COMBATING MONEY LAUNDERING ON THE BLOCKCHAIN

Bachelor thesis Industrial Engineering & Management

Author

Karia, Damian

Supervisors University of Twente

R.A.M.G. Joosten

A. Abhishta

Supervisor Smilo

E. Roelen

Publication date

29-10-2019

Smilo.

UNIVERSITY OF TWENTE.

Prologue

Dear reader,

I would like to represent you my bachelor thesis about preventing money laundering on the blockchain. I conducted my research at a blockchain start-up in Almelo, Smilo. For my research I was located in Almelo at the Smilo office for 3 days per week. The other two days were at the office of 20face at the University of Twente.

I would like to thank Elkan Roelen for the assistance and the great time at Smilo, and I hope to stay closely connected.

Furthermore, I would like to thank Reinoud Joosten and Abhishta Abhishta for guiding me through the process of writing a thesis and the helpful feedback they provided to strengthen my thesis.

At last I would like to thank all the experts I talked to. Richard Hoff and Margot Aelen from 'De Nederlandsche Bank', Patrick van der Meijde from 'Vereniging Bitcoin Bedrijven Nederland', Karen Sobie Hilbert from IdentityMind, Jacques Dahan from CipherTrace and Andre Kalinowski the CEO of Parsiq for being so open and friendly to provide me with answers regarding anti-money laundering and cryptocurrencies.

I hope you enjoy reading my thesis,

Damian Karia

Abstract

Money laundering through cryptocurrencies is a growing problem in the crypto industry. Being associated with money laundering can harm a firm's business. ABN Amro's stocks plummeted after the Dutch Public Prosecution Service announced that they would investigate ABN Amro for money laundering practices (NOS, 2019). ABN Amro is not the first bank that suffered from being associated with money laundering practices, also ING and Rabobank experienced this. That is why Smilo wanted to become pro-active in tackling money launderers on their blockchain.

The goal of this research is to investigate how, and which measures can be implemented on a hybrid blockchain to prevent money laundering.

I reached this goal by conducting a desk research. In this research, literature and the visions of experts are combined. I wrote down the prevention measures for the classical money laundering system to see whether those methods may contribute to solutions for money laundering with cryptocurrencies. The prevention measures for money laundering result from the anti-money laundering regulations. Therefore, the regulations are outlined in this research as well. After the regulations for cryptocurrencies, I summarized the anti-money laundering measures from the crypto industry.
Thereafter, experts from DNB and VBNL shared their vision on regulations and the practical implications of it.

Based on the regulations, prevention measures for the classical money laundering system and the vision of the experts, I defined requirements to improve Smilo's anti-money laundering practices.

Conclusion

Smilo can prevent money launderers from their blockchain by following the next recommendations:

1. Partner with exchanges that implemented KYC measures in order to avoid criminals from easily accessing the Smilo token and thereby Smilo's blockchain.
2. Create a solid AML policy and publish it internally and externally.
3. Conduct SIRA.
4. Implement KYC measures.
5. Create a custom transaction monitoring algorithm for Smilo's blockchain, which takes the recommended features into account.
6. Report every suspicious transaction/account to the FIU with as much evidence as possible.
7. Stay in contact with crypto companies that implemented AML practices (e.g. VBNL members).
8. Join the InnovationHub from DNB & AFM.
9. Keep up to date with the FATF guidelines, as those will almost certainly be translated in national laws.
10. Investigate whether Smilo falls under VASP when tokens are sent to partner companies in the future. If Smilo falls under the term VASP, they **must** comply with AMLD5 and the Wwft. Which implies that they need to register themselves at DNB, conduct a risk assessment, conduct enhanced customer due diligence, perform transaction monitoring and report to the FIU.

Table of Contents

Definitions

Abbreviations/technical words	Definitions
AFM	The Dutch Authority for the Financial Markets
AML	Anti-Money Laundering
AMLC	Anti-Money Laundering Centre
AMLD	Anti-Money Laundering Directive (European directive)
Belastingdienst	Tax and customs administration
CFT	Combating the Financing of Terrorism
Crypto	Cryptocurrency
DNB	The Dutch central bank
FEC	Financial Expertise Centre
FIOD	The Dutch Anti-Fraud agency
FIU	Financial Intelligence Unit
MPSM	Managerial Problem-Solving Method
OM	Public Prosecution Service
P2P	Peer-to-peer
PEP	Politically Exposed Person
VBNL	'Vereniging Bitcoin bedrijven Nederland' (Dutch association of bitcoin companies)
VCRA	Virtual Currency Risk Assessment
Wwft	'Wet ter voorkoming van witwassen en financieren van terrorisme' (National law translation of the AMLD)

1. Introduction

1.1. Smilo

Smilo is a unique blockchain platform founded in 2017. Blockchain is a growing list of records which cannot be modified. Those records are usually open to everyone in order to provide full transparency. This is not desirable in every case. Take medical records for example. You want this information to be visible for the physicians and nurses, but not for others. Therefore, Smilo designed a hybrid blockchain. On a hybrid blockchain, personal information can be kept private and collective data will be publicly available. They are the first in the Netherlands who built a hybrid blockchain.

To support this technology, smart contracts have been created. Smart contracts function in nearly the same way as regular contracts. The involved parties agree on the terms for a smart contract and those terms are written in code. Afterwards, the smart contracts are stored on the blockchain. The digital protocol is automatically triggered by an event. For example, you order a laptop at a company, but you do not want to pay upfront because you are not sure that you will receive the laptop. You can agree with the company that you will pay once you received the laptop. This agreement is stored in a smart contract. Once the delivery is confirmed by the delivery service or you, the smart contract will be executed, and the money will automatically be debited from your bank account.

The creation, modification or deletion of a smart contract requires a transaction on the Smilo blockchain. Therefore, they need their own token to perform these transactions. Their own token is also called Smilo. These tokens are particularly used to process smart contracts. Smilos can be bought at partnered cryptocurrency exchanges. With these tokens, customers can also send them to each other's online wallet or change them for other cryptocurrencies.

2. Problem identification

2.1. Problem identification

Smilo collaborates with several companies. Smilo wants to keep their profile clean and they do not want to be associated with money laundering practices. Therefore, they want to secure that they can identify criminal activities on their blockchain. The reality is that only big transactions can be noted as a potential criminal transaction now, although there is no system that keeps track of these high transactions. Only by 'accident' those large transactions can be noted. It can be said that there is a big discrepancy between norm and reality. The problem owner is the CEO of Smilo. He has to make sure that the company maintains a good image. When supervising instances (e.g. DNB) identify that Smilo's blockchain may be used for criminal activities like money laundering, it will hurt the company's image.

