Countering money laundering

Implications of the 5th Anti-Money Laundering Directive on virtual currency exchanges in the Netherlands

Cécile Jessie Volten

MSc Thesis
Engineering & Policy Analysis

Countering money laundering

Implications of the 5th Anti-Money Laundering Directive on virtual currency exchanges in the Netherlands

by

Cécile Jessie Volten

Master thesis submitted to Delft University of Technology in partial fulfilment
of the requirements for the degree of

MASTER OF SCIENCE

in Engineering & Policy Analysis
Faculty of Technology, Policy and Management

To be defended publicly on th 18th of August 2021 at 14:30.

Student number:	4475712	
Project duration:	th 8th of February 2021 – the 18th of August 2021	
Thesis committee:	Prof. dr. M. J. G. van Eeten,	TU Delft, Chairperson
	Dr. R. S. van Wegberg,	TU Delft, First supervisor
	Dr. A. M. G. Zuiderwijk-van Eijk ,	TU Delft, Second supervisor

TU Delft

Preface

Never before have I sat in such an empty study hall so often as this summer. However, it was a huge relief to be able to study at university, as for a while it appeared that this would not be possible. After the first few weeks of reserving the same spot in the study hall, on a daily basis, it really started to feel like my place. Especially when I noticed I did not have to adjust the seat anymore when I sat down, which simply means the seat was mostly occupied. Every process has its ups and downs although this process slowly but surely led to the thesis lying before you. With this thesis I will conclude my time at the Delft University of Technology after having walked through these halls over the last six years.

There are many people to thank for their contributions to this research, which have especially been important over the last weeks of this process. First, I would like to thank Selma for the many times she read different chapters and offered her advice. Next, I would like to thank JP for proofreading my whole thesis and correcting the many spelling errors that were in there. Margot and mom I would like to thank you for reading and making remarks on the first chapters. Saskia, thank you for the many coffee breaks we have had together, in which we motivated each other and offered a listening ear. Dad, I would like to thank you for the many times you drove me back to Delft on Sunday night so I could work on my thesis again early on Monday morning. Ceriel, thank you for just being there throughout the process.

I would also like to thank my supervisors. Anneke, over my TU Delft study career you have often supervised me. I am glad that at the start of my thesis you could do the same. Rolf, I would like to thank you for your quick replies to e-mails, the fact that you would always to want think along and the enthusiasm you kept showing about the topic. Michel, although I was slightly intimidated by your feedback at first, I can now see how much this has improved my thesis, thank you for that!

I hope you enjoy reading my thesis!

Cécile Jessie Volten
Delft, August 2021

Abstract

Virtual currency exchanges provide services that exchange fiat currency for virtual currency. Virtual currencies are not issued by any jurisdiction and are part of a decentralized system, bitcoin is an example of this. Fiat currency is money that the government guarantees as a legal tender, such as paper money and coins. The rising popularity of the adoption of virtual currencies provides new opportunities for money laundering due to their often anonymous nature. Money laundering is the process of disguising the origin of criminal funds and providing them with a legitimate status so that they can be used in the traditional financial system. Tackling the possibility of the adoption of virtual currencies for money laundering is important as not doing so compromises the integrity of the financial system by mixing laundered money with regular money. To regulate the system the European Union has decided to put the 5th Anti-Money Laundering Directive (AMLD5) in place. This directive, after being implemented in the Dutch legislation, entails that virtual currency exchanges have to register themselves at the Dutch National Bank (DNB) and now fall under the Wet Witwassen en Financieren Terrorisme (Wwft) and Sanctiewet, which both try to counter money laundering. Only limited research has been performed into the role of virtual currency exchanges in anti-money laundering. Also, the effectiveness of the regulations in place has only scarcely been researched. Therefore, in order to understand whether the implementation of the legislation has the desired effects it needs to be observed what the impact was of the implementation of the AMLD5 on virtual currency exchanges. This research answers the following question. *To what extent have virtual currency exchanges in the Netherlands altered their daily operations in order to comply to the Dutch implementation of the 5th Anti-Money Laundering Directive?*

A mixed methods research approach is adopted to answer the research question, it often consists of a qualitative and a quantitative part. First, desk research is performed in order to obtain an overview of the governance in place of the virtual currency ecosystem. Next, a blockchain analysis is used to obtain insights into changes in transaction behaviour at virtual currency exchanges. The period that was investigated was from 01-06-2018 until 31-05-2021. Third, interviews are held with players directly affected by the 5th Anti-Money Laundering Directive in the virtual currency ecosystem, namely the Dutch regulator DNB and virtual currency exchanges, to obtain more detailed insights in the influence of the legislation on the system.

Governance is here defined as the combination of the legislation in place and the parties involved in the system and relationships between them. From the legislation it was observed that the current state of governance in the ecosystem is focused on the image of virtual currency exchanges, who are seen as gatekeepers of the system. The implementation of the 5th Anti-Money Laundering Directive provided several new obligations to the virtual currency exchanges. First, they have to execute know your customer and customer due diligence measures, in order to understand who the client is they are in business with. Next, they are compelled to obtain a registration at the Dutch National Bank. Lastly, they are obliged to report unusual transactions at the Financial Intelligence Unit of the Netherlands (FIU-NL).

Moreover, the governance in the system is characterized by a combination of public and private actors. The private actors are represented by the United Cooperation of Bitcoin Companies in the Netherlands (VBNL), which is the interest group for virtual currency exchanges. The legislation made the Dutch National Bank responsible for the registration of the virtual currency exchanges and the supervision of the system. The legislation is formulated by two Ministries, namely the Ministry of Finance and the Ministry of Justice and Safety. The virtual currency exchanges have to report unusual transactions at the Financial Intelligence Unit in the Netherlands. Together the public and private parties cooperate in the Anti-Money Laundering Centre.

In the blockchain analysis bitcoin transaction data of 17 Dutch virtual currency exchanges is analysed, of which 5 exchanges were not registered at the Dutch National Bank. It was observed that after the implementation of the legislation less transactions were executed. However, the transaction value increased. This could imply that transactions were no longer split up, which in money laundering terms is called smurfing. It was observed that over time no difference was apparent in the origin or destination of transactions. Many explanations can be found for the observed patterns, therefore it is unknown whether these effects are caused by the implementation of the 5th Anti-Money Laundering Directive.

Five semi-structured interviews, with seven interviewees, were held in total. Four interviews are held with virtual currency exchanges and one with the regulator. The interviews encompassed the topics of the adoption of virtual currencies in money laundering, the anti-money laundering responsibilities of the parties, the introduction of the legislation, transaction monitoring, registration & supervision and an outlook on the future. It was observed from the interviews that the regulator had to set up a new form of supervision. Currently, they do so by sending out questionnaires on which they assess the risks at the virtual currency exchanges. This risk assessments can provide reasons for possible onsite visits.

Virtual currency exchanges, on the other hand, did not have to implement additional anti-money laundering measures as most of the measures following from the legislation were already put in place by the parties long before the implementation date. The adaptations for the daily operations of virtual currency exchanges were mostly administrative. They now have to further record their processes, write reports on unusual transactions and answer information requests by the Dutch National Bank. On the contrary, in the landscape other virtual currency exchanges were negatively influenced. It was mentioned that due to the high supervision costs which parties have to pay, other virtual currency exchanges either changed their services, quit their operation or moved abroad.

To conclude, it was found that the extent to which virtual currency exchanges in the Netherlands have altered their daily operations was limited, especially when considering the measures countering money laundering. The alterations of the daily operations of virtual currency exchanges can mostly be observed in their administrative processes by formalizing the processes already in place, providing information to DNB and reporting unusual transactions to the Financial Intelligence Unit in the Netherlands. The virtual currency exchanges have not actively altered their operations in countering money laundering.

The legislation of the Wwft and the AMLD5 has a goal that is twofold. On the one hand, preventing customers from misusing financial institutions to launder money. On the other hand, detecting and prosecuting crime effectively and efficiently. It seems as if the legislation surpasses the goal as the implementation of the 5th Anti-Money Laundering Directive will not have contributed to achieving the first goal. Since the virtual currency exchanges already performed several measures in countering money laundering. However, the reporting duty might have helped in prosecuting crime effectively, but this cannot be deduced from this research. For policy makers it is advised to start the conversation with the sector and establish better cooperation between supervisors, legislators and private parties, preferably at an international level. Together they can improve the countering of money laundering.

List of Acronyms

AML	Anti-money laundering
AMLC	Anti-Money Laundering Centre
AMLD	Anti-Money Laundering Directive
AMLD4	4th Anti-Money Laundering Directive
AMLD5	5th Anti-Money Laundering Directive
AMLD6	6th Anti-Money Laundering Directive
BCBS	Basel Committee on Banking Supervision
BTC	The currency of bitcoin
CDD	Customer Due Diligence
DNB	Dutch National Bank (De Nederlandse Bank)
EC	European Committee
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU-NL	Financial Intelligence Unit the Netherlands
FIUs	Financial Intelligence Units
KYC	Know Your Customer
MiCA	Markets in Crypto-assets
NRA	National Risk Assessment
SIRA	Systematic Integrity Risk Analysis
VBNL	Verenigde Bitcoinbedrijven Nederland
Wft	Wet Financieel Toezicht
Wwft	Wet ter voorkoming van Witwassen en Financieren van Terrorisme

Contents

List of Figures

List of Tables

1 Introduction

This chapter provides an introduction to the research problem at hand. First, the research problem is established in section 1.1. Next, the relevance of the research problem is considered in section 1.2. Then, the research objective is formulated by investigating previous research, identifying a knowledge gap and establishing research questions in 1.3. Finally, an outline of the thesis will be provided in section 1.4.

1.1. Initiation anti-money laundering regulation

On the 23rd of March 2021 a court case was held in Rotterdam, the Netherlands, between Bitonic and the Dutch National Bank. Bitonic is a large Dutch currency exchange provider, which promises to instantly buy and sell bitcoins [1] to your own wallet ("Bitonic", n.d.). In the courtcase they argued that the Dutch National Bank (DNB) applied rules that were too strict and did not adhere to the 5th Anti-Money Laundering Directive of the European Union. DNB is the regulator in the virtual currency ecosystem. They were appointed as the regulatory authority after the implementation of the 5th Anti-Money Laundering Directive. On the 7th of April 2021 the verdict was made that Bitonic was largely correct. The judge thus ruled that DNB should provide extra explanation as to the reasons for the strict measures ("ECLI:NL:RBROT:2021:2968", 2021). The strict measures merely pointed to the requirement of wallet verification in which the client should provide the exchange with evidence that they indeed have access to the wallet with which a transaction is executed.

Over the years the European Union and its member states have been focusing more on combatting criminality and prosecuting criminals. One often heard opinion is that crime should not be allowed to pay out. As such, the focus of the Dutch government is on financially-economically related crime ("Kamerstukken II, 31477, 1-2 (Rapport)", 2007). Often, however, a predicate offense cannot be proven, which is the act with which the criminal funds were collected. Nonetheless, before the money obtained can be used in the legal system its origin needs to be disguised. In the Netherlands money laundering is defined in a broad sense, meaning that the predicate offense does not have to be demonstrated in order to be penalized (Slot and de Swart, 2018). It is a crime in itself, separate from the predicate offense, partially because following the money is a common tool used in law enforcement for prosecution (Carruthers and Arslan, 2019).

Financially-economically related crime is especially being seen as a risk for the adoption of virtual currencies (DNB and AFM, 2018). Virtual currency is "a digital representation of value that can be traded and functions as a medium of exchange, and/or a unit of account, and/or a store of value" (FATF, 2014) but does not have legal tender status in any jurisdiction. Virtual currencies are not issued or guaranteed by any jurisdiction and only fulfil the above functions by agreement within the community of users of the virtual currency, therefore they often lack regulation (Brenig et al., 2015). Virtual currencies do not have an ultimately responsible party, as they are often part of a decentralized system. This is one of the characteristics of virtual currencies that is at odds with many of the before existing regulations and regulatory standards (DNB and AFM, 2018).

Next to virtual currencies providing new possibilities for financially-economically related crime, they also provide new opportunities for money laundering. In the National Risk Assesment 2019 (van der Veen and Heuts, 2020) several experts identified money laundering with virtual currencies as being in the top ten of money laundering risks. This was based on the the medium impact but especially the fact that the Netherlands has an

[1] It is common to differentiate between the currency and the system through the spelling, bitcoin stands for the currency and Bitcoin stands for the protocol or system.

extremely low resilience to it. Virtual currencies make it more difficult to trace the origins of a transaction, which provides a higher risk for money laundering (DNB, 2020). Moreover, money laundering using virtual currencies facilitates payments for various forms of cybercrime (Europol, 2020), it thus enables cybercrime (Chainalysis, 2020). Between 2004 and 2016 in several Crime Pattern Analyses of the Dutch Police an increase was seen in the adoption of virtual currencies in criminal offenses, furthermore illicit currency exchanges were also observed (Soudijn, 2019). Nonetheless, the destination of most transactions with illicit cryptocurrency are mainstream currency exchanges.

A virtual currency exchange provides a service in which fiat currency can be converted to virtual currencies or the other way around. Fiat currency is money that the government guarantees as a legal tender such as paper money and coins (The Investopedia Team, 2021). Virtual currency exchanges form the gateway between the traditional financial system and the new virtual currency financial system. The exchanges thus have a gatekeeper role. Based on this role the EU, in 2020, drew up the 5th Anti-Money Laundering Directive (AMLD5) (European Commission, n.d.) which aims to regulate the use of virtual currencies as a tool for money laundering. The Netherlands has transferred this directive in their national legislation mid 2020. The directive entails a duty for all virtual currency exchanges to register at a national authority. In order to obtain the registration the companies have to prove that they perform customer due diligence and monitor and track transactions continuously. Moreover, the companies are obliged to notify authorities when suspicious transactions take place.

1.2. Integrity and effectiveness

Dealing with money laundering is highly relevant to society due to three reasons. First, the financial system is based on trust. Money laundering facilitates the mixing of laundered money with regular money ("Kamerstukken II, 31477, 1-2 (Rapport)", 2007). This can compromise the integrity of the financial system. Moreover, it can harm the stability and reputation of the financial system and hamper the development of the system (Ministerie van Financien & Ministerie van Justitie en Veiligheid, 2020). This mixing of money can ensure that the Dutch legal economy can be embraced by criminals for illegal practises. All of this forms a risk for the trust the financial system is based upon. Secondly, ensuring that detection is possible and enabling the police to trace suspicious transactions allows them to prosecute criminals and adhere to the narrative that crime should not be rewarding. Lastly, it is important that the policies in place are effective. Understanding the effectiveness of the implementation of the fifth Anti-Money Laundering Directive helps in attaining this goal.

Moreover, understanding the implications of the 5thAnti-Money Laundering Directive to virtual currency exchanges is relevant to the Masters programme Engineering & Policy Analysis of the Delft University of Technology. The programme focuses on policy and politics of complex socio-technical systems and the analysis of data coming from these systems. Desmond et al. (2019) showed that cryptolaundering is part of a complex socio-technical system. Analysing the system thus adheres to one of the pointers of the education. With this research it will be attempted to provide a policy evaluation in order to improve the policy making for virtual currencies, which is directly linked to the policy aspect of the education. For these reasons the topic greatly connects to the Masters programme.

1.3. Research objective

First, an overview is given of previous research that was executed on money laundering and virtual currencies to obtain a better grasp of the research topic at hand. Next an exploration is made into the gaps in this current body of knowledge. These knowledge gaps will be adopted to formulate a research objective and further specify what will be tried to achieve with this research. Next, the main research question will be formulated and sub questions will be composed to help answer the main question.

1.3.1. Previous research

This subsection provides an overview of the previous research into money laundering with crypto currencies. First the phenomena of money laundering with virtual currencies is discussed. Then, the identification of virtual currency adopters will be explained. Next, an elaboration will be provided on the regulation of virtual currencies.

Phenomena of money laundering with virtual currencies

Virtual currencies pose a major risk to money laundering (van der Veen and Heuts, 2020). These risks find their basis in the nature of the transactions as well as in the characteristics of the system. Transactions in the system are irreversible (Fletcher et al., 2021). Therefore once a transaction has been made it cannot be undone. Moreover, the internet provides transnational opportunities for the transactions, contributing to difficulties with

jurisdictions due to the borderless nature of the system (De Vido, 2019; Fletcher et al., 2021; Tropina, 2014). The speed and ease with which these transactions can be performed enhances the appeal of the adoption of virtual currencies to launder money (Fletcher et al., 2021; Stokes, 2012; Tropina, 2014). Furthermore, the system is structured in such a way that no intermediary has to be involved. Also, no face-to-face contact has to be made in order to execute a transaction (Tropina, 2014) enabling user anonymity (De Vido, 2019; Limba et al., 2019; Stokes, 2012; Tropina, 2014), although pseudo-anonymity is a term better suited for most crypto currencies (Fletcher et al., 2021).

Several researchers have investigated how money laundering with virtual currencies can take place. Limba et al. (2019) and Custers et al. (2019) both identified several approaches to launder money. One of them being to disguise the origin using mixers, blenders or tumblers. The possibilities for reidentification of users is the main driver of the rising interest in mixers and tumblers as these tools remove links between the user and transaction (Crawford and Guan, 2020), which ensures that the correlation that can be found between coins becomes limited. Next, the money could be converted to fiat currency through a virtual currency exchange (Kruisbergen et al., 2019). Important to note is that there is a barrier to the amount of money that can be laundered unnoticeable. Meiklejohn et al. (2016) mentioned that if mixing services or Over-The-Counter brokers do not have the volume to launder thousands of bitcoins the attempt of laundering is immediately visible in the blockchain. However, due to virtual currencies becoming more popular and the increasing amount of licit transactions virtual currencies are becoming a more useful laundering tool since illicit transactions will not stand out as much (Stokes, 2012). Nonetheless, centrality within the system can still pose a unique threat to criminals (Meiklejohn et al., 2016) as this can lead them to being identified.

Identification of virtual currency adopters

The possibilities for re-identification can be classified into two categories. Clustering analysis is adopted by many different authors (see for example Liang et al., 2019; Meiklejohn et al., 2016; Reynolds and Irwin, 2017). In the analysis different wallets or addresses are grouped together based on different heuristics to identify important individuals. The second category is taint analysis. Taint analysis analyses which addresses have been used in previous transactions leading to the current transaction. It can thus be adopted to find the origin of the virtual currency. Moser et al. (2013) used transaction graphs to understand the modes of operation and laundering tools adopted by using taint analysis in a reverse-engineering manner. Ranshous et al. (2017) mentioned that when using transaction graphs in your analysis especially patterns around virtual currency exchanges can provide important information as all transactions travelling from virtual to real world have to go through that portal. Next to clustering and taint analysis other methods can be adopted to re-identify individuals such as using IP-addresses, public keys or other data found on the internet, especially drawing inferences between these data points can uncover identities (Reynolds and Irwin, 2017). In anti-money laundering efforts a combination of these different tools are adopted (Crawford and Guan, 2020).

Regulating virtual currencies

As virtual currencies pose a risk of money laundering regulations have to be put in place to limit them. Nonetheless, regulations often fail to affect virtual currencies due to lack of foresight by those creating the regulation leading to a legal grey area (Bryans, 2014). Böhme et al. (2015) identified four key categories of intermediaries namely currency exchanges, digital wallet providers, mixers and mining pools. On top of these four actor groups Sotiropoulou and Guégan (2017) identified the Bitcoin system itself and the users of the Bitcoin system or the use of bitcoins as being subject to regulation. Other aspects that were mentioned for regulation were keeping track of what bitcoins were sold instead of relying on the accounts and account holders (Moser et al., 2013), since the virtual currency system does not allow for an analogy with the traditional financial system. Next to that, Möser and Narayanan (2019) proposed to establish a blacklist to which coins can be checked in order to more easily detect illicit transactions, coins with questionable origins would be added to the list and could then be recognized. As the virtual currency system was not made for regulation, an idea was introduced of a three-tier regulatory framework consisting of self-regulation organized by a private sector technology company, namely the W3C (Fletcher et al., 2021). Although these other propositions were made for regulation, the European Union decided to apply regulation to virtual currency exchanges as anyone wanting to transfer funds from the virtual to the real world has to pass this portal. Therefore, exchanges have become chokepoints in the virtual currency economy (Meiklejohn et al., 2016; Stokes, 2012).

Many barriers for regulation of the virtual currency system can be identified. First, a descriptive challenge is apparent (Sotiropoulou and Guégan, 2017). Some countries consider virtual currencies to be an asset, others a commodity or even a currency. Moreover, the system lacks a governance structure other than its underlying

software which has several implications for the functioning of the system (Böhme et al., 2015). Governance is defined here as the relationship between actors involved, the legislation under and the context in which they operate. As there is no governance structure available by default, there is no obligation from the system for user verification, which checks users' identities and cross-checks them with the watch-list of embargoed countries, and there is no prohibition on sales of particular items (Limba et al., 2019; Sotiropoulou and Guégan, 2017). Furthermore, anti-money laundering (AML) efforts need to be adapted since all AML regimes were based on knowing the customer. As there is limited information on identities but perfect knowledge on transactions in the virtual currency system (Moser et al., 2013) this poses implications to the AML regime (Campbell-Verduyn, 2017; Tu and Meredith, 2015). The last barrier to regulation is the fact that no central organization can be held accountable as the system is decentralized (Stokes, 2012; Tu and Meredith, 2015).

The European Union implemented the regulation in the 5th Anti-Money Laundering Directive. Nonetheless, legislation is always running behind (Tropina, 2014). New technologies lead to a new governance response which leads to a constriction in the adoption of technology (Campbell-Verduyn, 2017). In the regulatory dialectic, policy makers form reactive regulations based on reacting to what happens (Dupuis and Gleason, 2020). Therefore, several shortcomings of the regulation were marked. First, the regulation does not apply to all trading platforms (De Vido, 2020; Dupuis and Gleason, 2020) since much trade is performed outside the centralized currency exchanges. Also, entities are outdated and there is a major problem with the territoriality of the legislation (De Vido, 2020) as it is unknown where an entity should be located in order to fall under the scope of the directive (De Vido, 2019). Moreover, Dupuis and Gleason (2020) identified several open doors and evasion tactics with which the regulation can be circumvented and money laundering can still be performed.

Not only were concerns voiced as to the effectiveness of the regulation, also worries were expressed on the mandatory adoption of tools to detect suspicious transactions by currency exchanges (Möser and Narayanan, 2019). It could lead to privacy concerns for virtual currency users. The tools are thought not to be sufficient to combat money laundering. Moreover, individual users making payments outside of these services do not have access to those services to perform customer due diligence and will thus have a heightened chance of acquiring illicit coins. Soudijn (2019) mentioned that the heightened attention could have made a dent in the amount of laundering activities. Nonetheless, it could also have led to displacement effects. The blockchain activities could also have shifted or further remained in the underworld (Campbell-Verduyn, 2017).

1.3.2. Knowledge gaps

Several knowledge gaps can be identified in the research surrounding virtual currency exchanges and money laundering. First, research surrounding the role of virtual currency exchanges in the virtual currency ecosystem is scarce. Mostly their gatekeeper role has been emphasized. Kruisbergen et al. (2019) show how virtual currency exchanges play a role in the laundering of money. They demonstrate using a case study that after disguising the origin of the funds it is converted towards fiat currency and next transferred towards a money mule. Here, the virtual currency exchange was thus a facilitator of the money laundering process. On the other hand, some authors showed that especially with regulation of virtual currency exchanges they have become a chokepoint in the virtual currency ecosystem (Meiklejohn et al., 2016; Stokes, 2012). Being a chokepoint demonstrates the difficulties of transferring value from one system to another financial system. Nonetheless, the role of virtual currency exchanges in anti-money laundering is not further described.

Secondly, only some research has been performed into the regulation of the virtual currency ecosystem and the effects of this. Some authors came up with new innovative ideas for regulation (Fletcher et al., 2021; Möser and Narayanan, 2019). Other researchers simply criticized the regulations in place. Christopher (2014) stated that prosecuting virtual currency exchanges will not help in AML. However, cooperation could provide opportunities for obtaining new information on transactions. De Vido (2020) on the other hand specifically criticized the implementation of the AMLD5, and demonstrated how the legislation was already outdated. Moreover, Soudijn (2019) showed that the heightened attention due to the new regulations could have led to a dent in the amount of money laundering activities. Nonetheless, Campbell-Verduyn (2017) stated that the activities could also have shifted someplace else or further remained in the underworld. The precise effects of the regulations are thus unknown.

The 5th Anti-Money Laundering Directive introduced further responsibilities for AML efforts for virtual currency exchanges in Europe. However, as the role, daily operations and current or previous AML efforts of virtual currency exchanges are unidentified it cannot be known whether the regulation put in place is able to have the desired effect. Therefore, in order to understand the effectiveness of the AMLD5 it needs to be understood what the implications of the legislation are for virtual currency exchanges. This research attempts to provide insights into the effects of the implementation of the AMLD5 on the daily operations of virtual currency exchange ser-

vices in order to fill this knowledge gap and understand the effectiveness of the regulation. The AMLD5 affects all virtual currency exchanges in Europe. Nevertheless, this research focuses on the virtual currency exchanges active in the Netherlands as the implementation in Dutch legislation is considered. Since the legislation provides room for differentiation between the different member states one member state was chosen. It was seen before that one of the legislation's shortcomings is defining what exchanges are actually active . According to the legislation, all virtual currency exchanges making trades with clients in the Netherlands should have a registration. Therefore, it was chosen to adopt a broad scope for virtual currency exchanges active in the Netherlands. Thus, considering exchanges that in any way possible seem to have a link to the Netherlands, be it through a Dutch website or Dutch payment methods.

