Factors affecting the decision to develop MPC for Collective action in Financial Fraud Industry

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

Kenny Ho

Student number: 5185629

Date: 20th of July 2022

Graduation committee

First Supervisor	: Dr. ir. G.A. Reuver, Information Communication Technology
Second Supervisor	: Dr. B. Wagner, Organisation & Governance
Third advisor	: W. Agahari, Information Communication Technology
External Supervisor	: E. Ogel, Deloitte Netherlands

Executive summary

The financial domain is losing ground to rapid-developing fraud schemes. It puts intense pressure on organizations such as banks to find new approaches to tackle financial misconduct. This financial crime has always existed and is present in the financial industry. However, the rise of technology and the use of online transactions has enhanced the presence of the impact of fraud in this industry. The increase in financial fraud cases in a technological era result from a lack of inter-organizational synergy and the privacy concerns that entail by making data available. On top of the increasing fraud cases, organizations are exposed to increasing regulatory, financial, reputational, and legal risks. Hence, the financial crime industry and fraud prevention organizations must act on this threat. Therefore, these actors need to improve their current workflow continuously to keep up with the new developments. Different studies propose that it is a potential opportunity to take the chance and bundle data together to learn from the existing environment and improve their workflows and prediction models. However, the main concern is that parties are reluctant to share data as it involves confidential and sensitive data, which malicious parties can leverage and abuse. Also, the increasing focus on privacy protection regulations makes it complex and challenging to exchange data easily. The dataset that actors are providing will contain personally identifiable information, which in fact cannot be shared and proposed without any legitimate reason and is subjected to the data privacy regulations.

The existing set of techniques for sharing and analysing data securely, such as differential privacy, homomorphic encryption and federated learning have been proposed in studies and use cases are built in the real world. However, these techniques are insufficient and capable enough to facilitate multi-actor (data owners) data exchange and analysis. Secure Multiparty Computation, however, is capable of having multiple data owners securely perform a joint analysis. For this reason, this study has been focused on SMPC. In the case of the financial crime industry, it requires the involvement of multiple stakeholders sharing data simultaneously. Especially in the case of banks, it is essential to have bundled data for all transactions as these are connected.

To understand the purpose and the concept of the study, it is essential to have a basic understanding of SMPC. Secure Multiparty Computation is a cryptographic method for parties to mutually compute a function over all parties' acquired inputs while keeping the intake private throughout the entire process. Independent computation nodes will perform and provide analysis outcomes to designated parties. The concept of Secure Multiparty Computation has been studied by academia since the 1980s (Yao, 1982). However, the applications and introduction of SMPC are relativity novel to organizations and will not be immediately accepted. A technique such as SMPC will require participating parties to share a mutual interest and willingness to contribute continuously. It is uncertain if organizations will accept and adopt SMPC as mentioned before. Therefore, the study will also incorporate the concept and theory of collective action to understand the motives and the common goal for stakeholders in the anti-fraud industry to accept the technique and collaborate. A common goal, also known as a collective goal or interest, would create acceptance among the group. In this case, it will help to identify the factors and interests that influence an organization's decision

to engage in collective action for developing MPC for fraud detection in the financial industry.

This study has formulated a central research question to help to structure the research: "What factors and barriers influence organizations' decisions to engage in collective action for developing MPC for fraud detection in the financial industry?"
To answer the research question, a study focused on the Dutch Financial Crime industry. This study has been performed at Deloitte Netherlands Forensic & Dispute services, which is one of the largest service providers in fraud detection and prevention in the Dutch industry. The aim was to find the factors and barriers that were relevant for the actors in the same market as Deloitte Netherlands. These factors and barriers would help to explain the behaviour of actors to engage in collective action to develop SMPC in the Dutch Financial crime industry. Therefore, semi-structured interviews are conducted with several actors operating in the financial crime industry. The literature on MPC and collective action in the financial crime industry is limited. However, the available studies show that the main incentives for organizations and actors are the benefits of bundling data. These bundled data could be used to improve productivity and workflow.

The primary collective goal that can be extracted from the empirical findings is that actors in the financial crime industry want to find a way to address privacy regulations while being able to exchange data to improve their current fraud prevention workflows and models. Therefore, actors would be willing to contribute to the collective action by sharing their data. Thus, the main driver is the actors' benefits of having a more extensive and richer dataset. In the current situation, actors cannot see the larger context of the cases, as they will only obtain the data defined within the investigation's scope. The idea of collective action in developing MPC in the financial crime industry showed positive feedback among the participants. However, some barriers still need to be addressed to help the adoption and acceptance of MPC in the financial crime industry. Safeguarding data privacy has been a predominant factor for the actors. The actors are concerned about the safety of the data due to the lack of knowledge and transparency. The participants do not possess a complete understanding of MPC. The lack of knowledge causes uncertainty among the participants. Especially, the added value for the organization and their contribution will be questioned.

There are other important factors and trade-offs before MPC can be taken into consideration by actors in the financial crime industry. The flexibility of their workflow after the implementation of MPC is important. Financial crime cases require the flexibility of executing the investigation with different toolsets and structures. Especially the lack of knowledge about MPC among the participants would decrease the participants' willingness to trust in the technique and its flexibility. Besides the uncertainty of the implementation outcome, three other trade-offs have been identified in this study. These trade-offs help to understand the important values for actors to engage and trust the collective action.

First, the way of governance had a mixed opinions among the participants. The majority preferred the government to facilitate and regulate collective action. However, certain traits make the government less suitable for leading and shaping collective action. The main reason would be the lack of expertise and the dynamics within the organization. For example, the pace of how interviews define "getting it done" is slower

than in the private sector. On the other side, the government is a reliable actor with a lot of power to influence and motivate parties to participate.

The second trade-off is the proposed group size. Stakeholders have mixed opinions on the size of the collaboration. Smaller groups tend to be more successful as they are more flexible, manageable, and easier to detect any lack of effort by participants. Also, it would be easier to have inclusivity in the smaller network. Inclusivity has been mentioned as an essential factor in motivating parties to contribute. However, larger groups do have advantages too. It can create wider acceptance easier than the smaller ones, as most market players would already be in collaboration.

Furthermore, the empirical findings and literature show that transparency is vital in building trust and convincing parties to engage in collective action. Currently, the participants expressed that transparency would affect their decision to participate. The lack of transparency makes the actors concerned about their data's safety and influences their trust in the technology and parties in the collaboration. The transparency concern is two-fold. First, the low trust in technology is caused by the lack of transparency. Actors do not fully understand the system, indicating that the lack of knowledge causes the lack of transparency—secondly, the openness in the contributions made by the participants. Any indication of free-rider behaviour affects the actor's trust but also demotivates to contribute to the collective action.

Preface

This thesis is my final graduation project for my Management of Technology Master's programme at the Delft University of Technology. The whole thesis was an exciting journey and helped me to understand the relevance of academia in the society and Financial Crime industry. The thesis was written as part of my internship at the Forensic and Dispute Services at Deloitte Netherlands. I have been working at the firm and industry for over five years, and it surprised me that academia can play a crucial role in shaping the markets. I was convinced I would understand the whole industry and the opinion of the market actors. However, the entire thesis showed that there is still much to learn. This project could never be achieved without the support of the actors in the Dutch Financial Crime industry and my university supervisors. I want to use this preface as an opportunity to thank everyone contributing or supporting my project.

First, I would like to thank my supervisor, Dr.ir. Mark de Reuver for his support, critical feedback, and enjoyable discussions. His supervision and support kept me motivated while I could not arrange an interview with a key actor. Secondly, I want to thank my additional advisor, PhD student Wirawan Agahari for the fruitful discussion, helpful feedback, and providing a lot of inspiration & resources. Thirdly, my appreciation goes to Dr. Ben Wagner, who showed a lot of interest in the first meeting and provided me with constructive and helpful feedback that I used during the entire research process. Furthermore, I want to thank my Deloitte colleagues for helping me connect with crucial financial crime actors. It is a small industry and challenging to communicate with parties without connections. Also, I want to thank my external supervisor Emir Ogel for the weekly discussion and supervision.

Finally, I would like to thank every participant that contributed to the research by responding to my interview invitations and helping me to gather valuable data.

Kenny Ho

July 2022

Contents

Table of Contents

List of Figures

Abbreviations

SMPC Secure Multiparty Computation
WBP Wet Bescherming Persoonsgegevens
GDPR General Data Protection Regulation
PII Personal Identifiable Information
NCSC Nationaal Cyber Security Centrum

1. Introduction

1.1. Background

The financial domain is losing ground to rapid-developing fraud schemes. It provides intense pressure on organisations such as banks to find new approaches to tackle financial misconduct. Essentially due to the increased exposure to regulatory, financial, reputational, and legal risks (Deloitte, 2018). Actors in the financial fraud prevention industry are urged to innovate or improve their workflows due to the rising threat. Their current methodologies, techniques, workflows, and technologies used to combat and prevent fraud and money laundering are becoming outdated as rapid-developing fraud schemes outpace them. In this case, the communication between actors and sharing of critical information becomes essential to combat fast-developing fraud. However, data sharing has been a predominant and sensitive topic for companies and financial institutions. Data sharing is often on a voluntary basis. This is illustrated in most financial investigations, as custodians are not required to cooperate in providing data until lawful order has been enforced.
The availability of information could significantly impact the results of the investigations. Acquiring data on a voluntary consensus basis is difficult. However, the rising attention on data protection regulations such as the predecessor WBP (Wet Bescherming Persoonsgegevens) and General Data Protection Regulation (GDPR) increased the data-sharing complexity.

The GDPR increased the focus on the possession and disclosure of any sensitive personal information without any legitimate reason (Liu et al., 2021). Organisations that could contribute to establishing an intra-organizational anti-fraud system are afraid to share information due to the consequences of a potential data breach or unlawfully storing of Personal identifiable Information (PII). The result would be a penalty that impacts the company's reputation and finances. However, the most concerning reason are the probability that information could fall into the competitors' hand, affecting the company's competitive edge. Yet, recent developments such as the 4th European Money Laundering Directive provide a new gateway to intra-organizational data sharing between public and private organisations (Eur-Lex, 2021). Introducing data-sharing enhancing regulations will be a breakthrough in the current financial industry. It will enable collaboration between multiple service providers such as banks, telecom, financial institutions, and the government to create an intra-organizational fraud prevention landscape to identify fraudsters promptly (Ali et al., 2019). This landscape will be empowered by parties exchanging their dataset for a collective purpose.

A variety of techniques for sharing and analysing data securely, such as differential privacy, homomorphic encryption and federated learning have been covered in studies. Companies and institutions have been trying to implement these innovative data-sharing and analysis methodologies to detect financial fraud and money laundering. Yet, none of these technologies allows having multiple parties to contribute, share, and analyse a bundled data set (with multiple data owners). Secure Multiparty Computation (SMPC), however can have multiple data owners perform a joint analysis in a secure manner.

Despite the behaviour of actors and influences of regulations on the willingness to share information, the traditional silo structure of parties plays a limiting factor in stimulating collaboration. These are isolated silos containing sensitive, confidential information that is not disclosed or shared with any stakeholder in the same process. Hemenway (2016) addressed that privacy-enhancing technologies such as SMPC could help to break the current structure. It would allow corporations, researchers, policymakers, and the government to discover new knowledge and enable data sharing securely (Hemenway, 2016).

The above-mentioned challenges could be potentially tackled with SMPC. This study will aim to discover the capabilities and acceptance of SMPC to facilitate secure data sharing to enhance the current fraud detection practices. More importantly, the study will also try to understand how SMPC can solve the mentioned challenges.

To understand the purpose and the concept of the study, it is utmost essential to have a basic understanding of SMPC. Secure Multiparty Computation is a cryptographic method for parties to mutually compute a function over all parties' acquired inputs while keeping the intake private throughout the entire process. Independent computation nodes will perform and provide analysis outcomes to designated parties. The concept of Secure Multiparty Computation has been studied by academia since the 1980s (Yao, 1982). However, the applications and introduction of SMPC are relativity novel to organisations and will not be immediately accepted. A technique such as SMPC will require participating parties to share a mutual interest and willingness to contribute continuously. Therefore, it is uncertain if organisations will accept and adopt SMPC as mentioned before. Therefore, the study will also incorporate the concept and theory of collective action to understand the motives and the common goal for stakeholders in the anti-fraud industry to accept the technique and collaborate. A common goal, also known as a collective goal or interest, would create acceptance among the group. In this case, it will help to identify the factors and interests that influence an organisation's decision to engage in collective action for developing MPC for fraud detection in the financial industry.

The contribution and purpose of this study are two-fold. First, it will help actors in the financial crime industry to understand the factors and drivers that are decisive to engage in collective action for developing SMPC in a fraud prevention and detection context. Second, it will contribute to the existing set of literature on MPC applications to combat financial crime and money laundering. The previous studies on MPC applications to combat money laundering and financial risks focused on the techniques and essential financial institutions such as Dutch banks (Kollar & Erkin, 2021; Lam, 2020). This study will be the first that builds on the studies and explore the capabilities of MPC applications from a financial crime investigation perspective.

The outcome of this thesis will be a conceptual model that helps explain how organisations will cooperate in a new intra-organizational fraud prevention landscape or engagements involving SMPC.

1.2. Research Objective

This research aims to create and test the conceptual model that explains the collective goals, factors, and drivers for organizations to engage in collective action to develop Secure Multiparty Computation in the Financial Fraud industry. This model will help organizations and actors operating in the financial industry to understand the critical factors, drivers, and barriers that are decisive for actors to engage in collective action. Also, it will have scientific relevance as it will fill the current gap in the existing literature about MPC applications to combat financial crime. This study has been performed at Deloitte Netherlands Forensic & Dispute services. The focus lies on understanding the workflow and the necessary factors to improve the current fraud detection techniques and models. The current landscape does not allow data sharing due to restrictions and limitations, as mentioned before. Also, the current methodologies are becoming obsolete and inefficient. Therefore, the research will focus on a novel technique that does differ from the existing toolset, which is SMPC. The research will use the collective action theory, current literature about financial crime, and SMPC to define the conceptual model. This conceptual model will be enhanced by conducting qualitative research. The findings will be compared and incorporated into the model to make the model more specific for the Dutch

financial crime industry. The conceptual model serves as a framework to clarify the factors and barriers.

1.3. Research Questions

The central research question is:
"What factors and barriers influence organizations' decisions to engage in collective action for developing MPC for fraud detection in the financial industry?"

To acquire crucial information in a structured manner, sub-questions are drafted to answer the central research questions. The first sub-question forms the theoretical fundament for the remaining questions. It aims to identify the existing literature that explains the phenomena and primary drivers for public and private parties to participate in an engagement involving SMPC.

SQ1. What theories in literature can explain the behaviour of actors to decide to participate in SMPC?

The literature review will be conducted as an attempt to answer the first sub question. This review will search for existing literature about multiparty computation, collective action, and the state of financial fraud detection in the financial industry. After the review, a qualitative study will be performed at Deloitte Netherlands Forensic & Dispute Services (FDS). Deloitte FDS is one of the largest market players in the Netherlands in the field of litigation support, fraud detection and prevention. The main objective of conducting the study from the perspective of FDS is to contribute to the existing literature from a perspective, that isn't covered yet. Also, the study will describe the collective goal to help to understand the motives for parties to engage in collective action to develop novel technologies such as SMPC.
In addition, stakeholders will have different interest. Therefore, it is essential to understand the interest of the actors and the weight of the interest. This interest can be translated into factors that are critical for collective action

The following three sub questions emerged based on the first question.

SQ2. What is the collective goal, drivers, barriers of adopting SMPC in financial industry?

Collective action requires a collective goal. The second question will target on discovering the collective objectives, drivers, and barriers for actors in the Dutch financial industry that needs to be incorporated into the conceptual model to explain the behaviour of actors.

SQ3. What are the trade-offs between the interests of key stakeholders?

The third sub question aims to identify the trade-offs between the interest of key stakeholders. In a collective action it is critical to have a synergy and seamless collaboration between participants. Therefore, this question will try to find the trade-offs based on the findings of the previous two questions. These values will help in shaping the conceptual model and testing the current literature.

SQ4. How does the conceptual model explain the interest of private and public organizations in accepting SMPC?

At final, the conceptual model that is drafted at the beginning of the research and validated throughout the study, will be reviewed. The final conceptual model will help to understand the interest of private and public organizations in accepting SMPC. This does not focus on the

acceptance of implementing SMPC but the factors that help to affect the decision of actors in engaging in collective action to develop SMPC use case in the financial industry.

The following diagram illustrates the structure of the thesis from a research set-up perspective.

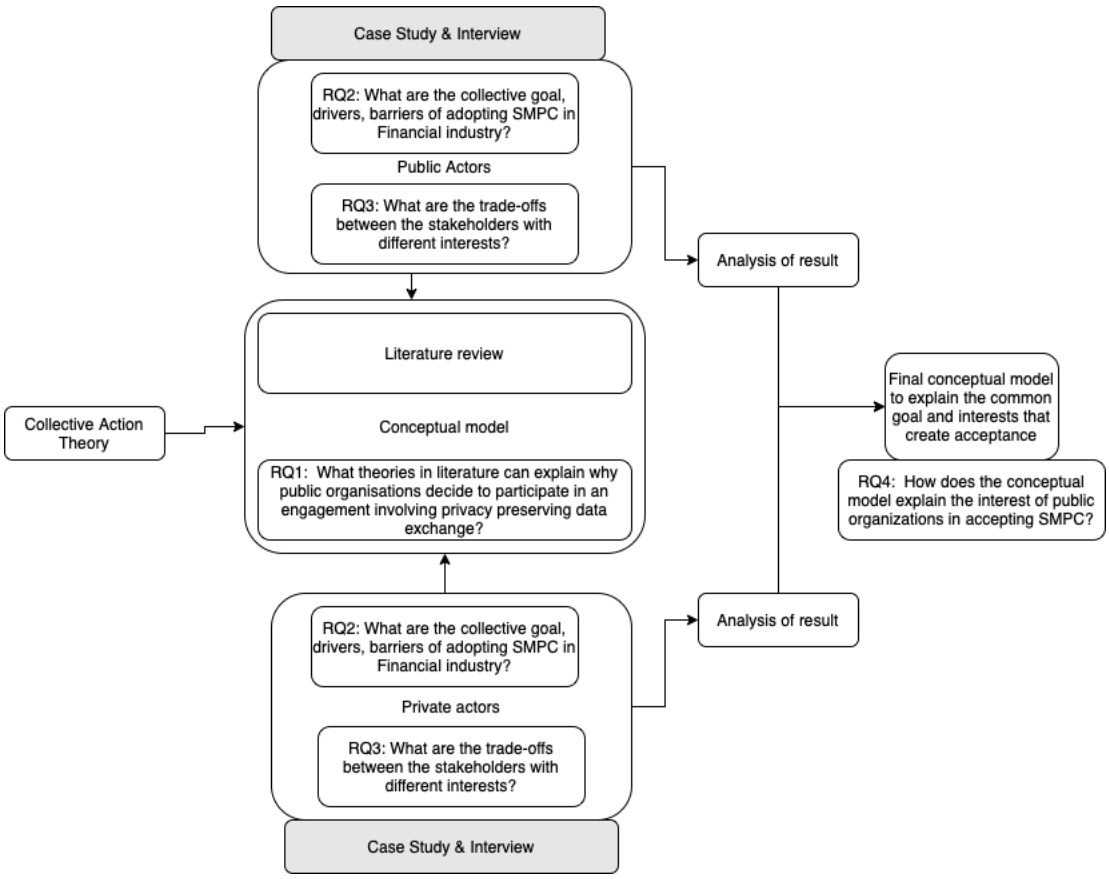


Figure 1 - Thesis structure diagram

1.4. Reading Guide

The previous sections described the background and the research definition for this study. The remainder of this research study is structured as the following: the literature review will discuss the existing literature and the gaps that have been identified. These findings of the literature gaps will help identify what theories can describe actors' behaviour to participate in collective action and MPC. As a result, the findings are the basis and will assist with forming the first conceptual model. This conceptual model tries to explain what factors would influence the actors' decision to engage in the development of MPC from a theoretical perspective. After the literature review, the methodologies for the study will be described. This chapter will elaborate on the data collection and analysis methods to acquire additional information that could potentially enhance and test the model. Next, the research findings will be discussed and compared to the conceptual model. The differences illustrate the additional knowledge that hasn't been captured by the literature. The conceptual model will be modified and enhanced based on these differences. Finally, the research questions will be answered in the conclusion. It will reflect on the result of testing the conceptual model and how it could help understand the current challenges. Also, essentially help actors to understand what factors would play a crucial role in affecting the decisions of potential participants in the financial crime industry. The final chapter would also provide insights into the limitations and potential ideas for future research.

2. Literature review

This chapter will elaborate on the literature review of the underlying theories in the research domain. First, the literature review will provide a chronological examination of Secure Multiparty Computation to understand the historical and current state of SMPC. Second, this research will review studies on collective action theory to understand the influence of collective action on the motives of parties to participate in developing SMPC. Third, the review will focus on the current fraud detection methodologies within the financial industry.

2.1 Secure multiparty Computation

Over the decade, empirical research and academic papers have captured main drivers and barriers to adopting Secure Multiparty Computation. However, most of the research were overwhelmingly focusing on the technological dimensions.