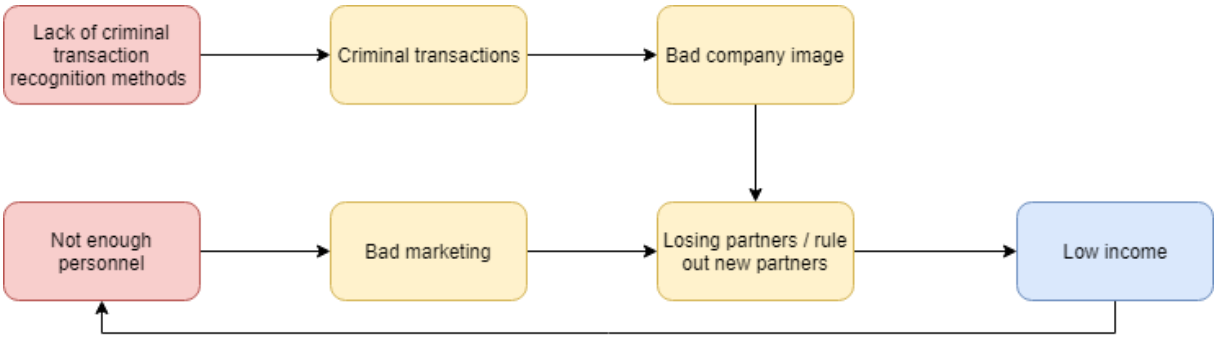

Figure 1: Problem cluster.

As we can see from Figure 1, the core problems are the ones at the beginning of the causal chain (depicted in red). Criminal transactions on the blockchain and the personnel shortages are the core problems for Smilo. The only problem that is realistic to solve is the criminal transactions on Smilo's blockchain. The personnel shortage cannot be solved, because it is a direct consequence of the low income.

With this specific problem, the number of potential criminal transactions identified is close to 0%, because only by accident big transactions are seen by a random employee of Smilo. Smilo ideally wants to identify 100% of the potential criminal transactions and report this to the FIU (Financial Intelligence Unit) and maybe even share this with the public to be completely transparent. Indubitably, it is unrealistic and impossible to identify all the criminal transactions. Because of the time limit I will only investigate the solutions to prevent transactions that are probably related to money laundering.
A supporting reason for choosing to prevent money laundering only, is because of its stake in the criminal world. The FIU collects evidence on criminal activities each year. In 2018, 53% of the collected files were related to money laundering, while the financing of terrorism occupied 20% (FIU-Nederland, 2019). Money laundering was the number one crime form in 2018 according to the FIU.

From here also the knowledge problems arises. How does money laundering work? What is the difference between regular money laundering and blockchain involved money laundering? How can money laundering transactions be recognized in cashless transactions? How can money laundering transactions be identified on the blockchain?

2.2. Problem-solving approach

The core problem is the criminal transactions on Smilo's blockchain. To reach a solution, I need certain knowledge. How do transactions work in Smilo's blockchain? How does money laundering work? What is the difference between regular money laundering and blockchain involved money laundering? How can money laundering transactions be identified on the blockchain? To get answers to these questions, I planned meetings with the CEO of Smilo, asked for the opinion of employers from DNB (the Dutch Central Bank) and I spoke to someone from VBNL (A Dutch association of bitcoin companies).
At last, some choices were made in the problem-solving approach. What kind of solution do I want to produce? Which are my data gathering methods? How do I reach out to experts? Do I produce a solution only for Smilo, or also for other blockchain companies that make use of transactions? These choices were made in the research design.

2.3. Research design

I investigate the ways to tackle criminal transactions on Smilo's blockchain. Money laundering via cryptocurrencies is a relatively new field. This was the reason for conducting an exploratory research. It is almost impossible to identify a transaction as guaranteed criminal, so descriptive research was not possible.
From the knowledge questions it can be derived that the research population is the group of people who are directly or indirectly involved with money laundering. These are the founders of Smilo, the employees of Smilo, the clients, the consumers, crypto exchanges, other crypto companies, AML solution providing companies and supervising instances. The subjects that I measured were those exact same parties.
One method of data gathering was asking the opinion of experts. I asked the opinion of experts to get answers to the questions which are noted in the problem-solving approach. The first experts I contacted were from DNB. I contacted them via a phone number from their website. The second expert I had a conversation with is from VBNL. I tried to contact experts from AML solution providing companies (Chainalysis, Elliptic, CipherTrace) as well. I successfully reached out to CipherTrace.
Another data gathering method that I used is literature study. I used literature to find answers to the same questions. This research is deep and not broad, because there was not enough time to do both. Depth was chosen, because there was not a very broad research population. It was better to dive into depth with acquiring knowledge from both experts and literature.

To process the data, I mostly used a qualitative method, because I did not gather a lot of data which can be plotted or processed in figures.
Obviously, the research design has some limitations. In advance, I knew that it was impossible to prevent all criminal transactions. Criminal transactions are not easily identifiable. Every transaction identified as possibly illegal, has to be investigated by the FIU first. This means that no factual numbers of identified criminal transactions could be generated. Given the limitation of time, I limited my research to the identification of possible money laundering transactions on Smilo's blockchain.

According to Heerkens & van Winden (2012) the assessment of validity can be divided into three parts: internal validity, external validity and construct validity.
Assessment of validity:

- Internal: Are the data I gathered valid? I needed to take into account that the opinions of experts are just opinions and that the scientific literature might differ from these opinions.
- External: Are the recommendations also valid on other blockchains? Smilo's blockchain is unique, so I had to take this into account when I wrote the Generalization Chapter 7.4.
- Construct: Are the variables and indicators in accordance with the scientific body of knowledge (Cooper & Schindler, 2014)? I needed to make sure that I used the right literature and checked the most recent literature that was available.

The assessment of reliability is just as important as the assessment of validity. The reliability of the prerequisites for the program cannot easily be assessed. As money laundering continues, new technologies and new tricks will be used. So, the list with requirements for the transaction monitoring algorithm given in Chapter 5.3. might not be up to date anymore once this research is published.

2.4. Knowledge questions

Smilo wants to become proactive in tackling money laundering practices. The research question that results from that goal is as follows:

What measures can Smilo take to combat money laundering on their blockchain?

To get an answer to the research question, several knowledge questions need to be answered first. Money launderers may use Smilo's blockchain to clean their illicit money. They can do this by making transactions on Smilo's blockchain. The first knowledge question that can be derived from the research question is:

- *How do transactions work on the blockchain?*

In order to collect prevention measures for money laundering, it is essential to know how money laundering works. I made a division in the classical money laundering system and the "new" money laundering system via cryptocurrencies. First, I wanted to find out how the classical money laundering system works and what was done to prevent money laundering in this system. This brings along the following knowledge questions:

- *What does money laundering look like in the financial market?*
- *What prevention measures are used in the financial market?*

After I found out the answers to these questions, I wanted to figure out if the prevention measures in the classical money laundering system can also be used in the new money laundering system. In order to know whether this is possible, I needed to know how money laundering works in the new money laundering system. The last step of my research was to find out which prevention measures were available for the new money laundering system. The last knowledge questions I want to answer are:

- *How does money laundering work via cryptocurrencies?*
- *What is being done to prevent criminal transactions with cryptocurrencies?*

Once the knowledge questions were answered, I started writing an answer to the research question.

3. Theoretical framework

3.1. Hybrid-blockchain

The blockchain is as the name says, a chain of blocks. Information is stored on each side of the block. It is superfluous to explain all information that is stored on a block because a variety of blockchains exist and therefore blocks differ per blockchain. To put it in simple terms, there are three important sides on each block. The hash of the previous block, the hash of the current block and blockchain specific data. A hash is a series of numbers and letters. It looks something like this:

e0353f146c84a328683d2f517f49c878a79501bca4b6180d3fbfa44cc6734aac

Every hash is unique. It identifies the block and its stored content. Each hash is built upon the previous hash. If the content of the block changes, also the hash of that block and all the other subsequent blocks in the blockchain will change. This is done for security reasons (Medium).