1.3.3. Research questions

In order to provide insights into the effects of the implementation of the AMLD5 on the daily operations of virtual currency exchange services and understand the effectiveness of the 5th Anti-Money Laundering Directive the following main research question has been formulated.

To what extent have virtual currency exchanges in the Netherlands altered their daily operations in order to comply to the Dutch implementation of the 5th Anti-Money Laundering Directive?

To understand how virtual currency exchanges have been affected by the AMLD5 it is imperative to first further investigate the definitions and characteristics of virtual currencies and the money laundering process in which they can be adopted. Furthermore, the landscape in which virtual currency exchanges operate and the governance framework that exists in the system needs to be identified to obtain an understanding of the system which can be adopted in the rest of the research. Doing so will answer sub question 1.

1. What is the current state of governance in anti-money laundering in the virtual currency ecosystem?

To develop further understanding of the ecosystem and the effects of the implementation of the legislation it is relevant to obtain insights from transaction data that can show patterns and changes due to the regulation. With this renewed understanding a foundation will be laid out for further analysis of the landscape. This foundation will be laid with the help of sub question 2.

2. What changes in transaction behaviour surrounding Dutch virtual currency exchanges can be observed from the blockchain after the implementation of the 5th Anti-Money Laundering Directive?

With a clear overview of the field the virtual currency exchanges play in, the understanding of the processes at hand and some insights into the transaction behaviour, the next research step can be taken. Different parties are involved in the ecosystem, with the regulatory authority and the virtual currency exchanges being the most important in understanding the impact on the daily operations. The regulatory authority, DNB, supervises the virtual currency exchanges. They have left a mark on the ecosystem, ever since they were appointed as regulator. In order to understand how daily operations of virtual currency exchanges have altered, it is relevant to understand what this mark consists of. Next it is essential to understand how virtual currency exchanges themselves would define their role in anti-money laundering and how they have altered their daily operations. This will be done with the help of sub question 3.

3. How has the implementation of the 5th Anti-Money Laundering Directive affected the parties involved in the Netherlands?

All in all, sub question 1 will provide theoretical background to the research problem. Sub question 2 will then provide empirical evidence for the implications of the introduction of the 5th Anti-Money Laundering Directive from transaction data. Lastly, sub question 3 will provide valuable insights from the main players in the ecosystem. Together these sub questions will present an overview of the implications and effectiveness of the regulation and aid in formulating an answer to the main research question.

1.4. Summary Chapter 1 and outline

Virtual currency exchanges provide services that can exchange fiat currency for virtual currency. Virtual currencies are not issued by any jurisdiction and are part of a decentralized system. They provide new opportunities for money laundering due to their often anonymous nature. Tackling the possibility of their adoption for money laundering is important as not doing so compromises the integrity of the financial system. To regulate the system the European Union has decided to put in place the 5th Anti-Money Laundering Directive. This directive

entails that virtual currency exchanges have to register themselves at the Dutch National Bank and perform certain anti-money laundering measures. From the previous research it was shown that only limited research was performed into the role of virtual currency exchanges and that the effectiveness of the regulation was not evaluated. Since the AMLD5 introduces further responsibilities for AML efforts at the virtual currency exchanges, the implications of the introduction need to be understood. This research attempts to provide insights into the effects of the implementation of the AMLD5 on the daily operations of virtual currency exchange services in order to fill these knowledge gaps and understand the effectiveness of the regulation. To do so the following question will be answered.

To what extent have virtual currency exchanges in the Netherlands altered their daily operations inorder to comply to the Dutch implementation of the 5th Anti-Money Laundering Directive?

The next chapter, chapter 2 provides information on the phenomena of money laundering with virtual currencies and it provides information on tools that can be adopted to limit the risk of money laundering. After that, chapter 3 provides an overview of the methodology and data collection methods adopted. It is followed by chapter 4, which provides an overview of the playing field involving all different actors. Moreover, an elaboration is given on the legislation in place on a national and international level. Then, chapter 5 provides the results of the blockchain analysis. Followed by chapter 6, which defines the perspectives of the players involved on the introduction of the legislation. Chapter 7 provides context to the found results and recommendations for future research. Finally, in chapter 8 the main research question is answered and a conclusion is provided.

2

Money laundering defined

This chapter looks at the phenomenon of money laundering as this is one of the main reasons for the introduction of the 5th Anti-Money Laundering Directive. The chapter first explores the phenomenon of money laundering in section 2.1. Next, the application of money laundering using virtual currencies is investigated in section 2.2. Lastly, the tools that are available to prevent and diminish the risks of money laundering are discussed in section 2.3.

2.1. Phenomenon

According to Koningsveld (2008) two definitions apply to money laundering. The empirical definition states that money laundering can be seen as disguising the criminal origin of funds and giving them a legitimate status, it comprises all actions the perpetrator takes to do so (Kruisbergen and Soudijn, 2015). The Dutch government approaches the empirical definition, which looks at the disguising of the origin of funds, as the economic definition, since it looks at the disguising of the origin in the economic system. The economic definition focuses on the manner in which money with a criminal origin is entered into the legal financial circuit and used, in such a way that the origin is disguised (van der Veen and Heuts, 2020).

Next to the economic or empirical definition a legal definition of money laundering is apparent. Article 420bis of the Dutch Penal Code states "Punished as guilty of money laundering…is he who conceals or disguises the real nature, origin, location, disposal or displacement of an object, or conceals who is the owner of an object or who possesses the object, while knowing that the object - directly or indirectly - derives from any crime". An object here can also be seen as money. Moreover, in the Dutch criminal law deliberate, guilt and habit money laundering are defined. Habit money laundering entails repeating the criminal offense multiple times, according to Article420ter of the Dutch Penal Code. Guilt laundering describes that someone obtained a certain object of which the person had ought to know that it originated in a criminal offense (Anti Money Laundering Centre, 2018). With deliberate money laundering the perpetrator consciously knew he was disguising the origin of the object (Anti Money Laundering Centre, 2018). In all cases the primary goal is to invest criminal money in the legitimate economy, without raising suspicion amongst the authorities that the money has an illicit origin (Koningsveld, 2008).

In the context of the risk on money laundering the Dutch government adheres to the economic definition of money laundering (van der Veen and Heuts, 2020). Therefore,throughout this research this definition is adopted when discussing money laundering.

To describe money laundering often a three stage model is applied (Koningsveld, 2008). The three phases are placement, layering and integration. Placement entails introducing criminal proceeds into the financial system to make it easier to transfer the funds (Levi and Soudijn, 2020). With layering distance is created between the unlawful origin of the money, often the money is moved around several times (Koningsveld, 2008). This will provide an appearance of legitimacy (Levi 2020). In the integration phase the disguised criminal proceeds enter the legal economy and are spend or invested (Levi and Soudijn, 2020).

There are many different constructions of classical money laundering, the complexity of them differs for the type of crime, revenue, offender's goals and the anti-money laundering regime (Levi and Soudijn, 2020). Classical money laundering constructions consist of fictitious turnover, fictitious gambling profits, loanback (Soudijn, 2019) or investment in real estate (Kruisbergen and Soudijn, 2015). Money laundering can also take place

through the direct spending on purchases via online shopping, purchasing of luxury goods or purchases of bitcoins (Custers et al., 2019). The latter making money laundering with cryptocurrencies possible. Moreover, according to Limba et al. (2019) two approaches can be adopted before the laundering process starts, namely money laundering wholesale, in which a large sum of money is laundered at once, or money laundering partitioning, also called smurfing. Smurfing is an easier way of structuring payments in which large sums of money are split up (Stokes, 2012), making the laundering less apparent in the financial system and avoiding suspicion (Custers et al., 2020). Often laundered money is used to finance new other crimes (Levi, 2015).

2.2. Money laundering with virtual currencies

This section provides more information on how the process of money laundering takes place when adopting virtual currencies. First, the model as previously explained will be altered to fit the characteristics of virtual currencies. Bitcoin is an example of a virtual currency. In order to understand effectively how virtual currencies can be adopted to launder money the process of transacting with bitcoins is set out after that.

2.2.1. Altering the model

As seen before money laundering follows the three-stage model of placement, layering and integration. However, virtual currencies are unique as they do not completely adhere to the model and they may enter or exit the process at any stage and serve as both input as well as output to a stage (Desmond et al., 2019). Despite the three stage model being generally accepted and adopted, Custers et al. (2020) found that in general for money laundering with virtual currencies a two stage model is better suitable. Often the placement stage can be skipped as with virtual currencies or cryptocurrencies the money is already in a financial system and at a place where the origin can 'easily' be disguised. Thus, removing the necessity of at first implementing the money into a financial system. A straightforward laundering method is to create a long string of several transactions. In this string money can be converted between different virtual currencies (Custers et al., 2020) or transferred between different addresses or individuals.

Moreover, for virtual currencies it might be beneficial to split up the money to be laundered into smaller amounts and to pursue the smurfing tactic (Stokes, 2012). When virtual currencies are used to launder money often mixing services are used to disguise the origin of the money (Custers et al., 2020). Mixers, blenders or tumblers (Custers et al., 2019) mix several funds together in such a way that no correlation can be established between the input and the output of a mixing service. The client of the service thus gets funds back that are not related to the funds they used as input to the service. Therefore, mixing services can be highly effective in disguising the origin of the money. In the second phase the virtual currency can be transferred towards one or more intermediaries to further exchange the money (Custers et al., 2020). Regularly money is laundered through the direct spending of it (Custers et al., 2019). Bitcoin can for example be used in online casinos, on hosting services or even during online shopping (Custers et al., 2020). Nonetheless, a criminal can also opt for adopting a virtual currency exchange in order to convert their now "clean" money to fiat currency (Kruisbergen et al., 2019).

2.2.2. Bitcoin transaction background

In order to execute a transaction through a blockchain several requirements exist. The person wanting to transfer money has to set up a wallet. A wallet is a place where bitcoin (BTC) is stored. There exist many different versions of wallets where one can store his coins. Connected to the wallet is an address. Nonetheless, one wallet can contain multiple addresses. Moreover, a user has a public key and a private key. The bitcoin wallet address is mathematically related to the public key of the user (Prypto, n.d.), the public key is a hashed version of the address. The private key of a user is necessary in order to spend BTC as it can be adopted to decode a public key (Paxful Team, 2020).

In other words if a person A wants to transfer bitcoin to a person B, person A sends a message stating that he wants to send bitcoin to person B. This message is encrypted using the public key of person B. Since only person B has the private key necessary to decipher the message, person B can then obtain the transaction. Next, the transaction will be published and new transactions that are published are grouped together into a block on the blockchain. A continuous synchronisation is performed in order to keep the transaction record up to date (Böhme et al., 2015). The grouping together of transactions is executed based on a time-stamp technology ensuring that funds cannot be spend multiple times (Nakamoto, 2008). The blockchain is publicly available and can be inspected through several websites. The encryption and use of addresses that are not directly linked to an individual enhances the privacy of blockchain adopters.

One interesting thing that blockchain transactions characterise is the multiple-input spending heuristic, or co-spending heuristic. In the whitepaper by Nakamoto (2008), the creator of Bitcoin, he showed that one transaction on the blockchain can consist of multiple input addresses. Each of these addresses might contain smaller amounts from other previous transactions. Together they can be adopted to pay one full transaction. The output can consist of at most two outputs since one is the output to the other party and the other output is the possible change going back to the person making the transfer. Due to the multiple-input spending heuristic it is possible to understand how several addresses can be linked together. Addresses that are used together as inputs in a transaction are under control of one entity, making clustering possible to identify individuals.

2.3. Anti-money laundering tools

In order to minimise the chances of the laundered money getting into the classical financial system governments and businesses have several tools. The first set of tools focuses on identifying and verifying the customer and beforehand assessing the risk of the client. The second set of tools is adopted to continuously monitor the transactions that are being executed in order to identify unusual transactions. Finally, unusual transactions have to be notified at the Financial Intelligence Unit in the Netherlands (FIU-NL) in order for them to identify whether the transactions was suspicious and whether prosecution should take place.

2.3.1. Customer Due Diligence

Know Your Customer (KYC) is the process in which an institution obtains understanding of who their customers are and what they do throughout the relationship with them (de Wit, 2007). Customer Due Diligence (CDD) is a slightly broader process consisting of not only the identification which KYC entails, but also of the monitoring of the clients transactions on a continuous basis (Tuba and Van Der Westhuizen, 2014). In order to obtain integrity in the business operations it is essential for institutions to know who they are entering into a business relationship with or for whom they are conducting an incidental transaction (DNB, 2020). According to the Basel Committee on Banking Supervision (BCBS) (2001) having sound KYC procedures are a critical element in the effective management of risks for financial institutions. Moreover, it helps protect the reputation and the integrity of the financial system by reducing the likelihood that the institution will become a vehicle or victim of financial crime (Basel Committee on Banking Supervision, 2001).

Risk-based approach

In order to put in place sound CDD procedures a risk-based approach is adopted. A risk analysis needs to be composed at different levels. First, the European Committee draws up a supranational risk assessment. Second, the member states draft a national risk analysis (Het Europees Parlement en de Raad van de Europese Unie, 2015). By adopting a risk-based assessment countries put in place an effective allocation of resources (FATF, 2020). With the national and supranational risks assessments the government of member states know what risks for money laundering are most apparent and what should be focused on.

According to article 8 of the consolidated directive (Het Europees Parlement en de Raad van de Europese Unie, 2015) businesses themselves have to compose a risk analysis to understand where the highest risks within their company lie in the money laundering area. This systematic analysis of integrity risks (SIRA) has several objectives (DNB, 2020). Namely, with it it is sought to establish adequate policy for risk management and to elaborate upon the policy principles in lines of conduct, procedures and measures. A manner for systematic testing and assessment of the adequacy of the control environment is provided in the SIRA. Moreover, a compliance function is set up, appropriate to the size and function of the organisation, and the institution needs to ensure that an independent audit function can be performed.

After having drawn up a company wide risk assessment for each client a separate risk assessment needs to be produced. Each client will be classified into a risk category after the onboarding of the client. Also, each client has a separate risk profile used to monitor the behaviour of the client with (DNB, 2020). The risk assessments are performed based on the type of client, the product or service offered, the channel of delivery and geographical factors (AFM, 2020). When the origin of a transaction is more difficult to trace the transaction or client provides a higher risk to the institution (DNB, 2020). The intensity of the KYC programmes should be tailored to the degree of risk (Basel Committee on Banking Supervision, 2001). This is also apparent in article 15 paragraph 1 of the EU directive (Het Europees Parlement en de Raad van de Europese Unie, 2015) as with lower risk simplified customer due diligence processes can be applied. The risk-based approach thus provides a flexible approach to the KYC and CDD process as it may differ per client (Tuba and Van Der Westhuizen, 2014).

Process

The Basel Committee on Banking Supervision (2001) identified four elements of a CDD policy; customer acceptance policy, customer identification, on-going monitoring of high risk accounts and risk management. Especially the customer acceptance policy is crucial as the information obtained during this stage will be used during the lifetime of the relationship (de Wit, 2007). The Financial Action Task Force (FATF) recommendations (2020) state four elements of the CDD policy which are in some ways very similar to the elements of the BCBS. They first identify the customer and verify that customer's identity using reliable independent source documents, data or information. This identity can be verified by using several documents such as but not limited to a passport, id-card or driving license (AFM, 2020). This consists of the first two steps of the BCBS CDD policy. Next, if business will be performed with a legal entity (AFM, 2020) the ultimate beneficial owner needs to be identified, and measures need to be taken to verify this entity. As for virtual currency exchanges their clients will most often be non-legal entities this phase can be skipped. The following step is to understand and obtain information on the purpose and intended nature of the relationship (FATF, 2020). In the case of exchanging virtual currency for fiat currency the conversion is the purpose. The intended nature of the business relationship can differ per client as some clients only want to conduct one transaction whereas others want to have a continuous business operation with the virtual currency exchange. Having information on the purpose of the relationship is part of step 2 of the BCBS CDD policy, namely customer identification. Lastly, the FATF (2020) identified conducting ongoing due diligence of the business relationship and scrutiny of transactions undertaken as being the last element of a sound CDD policy. This connects to the third element of the BCBS CDD policy. The FATF recommendation for a CDD policy was adopted in article 13 of the EU directive (Het Europees Parlement en de Raad van de Europese Unie, 2015), and is therefore in operation in the EU. All in all, the CDD measures institutions should implement consist of two main elements namely the know your customer measures and the continuous transaction monitoring.

Know your customer

To understand who the client is know your customer measures have to be taken at several points in time. First, for new clients client identification and verification needs to be performed when a new business relationship is set up. Moreover, when an incidental transaction is made of over €15000.-, when several incidental transactions are made which correlate with a total value of over €15000 or when the financial institution executes a money transfer of at least €1000.-. Also, if there are indications that a client is involved with money laundering or the financing of terrorism new KYC measures have to be taken. Lastly, when a client resides in a country or geographical location which provides a high risk of being involved with money laundering (AFM, 2020).

For existing clients some different indications are held up for the KYC measures. According to article 14 paragraph 5 of the EU directive (Het Europees Parlement en de Raad van de Europese Unie, 2015) it is stated that due diligence measures can also be applied to existing clients depending on the risk sensitivity of these clients and when their circumstances change. Mostly the KYC measures will be applied if there are indications that the client is involved with money laundering, when the client provides a high risk or when the institutions doubts the correctness of the data provided in advance (AFM, 2020).

At these different points in time a client may thus be asked to re-identify themselves and verify their identity. Moreover, the institution may have to perform new measures in order to understand the purpose and nature of the relationship between them and their client. Implementing KYC measures and executing them also for existing clients will ensure that the understanding remains up to date.

Continuous monitoring

A business relationship can be formed after accepting the client and knowing who they are, what their purpose is and having formulated a risk profile. An institution has to take reasonable measures in order to investigate complex and unusual transactions as well as any unusual transaction patterns that do not seem to have an economic or legitimate purpose (Ministerie van Financien & Ministerie van Justitie en Veiligheid, 2020). In order to do so, transaction monitoring has to take place. Transaction monitoring takes place based on several detection rules, transaction amount thresholds and the risk profile drawn up during the acceptance phase (AFM, 2020). All in all several indicators are used. The subjective indicator merely states that a transaction for which the institution has reason to assume that it is connected to money laundering can be seen as an unusual transaction (FIU, n.d.). Moreover, for virtual currency exchanges two objective indicators play a role. When a transaction is made of over €15000.-, this is an indicator to examine the transaction. When a transaction is made of over €10000.- for which an exchange takes place between virtual and fiat currency this also portrays an unusual transaction (FIU, n.d.). For all these unusual transactions a notification has to be made at FIU-NL. Especially the subjective indicator is important as this provides the opportunity for the institutions to compare the expected account activity

to the real activity. If continuous monitoring of transactions is not performed no suspicious or unusual transactions can be signalled (Basel Committee on Banking Supervision, 2001). The amount of continuous monitoring or how it is precisely executed, however, can differ for clients in different risk categories (de Wit, 2007).

2.3.2. Reporting duty

The novelty of the fifth Anti-money laundering directive of the EU lies partially in the fact that it imparts a duty to report on the virtual currency exchanges. After the institutions have discovered unusual activity in an account or an unusual transaction using the indicators described in section 2.3 this needs to be signalled to the financial intelligence unit the currency exchange resides in. The duty to report applies to both those transactions already carried out and those not yet carried out but already intended (Ministerie van Financien & Ministerie van Justitie en Veiligheid, 2020). The signals of money laundering in the Netherlands go to FIU-NL, through their online reporting portal. FIU-NL can start up a criminal investigation by judging the information provided and they pass on transactions that they have found to be suspicious to investigative services ("Kamerstukken II, 31477, 1-2 (Rapport)", 2007). When an institution makes a notification of unusual activities they must adhere to a duty of confidentiality (Het Europees Parlement en de Raad van de Europese Unie, 2015, article 39), meaning that the companies cannot provide information on the reports of unusual transactions which they made. Furthermore, the institution has to store all data important for the notification over the next five years (Ministerie van Financien & Ministerie van Justitie en Veiligheid, 2020t).

Next to FIU-NL investigating the signals they were provided with, which is an operational analysis, they are also in charge of executing immediate urgent action, according to article 32 paragraph 8 of the directive (Het Europees Parlement en de Raad van de Europese Unie, 2015). Also, the financial intelligence units are in charge of executing a strategic analysis of discovering new trends and patterns in the signals they are provided with.

2.4. Summary Chapter 2

Money laundering is the process of disguising the origin of criminal funds and providing them with a legitimate status so that they can be used in the traditional financial system. The process of money laundering with virtual currencies consists of two steps, layering and integration. Mixing services are adopted to remove a relation between the origin of the funds. Virtual currency exchanges can then be adopted to convert the funds between virtual and fiat currency. To remove the risks of money laundering different tools can be adopted. Customer due diligence entails understanding who the client is and what the business relationship is like. Based on risks associated with the clients different measures can be adopted to identify the client and monitor the transactions. Several indicators exist for identifying unusual transactions. For virtual currency exchanges the most important ones are the subjective indicator which involves all transactions they find unusual. The objective indicator states that all transactions which exchange €10000.- between virtual and fiat currency should also be notified. Notifications of unusual transactions have to be made at FIU-NL who can then investigate whether the transactions are also suspicious and prosecution has to be performed.

3

Methods and data

This chapter explains the methods adopted and the data collected and used within this research. First, the choice for an exploratory mixed methods research approach is explained in section 3.1. Next, an overview of the methods adopted to answer the research questions and the data collection methods are set out in section 3.2.

3.1. Approach

Within this research the effects of the introduction of the 5th Anti-Money Laundering Directive on virtual currency exchanges are explored. The research thus has an explorative character as it is so far unknown what these effects consist of. To answer the research and corresponding sub questions a mixed methods approach will be adopted. Within a mixed methods approach different methods are adopted that provide answers to the same questions, in this way providing context to the study. Although there is some speculation on the precise definition of a mixed methods approach, almost all researchers identify a qualitative and a quantitative component (Johnson et al., 2007). Within the mixed methods approach a combination can be sought of research techniques, methods, approaches, concepts or languages into a single study (Johnson and Onwuegbuzie, 2004). Here an equal status design will be adopted, in which both the quantitative and qualitative aspect have an equal importance (Johnson et al., 2007).

Three important advantages can be identified of using a mixed methods approach. Firstly, due to the combination of different methods the accuracy of the research can be improved and a higher confidence in the results can be obtained (Jick, 1979). This is due to the multiple perspectives complementing each other. Moreover, the weaknesses in a single method will be compensated by the counter-balancing strengths of the other method adopted (Jick, 1979; Johnson and Onwuegbuzie, 2004). Secondly, using multiple methods makes it easier to better answer the research question. Using different methods allows for obtaining more useful insights that will be better equipped to fully answer the research question. Also, it can lead to new insights and understandings that would have been missed when only a single method would be used (Johnson and Onwuegbuzie, 2004). Thirdly, stronger conclusions can be drawn. In mixed method research between method triangulation is adopted (Denzin, 2017; Johnson et al., 2007). Through the convergence and integration of findings stronger evidence can be found (Johnson and Onwuegbuzie, 2004).

Nonetheless, a mixed methods approach also poses some challenges as the researcher must learn about multiple methods and understand how to mix them appropriately (Johnson and Onwuegbuzie, 2004). The methods that will be adopted, see section 3.2, are complementary, which allows them to be mixed effectively. Moreover, the research can be more expensive as it is more time consuming (Johnson and Onwuegbuzie, 2004). Due to the time constraints a specific timeline is adopted, of in total twenty-five weeks. Lastly, replication is exceedingly difficult due to the qualitative methods (Jick, 1979). By adopting a clear approach and methodology the possibilities for replicability will be guaranteed.

3.2. Methodology

This section further focuses on the methods that are adopted in this research. Table 3.1 shows an overview of the three different phases in the research, the sub questions corresponding to the phase and the methods with which these sub questions are answered. Together the sub questions answer the main research question: *"To*

what extent have virtual currency exchanges in the Netherlands altered their daily operations in order to comply to the Dutch implementation of the 5th Anti-Money Laundering Directive?". This section provides information on how the methods are adopted and the data collected and used. First, the desk research method is explained. After that, an overview is given of how the blockchain analysis was executed. Lastly, the used interview methodology is set out. Together this provides the basis for the research performed.

