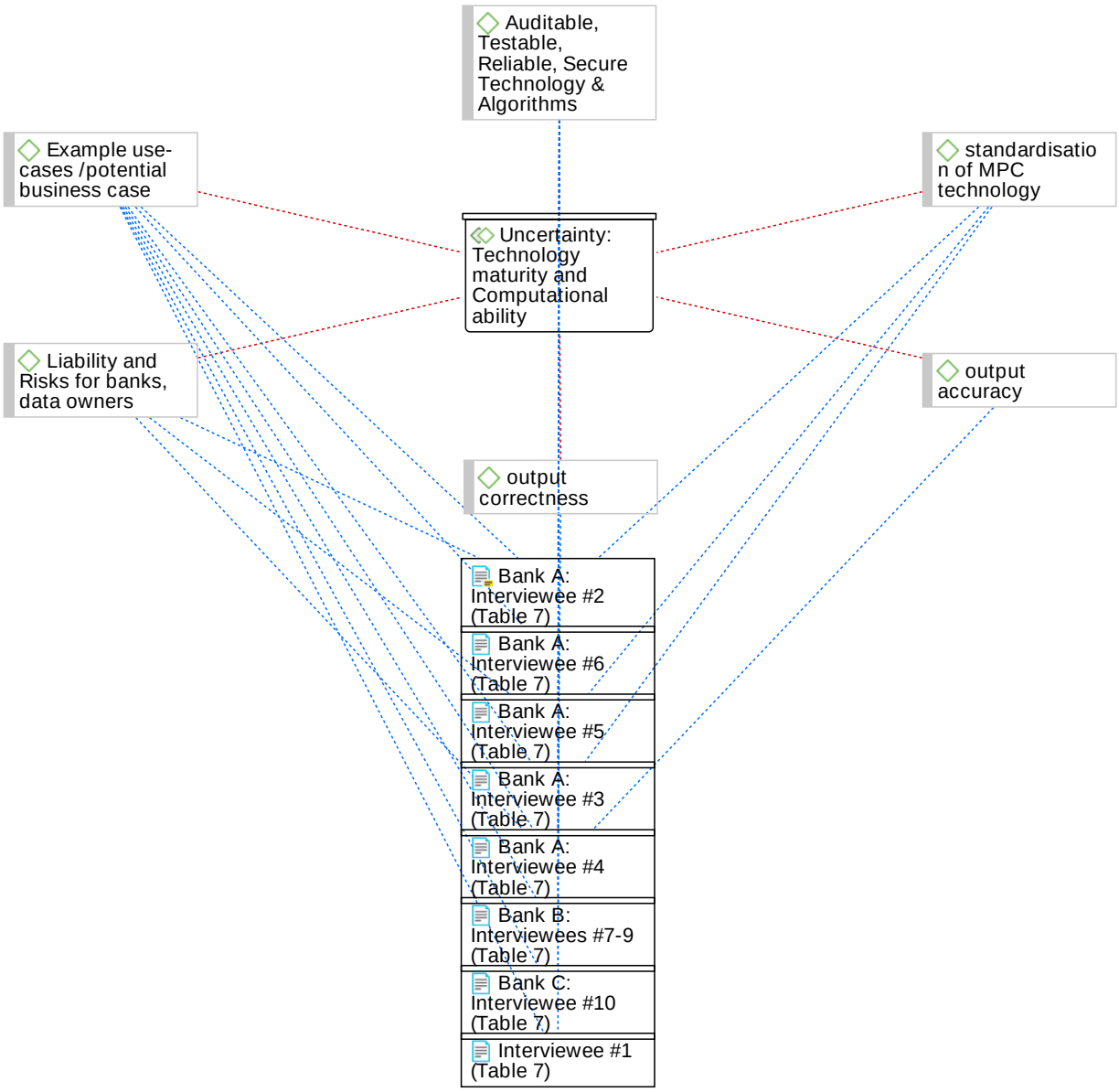
## Data Requirements



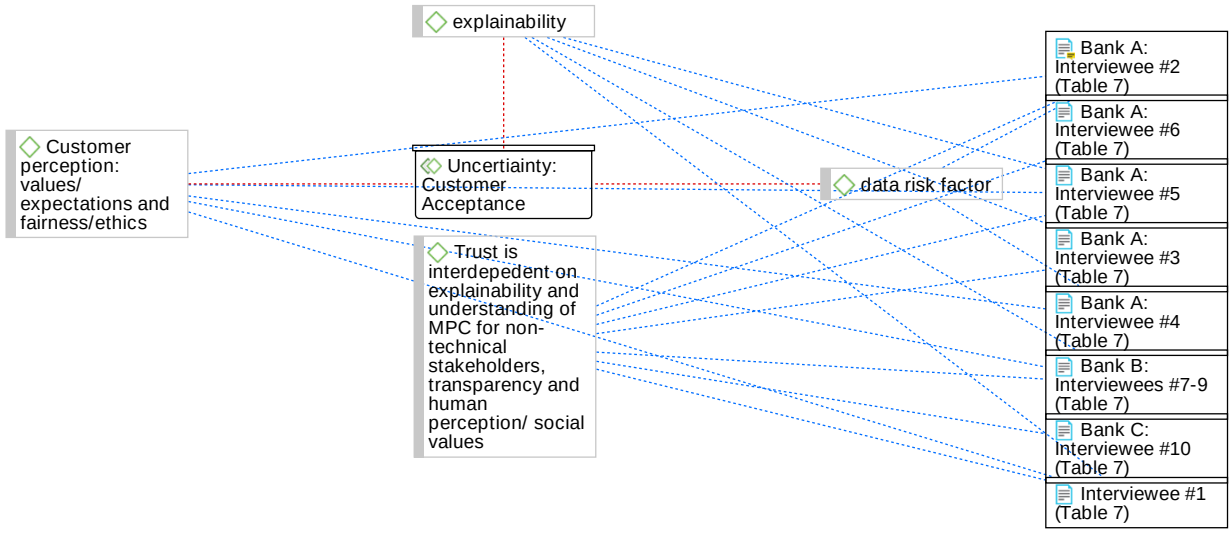

## Business Models



## Technological Maturity and Computational Ability

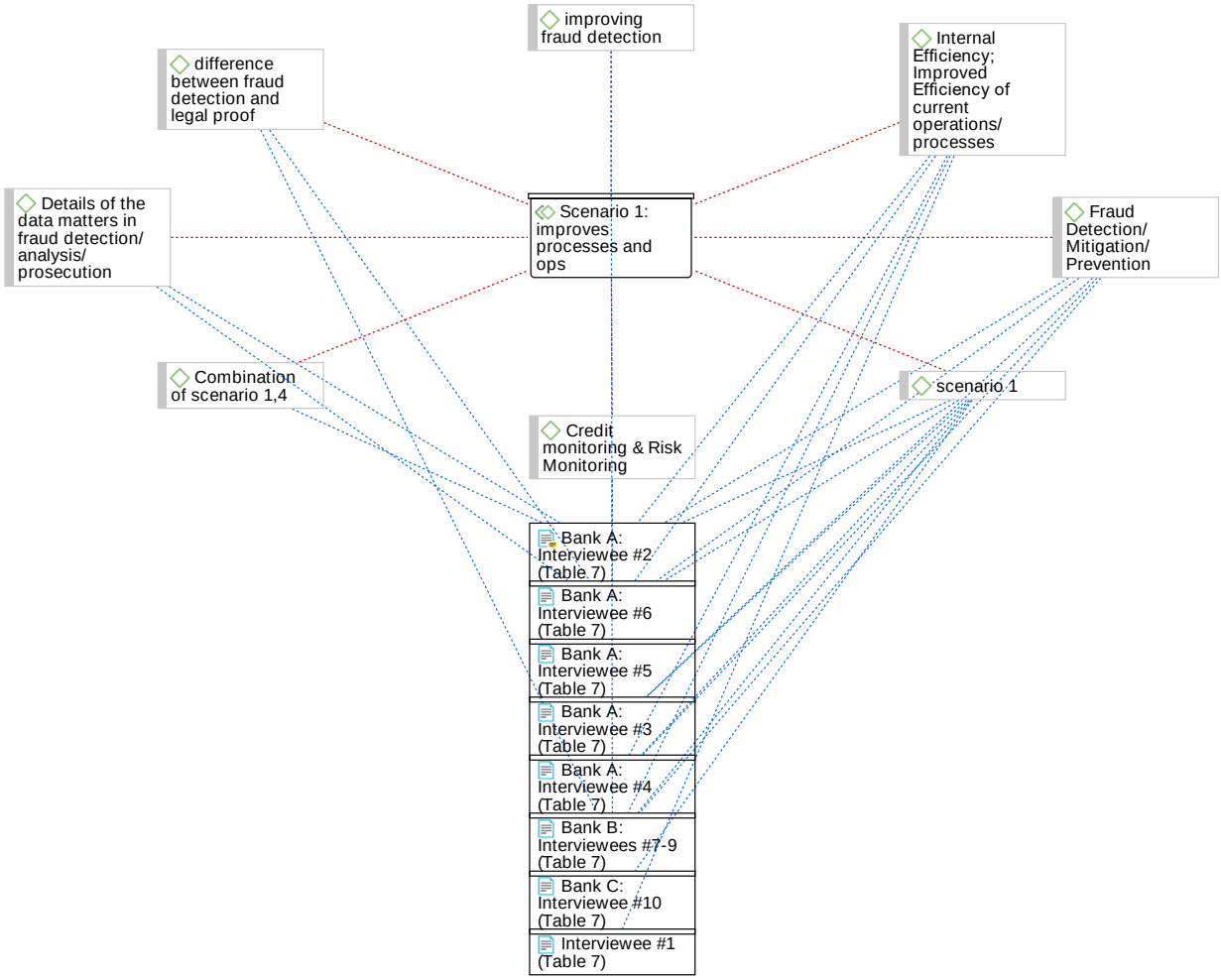


## Customer Acceptance

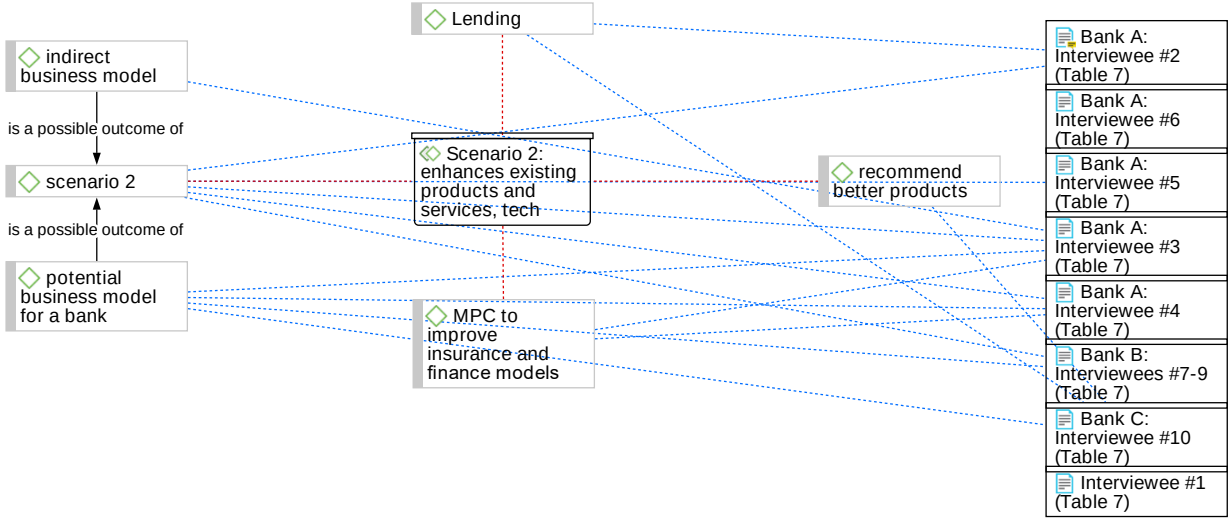


# Appendix G: Atlas.ti network reports filtered by scenario code groups

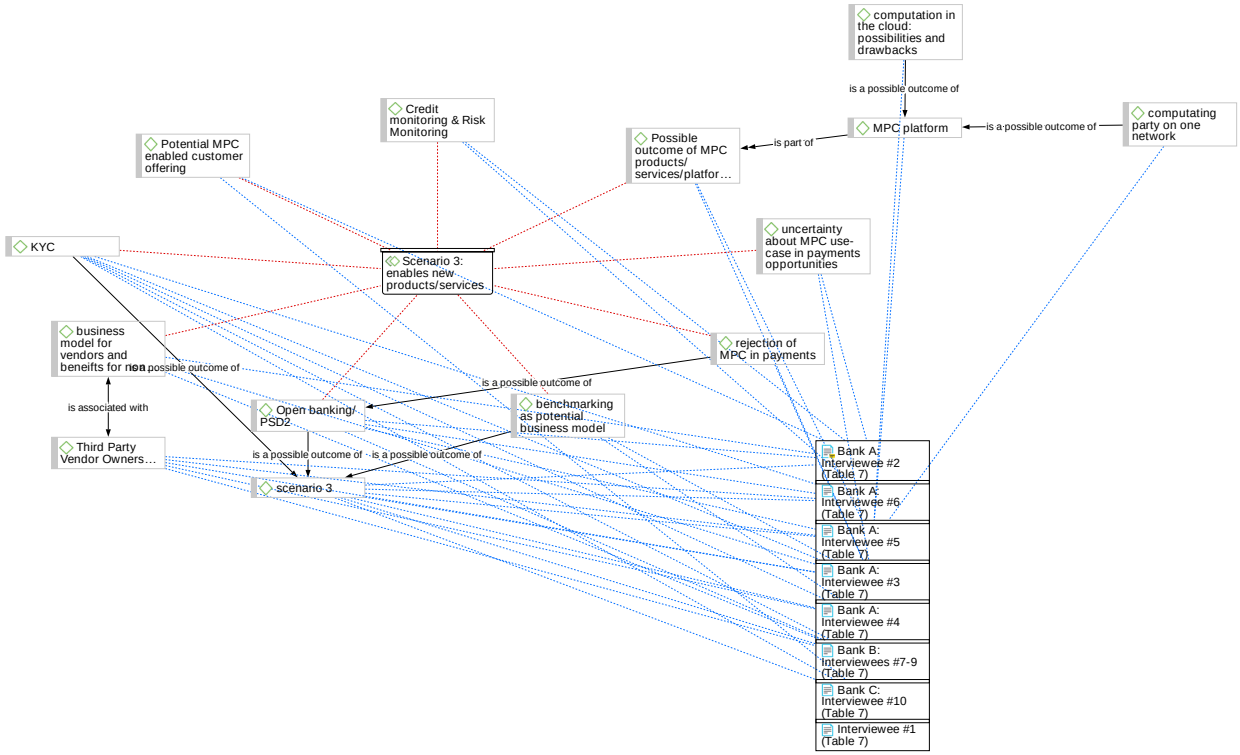