The data stored in the block depend on the blockchain. In Smilo's blockchain there are 13 sides on each block. One side is used for the hash of the previous block, one side for the hash of the current block and the other 11 for other information. The most important one for this research is the transaction data. These are also stored as a hash and contains: the public key of the sender, the public key of the receiver and the amount of Smilos (XSM) being sent. Smilos (XSM) are the "bitcoins" of Smilo's blockchain. Public keys are the addresses that are used to receive and send cryptocurrencies.

Before a transaction is added to the blockchain, it must be confirmed by a peer-to-peer (P2P) network. This P2P network is the group of block miners, who simply provide the computational power to add a block to the blockchain. When someone does not accept the transaction, the transaction is rejected. This most commonly happens when the transaction fee for the miner is too low. If everyone in the P2P network validates the transaction, it is combined with other transactions into a block. The new block is then added to the blockchain and the transaction is complete. The process is visualised in Figure 2.

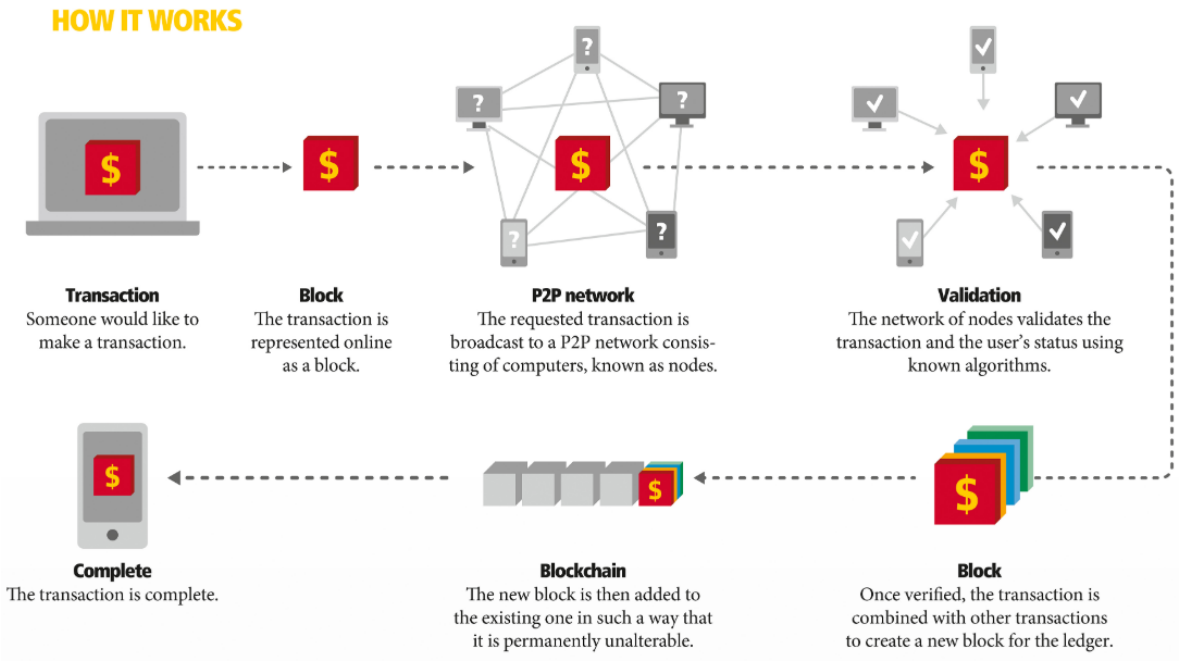

Figure 2: Validation of a transaction in the blockchain. C. Erhart, A. Gupta, (2017).

Transactions are traceable on the blockchain, but the main difference with the world of fiat currencies is that one's identity is not known (F. Xavier Olleros, 2016). In the world of fiat currencies, a transaction from one person to another (cash excluded) includes a central bank, where the identity of both persons is known. On the blockchain, no middleman is needed. That is why people call the blockchain a decentralized technology.

The blockchain is a transparent ledger. Every piece of information on the blockchain is visible for everyone, for evermore. Every public key with its whole transaction history and its holdings is forever visible on the blockchain. This level of financial transparency was unknown before and is not always desirable. Therefore, the private blockchain was invented. In private blockchains, sensitive information can be shared with trusted parties. Only the parties that have permission can access the information.

A hybrid blockchain is a combination of a private blockchain and an ordinary one. This combines the network of transparency and the option to privately share sensitive data.

3.2. Money laundering

The amount of money that is being laundered every year on a global scale is estimated on 2-5% of the global GDP by (United Nations Office on Drugs and Crime). In 2018 that equalled $1.7 trillion – $4.3 trillion US dollars (Worldbank). The lower figure represents even a bigger value than the total GDP of whole Russia. This underlines the magnitude of the money laundering problem around the world.

The definition of money laundering used by the (European Commission) is as follows: *"Money laundering is the process by which criminal proceeds are 'cleaned' so that their illegal origins are hidden. It is usually associated with the types of organised crime that generate huge profits in cash, such as trafficking in drugs, weapons and human beings as well as fraud. Although it is not possible to measure money laundering in the same way as legitimate economic activity, the scale of the problem is considered to be enormous."*

This may sound a little bit vague. Although money laundering has become more and more complex, because of digital money, the dark web and the global market, the schemes share 3 basics. Those basics are placement, layering and integration.

Placement is the first stage where illegally obtained money is introduced to the financial system (Ravenda et al., 2019). Money is converted into assets. Often, this is done by depositing funds into a bank account that is registered to an anonymous operation or a professional middleman, to avoid regulatory controls (see Figure 3).

After the placement, the second step begins. Layering is the process of distancing the funds from their illegal origin. This is done through multiple transactions through a complex web.

The last step of the process is integration. This is where the illegal money re-enters the mainstream economy. The illegal funds are converted into apparently legitimate business earnings, or luxury products are bought.