Table 3.1: Sub questions and the corresponding methodology

Sub question	Methodology
1. What is the current state of governance in anti-money laundering in the virtual currency ecosystem?	Desk research
2. What changes in transaction behaviour surrounding Dutch virtual currency exchanges can be observed from the blockchain after the implementation of the 5th Anti-Money Laundering Directive?	Blockchain analysis
3. How has the implementation of the 5th Anti-Money Laundering Directive affected the parties involved?	Interviews

3.2.1. Desk research

Desk research is adopted in obtaining previous research, the collection of background information on the topic and to answer sub question 1 *"What is the current state of governance in anti-money laundering in the virtual currency ecosystem?"*. Desk research is also sometimes called secondary research (Stewart and Kamins, 1993). It is complementary to primary research and often the starting position of a research project (Stewart and Kamins, 1993). It consists of looking at unobtrusive measures of information, which entails information in which the researcher does not influence the information by her presence (Piotrowski, 2007). The data consists of sources of information collected by others and archived in some form (Stewart and Kamins, 1993). Three different sources of information will be employed. First, academic literature will be used to establish the state of the art in anti-money laundering research. Second, grey literature, consisting of governmental websites and industry reports, will be adopted to provide the environmental context in which the phenomenon of money laundering with virtual currencies takes place. Lastly, legislation will be used to provide an overview of the legal landscape.

To obtain previous literature, a search is made in the Scopus database using a combination of the following key words: "crypto", "virtual", "currency", "bitcoin", "exchange", "money laundering" or "cyber laundering". Scopus produced 32 results. Papers are included if they are related to the governance or legislation and supervision in the system, they provide information on using technology to identify transaction behaviour or if it provides information on money laundering methods. If the research purely discusses human rights, such as privacy, was only related to online social networks or purely discusses the technology of blockchain it was left out of scope. The first round of search provided 15 results. After snowballing, 24 documents remained and are included in the overview of previous research.

During the collection of background information several sources are used in the desk research. First, to get a better insight into the Dutch situation https://www.wetten.overheid.nl is used to access the Dutch penal code. Also, grey literature is adopted consisting of industry reports explaining more on the process and role of virtual currency exchanges. Lastly, policy documents linked to the Wwft ("Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)", n.d.) and the anti-money laundering policy were identified and explored.

To identify the governance framework of virtual currency exchanges, the policy documents used to produce the Wet ter voorkoming van Witwassen en Financieren van Terrorisme ("Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)", n.d.) are taken as a basis. Moreover, legislation and their separate revisions and alterations are explored through https://www.wetten.overheid.nl. Next, governmental and industry websites provide information on the different actors involved and their roles and perspectives in anti-money laundering.

Desk research has many advantages. It is an inexpensive method (Piotrowski, 2007; Stewart and Kamins, 1993) which is easily repeatable if the method has clearly been laid out (Piotrowski, 2007). Moreover, it is a good starting point for further research. Incorporating grey literature has the advantage that it can contain new information earlier than other forms of research and that it simplifies difficult concepts for a non-specialist audience (Pappas and Williams, 2011). Nonetheless, to enhance confidence in conclusions, triangulation is adopted between different data sources as the sources may not be complete (Piotrowski, 2007) or relevant and might be outdated (Stewart and Kamins, 1993) and different sources can complement each other.

3.2.2. Blockchain analysis

To establish empirical evidence of the difference between the time before the implementation of the AMLD5 and after the implementation of the legislation a blockchain analysis performed. Only bitcoin transactions are taken into account as bitcoin is the most adopted virtual currency (Sim, 2021) and the blockchain transaction data is publicly available. First, the process of collecting transaction data is explained. Then, some light is shed on the criticisms of the data collection method. Next, an overview of the bitcoin transaction data that was collected is given. Finally, the aspects of the system that are considered are set out and the method of analysis is explicated. With the blockchain analysis an answer is provided to sub question 2 *"What changes in transaction behaviour surrounding Dutch virtual currency exchanges can be observed from the blockchain after the implementation of the 5th Anti-Money Laundering Directive?"*.

Data collection

As the blockchain data is publicly available it is possible to identify and investigate transactions that were made. To understand what transactions had to be investigated, first, an overview is made of active exchanges in the Netherlands. This process started by exploring the Dutch National Bank (DNB) registry of all Dutch virtual currency exchanges that obtained a registration. This led to 20 virtual currency exchanges being identified [1]. Next, of these exchanges an exploration is made of their size, period of activity and their services. To do so their webpages, newspaper articles and social media are investigated.

During the investigation of the registered exchanges several other exchanges being active in the Netherlands before the duty to register are identified. All exchanges are included which have a Dutch web page, Dutch owners or an office in the Netherlands. Moreover, to identify more exchanges that have not registered, a Google search is made using the keywords "Dutch", "Nederlands", "Exchange", "Crypto" and "stopped". The complete search led to a database of 37 virtual currency exchanges. For all of these again an exploration was made of their characteristics. The complete overview of exchanges identified and their characteristics can be found in appendix A.

In order to provide information over a range of time that is as complete as possible two requirements are set up. First, at least two-thirds of the exchanges in the data have to be active over the complete period of time that is going to be researched. It is attempted to achieve a coverage rate of 70%. The second requirement stated that it is tried to establish an equal period of time before and after implementation of the AMLD5. To adhere to these requirements the period chosen is between 01-06-2018 and 31-05-2021. The data is then collected using Chainalysis.

Chainalysis

Chainalysis is a blockchain analytics program. It specializes in visualization and analytics of the bitcoin blockchain. Chainalysis uses open blockchain transaction data and tries to link the individual addresses with which transactions were made into clusters which it then tries to categorize. To do so it adopts the multiple-spending input heuristic which means that someone who has access to both addresses, as can be seen by having both addresses as inputs to one transaction, belongs to one cluster (Nakamoto, 2008).

The other part of the operations of Chainalysis is the fact that the employees of the company transfer very small amounts of money to addresses of which they know who or what organisation the address belongs to. By transferring money to a known service they uncover another address which they can categorize (Chainalysis, n.d.). In this way they can add cluster categories to the identified clusters of addresses.

Chainalysis has had to deal with quite some criticism on several facets of their business. One often heard criticism is that Chainalysis goes against the ideals of crypto as their clustering and identification techniques remove anonymity from the blockchain (for more on this see Harrigan and Fretter, 2016). This is sometimes seen as being unethical as people's privacy is invaded by enabling pattern recognition on transactions (Kapilkov, 2020). Still, Chainalysis merely presents transaction data and only labels services, not individuals (Chainalysis, 2019). Next to that, it is impossible for Chainalysis to provide full information of all transactions. Due to the clustering methodology adopted only addresses used together in a transaction can be clustered. The data Chainalysis provides on transactions, and the clusters identified, may therefore not always be complete.

However, Chainalysis is the marketleader in blockchain analytics software (Azevedo, 2021). One of their largest clients is the US government (Nelson, 2020) and according to one of Chainalysis' employees other countries should start to depend on Chainalysis as well since it allows them to follow the money, leading to catching and prosecuting criminals (Grigg, 2021). Moreover, exchanges in the ecosystem also adopt the functionalities

[1] As the Dutch National Bank registered an extra exchange during the time of this research currently there are 21 virtual currency exchanges registered.

of Chainalysis in their transaction monitoring. Since these countries and companies all use the software in order to minimise illicit activities, Chainalysis also focusses on identifying those. It could, therefore, be the case that the rate of illicit activities identified by Chainalysis is higher than could be expected. Despite that Chainalysis provides the best and most accurate information thus far. They only label a cluster when they are absolutely sure that a cluster belongs to a certain category. This makes the information they provide very reliable and useful in a blockchain analysis thus providing the reason for adopting Chainalysis in the data collection.

Data description

For all 37 Dutch virtual currency exchanges identified before, Chainalysis provided data on 17 of them. They did not possess information on all exchanges active in the Netherlands, meaning that they have not yet identified all of them, or found their clusters. The 17 exchanges on which data was collected consisted of 12 registered exchanges and 5 non-registered exchanges. The data consisted of 17 separate datasets containing the following data on the transactions: date, counterparty cluster name, counterparty category, value and USD value.

After aggregation of the datasets every transaction got assigned the exchange at which the transaction was executed. Also, the exchange rate was calculated. In the documentation of Chainalysis they stated that all transactions having a value of 0.00 were transactions that were made of which they did not know what the precise value of the transactions was. These transactions were removed from the dataset since they do not provide information on the transaction values. Moreover, transactions having a negative value are input transactions, meaning that bitcoin is transferred towards the virtual currency exchange. Transactions with a positive value are output transactions, meaning that the virtual currency exchange transfers bitcoin to a different address.

In the end the final dataset contains 5,328,199 transactions. The dataset contains information on all of these transactions of the date, counterparty cluster name, counterparty category, value, USD Value, Exchange, Registered and Exchange rate. Table 3.2 shows what this information entails in the dataset. Chainalysis provides all values in USD or in BTC, to remove noise it was chosen to present the data Chainalysis provides and not convert the USD value given in the data to the corresponding value in Euro.

Table 3.2: Columns transaction data

Column name	Definition
Date	The date at which the transaction was executed.
Counterparty cluster name	Name of the group of addresses, if identified.
Counterparty category	The type of cluster to which the address belongs
Value	Value of transaction in BTC
USD Value	Value of transaction in USD
Exchange	The name of the exchange at which transaction was executed
Registered	Whether exchange is registered at DNB
Exchange rate	Calculated by Value/USD Value

System aspects

As observed in chapter 1.3.1 often used methods in understanding bitcoin transactions are clustering (Liang et al., 2019; Meiklejohn et al., 2016) and taint analysis (Möser and Narayanan, 2019). Taint analysis analyses which bitcoin addresses have been used in previous transactions, in the end leading to the origin of the bitcoins. With taint analysis the owner of specific coins can be found. Cluster analysis on the other hand is used to understand what goes in and out of a specific node in the blockchain which can have different addresses. Clustering ensures that the corresponding addresses can be found. Thus, clustering analysis can help in identifying all inputs and outputs of cryptocurrency exchanges in the Netherlands. Taint analysis can be adopted to understand where the inputs to the exchange originated from. Especially this last step is important when performing customer due diligence. As it is past the goal of this research to apply a clustering algorithm or a taint analysis algorithm, the necessary transaction data of Dutch virtual currency exchanges is thus extracted from Chainalysis. Chainalysis provides transaction monitoring software which they link to real-life entities, amongst others the virtual currency exchanges, using clustering algorithms ("The Blockchain Analysis Company", n.d.).

The data from the blockchain that will be investigated is the number of transactions executed, the value of transactions and the origin or destination of transactions. The objective indicators of identifying suspicious transactions are linked to the value of the transactions. Investigating the transaction volume is thus interesting to understand the effectiveness of the indicators. The subjective indicators of identifying transactions as being unusual are linked to having a presumption that the funds are obtained in an illicit manner. The origin or destination can provide information on this. Moreover, to understand the effects in the Netherlands on the adoption

of virtual currencies the number of transactions is adopted. Moreover, as was seen in chapter 2, with smurfing the number of transactions and the value of the transactions is of importance as it is deducible by observing many transactions of very small values. Together these three aspects will provide a blockchain analysis on the most important aspects of the system.

Python will be used to explore and analyse the extracted data as it is a powerful program for data analysis. Special focus lies in identifying differences in the trends before and after the implementation of the legislation. A trend is a pattern that is observed over a period of time and shows the difference of the values with respect to time (Vishwas and Patel, 2020). Therefore identifying trends will help in understanding and analysing the differences in transaction behaviour at the virtual currency exchanges. The trends are observed by plotting the data and investigating differences in the patterns. Python packages adopted for data wrangling are Numpy and Pandas and for the data visualization is Matplotlib through JupyterLab version 1.2.6.

3.2.3. Interviews

To answer sub question 3 *"How has the implementation of the 5th Anti-Money Laundering Directive affected the parties involved?"* interviews are held. Interviews are relevant when only little is known about the study phenomenon or where detailed insights are required from individual participants (Gill et al., 2008). Sub question 3 requires comprehensive inside information from those involved in the system, namely the virtual currency exchanges and the regulator, thus interviews provide a relevant methodology. Furthermore, interviews can lead to obtaining a greater depth of information (Kothari, 2004) and can provide extra context to results found in the blockchain analysis. First, this section explains which respondents are approached and who the interviewees are. Next, the interview set-up is explained.

Respondents

For the interviews only parties directly affected by the implementation of the AMLD5 are considered. Therefore, interviews are held with the virtual currency exchanges and the regulator DNB. Different interviewees are approached falling in these two categories. On the side of the exchanges interviewees are sought by approaching members at the interest group VBNL. This leads to virtual currency exchanges that registered at DNB. Employees in the field of anti-money laundering and supervision of virtual currency exchanges at DNB are approached for an interview. These contacts are obtained through the network of the supervisor of this research.

Five interviews are held with in total seven interviewees, as some interviews are held with two interviewees simultaneously. Five belong to virtual currency exchanges, the functions vary from compliance officer to chief financial officers and other board functions. All virtual currency exchanges are part of the interest group Verenigde Bitcoinbedrijven Nederland (VBNL) as the interviewees were approached through the interest group. Of the five virtual currency exchanges included, one non-registered exchange was incorporated. The non-registered exchange altered the services offered after the implementation of the AMLD5. The other four exchanges all registered at the Dutch National Bank. Two interviewees are part of the regulator of which one interviewee focuses mainly on market access and the registration applications whereas the other is specialized on the general supervision of virtual currency exchanges. Together these interviewees provide a wide span of perspectives on the system of parties that are directly affected. Table 3.3 provides an overview of the employment of the interviewees and the respondent number that corresponds to their statements.

Table 3.3: Employment of respondents

Respondent number	Employment
1a	Crypto supervision specialist at DNB
1b	Market access specialist at DNB
2	CFO of a registered virtual currency exchange
3	Co-founder of a non-registered exchange that altered the services they offered
4	Head of risk at a registered exchange
5a	Co-founder of a registered virtual currency exchange
5b	Compliance officer at a registered virtual currency exchange

Interview set-up

The interviews follow a semi-structured set-up. In this interview set-up respondents have to answer pre-set open-ended questions (Jamshed, 2014). According to Gill et al. (2008) using a semi-structured interview enables the researcher to find other areas to be explored that did not seem to be pertinent to the researcher beforehand.

A semi-structured protocol can only be created after research has been done, the desk research provides input for the interview protocol.

Interviews take half an hour and take place through a video conferencing tool. All interviews are conducted in Dutch. To capture the information in the interview effectively, the interviews are recorded and the recordings are transcribed. After that, the interviews are assimilated and the perspectives on several topics are compared to each other.

Not all interviewees are asked the same set of questions. Depending on the expertise and the background of the interviewee a different subset of questions is adopted in order to ensure a differentiation in interviews between on the one hand the regulator and on the other the virtual currency exchanges. The interview protocols can be found in appendices C and D. Six topics are discussed. First, to obtain insights into whether the parties also consider money laundering with virtual currencies a risk, the topic of the *adoption of virtual currencies* by criminal parties is discussed. Next, the *anti-money laundering responsibilities* of the parties are examined by identifying their role in the system and how they act in the system based on this responsibility. In order to obtain information on the effects of the legislation, the perspective of the parties on the introduction of the *legislation* is considered and the effects it has had. Next, insight is attempted to be obtained on the measures of *transaction monitoring* that the parties have in place. The following topic reviewed is the topic of *registration and supervision* which encompasses the whole registration procedure and what supervision currently looks like. Lastly, the parties are asked to provide a *future outlook*. Together these topics provide information on the situation before and after the implementation of the legislation and on any alterations that were observed in the system.

3.3. Summary chapter 3

Within this research the effects of the introduction of the 5th Anti-Money Laundering Directive on virtual currency exchanges are explored. The explorative research question will be answered using a mixed methods approach. A mixed methods research approach often consists of a qualitative and a quantitative part. The methods adopted in this research are desk research, blockchain analysis and semi-structured interviews. Desk research provides input for the governance framework in anti-money laundering. With the blockchain analysis insight will be obtained in the effects of the AMLD5 on transactions at Dutch virtual currency exchanges. The semi-structured interviews lead to detailed insights of the parties directly affected by the implementation of the legislation, namely the regulator and the virtual currency exchanges. Together these methods answer the main research question.

4

Governance

Governance is defined here as the relationship between actors involved, the legislation under and the context in which they operate. This chapter provides information on all aspects of this definition of governance. First, section 4.1 explores the legislation that is in place on an European and national level. Next, the landscape in which virtual currency exchanges operate is defined in section 4.2, the parties involved are discussed here on an European as well as a national level. It was chosen to look at the problem from an European and a national level since discussion on an EU level has a direct influence on the national discourse and directives also have a direct effect on the legislation in place. Moreover, the system has some partnerships between different member states that should also be taken into account. In section 4.3 sub question 1 is answered.

4.1. Legislation

This section discusses the evolution of the legislation in place to counter money laundering. Moreover, it sets out the legal context in which virtual currency exchanges operate and the conditions they have to adhere to. Thus, this section provides the fundamentals for possible changes of daily operations of virtual currency exchanges in the Netherlands. First, the European legislation will be provided. Next, an overview will be given of how the European legislation is reflected in the Dutch legislation. Figure 4.1 provides an overview of the timeline of the production of the legislation. It was chosen to focus on the legislation from the 4th Anti-Money Laundering Directive (AMLD4) onward as this provides the basis for many of the requirements that the virtual currency exchanges have to adhere to.

4.1.1. European legislation

The European legislation contains six revisions of anti-money laundering legislation. The 1st directive purely focused on the laundering of money stemming from drug offenses. The 2nd Anti-Money Laundering Directive extended the illegal acts and professions included in the legislation. Only in the 3rd Anti-Money Laundering Directive a start was made in focusing on the financing of terrorism as well ("Kamerstukken II, 34808, 3 (MvT)", 2017).

In 2015 renewed interest was awakened for money laundering and terrorism financing. The 4th Anti-Money Laundering Directive (2015/849) came into effect in June 2015 and had to be implemented in national legislation by the 26th of June 2017. Goal of this revision to the 3rd Anti-Money Laundering Directive was to strengthen regulation with regards to customer identification. Moreover, information on the ultimate beneficial owner had to be registered in a central register. Furthermore, the European Commission will implement risk assessments to increase the awareness of money laundering and terrorism financing risks. The last two key issues the AMLD4 tried to accomplish was establishing a course of action for treatment of countries outside the Union, by setting up a list of high risk countries and the cooperation between Financial Intelligence Units (FIUs) were to be increased by enhancing possibilities for the exchange of information. Next to the AMLD4, implemented simultaneously was the Regulation Traceability of Money Transfers (2015/847). This regulation obliged payment service providers to store name and account number of a transaction and check the correctness of the information obtained in order to facilitate AML efforts.

In 2018 the revision of the AMLD4 was implemented. The 5th Anti-Money Laundering Directive (2018/843) had to be implemented by January 10th 2020. The Directive entailed that also exchange services, exchang-

ing between fiat currency and virtual currency, and custodian wallet providers are obliged to notify suspicious transactions. Moreover, these entities have to be registered at a national authority. The directive included a definition of virtual currencies and stated that customer due diligence should not only be performed on new customers but also on existing customers. The member states themselves could choose how to implement this revised directive, which established some differences between the member states.

At the end of 2018 the 6th AMLD was set-up which captured specific illegal acts and specified sanctions that were effective, deterrent and proportionate. The directive had to be implemented by December 3rd 2020 but did not alter the legislation concerning virtual currency exchanges.

Currently, the European Committee is discussing new legislation as part of their Digital Finance Package (Betting, 2021). The proposed legislation is called Markets in Crypto-assets, MiCA. With this the EU tries to remove differences between member states by providing a common EU framework, in this way establishing a more even playing field (European Commission, 2020). Possibly, MiCA can lead to a licensing regime, however as it is still being discussed at present the precise results are not yet known. It is likely that MiCA will become operational in 2022, meaning that in 2024 virtual currency exchanges will have to comply to the new legislation (Betting, 2021).

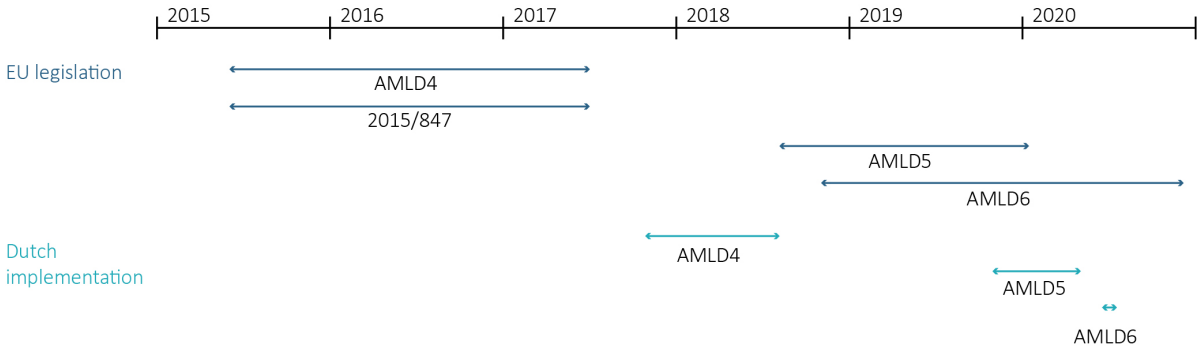


Figure 4.1: Timeline of the implementation of the Anti-Money Laundering Directives

4.1.2. National Legislation

The Dutch National Legislation has four main laws in which the legislation on money laundering is captured. Firstly, the definition and incrimination of money laundering is captured in the Dutch Penal Code, article 420. Moreover, the Wet op het Finacieel Toezicht (BWBR0020368 - Wft) regulates how the national government supervises financial institutions (Rjksoverheid, n.d.). The goal is to protect customers who entrust their money to these financial institutions. The supervision on these financial institutions will ensure that the financial markets work efficiently. Moreover, it guarantees the stability of the financial system (Rjksoverheid, n.d.), which can only be done by preventing money laundering. Thirdly, with the Wet ter voorkoming van Witwassen en Financieren van Terrorisme (BWBR0024282 – Wwft) the national government tries to combat money laundering and terrorism financing. To do so they impose several obligations on the entities involved. De Nederlandsche Bank, the Dutch National Bank, is jointly responsible with the Autoriteit Financiële Markten (AFM), Authority Financial Markets, for supervising compliance to these obligations ("Voorkomen van witwassen en terrorismefinanciering (Wwft)", n.d.), of which DNB specifically focuses on the compliance of virtual currency exchanges. The two core obligations are performing customer due diligence and the obligation of notifying suspicious transactions ("Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)", n.d.). Lastly, the Sanctiewet 1977 provides coercive instruments that can be used in response to violations of among other things international law or human rights (AFM, 2020). Sanctions that can be imposed are an order to freeze assets, a prohibition of making resources available to certain persons or organizations or a ban or restriction on the provision of financial services.

At the time of the Dutch implementation of the AMLD4 during most debate discussions talked about the implementation of the Ultimate Beneficial Ownership registry. Moreover, all agreed that tackling money laundering was important in combating crime and preventing the risking of the financial integrity of the economic system ("Kamerstukken II, 34808, 6 (NV)", 2018). During the last stage of the implementation process politicians for the first time refer to and talk about Bitcoin as a means of payment and the possible role of the currency in money laundering. At the time that this was noticed new legislation was in the pipeline of the European Union, but the AMLD4 did not yet cover virtual currencies.

In July 2019 the Dutch implementation of the 5th Anti-Money Laundering Directive started. In the process the Dutch legislation had to be altered in order to effectively transfer the European Directive towards the national legislation. The alterations can be found in the Wwft. There were three reasons for the implementation of the AMLD5. Namely, the emergence of technological services as alternatives to financial systems that were outside the scope of the current legislation, the increasing interdependence of organized crime and terrorism threatening the security of the Union and the desirability of better cooperation between competent authorities of Member States ("Kamerstukken II, 35245, 3 (MvT)", 2019). The directive ensures that only custodian wallet providers fall in the scope which entails that the provider can control the virtual currency of the user. According to the legislation customer due diligence needs to be performed which entails identifying the customers' identity based on documents or information from an independent source. Moreover, the relation needs to be assessed continuously and transactions need to be closely monitored. For all parties originating in countries outside the EU without an establishment in the EU there is a prohibition to offer services with virtual currencies in the Netherlands ("Kamerstukken II, 35245, 6 (NV)", 2019) and for all of them being able to operate in the Netherlands a registration is required.

In the Dutch implementation a licensing system was desired by parliament however the Raad van State, the advisory organ, advised against this as it was disproportionate ("Kamerstukken II, 35245, 4 (Advies RvS)", 2019). Thus, in the end exchanges and wallet providers only need to register at the Dutch National Bank. DNB is also the regulator. They can have three grounds for declining a registration request: the supply of incorrect data, the supply of incomplete data or when the ones in charge of day-to-day operations are not reliable or trustworthy ("Kamerstukken II, 35245, 6 (NV)", 2019). After the implementation all Dutch currency exchanges had up to six months to obtain their registration ("Kamerstukken II, 35245, 3 (MvT)", 2019). The providers of exchange services or wallets have to continuously set-up a user profile of their customer and based on this profile assess the risk or a transaction by identifying whether the transaction is different from the expected profile ("Kamerstukken II, 35245, 3 (MvT)", 2019, p.29). In this way the customer due diligence should be performed. It has to be noted that the Dutch government did not manage to transfer the AMLD5 in time into the national legislation. They only implemented the AMLD5 by May 20th which entailed that virtual currency exchanges had until November 20th to obtain their registration and comply to the new legislation.