The changing purpose of Secure Multi-party computation

Andrew Yao introduced the first concept of Secure computation (SC) in the 1980s when he developed a protocol for secure computation among two parties. The purpose of this secure protocol was to find out who was the wealthiest individual among the two participating parties without disclosing their direct information about their wealth (Yao, 1982). Goldreich et al. (1987) elaborated on Yao's work and proposed that the protocol could take more parties into account. The idea was that parties could generally determine which data they would share while it remained secret throughout the process (Goldreich, 1987). However, this academic work did not provide context nor define the added value for the business and industries. The basic principles of sharing information without revealing their input remained the same over the years. Lindell and Pinkas (2009) contributed to this void. They argued that secure computation should not be seen as a cryptographic technique but as an opportunity to serve a broader purpose and not solely a general protocol without business-added value. Multiple parties can share confidential datasets and mine the combined data to contribute and acquire new insights (Lindell & Pinkas, 2009). This new purpose was introduced as secure multiparty computation.

The work by Lindell and Pinkas attracted scholars to contribute to applying SMPC within industries such as banking, finance, insurance, and healthcare. Data sharing is one of the core processes within their operations, and they were required to collaborate with internal and external parties (Resende et al., 2021; Wong & Kim, 2010). The added value of SMPC would help industries learn from each other and enhance the current workflows by collaborating without worrying about revealing their confidential data. Veeningen et al. (2018) proposed that SMPC would be the righteous technology to enable analytics on sensitive medical data while preserving privacy and complying with regulations such as the GDPR (Veeningen et al., 2018). Literature in fraud detection emphasized that SMPC could enable corporations to improve their detection accuracy and rates.

Furthermore, it would serve as a role to protect any privacy infringements and workaround for sharing sensitive data (prohibited and protected by law). In addition, Ali et al. (2019) mentioned that no existing mechanisms enable public-private collaboration due to privacy concerns (Ali et al., 2019; Clifton et al., 2004). This means the mechanism is lacking in the current situation and needs to be developed before SMPC can be used to enhance public-private collaboration in the intra-organizational landscape.

These studies showed the potential of SMPC serving the business within the industries, while these were lacking in the previous literature, forming the building blocks for SC and SMPC.

The most prevailing function is to safeguard privacy, allowing collaboration within industries and public-private parties. Although, these industry-focused studies did not cover or remain general in discussing the potential of SMPC as a public-private collaboration from a corporate view. As it stuck to the basic roles within SMPC, which are the data providers, computation parties, and data-receiving parties. Hemenway (2016) did mention the role of and the potential of SMPC for researchers and businesses (Hemenway, 2016). However, it argued from a governmental perspective and reasoning why governments should allow data sharing and collaboration. Lapets et al. (2019) did elaborate on the role of the software engineers, government regulators, corporate executives, and end-users within the SMPC and how new opportunities could be discovered. Nevertheless, these topics were discussed remained on a software level (Lapets et al., 2019).

Furthermore, the studies highlighted the government as a collaboration limiting and privacy regulating role. They did not consider the participating role of the government in enhancing their processes. It either addressed the purpose of the SMPC contributing to the industries or serving as a privacy-protecting role. However, seeing the SMPC enabling public-private collaboration and serving as a business enabler between government and corporates is lacking in the current literature. It might be explained by the finding of Ali et al. (2019), which states that the current mechanism is missing that enables public-private sector collaboration. For instance, in the case of fraud detection, it discussed the benefits for the corporates to improve their detection but not how it would impact the relationship between law enforcement and corporates (Ali et al., 2019).

The evolution of the techniques

The secure computation protocol founded by Yao aimed to perform basic descriptive computation based on two parties. This concept has been labelled as Yao's Millionaire's problem because he tried to calculate the wealthiest individual among the two participants without disclosing information to each other (Yao, 1982). As previously mentioned, the concept has been elaborated on by Goldreich. The same protocol has been extended by involving multiple parties instead of the sole two parties (Goldreich, 1987). The technique that this protocol was using has been referred to as Oblivious transfer by the literature. The principle of this technique is primarily secret information sharing without revealing the inputs. It became an interesting research direction for researchers working in the Multiparty Computation field (Yang et al., 2021). The mechanism created the foundation for secret sharing within the MPC domain. The development and research work into this protocol brought to the ubiquitous secure multiparty computation techniques such as addictive homomorphic encryption and fully homomorphic encryption (Liu et al., 2021). Subsequently, the concept touched upon other theories and practices that had the same purpose: processing data without revealing the input. These topics are commonly included and combined in the existing literature. For instance, zero-knowledge proof. It is a cryptographic protocol that allows one party to prove the possession of certain information to another without disclosing it to the counterparty (Kanjalkar et al., 2021).

Main drivers to participate

The concept of SMPC is highly dependent on the participation of multiple parties to provide input data. Therefore, it is crucial to identify the incentives and motives to make it appealing to potential participants. Clifton et al. (2004) mention three general incentives for companies to collaborate in data mining with privacy-enhanced technologies. First, interested parties could exchange information to boost productivity and improve their business. Second, healthcare can share data with each other to improve scientific research. Third, public agencies can improve their public safety in case of data openness (Clifton et al., 2004).

Lapets et al. (2019) add a new perspective to participation in SMPC. Incentives are needed to convince parties to join but do not entirely rely on them to make it appealing. SMPC requires collaboration between multiple parties, which means every stakeholder would have a different interest. Therefore, it is required to have a thorough understanding of all the potential participants. However, acquiring insights into the interest of stakeholders is difficult since basic research alone is not sufficient, and interest may vary in different cases. Lapets mentions two additional drivers that are critical for creating acceptance and trust in the system, which are transparency and auditability (Lapets et al., 2019).

Development of barriers

This section will discuss the four most prevailing barriers to the current state of Secure Multi-party Computation. The barriers have different points of view, which can be categorized as technical boundaries or social-technical challenges. The first barrier is the complex challenge of building trust. Second, the lack of consideration of integration limits the operation of the SMPC. Third, the performance and inscalability make it less robust. Finally, the underestimated risk of processing sensitive data within SMPC.

Trust is essential to create the adoption of SMPC among the parties. However, Veeningen (2018) states that acquiring the trust of key stakeholders can be very challenging since the current techniques are sophisticated and challenging to understand for non-technical entities (Veeningen et al., 2018). In addition, identifying all stakeholders and their concerns cannot be performed with sole basic research (Lapets et al., 2019).

Clifton et al. (2004) argue that these studies lack crucial factors such as data integration. Therefore, it is not the case to assume that the data integration and standardization for the input parties are performed. This can hamper the data mining and sharing techniques because of their inability to share data (Clifton et al., 2004). Balamurugan et al. (2012) added a new perspective to the limitations. The failure to share data caused by data integration can be severe, but the current state of SMPC can only share data and not a file (Balamurugan et al., 2012). This implies that the form of input and output can be challenging.

These latter two studies focused on the implications that occur because of data discrepancy or format. However, more implications exist from a broader perspective. Data integration is essential, but the SMPC also needs to integrate with the existing system. Data entries are manually inserted because of incompatibility, explaining data discrepancies and format issues (Veeningen et al., 2018). Furthermore, the amount of data entries is currently the limiting factor. The performance of the computation techniques is not efficient and robust enough, which means it is impractical in the sense of scalability (Resende et al., 2021; Tang & Soundarajan, 2017). Millions of regressions within the SMPC can take time to complete, making it less robust.

The final barrier is the willingness to share data with other parties and processing. Parties are afraid of sharing data because it contains sensitive data that their competitors can exploit (Clifton et al., 2004). On top of that, it is prohibited to disclose and possess sensitive personal information according to the General Data Protection Regulation. Furthermore, privacy-

sensitive industries are highly forbidden to consolidate data crossing (Liu et al., 2021). All studies promoted secure multi-party computation as the solution and enabler for collaboration while preserving privacy. However, Veeningen (2018) proposed that processing highly sensitive with SMPC techniques can still be risky, especially because confidential data possess generally possess more significant risks (Veeningen et al., 2018).

This study will primarily focus on the first barrier, “trust”, as it aligns with the objective of the research. It is essential to understand how to create acceptance of using SMPC among the actors by “Trust”. The literature about financial crime and techniques will also highlight that fraud cases are caused by the lack of inter-organization synergy and availability of data. The assumption is that the lack of available data and synergy could be caused by trust. Especially with the novel technologies, they will not be adopted and implemented immediately. Therefore, the study will focus on the factor “trust” and assess the effect on developing SMPC for the financial industry. The following sections will elaborate on the factor as well.

2.2 Collective Action Theory

There is considerable literature about "collective action". This research will include the theory of collective action in the studies, as it might help to understand how organizations can be convinced and motivated to participate in developing SMPC in the financial industry.

The first "Collective action theory" was introduced by Olson (1965), which studied the behaviour of individuals in deciding to collaborate for a common goal— attempting to identify the conditions that explain why individuals would cooperate to achieve a common goal. A common goal can be defined as the collective interest of all the participants. Olson states that the classical dilemma of collective action is "Rational, self-interested individuals will not act to achieve their common or group interest…". In other words, the theory notes that individuals will not advance their common or group goals unless they are coerced to do so, or selective incentives are offered to the concerned parties to motivate them (Oliver, 1980; Olson, 1965). This theory coincides with the research question of how incentives will affect 'parties' motivation to participate in the development of SMPC, as mentioned in the previous section. Oliver (1980) introduces rewards and punishment as selective incentives for collective action theory, also known as positive and negative selective incentives. Positive incentives effectively motivate a small group of cooperators since it exercises pressure on the smaller ones, while negative incentives are intended for unanimous cooperation. The work of Oliver (1980) criticizes the prior work because of the lack of focus on the critical implication of using rewards and punishment of parties as selective incentives. The previous studies examined the decisions to collaborate, but they didn't cover the decision to use incentives to induce others to participate in a collective goal (Oliver, 1980). More specifically, Olson (1965) neglected the aspects of considering why and when someone would want to use selective incentives.

Ostrom (2000) builds upon the collective action theory by looking at multiple types of players instead of an individual. He elaborated on the motivations of rewarding and punishing parties, which introduced two types of players: conditional cooperators and willing punishers. Conditional cooperators are individuals that are willing to initiate and establish cooperative actions if other parties are reciprocating. Therefore, their contributions are highly reliant on the actions of other parties, as they can be reduced if there is free-rider behaviour. The impact of diminishing contribution will discourage other conditional cooperators too. The second player is the willing punishers that punish free-riders if it allows them (Ostrom, 2000). Nikayin & Reuver (2013) states that free-riding on the contribution of others can sabotage the efforts for collective action. Therefore, the solution to the proposed collective action dilemma with free-ride behaviour is to deploy selective incentives (Nikayin et al., 2013).

Selective incentives have been addressed in many previous studies. Therefore, this research will test the following hypothesis:

Proposition 1. Selective incentives affect the decision to participate in developing SMPC.

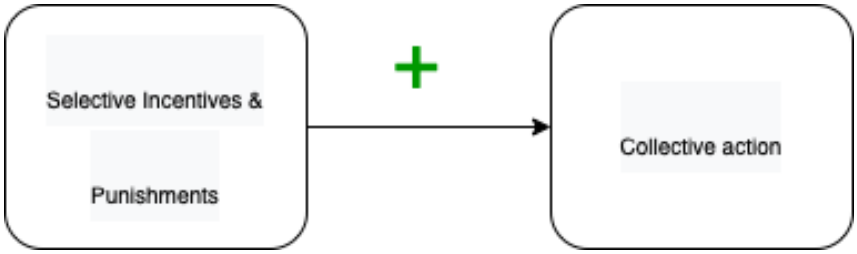


Figure 2 - Proposition 1

Certain studies have emphasized the use of selective incentives and punishment. The ideal situation would be a contribution by parties voluntarily. However, Ostrom (2000) highlights two types of players. Some conditional cooperators depend on their actions and contribution to the actions of other cooperators (Ostrom, 2000). The occurrence of free-rider behaviour will have a diminishing impact on the contribution and trust of the efforts for collective action. The proposed solution by Nikayin & Reuver (2013) might eventually help to mitigate the risk of free-rider behaviour (Nikayin et al., 2013). Therefore, this study will measure the effectiveness of the usage of incentives and punishment on the participation grade.

The second proposition emerges based on this proposition.

Proposition 2. Selective incentives and penalties will reduce the risk of free rider behavior.

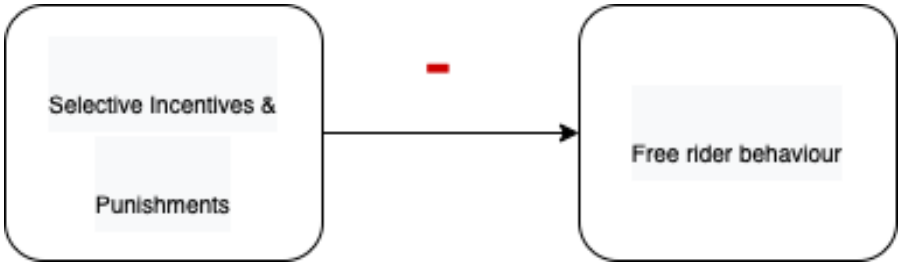


Figure 3 - Proposition 2

The second proposition is necessary to provide an answer to the first hypothesis. It will test if incentivizing actors reduces the level of free rider behaviour. Free rider behaviour tends to sabotage the effort of collective action. The anti-fraud landscape is strict and regulated by the government. Whether introducing selective incentives and punishments is suitable and ethical can be questioned. In addition, in a strict environment with many regulations, free rider behaviour might not exist as a lack of contribution is immediately noticeable.

Factors of collective action

Despite free-rider behaviour, there are several factors that are decisive and important within collective action. The theory elaborated by Ostrom (2000) highlights certain factors and characteristics about the group that could potentially affect the outcome of collective action:

(I) *The size of the group*
(II) *Heterogeneity of the group*
(III) *Size of the total collective benefit*
(IV) *Marginal contribution by the individual to collective good*
(V) *Temptation to free ride*
(VI) *Loss of cooperators*
(VII) *Choice of participation*
(VIII) *Presence of leadership*

De Reuver et al. (2014) suggest various challenges that affect the collaboration for a common goal: differing objectives and interests, conflicts, interdependencies, and governance or leadership. These are like the factors mentioned in prior work. The interests of individuals may vary which can lead to a conflict of interests within the group (heterogeneity among group members). The conflict can fragment the group, creating rivalry and making it difficult to achieve a mutual consensus. The interdependency in a network of organizations could solve the free-rider problem in collective action. The interdependency urges organizations to collaborate(De Reuver et al., 2014). However, Nikayin et al. (2013) mention that interdependencies are not always crucial for collaboration. It involves different challenges, such as the lack of trust. The theory also suggests that the size of the groups matters as smaller groups tend to be more successful than large ones. The lack of contribution is noticeable in a smaller environment, and in addition, it is more feasible to organize (Nikayin et al., 2013). Bimber et al. (2005) propose that the communicative and organizational aspects are the most prevailing barriers. Therefore, it is critical to find resourceful potential participants as a beginning. These participants might have networks containing people who share the same interest in contributing to the collective good, referred to as interdependency (Bimber et al., 2005).

Role of Trust in Collective Action

The previous sections briefly mentioned the role of trust. Many previous studies have highlighted the importance of trust in collective action as and a critical factor in enabling collaboration between parties (Kahan, 2005; Miao et al., 2021; Murunga et al., 2021; Ostrom, 2000). Trust is the crucial component of social capital and is considered critical for collective action (Miao et al., 2021).

Kahan (2005) extends it by researching the correlation with selective incentives. He discovers that incentives may potentially undermine the condition of trust to hold collective-action problems at bay as rewarding and punishing would display the weak commitment of the individuals. Although, Miao et al. (2021) disagree and emphasize that collective action is affected by governance challenges such as lack of incentives that eventually impact trust quality (Miao et al., 2021).

Harring et al. (2021) adds a new perspective and states that trust is affected by the associated risk and uncertainty. Entities aware of the risks and uncertainty tend to distrust, which would have consequences on deciding to cooperate. Fruitful collaborative arrangements and opportunities are affected due to the high perceived risk of information being disclosed to competitors or companies handle the way personal information (Harring et al., 2021; Shimizu et al., 2021). One way to address this challenge is the involvement of institutions. Governmental institutions can enforce policies that would weaken the collective stressors and

eventually reinforce the facilitators of the collective action initiative (Harring et al., 2021). It all implies that leadership and governance mechanisms are required to increase trust and reduce the risk during collective action.

Governments could influence firms, individuals, and NGOs through punishments and incentives. Firms are also capable of shaping the action. They can use sophisticated public relations strategies to influence the opinion of others (York et al., 2021)

Sebhatu et al. (2020) mention that the group size will affect the trust. The larger the group, it tends to increase the degree of distrust among the participants. Yet, he still promotes that group size may increase the benefits of cooperation . Other studies agree that group size is a crucial factor affecting collective action. However, Yang et al. (2013) hypothesize that only focusing on the group size will lead to biased conclusions (Yang et al., 2013).

These studies motivate the researcher to test the following propositions:

Proposition 3. Selective incentives, group size and governance will decrease the risk and uncertainty among the individuals.

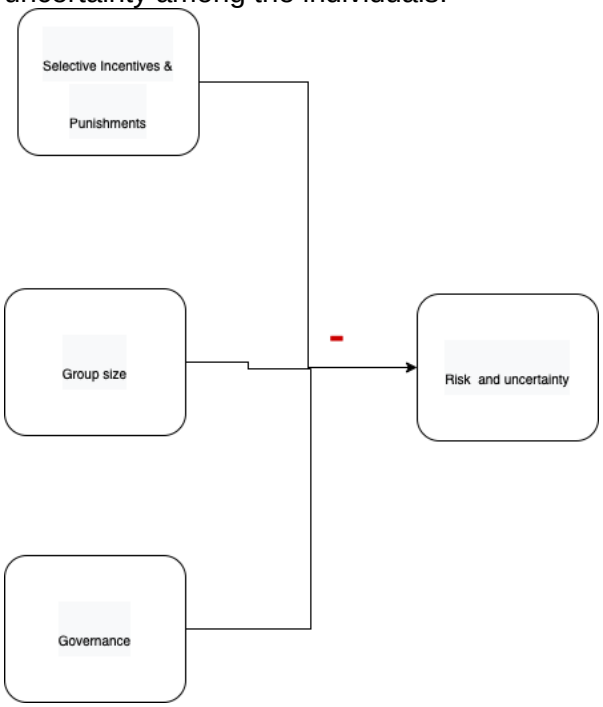


Figure 4 - Proposition 3

Previous studies state that selective incentives and punishment, governance mechanisms, and group size decrease exposure to certain risks, such as free-rider behaviour. Therefore, this research will test whether conditioning actors by enforcing policies and providing selective incentives and punishment will adjust the entities' behaviour. The risk and uncertainty seem to be critical factors in building trust among the members. At last, the impact of the group size will be determined. The question arises if the larger group size will affect the decision-making and governance mechanism and eventually make risk more noticeable. Nikayin et al. (2013) note that free rider behaviour is more visible in larger groups than in smaller groups.

The risk and uncertainty will affect the decision and the level of trust among the members. Therefore, the fourth proposition is created.

Proposition 4. Selective incentives, group size and governance, will increase the trust of actors to decide to participate in developing SMPC.

The previous proposition will measure the effect of selective incentives and punishment, governance mechanism and group size on mitigating risk. These three factors have been promoted by studies, but it is still uncertain if these factors will help to motivate actors to participate in developing SMPC in an anti-financial fraud landscape. The current landscape is based on cooperation voluntarily, which can be a challenge if any incentives or punishments are introduced. Incentives and penalties can be coercive, which might eventually impact their decision on participation and level of trust. In addition, it remains unclear what actor should lead the collective action initiative. York et al. (2021) note that governments can easily influence the decision of firms, individuals, and NGOs because of their authority by introducing policies, incentives, and penalties (York et al., 2021). This would reduce the tension exercised by collective stressors and reinforce the facilitators (Harring et al., 2021). However, influential firms can also play a role in shaping the whole action.

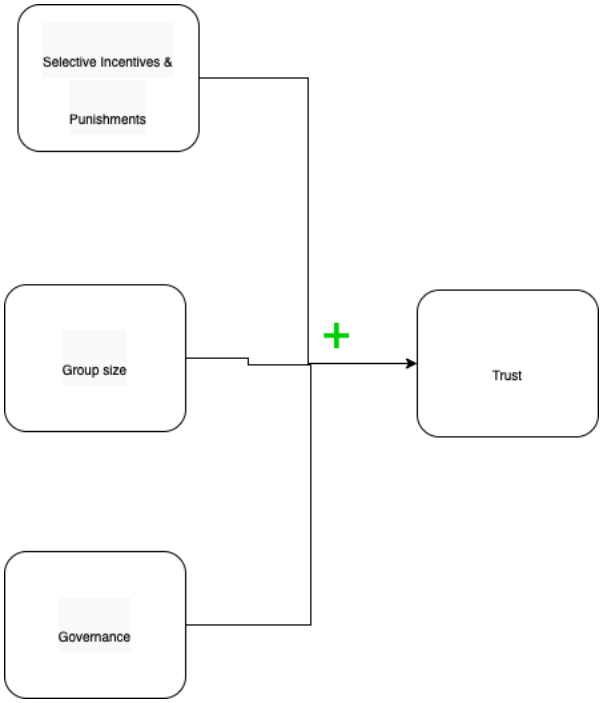


Figure 5- Proposition 4

2.3 Financial fraud detection in the financial industry

Understanding the current state of literature about financial crime and the development of detection methodologies is essential. It will provide a general understanding of the existing landscape and the relationship with the methodologies that emerged based on this phenomenon. The previous section already stated that the existing set of methodologies had a limitation that could potentially be tackled with SMPC. The aim of performing a literature review on these topics is to understand the differences with SMPC and how these methodologies are applied in practices and documented in the literature.