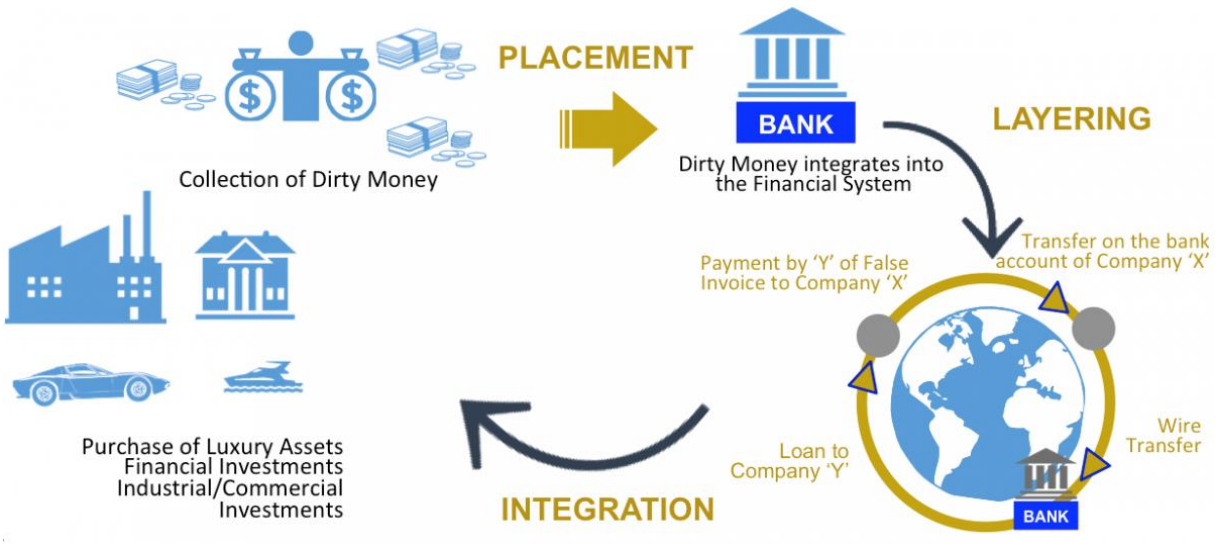

Figure 3: The three basic principles of money laundering. European Institute of Management & Finance, n.d.

3.3. Safeguarding the financial system

The first law against money laundering was introduced in 1970. This law is known as the Bank Secrecy Act (BSA). The BSA was the first act that tried to safeguard the financial system in the United States of America from abuses like money laundering (FinCEN). With this act, banks were required to report suspicious transactions, transactions over $10,000, and to properly identify persons who conduct transactions.

The BSA is the basis for following AML laws. Also, the first European Union's directive took over those basis rules. The awareness of the European Council regarding the importance of money laundering in organized crime rose. The Council was convinced that tackling money laundering would be one of the most effective means to reduce organised crime (UNION, Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering, 1991). The first EU directive against money laundering was adopted in 1991. The most important regulations were the duty to report suspicious transactions and to identify and verify clients before starting a business relation. The ways of money laundering have become very complicated and sophisticated because of technological developments like the Dark Web and cryptocurrencies. To mitigate the risk of money laundering, the European Council responds to those developments with new regulations and laws.

Laws and regulations are one side of safeguarding the financial system, but the development of software to comply with these regulations is the other side. It is a great challenge to develop software that can detect money laundering. Several investigations on how to detect suspicious transactions have been conducted. With the development of the technology, also the algorithms changed over time. A lot of different algorithms are able to detect anomalous transactions. The most recent algorithms are mostly based on machine learning and data mining. Within the machine learning and data mining domain, different methods are used (i.e. statistical-, clustering-, classification- and pattern recognition methods). Most of the algorithms use a mix of methods to accurately detect anomalous transactions and to reduce the false-positive- and false-negative outcomes. I will describe three recent anomalous transaction detecting methods to give an idea of what they look like.

CoDetect
An algorithm which caught attention in the field of fraud detection is CoDetect. CoDetect is a financial fraud detection algorithm with an anomaly feature (Huang et al., 2018). The algorithm is based on the combination of two techniques. The first one is the attribute-feature technique. This method generates data points from transactions e.g. from Company X, €2000, to Company Y. According to Huang et al. (2018) data points are generally seen as independent and identically distributed, but the researchers claim that the money laundering characteristics vary from attribute-feature data. They explain this by saying that transactions are always between two entities, which makes the data points not independent and identically distributed.
The second technique is graph-based detection. This method can detect the relations between data points. With graph-based detection, suspicious interactions between entities can be identified. Authorities can use graph-based detection to identify if entities are involved in money laundering, but not how the activities are executed. The information about how the activities are executed is mostly hidden in the data points. That is why CoDetect combines the two techniques.

Anomaly detection with machine learning and graph databases
The algorithm used the nearest neighbour heuristic in combination with “volcano” and “black hole” patterns. Suppose we have a network of entities that send transactions to each other. In a money laundering network, there can be so-called “black holes”. This refers to the entities that chiefly have incoming transactions and no outgoing transactions (Magomedov et al., 2018). The money is absorbed by those “black holes”. “Volcanoes” on the other hand particularly have outgoing transactions. On the basis of those principles an algorithm is developed to detect those black holes and volcanoes. This is important to map money laundering networks. In Figure 4 you can find an example of a volcano and a black hole. Note that not every volcano is marked in the figure.

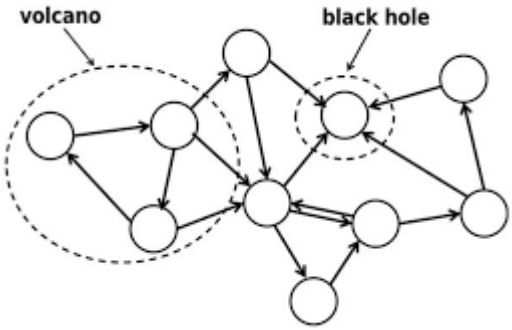

Figure 4: Example of a "volcano" and a "black hole". S. Magomedov et al., (2018).

SARDBN
SARDBN (Suspicious Activity Reporting using Dynamic Bayesian Network) is a method that uses a combination of distance based clustering and dynamic Bayesian network to detect anomalies in a sequence of transactions (Raza & Haider, 2011). The idea behind this method is that the overall monthly transactions of a customer form a pattern. Customers with similar patterns are classified in the same cluster. When a customer’s pattern deviates from these patterns, it is marked as suspicious. This method identifies anomalies in sequences of transactions instead of single transactions. A transaction may look normal on its own but may be anomalous when the corresponding sequence is tracked. This method differentiates itself from other methods, because it looks at abnormalities in transaction sequences instead of single transactions.

There are many more methods that use different perspectives on how to identify anomalous transactions (e.g. Rao & Kanchana’s Dynamic approach (2018), Jayasree & Balan’s Probabilistic relational audit sequential pattern (2015) or Larik & Haider’s clustering approach (2011)), but there are simply too many of them to describe them all.

3.4. Money laundering on the blockchain

The pseudo-anonymity character of bitcoin led to illegal use cases. For instance, bitcoin was the only accepted payment method on the illegal online market Silk Road, where drugs, weapons and other illicit goods were sold (Campbell-Verduyn, 2018). This shed light on the possibilities of cryptocurrencies for criminal purposes and awareness for money laundering practices with cryptocurrencies was created.

Money laundering on the blockchain contains the same three basics as in classical money laundering. The first step is the placement of money. Dirty money is collected and introduced into the financial system. The way in which this is done differs from the classical way.

3.4.1. Placement

Five methods for placement are known. Three of them are conducted when a criminal wants to clean dirty cash. The other two methods are used when the criminal has dirty money in the form of electronic money.

Dirty cash

The first method for cleaning cash is to buy cryptocurrency person-to-person on the street (AMLC, Witwasindicatoren, 2017). Meetings can be organised at places without cameras to ensure anonymity.