Lastly, the 6th Anti-Money Laundering Directive was implemented June 8th 2020 by a governmental decree ("Staatsblad 2020, 163 (AMvB)", 2020). As the AMLD6 only further explains the legislation implemented earlier a decree could be adopted. The implementation states that Dutch criminal law is also applicable when you are guilty of money laundering according to article 3 and 4 of the directive and further establishes new categories of criminal offenses as predicate offenses to be considered. No new legislation concerning virtual currencies was implemented and thus transferred to the national legislation.

4.2. Landscape

This section looks at the landscape in which virtual currency exchanges operate. The landscape consists of government actors, law enforcement, virtual currency exchanges and other partnerships that together help in shaping the system.

4.2.1. National level

On the Dutch national level governance takes place in a top-down hierarchical structure. From a policy perspective two Ministries are responsible ("Kamerstukken II, 31477, 41 (Kamerbrief)", 2018), the Ministry of Finance and the Ministry of Justice and Safety. In the Dutch system the former tries to protect the integrity of the financial system, the latter fights crime and tries to prevent undermining. In the Wwft a double goal is apparent ("Kamerstukken II, 31477, 1-2 (Rapport)", 2007). The first goal of the Wwft is directly related to the purpose of the main responsible, namely the Ministry of Finance (Parlement.com, n.d.). The law is devised to prevent the occurrence of integrity breaches by financial institutions in order to prevent clients to use financial institutions in their money laundering regime. Secondly, a goal of the Wwft is to effectively detect and prosecute crime which is related to the objective of the Ministry of Justice and Safety (Rijksoverheid, n.d.).

The Wwft provides an overview of all different organisations having an obligation to notify when unusual transactions take place. Six regulatory authorities are appointed to monitor them. The Authority Financial Markets (AFM) monitors investment firms and financial service providers (AFM, n.d.). The presidents, local and national, of the Dutch Bar Association monitor several law firms (Nederlandse Orde van Advocaten, n.d.). The Bureau Financial Supervision (BFT) supervise notaries, bailiffs, several accountants and administrative offices (Bureau Financieel Toezicht, n.d.). The Bureau Supervision Wwft (BWft) monitors those involved in real estate

and rental agreements and appraisers and sellers and buyers of certain valuable goods (Belastingdienst, n.d.). The Dutch Gambling Authority (KA) supervises casinos and licensees for online gambling services (Kansspelautoriteit, n.d.). Lastly, the Dutch National Bank (DNB) provides prudential supervision of investment institutions, payment institutions, insurers, pension funds, banks and crypto service providers (DNB, n.d.). Prudential supervision entails that DNB monitors whether all parties on the financial markets adhere to their financial duties (AFM, n.d.).

The regulatory authority for virtual currency service providers is thus DNB. They monitor according to the Wwft custodian wallet providers and currency exchanges. DNB only monitors mainstream exchanges as these are the ones falling under legislation, these virtual currency exchanges obtained a registration at DNB. Shadow exchanges which are hidden and unknown to the authority cannot be monitored, as they are not registered at the regulator. The United Cooperation of Bitcoin Companies in the Netherlands (VBNL) serves the interests of those companies and tries to enhance the reputation and integrity of their members by focussing on self-regulation (VBNL, n.d.).

When an unusual transaction is detected a notification has to be made at the Dutch Financial Intelligence Unit (FIU-NL) (FIU-Nederland, n.d.-d). FIU falls under the Ministry of Justice and Safety and is part of the National Police, however they operate independently (FIU-Nederland, n.d.-c). With financial intelligence FIU-NL tries to prevent and combat crime, more specifically money laundering and the financing of terrorism, and secure the integrity of the financial system. Their main goal is to further investigate transactions in order to decide whether they are suspicious. Moreover, they try to enhance awareness at different organisations and spread the information found on suspicious transactions with other organisations, such as the Financial Intelligence and Investigation Service (FIOD) (FIU-Nederland, n.d.-c).

Next to obtaining information on suspicious transactions from FIU-NL, FIOD performs their own examinations into suspicious transactions in order to combat financial and tax fraud (FIOD, n.d.). FIOD is a subdivision of the Dutch tax authority, which belongs to the Ministry of Finance. Operations take place along three strategic objectives. They strive to investigate with effect, cooperate with the environment and take away the criminal assets (FIOD, 2019). FIOD contains several highly specialised teams. The Team Criminal Intelligence (TCI) is specialised in detecting and combating large-scale fraud and organized crime, such as money laundering. Moreover, the Financial Advanced Cyber Team focuses on online financial fraud (van Teeffelen, 2020).

The Anti-Money Laundering Centre (AMLC) possesses a unique role in the landscape as it is one of the few organisations in which supervising and detecting authorities and public as well as private parties cooperate (AMLC, n.d.). They strive to improve national and international anti-money laundering efforts (AMLC, 2021). Furthermore, they want to disseminate knowledge and expertise on money laundering within the chain.

4.2.2. Supranational level

Anti-money laundering regimes are heavily influenced by supranational governance. The European Committee (EC) has the right to initiative which entails that they are allowed to submit legislative proposals (Europa Nu, n.d.). They monitor whether European legislation is properly applied and is responsible for the financial budget (European Union, n.d.-a). The EC was responsible for the introduction of the different Anti-Money Laundering Directives. In order to implement the proposed legislation, the European Parliament and the Council of the European Union have to pass EU laws (European Union, n.d.-b). To do so they were accompanied by several expert committees helping them in the policy making process.

One of those expert groups is the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, also called MONEYVAL (MONEYVAL, n.d.-a). MONEYVAL is a permanent monitoring body of the Council of Europe. It is tasked with assessing the compliance to international standards of the anti-money laundering regime and the effectiveness of the implementation thereof (MONEYVAL, n.d.-b). They aim to improve the capabilities of national authorities in the countering of money laundering and terrorism financing.

On European Level another important governing body is the Joint Committee European Supervisory Authorities (ESA). It plays a role in being a forum of cooperation and it provides opportunities for the exchange of information of supervisory experiences and practises between regulatory authorities in relation to AML. They provide regulatory and supervisory input to the European Union (Joint Committee ESA, n.d.). They attempt to establish cross-sectoral consistency (Joint Committee ESA, 2016).

Another platform within the EU focussed on the exchange of information is the FIU platform. The platform helps nations in aligning the processes of implementation of new Directives, in this way enhancing cooperation (FIU-Nederland, n.d.-a). Moreover, between the different Financial Intelligence Units experiences can be shared.

Financial Intelligence Units globally can unity in the EGMONT Group. It is an international organisation in

which national Financial Intelligence Units cooperate to share intelligence in order to counter money laundering and to research and prevent the financing of terrorism (Egmont Group, n.d.). Currently, the EGMONT Group consists of 166 Financial Intelligence Units.

Lastly, the Financial Action Task Force is an independent intergovernmental organisation that develops international standards, that are continuously being improved, in the fight against money laundering (FATF, n.d.). The FATF consists of 39 members globally, all of them have to adhere to the 40 recommendations the organisation produced (FIU-Nederland, n.d.-b). One of them for example is the fact that financial institutions are obliged to perform Customer Due Diligence (FATF, 2020).

On a supranational level the Netherlands is being seen as a tax haven (Rooijendijk, 2020). Moreover, the Netherlands has a bad image when it comes to money laundering practices. The International Monetary Fund stated that the Netherlands is susceptible to money laundering risks due to the open structure of the financial system and the relatively large financial system and the amount of criminal proceeds in the system (International Monetary Fund, 2011), which could explain the negative image. Nevertheless, the Dutch government is very involved in the anti-money laundering bodies on international level. The Netherlands was one of the founders of the EGMONT Group showing their willingness to counter money laundering internationally. Furthermore, they are also committed to pursuing a European approach (Nu.nl, 2020).

4.3. Summary Chapter 4

Governance is here defined as the combination of legislation and the parties involved in the system. The legislation virtual currency exchanges have to adhere to is characterised and formed from several directives on EU level. The AMLD5 for the first time made sure that virtual currency exchanges also, next to other financial institutions, had to comply to the aml regulations. It encompassed requirements for a registration at a national authority and it imposed the duty to notify unusual transactions. In the coming years the legislation might change with MICA possibly providing harmonisation of the regulation throughout Europe. Nonetheless, the discussions on this have only started just now and before this will be implemented a couple more years will have passed by. On a landscape level the system is characterised by two Ministries who are responsible to counter money laundering and the policies related to it. Moreover several law enforcement agencies are involved. Also, the system is characterised by multiple private-public partnerships.

After having investigated the governance from a legislation and actor point of view sub question 1 can be answered *"What is the current state of governance in anti-money laundering in the virtual currency ecosystem?"*. The current state of governance in the ecosystem is focused on the image of virtual currency exchanges who are seen as gatekeepers. Due to this image they have the responsibility to identify unusual transactions before the funds can be mixed with the traditional financial system. The 5th Anti-Money Laundering Directive was transferred in Dutch legislation in the Wwft. Also, the Sanctiewet provided some important new requirements for the virtual currency exchanges. The implementation of the 5th Anti-Money Laundering Directive made sure that the exchanges had to obtain a registration at DNB, that they have the obligation to report unusual transactions and that they have to perform customer due diligence procedures and transaction monitoring. The Sanctiewet added a requirement of wallet verification. Moreover, governance in the system is characterised by a combination of public and private actors that together govern the system, in which DNB is the regulator of the virtual currency exchanges. The virtual currency exchanges have to report unusual transactions at FIU-NL.

5

Blockchain analysis

This chapter explores the transaction data of 17 virtual currency exchanges in the Netherlands, see chapter 3 for more information on how the exchanges were identified and the data collected. In section 5.1 the development of the transaction count is discussed. Next, section 5.2 delves into the transaction values. After that, section 5.3 looks at the origin and destination of transactions. Lastly, the found results are interpreted in section 5.4. Finally, the chapter will provide an answer to sub question 2 in section 5.5.

Throughout the whole chapter different timestamps are adopted in order to show the different moments in time in relation to the transaction data. As was seen in chapter 4, three dates are especially important for the implementation of the 5th Anti-Money Laundering Directive in the Netherlands. The presumed implementation of the AMLD5 relates to the date at which the legislation should have been incorporated in national legislation, January 10th 2020. Since this date was not met, the second timestamp shows the date at which the AMLD5 was actually implemented in the Dutch legislation, May 20th 2020. The last moment that is important to highlight is the moment when the virtual currency exchanges had to comply to the legislation and had to be registered, which was November 20th 2020.

Chainalysis provides the values for the transactions in USD which is why throughout the chapter USD values will be presented. Moreover, a difference will be presented between input and output transactions. Figure 5.1 shows the difference between the types of transactions. With input transactions the client sells bitcoins to the virtual currency exchange and obtains a different currency. For the output transactions the client buys bitcoins with a different currency. From the perspective of money laundering input transactions can be seen as those transactions where the origin was already disguised. Output transactions on the other hand are transactions where the money launderer tries to place the money in the virtual currency system in order to launder it using this system.

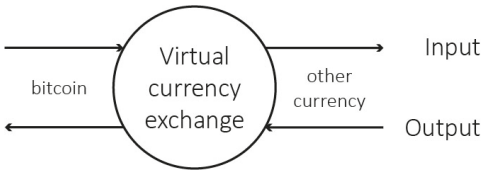


Figure 5.1: Input and output transactions

5.1. Transaction count

Figure 5.2 shows an overview of how the total number of transactions executed per month changes over time. The plot shows the count of the number of transactions at the virtual currency exchanges per month. Figure 5.3a shows the course of the input transactions. Figure 5.3b shows how the number of output transactions progresses over time. The figures show the development for registered exchanges, non-registered exchanges, an aggregate for all exchanges and the exchange rate. On the left y-axis the number of transactions per month can be explored. The right y-axis shows the exchange rate in USD/BTC. The x-axis shows the date.

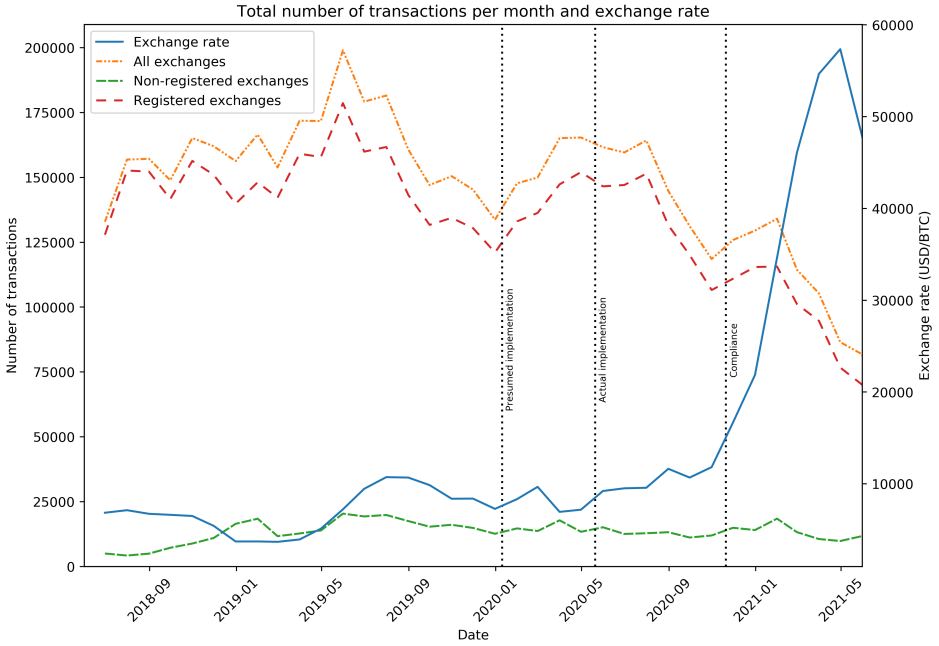
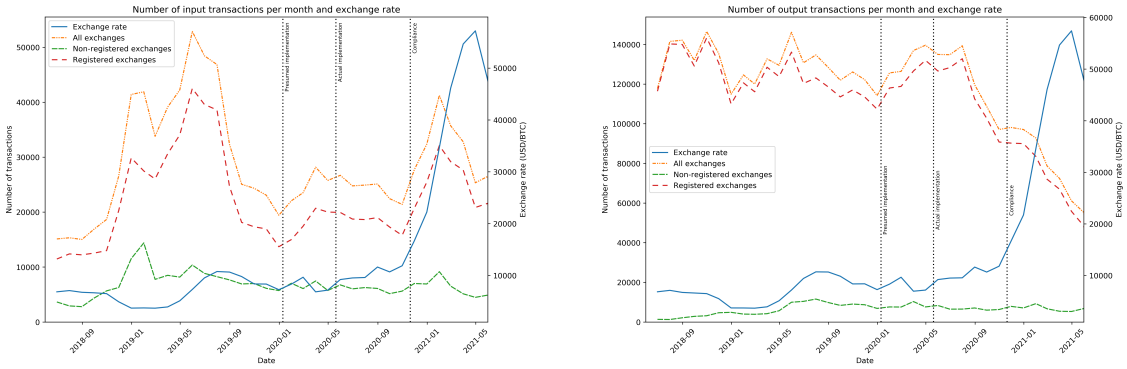


Figure 5.2: Total number of transactions per month

It can be observed that only a limited number of transactions is executed in the system. Moreover, it can be observed that registered exchanges have very fluctuating numbers of the amount of transactions they execute per month. The number of transactions executed at non-registered exchanges seems to show a more stable pattern. In the dataset more registered exchanges are included which provides a large influence on the pattern for all exchanges. Thus, the total number of transactions at all exchanges seems to decrease over time. The exchange rate calculated by the transaction data shows a huge exponential increase, as was also seen in the market (Investing.com, n.d.).

When looking at the character of the input versus output transaction flow, it is apparent that in both flows the non-registered exchanges portray a more stable pattern. The input transaction flows also show higher peaks and deeper valleys. Also, it can be observed that the exchanges execute more output transactions than input transactions. This means that people buy bitcoin more often than they convert it to a different currency. Moreover, the output transaction numbers have stabilized in a range of 110,000 and 140,000 transactions but have steadily decreased since June 2019.



(a) Input transactions per month

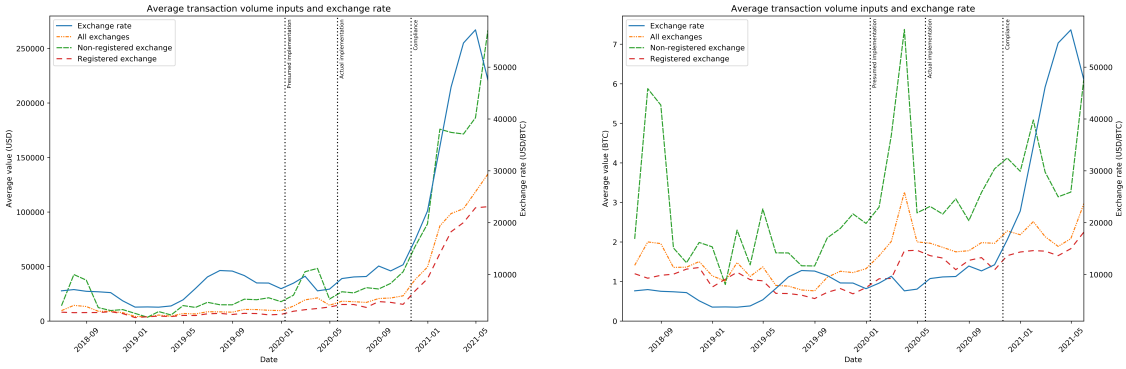
(b) Output transactions per month

Figure 5.3: Number of transactions

5.2. Transaction value

Virtual currency exchanges have to adhere to the objective indicator of reporting transactions over 10,000 Euro (FIU, n.d.), which is about 11,855 USD. As the transaction value is thus an important indicator of possible illegitimate transactions, it provides important insights into the system. Since the transaction value is dependent on the exchange rate, the USD Value as well as the BTC Value are investigated.

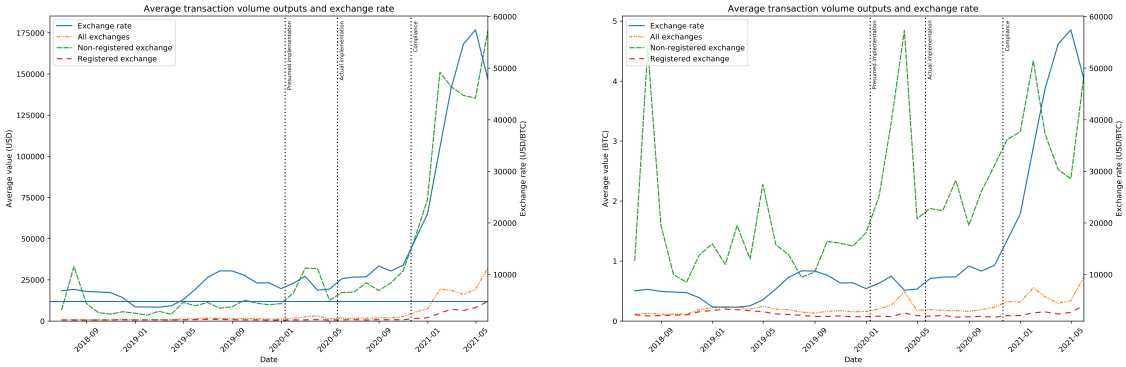
Figures 5.4a and 5.4b show the average transaction value of the inputs per month, where the first shows the USD value and the latter shows the BTC value. Figures 5.5a and 5.5b show the average transaction value of output transactions per month, the first shows the USD value and the latter shows the BTC value.



(a) USD Value

(b) BTC Value

Figure 5.4: Average transaction value inputs



(a) USD Value

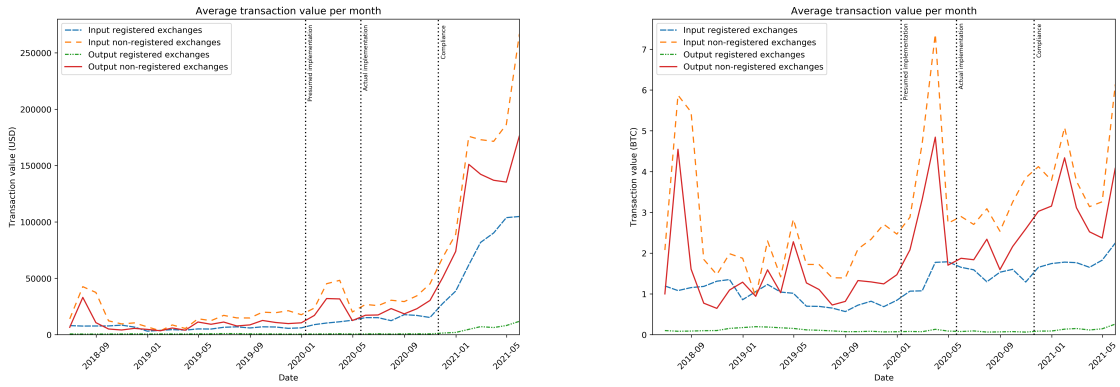
(b) BTC Value

Figure 5.5: Average transaction value outputs

The transaction values of input transactions changed over time. Until the introduction of the 5th Anti-Money Laundering Directive almost all of the average transaction values for all exchanges fell below the boundary value of 11,855 USD, which corresponds to the objective indicator of 10,000 Euro leading to a transaction having to be reported as an unusual transaction. At all exchanges the average transaction values seem to be increasing over time. In March 2020 a huge spike can be seen in the transaction value of input transactions at especially non-registered exchanges. The registered exchanges compared to the non-registered exchanges, seem to show a more stable pattern, whereas the non-registered exchanges exhibit a more volatile pattern.

For a long time the average transaction value is lower than 10,000 Euro for the output transaction values of all exchanges. The output transaction values at registered exchanges are very low. The non-registered exchanges also show that their transaction values are always higher than those at the registered exchanges. Moreover, the registered exchanges provide quite a stable pattern in transaction values while the transaction values at non-registered exchanges seem to change more often over time. The transaction values of output transactions also show a peak between the supposed introduction and the actual implementation of the AMLD5.

Figure 5.6a and 5.6b are showing the height of transaction values at the registered and non-registered exchanges for the different transaction flows in order to compare them to each other. Figure 5.6a portrays the USD value and figure 5.6b the BTC value. The y-axis provides the transaction value in the corresponding currency and the x-axis provides the date. In this way for all four transaction flows their progression throughout the time period that can be observed.



(a) USD Value

(b) BTC Value

Figure 5.6: Average transaction value per month

When comparing the different transaction flows to each other, three things can be observed. First, the non-registered exchanges have higher transaction values for input as well as output transactions. Moreover, the non-registered exchanges show more volatile behaviour than any of the transaction flows of registered exchanges. Lastly, all transaction values increase over time.

5.3. Origin and destination of transactions

The goal of the AMLD5 is to prevent integrity breaches by financial institutions in order to prevent the use of these institutions by money launderers. This entails that the institutions know who their customers are and based on that limit the risks that they are involved in anyone's laundering scheme by executing transaction monitoring in order to detect unusual transactions. This transaction monitoring also looks at the origin or destination of a transaction. This section first explores the overview of the development of the number of transactions and their origin and destination over time. After that, the difference in the portfolio of the virtual currency exchanges before and after the implementation is discussed.

The data collected through Chainalysis consisted of over 5 million transactions. For this section, only the subset is used that contained information on the cluster category. 80% of the data did not contain a counterparty cluster category. This entails that Chainalysis did not know whether these are loose transactions to private wallets or whether they are clusters that are still unidentified. This could be the case due to these addresses not having co-spent on transactions, meaning that no coherence could be found between addresses. For all analyses here, it thus needs to be taken into account that there are many more transactions made that did not belong to the identified service categories. The identified categories and their explanations can be found in table 5.1.

5.3.1. Origin and destination over time

To provide a clear overview all transactions of the remaining data have been plotted over time in order to investigate changes in the origin or destination of the transactions. Over the period of time the number of active virtual currency exchanges changes as some exchanges stopped operating due to the legislation and others started their operation halfway through the period. In order to enable a fair comparison over time the count of origin or destination of transactions is normalised. This is done by dividing by the number of active exchanges in the specific month. Thus, all values in the plots show the average number of transactions per month for one virtual currency exchange. On the y-axis the number of transactions can be found. On the x-axis the date is provided. The figures show a stacked plot in order to provide information on the origin or destination of the transactions that were executed.