## Scenario 1



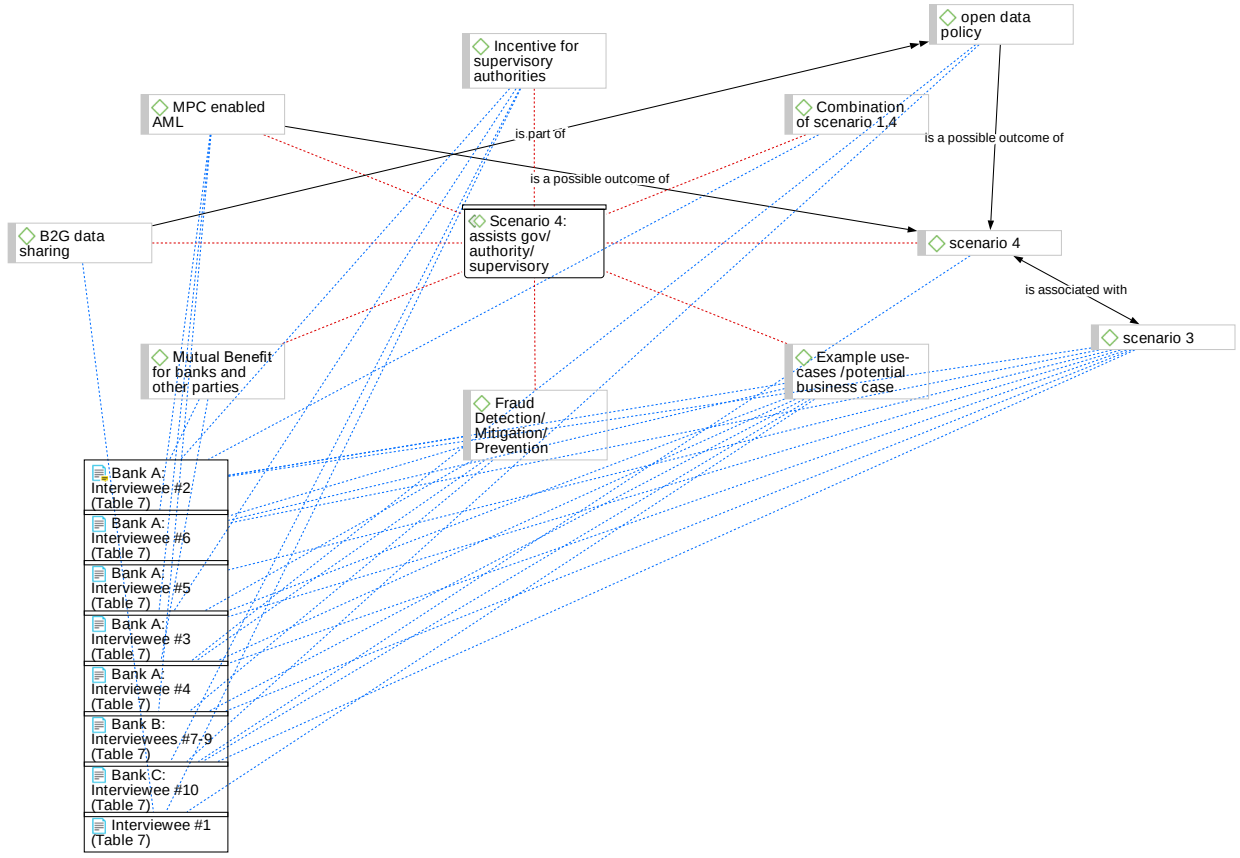

## Scenario 2



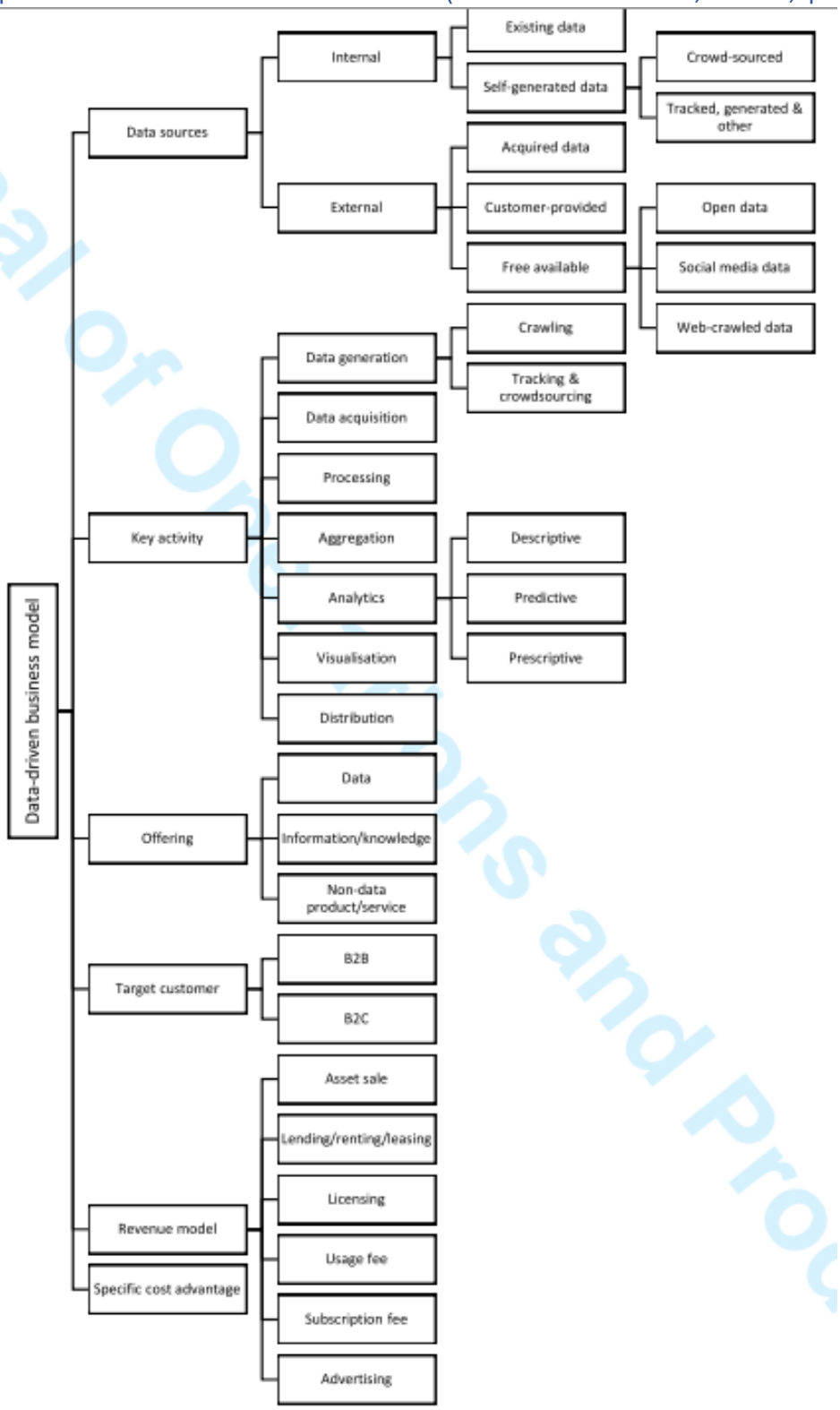
## Scenario 3




## Scenario 4



## Appendix H: DDBM Framework (Hartmann et al., 2014, p. 6)



# Appendix I: Summary of Interview Reponses concerning business models

***Interviewee 2*** remarks that new customers can be onboarded or attracted by personalized financial products within lending. The premise of this use-case is to allow the customer or client to upload information about their financial records such as statements, accounts, etc. The differentiator is that MPC could provide input for the bank to determine how much money they can lend whilst not having insight into the data that the customer provided. This allows the anonymization in calculating a customer's financial health or ability to receive/pay a loan. The bank can 'pledge' that they do not have insight to data and the customer does not have to become a customer of the bank in order to request personalized financial services.

Another potential business case offering security monitoring as a service to their clients and customers who do not have their own resources to implement it themselves. Depending on MPC maturity, allowing third parties to receive data about their network for security monitoring via MPC would benefit the privacy of the company's assets and data.

The third use-case is on the operational aspect of the business wherein employees working from home can access data more securely via MPC. In a bank setting, workers need to access core banking applications in order to perform their jobs but if they can still perform certain functions without having the actual data stored on their home devices then it would be a more secure environment. It would make it safer to work remotely and also make it easier for security if they do not have to protect the data within the MPC environment.