The second method is buying cryptocurrency at a cryptocurrency ATM (OECD, 2019). At this ATM, only a few different coins can be bought. First the amount of cash someone wants to convert into their preferred cryptocurrency need to be entered. Secondly, a new paper wallet should be generated by the machine to avoid using the same addresses (Coin ATM Radar). Depending on the ATM, verification is only needed from an ATM specific amount of money. The verification can be in the form of an SMS verification or an ID scan (Coin ATM Radar). Some ATMs do not require any kind of verification up to €10,000. This means that someone can just buy less than €10,000 worth of cryptocurrency every time, until all the dirty cash is in the system, while staying completely anonymous. Another option to stay anonymous is to use a fake ID and a phone which is not coupled to any personal information.

The third method is buying prepaid cards (e.g. gift cards, cards with calling credits or credit cards) and converting them into cryptos (Odinot et al., 2017). Those can be bought at most supermarkets and pharmacies. Once the prepaid cards are bought, criminals can sell those cards for their favoured cryptocurrency at P2P websites.

Dirty e-money

It is also possible that a criminal got the funds in the form of e-money. In this case there are two possible ways to obtain cryptocurrencies while protecting one's anonymity.
The first option is to use an exchange where no personal verification is required. There are a few exchanges that do not require any verification at all to trade, but there are also a few exchanges on which someone can trade up to a certain amount of money per day, without verification.

The second option is to use a P2P exchange and convert the electronic money into a cryptocurrency.

Aside from these methods, criminals can also have obtained cryptocurrencies directly via dark web marketplaces, by selling drugs, weapons or other illicit goods.

3.4.2. Layering

After the dirty money is spread over different cryptocurrency addresses, the layering stage begins. In this stage the funds are being laundered further, to distance them from their illegal origin. A typical method that is used to facilitate this is the cryptocurrency mixer, also called 'tumbler'. Before the mixer is being used, users safeguard their anonymity by making use of VPNs, the Tor Browser or other methods which block the opportunity to trace back the user's activities (Dyntu & Dykyi, 2019). The crypto mixer is a service which pays out the user from their reserve pool, which is created by earlier users. The user enters the address(es) on which the cryptocurrencies need to be received. To provide anonymity, some randomness is generated in the form of a transaction fee, the division of the amounts and the pay-out over time (van Wegberg et al., 2018). Users are able to adjust this randomness by simply sliding some bars. When everything is filled in, the user only has to send the cryptocurrencies to the address(es) provided by the tumbler and the rest is done by the mixing service.

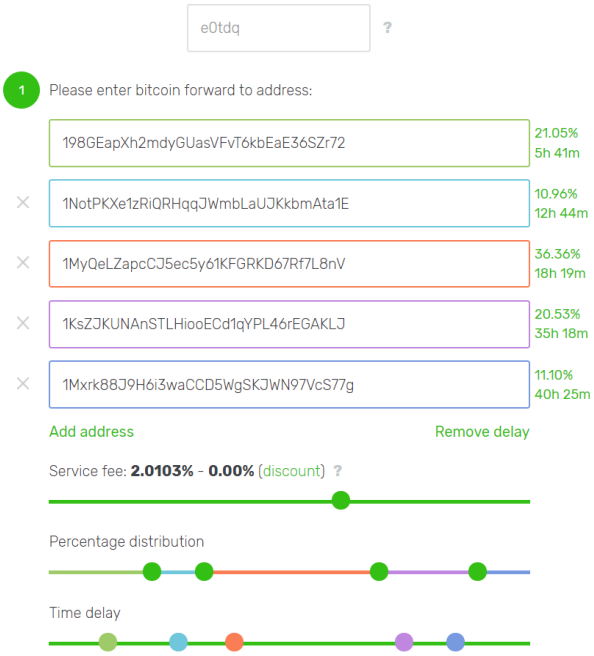

Figure 5: Example of a cryptocurrency mixing service from: https://cryptomixer.io/.

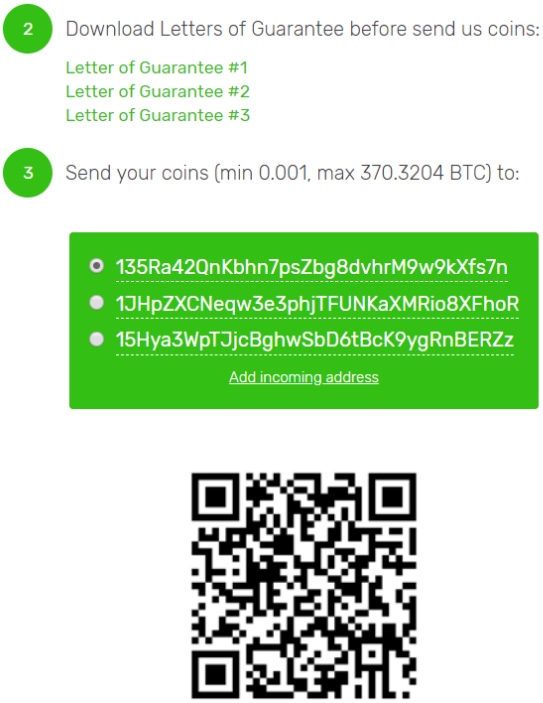

Figure 6: Example of a cryptocurrency mixing service from: https://cryptomixer.io/.

Mixing services make it very hard for forensics to trace the cryptos back to the money launderer. There is a special option for people who use the service more than once. A key is generated every time the mixing service is used. This key is unique (e0tdq in Figure 5). When someone uses the mixing service again, this key can be filled in. This assures that the cryptos someone deposited the previous time will not come back to the same person. Money launderers want to avoid this, because it may connect information which can be useful for forensics. The same holds for the reuse of addresses. Once an address is used, using it a second time might be very helpful for forensics to detect the money launderer. Although the mixing method sounds sophisticated, de Balthasar & Hernandez-Castro (2017) discovered that tumbling services can have serious privacy and security limitations.

Another method that is used in the layering stage is called CoinJoin. This method brings together (joins) the coins of different users into one transaction. A number of users (X) agree on a certain output size (Bitcoin Wiki). Then they all send at least the agreed amount of coins as an input for the transaction (the exceeded amount will be returned as change to the sender). Once everyone has sent their coins, the transaction will have X outputs of the agreed size and a maximum of X more outputs if users exceeded the amount of coins they agreed on. This implies that everyone receives the

amount of coins agreed on. Once the transaction is done, it is hard to trace who received which coins. A simple example is given in Figure 7 where X = 2. Let's take a look at transaction 2. Suppose that 1A1 is the address from Alex and 1C3 is the address from Chris. Alex and Chris agreed to CoinJoin 0.8 BTC. Alex combines two inputs, one of 0.5 BTC and one of 0.3 BTC. Chris sends an input of 0.8 BTC. There are two outputs, 1D4 and 1E5 of both 0.8 BTC. From this moment it is hard to identify who received which coins. The level of anonymity increases with the number of users that agree on an output size for a CoinJoin transaction.