As can be seen in figure 5.7 the category "exchange" is very dominant. Most of the transactions thus either go to or come from other exchanges. It was chosen to remove the categories "exchange", "other" and "unnamed

Table 5.1: Overview of counterparty cluster categories

Category	Description
Atm	A Bitcoin atm is an automated teller machine that allows the user to buy Bitcoin at a kiosk (bitcoin.com, n.d.). Some work bidirectionally enabling the user to also sell Bitcoin in order to obtain cash.
Child abuse material	Child abuse material relates to websites where one can purchase or sell access to child pornography (Sephton, 2020). It thus contains address related to these websites.
Darknet market	Darknet markets are dark web black markets where often illicit goods are sold and bought (Frankenfield, 2021).
Exchange	Exchanges provide services where virtual currencies can be exchanged for other currencies, virtual as well as fiat.
Fraud shop	Fraud shops sell services that help with committing different types of fraud, for example selling fake pictures with an id in hand to accompany Identity fraud (Chainalysis Team, 2021).
Gambling	Stands for all websites and services where users can gamble with crypto.
High risk exchange	Exchanges that according to the platform violate anti-money laundering and know your customer rules (Weeks, 2020).
High risk jurisdiction	Contains addresses linked to jurisdictions in which anti-money laundering and know your customer rules are violated.
Hosted wallet	Platforms that host wallets for their users, also called custodian wallet providers (Chainalysis Regulatory Team, 2020).
Illicit actor-org	Actors and organisations performing malicious activities.
Infrastructure as a service	A form of computing that provides pay on the go computing, network and storage resources (IBM Cloud Education, 6.
Merchant services	Merchant services providers allow conventional businesses to accept bitcoin from customers making purchases (Chainalysis Team, 2020a).
Mining pool	For every new block mined miners obtain a reward (Chainalysis Team, 2020b). This categories portrays addresses linked to this activity.
Mixing	These services mix together funds through a complicated series of transactions after which it is difficult to establish a correlation between the input of a user and the output (Crawford and Guan, 2020).
P2P exchange	A marketplace where people can trade directly with each other without a central entity functioning as a marketplace (Binance, n.d.).
Other	Clusters of services that do not fall into the other categories.
Ransomware	Addresses that are linked to a certain ransomware strand on which money has been deposited as ransom after access to certain systems were limited (Nationaal Cyber Security Centrum, n.d.).
Scam	Transactions related to ”a fraudulent or deceptive act or operation” (Merriam-Webster, n.d.) that were performed to obtain funds.
Stolen funds	Stolen funds can link to stolen funds from other exchanges or markets.
Terrorist financing	Addresses that were linked to the financing of terrorism.
Unnamed services	Identified clusters of which it is unknown what category they belong to as of yet.

service” from the plots. ”exchange” as it was overpowering the other categories making further exploration difficult. ”other” and ”unnamed service” were left out of consideration as it is unknown what services these clusters consist of. From here on thus in the analysis these categories have been removed from the data. The figures of the origin of the inputs at non-registered exchanges or the destination of outputs at registered as well as non-registered exchanges including these categories can be viewed in appendix B.

For all figures in this section the risky services are considered as these provide the most integrity risks and are used most often in money laundering schemes. Risky services as identified by Chainalysis in their 2021 Crypto Crime report are composed by the categories “P2P exchange”, “mixing services”, “high risk exchange” and “gambling”.

When clients want to sell their bitcoin and obtain a different currency, an input transaction, the bitcoin mostly finds it origin in merchant services, as can be seen in figure 5.8. However, a large part also comes from high risk exchanges, gambling and darknet markets. A large part of the number of transactions came from risky services. As over time the number of transactions changes the ratio compared to the other transactions is relevant to understand the effects. The share of these services of the total number of transactions increases slightly over time, but it has also decreased again.

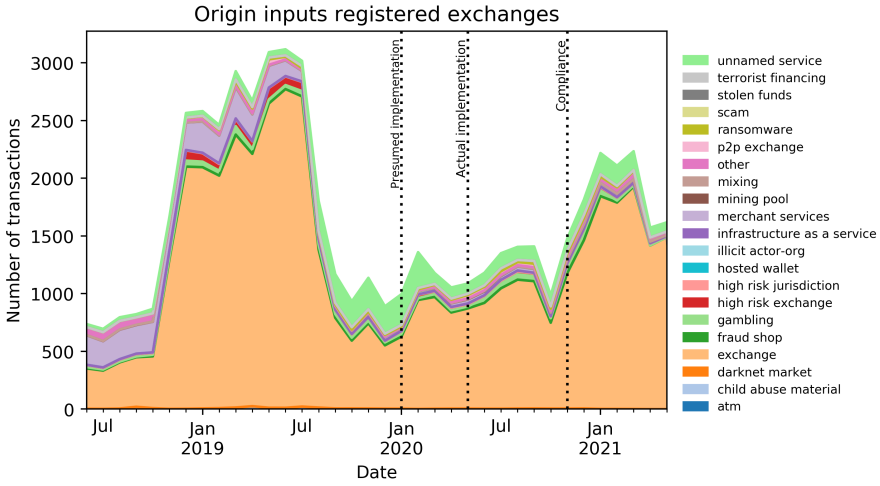


Figure 5.7: Registered inputs including all categories

If clients bought Bitcoin, an output transaction, they mostly transfer it towards p2p exchanges, which are decentralized exchanges without a financial institution intervening in an exchange. This can be observed in figure 5.9. Also for the output transactions quite some transactions find their destination in “high risk exchanges”, “gambling” and “darknet markets”. After the legislation was introduced there was a huge peak in transactions going towards p2p exchanges. The share of risky services increases over time due to this. But after this peak, the levels also stabilize again.

The pattern at the origin and destination of non-registered exchanges seems to show a similar pattern over time. Both figure 5.10 and 5.11 show that a large number of transactions either comes from or goes to risky services, especially towards high risk exchanges. However, the levels stay similar over time and do not seem to change.

From the evolution over time of the input and output transactions it can be observed that before and after implementation of the legislation for all categories not much changed on a relative basis. Therefore, looking at the different moments in time no large effects can be observed from the figures, only slight changes in the numbers of transactions that were executed.

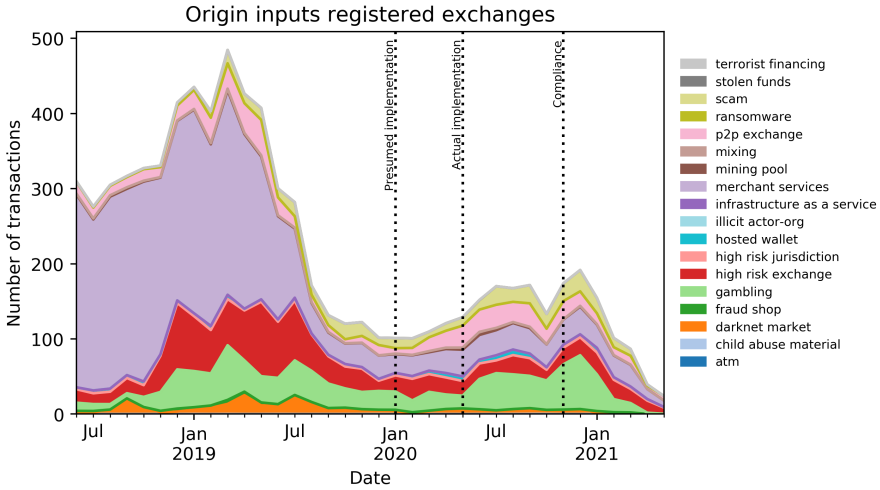


Figure 5.8: Origin transactions registered exchanges

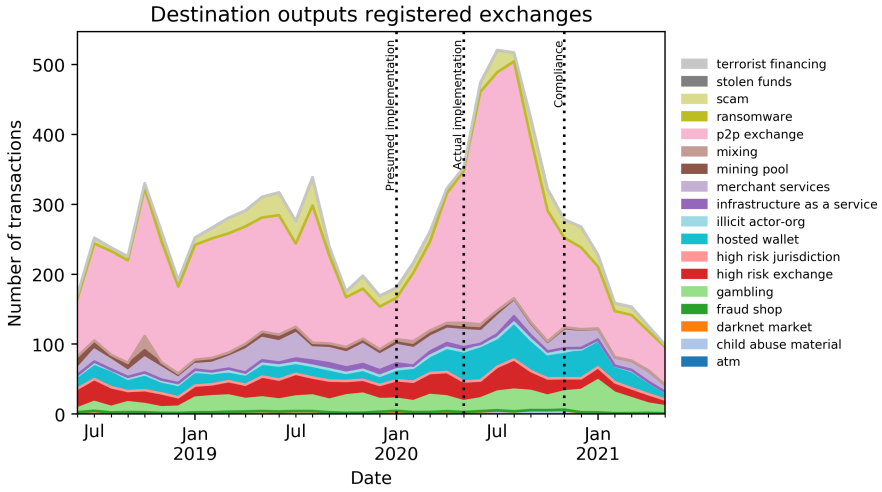


Figure 5.9: Destination transactions registered exchanges

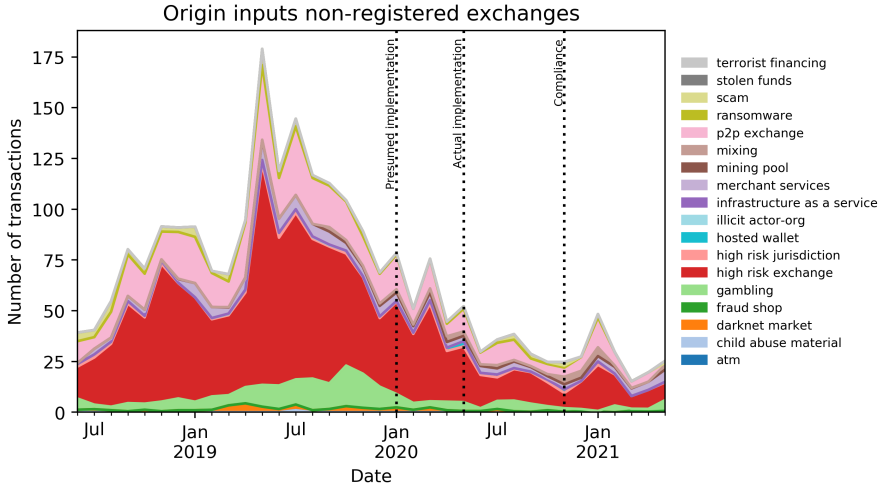


Figure 5.10: Origin transactions non-registered exchanges

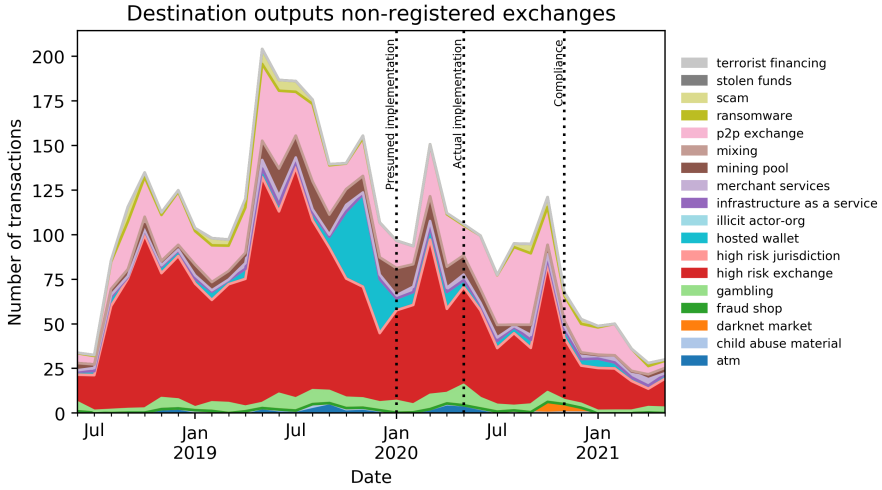


Figure 5.11: Destination transactions non-registered exchanges

5.3.2. Portfolio

To get a better idea of the relative importance of several categories in the portfolio of the input and output flows and how they change over time, a stacked plot is made of the percentages. To remove the skewness in the data, the data is first logged (Robbins, 2012). Next, the log values were transformed into the percentages of the portfolio in order to show the relative importance of different categories, the result can be found in figure 5.12. Important to note is that small changes get a higher significance due to the logging of the values. Therefore, only if major differences are found it can be stated that there is a difference in the portfolio of the transaction flows. May 20th is taken as the date to split the transaction data before and after the implementation of the legislation, as this is the moment in time when the implementation was made into the Dutch legislation.

The y-axis shows the percentage of the total number of transactions, in which the total number of transactions was logged. The x-axis shows what transaction flow the bar corresponds to and what exchange it belongs to. For all transaction flows, two moments in time are investigated. Bars stating “pre” refer to all transactions before May 20th. The bars stating “post” refer to all transactions executed after May 20th. The different colours portray the different categories of counterparties which were also observed earlier.

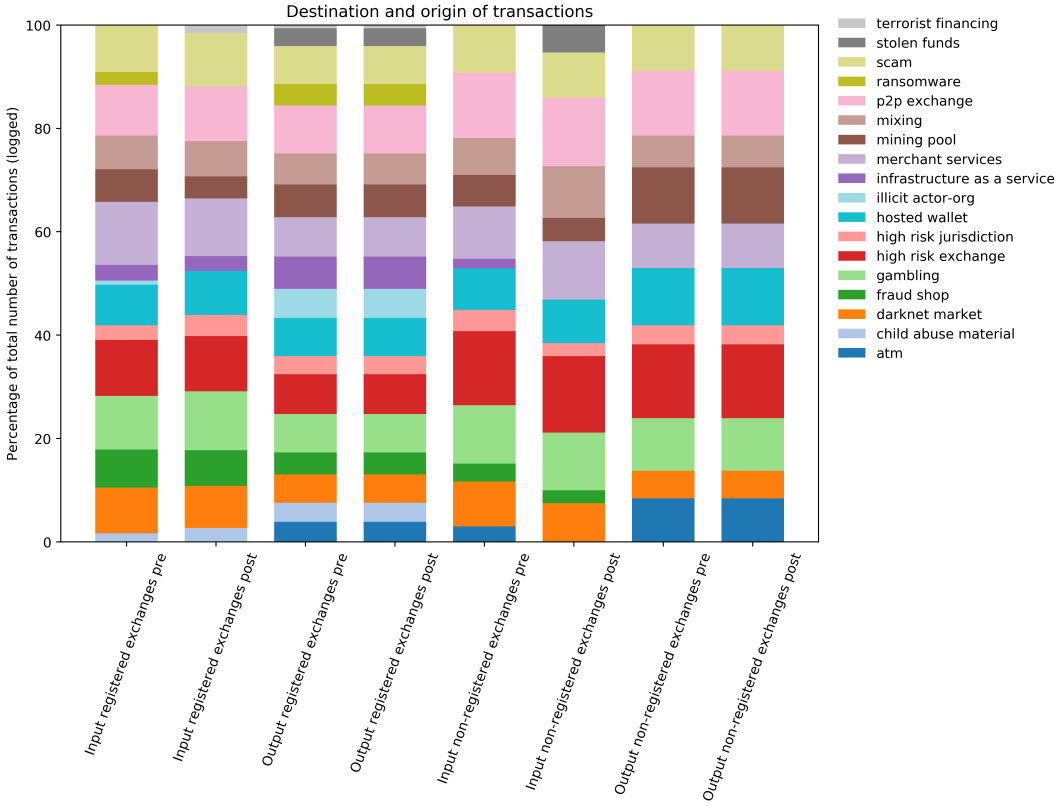


Figure 5.12: Overview exchanges before and after implementation

Looking at the input flow of registered exchanges before the legislation came into being, some differences can be observed, namely that ”ransomware” and ”illicit actor-org” had a bit more relevance before the introduction of the AMLD5. After, however, it seems that ”terrorist financing” is a bit more relevant. Nonetheless, the differences are very small and probably even smaller due to the data wrangling. Therefore, these differences are too small to provide a conclusion. The destination of the output transactions at registered exchanges did not change much before and after the legislation as well. The only difference seen is the fact that some transactions were identified as belonging to ”terrorist financing”, but again this difference is negligible.

For non-registered exchanges one thing that is apparent is that for both the input and output transactions after implementation some transactions seem to be linked to ”stolen funds”. For the input flow of transactions very slim decreases can be seen before and after the implementation of ”high risk jurisdiction” and ”infrastructure as a service”. For the output flow of transactions at non-registered exchanges, another observation is that after implementation of the legislation no transactions seem to fall in the category ”high risk jurisdiction”. The differences observed are also trivial for non-registered exchanges, meaning that the relative importance of the

counterparty categories stays the same.

Before and after the implementation of the 5th Anti-Money Laundering Directive the portfolio of virtual currency exchanges remained similar. Only some small changes were observed in the construction of the portfolio, but these were too small to provide relevant conclusions. In other words, the implementation did not lead to massive changes in where transactions came from or went to, regardless of looking at registered or non-registered exchanges.

5.4. Interpretation of results

For the observed results different explanations can be found. First, this section focuses on the effects of the legislation in place. After that, the influence of several system characteristics, namely the exchange rate and the bitcoin halving date, are discussed. Thirdly, the influence of the Covid-19 pandemic is considered. Finally, the influence or possible effects of criminality is reviewed.

5.4.1. Legislation

Multiple things are apparent when looking at the effects of the introduction of the 5th Anti-money laundering directive on the system of virtual currency exchanges. The first thing that is striking is the limited number of transactions that are influenced by the governance framework. Compared to the traditional financial sector only a minimal number of transactions are executed at the virtual currency exchanges. In May 2019, when the total number of transactions executed at virtual currency exchanges was around 200,000 transactions per month, see figure 5.2, 75.8 million transactions were executed per month with Pin or iDeal (CBS, 2021) . A whole governance framework has thus been set up which requires many organisations to put in place new extensive measures for only a very small fraction of transactions.

Figure 5.9 shows that around the time the AMLD5 should have been introduced in the Netherlands the number of transactions going to ”p2p exchanges” increased rapidly. These ”p2p exchanges” are exchanges where clients can directly trade with each other on their own terms without a financial institution functioning as a gatekeeper (Binance, n.d.). Possibly, in anticipation of the legislation people wanted to transfer their money to places that had less stringent measures in place as they felt uncertain what the precise effects would be of the legislation.

It was observed that the total number of transactions decreased, see figure 5.1. This could be due to the effects of the implementation of the 5th Anti-Money Laundering Directive. The decline started in June 2019 right after the legislation went into effect. On the one hand, the AMLD5 could have led to a deterioration in the competitive position of Dutch virtual currency exchanges. Due to more measures for clients they could have opted to trade at different exchanges outside of the Netherlands. Also, it could be the case that due to the measures that were put in place the virtual currency exchanges decided to execute less transactions as they found more unusual transactions or decided that some clients were too risky to get into a business relation with.

Moreover, the legislation could also have had an effect on the transaction volume. Especially at the input transaction flow of non-registered exchanges it can be observed that the volume stays around 10,000 Euro before the implementation of the legislation. After, it starts to increase. Possibly the registration led to more trust of virtual currency exchanges in their clients, as in order to register the client has to fully verify themselves. Ensuring that the virtual currency exchanges know who they are dealing with. A client will be put in a risk category during this process.After the introduction of the legislation it could be that due to this clients had higher payment limits as they all had to verify themselves. Therefore limiting the threat of being reported on the basis of the subjective indicator. In this way possibly, removing the necessity to split up larger transactions into smaller ones.

At the non-registered exchanges however a different pattern can be observed. After deciding not to register the non-registered exchanges decided to move to a different legislation to evade supervision or to quit their practise. This might provide the explanation for the increase in the transaction volume of both the input and output transactions, as observed in figure 5.4 and 5.5, as the non-registered exchanges did not have to adhere to the boundary value for notification of 10,000 Euro. However, peaks in the values at these exchanges are also observed in August 2018 showing the fact that the market is very volatile.

Furthermore, just before the implementation of the legislation, see figure 5.4 and 5.5, the transaction values decreased, which then increased after the legislation went into effect. As a decrease in the transaction values can also be observed at non-registered exchanges when the AMLD5 was supposedly introduced it could be stated that it is an effect of the implementation of the legislation.

Finally, the effect of the legislation on the origin or destination of transactions can be discussed. For registered exchanges the rate of risky services seems to slightly increase over time. The differences, however, at

registered exchanges and non-registered exchanges are very slim. The portfolio analysis, figure 5.12, even shows that the effects are negligible. It therefore seems that the legislation does not accomplish the goal and does not have the desired effect.

5.4.2. Bitcoin system

As bitcoin is often used in a speculative manner for trading or investing, the exchange rate is an important aspect of the system. First the decreasing number of transactions can be caused by an increase in the exchange rate. A high exchange rate means that an investor gets more USD for the BTC, which can make it attractive to trade. In 5.3a it can be observed that when the exchange rate increases the number of input transactions also increases. However, it can also be observed that after a small peak in the exchange rate in August 2020 the number of input transactions started to decrease. This could implicate that traders were holding on to their bitcoin, as less bitcoin was converted to USD. At the output transaction flow the opposite can be observed. A high exchange rate means it is more expensive to obtain bitcoin and thus less people will start buying bitcoin, this can be observed in figure 5.3b. Since more output transactions are made, this effect is larger and this causes the total number of transactions executed to decrease.

Moreover, when looking at the average transaction volume in figures 5.4 and 5.5 it seems to increase over time. At the same time the exchange rate increases. Possibly, the exchange rate could be the explanatory factor in this increase. Furthermore, a large peak value can be observed at the input and output transactions. This can be observed both at the registered as well as at the non-registered exchanges, see figure 5.6. The peak observed might have been caused by a change in the exchange rate leading it to become more attractive to buy crypto. As the demand becomes higher so does the price since there is only a limited number of the currency available. But the precise effect of the exchange rate is unknown.

Another important aspect of the system is the Bitcoin halving date. After roughly four years in the system the reward for Bitcoin miners is halved. This ensures that the rate at which new bitcoin is released in the system is halved (Conway, 2021). The last halving took place May 11th 2020. The known halving of the reward ensures that in anticipation of the halving the price of bitcoin starts to increase. Since the date can be roughly estimated investors may start to buy more bitcoin leading to an increase in the output flows leading up to the halving date. In other words, more people will buy bitcoin in anticipation of the block halving (Wuestenfeld, 2020). This effect can be observed in figure 5.3b.

5.4.3. Pandemic

In March 2020 the world was startled by a new crisis, the Covid-19 pandemic. Jabotinsky and Sarel (2020) researched the influence of the pandemic on the bitcoin market. They found that bitcoin becomes more appealing during a crisis as they bear some unique characteristics namely that their trade is not performed via a centralized institution and they are neither restricted or tied to a single jurisdiction. In a time of uncertainty in the policies of different countries this means that these currencies are independent of the policy shocks of individual countries, enhancing the appeal of the crypto market.

Seeing the total number of transactions decline could be due to the second half negative effects of the pandemic pointed out by Jabotinsky and Sarel(2020). First the cryptomarket is seen as a safe haven and money is transferred there as a panicking reaction. Then, however, after the dimensions of the crisis became clear investors took their money back to the traditional financial market. This can be observed as the number of output transactions first increases and then decreases, see figure 5.3b. Moreover, the number of input transactions first decreases, which entails that less money went back into the real world financial system. But after about half a year of crisis this started to increase again, see figure 5.3a.

Furthermore, figure 5.4 and 5.5 show a peak in the transaction volume. Jabotinsky and Sarel (2020) found a positive correlation between the transaction volume and the number of Corona cases. They state that the more threatening the pandemic became the higher the transaction volume was. Thus, the peak found in the graphs could show the effects of the Covid-19 pandemic as during April 2020 the pandemic was really threatening and people felt desperate due to the high number of corona cases.

5.4.4. Criminality

The numbers of transactions executed at non-registered exchanges seem very stable and not really affected by anything, see figure 5.1. This could imply that certain people will always use specifically these exchanges. Looking at it from a criminal viewpoint it can be stated that criminals will have a base level of transactions that they adopt. They will always go to exchanges where they know the measures are minimal. Thus, providing an argument for the fact that only those knowing about and needing these minimal measures will adopt the

non-registered exchanges.

For input and output transaction values a high volatility can be observed at non-registered exchanges, see figure 5.4 and 5.5. As they show a stable number of transactions executed it could possibly be due to criminals having different amounts of money to put into the system but this cannot be known from this analysis.

Lastly, one of the techniques adopted in money laundering is smurfing. Possibly less smurfing took place as the number of transactions decreased but the transaction values increased. This could implicate that the exchanges were used less often in money laundering practises.

5.5. Summary Chapter 5

In this chapter a blockchain analysis was provided on three aspects of the transaction data. First, the number of transactions was observed. It was seen that the total number of transactions started to decrease after the introduction and implementation of the AMLD5. It was further found that the average transaction value at registered exchanges did not seem to be altered affected by the introduction of the legislation. Finally, the origin and destination of the transactions were explored. It was seen that over time the formation of the portfolio of transactions did not change. Many explanations can provide insights into the reasons for these observations based on the legislation in place, several bitcoin system characteristics, the occurring pandemic and possible effects of criminality. However it is uncertain whether these effects are caused by the implementation of the 5th Anti-Money Laundering Directive.