***Interviewee 3*** agrees with the B2B data sharing business models except data monetization of customer data. Furthermore, the utility of the data outputs is not unique to the other members within the computation which makes data differentiation unlikely for a business model. Therefore, combining the data with something really specific to create new products and services is necessary. MPC arrangements and consortiums may need to have incentives for banks to monetize their data is some way. With regards to new products and services, MPC can be used to develop a benchmarking service for businesses or consumers themselves. However, explainability of MPC to external parties may be difficult to sell or convince that the "data will not be used". When asked about other core banking services that MPC could resolve, interviewee 3 comments that MPC would be beneficial in overcoming data localization and data transportation barriers for cross-border purposes for the bank. Furthermore, MPC can possibly "open new internal business models for getting more insights into customer data".

**Interviewee 4** comments that the bank's data and trust give them competitive advantage and therefore, sharing data goes against those values. Unless, MPC can enable it so that banks share as minimally as possible and without violating the trust and privacy values of the bank. The plausibility and relevancy for adopting a data monetization or data marketplace business model were rejected. It can become possible but not in the near future or applicable for the bank. Industry data platforms poses a high risk even via MPC due to the plausibility that banks or dishonest parties can manipulate the system and commit market abuse, misconduct which can lead to market inefficiencies. Three participants mentioned that when determining banks' interest rates from the ECB, MPC can either benefit banks or lead to corruption. Moreover, the interviewee also disagreed with the open data policy unless regulation changes and allows banks to share their data. The only plausible MPC enabled business model was technical enabler but instead of owning MPC and providing a technical solution for data sharing, offering AML and KYC as a service was suggested as a business case. Within this potential use-case, integrity services could be

provided to webshops or validation for someone who wants to get a mortgage but, is not a customer of the bank. The latter idea is a similar proposition that interviewee 2 made about pledging to provide financial products to people without needing insight into their data or business as a customer. Other ideas were presented such as storing or validating data via MPC, improving regulatory efficiency by using MPC to better comply or adhere to regulations, or assisting others in calculating insurance rates whereby the bank provides their data or MPC participation for a fee.

**Interviewee 5** remarks that a data monetization model for B2C is plausible but not for a B2B platform because the combining of customer data can be a business strategy for the bank but unethical for consumers. On the other hand, a B2B business model would be viable for data marketplaces if customer data is not shared. As for industrial data platforms, it can be beneficial but also used for market abuse or cartel forming, so it is restricted by use-case. A technical enabler business. Model is possible to adopt in the case of secure storage of data and creating value from data that does not require decryption. Furthermore, data leakage which is plausible needs to be prevented. Open data policy does not present a string business case for the bank but rather for research purposes. Other business cases beyond the scope of these definitions were private-public data sharing and B2C privacy preserving data analytics which gives customers control of their data.

**Interviewee 6** mentions that in order to monetize data such as transaction data, personal data must be shared on a granular level. For high-level transaction data such as income level, which does not have personally identifiable information, is not really necessary to use MPC or build a business case from. On the other hand, MPC can be useful if the bank does not want to be identifiable when sharing data about recent security threats or vulnerabilities.

**Interviewee 7** mentioned that banks are exploring or interested in creating new businesses for enabling fraud and AML detection. However, new business opportunities with MPC have value wherein the 'guarantees on the output' are not so important. On the other hand, third party security vendors can benefit from MPC because they can aggregate security intel of all their customers which is normally not possible. This is a trend in security and with the bank's customers but not a business model for the bank itself.

**Interviewee 8** also mentions that any business opportunity via MPC is most likely in improving existing processes and businesses such as better fraud detection with data from other banks. New products and services need to be re-evaluated when more is known about the MPC itself. Interviewee 8 and 9 could only comment on business aspects of security since that is their expertise and knowledge. A notable mention is that equal ownership and usage rights from shared data should be the case (Interviewee 8) but, that is not always the case and dependent on the application (Interviewee 7). In this regard, Interviewee 7 remarks that the output might not be owned by anybody, but **interviewee 9** interjects that there should be ownership for legal liability and accountability reasons. In general, privacy preserving data analytics is important but there's no way for the customer to verify that it is private and it can also be done without MPC. Furthermore, privacy preserving data analytics lacks an incentive for big banks because they already have the data to understand what the market is doing.