Financial crime can be seen as a widespread phenomenon impacting countries and has a significant impact on a country or company (Amara & Khlif, 2018). The term financial crime is broad and has different forms, as Gottschalk (2010) would describe this phenomenon consisting of fraud, money laundering, terrorist financing, financial markets offences and cyber- or technology-enabled crimes linked to financial activities (Gottschalk, 2010). Especially the rise of technology and the use of online transactions has enhanced the presence of fraud in the financial industry (B. B Sagar et al., 2016; Hasan et al, 2022). Sagar et al. (2016) mention that the increase in financial fraud cases in a technological era is the result of the lack of inter-organization synergy and privacy concerns to make data available. Actors in the financial industry are urged to act on fraud cases, as the consequences will result in financial losses and reputation and harm the customers' trust. The solution to fraud cases is to perform fraud detection, which is a complex task and cannot be achieved solely by techniques and technologies. Fraud detection would require regulatory support by the government and organizational support in combination with the existing technologies (AKGUL, 2021).

The existing set of literature proposes a variety of fraud detection techniques and algorithms, as one of the predominant techniques within the industry is data mining. Data mining is exploring and extracting hidden information from a large database or provided datasets. It involves statistical and machine-learning techniques to cascade the raw data into models for the purpose of finding interesting patterns (Hsu et al., 2012; Mabroukeh & Ezeife, 2010). However, Sagar et al. (2016) argue that data mining alone is not sufficient to prevent and detect fraud.

The primary concern mentioned above is the lack of inter-organization synergy and privacy concerns to make data available. Hasan et al (2022) propose that it would require a robust and privacy-preserving approach. The study suggested using blockchain to secure the privacy of the data. However, it would still be essential to convince organizations to collaborate to connect and adopt a novel technology such as blockchain. As a result, an incentive mechanism is introduced that motivates organizations to participate and be rewarded based on the difficulty of updating the model (Hasan et al., 2022). The concept of implementing incentives has also been highlighted in the previous section about the collective action theory. It assumes that incentivizing organizations and actors would positively affect the participation and adoption rate.

Other techniques that serve a similar function as blockchain (acting as a privacy-enhancing technique) have been captured by the literature as well. Kollar (2021) illustrated the case of privacy-friendly data analysis to combat money laundering in the Netherlands. In the initiative (formed by ABN Amro, TNO, and Rabobank), several techniques, such as Secure PageRank, have been used in combination with homomorphic encryption (Kollar & Erkin, 2021). Homomorphic encryption can perform mathematical operations on encrypted data, which converts the data into readable text for analysis (while holding it secret for the third party). Another identical privacy-preserving technology is differential privacy. Agahari et al. (2022) mention that this technique will add additional noise to the dataset in order to maintain anonymity. The study also argues that these techniques differ from MPC, as these will only

allow one data owner (Agahari et al., 2022). In the case of fraud detection, it would require more than one data owner, which makes these techniques less viable.

3. Methodology

The following chapter will discuss the methodologies. A case study has been selected for this research. The objective of the research is to identify the factors and barriers that affect the actors' decision to engage in collective action. These factors and barriers will help to understand how or why it would affect the decision to participate. Yin (2018) mentioned how and why questions are typical questions that fit into a case study. Also, protocols are needed to increase the reliability of the research.

3.1. Qualitative study protocol

The study initially started with an embedded multiple-case study approach. The aim was to analyse several companies and agencies within the financial industry. However, the study had to be converted into a qualitative study due to the given duration and the reflection on the study in the later stage. Yet, the approach of the case study has been used to guide the research study. Creating a protocol similar to a case study protocol will help strengthen the research's reliability. Yin (2018) suggests three strategies that should be used during the data collection phase, which are (1) the use of multiple sources of evidence, (2) creating a case study database, and (3) maintaining a chain of evidence. The following chapters will discuss these three strategies (Yin, 2018).

3.1.1. Data collection

Yin (2018) proposes to use five levels of questions in the data collection phase within case studies. These five layers will help shape a procedure to identify what information will be collected in a case. The levels of questions are not necessarily focused on the interviewee but help as an instrument to determine what should be asked and why.

- Level 1: Questions that are focused on specific interviewees
- Level 2: Questions at a level of individual cases.
- Level 3: Questions to find certain patterns across the cases
- Level 4: Questions at a level of the entire research
- Level 5: Normative questions going beyond the narrow scope of the study. This may cover policy recommendations and conclusions.

The first level of questions is the interview questions that have been asked to the specific interviewees. In this case, there were two interview protocols for an MPC expert and a non-expert. These MPC experts were not actively engaged in the financial crime domain but had existing use cases with the actors in this industry. Therefore, specific questions differed from the non-expert protocol.

The second-level questions are the primary focus of the case study protocol. This level addresses the second and third sub-questions of the research. The third and the fifth levels are not relevant to this study, while the fourth level addresses the fourth sub-question of the research. These are questions asked on an entire study basis.

The case study will rely on two different sources of evidence. Using triangulation will strengthen the findings of the case but, in most cases, would be difficult because documents in the financial crime industry are likely confidential. Therefore, the first data source will be obtained through interviews. These interviews will be recorded and transcribed. As it is crucial to safeguard the confidentiality and privacy of the human subjects, all recordings will be destroyed after completing the transcription. In addition, this transcription will be anonymized as the industry is small and isolated. The final transcription is shared with the interviewees to validate the reports' correctness.

Finally, the fourth level will question the whole study. In this research, the fourth level of questions will help to address the fourth research question.

3.2. Interview protocol

The research will use a semi-structured interview structure for the interview. The benefit of a semi-structured interview is that open questions would allow adapting the questions to the conversation. This study focuses on identifying the factors and barriers to collective action. Therefore, the responses of the participants can be unpredictable. Consequently, it would require an open approach. Furthermore, the semi-structured interview protocol allows for incorporating the theory proposed by the literature in the interview questions.

3.2.1. Interviewee selection

There is a broad spectrum of experts within the Financial Crime industry with different roles and expertise. However, this research will sample interviewees based on two conditions, as not every participant would suit the scope of the study.

The first essential criteria are based on the knowledge level of MPC and their understanding of the current technology landscape. As data and sophisticated technologies highly drive the current industry, it would be less viable to invite an expert without any technological capabilities. Therefore, a participant will be assessed prior to the interviews based on their experience (by developing MPC in real use cases) and their knowledge about the function that MPC serves. In addition, the findings of the interview expert will be re-evaluated and help to determine if the participant was knowledgeable and a genuine expert. Therefore, the studies will include a mix of MPC experts and non-experts, whereas the findings of the experts will be used for validating the responses of the non-experts. The second criterion will help to assess whether the interviewee is an expert or non-expert.

The second criterion is based on their experience and the power of their position. As the financial industry is complicated to understand, it would require interviewees with significant experience and background to acquire relevant information. Also, their high degree of power in decision-making processes was considered suitable. Hence, introducing or engaging in collective action would require a managerial position. Therefore, potential participants with less power in decision-making or business strategies were excluded from the interviews.

The majority of the interviews were obtained through the network of the researcher's connections, as the domain is isolated and small. To arrange interviews within this isolated industry, the connections established initial communications. These connections provided the contact details and informed the potential participant about the research project. It was followed by communications concerning the willingness to participate and availability. The desire to participate, or most of the candidates would phrase it as "contributing", was decisive by the interview questions and the interview presentation.

The following table contains a list of all potential interviewees before the communications. Some potential candidates did not respond to the interview invitation, and some declined to participate. Nine out of the 12 interviewees agreed to participate in the studies. However, two candidates withdrew from the studies after receiving the interview script. The reason will be discussed in the findings as it could indicate parties' interest in MPC developments.

	Sector	Expert/Non-Expert	Function/Role	Agreed to interview	Interviewee code
1	Public	Expert	MPC developer	Yes	INT- 2
2	Public	Expert	MPC Researcher	No	-
3	Public	Non-expert	Prosecutor	No	-
4	Public	Non-expert	Strategic Analyst AML	Yes	INT- 1
5	Public	Non-expert	Digital Investigator	Yes	-
6	Public	Non-expert	Digital Investigator	Yes	INT- 4
7	Public	Non-expert	Forensic Examiner	Yes	INT - 6
8	Private	Non-expert	Attorney specialized in Fraud cases	Yes but withdrew	-
9	Private	Non-expert	Attorney specialized in Fraud cases	No	-
10	Private	Non-expert	eDiscovery Manager	Yes	INT - 3
11	Private	Non-expert	Financial Crime Data analyst	Yes	INT – 5
12	Private	Non-expert	Forensic Examiner	Yes	INT - 7

Figure 6 - Interviewees

3.2.2. Interview procedure

Yin (2018) mentions that ethical considerations can arise in research that involves human subjects. It requires several actions to protect human subjects and their data within the case study (Yin, 2018).

First, formal approval for the plan needs to be acquired. The plan aims to identify and assess the risks within the case study research involving human subjects. A data management, data risk assessment, and informed consent form have been drafted for this research.

The second action is gaining informed consent from the interviewees who participate in the study. These informed consent forms are distributed before the interview, as it is essential that participants volunteer for the research study. The document also states that interviews will be recorded to be revisited easier. This statement is repeated at the beginning of the interview.

Finally, the privacy and confidentiality of the participants need to be ensured before, during, and after the interviews. Therefore, the recording has been turned into transcriptions. These transcriptions are completely anonymized because of the characteristics of the industry, which is isolated and small. Once all recording is transcribed, the recordings will be removed immediately. The transcription is used to corroborate the findings and validate the propositions.

3.2.3. Interview questions

The study will involve participants with knowledge of MPC and non-experts. These two groups have different interview questions. The non-experts are the key actors in the current Dutch financial crime industry. These actors have not been exposed to Multiparty Computation yet. Hence, these interview findings need to be cross-validated with the existing literature. The interview script for the experts will be based on their current use cases. The outcome will be validated with the literature but will illustrate the practical examples and values.

3.2.3.1. Non-experts

Interviews with non-experts were conducted to collect their opinion, experience, and values. These findings are used for evaluating and testing the conceptual model developed at the start of the study. The purpose of the conceptual model is to provide stakeholders and academia with an overview of the factors that are essential in the actor's decision-making process of engaging in collective action. The non-experts will help to illustrate the perspective of the actors operating in the financial crime industry with minimal exposure to MPC.
There are primarily 13 questions in the interview script for the non-experts. These questions are derived from the existing literature and the conceptual model. The questions are sorted in a sequential order, which will cover the concepts.

1. Could you please briefly tell me about your background and position?
2. What are the common or critical challenges that you have face or seen in a financial fraud prevention project? Challenges that are more focused on the technological side such as data sharing or technical capabilities? Please do not mention any company names or confidential information
3. Have you heard of MPC or seen any use cases of MPC before?
4. What kind of technologies does the organization use? (if it's confidential or critical, please describe the kind of technology)
5. I introduced the concept of MPC. What would be the reasons or factors for you to consider multiparty computation in your working field or company?
6. What kind of challenges or discouraging factors should be addressed when it comes to introducing MPC into the "forensic" landscape? By landscape, I refer to the ecosystem, networks (stakeholders and partners), and technology.
7. Thanks for sharing your thoughts. Previous questions focused on the factors. Lets assume you are considering to work on MPC. What would be the role of "trust" in developing and adopting multiparty computation?
8. Proceeding with the focus on "trust". Would specific companies or organizations have an influence on the trust? If so, in what way? And why?
9. Would working with new parties affect the level of trust on the cooperation? If so, would it increase/decrease the trust in the technology too?
10. The technology or use-case development can be led by the private as well as public sector. How important is the structure of leading the project for considering to take part into the development? and why?
11. What is your preference in regard to the structure (private or public)? And why? Would that increase the "trust" in deciding to participate?
12. Would the group size affect your decision to participate? What would be the ideal group size for you (small or large)?
13. Would enforcing selective incentives or punishment increase your trust in partnering up with new parties? And why?
14. Do you have other remarks that you would like to share or address?

The purpose of the first four questions is to acquire the interviewee's background. The interviewee's background is used for post-interview assessment to validate their relevance in the studies. Also, it helps to obtain the first impression of the knowledge level and the respondent's challenges. The fifth and sixth questions aim to extract the motives and reasons

that demotivate parties to engage in the development or adoption of MPC. Starting from the seventh question, the focus is put on the trust factor. Questions eight through eleven aim to collect information about the governance and the trust in public and private parties. The twelfth question targets the group size. The question aims to identify if the group size will affect the trust. The final question thirteen will go into the concept of introducing selective incentives and punishments.

3.2.3.2. Experts

Experts were interviewed to extract the essential factors and barriers based on their experience and recollection. It helps to understand the actual need of the actors in a real case. The interview findings with the experts were also used to validate the findings given by the non-experts. Any similarities or differences would help to evaluate whether the current set of propositions or factors is sufficient to explain the behaviour of financial crime actors in engaging in collective action. The experts were assessed prior to the interview. It is essential to have experts with a lot of understanding of MPC and preferably have worked on real cases. The findings were also used as a post-interview expertise assessment. The second interview script was tailored in a way to extract the experience of the experts. This script consisted of ten questions.

The questions differ from the non-experts, as they mainly focus on the existing use cases.

1. Could you please briefly tell me about your background and position?
2. What are the common or critical challenges that you have face or seen in MPC use-cases?
3. What would be the reasons or factors for you to endorse multiparty computation to parties that are not familiar with the concept or new potential partners?
4. Have you managed to identify what motivates party to work on MPC? (I'm referring to previous MPC use cases that you have been working on)
5. What would be the role of "trust" for you in developing or adoption multiparty computation? What is the role of "trust" in finding new partners to create use-cases? How? And why?
6. Would working with certain type actors play a role in deciding to participate? Who, why and how would it affect the development of use-cases? Would working with new parties affect the level of trust? If so, in what way?
7. The technology or use-case development can be led by the private as well as public sector. How important is the structure of leading the project for partners to consider to take part into the development? and why?
8. Did the size of collective group in your existing use-cases affect the outcome? How? And why?
9. Does your existing or previous use-cases considered to enforce selective incentives or punishment to enhance the collaboration? Does that increase the trust in the partnerships with existing or new partners? How? And why?
10. Do you have other remarks that you would like to share or address?

The first two questions' purpose is to acquire the interviewee's background. As mentioned earlier, the interviewee's background is used for the post-interview assessment to validate the relevance of the participant in this study. The third and fourth question aims to identify the factors that motivate parties to participate but also reasons to demotivate. Since the expert especially developers already trusts the technology (because it is developed by them), the fifth through seven questions will focus on the role of trust and the type of structure. The eighth question tries to discover the effect of the size of the collective group on the outcome in their

existing use cases. Finally, the ninth question aims to identify the impact of introducing selective incentives and punishments in the current use cases.

The following table summarizes the research concepts and the corresponding questions.

Relate to the concept	**Question**
Contribute to the collective goal (Proposition 2)	ProtA_Q5, ProtB_Q3, ProtB_Q4
The role of trust on collective action (Proposition 4)	ProtA_Q7 ProtB_Q5 ProtB_Q6
	ProtA_Q8
	ProtA_Q9
The role of governance on trust and collective action (Proposition 4)	ProtA_Q10 ProtB_Q7
	ProtA_Q11
The role of group size on trust and collective action (Proposition 3)	ProtA_Q12 ProtB_Q8
The role of selective incentives or punishment on trust and collective action (Proposition 1, 2, 4)	ProtA_Q13 ProtB_Q9
The challenges / barriers of MPC	ProtB_Q2

Figure 7 - Questions per concept covered

3.2.4. MPC interview presentation

The respondents were asked to evaluate their knowledge of Multiparty Computation before the interviews. It would help to assess whether the provided information was valid for the study. Most of the participants had never heard of or been exposed to the concept of MPC. Therefore, a presentation was created to help the interviewees to understand the fundamentals and potential use case of MPC.

The presentation was divided into four elements:

- The definition of MPC and the basic concept (Slide 2)

  The basic concept and definition of MPC has been illustrated in the first element. It would provide the interviewee a general understanding of the function of MPC. The first element has been validated with an external, which helped in advising and worked on MPC studies as well. Also, the literature of MPC have been used to create a common definition and understanding of the concept.

- An example case of MPC (Slide 3)

An example case of MPC has been provided to the interviewee, as it could be difficult to create a vision the function of MPC. In this case, a classic example of calculating the average salary among employees have been used. The main reason for choosing this example is that it reflects on a sensitive case where actors would not disclose their information with other actors. Also, the example has been typically used in different studies as well.

- The current situation for the use case (Slide 4)

The third element tried to illustrate the current situation and especially the limitations in the financial industry. The figure emphasizes on the lack of available data because data sharing is on a voluntarily basis (without a court order). The situation is drafted based on the perspective of Deloitte Netherlands Forensic workflow as well as literature that describes that actors are reluctant to share data.

- The introduction for the use case (Slide 5)

The fourth element shows the potential of SMPC and how the current data sharing barrier can be tackled with a privacy-preserving technique. It helps the interviewees the objective of adopting the technique. This section was essential because it would affect their answers on the interview questions. Interviewees with an unclear vision and understanding of the whole concept and use case would provide invalid or irrelevant information to the study,

These elements can be found in the Appendix C – Interview presentation.

3.3. Data analysis

A data analysis approach has been set for this research to strengthen the reliability of this research. Yin (2018) mentions that a procedure for data analysis is required as part of the research design. The interview transcripts will be reviewed and coded according to a specific system. This section will describe the coding process and the data comparison.

3.3.1. Coding process

The Atlas.ti data analysis software for analyzing qualitative data is used to perform the coding of the interviews. The literature review helped to identify the relevant concepts for the topic. These concepts are used to shape the first initial coding list. Some codes are also derived from breaking the questions and propositions into separate concepts. The research used open, axial, and selective coding to structure the findings and reduce the number of codes.

The first coding round used the initial coding list but remained open to new codes. The coding list contained 32 codes based on the literature and broke the propositions and questions down into single terms. In addition, the open coding helped to identify 16 more codes that could be used for analyzing the other transcripts. However, these open coding contained duplicates, and finding patterns in the transcripts remained challenging. Also, some early codings created did not have a relevant hit. These codings were removed, and the remaining codes were listed to identify any concepts. The subcategories, reasons, and factors were not mapped or grouped into the corresponding category. Therefore, the codes were aggregated with the main concept. For instance, any code that belongs to a barrier would have a prefix of barrier, and the concept would be separated from the subcode by a colon. Based on the aggregation, a subcategory could be identified. It provided much more insights into the responses compared to the first iteration of coding. The subcategory can also be seen as the pattern within the empirical findings. The final iteration merged the main concept with the pattern and the detailed response.

An example is that free rider behaviour can exist in the industry. However, it cannot be guaranteed that the behaviour will exist. Free rider behaviour is asked during the part of selective incentives and punishments. If some participants deny the existence of free rider behaviour, then the incentives and punishment would also not affect the trust. Therefore, the code would be Freerider:SelIncen:NoEffect, as the first part illustrates the concept, the second part the pattern, and finally, the specific response.

The following table illustrates the coding rounds with the total codes. These codes can also be found in the appendix. There is a relatively low number of codes for this study due to the semi-structured interview. In addition, the structure assisted with reducing the noise (irrelevant) information from the interview scripts.

Coding round:	Number of codes:
Open Coding (Initial list)	48
Axial Coding (Reduction of initial)	41
Selective Coding (Final list)	28

Figure 8 - Coding rounds

3.3.2. Data comparison

The empirical findings provide a certain understanding of the perspectives of the participants. However, these findings need to be validated with a different source of evidence. The risk of using sole empirical findings is that it will impact the quality of the research and is subjected to participation or recall bias. Therefore, the data will be compared with two different sources of evidence. The first step is to compare the empirical findings with the conceptual model. It helps to understand the differences and the similarities. The second step would be combining the outcome with the existing studies. The triangulation of the data would help to identify possible anomalies and to support certain patterns.

4. Results

The primary objective of this research is to find the factors and barriers that influence an organization's decision to engage in collective action for developing MPC for fraud detection. Several interviews have been held with different actors operating in the Dutch Financial Crime industry to acquire insight into their perspectives and experience. In order to answer the research question, a set of sub-questions has been drafted to break these findings down in a structured manner.

4.1. Current fraud detection landscape

It is essential to understand the current Dutch fraud detection landscape as it might explain the behaviour of certain actors. Therefore, this section tries to answer the second sub-question, "*What are the collective goal, drivers, and barriers to adopting SMPC in the financial industry?"*. This sub-question has been broken down into three questions to understand the individual subjects.

- What are the barriers in the existing landscape?
- What motives are the financial crime prevention actors to develop and adopt SMPC?
- What are the reasons the financial crime prevention actors do not collaborate in developing SMPC?

4.1.1. The barriers in the existing environment

Identifying the current barriers in the existing environment is necessary to understand the status quo. It can help to indicate the potential role and value of Multiparty Computation for the industry. The participants have been asked to summarize and exemplify barriers that they have been experiencing in their current working field. At the end of the question, the focus is shifted to the "data sharing" aspect. The interviews showed similarities but also differences in response.