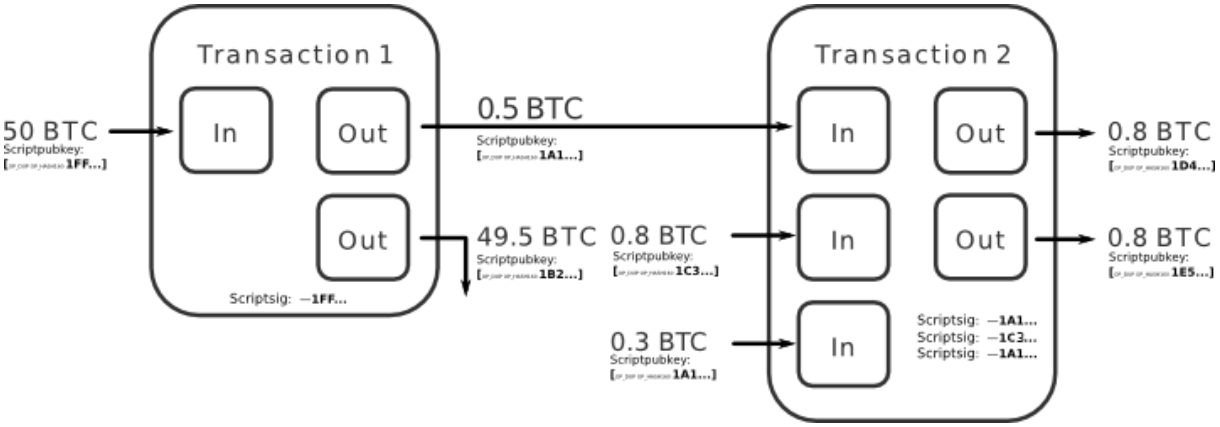

Figure 7: CoinJoin example. Bitcoin Wiki, (2013).

To further launder the money, cryptocurrencies can be converted into anonymous cryptocurrencies. This can be done on exchanges where no verification is needed. Anonymous cryptocurrencies, also called 'private coins', are secure, private and untraceable. The most popular private coins are Monero, Dash and Zcash.

3.4.3. Integration

Criminals can now either keep the cryptocurrencies or cash out. Cashing out can be done in the same ways that are used in the placement stage. Money launderers can sell their cryptocurrencies via P2P exchanges, at a cryptocurrency ATM which does not require identification or on the street for fiat currencies.
Other options are buying prepaid cards with the cryptos (Odinot et al., 2017) or investing in online casinos with weak customer verification (OECD, 2019). The criminals balance at the online casino can be withdrawn to a bank account or to prepaid cards. The criminal can now either sell the prepaid cards for money or pay other criminals with it.

The next step is either extending the transaction trail to disguise the illicit path or to spend the money. Criminals who launder money, often own enough money to afford a lavish lifestyle. They buy luxury products like cars, art and big houses.
Although the money appears to be clean, it is suspicious if somebody suddenly buys a lot of new expensive products. Therefore, criminals are more likely to invest the money first. 'Legal wealth' is slowly generated by investing in companies and mixing the company's money with the illegally obtained money. This is done by generating fake bills and fake invoices. Let's say a criminal owns a furniture company. This company buys 500,000 euro worth of materials from their supplier, but supplier invoices 200,000 euro worth of materials. The company sells the material for 500,000 euro, thus 300,000 euros of legal profit is generated. This 300,000 of legal profit obviously does not exist, because only the invoice is changed. In this way 300,000 euro of the illegally obtained money can now be spent completely legally, because it looks like this was generated from the company's profits. More complex methods for the integration of 'clean' money into legitimate businesses are used. The

assistance of financial experts is required in criminal networks, because they have unique skills and expertise (Soudijn, 2012).
Further investment options are real estate, stocks and securities (OECD, 2019).

3.5. Identification measures for money laundering on the blockchain

3.5.1. Legislation

Bitcoin was founded in 2008 by a group or a single person under the pseudonym Satoshi Nakamoto. It was the first decentralized coin that worked without a central bank, and solved the double spending problem (Maksutov et al., 2019). The technology behind bitcoin was ground-breaking and it inspired other people to expand this technology. New cryptocurrencies like Litecoin and Ripple were created. The rise of cryptocurrencies led to the founding of many cryptocurrency exchanges. Most of them were based in New York, until legislation restrained those exchanges. In 2014 the state Department of Financial Services introduced BitLicense, a bill which stated that companies who deal with virtual currencies had to comply with several rules (Department of Financial Services). Exchanges had to collect a ten year record of all their customer transactions, a customer identification program and other privacy invading data to apply for BitLicense (Campbell-Verduyn, 2018). Some cryptocurrency exchanges feared the privacy of their customers and felt restriction on innovation (Brave New Coin). That is why multiple crypto exchanges (e.g. Bitfinex, Kraken and Poloniex) left New York. They moved to places where legislation was not an issue for crypto exchanges. This was a sign that cryptocurrencies needed to be regulated on international level instead of national- or even state level to be effective.

The Financial Action Task Force (FATF), an intergovernmental body with 37 member states and two regional organizations, focusses on combating money laundering (FATF). In 2015 they wrote global guidelines with a dual purpose to help identifying money laundering threats posed by cryptos and to aid national authorities to develop a legal framework to support global AML efforts (Campbell-Verduyn, 2018). The FATF guidelines suggest targeting the nodes that are most likely to be the forefront of money laundering. Exchanges are the link between fiat currencies and virtual currencies, which makes them a good target for regulations. FATF suggested that exchanges should execute due diligence efforts, to know their customers (KYC).
The guidelines of FATF are followed by the European Parliament and the European Council. The European Parliament and the European Council published AMLD5 in June 2018. In this directive it became clear that exchange services between fiat currencies and virtual currencies, as well as custodian wallet providers fall under Directive (EU) 2015/849 from the 10th of January 2020 (European Union Law). This means that crypto exchanges and custodian wallet providers have to implement KYC methods to identify and verify their customers, monitor all transactions, report suspicious transactions and need to be registered at one or more instances. They need to comply with the law before the 10th of January 2020.

At the beginning of 2019, AFM and DNB wrote a complementary joint advice. The AFM and DNB wanted a national licensing regime for crypto exchange platforms and crypto wallet providers, instead of only registering them. By creating a national licensing regime, they wanted to create a safer market. With those licenses, potential market parties can be assessed - and rejected preventively (AFM).
This advice was backed up by FATF and in addition to AFM's and DNB's joint advice, the FATF wrote new guidelines for VASPs (Virtual Asset Service Providers).

"Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

1. *Exchange between virtual assets and fiat currencies;*
2. *Exchange between one or more forms of virtual assets;*
3. *Transfer of virtual assets;*
4. *Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;*
5. *Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset."* (FATF)

Suppose a transaction happens between two customers on two different VASPs. FATF suggests that these VASPs should both know the identity of the two customers, the account numbers of both customers and data that uniquely identifies the sending customer to the ordering VASP when a transaction of 1000 USD/EUR from VASP to VASP is performed (FATF, 2019). These suggestions are also known as the Travel Rule. Furthermore, FATF suggests that the supervision of supervising instances should be expanded to VASPs.