With this information sub question 2 can be answered. *"What changes in transaction behaviour surrounding Dutch virtual currency exchanges can be observed from the blockchain after the implementation of the AMLD5?"* From the blockchain transactions it can be observed that less transactions were made after the implementation. The average transaction value went up at all exchanges. Therefore, it looks as if less smurfing took place. But, the implementation of the legislation made no difference in ensuring less transactions were made with services with a questionable origin. It is therefore questionable how effective the legislation has been in tackling the criminal transactions.

6

Perspectives on the AMLD5

The goal of the interviews held was two-fold. On the one hand, for virtual currency exchanges it was attempted to understand how virtual currency exchanges have adapted their day-to-day operations in order to comply to the duty to report and KYC procedures arising from the AMLD5. On the other hand, it was tried to find out how supervision in the ecosystem is carried out by the regulators in practice. It was chosen to focus on the virtual currency exchanges and the supervising authority as these are the main players involved in the system. The process started by setting up an interview protocol based on the goals of the interviews and the literature gathered. The interview protocols can be found in appendices C and D. An overview of the respondents can be found in section 3.2.3.

First, the use of virtual currencies in money laundering is discussed in section 6.1. Next, the anti-money laundering responsibilities of the parties will be set out in section 6.2. After that, section 6.3 explicates the perspectives on the introduction of the 5th Anti-Money Laundering Directive. Section 6.4 then delves into the monitoring process adopted by the virtual currency exchanges. After that, section 6.5 investigates the registration process and supervision in the system. An outlook on the future is given in section 6.6. Finally, in section 6.7 sub question 3 is answered.

6.1. Adoption of virtual currencies in money laundering

"We do see money laundering as risks that we must mitigate" – respondent 2

All respondents acknowledged that money laundering is a risk of cryptocurrencies. Respondent 2, 3 and 5a even mentioned that the potential of adopting cryptocurrencies in money laundering regimes is quite large. It was mentioned by respondent 1a that the risks are larger when considering privacy coins, which are coins on which no blockchain analysis can be performed. Several respondents identified that this is caused by several characteristics of the system. According to respondent 1b, the properties that facilitate anonymity play an important role here. This was also mentioned in research by De Vido (2019), Limba et al. (2019), Stokes (2012) and Tropina (2014). Moreover, the intractability of transactions due to this (pseudo) anonymity of the currencies was mentioned by two respondents, namely respondent 1b and respondent 3. Another risk posed by the character of the system is the fact that it is decentralized. "You can create an address yourself without having to identify yourself of verify your identity" (according to respondent 1a). This means that no financial institution can upfront prevent a client with possible money laundering objectives from entering the financial system. Furthermore, Tropina (2014) already highlighted that the speed and ease of transactions form one of the risks of the system for money laundering. Respondent 4 stated that linked to this characteristic it is important to keep in mind that the crypto system goes on 24/7. This entails that money launderers do not have to wait until business hours but can immediately execute their plans.

"As a potential it is an extra layering that you can add." - respondent 4

All in all, as was seen in the literature the characteristics of the system lead to a higher chance of money laundering with virtual currencies. On top of that, two functional advantages of using virtual currencies in money laundering can be identified. Custers et al. (2019) and Limba et al. (2019) showed that several services can be

adopted to easily transfer money through the system, which is part of the layering step. These services can for example be mixers or tumblers. Respondent 1b stated that the easy transfer of money around the system is one of the functional advantages of the adoption of virtual currencies. Moreover, respondent 4 mentioned that virtual currencies are an extra currency or layer that can be adopted in money laundering, making it possible to set up a more extensive laundering scheme.

"It is still the case that on the basis of blockchain analysis quite a lot can be found out. So at this point I would say cash is much riskier." - respondent 3

Despite these advantages the respondents showed one important barrier for the adoption of virtual currencies to launder money. Respondents 1a, 3 and 5a identified that the blockchain can easily be employed during the investigation of unusual transactions. Already in 2016 Meiklejohn et al. showed how transactions can be traced throughout the blockchain. Respondent 3 and 5a stated that due to this reason cash might still be more appropriate to be used. Although, in the National Risk Assessment 2019 (van der Veen and Heuts, 2020) it is stated that the potential impact of money laundering via cash is limited.

6.2. Anti-money laundering responsibilities

"We make a preventive contribution, we try to ensure that the threshold for money laundering is as high as possible" - respondent 1a

The two parties of respondents provided a clear overview of the role they envision for themselves within the virtual currency ecosystem. On the one hand, the regulator emphasized their role as being the regulatory authority. Respondent 1a stated that they want to make a preventive contribution by investigating to what extent institutions comply to the law and monitoring them so they can properly perform their gatekeeper function. Respondent 1b added that they are not an advisor to the parties in the system, however, they do want to clarify the requirements that the legislator has. The regulator sees themselves as being supportive both for the virtual currency exchanges as well as for the legislator as they are an executive organization in the ecosystem.

"We like to see ourselves as a sparring partner." - respondent 2

When asked about their role in the virtual currency ecosystem, respondent 4 firmly responded they were the gatekeeper of the system as this was established in the policy documents, respondent 5a agreed to this role. Respondent 2 mentioned that they *"like to see [themselves] as a sparring partner for the government and the Ministry of Finance, but also with other stakeholders: banks, payment service providers and certainly the investigative services"*. Also, on the field of supervision it was mentioned that the virtual currency exchanges want *"to stand next to the regulator and not across from them"* (respondent 5a). Respondent 5b stated that the virtual currency exchanges have an intrinsic motivation to do things differently than the traditional financial sector. Therefore, they want to show how good of an alternative cryptocurrencies are for the traditional system. In order to do so respondent 3 mentioned that they want to prevent themselves from purely being associated with crime and money laundering. Virtual currency exchanges thus see themselves as being an important actor with regards to money laundering. They want to act in order to counter money laundering by taking measures to execute their gatekeeper function but also by being a partner to cooperate with in order to enhance the system.

"We were already doing what is now expected from us before the Wwft and AMLD5" – respondent 4

All virtual currency exchanges mentioned that almost all of the requirements that have been put in place by the implementation of the 5th Anti-Money Laundering Directive were already in place before the directive went into force. The requirements mentioned here, refer to the measures of customer due diligence and transaction monitoring. All respondents are part of VBNL which has a code of conduct stating that these measures should be in place (respondent 2). On top of that, respondents 3 and 4 mentioned that when they started their business it was hard to obtain a bank account since the financial institutions wanted to minimize their integrity risks, in this way compelling them indirectly to put in place these measures. Measures that the virtual currency exchanges already put in place were that no cash was allowed, strict payment limits, the identification of customers and (video) verification. Respondent 3 mentioned that *"[they] also went much further than what was expected from [them]"*. Taking these extra steps and taking into account the fact that these measures were in place long before

regulation was established shows the intrinsic motivation of the virtual currency exchanges.

The virtual currency exchange provide a large emphasis on their role in AML whilst the regulator merely states that they contribute in executing the legislation, they do not share the same amount of feeling of responsibility. It is important to note that due to their roles there is no shared responsibility according to the legislation. However, proper anti-money laundering can only take place through proper cooperation. This difference in feelings of responsibility could threaten proper cooperation, although both parties do observe this as being essential. The responsibility of executing money laundering countering measures lies purely at the virtual currency exchanges. Despite that, both feel responsible in the system. The large feeling of responsibility of virtual currency exchange in countering money laundering can also be observed in the fact that they already had many measures in place before the directive.

6.3. Introduction of the 5th Anti-Money Laundering Directive

"The question is not how we view this, because we simply have an order from the legislator." - respondent 1a

When the regulator was asked about their perspective on the implementation of the regulation it was stated that their perspective is irrelevant since they are not the ones implementing the regulation or having to adhere to the regulation. Respondent 1b especially pointed to the fact that the regulator simply executes the mandate they have. Despite that, they acknowledged that the law was introduced very quickly (respondent 1b), while it has extensive consequences for several companies. In chapter 5 it was observed that the total number of transactions executed decreased. It could be that due to this rapid introduction several negative effects were unforeseen such as the possible deterioration of the competitive position due to higher barriers, seen in this decrease of the number of transactions.

"We were actually not surprised that the legislation was coming. We have been preparing ourselves to confirm to the Wwft since 2016/2017" – respondent 5a

On the other hand, respondent 3 and 5a mentioned that the virtual currency exchanges were not surprised by the introduction of the legislation. Respondent 5a stated *"it was clear to us that we were trading a financial product and that legislation was inevitable"*. It shows that the sector itself saw how their sector was similar to the traditional financial system and that they were awaiting the regulation. In contrast to the regulatory authority, the virtual currency exchanges are very opinionated on the introduction of the legislation. Respondent 3 stressed the negative effects of the legislation on innovation in the Netherlands, as he believes that due to the high barriers many small firms do not have the opportunity to execute their ideas. However, all other respondents highlighted that the introduction of legislation is a positive development. Respondent 4 and 5a stated that the legislation leads to a professionalization of the market. According to respondent 2 it brings more clarity and transparency to the market and they are pleased to finally be able to report unusual transactions.

Despite most of the virtual currency exchanges identifying the introduction of the legislation as a positive development, the parties also provide some criticisms on the legislation. Respondent 5a felt that this is caused by having only a limited dialogue with the sector. Due to the legislator not fully understanding the system they are regulating, the legislation does not completely fit the system. Moreover, the fact that an old set of rules is imposed on a new system aggravates this effect. Respondent 5a stated *"We are working with a new piece of technology that is inherently different from the traditional system"*. Therefore, no full connection can be seen between the legislation and the system.

"Yes, there are exchanges operating in the Netherlands without registration, I think quite a lot even." - respondent 5a

De Vido (2020) mentioned, before the legislation went into effect, that the fact that the global character of the system was not considered would provide some difficulties. Respondent 2 and 5b also mentioned that this is one of the causes of the difficulties. Furthermore, De Vido (2019) stated in advance that the legislation provided a difficulty with the territoriality of the legislation. Now that the legislation is into effect this difficulty is encountered. Respondent 2 stated that especially deciding when an exchange is actively operating in the Netherlands is difficult in light of the definition of freedom of service provision in the European Union. Due to this difficulty virtual currency exchanges exist that are active in the Netherlands but not registered at the Dutch National Bank

"But of course the case is that it is a new sector that still has to get used to these new criteria" - respondent 1b

The regulator, however, did not stress the difficulties with the legislation. Respondent 1b stated that it is still a challenge for the sector to adjust to the new criteria. He mentioned that the difficulty for the virtual currency exchanges lies in classifying themselves in one of the boxes of the legal framework but the regulator does not see the boxes itself, the regulatory framework, as a difficulty. All in all, the virtual currency exchanges thus pointed out the difficulties that the legislation imposes on them, which, when looking at the literature, could have been foreseen. Whereas the regulator stated that the exchanges simply have to get used to the new legal framework they have to adhere to.

"We no longer do the conversion between euro and bitcoin. Which means you no longer fall under the supervision of the Dutch bank." - respondent 3

Many different effects can be observed in the organizations of virtual currency exchanges. However, there were huge differences between the organizations. Respondent 3 stated that they no longer perform the conversion between BTC and Euro, in this way they do not have to adhere to the legislation anymore. Other virtual currency exchanges changed their operations in such a way that they complied to the legislation. All respondents mentioned that they had to take a deep dive into the legislation in order to understand what they had to change. Respondent 2 stated that they merely had to further record their procedures and processes. Moreover, due to the obligation to report unusual transactions to FIU-NL the virtual currency exchanges had to ensure that the reports would give clear reasoning for identification of the unusual transaction. For this the reporting functionality had to be developed but respondent 2 and 4 mentioned also the process of identifying transactions had to be further recorded. Another functionality that had to be developed was the wallet verification functionality, although the judge ruled that DNB should provide more information on why this functionality had to be implemented ("ECLI:NL:RBROT:2021:2968", 2021). Respondent 5a stated on the wallet verification measure that *"a citizen who simply has good intentions and who does nothing wrong, faces really high barriers, while a malicious person can easily get around that"*. Due to these changes operational processes and training for staff had to be changed. Furthermore, respondent 4 stated that more staff had to be hired in order to comply to the separation of functions. Respondent 3 stated that another large effect on the organisation is that the registered parties are now very busy with answering the information requests by the regulator. It seems that the effects on the organisation took place on an administrative level in such a way that processes had to be recorded and information requests answered. However, no new measures were taken to counter money laundering outside of the wallet verification procedures, especially considering the controversy of this measure.

"We have heard some mentioning from parties who have left abroad." - respondent 1a

Next to many effects being identified on the organisations, also large effects are visible in the virtual currency exchange landscape. First, Dutch parties have to spent enormous amounts of money on supervision costs, according to respondent 3 and 4. The virtual currency exchanges have to pay for their supervision themselves (Schnezler, 2020). Due to the height of these costs the regulator and the virtual currency exchanges see that some parties have moved abroad or stopped or altered their operations. Another reason for this, according to respondent 5a, is the fact that some companies were simply too little so they could not uphold a segregation of functions. Respondent 3 mentioned that the high supervision costs is bad for the competition of Dutch companies. This effect was also observed by respondent 5a since Dutch customers can simply buy crypto at a different company abroad where the barriers are lower than they are in the Netherlands. In the landscape companies, thus, either stopped providing their services, moved abroad or they have larger barriers which could lead them to become less attractive to customers.

6.4. Monitoring process

"CDD is the entire customer due diligence package. That is the identification of the customer: who is your customer. But also the verification of your customer: is the person you are talking to really the person who he says it is " - respondent 2

When asked about the monitoring process of the virtual currency exchanges it was observed that the process falls into two steps namely the onboarding and the ongoing transaction monitoring. Customer Due Diligence

(CDD) and Enhanced Due Diligence (EDD) are both part of the onboarding procedure respondent 2 mentioned. CDD merely consists of the identification and verification of the client. Respondent 4 mentioned that for this Onfido can be used which takes out fake IDs. Respondent 2 explained that EDD consists of performing extra checks when risk flags pop up. Respondent 5 stated that during the onboarding process they ask proof of address, phone numbers and IDs. They also check the names registered on the IBAN account and compare them with what was entered in the system. All in all, these different onboarding procedures ensure that the virtual currency exchanges upfront make a risk estimate of who they are starting a business relationship with. They can, based on all the information asked upfront, decide what risk profile a client falls into. Moreover, respondent 2 elaborated that every year a full customer profile review takes place in order to ensure that the data remains up to date. The virtual currency exchanges all state that they have these measures in place which is what is required from them in the Wwft.

"We use all the information we ask for at the front to check whether we know enough about the customer to let the order take place." - respondent 5b

During the ongoing transaction monitoring process continuously unusual transactions are being identified. The regulator mentioned that they know that transaction monitoring tools exist, however they also state that they are not an expert on the specifics of each individual provider of monitoring software (respondent 1a). All respondents from virtual currency exchanges mentioned that both manual and automated blockchain analysis software is adopted. Respondent 2 stated that they adopt risk flags, they pop up based on several properties. When they come up extra inspections have to be performed to see if a transaction is unusual. The risk flags are especially adopted in applying the subjective indicators. Respondent 5b commented that they compare the transaction behaviour to what they know about a client upfront. This shows why especially the onboarding procedure is so important. Respondent 4 and 5a stated that taint analysis is not yet fully formalized and implemented. This entails looking at whether the cryptocurrency was somewhere linked to for example darknet markets. However, transaction monitoring is a continuously developing process at the developer of the blockchain analysis software as well as at the virtual currency exchange. It seems that currently blockchain analysis software is the main tool adopted by all virtual currency exchanges, however the organizations adopt different extra tools to complement this tool.

The next step in the process is making a report at the FIU-NL. The crypto sector has to do this by uploading a XML file. Respondent 2 stated that after making a report they get a confirmation. Respondent 5a mentioned that sometimes general feedback is provided on the reports however that no standard feedback is given on individual reports. The consequence of this is that it is unknown whether reports are made on actual suspicious transactions. After having made a report at FIU-NL the virtual currency exchanges can then block a customer or ask further questions to understand why the transaction was made, according to respondent 5a.

6.5. Registration and supervision

"There is not 1 sector but there are very different companies. It is very important for each business model to see what risks are associated with this." – respondent 1b

The registration process started, according to the regulator, by them sending out a call to gather all parties interested in obtaining a registration, this was done in September 2019. In the process they tried to provide as much information as possible in advance in order to prepare the companies as good as possible. *"More than half ultimately did not proceed with their application"* according to respondent 1b. However, the regulator showed that they have registered 21 parties. They are pleased that they have been able to register 21 parties this far, especially keeping in mind that just over a year and a month ago there were no parties registered. The regulator explained that the legislation consists of many open standards for which the companies themselves have to decide how they are going to fill these in and take measures on them. Moreover, the risks per company are different due to the different business models. Respondent 1a mentioned that the companies were thus required to make an analysis of these risks. Next, respondent 1b further elaborated that they had to be convinced that the measures put in place were effective in order for them to hand out the registration. It seems that the regulator tried to support the companies to the best of their ability during the registration process.

"It was not simply an excel sheet at DNB where a few ticks would be put next to your name" – respondent 3

The virtual currency exchanges showed a different apprehension of the registration process. Respondent 4 mentioned that the application process itself was easy. However he also mentioned the process was a lot of work. Respondent 2 and 3 mentioned that they had to upload about 15-20 different documents containing the Systematic Integrity Risk Assessment (SIRA), of which the necessity was also pointed out by the regulator, but also documents on the directors of the companies. On top of the registration process being a lot of work, it was also experienced negatively by the virtual currency exchanges it was described as being "turbulent" (respondent 4), messy and not very nice (respondent 5b). One reason for this was that only halfway through the process the wallet verification was mentioned. Respondent 5a explained that the consequence for their organization was that the whole focus was shifted towards developing this functionality.

"It did not feel right to handover everything we earned to DNB" - respondent 3.

Another point of agitation arose when two weeks before the end of the registration procedure the supervision costs were mentioned, as set out by respondent 3. Respondent 5a stated that they were told the costs would be around 1.7 million Euro which would be divided by 50-75 parties. However, the result of having only 21 parties registered meant that the costs had to be divided over less parties. Respondent 5a further elaborated that the total supervision costs became somewhere between 2.2 and 2.5 million Euro. Respondent 3 described that the high costs for supervision are the main reason for them to quit operating.

It is striking that the largest difference in opinion of the virtual currency exchanges and the regulator is on the amount of exchanges that got registered. Whereas the virtual currency exchanges see that many dropped out, the regulator is pleased that 21 companies were eligible for registration and sees it as an achievement that 21 parties were registered. The parties do not seem to share open communication on this topic or much incomprehension between the parties exists.

"We conduct risk-based supervision, which means that we want to deploy our resources and supervision where the risks are greatest" – respondent 1a

The regulator stated that they publish a questionnaire where they try gather information on the risks and the scope of activities of the different companies. They also want to obtain more information on what measures are in place. Based on this questionnaire the regulator performs thematic research at certain companies. Moreover, respondent 1a stated that this form is a sort of risk-based supervision which ensures that they can use the resources they have as effectively as possible.

"We have just completed the questionnaire for DNB that started in April. I have never had so many questions in my life. Not even compared to the bank where I worked before." – respondent 4

Respondent 3 and 4 provided a critical perspective on the supervision since they pointed out that the process was presented as being simply a registration, however practise shows that it is much more than that. They feel that sometimes even more is required than would be in a licensing regime. Respondent 2, 3 and 4 also stated that the main form in which supervision takes place is through the DNB questionnaire. They stressed the enormous workload that comes along with this form of supervision. Respondent 3 mentioned *"those are not things that you just write down in half an hour. For this the compliance officer really spends hours or even weeks to get that done"*. Moreover, respondent 4 stated that the regulator does not fully comprehend the complex system they are supervising as they feel that they are the ones having to answer questions which merely explain the system basics in the questionnaire. Another form of supervision mentioned is the fact that DNB can come by for an onsite visit. Respondent 5a mentioned that *"Due to the attitude they adopt we experience a certain sense of mistrust towards the sector and the institutions"*.

Amongst the virtual currency exchanges there is much dissatisfaction on the supervision. On the one hand, the fact that the whole process was presented as merely a registration was already a bitter pill to swallow. Especially, seeing that the workload accompanying the supervision of the virtual currency exchanges for them is though. Moreover, dissatisfaction arises by the virtual currency exchanges feeling that the regulator does not understand what they are dealing with whilst they are paying exorbitantly high costs for this supervision. Due to all of this the virtual currency exchanges feel a sense of mistrust towards the sector. The regulator on the other hand merely executed their mandate.

6.6. Outlook on the future

"The EU legislation will probably ensure that crypto services are subject to broader supervision, not only for money laundering" – respondent 1a

On a European level currently new legislation is being worked on, MiCA, this will probably provide new tools for the regulator, according to respondent 1a. The regulator mentioned that in order to get a grip on money laundering with cryptocurrencies it is vital that regulation is established internationally, keeping legislation on a national level will not be effective, mentioned respondent 1b. Respondent 2 stated *"We are also looking forward to MiCA in that regard. Because MiCA's objective is to bring the regulations more evenly at EU level"*. Respondent 5a and 5b also stated that they are looking forward to this new legislation as it provides harmonization in the EU which will lead to more clarity for the clients. However, respondent 5b mentioned that still the legislation allows for pigeonholing, meaning that still focus is put on adopting existing legislation for the traditional financial system.

Both the regulator and the exchanges look forward to the new legislation on EU level as they both identify harmonization of EU legislation as being essential for effective anti-money laundering. The virtual currency exchanges however are concerned with the pigeonholed thinking that the new legislation might encompass.

"Bitcoin will always remain the largest and the most important. Criminals will probably not deviate from it" – respondent 4

Respondent 2 mentioned that when thinking about future developments of coins that will be adopted probably a distinction will arise between coins on which blockchain analysis is possible and those on which that is not possible, privacy coins. Respondent 3 and 5a also mentioned that probably criminals will find that the privacy coins become more and more difficult to use due to the more aggressive stance that regulators will take on privacy coins. This can lead them to again opt for bitcoin, which can be highly valuable for investigative services. Meanwhile, the Bitcoin community is focusing on having a higher transactions throughput but due to these developments the system might become more anonymous, according to respondent 3. This could also enhance the attractiveness of bitcoin. Thus, both the regulator as well as the virtual currency exchanges see the potential of bitcoin remaining a tool for money laundering regimes.

When looking at the development of tools in the system respondent 2 mentioned that there are currently many opportunities for the development onboarding tools. *"Compliance is also just a service"* according to respondent 2. Over the years, virtual currency exchanges are thus likely to hand over more of their onboarding procedures to external services. Moreover, the exchanges will become more reliant on what customers tell them about their money instead of what can be seen in the blockchain, as the effectiveness of blockchain analysis tools might start to diminish over the years according to respondent 3. Moreover, respondent 5a stated that interweaving will probably more often take place between systems that are really developed for the crypto sector and systems that have been developed for the traditional sector.

The fact that the crypto sector is moving more towards the traditional financial sector is also observed by respondent 2. He mentioned that the traditional financial sector is also becoming more and more interested in crypto. However, respondent 4 stated that two sectors can be observed. On the one hand, the blockchain projects that provide decentralized developments. On the other hand, the legal side consisting of legislation and the regulators who have responsibilities to ensure financial stability and fair markets. Each of them moves in their own direction, one becoming more anonymous and the other more strict and regular like the financial world. There will thus arise some friction. All in all, the virtual currency exchanges do not fully agree on how the sector will develop over the coming years. One thing that respondent 5a hopes is that the regulators will cooperate better in the field of crypto and gain more knowledge on the system.

The virtual currency exchanges have many ideas on what the system needs in order to get better, showing that they are still hopeful that the virtual currency ecosystem and regulation of it can improve. Respondent 2 mentioned that partnerships are extremely important in which the virtual currency exchanges can play a major role to learn from each other and help prevent fraud. To do this effectively, knowledge sharing between actors will become key. Respondent 5a stated that the crypto industry would love to sit at the table to actively think along. During this meeting respondent 5b wants to discuss the system of objective indicators and explain how the characteristics of the crypto system differ from those of the traditional financial system. The virtual currency exchanges have also some desires of the government. Respondent 5b stated that they would appreciate the government to contribute ideas on optimizing identification documents or other instruments to ensure that remote onboarding becomes easier, and thus the costs for supervision can be reduced. Lastly, respondent 4

mentioned that they would welcome an improved feedback loop from FIU-NL so they can further strengthen their unusual transaction detection systems.

6.7. Summary Chapter 6

This chapter showed that virtual currency exchanges as well as the regulator both regard virtual currencies as having potential threats of being used in money laundering regimes due to the anonymous aspects of them. The legislation imposed to minimize these threats is by both parties received positively. Despite that, the virtual currency exchanges also noticed many negative influences on the system of which the decrease to innovative power is the most important one.

Before the implementation of the AMLD5 the virtual currency exchanges largely already complied to the Wwft. They were also not surprised that the legislation was introduced as they had been in the process to comply to it for a few years. Measures that were already in place were strict payment limits, Know Your Customer measures and transaction monitoring, for which all use blockchain analysis tools. After implementation of the legislation not much changed in these measures. Big differences were that reports had to be made to the FIU and that wallet verification had to be implemented. Moreover, changes can be observed within organisations on an administrative level as procedures had to be better recorded. In the landscape, however, much differences were observed by parties moving abroad, quitting their operation or altering their services.