Similarities

Almost every interviewee mentioned that the data privacy regulations partially cause the current data sharing restriction. These regulations do not allow any party to collect or process data without a purpose (***Barrier:Datasharing:RequiresPurpose***). One of the interviews also illustrated this in a banking industry case. The banking industry possesses a lot of data that can be used to predict and improve the current fraud detection models by collaborating. However, the banks need to comply with the regulation of private organizations. Therefore, banks require a valid purpose to legitimize their data sharing action involving personally identifiable data. The participant has been involved in certain bank cases and stated it as follows:

> *"The GDPR is of course making it difficult for banks to exchange data. To save data and re-use it, it requires a purpose"* (**INT-5**)

Consequently, the interviewee argued that regulations might be the predominant barrier limiting actors from collaborating with other parties by sharing data. However, it does not entirely rely on the data protection regulations as people might think. As the interviewee argues that key stakeholders such as the banks do not put enough effort into improving their current landscape and collaborating with other parties for a beneficial collective goal (***Barrier:Datasharing: Lackofeffort***). According to his experience, the most prevailing reason for the lack of effort and banks are reluctant to participate or improve their current workflows – is the lack of incentives and benefits (***Barrier:DataSharing:Lackofincentives***). The banks do not see any benefit in sharing their data with their competitors and investing their own money into new technologies that could improve their systems. The following quote describes this situation:

> "*Besides banks being fined, they do not have any incentive or reason to use their own money to invest or improve their current systems.*" (**INT-5**)

An alternative perspective is that regardless of the financial resources and the data protection regulations, there might be internal reasons for actors not sharing data with external parties. This is because the data contains valuable information that parties with malicious intentions can use to gain a competitive edge. The interviewee emphasized that it might be a reason for banks to be hesitant due to the competitive advantage it possesses. This is especially since data is becoming the "new gold". The meaning of "new gold" is that data becomes a valuable resource for parties.

The figure below summarizes the potential factors and reason that causes the current data sharing challenge.

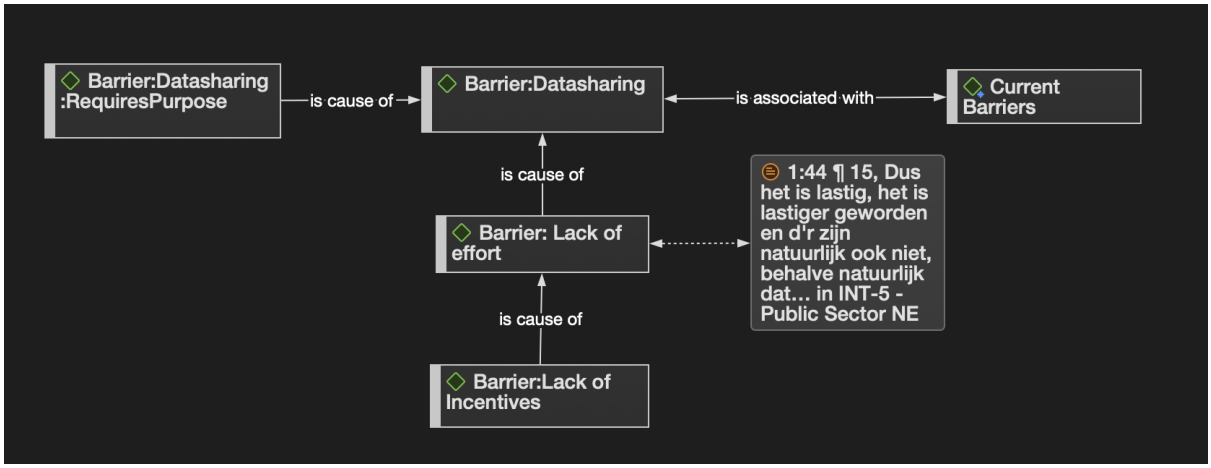


Figure 9 - The barriers in the existing environment

Differences

The interviews (**INT-5**, **INT-6**, **INT-7**) also brought up new perspectives that were not captured by the literature and mentioned by the other participants. For example, interviewees, operating in the private sector mentioned that in some cases, there is still a way to issue data.

> "*If we have a good relationship and we are requested by the Board of Directors. That should be okay, and we will be able to get it. However, if the Board of Directors are not consenting with the project or the way of how the project is heading, or data that we want to analyze, or additional data that we need then they could be hesitant*" (**INT-5**)

This infers that data sharing barriers are not exposed to only regulatory influence but also depend on the force exercised by the management. The quote above also highlights that departments need to comply with upper management orders. Additionally, it shows that there are workarounds to acquire data, which means the data sharing barrier can be overcome through authority and consensus.

It was also mentioned that sometimes analysis can be performed without sharing any data. As quoted by the interviewee:

> "We performed analysis on their system, which means that the data had not to leave the client's premises. It happens occasionally that we collect data but that generally involves just one client. There has been one occurrence which five clients shared data with us." (**INT-1**)

The quote illustrated above shows that data sharing barrier solely exists in certain cases but can be avoided depending on the circumstances. The latter mentioned has been confirmed and expressed in the interviews with actors operating in the public sector. Data protection regulations can influence actor's decision in exchanging data, but it does not apply for agencies or law enforcement. Criminal investigations or litigations are not directly subjected to the regulations if they have lawful purpose of collecting data for litigations or criminal cases.

> "We work from a criminal investigation perspective, so we are less subjected to the AVG… Sometimes it would be great to acquire more data but then we would go to the AVG again. You will have to look at the privacy impact." **(INT-4**)

However, if law enforcement or public agencies want to acquire more data outside their scope and boundaries, they will be subjected to the data privacy regulation again. A different interviewee in the public sector also confirmed it and stated:

> "...Separate from the police and from any other investigative agencies. This implies that you won't be able to access the other party's system. Hence, you cannot provide for example a zip-file on a network drive and tell the police where to find it. You are a stand-alone institute, but you share data with your client." (**INT-6**)

It means that their power is only extended to a certain limit which is defined within their legal and criminal investigation cases. The agencies do not have mutual access to their systems. If they still want to acquire more data for the sake of the investigation, they will have to request as the private parties. The next section will shed a light on their opinion on the suggested technology of MPC to overcome the privacy concerns and enabling safe data sharing.

4.1.2. The motives for parties to develop MPC

A vast majority of the interviewees have never been exposed to the concept of multiparty computation. Therefore, an interview presentation has been presented to the participants, as mentioned in the previous sections. In this presentation, the concept of MPC and the use case have been explained to the participants. The main question that arose during the interview was, "What motivates the parties to develop or adopt MPC?" the brief introduction. Therefore, whereas MPC experts provided actual examples in their use cases, non-experts will provide their opinion about participating in developing MPC for a collective goal.

The interviews with the expert and non-experts showed commonalities in their response, as they mutually agreed on the motives in different phrasing. The interviewees from the private sector framed it as a solution to comply with the data protection regulations such as GDPR. Whereas Multiparty computation would facilitate privacy and regulation complying data exchange among parties to acquire a richer dataset for better analysis (**Motive:RicherDataset:BetterAnalysis**). This has also been illustrated in the following quotes on how multiparty computation could act as a data-sharing and privacy-complying enabler:

"… but on the other side, we cannot see the source of the money, whether it originates from a criminal group which invests more money into. That would then indicate that it is not progressing in the right way. This motivates companies to share data and helps to circumvent the GDPR." (INT-5)

Another interview with a company that develops Multiparty Computation solutions for different sectors, industries, and organizations has confirmed the vision of how the private sector thinks about MPC. The response of the MPC developer was based on their experience and existing collaborations with public and private parties building MPC use cases. The company (INT-2) noticed that interested parties are primarily seeing multiparty computation as a way to address the current regulations but also to satisfy the data protection officers. The following quote describes this:

"Well, the most important is that people, parties will say: we want to collaborate on a data level. We want to combine data and analyse it together, but that cannot be performed now because our privacy officer isn't comfortable that we are sharing data with other parties… And yes, if they hear about the opportunities with MPC, they'll understand that it could facilitate it…." (INT-2)

The same vision is shared in the public sector as they framed it differently. The public actors see the potential of MPC as a technology to minimalize privacy impact while acquiring more data. The additional data could help to provide more essential insights into the investigation while safeguarding privacy and confidentiality (**Motive:Richerdata:ReferenceSet**). However, there was a different interpretation of "insights" among the interviews.

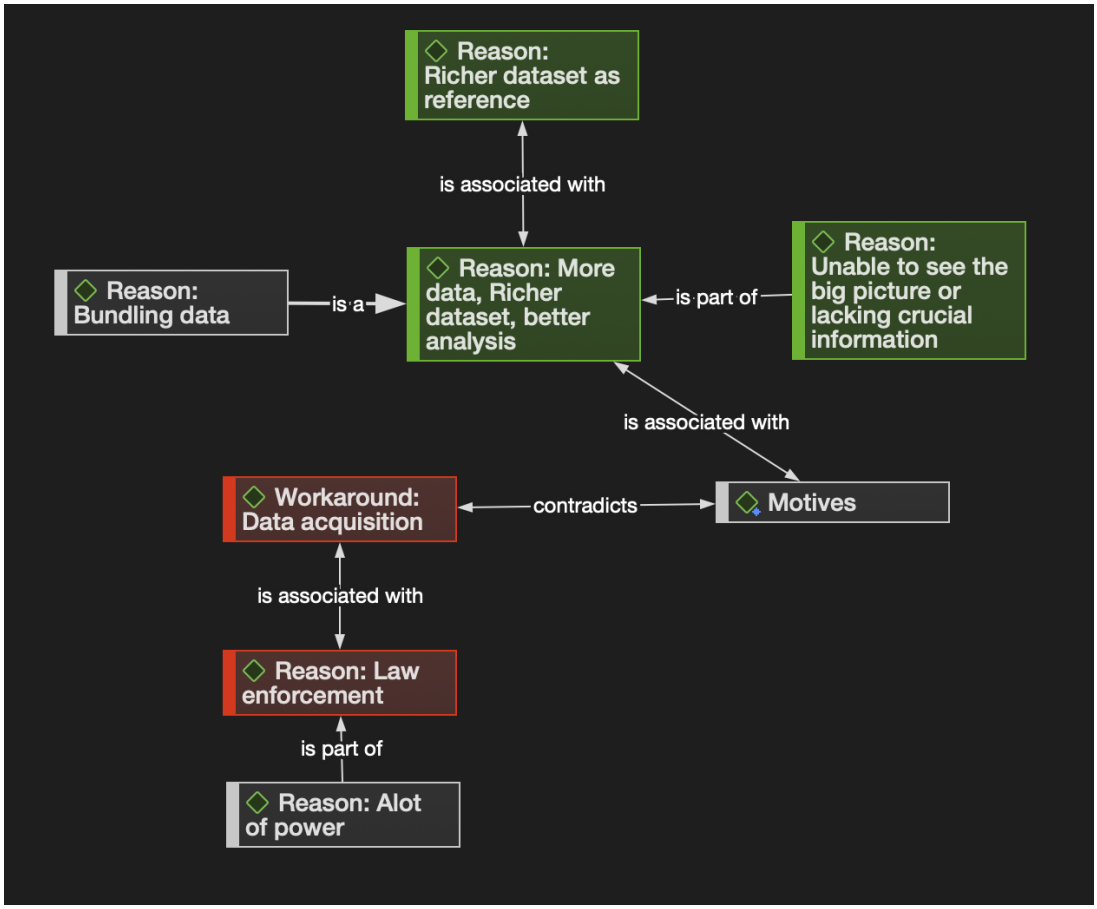


Figure 10 - The motives to develop MPC

> "Well, you can imagine that in some situation that it would be great to have access to more transactional data. For instance, you could identify the pattern of a criminal organization."
>
> "I rather have a lot of data that I will need to perform data analysis. To recognize the fraud cases better."
>
> "I think there are a lot of opportunities because it might help to reduce the privacy impact while it could provide insights for the investigation."

All the interviewees were working in the Financial Crime industry, but they had a different set of responsibilities. Some (INT-1 , INT-5) are working on the analytical part of the fraud detection (pre-emptive) and others on the actual case reactively. The data would serve a different purpose depending on their responsibilities. However, both saw the benefit of having bundled data as reference for their analysis.

Although, it is important to take the differences in legal boundaries for public and private parties into consideration. In case of the public sector, there are workarounds for the data sharing and acquisition barrier (***Motive:Workaround:DataAcquisition***). As the law enforcement or any public agency will work on a criminal and legal basis, which can exempt them from certain law or regulation (***Motive:Workaround:Power***). This will be elaborated in the next section, which covers the reasons that affect parties' decision to not collaborate with other parties.

4.1.3. The reasons to not to participate

The previous section identified that the main motive for parties to collaborate and develop MPC is primarily the merits that entail acquiring more data while complying with the data privacy regulations. Yet, there might also be reasons for actors not participating in developing or adopting MPC.

The main motive for parties to collaborate and develop MPC is primarily the merits it brings by complying with data privacy regulations while having a larger reference dataset. Yet, there might also be reasons for actors not participating in developing or adopting MPC. The literature outlined four prevailing barriers for MPC:

- The complex challenge of building trust.
- Lack of consideration of integration.
- The performance and lack of scalability.
- Underestimated risk of processing sensitive data within SMPC.

The barriers hypothesized by the existing literature were not the primary focus of the interviewees. However, it did relate to the challenge of building trust, lack of consideration of integration, and underestimated the risk of processing sensitive data within SMPC but very insignificant and interpreted differently.

First, Veeningen (2018) mentioned that acquiring the trust of key stakeholders can be very challenging since the current techniques are sophisticated and challenging to understand for non-technical entities (Veeningen et al., 2018). The interviews showed the contradiction, as only one interviewee emphasized "trust" as the key factor of potentially not collaborating during the interviews.

"*A reason not to use, that's a good question. I don't see many downsides except vulnerability… if a vulnerability exists and you are not aware of it, even if it's temporary, it could lead to reputational damage for the banks.*" (INT-5)

As the quote highlights, the trust factor does influence the reason not to participate but in a different manner. The trust defined by Veeningen (2018) argues from a transparency and knowledge perspective. In comparison, the interview shows that trust starts with the safety of the MPC. This infers actors are less concerned about transparency and the encryption algorithm than safeguarding data privacy. The interviewees predominantly mentioned the emphasis on data privacy during the question of motives to develop MPC. Hence, an alternative explanation for parties to have trust concerns would be the trust in safeguarding the data integrity.

Second, Clifton et al. (2004) and Balamurugan et al. (2012) highlighted that data integrity and standardization of the MPC input or data integration could be challenging (Balamurugan et al., 2012; Clifton et al., 2004). Yet, the interview illustrated that actors are not concerned about data integrity, standardization, or integration but, more importantly, how MPC can be utilized in their current processes. Also, questioning whether it would be limiting their workflows, as quoted by INT-6

> "*And yes if it would limit the research. If it would have a certain amount of limiting factors that won't allow me to perform my job well then it would be a reason for me not to use it.*" (INT-6)

Another perspective regarding the integration illustrated by the interviewee (**INT-5**) is the integration of the system in the current technology landscape. For instance, banks might be still using legacy systems which cannot be replaced easily by new technology such as MPC.

Other interviews proposed that the most prevailing reason affecting parties' decision not to participate or develop MPC is the uncertainty of what MPC potentially could bring to the organization. This uncertainty is two-fold. First, there might be cases for the public sector to not use MPC for acquiring additional data for their investigations. This can be explained by the response of the interviews in the previous section, which shows that public agencies and law enforcement are working on a legal basis. It exempts public actors from specific regulations and allows them to perform their job within their investigation boundaries. In addition, collecting too much data might violate entities' freedom, as illustrated in the quote below.

> "*On the one side, ideally, you want to have as much data, but on the other side, you don't want to become a police state where nobody has their secrets*." (**INT-4**)

It displays that there should be a balance between the data being collected and acquiring too much information that might violate the freedom of entities. The private sector is uncertain about what the added value could bring to their organization and workflows. The explanation for this uncertainty is the lack of knowledge, which the interviewees repeatedly highlight.

Interview participation
Several actors have been asked to participate in the interviews. These actors were attorneys and public agencies. Some of the potential participants requested further information about the topic and decided to decline the interview. Other invited participants chose to withdraw from the interviews without providing any reasons.

All potential participants who withdrew or showed interest in the study did ask for more information about the topic because they were unfamiliar with the MPC concept. The assumption is that the invited participants decided not to participate because of their lack of knowledge. To validate the assumption, a question has been asked to the participants that did not make it into the interviews. Eventually, one response was received. The primary reason for not participating was the lack of knowledge and inability to contribute to the study, as MPC would not fit into their workflow.

Finally, the previous section showed that the current data sharing barriers are partially caused by the lack of incentives for parties to collaborate, as they might not be interested in investing money into a technology to improve their workflow, especially if it is costly. This has been mentioned in an interview as the interviewee quoted below.

> "*Yes, it will be costly to implement, of course. It probably will take a lot of time to set it up and diffuse the knowledge. Also, I think it is difficult to explain it to people that never used it before.*" (**INT-7**)

This quote displays that financial distress can influence and demotivate actors to develop MPC. Their lack of knowledge could explain it, but it also takes time to implement a system like MPC. It might be the case that entities will not be willing to invest in any technology such as MPC because they are not aware of the merits it can bring but also do not possess sufficient knowledge to understand what they are investing in.

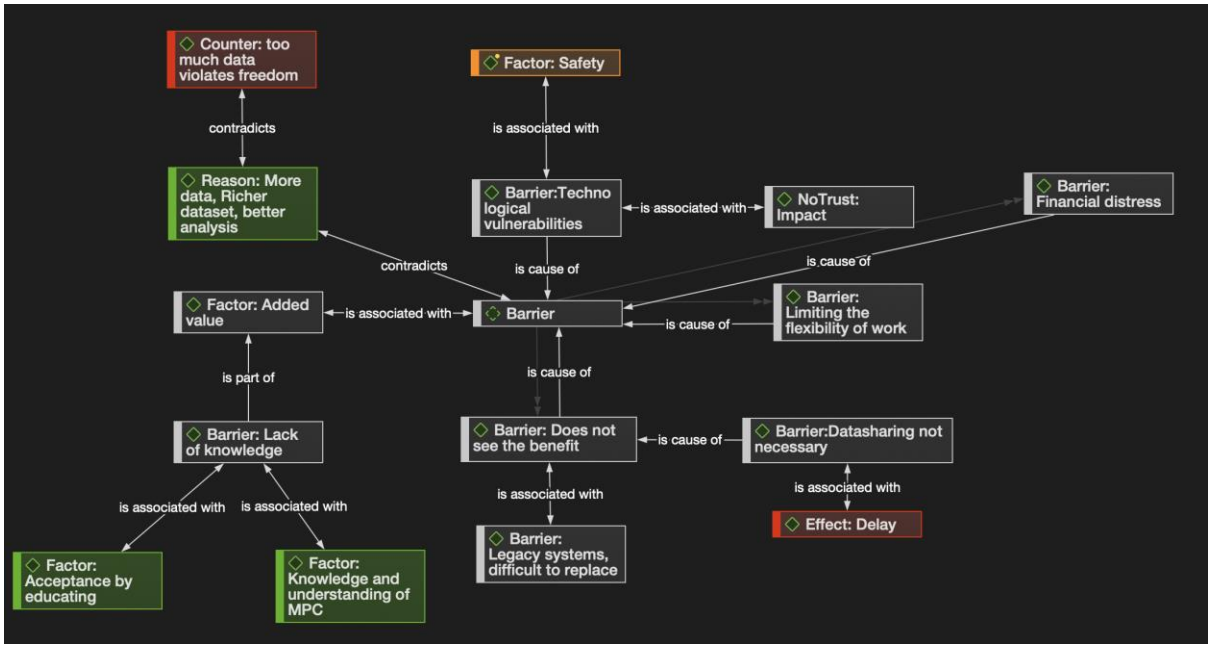


Figure 11- Reasons not to participate in developing MPC

4.2. The interests of stakeholders in MPC

The previous section tried to answer the second sub-question, "What are the collective goal, drivers, and barriers to adopting SMPC in the financial industry?". It helped to get a basic understanding of the important barriers and what potentially motivates parties to engage in collective action in developing MPC. The results illustrated similarities and differences between the factors identified from the interviews with actors operating in the Dutch Financial crime industry.

This section will try to answer the question, "What are the trade-offs between the interests of key stakeholders?". Veeningen (2018) highlighted that identifying all stakeholders and their concerns cannot be performed with some basic research. Therefore, the output of the previous section and the input of the interview, in combination with the literature, will be used to get a better understanding of the following:

- How does trust play a role in the decision of developing and adopting MPC?
- Would the type of organizations influence the trust of parties?
- Would the type of governance affect the party's decision to participate?
- Would the group size affect the party's decision to participate?
- Would selective incentives or punishment help to motivate parties and improve the trust?

4.2.1. The role of trust

It could be concluded from the previous section that "trust" was not the main factor for parties that would affect parties' decision to engage in an MPC collaboration. Yet, it is still essential to understand the role of trust in the decision-making process of actors, as participants might not have considered the factor.

The interviews showed a diverse view of how the trust would affect the actor's decision to participate and how actors would overcome specific trust challenges. The interview with the expert (INT-2) pointed to a shift in the type of "trust". The expert defines the shift as follows:

"There is a shift of trust, from the trust of the party which will be collaborating with. In the past it was primarily focused on this type of trust… but its shift to the trust in technology." (INT-2)

This implies that the type of "trust" has changed over time. The parties would consider trust in technology a more critical factor than the counterparty. This phenomenon can be validated by the responses discussed in the "The reasons for not to participate" section. The actors were primarily concerned with safeguarding their data privacy and the safety of MPC technology. Therefore, the trust among parties is less relevant in the decision-making process for stakeholders to engage in the collective action to develop MPC.
Moreover, an interview with a financial crime investigator that provided litigation support shared the same opinion. His experience showed that clients find the trust in the relationship less relevant. Their clients are comfortable with the technology if the firm recommends it. Their logic is that clients depend on any organization's expertise and resources. Despite those emerging technologies are not transparent, their customers do still trust the technology. The firm does not possess complete knowledge about the technology or algorithm but is still confident with trusting it. The reason is that it is widely used across the market. This may infer that adoption and acceptance of new technology can be accomplished by introducing it to the remaining of the market.