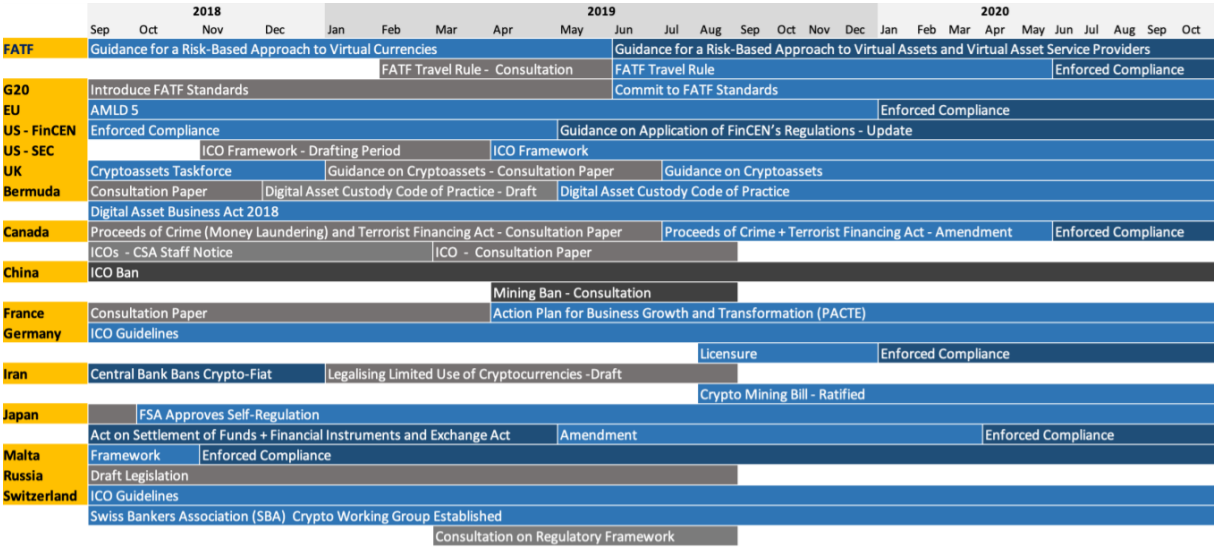

Figure 8: Global cryptocurrency AML timeline. CipherTrace, (2019).

In the last years, a lot of new laws and regulations around cryptocurrencies have been designed, see Figure 8. The guidelines around cryptocurrencies are updated continuously, while money laundering structures change constantly. The cross-border characteristics of cryptos make them hard to regulate and require international regulation in order to be helpful in fighting money laundering practices. Intergovernmental bodies like FATF are very essential to combat money laundering practices where cryptos are involved. Besides guidelines and legislation, algorithms and software must be created which can execute the rules and laws.

3.5.2. AML practices

Cryptocurrencies have been a real hype in 2013 because of their controversial applications. Since that moment, governmental bodies felt the urge to come up with legislation around cryptos to minimize the risks of fraud, money laundering and financing of terrorism. But not only was there an urge for legislation, also an urge for innovation was born. Innovative start-ups from all around the world have been founded to mitigate the risk of money laundering and identity fraud.

One company that wants to combat money laundering and identity fraud is IdentityMind. Since 2013 they have been active in fighting financial crime. IdentityMind provides an all-in-one AML compliance. They provide Know Your Customer (KYC) solutions, monitor transactions and sanctions screening. IdentityMind has some big clients from the cryptocurrency industry. Two of them belong to the largest crypto exchanges (i.e. Huobi and Binance). Crypto exchanges are a big target for

hackers because of the great volumes of money traded each day. Although most crypto exchanges have a solid security system, hackers are successful in hacking a crypto exchange on a regular basis. Once hackers possess the cryptocurrencies, they try to make them untraceable and mix them with other cryptocurrencies. Hackers often use CoinJoin and crypto mixers to make the stolen cryptocurrencies harder to trace. After an exchange is hacked, an investigation is started to trace back the stolen cryptos and find the thieves. Exchanges often do not get the right expertise to perform such investigations. That is why third parties step in. Chainalysis helps crypto exchanges and governments to trace the stolen cryptos. They investigate the transaction chain and try to identify the suspects. In the big Mt. Gox hack Chainalysis traced back 650,000 missing bitcoins (Forbes). In the crypto world they are well known for their anti-crypto crime missions.

Methods that tackle money laundering cannot lack in the fight against financial crime. Governments, supervising instances and scientists became increasingly interested in a variety of those methods to combat money laundering. Since the foundation of Bitcoin, a lot of research has been conducted on Bitcoin and its consequences. Bitcoin was commonly associated with a certain amount of anonymity, but Yin et al. (2019) put the degree of anonymity in a more accurate perspective. Bitcoin's anonymity is not as high as what people previously thought. The machine learning approach from Yin et al. even showed that the potential owners of a certain Bitcoin address could be narrowed down to a certain degree.

Narrowing down the potential owners of a Bitcoin address was done earlier. Juhász et al. (2018) developed a mathematical model using naïve Bayes classifiers which could establish which clients were most likely to control a certain Bitcoin address. They linked IP addresses to Bitcoin addresses of clients. This made it possible to track down the geographical location of the clients.

Even the anonymizing methods that disguise transaction paths are not as secure as one might think. Maksutov et al. (2019) also developed a mathematical model. Their research showed that tracking transactions in tumblers which use CoinJoin transactions as well as regular transactions is a feasible task.

The possibilities to combat money laundering practices are growing, but so are the money laundering methods via the blockchain. The decentralized character of the blockchain makes it attractive for criminals to clean their money. Therefore, it is utterly important that regulations are reviewed on a regular basis, that supervising instances as well as crypto businesses share information, proactive instances in fighting money laundering practices keep updating their strategy and scientist keep exploring the blockchain technology and their consequences.

3.5.3. Opinion of experts

3.5.3.1. De Nederlandsche Bank

As mentioned in Section 3.5.1. the fifth Anti-Money Laundering Directive (AMLD5) was published in June 2018, but the directive will become operative from the 10th of January 2020. In this directive, the biggest changes occurred for crypto exchanges and custodian wallet providers. Previously, they were not under any supervision because they occupied a new market segment. The most important consequences of AMLD5 regarding crypto exchanges and custodian wallet providers are summed up below. From the 10th of January 2020, they need to:

- Draw up and note risk assessments (Brugman & Tonino, 2019).
- Conduct customer due diligence.
- Monitor customer transactions.
- Report suspicious transactions at the NFIU (Dutch Financial Intelligence Unit).

- Ensure that they have adequate policies to mitigate and control the risks of money laundering and the financing of terrorism.
- Register themselves at (at least one) supervising instance.

The last consequence requires an instance that supervises those particular crypto companies. Heretofore, there was no instance in the Netherlands that supervised any crypto company. In the Wwft, DNB is assigned to supervise the crypto exchanges and custodian wallet providers in the Netherlands.

Thanks to Corina Ruhe, spokesperson of DNB, I got in contact with two supervisors from DNB, Richard Hoff and Margot Aelen. Both supervisors at DNB were willing to talk with me about cryptocurrencies, their potential risks for money laundering practices and the ways to minimize the risk of money laundering at crypto companies.

Point of view on cryptocurrencies
DNB sees a lot of risks in cryptos. They warn consumers, just like AFM does. They do this because cryptocurrencies are really volatile and therefore not have a fixed value. In the meantime, DNB also warned for the misuse of cryptocurrencies for practices like money laundering and the financing of terrorism. This is due to the (pseudo) anonymity that some cryptos have.
On the other hand, DNB does not want to limit the innovation that cryptocurrencies bring along. That is why DNB got a joint initiative (i.e. InnovationHUB) with AFM where crypto companies and companies that work on innovative solutions to pay are brought together. Here they discuss their goals, the supervision on crypto companies, and ways to responsibly integrate their companies into the Dutch market.