Currently, the virtual currency exchanges fall under risk-based supervision of DNB. DNB executes this by providing the exchanges with a questionnaire based on which they estimate the risks. These questionnaires have proven to be very large and labour intensive information requests according to the exchanges. This leads to much dissatisfaction amongst the virtual currency exchanges as they sometimes feel misunderstood or mistrusted.

All parties hope that in the coming years harmonisation of the legislation in the EU will take place. Moreover, they expect knowledge sharing to become more important within the sector, in public private partnerships and between the regulator and exchanges.

With this information sub question 3 can now be answered. *"How has the implementation of the 5th Anti-Money Laundering Directive affected the parties involved in the Netherlands?"* After the implementation of the AMLD5 the regulator had to ensure that the registration process was set up and had to gain more knowledge on the virtual currency ecosystem in order to be able to reliably supervise the system. Currently, the regulator has to enforce supervision with questionnaires and onsite visits. Virtual currency exchanges, on the other hand, did not have to adapt many measures in place for KYC or CDD and transaction monitoring as they had already implemented these measures. Despite that, many of the processes already there had to be formalised and recorded. New measures that had to be executed were merely the reporting duty and wallet verification. Also, answering information requests by DNB provided new operational activities. Still, they feel that the legislation led to less innovation power, although this may not be relevant currently this can become relevant over the coming years. Moreover, other parties were negatively influences by the AMLD5 as due to this they had to stop operating, altered their services or moved abroad.

7

Public policy takeaways

This chapter will further elaborate upon the results derived from this research. It first provides context for the results, in section 7.1, by placing it in the field of research performed before. Next, this in section 7.2 the limitations of the research at hand are discussed. The chapter will be concluded, in section 7.3, by providing recommendations for future research and implications of the research for policymakers.

7.1. Context

According to Stokes (2012), over the years more licit transactions were being executed. They showed that this made Bitcoin more suitable to be adopted by criminals as the illicit transactions executed would obtain less scrutiny and would not stand out as much. It was expected that this could be observed. Nevertheless, the blockchain analysis showed that the overall number of transactions was actually decreasing, this was not expected up front. A possible explanation for this could be the scope of only investigating virtual currency exchanges in the Netherlands and not the full bitcoin economy. It was however, identified that the blockchain analysis showed the exponential increase of the exchange rate, as was observed in the market over the years. This provides validity for the fact that enough data was present to represent the patterns seen in the system.

The research concludes that the effectiveness of the implementation of the 5th Anti-Money Laundering Directive can be disputed. Whereas the effectiveness was here evaluated afterwards, Covolo (2019) and De Vido (2019) tested the legislation ex ante. They found that the legislation provided several large shortcomings which could lead to a lower effectiveness of the legislation. It was indeed found that several things lead the effectiveness to be doubtful.

Moreover, Campbell-Verduyn (2017) stated that legislation could lead to a displacement effect in which the illicit transactions move to other institutions that do not fall under the regulation. In the interviews this effect was mentioned several times. Also, the blockchain analysis showed that the number of transactions decreased indicating that this displacement effect took place. The same was mentioned by De Vido (2019) who stated that due to the regulation of virtual currency exchanges the reaction might be for the system to go ”darker” in order to circumvent regulation.

Several things were mentioned in the interviews that provide shortcomings for the regulation that have been addressed earlier. First, the interviewees mentioned that old rules are imposed on the system. Already in 2013 Moser et al. stated that the traditional financial system cannot function as an analogy for the virtual currency ecosystem, but the legislation seems to do so. Moreover, Covolo (2019) stated that successful enforcement in AML is dependent on the smooth cooperation and coordination between regulators, supervisors and other entities throughout Europe and beyond. It was interesting to find that the interviewees indicated this need as well.

As was observed in chapter 4 the Wet witwassen en financiering terrorisme had two goals (“Kamerstukken II, 31477, 1-2 (Rapport)”, 2007). On the one hand, it was implemented to prevent integrity breaches at financial institutions and disable them from being used in money laundering regimes. On the other hand, with the legislation it is attempted to detect crime effectively and efficiently. This research showed the effects on the virtual currency ecosystem of the implementation of the 5th Anti-money laundering directive in the Wwft. It is deplorable that the directive does not seem to have obtained any step towards accomplishing these goals. First, the amount of transactions falling under the legislation is microscopic as only conversion between fiat and virtual

currency is considered, compared to the traditional financial system only a very small number of transactions are executed at these exchanges. Also, the legislation is purely focused on the Netherlands while the system has many global characteristics. Thus, it can be seen that the legislation in place does not fit the system at hand. This is the case due to the fact that only a limited dialogue had taken place, as stated by the respondents, and the fact that old rules are imposed on a new system. Moreover, it is regrettable that the legislation was already outdated when it went into effect. The measures that the virtual currency exchanges were obliged to put in place had namely already been put in place many years earlier. In addition, it seems as if almost no advances were made in preventing the institutions from being used in money laundering regimes due to the directive as the blockchain analysis showed that almost no difference was observed after implementation. This was largely due to the fact that the virtual currency exchanges already had the intrinsic motivation to counter money laundering. It seems as if the legislation is overshooting the mark, which is the only reason for implementing the wallet verification measure, of which the judge ruled it needed extra explanation from the regulator. Due to this measure having been put in place and comments by the respondents it is questionable whether the legislator and regulator have the necessary knowledge at hand to effectively regulate the system in order to obtain the goals set in the legislation.

7.2. Limitations

One limitation of the research is the fact that it focused purely on the Netherlands. There are multiple reasons for this. First, the nature of virtual currencies are in itself border crossing. Moreover, the legislation in place has an effect throughout Europe. By only investigating the Dutch sector, one of the things that has been left out is the effect that differences in legislation between member states of the EU can provide large effects for the ecosystem. Looking at an international perspective would provide more context to the findings of the research. Also, possible displacement effects could be further investigated. The outcomes could then thus slightly differ as more information on what precisely happens in the field can be gathered.

For the blockchain analysis only bitcoin was considered. However, in the virtual currency ecosystem people do often not just focus on one crypto currency. As crypto is also seen as a trading asset often risk is diversified by adopting a portfolio containing several different coins. These other coins also fall under the legislation but were not investigated in the research. However, as bitcoin provides for the largest market and is still the most popular coin a good representation could still be given. Moreover, it is unknown whether all virtual currency exchanges active in the Netherlands were investigated in the research. As was stated by De Vido (2019) one of the major problems with the legislation lied in the territoriality of the legislation making it difficult to know where an entity should be located in order to fall under the scope of the directive. Also, no real criteria are set up to define whether an exchange is actively targeting the Dutch market, as was apparent from the interviews in chapter 6 as well. This could therefore leave the list of currency exchanges included to be incomplete.

Several other limitations of the data adopted in the blockchain analysis can be observed. Next to not having included all non-registered exchanges, also not all registered exchanges were included in the dataset. Due to Chainalysis not having identified clusters for all exchanges, only 17 out of the 20 in advance identified registered virtual currency exchanges were included. Moreover, not for all transactions the counterparty cluster category was provided. This led another part of the data to be unusable for one part of the analysis. Furthermore, only Chainalysis was used to collect the data. By extracting transaction data from multiple resources a more complete overview could have been provided and a more complete dataset could have been gathered. However, due to constraints in time and resources, this was not feasible. Nevertheless, as this research tries to explore the effects on virtual currency exchanges it is possible to do so with the help of this limited dataset. This research set a first step in identifying the effects of the legislation. Since it is only the first step not a complete overview of all transactions from all virtual currency exchanges in the Netherlands is necessary. For both types of exchanges, registered as well as non-registered, multiple organizations were included and the different types of exchanges were properly represented. Therefore the data suffices for the goal of exploring the effects.

Chapter 5 showed that the patterns observed in the blockchain analysis, especially the decrease in executed number of transactions and the increase in the transaction volume, can have multiple explanations for being observed. Furthermore, the effects of the differences in origin or destination of transactions seem to be negligible. Also, the interviewees explained that the virtual currency exchanges have been trying to counter money laundering since 2015 and 2016 and already had measures in place since that time. Therefore, the time frame that was chosen was not broad enough to identify differences in the patterns.

Lastly, interviews were held with several different virtual currency exchanges. However, the thing that they all have in common is that they are a member of the interest group VBNL. Although, some of them were regis-

tered and some were not, this still provides some bias in the interview results. Being part of the VBNL automatically shows an intrinsic motivation to counter money laundering due to their code of conduct. Therefore, the perspective of being willing to counter money laundering might be over represented. Furthermore, no interviews were conducted with virtual currency exchanges who moved abroad or with other parties in the sector, such as policy makers who could provide information on the choices for this type of legislation. Lastly, only a limited number of interviews were held due to time constraints. For the regulatory authority it was impossible to perform more interviews, since there is only a small department working on the supervision of virtual currency exchanges.

7.3. Recommendations

This section identifies recommendations for future research. Also, it provides an advise to policy makers willing to change the virtual currency ecosystem to counter money laundering in order to improve the policy framework.

7.3.1. Future research

First, for future research, in order to keep in mind the global characteristics of the system, it is advised to add a reference group with which the country can be compared. With this it could be understood whether changes in transaction volume of average transactions are a global trend or just something seen in the Netherlands. Also, by incorporating a reference group of countries with limited regulation it can be seen whether a displacement effect can be apparent, thus whether the number of transactions there increased much. Moreover, a benchmark can be produced with other virtual currency exchanges on an international level to better be able to understand and compare the effects seen at several exchanges. In addition, research can further be performed into how effects at virtual currency exchanges can be noticed. Another method that can be adopted to further investigate the precise effects on virtual currency exchange is by adopting a survey method to understand whether different employees within the virtual currency exchanges see their tasks as having changed, possibly on the administrative side to validate the results of this research.

From the interviews it appeared that many anti-money laundering procedures were already in place since 2016. Therefore, it might be interesting to investigate a longer period of time. In this way it can be observed whether indeed at that time it is possible to detect differences after these procedures were put in place and thus observe the effects of the measures. Moreover, a more complete dataset could be adopted in this investigation by for example using of different blockchain analysis software or purely using the blockchain itself.

Lastly, looking at the MiCA regulation that is currently being drawn up the conclusions this research came to may already be almost outdated as new regulation is in the pipeline. Therefore, it is advised to already investigate the effects of the MiCA regulation to ensure that of the legislation that will be established the shortcomings are known and can be addressed in advance.

7.3.2. Policy advice

For policy makers it is advised to start the conversation with the sector. The sector has much knowledge and ideas to counter money laundering and is willing to join in the conversation. By letting them provide input the regulation can be adapted in such a way that it fits the sector and that it provides the effects desired. Moreover, this can lead the knowledge base on which policy is based to increase. Furthermore, it will remove feelings of dissatisfaction when parties are involved from the start.

It is further advised to establish better cooperation between supervisors, legislators and private parties. Due to this cooperation more effectively transaction monitoring for example can be altered. Also, direct input can be delivered for the policy or desires and needs can be discussed. It is advised to do this on an international level since only in this way will the global, international characteristic of the system be handled.

8

Conclusion

Over the years, the European Union and its member states have been focusing more on combatting criminality and prosecuting criminals. Financially-economically related crime is especially being seen as a risk when using virtual currencies, which are not issued or guaranteed by any jurisdiction and are often part of a decentralized system. Virtual currencies also provide new opportunities for money laundering. In the National Risk Assessment (van der Veen and Heuts, 2020) it was seen that the risk for money laundering with virtual currencies is estimated to be high due to the low resilience in the Netherlands against this form of crime. Moreover, adopting virtual currencies to launder money facilitates payments for various other forms of cyber crime.

To prevent this from happening the 5th Anti-Money Laundering Directive (AMLD5) was introduced on an European level. This led virtual currency exchanges to fall under the Wwft. Virtual currency exchanges provide services to convert fiat currency and virtual currency. The introduction of the AMLD5 led to new responsibilities and requirements for virtual currency exchanges. It is important to understand the effects of policies on money laundering as the financial system is based on trust. Mixing laundered money with regular money can compromise the integrity of the financial system. In addition, understanding the effects of the policy in place can lead the prosecutive organizations to trace suspicious transactions.

It was found that the role of virtual currency exchanges in money laundering has only scarcely been researched. Furthermore, it was seen that only limited research has been done into the effects of the regulations imposed. As it has not been researched before what the role, daily operations or previous anti-money laundering efforts is of virtual currency exchanges while the AMLD5 intends to regulate the system by appointing several duties on these services it cannot be understood whether the regulation in place will have the desired effects. This research provided insights into the effects of the implementation of the AMLD5 on the daily operations of virtual currency exchange services in order to fill this knowledge gap and understand the effectiveness of the regulation.

To understand the landscape that virtual currency exchanges operate in, an attempt was made to provide a sketch of the governance in place. Governance is defined as the legislation in effect and the actors in the playing field and the relationships between them. To present this outline a combination of policy documents, legislation and grey literature was adopted. It was found that the current state of governance in anti-money laundering in the virtual currency ecosystem is focused on virtual currency exchanges being seen as gatekeepers between the traditional financial system and the new virtual financial system, making them largely responsible to counter money laundering.

The 5th Anti-Money Laundering Directive was transferred into the Dutch Wet Witwassen en Financiering Terrorisme (“Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft)”, n.d.) in May 2020. With the new legislation coming into effect several things changed for virtual currency exchanges. The AMLD5 made virtual currency exchanges become obligated to obtain a registration, at the regulator the Dutch National Bank (DNB), and thus fall under the restrictions imposed by the Wwft. The requirements coming forward from it included performing customer due diligence and having a transaction monitoring system in place. Furthermore, virtual currency exchanges now also have to report unusual transactions at the Financial Intelligence Unit of the Netherlands (FIU-NL). Moreover, the Sanctiewet provides important requirements for the virtual currency exchanges as from here on the exchanges have to perform wallet verification. Governance is further characterised by a combination of public and private actors. VBNL is the interest group for virtual currency exchanges. Two

Ministries formulate the legislation. FIU-NL investigates unusual transactions to identify suspicious transactions. DNB is the regulator in the system who monitors whether the supervised virtual currency exchanges comply to the legislation.

To identify the effects that these requirements had on the virtual currency exchanges, an exploration was made of the transactions observed. Transaction data was collected of Dutch virtual currency exchanges from the blockchain, through Chainalysis. Next, the analysis was performed with the help of Python. Two things were found to have changed in the transaction behaviour surrounding Dutch virtual currency exchanges that could be observed from the blockchain after the implementation of the 5th Anti-Money Laundering Directive. First, less transactions were being made after the implementation of the legislation. Second, the average transaction value increased. All in all, this could imply that less splitting of transactions took place. Due to the fact that after having gone through the onboarding procedure it would be less risky for the virtual currency exchanges to heighten payment limits as they know who they are in a business relationship with. On the other hand, the fact that the number of transactions decreased drastically could also indicate that clients took their transactions to other exchanges, possibly abroad. However, when looking at the origin or destination of transactions, the changes observed were minimal. Still, many other explanations can also be observed for these effects which are not linked to the implementation of the legislation. Therefore, the effectiveness of the legislation in identifying more criminal transactions is questionable.

Next to identifying what changed in the transaction behaviour, understanding the effects of the AMLD5 on the parties involved were tried to be understood by holding five interviews with the regulator and several virtual currency exchanges. It was found that the implementation of the 5th Anti-Money Laundering Directive affected the parties involved in different manners. The regulator had to ensure that a smooth process took place for the registration procedure. Currently as tool for their supervision they spread out several questionnaires to gain more information on where risks arise in order to perform risk-based supervision. Virtual currency exchanges have to answer these questionnaires, which according to them is very labour intensive as the information requests of the regulator are quite extensive. It was seen that much dissatisfaction is present with the manner of supervision at virtual currency exchanges. When looking at the requirements arising from the legislation it is striking that the measures to counter money laundering were already in place before the legislation was present. Alterations at virtual currency exchanges were merely administrative since they had to further record processes and procedures and have to answer the information requests by DNB. In the landscape however, many differences were observed as the barriers imposed by the legislation led other virtual currency exchanges to move abroad, quit their operation or alter their services, which could lead to less innovative power in the sector.

The main question of this research was *"To what extent have virtual currency exchanges in the Netherlands altered their daily operations in order to comply to the Dutch implementation of the 5th Anti-Money Laundering Directive?"* It was found that, according to the interviews, many of the virtual currency exchanges did not alter their daily operations in their money laundering countering measures. They were merely focused on complying to the new duty to report and answering the information requests by the regulator. The extent to which virtual currency exchanges in the Netherlands have altered their daily operations is thus merely administrative by recording processes, providing information and writing reports on unusual transactions. They have not actively altered their operations in countering money laundering. This was also observed in the blockchain analysis as the origin or destination of transactions was not altered after the implementation. But, looking at the full ecosystem it was observed that other parties altered their operation, quit or moved abroad. All in all, the legislation seems to surpass the goal. As the goal was twofold on the one hand, preventing customers from misusing financial institutions to launder money. On the other hand, detecting and prosecuting crime effectively and efficiently. Thus, the AMLD5 will have not made a difference on the first part as preventing the financial institutions from being used in money laundering was already performed by virtual currency exchanges beforehand. Nonetheless, the reporting duty might have made a difference for investigative services in having insight into the unusual and sometimes even suspicious transactions, but the effect of this is unknown.

Bibliography

AFM. (n.d.). Rol- en taakverdeling. https://www.afm.nl/nl-nl/over-afm/werkzaamheden/verantwoordelijkheden

AFM. (2020). *Leidraad Wwft en Sanctiewet* (tech. rep.). Amsterdam.

AMLC. (n.d.). Wie zijn wij en wat doen wij? https://www.amlc.nl/wie-zijn-wij-en-wat-doen-wij/

AMLC. (2021). *Jaarplan 2021* (tech. rep.).

Anti Money Laundering Centre. (2018). Witwassen, wat is dat? https://www.amlc.nl

Azevedo, M. A. (2021). Crypto boom continues as Chainalysis raises $100M, doubles valuation to over $2B. https://techcrunch.com/2021/03/26/chainalysis-raises-100m-doubles-valuation-to-over-2b

Basel Committee on Banking Supervision. (2001). Customer due diligence for banks. (October).

Belastingdienst. (n.d.). Beroepsgroepen voor de Wwft. https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/aangifte_betalen_en_toezicht/wwft-voorkomen-van-witwassen-en-terrorismefinanciering/beroepsgroepen/beroepsgroepen

Betting, R. (2021). Markets in Crypto Assets Regulation (MiCA). https://charcoendique.nl/artikelen/markets-in-crypto-assets-regulation-mica/

Binance. (n.d.). Binance P2P: Buy/Sell Your Crypto Locally. https://p2p.binance.com/en

bitcoin.com. (n.d.). Bitcoin ATM. https://www.bitcoin.com/bitcoin-atm/

Bitonic. (n.d.). https://bitonic.nl/en/

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, *29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Brenig, C., Accorsi, R., & Möller, G. (2015). Economic analysis of cryptocurrency backed money laundering. *23rd European Conference on Information Systems, ECIS 2015*. https://doi.org/10.18151/7217279

Bryans, D. (2014). *Bitcoin and Money Laundering: Mining for an Effective Solution* (Vol. 89).

Bureau Financieel Toezicht. (n.d.). Wat doet het BFT. https://www.bureauft.nl/bft/

Campbell-Verduyn, M. (2017). *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance*. https://doi.org/10.4324/9781315211909

Carruthers, B. G., & Arslan, M. (2019). Sovereignty, Law, and Money: New Developments. *Annual Review of Law and Social Science*, *15*, 521–538. https://doi.org/10.1146/annurev-lawsocsci-101518-042625

CBS. (2021). Betalingstransacties naar betaalmethode, aantallen en bedragen per week. https://www.cbs.nl/nl-nl/maatwerk/2021/29/betalingstransacties-naar-betaalmethode-aantallen-en-bedragen-per-week

Chainalysis. (n.d.). Knowledge base - Chainalysis.

Chainalysis. (2019). It's Not Personal: How Chainalysis Collects and Uses Service-Level Data. https://blog.chainalysis.com/reports/service-level-data

Chainalysis. (2020). *The 2020 State of Crypto Crime* (tech. rep.). Chainalysis.

Chainalysis Regulatory Team. (2020). What You Need to Know About Treasury's 72-page NPRM for Transactions with Unhosted Wallets and Certain Foreign Jurisdictions. https://blog.chainalysis.com/reports/treasury-department-nprm-unhosted-wallets-2020

Chainalysis Team. (2020a). Covid-19 is Changing the Relationship Between Bitcoin Price and Bitcoin Spending. https://blog.chainalysis.com/reports/covid-19-bitcoin-price-bitcoin-spending

Chainalysis Team. (2020b). Mining Pools' Activity Suggests They're Preparing for a Bitcoin Price Surge Following the Halving. https://blog.chainalysis.com/reports/mining-pools-bitcoin-halving-2020

Chainalysis Team. (2021). U.S. Government Targets Russian Influence Operations with Cryptocurrency Nexus. https://blog.chainalysis.com/reports/ofac-fbi-russian-influence-synthetic-identity-document-vendor-sanctions

Christopher, C. M. (2014). Whack-a-mole: Why prosecuting digital currency exchanges won't stop online money laundering. *Lewis & Clark Law Review*, *18*(1). http://ssrn.com/abstract=2312787Electroniccopyavailableat:http://ssrn.com/

Conway, L. (2021). Bitcoin Halving: What You Need to Know. https://www.investopedia.com/bitcoin-halving-4843769

Covolo, V. (2019). The EU Response to Criminal Misuse of Cryptocurrencies: The Young, Already Outdated 5th Anti-Money Laundering Directive. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3503535

Crawford, J., & Guan, Y. (2020). Knowing your bitcoin customer: Money laundering in the bitcoin economy. *Proceedings - 2020 13th Systematic Approaches to Digital Forensic Engineering, SADFE 2020*, 38–45. https://doi.org/10.1109/SADFE51007.2020.00013

Custers, B., Oerlemans, J.-J., & Pool, R. (2020). Laundering the Profits of Ransomware. *European Journal of Crime, Criminal Law and Criminal Justice*, *28*(2), 121–152. https://doi.org/10.1163/15718174-02802002

Custers, B., Pool, R. L. L., & Cornelisse, R. (2019). Banking malware and the laundering of its profits. *European Journal of Criminology*, *16*(6), 728–745. https://doi.org/10.1177/1477370818788007

De Vido, S. (2019). The Regulation of Virtual Currencies in the New EU V Anti-Money Laundering Directive. *DPCE online*, *1*(May), 59–76.

De Vido, S. (2020). Virtual Currencies: New Challenges to the Right to Privacy? An Assessment under the v AML Directive and the GDPR. *Global Jurist*, *20*(2), 1–14. https://doi.org/10.1515/gj-2019-0045

Denzin, N. K. (2017). *The Research Act*. Routledge. https://doi.org/10.4324/9781315134543

Desmond, D. B., Lacey, D., & Salmon, P. (2019). Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. *Journal of Money Laundering Control*, *22*(3), 480–497. https://doi.org/10.1108/JMLC-10-2018-0063

de Wit, J. (2007). A risk-based approach to AML. *Journal of Financial Regulation and Compliance*, *15*(2), 156–165. https://doi.org/10.1108/13581980710744048

DNB. (n.d.). Open Boek Toezicht. https://www.dnb.nl/voor-de-sector/open-boek-toezicht/

DNB. (2020). *Leidraad Wwft en Sanctiewet* (tech. rep.). Amsterdam.

DNB, & AFM. (2018). *Crypto's - aanbevelingen voor een regelgeven* (tech. rep.).

Dupuis, D., & Gleason, K. (2020). Money laundering with cryptocurrency: open doors and the regulatory dialectic. *Journal of Financial Crime*, *ahead-of-p*(ahead-of-print). https://doi.org/10.1108/JFC-06-2020-0113

ECLI:NL:RBROT:2021:2968. (2021). https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBROT:2021:2968&showbutton=true

Egmont Group. (n.d.). About. https://egmontgroup.org/en/content/about

Europa Nu. (n.d.). Europese Commissie (EC). https://www.europa-nu.nl/id/vg8xdjeo1zoj/europese_commissie_ec

European Commission. (n.d.). Anti-money laundering and counter terrorist financing. https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en

European Commission. (2020). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

European Union. (n.d.-a). European Commission. https://europa.eu/european-union/about-eu/institutions-bodies/european-commission_en

European Union. (n.d.-b). European Parliament. https://europa.eu/european-union/about-eu/institutions-bodies/european-parliament_en

Europol. (2020). *Internet Organised Crime Threat Assessment 2020* (tech. rep.).

FATF. (n.d.). Who we are. https://www.fatf-gafi.org/about/

FATF. (2014). *Virtual Currencies Key Definitions and Potential AML/CFT Risks* (tech. rep.). Financial Action Task Force. www.fatf-gafi.org

FATF. (2020). *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (tech. rep.). FATF. Paris, France. www.fatf-gafi.org/recommendations.html

FIOD. (n.d.). Wat doet de FIOD? https://www.fiod.nl/wat-doet-de-fiod/

FIOD. (2019). *FIOD, specialist in financiële fraudeopsporing* (tech. rep.). Belastingdienst.