> "[…] that is almost the same with predictive coding in eDiscovery" (**INT-3**)

The quote above illustrates that the firm and market currently use similar existing technologies. Predictive coding is an example in the eDiscovery domain. This domain is specialized in finding fraudulent electronic evidence that will be provided to clients for litigation support. This predictive coding has an algorithm that is not transparent. Although, it is widely used and adopted by practitioners. Multiparty Computation is a technology that has not been introduced to the market yet. It can be argued that if multiple parties decide to engage in collective action, peers in the same market would follow and participate in the development.

> "*At the start, you could possibly use the classical techniques to identify the differences in outcomes*" (**INT-3**)

Additionally, the statement above shows that a comparison between conventional techniques with newer technology can be proposed to acquire the trust of other market parties. Using benchmarks would convince and build trust among parties by displaying evidence, in this case, the performance and the result of MPC. In addition, the MPC expert has stated in their interview:

> "*It is not transparent; it is unknown now, but to the people we explained it – they say they understand it. They will not be able to look at the MPC on a detailed level, but*

they have enough trust to work with it […]. A client wants to know it on a system-level and later code-level. They want to be ensured that it does what it should do.". (**INT-2**)

This conversation shows that trust can be accomplished by educating and providing the proper knowledge to the stakeholders. The stakeholders do not need a complete understanding of MPC on a detailed level. However, in some cases, actors want to be ensured and audit the system and code. The demand for a full audit of the technology might confirm that trust in technology is an essential factor, as it was mentioned before. A potential explanation is that it could depend on the industry in which the MPC use case is developed. The data that is processed and used in their workflows are highly sensitive.

An alternative explanation could be the lack of knowledge and uncertainty on what the added values of MPC hold for their organization. The interviews showed that actors were interested in MPC to address the GDPR and collect more data. Although, MPC is not a solution for sole addressing GDPR. The purpose of MPC is to perform joint analysis based on multiple data sources that are encrypted throughout the process. That might clarify the interviewees' hesitation in answering the interview question, "I introduced the concept of MPC. What would be the reasons or factors for you to consider multiparty Computation in your working field or company? ". An example displays the lack of knowledge can be illustrated with the quote below.

"*Everything that we do is highly confidential. We could potentially use MPC, but I don't know how it is set up and if we use our servers or public hosted servers*." (**INT-6**)

Actors do not have adequate knowledge of what MPC holds and providing the fine details of MPC would not be possible, as the interview (**INT-2**) mentioned. Therefore, different approaches will be necessary to provide sufficient basic knowledge to reduce uncertainty and gain trust.

Finally, other interviews mentioned that societal trust might also be necessary. It can be argued that the Financial Crime industry can be seen as a domain serving the public. The information will originate from society and companies, so it will require consensus to process and analyze their data. Moreover, their data will be put at risk for improving the data analysis, as quoted below.

"*It is a problem of the society, where the whole society suffers and needs to be solved by the society. In terms of fraud, a societal challenge and therefore you will need to let the society have a word too."* (**INT-4**)

"*Maybe the trust of the society because they surely want the banks to make it a safer environment and encourage them not to participate in money laundering or terrorist financing. They will block it for their clients and society in general."* (**INT-5**)

The quotes try to emphasize that implementing a new technology that serves or supports a public serving industry requires the involvement or trust of society. Therefore, the following section will elaborate on how the collaboration type affects trust. Furthermore, it tries to identify how the kind of collaboration will help to promote and acquire the trust of the actors and society.

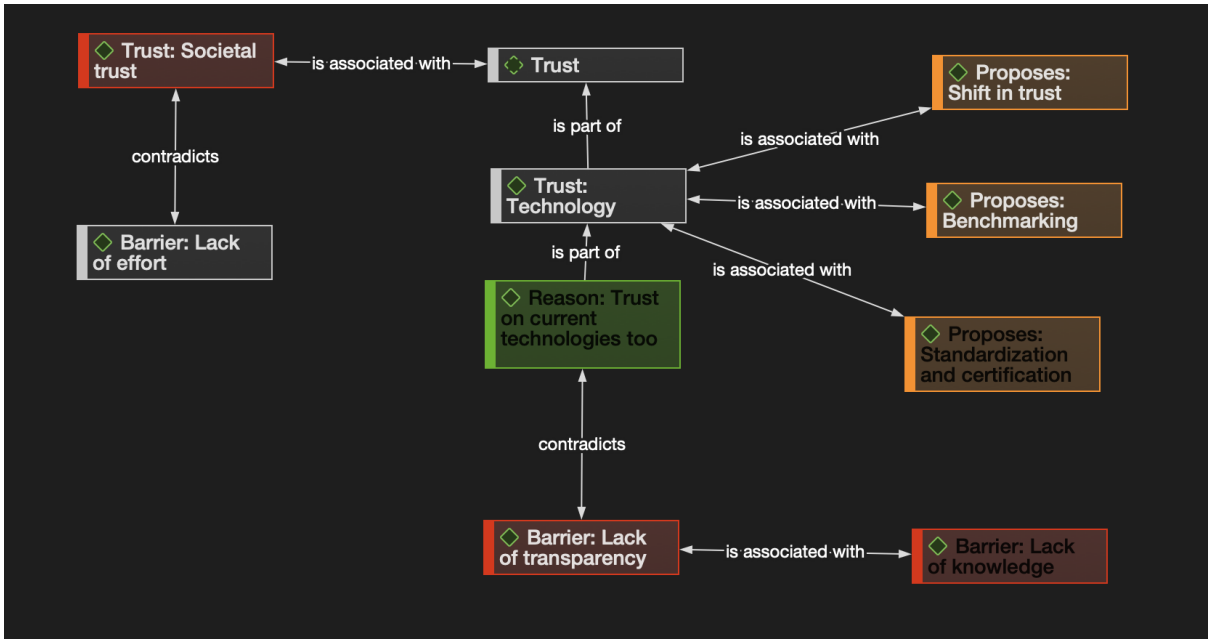


Figure 12 - The role of trust in collective action to develop MPC

4.2.2. Collaboration type

The previous section defined the role of trust in actors' decision-making to develop or adopt MPC. Creating trust among the parties and society can be challenging. This section will try to answer, "What type of organizations influence the trust of parties?" and "Would the type of governance affect the party's decision to participate" with a lens on building societal trust.

The literature illustrated the role of the government as the collaboration limiting and privacy regulating role. It did not consider the government's potential role in facilitating the development or creating acceptance of the technology. The interviews illustrated a diverse view on the role of the public and private sectors. However, it is more important to understand the openness to collaborate with new parties before discussing the roles of the public and private sectors.

According to the interviews, most participants are open to collaborating with new parties that do not exist in their current ecosystem. It reflects the findings of the previous questions in which trust in parties does not play a significant role. Yet, there was one actor that was not comfortable with engaging with all new parties.

> "*Well, indeed, we will not collaborate with everyone. We must trust them and the parties connected to them. Of course, we have existing relationships, but we are open to new engagements. That is sure, but we want to know what is behind the company.*" (**INT-3**)

The quote illustrates that there is a contradiction in their opinion. Parties do not want to collaborate with others if they do not know their background. In the previous section, it was mentioned that trust in parties did not influence the collaboration. However, it seems that it is still essential to understand the background of the companies. Due diligence might indicate that actors want to know the motives and ensure the least risk mitigation is conducted. An interviewee also mentioned due diligence as there were two critical conditions for selecting potential collaboration partners. The first condition is the reputation built by the company. A company with a lot of experience, a certain reputation or an extensive established network indicates a fruitful collaboration. However, the participant highlighted that being selective can

be detrimental, too, as it lowers the probability of finding partners to collaborate. The second condition is whether participants are seeking sole financial merits. This kind of interest would affect the collaboration's authenticity and the party's trust (INT-5). Hence, these two conditions illustrate that trust can be affected by new parties.

The need for due diligence could indicate that trust in parties is still crucial while the actors did not address it. An explanation is that actors are vigilant and aware of the risk that can possess by engaging with new parties. It could be that actors are reluctant to collaborate with new parties if they know that the underestimated risk of processing sensitive data within SMPC exists. An interviewee has provided an example to highlight their reason.

> "[…] that is complicated, for example, the companies such as Microsoft maybe not. But a company as Google, it is not unknown if they will collect information." (**INT-6**)

The quote above might clarify why actors should be more careful in engaging with new parties. Entering a collaboration without knowing the company's background and motives can decrease the actor's trust. The previous section already mentioned that their data would be put at risk to improve the data analysis. This aligns with one of the provided factors of not participating: safeguarding privacy. In this case, the interviewee used Big Tech companies such as Microsoft and Google to exemplify parties that might have a malicious intention instead of contributing to the development.

Some other interviewees expressed their openness to collaborating with new parties. They are aware of the malicious intentions and the risk of engaging with parties that cannot contribute or do not have an extensive history. However, they are still opportunistic because the unknown parties cannot measure their capabilities before the collaboration. As quoted below, the actors are keen and eager to know what other companies could bring to the development of MPC.

As the openness to collaborate with new parties is clear, the interviews showed different preferences for the type of collaboration. Interviews showed three different styles of governance. First, some interviews emphasized the choice for private parties to lead the entire development and cooperation. Their main reason is the lack of capabilities by the public sector. The pace of the public sector is slower than the private sector. It would mean that the project might be delayed while it can be faster accomplished by the private sector, as quoted below.

> "*The public sector has a culture or picking up things slowly. It can rather be fast executed by the private sector."* (**INT-6**)

Second, most interviews illustrated no preference in the type of collaboration or a combination of public and private sectors. The private sector possesses the resources and the market knowledge, and the public sector can be seen as a trustworthy actor in promoting trust and creating acceptance of the technology.

At last, the interviews also highlighted the preference for having the public sector as the leading facilitator of the collaboration. Therefore, the next section will go in-depth into the role of the public sector in promoting societal trust.

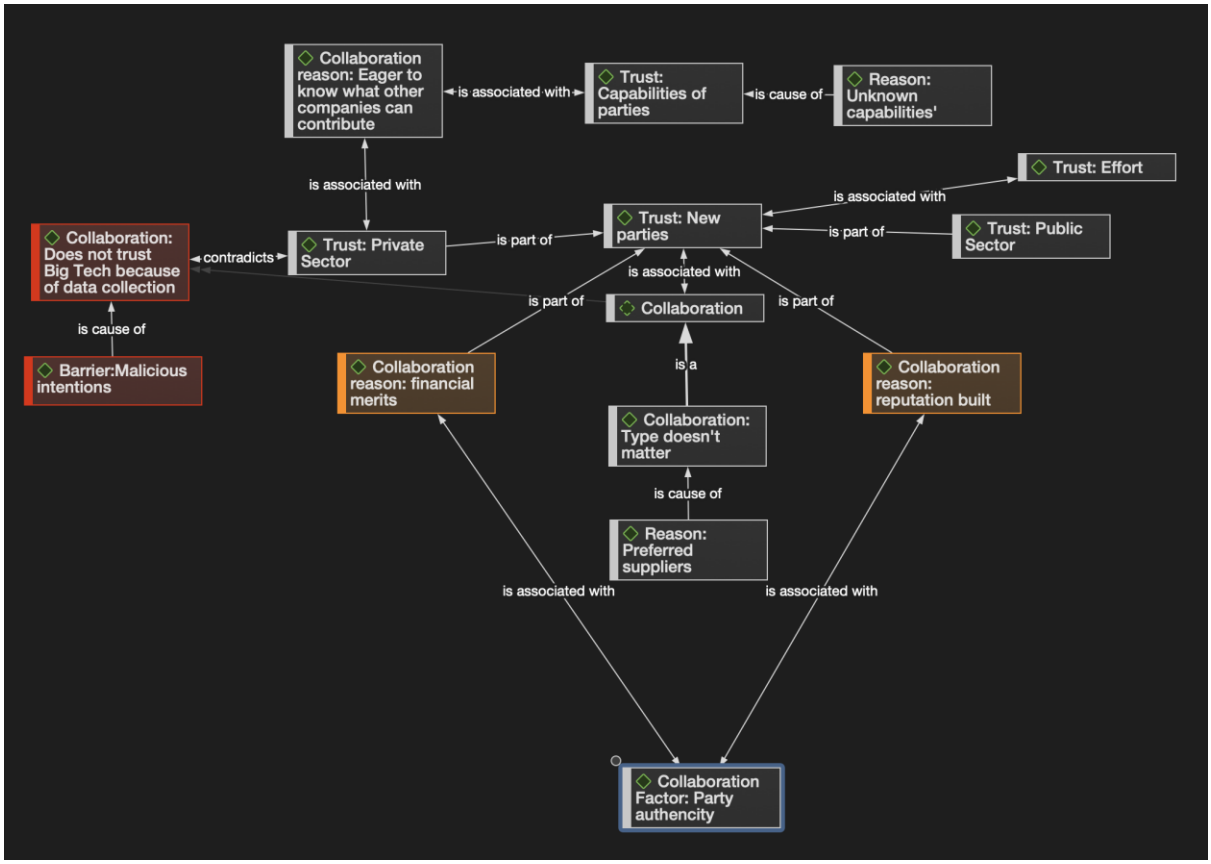


Figure 13- The effect of collaborative form on trust

4.2.3. Public sector as the trust promotor for collective action

The previous section illustrated the preference in having the public sector as the main facilitator of the collaboration. The literature describes that government could influence firms, individuals, and NGOs through punishment and incentives. Also, they can use sophisticated public relations strategies to influence the opinion of others. It indicates the effective role of the government as promotor and can be seen as a reliable and public serving actor. As mentioned before, some interviewees proposed due diligence. Their main reason is that companies could have a malicious intention, which is a major factor since sensitive data will be shared. This would indicate that the government would the sole candidate that can acquire trust from the society (***Trust:Public:SocietalTrust)***. Finally, governmental institutions can enforce policies that would weaken collective stressors and eventually reinforce the facilitators of the collective action initiative. These are instruments which parties in the private sector do not possess.

The interviews provided three reasons for assigning the public sector as the facilitator. Fraud and financial crime are societal challenges that needs to be solved by the society. To tackle these challenges, parties in the public sector would be more reliable than private as they tend to have a better reputation. Thus, the probability for having malicious intentions would be also lower.

Another reason is that it is the responsibility of the public sector to safeguard the society's safety and enforcing the criminal law. As fraud falls within the criminal law boundaries, it would mean that it inevitable that public sector will be part of the collaboration and one of the key actors (INT-4). Assuming that the key findings will be presented to the Ministry of Justice, it will be essential to have the full acceptance and trust of their key stakeholder. A different interview also addressed the importance of the public sector, as quoted below.

> "The private sector wants to keep the public sector happy of course. So, if the push is initiated by the public sector, that would it much better than private" (INT-5)

The quote shows that the public sector would be the most important actor within the whole process and collaboration (***Trust:Public:Serve***). As private sector needs to comply within the legal boundaries and will only serve as the data and evidence provider to the ministry of Justice in litigations and criminal cases.

Finally, the interviews (INT-4, INT-5) displayed the potential of having the public sector as the trust promotor to convince parties to engage in collective action to develop MPC (***Trust:Public:Publicity***). The interviewees emphasized on the reputation and reliability of the public sector.

> "I think that it will create more trust if a public sector participates. They can help to promote. […]" (INT-5)

In short, the public sector would have a better reputation and more power than the private parties (***Trust:Public:Power***). In addition, they would be the key stakeholder within the whole process and collaboration, which means the acceptance of the MPC would be dependent on the public sector too. This makes the public party the ideal candidate in promoting and educating the society to create acceptance and build trust (***Trust:Public:Educate***) . As public parties might not possess sufficient knowledge about MPC, it would still require the expertise from the private sector. This is also illustrated in the quote below.

"The ideal situation would be the publics sector collaborating with the private sector. Hence, not only the public or the private but a combination of both would be great. As we could use the skills from the private sector and the image of the public." (INT-5)

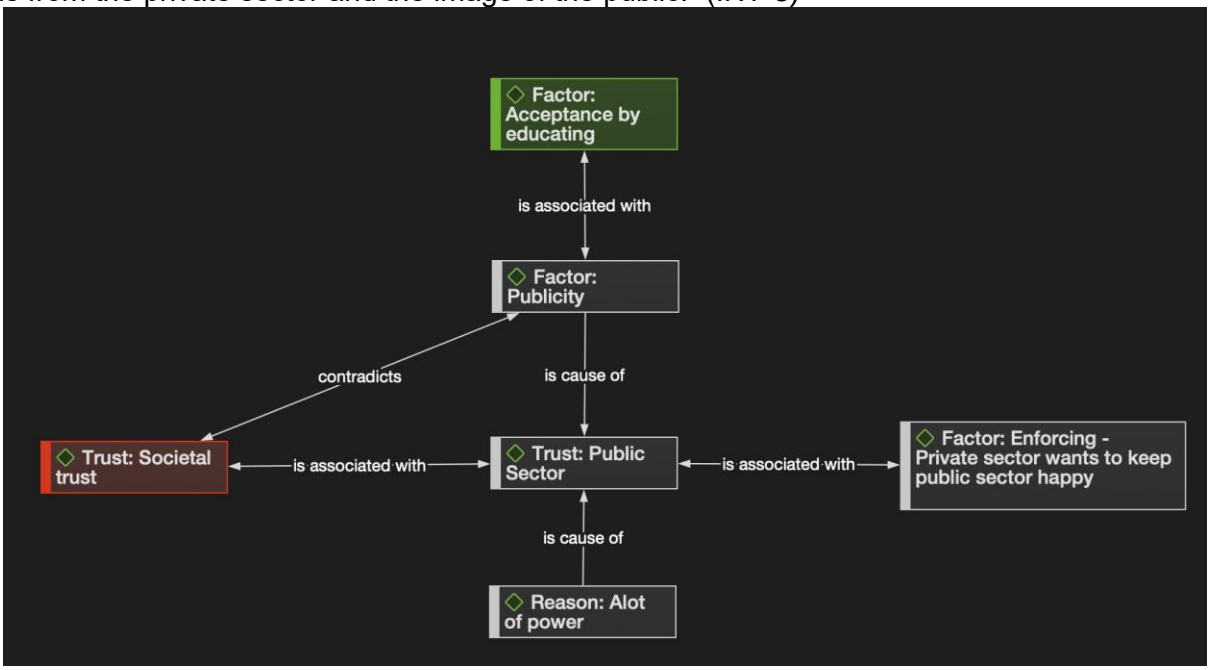


Figure 14 - Overview of the public sector as trust promotor

4.2.4. The effect of size on building trust

The study hypothesized that the size of the group does affect building trust. The previous findings indicated that some actors are careful in engaging with new parties or collaborations. Therefore, interviewees were asked to express their preference for the group size with which they would collaborate. The primary purpose is to find if there is a causal relationship between the size of groups and building trust. The interviews showed similarities but also differences.

First, some interviews stated that the size of the group does not affect the collaboration's trust and efficiency (**Size:Collaboration:NotEffect**). The MPC expert and developer provided several use cases illustrating that the size does not affect the potential participant's decision. The primary factor crucial within these use cases and collaboration is "effort" (**Size:Trust:Effort**). It all depends on the effort made by the participating organizations and agencies. The lack of effort will demotivate other parties to engage or have trust in the collaboration.

> "A use case that is commonly presented, is the Dutch National Cyber Security Centre, who uses our MPC solution. The purpose of the solution is to collect threat intelligence from companies in the Netherlands in a 100% anonymized way. The NCSC is the major party collecting information for many parties, which is currently around 100 but will 1000." (**INT-2**)

The use case exemplifies that proper governance and effort would not affect trust or collaboration. This infers that governance would play a crucial role in helping to build and maintain trust among parties. The previous findings also indicated that parties from the public sector tend to be more reliable and suitable for leading the collective action. In this use case, the National Cyber Security Centre was the leading actor in the MPC development. The NCSC is a public party, which might explain why parties were willing to share their threat intelligence. Also, many participants were involved and engaged in a collective action to adopt MPC to improve resilience against cyber threats. This indicates that the group size does not influence the decision of potential partners. Moreover, it could also mean that proper governance and having a public party as the promotor are more critical factors than the group's size.

An alternative explanation that was provided by a different interview was related to the organizational structure. The assumption was that a smaller company could be a subsidiary or acquired by a larger company (**Size:Affect:Acquired**). This, in turn, shows that size as an indicator is not a representative measurement. The previous finding illustrated that parties are careful when interacting with private parties. The example of large technology companies exemplifies why actors have more trust in the public sector than the private, as there could be more underlying parties involved in the collaboration.

A different perspective is that the group size would influence the initiative's outcome and trust. Several interviews proposed that the collaboration or initiative should start with a small group (Size:Collaboration:StartSmall). In addition, smaller groups tend to have more benefits than larger groups. The first reason is the ease of managing the initiative. The second argument is that any lack of effort, also known as free-rider behaviour, can be identified earlier and is more noticeable. Lastly, a smaller structure would allow more flexibility within the development of MPC.

> "The advantage of small group size in collective action is that everyone can contribute to it and would feel part of the collaboration. A larger group size would probably bring

fewer advantages. However, the advantage of larger group size is that the outcome would result in a wide acceptance." (**INT-3**)

The following quote indicates that larger groups do affect building trust. However, there would be no balance between the advantages and disadvantages. There would be more disadvantages than benefits. Therefore, starting with a smaller group and increasing the group size as the initiative develops is suggested. The tight proximity of the small group will allow parties to contribute equally and help to enable inclusivity within the collaboration.

The final perspective is the preference of a large group. The previous finding showed that larger groups are challenging to measure the contribution, be less flexible, and are difficult to manage. However, larger groups can also bring advantages like acquiring a wide acceptance.
The logic behind wide acceptance is the more parties are involved in the initiative, the more trust and acceptance can be created (**Size:Large:Acceptance**). The involvement of a large number of parties might indicate that most market players are part of the development. This has also been quoted by one of the interviewees:

"Well, I think the output would be more valuable if a lot of companies contribute to it. Also, wider acceptance can be accomplished easily, as many parties are already involved." (**INT-4**)

The interviews showed diverse opinions on the effect of the group size on collective action and collaboration. A minority of the interviewees addressed the lack of transparency on the effort as the primary factor influencing trust. Actors fear the lack of effort will be less noticeable in a more extensive collaboration. The caveat would be the trade-off between the wide acceptance in a more extensive setup and equality & flexibility for smaller group sizes. The following section explores the effect of selective incentives and punishments on the lack of effort by participants.

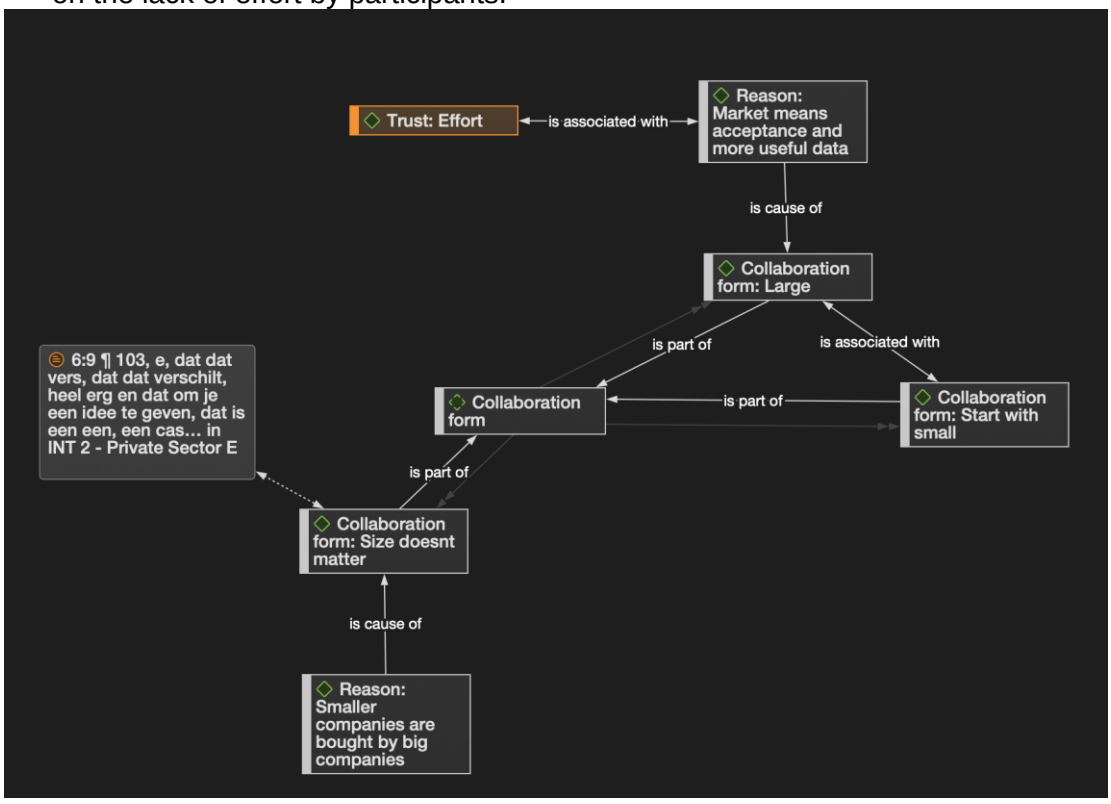


Figure 15 - The effect of group size on building trust

4.2.5. Effect of incentives and punishments on collective action

The "lack of effort" aspect has been a predominant factor mentioned by the participants. The participants are asked to share their thoughts on introducing selective incentives and punishments to tackle free rider behaviour. The study hypothesized that enforcing incentives and penalties would reduce the probability of free rider behaviour. The interviews showed commonalities but also differences.

First, Some respondents mentioned that free-rider behaviour is non-existent (Freerider:NonExistent). The assumption was that every participant would put enough effort into the collective action. The parties would not decide to engage in collective action to develop MPC if they would not contribute to it actively. Moreover, the Financial Crime industry is an isolated industry continuously under regulatory pressure. The lack of "effort" would be noticeable, and since the industry is small, it would make parties reconsider taking advantage without contributing.

Second, one of the interviews highlighted that it is impossible to measure free-rider behaviour (***Freerider:UnableMeasure***).

> "[…]. Hence you will not be able to see who is benefitting from it without contributing. That will be an important factor" (INT-5)

The quote above emphasizes the lack of transparency. This aligns with the previous findings, as the lack of effort is one of the essential aspects that affects trust. The transparency challenge could affect the actor's decision to engage in collective action, creating uncertainty among some parties. Certain actors are not comfortable with the uncertainty, as it was illustrated before. The lack of knowledge and the uncontrollable factor in MPC make actors consider it carefully. An interview highlighted that if many parties are not contributing to the collective action, there would be no benefit of entering the collaboration. As the interviewee quoted as following:

> "[...], If there aren't a lot of parties contributing by sharing information, then it does not even work. You could rather keep the information within your organization." (INT-7)

Lastly, a group acknowledges the chance of free-rider behaviour in the collective action. This group had split opinions on the enforcement of selective incentives and punishment as a measure to act against free-rider behaviour. Another interview mentioned that introducing sole incentives will not work (***Freerider:SelIncen:Sole***).

> "[…] incentives would help to attract new parties, but the problem is that if you have only incentives and no consequences, it can be impactful. If they participate and something goes wrong. I would not trust them, but if punishments are in place…." (INT-5)

This infers those sole incentives can attract new parties, but there will be no consequences for the participants that impact the collaboration. Therefore, punishment would need to be in place as a preventive measure. Another interview adds a new perspective to this topic.

> "I don't think it will work because we have seen it in the past. If there are just only incentives, the banks won't be bothered. They want to keep their minimum compliance cost low. However, punishments do work better. A regulator needs to check the banks day to day tightly." **(INT-5**)

The quote illustrates that in a regulated industry such as banking or financial, actors are not motivated to act if there are only incentives. The financial cost of participating is the banks' most essential factor. However, introducing consequences is a potential approach to motivate parties. Actors consider the negative effect or consequences more than being incentivized. The introduction of punishments would not that work. Therefore, a public actor such as a regulator must continuously check to keep the actors motivated.

Other participants argued that introducing selective incentives and punishment will not work in an industry such as financial crime (***Freerider:SelIncen:NoEffect***). The previous findings showed that the inclusivity of participants in a collaboration or collective action is essential. Implying selective incentives or punishments will exclude certain parties that might still be interested in the collaborative effort.

> "Well, some parties cannot contribute a lot but want to use it. They will feel like they are excluded." (INT-7)

> "Because small organizations would also be involved. Suppose they have interesting data that they could share. It could potentially make the end-product less costly." (INT-6)

This implies that organizations that cannot actively contribute to the development but are interested in the outcome of the MPC will be excluded by the selective incentives and punishments. They could potentially provide valuable resources such as exciting data for the sake of development. Also, the previous findings mentioned the wide acceptance. Excluding actors or interested parties might affect the broader acceptance by the market players.

The interviews also proposed several ideas facilitators could use to tackle the free-rider behaviour in the collective action to develop MPC. The first suggestion is introducing the concept of "licenses", as parties need to contribute to the collective action with a certain fee (***Freerider:Proposes:Licenses***). The financial commitment would incentivize parties to put effort into the collective action. Also, licenses can be used as the main object to motivate participants. The interview provided the example of offering discounts on the license fees if they contribute to the collective action actively, as it has been quoted as follows:

> "[…] You can make the license fees cheaper for the parties that are actively sharing data in the MPC initiative. However, we use open-source projects too. Those open sources are also being worked on." (INT-6)

The question that arose during the interview was, "What is the effect of introducing licenses to tackle free-rider behaviour if the community is using open-source tooling, too?". It contradicts their current practices and stimulates to exclude parties from the collective action. This, in turn, shows that a balance between licensing and open source needs to be found, as it will trigger inclusivity challenges.

The final suggestion is proposing a rating system for the participants, as quoted:

> "[…] You can maybe introduce a kind of rating, hence a rating system for all the parties that are participating. This rating would be based on their performance and contribution." (INT-4)

A rating system would help track the performance and contributions of the individual participants (***Freerider:Proposes:Rating***). It helps to provide the transparency that has been mentioned as a limiting factor before. Identification of potential free riders can be easily performed with the help of such implementation. However, this will bring other concerns, such as excluding interested parties that cannot contribute as much as the more significant players.

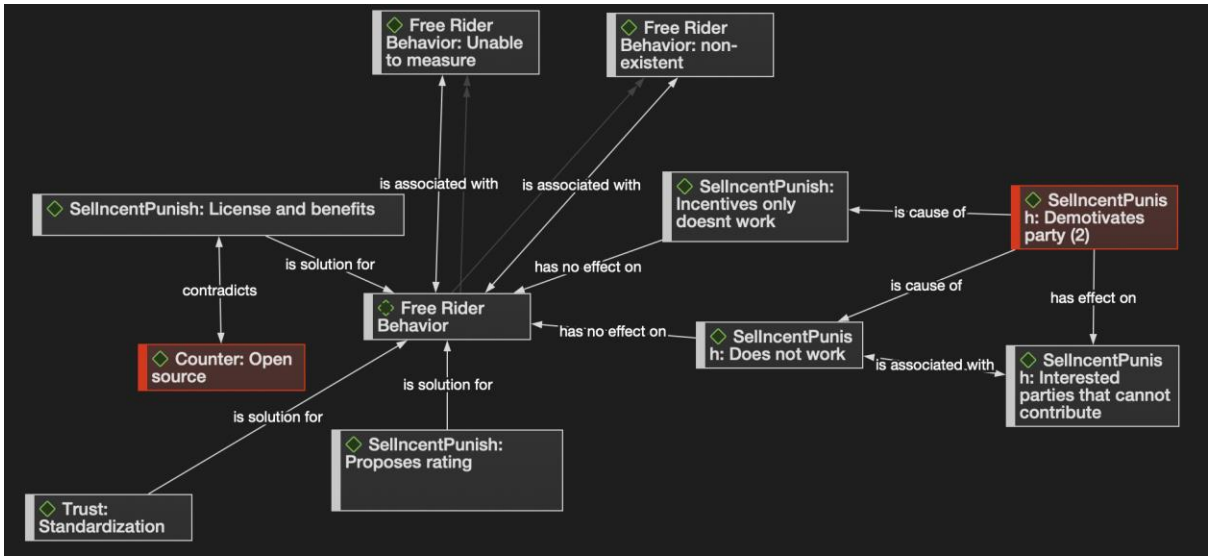


Figure 16 - The effect of incentives and punishments on collective action

4.3. The conceptual model and empirical findings

This chapter aims to compare the conceptual model with the empirical findings. The purpose of this comparison is to enhance the initial conceptual model that was created at the beginning of the research.

4.3.1. The conceptual model

This study formulates a conceptual model based on the available theories to describe the role of governance, selective incentives & punishments, and group size in building trust to convince actors to engage in collective action. There were similarities with the available studies and differences that were not captured by the literature. This section will discuss how these empirical findings will help to enhance the initial model.

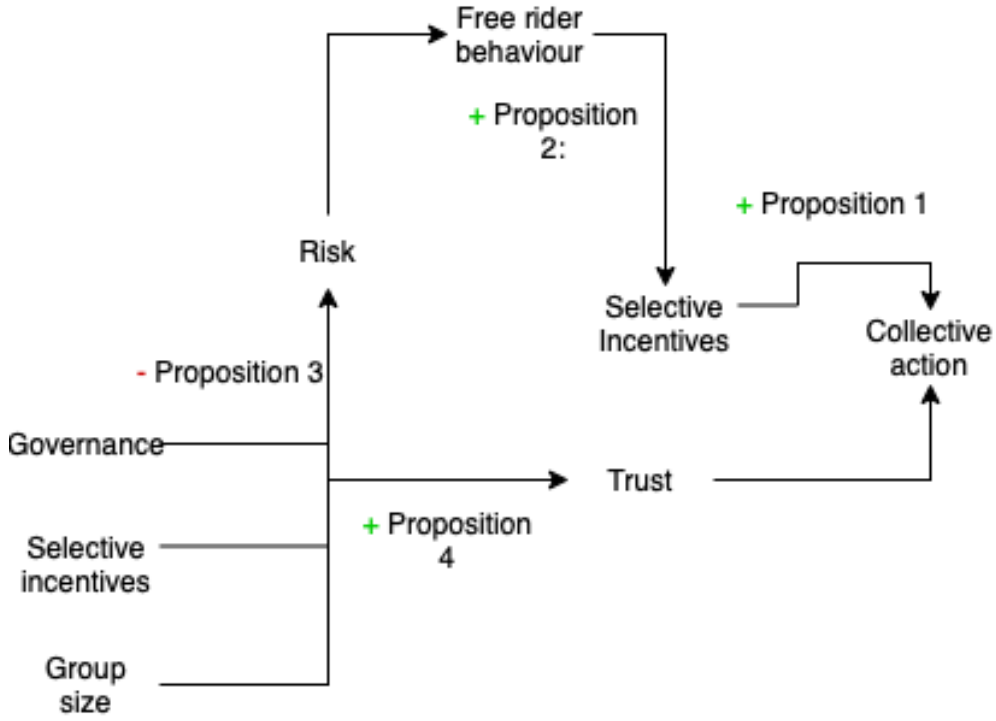


Figure 17 - Conceptual model

4.3.2. Role of trust

The initial model hypothesized that trust is crucial for actors to engage in collective action to develop MPC. This study's definition of trust initially was the trust in the parties. However, the empirical findings show that there are two types of trust—first, the trust in technology, as mentioned earlier. The parties are more concerned about the underlying technology that will process their data. The main reason is that these data are highly sensitive. Also, any technical vulnerabilities or leakages could be detrimental to the organization. Therefore, trust in technology is critical to ensure that MPC will safeguard all their data. The role of governance and group size can influence the trust in technology. The following paragraph will discuss these two factors. The factor of selective incentives & punishments would not apply to the trust in technology. Introducing incentives or penalties would not influence the trust in the technology, but it will affect the second type of trust.

The case also showed a second type of trust: trust in the participating parties. It focuses on the background and motives of the interested parties. The case showed that parties are careful in participating because MPC and participants will use their sensitive data. All the factors defined within the conceptual model could potentially affect the trust in parties.

4.3.3. Role of governance

The empirical findings show that the role of governance is a predominant factor in building trust among parties (Type 2). The case showed the importance of governance in convincing parties to collaborate. The participants tend to trust the public sector more than the private sector. The main factor that affects trust is the intention and the power of the participants. The public sector has mainly been pointed out as the trust facilitator within the collective action in developing MPC. Hence, it shows that the power and intention affect the role of governance but also the trust in the collective action.

4.3.4. Role of group size

Group size seemed to affect the trust in collective action to develop MPC. However, the empirical findings illustrated that there could be a compromise between smaller and larger groups.
The factors such as a noticeable lack of effort and flexibility were mentioned in the interviews, which were also defined in theory. However, it did not include the advantages of having a larger group. A larger group will help accomplish a "wider acceptance" of the technology and the initiative. Furthermore, the organizational structure has been found as a new factor influencing the group's trust. This factor is related to an overarching factor affecting the multiple concepts: transparency. At last, inclusivity has also been mentioned as a new factor. Excluding certain parties from a collaboration or group might affect the trust in the group.

4.3.5. Role of selective incentives and punishments

The initial model hypothesized that selective incentives and punishments would help build trust. However, the empirical findings showed that incentives and punishments are not the most crucial factors. Yet, the respondents mentioned that transparency is an essential factor that plays a role in acting against free-rider behaviour. The transparency in what parties can contribute helps to increase the trust in the groups. In addition, it helps to identify malicious parties. However, introducing selective punishments can exclude interested parties in the collective action. Therefore, the "inclusivity" mentioned in the role of group size will affect the function of incentives and punishment and the trust in the collective action.

The empirical findings showed differences with the initial conceptual model. The literature has not captured these differences. Based on these outcomes, the conceptual model has been revised.

5. Analysis of the results

This chapter will use the empirical findings to assess the propositions drafted at the beginning of the study. These findings illustrated perspectives of an individual, group, or sector. Next, the section will combine the results with the literature to validate the propositions. At the end of the chapter, the fourth research question, "*How does the conceptual model explain the interest of private and public organizations in accepting SMPC*?".

5.1.1. Proposition 4a - Trust

The literature mentioned that building trust can be a complex challenge and is one of the barriers to collective action and MPC. The previous findings showed that "trust" was not the main reason for parties not participating. The empirical results showed a shift in the type of trust, which the previous studies did not strongly capture. The trust in parties and collaborations is less relevant than the trust in the technology. Parties are mainly concerned about safeguarding their data privacy and the safety of using MPC. The characteristics of the industry might clarify why the actors are more concerned about the risks of using the technology instead of the collaborating parties. It is an isolated and small industry which is continuously under regulatory pressure. Hence, the role of trust in participants would therefore be less relevant. However, there is a condition also seen in the previous findings. The actors are careful with engaging in new collaborations that involve new parties.
This might indicate that the trust in participants does affect the actors' decision to engage in collective action.

5.1.2. Proposition 4b – Governance

The study hypothesized that governance would increase actors' trust and eventually help convince actors to engage in collective action to develop MPC. The empirical findings answered two questions "What type of organizations influence the trust of parties?" and "Would the type of governance affect the party's decision to participate?".

The empirical findings displayed the preference of the participants to have the government as the facilitator. It aligned with some studies that showed the government's potential in helping to influence the decisions of individuals, organizations, and NGOs. The respondents mentioned several reasons for the government's role as the trust facilitator. First, the actors are afraid of the malicious intention of the private parties. It has been exemplified in the cases of the big technology companies that collect the data of individuals and companies. Actors prefer not to have the private sector lead the collective action as they might not be independent and can have malicious intentions. The second reason is the government's power, which is also captured in the literature. The government can use instruments such as punishments or incentives to influence the parties. In addition, they can use sophisticated public relations strategies to influence the opinion of others. The participants also addressed the power of the government. Private parties do not have the power of the government to punish actors lawfully. Also, the majority of the interviewees agreed on the reliable role of the government. The reliable role could be clarified with the independent and regulatory functions. Therefore, it would be less likely that the government would have malicious intentions like some companies.

However, the interviews showed a high need for education about MPC. The lack of knowledge is one factor that makes actors uncertain about the opportunities that can be created. Furthermore, the empirical findings showed that the government do not possess the expertise and complete understanding of MPC. Therefore, the collaborative structure will require a combination of the public and private sectors. Whereas the public sector would help to promote and acquire the trust of the potential partners and the private sector in providing their expertise and resources to educate the stakeholders and interested parties.

Furthermore, the government has a function to safeguard society's safety and enforce criminal law. In this case, the government must tackle and prevent society's fraud. As fraud falls under their criminal law boundaries, it would make the public sector a central actor in the initiative—for instance, the Ministry of Justice. Organizations will provide the evidence and information to the ministry of Justice. Therefore, it would be essential to have their complete acceptance and trust in the system. This implies that the private sector and public agencies will serve as data and evidence provider to the ministry of Justice.

In conclusion, the type of governance and organizations affect the actors' trust in deciding to engage in collective action. The government would be the leading facilitator in promoting trust and the private sector in educating society. The findings showed that the public sector should lead and facilitate collective action. The participants indicated that the involvement of the public sector would increase their trust in the collaboration and MPC.

5.1.3. Proposition 4c – Selective incentives and punishments

The studies illustrated that selective incentives and punishments would help to tackle free-rider behaviour. The diminishing contributions by the participants would discourage other actors in the collective action. Nikayin & Reuver (2013) mentioned that free-rider behaviour could sabotage the efforts for collective action. The empirical findings showed a mixed opinion on the existence of free-rider behaviour in the financial crime industry. Some argue that the industry is isolated, small, and continuously under regulatory pressure. This, in turn, may indicate that the free rider behaviour would less likely occur in this domain. Others think that free-rider behaviour might exist in the industry. The last group expressed that any lack of effort made by any participating party would discourage the actors from contributing to the collective action.

The introduction of selective incentives and punishments is proposed by the studies to tackle free-rider behaviour. However, the interviews were differentiated from the literature. Enforcing incentives and penalties would lead to other concerns, such as inclusivity. The participants addressed that excluding parties would affect the trust and acceptance of other parties. There could be parties that cannot contribute like the more giant corporations but still have valuable resources that parties can use to develop the MPC.

Although, the findings also show that only incentives will not be effective. The banks, for example, would not be bothered if there were incentives to participate in the collective action. Instead, the banks would only consider punishment, as it will affect their reputation and finances. Financial consequences are especially effective in motivating banks as they consider it the essential factor.

Hence, the empirical findings show that selective incentives and punishment would negatively affect the trust and motivation of the participants. Therefore, there is no causal relation between the enforcement of incentives and the penalty for obtaining trust from the actors.