FIU. (n.d.). Beroeps- of bedrijfsmatige aanbieders van diensten voor het wisselen tussen virtuele valuta en fiduciaire valuta. https://www.fiu-nederland.nl/nl/meldergroep/300

FIU-Nederland. (n.d.-a). Europese Unie. https://www.fiu-nederland.nl/nl/over-fiu/internationale-samenwerking/europese-unie

FIU-Nederland. (n.d.-b). FATF. https://www.fiu-nederland.nl/nl/over-fiu/internationale-samenwerking/fatf

FIU-Nederland. (n.d.-c). Organisatie. https://www.fiu-nederland.nl/nl/over-fiu/organisatie

FIU-Nederland. (n.d.-d). Over de FIU. https://www.fiu-nederland.nl/nl/over-de-fiu

Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. *Research in International Business and Finance*, *56*(January), 101387. https://doi.org/10.1016/j.ribaf.2021.101387

Frankenfield, J. (2021). Darknet Market Definition. https://www.investopedia.com/terms/d/darknet-market-cryptomarket.asp

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal*, *204*(6), 291–295. https://doi.org/10.1038/bdj.2008.192

Grigg, G. (2021). Why I Joined Chainalysis After 23 Years at the FBI. https://blog.chainalysis.com/reports/gurvais-grigg-chainalysis

Harrigan, M., & Fretter, C. (2016). The Unreasonable Effectiveness of Address Clustering, 1–6. https://doi.org/10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.136

Het Europees Parlement en de Raad van de Europese Unie. (2015). RICHTLIJN (EU) 2015/849 VAN HET EUROPEES PARLEMENT EN DE RAAD van 20 mei 2015 inzake.

IBM Cloud Education. (6). What is IaaS (Infrastructure-as-a-Service). https://www.ibm.com/cloud/learn/iaas

International Monetary Fund. (2011). *The Netherlands - Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism* (tech. rep.). Washington, D.C.

Investing.com. (n.d.). Bitcoin Price Chart Live. https://www.investing.com/crypto/bitcoin/chart

Jabotinsky, H. Y., & Sarel, R. (2020). How Crisis Affects Crypto: Coronavirus As a Test Case. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3557929

Jamshed, S. (2014). Qualitative research method-interviewing and observation. *Journal of Basic and Clinical Pharmacy*, *5*(4), 87. https://doi.org/10.4103/0976-0105.141942

Jick, T. D. (1979). Mixing Qualitative and Quantitative Methods: Triangulation in Action. *Administrative Science Quarterly*, *24*(4), 602. https://doi.org/10.2307/2392366

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed Methods Research: A Research Paradigm Whose Time Has Come. *Educational Researcher*, *33*(7), 14–26. https://doi.org/10.3102/0013189X033007014

Johnson, R. B., Onwuegbuzie, A. J., & Turner, L. A. (2007). Toward a Definition of Mixed Methods Research (K. O. Korgen, Ed.). *Journal of Mixed Methods Research*, *1*(2), 112–133. https://doi.org/10.1177/1558689806298224

Joint Committee ESA. (n.d.). Anti-Money Laundering - Objectives and Tasks. https://esas-joint-committee.europa.eu/Pages/Activities/Anti-Money-Laundering-Objectives-and-Tasks.aspx

Joint Committee ESA. (2016). *Towards European Supervisory Convergence* (tech. rep.). Luxembourg. https://doi.org/10.2854/73366

Kamerstukken II, 31477, 1-2 (Rapport). (2007).

Kamerstukken II, 31477, 41 (Kamerbrief). (2018). https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2019Z13803&did=2019D28409

Kamerstukken II, 34808, 3 (MvT). (2017).

Kamerstukken II, 34808, 6 (NV). (2018). https://zoek.officielebekendmakingen.nl/kst-34808-6.html

Kamerstukken II, 35245, 3 (MvT). (2019). https://zoek.officielebekendmakingen.nl/kst-35245-3.html

Kamerstukken II, 35245, 4 (Advies RvS). (2019). https://zoek.officielebekendmakingen.nl/kst-35245-4.html

Kamerstukken II, 35245, 6 (NV). (2019). https://zoek.officielebekendmakingen.nl/kst-35245-6.html

Kansspelautoriteit. (n.d.). Toezicht op de Wwft & matchfixing. https://kansspelautoriteit.nl/over-ons/bestuur-organisatie/wwft-matchfixing/

Kapilkov, M. (2020). Antonopoulos: Chainalysis Is Helping World's Worst Dictators & Regimes. https://cointelegraph.com/news/antonopoulos-chainalysis-is-helping-worlds-worst-dictators-regimes

Koningsveld, T. J. V. (2008). Witwassen : de fasen van het witwasproces getoetst, 88–104.

Kothari. (2004). *Collection of data through questionnaires*.

Kruisbergen, E., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2019). Money talks money laundering choices of organized crime offenders in a digital age. *Journal of Crime and Justice*, *42*(5), 569–581. https://doi.org/10.1080/0735648X.2019.1692420

Kruisbergen, E., & Soudijn, M. (2015). Wat is witwassen eigenlijk? *Justitiële verkenningen*, *41*(1), 10–23. https://doi.org/10.5553/JV/016758502015041001002

Levi, M. (2015). Money for Crime and Money from Crime: Financing Crime and Laundering Crime Proceeds. *European Journal on Criminal Policy and Research*, *21*(2), 275–297. https://doi.org/10.1007/s10610-015-9269-7

Levi, M., & Soudijn, M. (2020). Understanding the Laundering of Organized Crime Money. *Crime and Justice*, *49*(1), 579–631. https://doi.org/10.1086/708047

Liang, J., Li, L., Chen, W., & Zeng, D. (2019). Targeted addresses identification for bitcoin with network representation learning. *2019 IEEE International Conference on Intelligence and Security Informatics, ISI 2019*, 158–160. https://doi.org/10.1109/ISI.2019.8823249

Limba, T., Stankevičius, A., & Andrulevičius, A. (2019). TOWARDS SUSTAINABLE CRYPTOCURRENCY: RISK MITIGATIONS FROM A PERSPECTIVE OF NATIONAL SECURITY. *Journal of Security and Sustainability Issues*, *9*(2), 375–389. https://doi.org/10.9770/jssi.2019.9.2(2)

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A fistful of Bitcoins. *Communications of the ACM*, *59*(4), 86–93. https://doi.org/10.1145/2896384

Merriam-Webster. (n.d.). Scam. https://www.merriam-webster.com/dictionary/scam

Ministerie van Financien & Ministerie van Justitie en Veiligheid. (2020). *Algemene leidraad Wet ter voorkoming van witwassen en financieren van terrorisme (WWFT)* (tech. rep.). Rijksoverheid.

MONEYVAL. (n.d.-a). At a glance. https://www.coe.int/en/web/moneyval

MONEYVAL. (n.d.-b). MONEYVAL in brief. https://www.coe.int/en/web/moneyval/moneyval-brief

Moser, M., Bohme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. *eCrime Researchers Summit, eCrime*, 1–14. https://doi.org/10.1109/eCRS.2013.6805780

Möser, M., & Narayanan, A. (2019). Effective Cryptocurrency Regulation Through Blacklisting. *Preprint*. https://allquantor.at/blockchainbib/pdf/moser2019effective.pdf

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Nationaal Cyber Security Centrum. (n.d.). Ransomware. https://www.ncsc.nl/onderwerpen/ransomware

Nederlandse Orde van Advocaten. (n.d.). Toezicht door de deken. https://www.advocatenorde.nl/toezicht-door-de-deken

Nelson, D. (2020). Inside Chainalysis' Multimillion-Dollar Relationship With the US Government. https://www.coindesk.com/inside-chainalysis-multimillion-dollar-relationship-with-the-us-government

Nu.nl. (2020). Hoekstra waarschuwt: 'Komt nog meer ellende over witwassen naar buiten'. https://www.nu.nl/politiek/6079119/hoekstra-waarschuwt-komt-nog-meer-ellende-over-witwassen-naar-buiten.html

Pappas, C., & Williams, I. (2011). Grey Literature: Its Emerging Importance. *Journal of Hospital Librarianship*, *11*(3), 228–234. https://doi.org/10.1080/15323269.2011.587100

Parlement.com. (n.d.). Ministerie van Financiën (Fin). https://www.parlement.com/id/vhnnmt7hvi78/ministerie_van_financien_fin

Paxful Team. (2020). What are Public Keys, Private Keys, & Wallet Addresses? https://paxful.com/blog/what-are-public-keys-private-keys-wallet-address/

Piotrowski, S. J. (2007). 18 Obtaining Archival and Other Existing Records. In G. J. Miller & K. Yang (Eds.), *Handbook of research methods in public administration* (2nd). CRC Press. https://doi.org/10.1201/9781420013276

Prypto. (n.d.). Bitcoin Public and Private Keys. https://www.dummies.com/software/other-software/bitcoin-public-private-keys/

Ranshous, S., Joslyn, C. A., Kreyling, S., Nowak, K., Samatova, N. F., West, C. L., & Winters, S. (2017). Exchange pattern mining in the bitcoin transaction directed hypergraph. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *10323 LNCS*, 248–263. https://doi.org/10.1007/978-3-319-70278-0{_}16

Reynolds, P., & Irwin, A. S. (2017). Tracking digital footprints: anonymity within the bitcoin system. *Journal of Money Laundering Control*, *20*(2), 172–189. https://doi.org/10.1108/JMLC-07-2016-0027

Rijksoverheid. (n.d.). Ministerie van Justitie en Veiligheid. https://www.rijksoverheid.nl/ministeries/ministerie-van-justitie-en-veiligheid

Rjksoverheid. (n.d.). Wet op het financieel toezicht (Wft). https://www.rijksoverheid.nl/onderwerpen/financiele-sector/wet-op-het-financieel-toezicht-wft

Robbins, N. (2012). When Should I Use Logarithmic Scales in My Charts and Graphs? https://www.forbes.com/sites/naomirobbins/2012/01/19/when-should-i-use-logarithmic-scales-in-my-charts-and-graphs/?sh=5182fd195e67

Rooijendijk, L. (2020). Nederland in top 10 meest heimelijke landen in Financial Secrecy Index 2020. https://www.transparency.nl/nieuws/2020/02/nederland-top-10-financial-secrecy-index-2020/

Schnezler, J. (2020). Veel crypto-ondernemers stoppen vanwege aanpassing Wwft. Kunt u nog (wel) cryptodiensten aanbieden? https://rwv.nl/nieuws/2020/07/veel-crypto-ondernemers-stoppen-vanwege-aanpassing-wwft-kunt-u-nog-wel-cryptodiensten-aanbieden

Sephton, C. (2020). Chainalysis: Child pornography buyers flocking to bitcoin. https://modernconsensus.com/cryptocurrencies/bitcoin/chainalysis-child-pornography-buyers-flocking-to-bitcoin/

Sim, B. (2021). It's not just bitcoin — here are the top 10 biggest cryptocurrencies. https://www.fnlondon.com/articles/its-not-just-bitcoin-here-are-the-top-10-biggest-cryptocurrencies-20210309

Slot, B., & de Swart, L. (2018). *Monitor anti-witwasbeleid 2014 - 2016* (tech. rep.). Ecorys, WODC. Rotterdam.

Sotiropoulou, A., & Guégan, D. (2017). Bitcoin and the challenges for financial regulation. *Capital Markets Law Journal*, *12*(4), 466–479. https://doi.org/10.1093/cmlj/kmx037

Soudijn, M. R. J. (2019). Using Police Reports to Monitor Money Laundering Developments. Continuity and Change in 12 Years of Dutch Money Laundering Crime Pattern Analyses. *European Journal on Criminal Policy and Research*, *25*(1), 83–97. https://doi.org/10.1007/s10610-018-9379-0

Staatsblad 2020, 163 (AMvB). (2020). https://zoek.officielebekendmakingen.nl/stb-2020-163.html

Stewart, D., & Kamins, M. (1993). *Secondary Research*. SAGE Publications, Inc. https://doi.org/10.4135/9781412985802

Stokes, R. (2012). Virtual money laundering: the case of Bitcoin and the Linden dollar. *Information & Communications Technology Law*, *21*(3), 221–236. https://doi.org/10.1080/13600834.2012.744225

The Blockchain Analysis Company. (n.d.). https://www.chainalysis.com/

The Investopedia Team. (2021). Fiat vs. Representative Money: What's the Difference? https://www.investopedia.com/ask/answers/041615/what-difference-between-fiat-money-and-representative-money.asp

Tropina, T. (2014). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. *ERA Forum*, *15*(1), 69–84. https://doi.org/10.1007/s12027-014-0335-2

Tu, K. V., & Meredith, M. W. (2015). Rethinking virtual currency regulation in the bitcoin age. *Washington Law Review*, *90*(1), 271–347.

Tuba, M., & Van Der Westhuizen, C. (2014). An analysis of the 'know your customer' policy as an effective tool to combat money laundering: Is it about who or what to know that counts? *International Journal of Public Law and Policy*, *4*(1), 53–70. https://doi.org/10.1504/IJPLAP.2014.057870

van der Veen, H., & Heuts, L. (2020). *National Risk Assessment Witwassen 2019* (tech. rep.). WODC. https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2020/07/03/cahier-national-risk-assessment-witwassen/cahier-national-risk-assessment-witwassen.pdf

van Teeffelen, K. (2020). TU Delft en Fiod gaan 'unieke' samenwerking aan om online criminaliteit aan te pakken. https://www.trouw.nl/nieuws/tu-delft-en-fiod-gaan-unieke-samenwerking-aan-om-online-criminaliteit-aan-te-pakken~bea6c715/?referrer=https%3A%2F%2Fwww.google.com%2F

VBNL. (n.d.). Welkom. https://verenigdebitcoinbedrijvennederland.org/

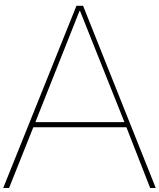
Vishwas, B. V., & Patel, A. (2020). *Hands-on Time Series Analysis with Python*. Apress. https://doi.org/10.1007/978-1-4842-5992-4

Voorkomen van witwassen en terrorismefinanciering (Wwft). (n.d.). https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/aangifte_betalen_en_toezicht/wwft-voorkomen-van-witwassen-en-terrorismefinanciering/

Weeks, R. (2020). Chainalysis says BitMEX is now a 'high risk' exchange. https://www.theblockcrypto.com/post/79959/chainalysis-bitmex-high-risk-warning

Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). (n.d.). https://www.afm.nl/nl-nl/professionals/onderwerpen/wwft-wet

Wuestenfeld, J. (2020). Halving Cycles and the Bitcoin Price. https://medium.com/coinmonks/halving-cycles-and-the-bitcoin-price-7b95130f74d0



Dutch virtual currency exchanges

The overview of virtual currency exchanges can be requested from the author.

B

Origin and destination of transactions

In this appendix three different figures can be found showing the origin and destination of transactions. On the y-axis the date is shown. On the x-axis the number of transactions executed can be found. For all figures the data has been normalized in such a way that they only show the average number of transactions for one virtual currency exchange. The figure of the origin of inputs at registered exchanges can be found in chapter 5.

The figures show how the number of transactions evolve overtime when looking at the cluster in which the counterparty, the party with whom the transaction is being executed, can be found. In all figures it can be observed that the largest part of transactions either go to or come from a different exchange. The three different date stamps are adopted to identify whether an influence can be seen in the origin or destination of the transactions. Since the ”exchange” category is largely overpowering no conclusions can be presented with regards to this. Figure B.1 shows the overview of all output transactions at registered exchanges. Figure B.2 shows the overview of the input transactions at non-registered exchanges. Lastly, figure B.3 shows the overview of output transactions at non-registered exchanges.

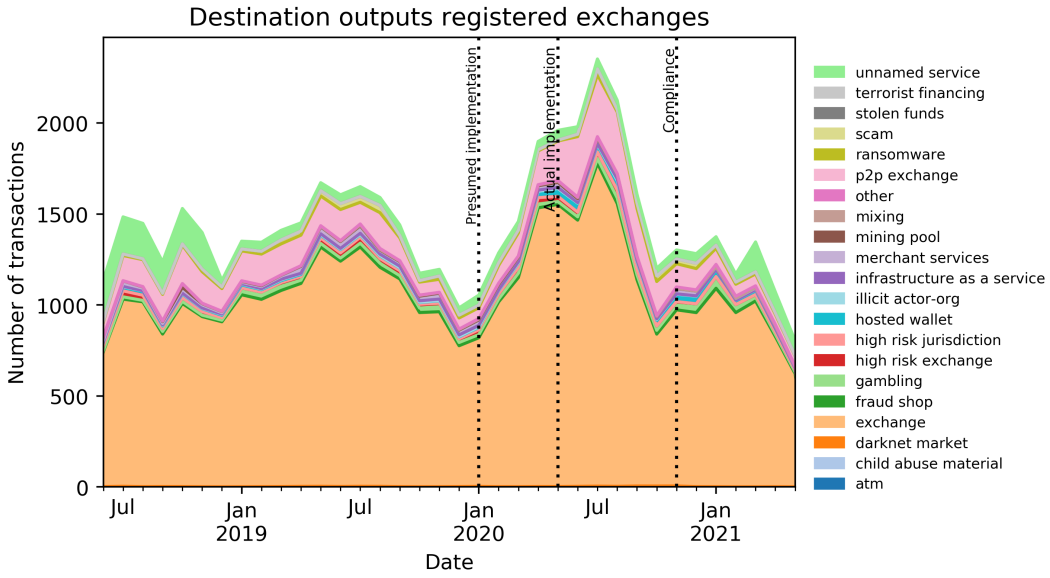


Figure B.1: Registered outputs

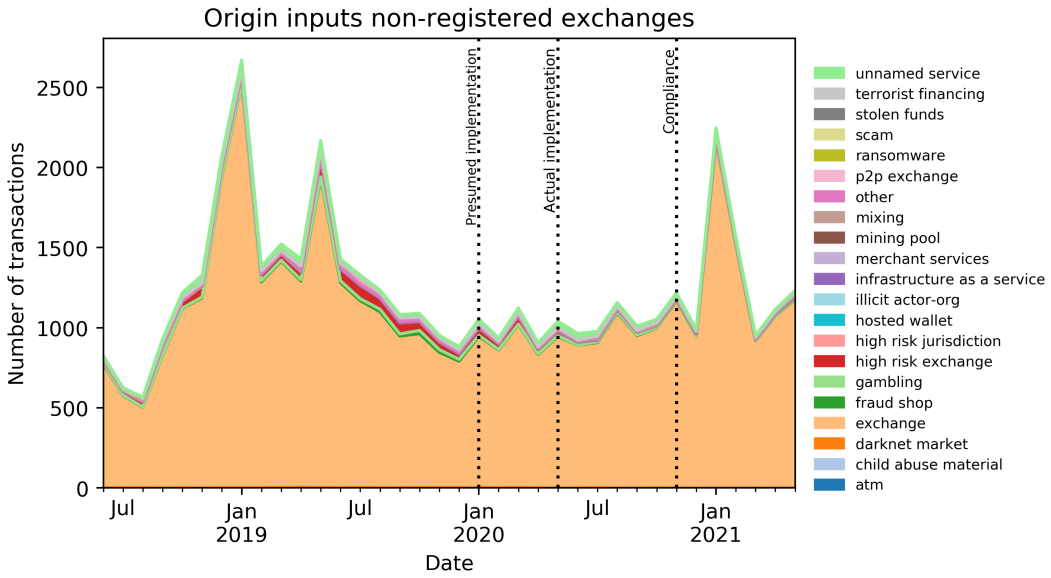


Figure B.2: Non-registered inputs

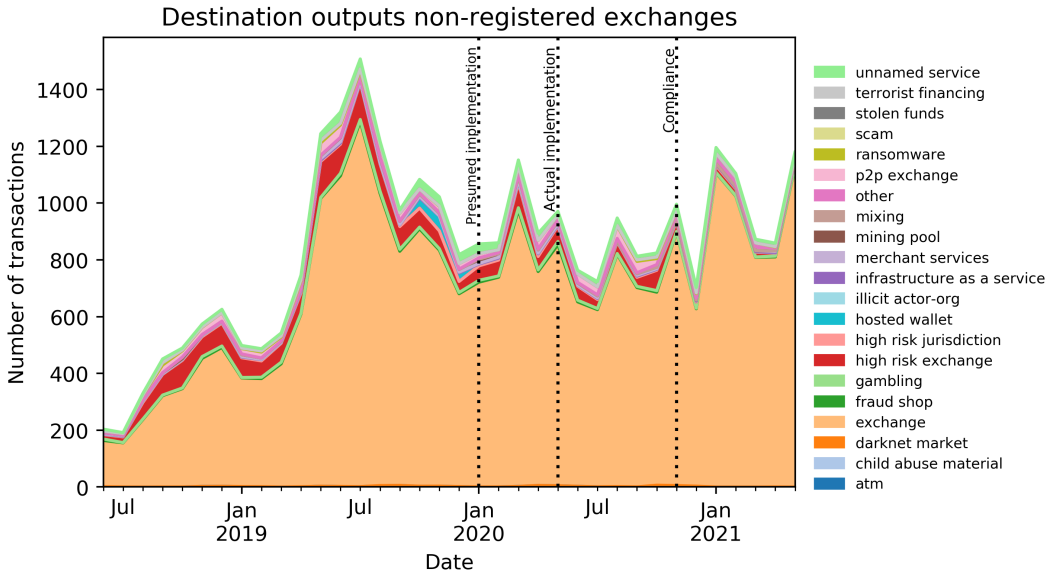


Figure B.3: Non-registered outputs

C

Interview Protocol Supervisor

This appendix shows the interview protocol that was adopted in the interviews with the supervisors of DNB. The goal of the interview was to find out how supervision of exchange services from Bitcoin to fiat currency is carried out in practice by the regulators.

Use

1. What is the potential of the use of virtual currencies in organized crime and what threat does this pose?
2. What do you come across in the flow of virtual currencies that may be prosecutable? Do you see certain patterns?

Legislation

3. What is your perspective on the introduction of the AMLD5?
4. Do you believe the legislation is effective?
5. What impact do you observe following the implementation of the AMLD5:
   (a) In the landscape;
   (b) Within your organization.

Anti-money laundering responsibility:

6. How do you describe your role within the anti-money laundering chain?

Supervision and registration

7. How did the registration process work?
8. Are there opportunities for exchanges to operate without a registration in the Netherlands and what are the effects of this?
9. Which exchanges that did apply for registration have dropped out of the registration process? And why?
10. The registry lists parent companies with their subsidiaries. Who is responsible for complying to the duty to notify and for ensuring the correct procedures are in place?
11. How are virtual currency exchanges supervised?
12. What tools are used to carry out supervision? If tools that look into the blockchain are used:
    (a) How many steps do you look back to see if a coin is tainted? After how many steps is a coin clean?
    (b) Which heuristic is adopted in this research?
13. How do you expect the system to develop over the next 5 years based on:
    (a) Tools
    (b) Coins
    (c) Legislation

D

Interview Protocol Virtual Currency Exchanges

This appendix provides the interview protocol that was adopted in the interviews with the virtual currency exchanges. The goal of the interview was to find out how exchanges have adapted their day-to-day operations in order to comply to the duty to report and Know Your Customer procedures arising from the 5th Anti-Money Laundering Directive.

Use

1. What is the potential of the use of virtual currencies in organized crime and what threat does this pose?
2. What do you come across in the flow of virtual currencies that may be prosecutable? Do you see certain patterns?

Legislation

3. What is your perspective on the introduction of the AMLD5?
4. What impact do you observe following the implementation of the AMLD5:
   (a) In the landscape;
   (b) Within your organization.

Anti-money laundering responsibility:

5. How do you describe your role within the anti-money laundering chain?
6. What did anti-money laundering tactics did you adopt before the AMLD5 implementation?
7. How did you have to adapt your daily operations after the implementation of the AMLD5?
8. What else could crypto companies do to combat money laundering?
9. What are the biggest challenges in this?
10. Does the legislation help you with your anti-money laundering responsibilities?
11. What would you need from legislation to help you?

Transaction monitoring

12. How do you apply the following anti-money laundering principles:
    (a) Know Your Customer
    (b) Customer Due Diligence
13. What tools do you use to monitor transactions? If tools are adopted that analyse the blockchain:

   (a) How many steps do you look back to see if a coin is tainted? After how many steps is a coin clean?
   (b) Which heuristic is adopted in this tool?

14. When a transaction is marked as unusual:
   (a) What do you do with this unusual transaction?
   (b) Is there some kind of feedback loop that comes back to you after you have reported the transaction?

Supervision and registration

15. How did the registration process work?
16. How should you demonstrate compliance as an exchange?
17. How are you as a virtual exchange monitored by the supervisor?
18. Are there opportunities for exchanges to operate without a registration in the Netherlands and what are the effects of this?
19. How do you expect the system to develop over the next 5 years based on:
   (a) Tools
   (b) Coins
   (c) Legislation