5.1.4. Proposition 4d – Group size

The findings illustrated the benefits and downsides of the size of the group. The literature proposed that larger groups are more likely to fail because of several factors. Nikayin et al. (2013) suggested that smaller groups have a higher chance of success. It is more feasible to organize and notice any lack of contribution by the participants. The empirical findings also indicated a preference to start with a few parties, as it would provide more flexibility. However, it will require proper governance and effort as building trust begins from these two factors. Bimber et al. (2005) proposed that it starts with finding the relevant participants that might have networking containing people who share the same interest in contributing to the collective good. The interviews also showed that participants are more comfortable working with the existing network than collaborating with new parties. Their intention is unclear and might be detrimental to their collaboration or safety.

Furthermore, Sebhatu et al. (2020) mentioned that the group size would affect trust. The larger the group, the degree of distrust among the participants would also increase. The empirical findings showed that a larger group would affect the confidence. In a larger group, who is actively contributing to the collective action is not transparent. The lack of transparency might motivate people as there might be free riders within the initiative. Without sufficient contributors, it would have no sense to share their data. This would let other parties benefit from a specific actor's contributions. However, a larger group does also bring advantages to the collective action. A larger group implies that a wide acceptance can be accomplished, as most players would already be in the initiative. Also, an essential factor that was crucial for the participants was inclusivity. A smaller group would exclude interested parties.

Hence, the group size affects the actors' trust in deciding to engage in collective action. There is a mixed opinion on the preference of the group size but starting with a small group. The main reasons are the flexibility and transparency in the contributions made by the participants. The latter-mentioned factor is decisive for the actors' trust in the collective action. On the other hand, a lack of transparency, especially in a more extensive setup, will bring uncertainty to the participating actors. Therefore, a smaller group, as suggested, would increase the trust as it tends to be more transparent. However, it still needs to consider inclusivity.

5.2. Summary of the propositions

The following table summarizes testing of the propositions and if these propositions possess enough support to validate it.

Nr	Proposition	Support	No Support found
4a	The *trust* is an important factor for actors to decide to engage in collective action.	X	
4b	*Governance* will increase the trust of actors in deciding to engage in collective action in developing MPC.	X	
4c	*Selective incentives and punishments* will increase the trust of actors in deciding to engage in collective action in developing MPC.		X
4d	Smaller *Group size* will increase the trust of actors in deciding to engage in collective action in developing MPC.	X	

6. Conclusion & Discussion

This chapter aims to answer the main research question defined at the start of the study. This answer will be based on the findings of the literature review and the empirical outcomes during the data acquisition phase. Also, the chapter will discuss the consistent and contradictory results between the conceptual model and the analysed data. It will help to understand the concept and their effects on the actor's decision to engage into collective action within the financial industry. At last, the limitations of the research and the practical recommendations for the development of MPC in the financial industry will be provided. This is followed by some suggestions for future research.

6.1. Conclusion

The finance domain is losing ground to rapid-developing fraud schemes, as mentioned at the start of this study. It provides intense pressure on organizations to find new approaches to tackle financial misconducts, mainly due to the increasing exposure to regulatory, financial, reputational, and legal risks. Therefore, actors in the financial industry (especially banks and financial crime consultancy) are urged to find new approaches to improve their workflow. The existing set of techniques, methodologies, and workflows are becoming obsolete and ineffective because of the fast-paced developing fraud schemes. A reason that the current set of toolsets are ineffective can be explained by one of the findings by Sagar. The study mentions that there is lack of inter-organization synergy and privacy concerns to make data available for others. It would make it difficult for other parties act on time and identify the fraud due to missing information. This creates a potential opportunity for bundling data to enhance the current fraud prediction models. In addition, it would create an opportunity to discover the potential of Multiparty Computation for performing encrypted joint analysis. However, it is still unsure what can influence actors' decision to engage in collective action to develop MPC. This thesis aims to create a conceptual model that illustrates the factors and barriers influencing actors' decisions to engage in collective action for developing MPC in the financial crime industry. This can be accomplished by answering the formulated research question:

"What factors and barriers influence organizations' decisions to engage in collective action for developing MPC for fraud detection in the financial industry?"

The research question has been broken down into separate sub-questions. The purpose of the sub-questions is to investigate the individual concepts in a structured manner. The existing studies proposed certain factors and barriers. However, the empirical findings showed similarities and differences that the literature did not capture yet.

SQ1 - What theories in literature can explain the behaviour of actors to decide to participate in SMPC?

The literature that aims to explain the behaviour of actors to decide to engage in developing SMPC in the financial industry is limited. The available studies suggested that the participation and decision of the actor is based on the presence of incentives. Incentivizing actors would trigger actors in deciding to participate as they will benefit from the developments. The literature illustrated three examples of how it would benefit organizations by adopting SMPC: (1) interested parties could exchange information to boost their productivity and their business (2) Health care and industry, can share data among each other to improve the scientific research, and (3) public agencies can improve their public safety in case of data openness.

These three examples illustrates that the main reason for actors to participate is to acquire rich, bundled data that could be used to improve their productivity and workflows. However, it did not illustrate in the case of combating financial crime. Therefore, this study acquired

additional information through interviews to test whether incentives would affect the behaviour and decision making of actors. The interviews could not provide solid evidence for the effect of incentives on the decision making of actors. This could be explained by the empirical findings, as the actors interpret and associated selective incentives and punishments with free-rider behaviour instead of their individual benefits. The implementation of selective incentives and punishments will lead to inclusivity concerns, which was not captured in the literature. Companies that are interested in developing SMPC but not capable of contributing would be excluded from the process. Also, the findings showed that selective incentives and punishments will have no effect on preventing free-rider behaviour. The main reason is that the presence of free-rider behaviour is inexistent, as the industry is relatively small and isolated. Actors in this industry would actively contribute as their reputation is on the line.

The literature also argued that there are other factors that could affect the behaviour of actors in deciding to participate in developing SMPC. The studies proposed that acceptance and trust is critical in the decision-making process. The trust in technology and collaboration is highly dependent on two predominant drivers: “transparency” and “auditability”, as lack of transparency will create uncertainty and increased risk. This study could find empirical findings to support the relationship between trust and decision of actors to engage in developing SMPC. Trust has been interpreted by the interviewees differently. The first group as mentioned trust has been shifted from trust in collaborating with other parties to technology. The responses showed that actors do not trust the technology due to the lack of transparency. Their main concern is that their sensitive data is put at risk by trusting a technology without having the full understanding of it.

The second group expressed that the trust in the participating parties is important. The motives and the contribution by the companies are not transparent. Especially in a regulated industry organizations and institutions are careful with whom they are collaborating.

This shows that the only theory that is found in the literature and can be supported by the findings is the effect of trust in technology and collaboration on the actors’ decision.

SQ2 - What are the collective goals, drivers, and barriers to adopting MPC in the financial industry?

The literature captured several drivers and obstacles as an attempt to explain circumstances in which actors would participate or not participate in collective action to develop MPC. The previous sub question already introduced three examples of the benefits that could motivate organizations or actors, in which the benefit would serve for a collective goal as well. The first goal introduced by the studies is exchanging information to boost their productivity and improve their business. This study showed that the introduction of MPC would potentially help to facilitate exchanging information. In this case, it would help to enhance the current fraud detection models. The difference between the empirical findings and the literature is that the privacy regulations play a crucial role in deciding to adopt MPC. The empirical findings illustrates that the actors see the MPC technique as a solution to allow data exchange while complying with the GDPR. The second goal exemplified in the studies is that data sharing would help to improve the scientific research. In this study, it would not be applicable as the financial industry would not contribute or perform any scientific research. Instead, the actors would apply the knowledge generated by the academia. However, it does share commonalities as it would improve their inhouse detection knowledge. The last goal is public agencies could improve their public safety in case of data openness. This goal does have similarities with this study but in a different context. The data openness, especially the data exchange to collectively improve the fraud detection models would improve their ability to combat financial crime. In the end, the society and organizations would benefit from the collaboration to improve the models. It aligns with the empirical findings, in which actors in the financial crime industry

are willing to share their data for a common benefit. However, the sole barrier that keeps the actors from facilitating data exchange was the emergence of the data privacy regulations. The interviewees mentioned that without the limitation it would help their daily operations. In the current situation, assumptions are made as the available data is limited.

The collective goal within the financial crime industry has been found in this study. The actors are willing to develop and exchange their data to combat financial crime. The collaboration would allow to have a more extensive and richer dataset to discover patterns in time. As mentioned before, actors cannot see the larger context of their financial crime cases, as they are not permitted to obtain any data that are not defined within the investigation's scope. The idea of collective action in developing MPC in the financial crime industry showed positive feedback among the participants. This indicate that a mutual acceptance can be achieved if a collective goal exists.

However, a collective goal would not suffice and create a wide-spread adoption and acceptance within the financial industry. The adoption and acceptance are necessary to promote and convince parties to take part in developing MPC in this industry. Safeguarding data privacy has been a predominant factor for the actors. The actors are concerned about the safety of the data due to the lack of the knowledge and transparency. In this case, the participants did not possess a complete understanding of the MPC. The lack of knowledge clearly created uncertainty among the interviewees. The uncertainty primarily existed in how MPC would benefit the organization and whether MPC would be redundant and obsolete. The main concern is that organization find it challenging to see the added value of developing MPC. Also, the flexibility of their workflow after the implementation of MPC has been questioned. A possible explanation for this concern would be the consequences and difficulty to justify a novel technology that is still unclear and uncertain.

This shows that a collective goal can be found for actors within the financial crime. Yet, barriers still exist, which need to be addressed before actors would be willing to participate. This mainly has to do with the uncertainty and the lack of knowledge on the capabilities of MPC.

SQ3 - What are the trade-offs between the interests of key stakeholders?

The literature did not capture the trade-offs between the interest of the key stakeholders in the financial industry. This case has not been discovered by any study yet. It was important to understand the potential trade-offs between the interest to understand the key values for the individual actors. The previous question focused on holistic view, which describes the common interest and barriers. This study investigated the proposed concepts individually on an individual basis. There are certain trade-offs between the stakeholders extracted from the empirical findings. The form of governance is crucial for the decision to engage into developing MPC in the industry. The form of governance would affect the trust of the actors as the majority preferred the government to regulate and facilitate the collective action. However, the role of the government can also be challenged as governments tend to be less suitable for leading and shaping collective action. The main reason would be the lack of expertise and the dynamics within the organization. For example, the interviews mentioned that the pace of the public sector is slower compared to the private sector. On the other side, actors would prefer the public sector as it is a reliable actor with a lot of power to influence and motivate parties to participate. Also, the regulations are formed by the governments too.

This study also suggests the group size is a trade-off between the key stakeholders in this case. Stakeholders have mixed opinion on the size of the collaboration. Smaller groups tend to be more successful as the form are more flexible, manageable, and easier to detect any lack of effort by the participants. Decisions and actions can be executed quicker rather than in a larger collaborative form. In addition, developing MPC in a small collaborative form would

allow inclusivity in the network. The factor 'Inclusivity' has been primarily mentioned within the interviews. This aligns with the literature about collective action. As smaller groups would allow more inclusivity but also less free-rider behaviour as it is easier to detect free riders. However, the empirical findings also illustrate that larger groups could have advantages too. It can create a wider acceptance easier than in smaller networks, as vast majority of the market players would already adopt and participate in the development of MPC.

SQ4. How does the conceptual model explain the interest of private and public organizations in accepting SMPC?

The initial conceptual model based on the literature review provided an indication of the effects of the factors on the development of SMPC in the financial industry. However, the literature was not covering the financial industry. The empirical findings in this study brought new factors which were not captured in the studies and were not applicable for the other industries.

At the beginning of this study, four propositions have been drafted based on the literature review. The empirical findings provided support to three out of the four propositions. The findings showed that trust would affect the actors' decision to engage in collective action. There were two types of trust identified in this study; the trust in technology and the participants in the collaboration to engage in a collective action to develop MPC in the financial industry. Along these two types of trust, there were two other underlying concepts that also affected trust.

First, the form of governance plays a crucial role in creating trust among the potential participants. A proper governance is required, in which the study showed that government would be a candidate to be a trust facilitator in this collective action to increase and ensure the trust among participants in the development of MPC. The participants expressed that the government's involvement would positively influence their decision, as the public sector can be seen as a reliable actor. The other explanation for the choice is that government possess a lot of power and instruments that they could utilize to promote and build trust among the parties. However, the government as a leading role would not suffice in a collective action. It would require the strength and the capabilities of the private sector, as these types of stakeholders would possess the right expertise and knowledge.

The second concept that affects the trust is the size of the groups, as shown in this study. The size of the groups does affect the decision of the participants. A large group might lead to transparency and flexibility concerns. The study as well as the literature both displays that transparency is a predominant factor that would affect and influence the actors' decision strongly. Parties in the collective action wants to be ensured that every stakeholder in the initiative would contribute equally to the collective goal, in this case the development of MPC in the financial industry. The presence of free-rider behaviour in the collective action would demotivate parties to contribute and participate. This, in turn, means that smaller groups tends to increase to increase the trust among the parties as it more likely to be transparent compared to large networks. The empirical findings also provided alternative explanation for the preference and effect of smaller groups, as it would allow inclusivity among the group. The actors expressed that inclusivity would is one factor that motivates the party to contribute and participate. The introduction of selective and punishments would therefore be less practical. The incentives and punishments will exclude parties that cannot contribute actively compared to players with a significant expertise. This will demotivate the smaller parties to participate and affect the trust. Also, the presence of free-rider behavior can be questioned, as the stakeholders in this study mentioned that the isolated and small industry based on trust and reputation would be less likely to have free riders.

This shows that trust and the underlying concepts such as group size and form of governance are the main interest and concerns for the public and private sector to engage in the collective action.

RQ - "What factors and barriers influence organizations' decisions to engage in collective action for developing MPC for fraud detection in the financial industry?"

The empirical findings and literature show that the transparency of the technology and the collaboration is vital in building trust and convincing parties to engage in collective action. The participants expressed that transparency would affect their decision, as the lack of transparency make the actors concerned about their data safety and the influences their trust in the technology and parties in the collaboration. The transparency concern is in two-fold. First, the low trust in the technology is caused by the lack of transparency. Actors do not understand the concept of MPC sufficiently. It indicates that there is a lack of knowledge which causes the lack of transparency. Uncertainty rises as the technique is not auditable and transparent enough to provide certainty in which actors' data will be safeguarded throughout the process. The second transparency is the lack of transparency in the collaborative form. Participants could engage in collective action to develop MPC in the financial industry without contributing equally. The openness of the contributions made by the participants would indicate that participants are reluctant to engage due to lack of trust. Any indication of free-rider behaviour affects the actor's trust but also demotivates the actively contributors.

There are also other factors that play a crucial role in helping to influence the organizations' decision to engage in collective action. The size of the group and the form of the governance mentioned in the previous sub question are the main interest and concerns for public and private parties in this study. This study proposes to start with a smaller group, as it is more beneficial due to the inclusivity, flexibility, and the transparency. Furthermore, a proper governance is essential to create trust among the participants. The empirical findings suggested that the government is the suitable candidate in facilitating trust. The government has been seen as a reliable actor and possess a lot of power and resources to promote and convince parties to participate. Also, it is crucial to take the role of private parties in consideration, as these stakeholders have the expertise.

6.2. Limitations

This study has certain limitations as these are related to and derived from the research design. First, the participation and recall bias are discussed. Secondly, the quality indicators for the research such as construct, internal validity, external validity, and reliability are being assessed.

First, in this study, several participants were asked to participate in the studies by answering question in the interview. Most of the participants have been obtained through the network of the researcher' connections. The main concern is that the interviewee will provide answers that might be far from the truth. This phenomenon is also known as the participation bias. This means that any factor could influence the interviewee to answer differently. For example, the participants are aware that they have been recommended by a connection close to the researcher. Therefore, the participant might provide different answer, as they tend to be afraid that the answers will be disclosed to others. At the beginning of every interview, it was stated that the responses captured in this study will be completely anonymized and not disclosed to any parties. The purpose of the statement was an attempt to convince the interviewees to answer truthfully. However, the risk would always exist, in which participants would provide 'desirable' answer to help the research or is socially acceptable.

The second concern is the recall bias. This implies that interviewees could provide an answer based on their interpretation of event and memories. The interview script consisted of questions that reflected on the participant' previous events and use cases. Therefore, there is a probability that findings are based on their inaccurate recollection. The inaccurate recollection would impact the accuracy and the quality of the research study. Therefore, other interviews and literature have been used as a reference to validate the sense of the answers. However, these were purely assumptions, mainly due to the lack of supporting evidence such as documents to validate the findings. This infers that the responses involving recollections are subjected to recall bias.

The third concern is the execution of explaining the concept of MPC to the participants. A vast majority of the interviewees did not possess the knowledge about the fundamentals of MPC. The presentation used for the interviews have been drafted as the researcher expects to be sufficient to explain the concept. Different execution of the explanation could possibly influence the results. However, the researcher insisted to use the same slide deck to maintain consistency in the results.

The fourth limitation is the knowledgeability of the respondents. The study involved a small group of experts and non-experts. The assessment of the knowledgeability of the participants could affect the quality and the outcome of the study.

Finally, Yin et al. (2018) also proposed several quality indicators important for research. These are construct validity, internal validity, external validity, and reliability.

Construct validity

Yin et al. (2018) highlight that identifying the valid and correct operational measures for the research is essential. It is challenging in a case study as it has often failed to develop a set of operational measures. The missing or wrong operational measures will make the research less valid as it could misinterpret the questions or make what is being investigated unclear. In this case, the study focused on factor "trust". Trust is a broad term, which can involve a lot of forms.

Therefore, a strategy for increasing the construct validity has been used during the research study. Multiple sources of evidence have been consulted to find the definition of trust that suited the nature of this study. There is always a chance of subjectivity in the interpretation of the operational measures. Therefore, the measures such as trust and the underlying concept like group of size, selective incentives and punishments, and governance were based on the literature. A great example is governance, as governance could be managing the collective action or managing the technology. Additionally, a data analysis procedure has been drafted to clarify how data and operational measures have been analysed.

Internal validity

Yin et al. (2018) addressed that internal validity is required for explanatory studies. The purpose is to identify if the researcher has made the correct causal relations between event X and event Y. Any missing factor that might be involved in the causal link can cause the research design to fail. This study focused on an industry that involved a small group of market players. The findings provided by the interviewees would be representative for the remaining of the industry. Yet, a strategy was required to eliminate bias and find correct causal relations between events. The strategy that is used in this research was the rival explanation during the analysis phase. Rival explanation means conceptualizing the rival theory or explanation by considering other stakeholders' opinions and arguments. For example, this study compared the common answered questions with the unique responses. It would help to find alternative explanations but also to understand the causal relation between the alternative factors with the general response.

External validity
Yin et al. (2018) mentioned that it is difficult to generalize the findings to a population in a case study. It should help generalize the results to validate certain propositions or theories. A statistical generalization can therefore not be reached. In contrast, an analytical generalization is still available—the case study aimed toward a particular part of the financial crime industry and the Dutch market. The findings could be different for any other cases in the industry. For example, the opinions of public organizations such as the Ministry of Justice and the attorneys are not included in the empirical finding. These are actors that are also important in the industry. Therefore, the current results might not be representative, as MPC might have a different purpose for the excluded actors. The research decided to use replication of logic in multiple cases to strengthen the external validity. This means that every case has been carefully selected to have similar results or equally measurable results. All these cases are working in the same field within the financial crime industry.

Reliability
The last quality indicator is reliability. Yin et al. (2018) define reliability as the ability to design a research procedure to reproduce the study. The objective of reliability is to minimize the error and absence of bias in the study. The general approach is to develop a protocol to allow the reproducibility of the study. Yin also proposed that creating a database would address the reliability of the study. In this case, a database has been maintained to store the interviews in Atlas.ti, which contains the transcripts, memos, and the networks. Additionally, the researcher has been performing the coding by himself without validating with an expert. This would also affect the reliability of the results and outcome of this study.

6.3. Recommendations

Some practical recommendations are based on the case study and the empirical findings. These are primarily caveats that interest parties or parties developing MPC in the financial crime industry could consider.

Trust
The empirical findings showed an interesting perspective that has not been properly addressed in the literature. The literature assumes that trust in parties and collaboration is still the predominant factor while trust is shifting. In this case, actors are concerned about the risks that arise from using technology such as MPC. The lack of transparency is the main reason parties do not trust the technology. The lack of knowledge causes this lack of transparency. Therefore, it is essential to consider the value of educating the society or market. It helps raise awareness and eliminates the doubts and questions that arise when actors are unfamiliar with technology. It has also been seen in the case of the MPC developer, whereas the parties are more comfortable collaborating when they understand the fundamentals of the concept.

Parties to promote trust
The second recommendation is to consider the critical role of the public sector. The study also illustrated the strong preference for having the government's involvement in the collective action to develop MPC. It helps convince parties to trust the initiative, as the empirical findings have shown that the government is the most reliable actor. In addition, the government has the power and resources to help to promote and build trust in the market or society. Actors are less comfortable engaging in collective action if private parties lead the initiative. The example of the study, in which the malicious intentions of the big technology companies are highlighted, could explain why participants prefer public organizations. Therefore, it is essential to consider including parties from the public sector as they will help to build trust. These parties could be institutions that are responsible f

6.4. Future research

This research developed a conceptual model that illustrates the factors and barriers influencing actors' decision to engage in collective action for developing MPC in the financial crime industry. In addition, it brings more opportunities for future research, as only one of the four propositions has been tested and answered.

The study showed that the government could act as a trust promotor and collective action facilitator. Many respondents preferred the government's involvement because it creates trust, as they are the most reliable party in the initiative. The research described the governance on a very descriptive and high level. It would be interesting to explore effective governance mechanisms that parties can introduce. Also, governments can use instruments to create awareness and acceptance among the parties. In addition, the opinion can change over time. There are no representative use cases for developing MPC in the financial industry. Once certain use cases are developed, it would be interesting to see if the findings will change.

The second opportunity would be to understand the larger financial crime market. At the beginning of the research, the plan was to conduct interviews with more public agencies and attorneys. However, these parties had to be excluded due to the lack of responses by the parties. As mentioned earlier, there are still actors in the market that play a crucial role in the financial prevention and detection workflow. The study might not cover these actors but can bring new perspectives to the conceptual model.

The third opportunity is related to the unanswered propositions. The research focused on the effect of trust and the underlying factors such as "Governance", "Selective incentives and punishments", and "Group size'. In the financial crime industry, actors are very careful with their actions and data because all information is considered highly confidential. The unanswered part of the conceptual model is a risk. Future studies can focus on how risk will affect actors' decision-making to develop MPC. The empirical findings have shown that actors are afraid of the risks. It seemed to affect the trust in the technology and the decision to participate. However, it does not address how actors can mitigate risk.

The last opportunity is a cross-analysis with other industries. The current case study is focused on one sector. However, the other industries might have factors that this study did not include or consider. Comparing the case studies helps to understand the factors that are generally applicable and which elements are case specific. This provides insights into the crucial factors that could be used for development and creating acceptance in new industries.

References

Agahari, W., Ofe, H., & Mark De Reuver, ·. (2022). *It is not (only) about privacy: How multi-party computation redefines control, trust, and risk in data sharing*. https://doi.org/10.1007/s12525-022-00572-w

AKGUL, M. (2021). A Cost-Based Fraud Detection System for Financial Sector. *AMCIS 2021 Proceedings*. https://aisel.aisnet.org/amcis2021/art_intel_sem_tech_intelligent_systems/art_intel_sem_tech_intelligent_systems/25

Ali, M. A., Azad, M. A., Parreno Centeno, M., Hao, F., & van Moorsel, A. (2019). Consumer-facing technology fraud: Economics, attack methods and potential solutions. *Future Generation Computer Systems*, *100*, 408–427. https://doi.org/10.1016/J.FUTURE.2019.03.041

Amara, I., & Khlif, H. (2018). Financial crime, corruption and tax evasion: a cross-country investigation. *Journal of Money Laundering Control*, *21*(4), 545–554. https://doi.org/10.1108/JMLC-10-2017-0059

B. B Sagar, Pratibha Singh, & S. Malika. (2016, October 31). *Online transaction fraud detection techniques: A review of data mining approaches | IEEE Conference Publication | IEEE Xplore*. 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom). https://ieeexplore.ieee.org/document/7724963

Balamurugan, M., Bhuvana, J., & Chenthurpandian, S. (2012). Shared and secured data partitioning for privacy preserving of collaborative file transfer in multi path computational mining. *IFIP International Conference on Wireless and Optical Communications Networks, WOCN*. https://doi.org/10.1109/WOCN.2012.6335528

Biagioli, A. (2008). Financial crime as a threat to the wealth of nations: A cost-effectiveness approach. *Journal of Money Laundering Control*, *11*(1), 88–95. https://doi.org/10.1108/13685200810844523/FULL/XML

Bimber, B., Flanagin, A. J., & Stohl, C. (2005). Reconceptualizing Collective Action in the Contemporary Media Environment. *Communication Theory*, *15*(4), 365–388. https://doi.org/10.1111/J.1468-2885.2005.TB00340.X

Clifton, C., Kantarcıoˇglu, M., Kantarcıoˇglu, K., Doan, A., Schadow, G., Vaidya, J., Elmagarmid, A., & Suciu, D. (2004). Privacy-Preserving Data Integration and Sharing. *Proceedings of the 9th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery - DMKD '04*. https://doi.org/10.1145/1008694

De Reuver, M., Verschuur, E., Nikayin, F., Cerpa, N., & Bouwman, H. (2014). *Collective action for mobile payment platforms: A case study on collaboration issues between banks and telecom operators*. https://doi.org/10.1016/j.elerap.2014.08.004

Deloitte. (2018). *Overcoming Data Challenges in Forensic Investigations | Deloitte US*. https://www2.deloitte.com/us/en/pages/advisory/articles/overcoming-data-challenges-in-forensic-investigations.html

Eur-Lex. (2021, October 27). *Directive (EU) 2015/849 of the European Parliament and of th... - EUR-Lex*. https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L0849

Goldreich, O. (1987). *Secure Multi-Party Computation (Final (incomplete) Draft, Version 1.4)*.

Gottschalk, P. (2010). Categories of financial crime. *Journal of Financial Crime*, *17*(4), 441–458. https://doi.org/10.1108/13590791011082797

Harring, N., Jagers, S. C., & Löfgren, Å. (2021). COVID-19: Large-scale collective action, government intervention, and the importance of trust. *World Development*, *138*, 105236. https://doi.org/10.1016/J.WORLDDEV.2020.105236

Hemenway, B. (2016). A new era for data sharing? *Significance*, *13*(3), 8–9. https://doi.org/10.1111/J.1740-9713.2016.00910.X

Hsu, F. M., Lu, L. P., & Lin, C. M. (2012). Segmenting customers by transaction data with concept hierarchy. *Expert Systems with Applications*, *39*(6), 6221–6228. https://doi.org/10.1016/J.ESWA.2011.12.005

Kahan, D. M. (2005). The Logic of Reciprocity: Trust, Collective Action, and Law. *SSRN Electronic Journal*. https://doi.org/10.2139/SSRN.361400

Kanjalkar, S., Zhang, Y., Gandlur, S., & Miller, A. (2021). Publicly Auditable MPC-As-A-Service with succinct verification and universal setup. *Proceedings - 2021 IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2021*, 386–411. https://doi.org/10.1109/EUROSPW54576.2021.00048

Kollar, E., & Erkin, Z. (2021). *Cleaning Up Our Financial System: Combating Money Laundering Using Multiparty Computation*. https://repository.tudelft.nl/islandora/object/uuid%3A4281b5e4-3e0f-4dfe-adb9-4bdea726814c

Lam, J. (2020). *Scenario Analysis of Secure Multi-party Computation implementation in EU-based multinational banks*. https://repository.tudelft.nl/islandora/object/uuid%3A4916b73e-a496-48c0-b0f7-8a1c78bf5749

Lapets, A., Albab, K. D., Issa, R., Qin, L., Varia, M., Bestavros, A., & Jansen, F. (2019). Role-based ecosystem for the design, development, and deployment of secure multi-party data analytics applications. *Proceedings - 2019 IEEE Secure Development, SecDev 2019*, 129–140. https://doi.org/10.1109/SECDEV.2019.00023

Lindell, Y., & Pinkas, B. (2009). *An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries **.

Liu, J., He, X., Sun, R., Du, X., & Guizani, M. (2021). Privacy-Preserving Data Sharing Scheme with FL via MPC in Financial Permissioned Blockchain. *IEEE International Conference on Communications*. https://doi.org/10.1109/ICC42927.2021.9500868

Mabroukeh, N. R., & Ezeife, C. I. (2010). A taxonomy of sequential pattern mining algorithms. *ACM Computing Surveys*, *43*(1), 3:1. https://doi.org/10.1145/1824795.1824798

Miao, S., Zhu, X., Heijman, W., Xu, Z., & Lu, Q. (2021). Trust or Control? The Role of Group Size in Governing Small-scale Irrigation Facilities*. *Rural Sociology*, *86*(2), 357–384. https://doi.org/10.1111/RUSO.12346

Murunga, M., Partelow, S., & Breckwoldt, A. (2021). Drivers of collective action and role of conflict in Kenyan fisheries co-management. *World Development*, *141*. https://doi.org/10.1016/J.WORLDDEV.2021.105413

Nikayin, F., De Reuver, M., & Itälä, T. (2013). Collective action for a common service platform for independent living services. *International Journal of Medical Informatics*, *82*(10), 922–939. https://doi.org/10.1016/J.IJMEDINF.2013.06.013

Oliver, P. (1980). Rewards and Punishments as Selective Incentives for Collective Action: Theoretical Investigations. *AJS*, *85*(6). https://www.ssc.wisc.edu/~oliver/wp/wp-content/uploads/2015/06/Oliver1980AJSRewardsPunishSelectiveIncentive.pdf

Olson, M. (1965). *The Logic of Collective Action: Public Goods and the Theory of Groups* -

Mancur Olson - Google Boeken. https://books.google.nl/books/about/The_Logic_of_Collective_Action.html?id=-ClHAAAAMAAJ&redir_esc=y

Ostrom, E. (2000). Collective action and the evolution of social norms. *Journal of Economic Perspectives*, *14*(3), 137–158. https://doi.org/10.1257/JEP.14.3.137

Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. K. M. N., & Rahman, R. M. (2022). Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive Based Approach. *IEEE Access*, *10*, 87115–87134. https://doi.org/10.1109/ACCESS.2022.3198956

Resende, J. S., Magalhães, L., Brandão, A., Martins, R., & Antunes, L. (2021). Article towards a modular on-premise approach for data sharing. *Sensors*, *21*(17). https://doi.org/10.3390/S21175805

Tang, Y., & Soundarajan, S. (2017). Social-Aware Decentralization for Secure and Scalable Multi-party Computations. *Proceedings - IEEE 37th International Conference on Distributed Computing Systems Workshops, ICDCSW 2017*, 246–251. https://doi.org/10.1109/ICDCSW.2017.56

Veeningen, M., Chatterjea, S., Horváth, A. Z., Spindler, G., Boersma, E., Van Der Spek, P., Van Der GaliËn, O., Gutteling, J., Kraaij, W., & Veugen, T. (2018). Enabling Analytics on Sensitive Medical Data with Secure Multi-Party Computation. *Studies in Health Technology and Informatics*, *247*, 76–80. https://doi.org/10.3233/978-1-61499-852-5-76

Wong, K. S., & Kim, M. H. (2010). Semi-trusted collaborative framework for multi-party computation. *KSII Transactions on Internet and Information Systems*, *4*(3), 411–427. https://doi.org/10.3837/TIIS.2010.06.013

Yang, H., Zhou, T., Wang, C., & He, D. (2021). *A Secure and Privacy-Preserving Data Transmission Scheme in the Healthcare Framework*. 374–391. https://doi.org/10.1007/978-3-030-93206-0_23

Yao, A. C. (1982). *Protocols for Secure Computations*.

Yin, R. (2018). *Yin, R. K. (2018). Case Study Research and Applications Design and Methods (6th ed.)*. https://www.scirp.org/%28S%28351jmbntvnsjt1aadkposzje%29%29/reference/referencespapers.aspx?referenceid=2914980

Appendix A: Interview Protocol – Non-expert MPC

Interview Protocol A: New to MPC

Interviewee details

Name:
Role:
Domain:

Introduction

Thank you for taking part in my research. The purpose of this interview is to extract factors, opinions, and experiences of experts (working in the field of financial fraud prevention). In my current research I have created a conceptual model for the development and adoption of multi-party computation. The goal is to verify certain propositions by collecting information from experts.

I am aware that you might not have heard or am unfamiliar with the concept of multi-party computation. Therefore, I will briefly explain the concept of multi-party computation and illustrate the potential use-case for enhancing certain workflows within the fraud prevention by utilizing MPC.

Recording instruction:
I would like to record the conversation with your consent. The recording will be used for post-interview reviewing in case of missing important details. Safeguarding the privacy and confidentiality is important. Therefore, the recording will not be shared with any party and processed for the master thesis. A summary will be written, which helps to anonymize your identity, the company's workflow and name.

Interview questions:

1. Could you please briefly tell me about your background and position?

2. What are the common or critical challenges that you have face or seen in a financial fraud prevention project? Challenges that are more focused on the technological side such as data sharing or technical capabilities? Please do not mention any company names or confidential information.

3. Have you heard of MPC or seen any use cases of MPC before?

4. What kind of technologies does the organization use? (if it's confidential or critical, please describe the kind of technology)

5. I introduced the concept of MPC. What would be the reasons or factors for you to consider multiparty computation in your working field or company?

6. What kind of challenges or discouraging factors should be addressed when it comes to introducing MPC into the "forensic" landscape? By landscape, I refer to the ecosystem, networks (stakeholders and partners), and technology.

7. Thanks for sharing your thoughts. Previous questions focused on the factors. Lets assume you are considering to work on MPC. What would be the role of "trust" in developing and adopting multiparty computation?

8. Proceeding with the focus on "trust". Would specific companies or organizations have an influence on the trust? If so, in what way? And why?

9. Would working with new parties affect the level of trust on the cooperation? If so, would it increase/decrease the trust in the technology too?

**** POTENTIAL USE CASE IN FORENSIC INDUSTRY ****

10. The technology or use-case development can be led by the private as well as public sector. How important is the structure of leading the project for considering to take part into the development? and why?
11. What is your preference in regard to the structure (private or public)? And why? Would that increase the "trust" in deciding to participate?

12. Would the group size affect your decision to participate? What would be the ideal group size for you (small or large)?

** Managing a group can be quite challenging when it comes to a large group **

**** FOCUS ON THE GROUP EFFORT REGARDLESS OF THE SIZE****

13. Would enforcing selective incentives or punishment increase your trust in partnering up with new parties? And why?

14. Do you have other remarks that you would like to share or address?

Wrapping up:

Thank you again for your participation. Once again, the privacy and confidentiality of this interview will be safeguarded. The summary will be shared with you for your review. After your approval, the summary will be included in the master thesis.

Kind regards

Kenny Ho

Master Student

Delft University of Technology, Delft, The Netherlands

Appendix B: Interview Protocol – Experts MPC

Interview Protocol B: MPC expert

Interviewee details

Name:
Role:
Domain:

Introduction

Thank you for taking part in my research. The purpose of this interview is to extract factors, opinions, and experiences of experts (working or are familiar with the concept of Multiparty computation). In my current research I have created a conceptual model for the development and adoption of multi-party computation. The goal is to verify certain propositions by collecting information from experts.

I am aware that you might have heard or are familiar to a certain degree with the concept of multi-party computation. I'll introduce the potential use-case for developing MPC and enhancing certain workflows within the fraud prevention because some interview questions will be referred to this use-case.

Recording instruction:
I would like to record the conversation with your consent. The recording will be used for post-interview reviewing in case of missing important details. Safeguarding the privacy and confidentiality is important. Therefore, the recording will not be shared with any party and processed for the master thesis. A summary will be written, which helps to anonymize your identity, the company's workflow and name.

Interview questions (based on their experience such as developing use-cases):

1. Could you please briefly tell me about your background and position?

2. What are the common or critical challenges that you have face or seen in MPC use-cases?

3. What would be the reasons or factors for you to endorse multiparty computation to parties that are not familiar with the concept or new potential partners?

4. Have you managed to identify what motivates party to work on MPC? (I'm referring to previous MPC use cases that you have been working on)

5. What would be the role of "trust" for you in developing or adoption multiparty computation? What is the role of "trust" in finding new partners to create use-cases? How? And why?

**** POTENTIAL USE CASE IN FORENSIC INDUSTRY ****

6. Would working with certain type actors play a role in deciding to participate? Who, why and how would it affect the development of use-cases? Would working with new parties affect the level of trust? If so, in what way?

7. The technology or use-case development can be led by the private as well as public sector. How important is the structure of leading the project for partners to consider to take part into the development? and why?

8. Did the size of collective group in your existing use-cases affect the outcome? How? And why?

**** FOCUS ON THE GROUP EFFORT REGARDLESS OF THE SIZE****

9. Does your existing or previous use-cases considered to enforce selective incentives or punishment to enhance the collaboration? Does that increase the trust in the partnerships with existing or new partners? How? And why?

10. Do you have other remarks that you would like to share or address?

Wrapping up:

Thank you again for your participation. Once again, the privacy and confidentiality of this interview will be safeguarded. The summary will be shared with you for your review. After your approval, the summary will be included in the master thesis.

Kind regards,

Kenny Ho

Master Student

Delft University of Technology, Delft, The Netherlands

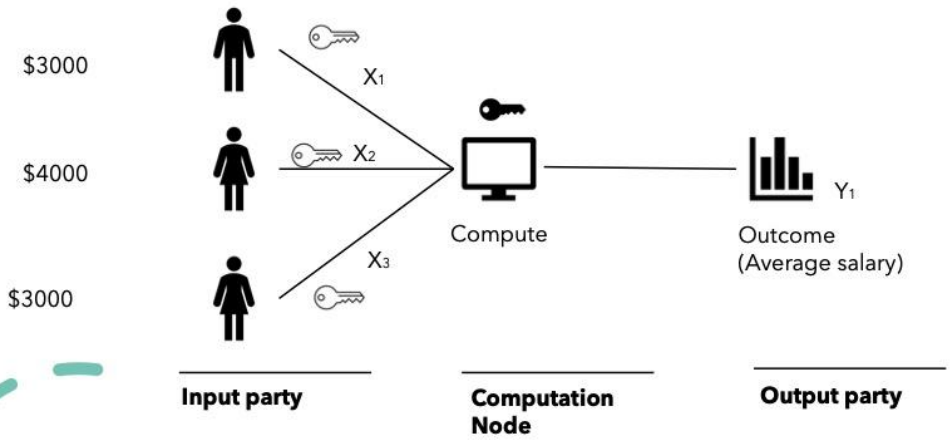
Appendix C: Interview Presentation

The basic concept of MPC: Secret sharing

- "Privacy preserving technology"
- Cryptographic technique
- Joint analysis without any privacy infringement

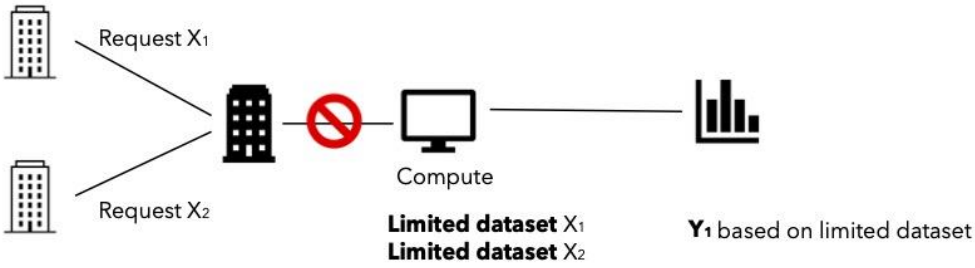
The basic concept of MPC: Secret sharing

Salary calculation



USE CASE: MPC in Fraud detection

As-is: data sharing




1010
1010
Multi-party Computation (MPC)

Appendix D: Initial coding list

Codes	Subcodes
○ Barrier	
○ Barrier: Lack of effort	
● Barrier: Lack of knowledge	
○ Barrier: Legacy systems, difficult to replace	
○ Barrier:Datasharing	
○ Barrier:Datasharing not necessary	
○ Barrier:Datasharing:RequiresPurpose	
○ Barrier:Lack of Incentives	
● Barrier:Malicious intentions	
○ Barrier:Technological vulnerabilities	
○ Collaboration	
○ Collaboration Factor	
	○ Party authencity
○ Collaboration form	
	○ Large
	○ Size doesnt matter
	○ Small
	○ Start with small
○ Collaboration reason	
	○ Eager to know what other companies can contribute
	● financial merits
	● reputation built
○ Collaboration: Type doesn't matter	
○ Counter	
○ Current Barriers	
○ Effect	
○ Factor	
○ Factor: Added value	
○ Factor: Publicity	
○ Free Rider Behavior	
○ Governance	
○ Governance reason	
○ Governance: Private preference	
○ Governance: Public preference	
○ Motives	
○ NoTrust: Impact	
○ Proposes	
○ Rapid developing fraud methodologies	
○ Reason	
● Reason: More data, Richer dataset, better analysis	
● Reason: Unable to see the big picture or lacking crucial information	
○ Role of Private	
○ SelIncentPunish	
○ SelIncentPunish: Decrease the trust	

- SelIncentPunish: Demotivates party (2)
- SelIncentPunish: Increase the trust
- SelIncentPunish: Motivates party
- Trust
- Trust: Capabilities of parties
- Trust: Effort
- Trust: New parties
- Trust: Private Sector
- Trust: Public Sector
- Trust: Societal trust
- Trust: Technology
- Workaround: Data acquisition

Appendix E: Final coding list

Codes

- Freerider:Proposes:Rating
- Freerider:Proposes:Licenses
- Freerider:SelIncen:NoEffect
- Freerider:SelIncen:Sole
- Freerider:UnableMeasure
- Size:Collaboration:NotEffect
- Size:Trust:Effort
- Size:Large:Acceptance).
- Size:Collaboration:StartSmall
- Size:Affect:Acquired
- Size:Collaboration:NotEffect
- Trust:Public:Serv
- Trust:Public:Educate
- Trust:Public:Publicity
- Trust:Public:SocietalTrust
- Trust:Public:Power
- Motive:Workaround:Power
- Motive:Workaround:DataAcquisition
- Motive:Richerdata:ReferenceSet
- Motive:RicherDataset:BetterAnalysis
- Barrier:DataSharing:Lackofincentives
- Barrier:Datasharing: Lackofeffort
- Barrier:Datasharing:RequiresPurpose

- Trust: Capabilities of parties
- Trust: Effort
- Trust: New parties
- Trust: Technology
- Workaround: Data acquisition