Supervising Wwft
Companies under DNB's supervision got the responsibility to monitor transactions, detect suspicious transactions and perform due diligence measures. DNB oversees if those instances are doing this in an accurate way. The supervision tests on two different aspects. The first aspect is the client-risk-assessment of a company. What measures are executed by those companies in order to detect suspicious clients? Examples are place of residency checks, background checks and comparing the product clients buy in comparison with their profile. The second aspect is testing how transactions are monitored. In practice there are multiple solutions for monitoring transactions. This reaches from small businesses that record all their transactions by hand on paper, to large businesses with automated monitoring systems that are based on algorithms which can identify suspicious transactions. The monitoring methods are business specific but should be powerful enough to recognize suspicious transactions.
In addition, FIU has a list of money laundering typologies for cryptocurrencies which directors need to recognize in their own business. An enhanced version is published in OECD's (2019) money laundering awareness handbook (see Appendix B). DNB inspects if companies are able to recognize those money laundering typologies, but also takes the uniqueness of the business into account. Every instance has a different variety of customers and sells other products. Consequently, each instance has a different risk-profile. Companies that only have domestic transactions got a different risk-profile than companies that also perform international transactions.

DNB works with multiple other organizations to achieve sound supervision. An example is the partnership at FEC (Financial Expertise Centre). FEC is a partnership between authorities who all have different roles. These roles cover supervision, controlling, prosecution and investigation. In this partnership DNB works together with AFM, OM, Police, FIOD, the 'Belastingdienst' (Tax and customs administration) and the FIU. Every authority has their own role in the partnership and therefore brings their own piece to the puzzle. Information sharing is necessary to create the bigger picture and

to find the core problems. Together with DNB's partners, they talk about which money laundering methods exist in the world of crypto.
Therefore, they also meet with companies from the crypto sector to talk about what they see happening in and around their business. These meetings often yield important information. From these meetings DNB learned that alarm bells should ring when people do odd things with mining fees, when people use mixers to anonymise the origin of their funds and when people anonymise their transactions in other ways.

National registration system
AMLD5 states that crypto exchanges and custodian wallet providers need to register themselves at at least one instance, but DNB and AFM warned the legislator that this method still contains high risks. They think that crypto exchanges and custodian wallet providers should visit DNB before they become active on the market or before they obtain a registration.
The European directive further states that directors of crypto exchanges and custodian wallet providers need to be tested on reliability and suitability. In addition to that, DNB wants to know who the directors are, what they do, what they are planning to do and how they will comply with the Wwft. In this manner DNB has supervision on who they are and can sketch a risk-profile. It is a way to test whether the parties take the laws seriously and to assess if DNB wants them active in the market.

On the 2nd of July 2019 the bill was sent to the Dutch House of Representatives. In this bill is stated that the previously recommended national licensing system will change into a national registration system. Two requirements for registration are mentioned in the bill. The first requirement regards the correctness of the delivered documents from the submitter (Hoekstra, 2019). The second requirement concerns the reliability and suitability of the directors. The latter is in line with Article 47(2) of the fifth Anti-Money Laundering Directive. DNB needs to be convinced about the correctness of the delivered documents and have to trust the directors in order to approve the registration.

Detecting money laundering transactions
DNB is in their last preparation phase before their supervising role starts at the 10th of January 2020. Consequently, DNB has no supervision yet on the crypto exchanges and custodian wallet providers and is therefore not entitled to take any kind of action. Therefore, it is hard to know what kind of solutions those particular crypto companies implemented or will implement.
However, there are foreign countries which already have a registration/licensing system. This makes it plausible that in those countries crypto businesses are located which already have a solution for detecting money laundering transactions.
Furthermore, in the regular financial market are some money laundering detection algorithms. However, it is not easy to translate money laundering detection methods from the regular financial system to blockchain compatible algorithms. This is due to the uniqueness of algorithms. Algorithms are most of the time not scalable. A private bank will use a different algorithm to detect money laundering than retail banks or wholesale banks. Algorithms differ because every company has a different customer base, different products or services and operates in different countries.

Expectations from the other crypto companies
DNB was assigned to supervise custodian wallet providers and companies that change fiat currencies for cryptocurrencies and vice versa. This means that other crypto companies simply are not covered by their supervision and no specific action is expected from those companies. Although there are no direct legal expectations, the crypto market will almost certainly have their expectations from the other crypto companies. Wwft requires crypto exchanges and custodian wallet providers to conduct risk analysis on their customers. This probably stimulates other crypto companies to create a reliable profile. These crypto companies will indirectly be stimulated to apply money laundering- and terrorism financing prevention measures.

Furthermore, the general laws hold. This means that no one is allowed to be involved in money laundering or the financing of terrorism practices. Again, this will be a stimulator for companies to think about solid AML/CFT policies.

Advice for the other crypto companies to combat money laundering
The FIU is actively creating typologies to think about/identify manners where cryptos are used for money laundering structures. With those typologies a risk-profile for companies can be developed to assess the chance of getting unknowingly involved in money laundering practices. The first advice is to create a risk-profile.
The second advice is to find published investigation- and lawsuits, where money laundering practices via cryptocurrencies are explained. Those cases must be read, and company owners must think about ways to prevent that the same thing will happen to their company.
The last advice is to talk with other companies in the crypto sector. Information can be shared with each other and solutions for combating money laundering can be generated.

Stricter plans
FATF has expanded their standards for combating money laundering at the 1st of June 2019. With these new standards, member states are required to expand the spectrum of crypto companies under their supervision. FATF wants that every VASP will become part of the supervision.
FATF has no legal power, but they have enough authority. Which means that member states will translate their standards into laws and regulations either way. The Kingdom of the Netherlands and other member states of FATF have committed on the highest political level to implement FATF's standards and translate them into national laws. Member states are audited on this by FATF. The auditing leads to a score which give member states a better or worse access to payments with other countries. For member states there depends a lot on those scores. That is why we can say with a significant certainty that The Netherlands will translate new FATF standards into national laws.

Magnitude of money laundering via cryptos
Cryptos have characteristics which make them attractive to money launderers. When those characteristics exist in financial methods, it is almost certain that those methods will be used by money launderers. In the regulated world it becomes harder and harder for criminals to launder their money, while regulations tighten. This creates a shift to money laundering with cryptos, which makes it a serious issue. The size of the problem at this moment and the size of the problem in the future, is hard to measure. However, the risks of money laundering via cryptocurrencies should not be underestimated and be mitigated as much as possible.

3.5.3.2. VBNL
VBNL is a Dutch association of nine bitcoin companies which are proactive in combating money laundering practices, financing of terrorism and fraud. They have monthly meetings to address those issues and to foster self-regulation.
I contacted the chairman of VBNL, Patrick van der Meijde, one of the founders of BitKassa. Patrick was willing to answer some questions regarding the implementation of the Wwft into the member bitcoin companies of VBNL.

Complying with the Wwft
This moment (31st of July 2019) members of VBNL do formally not need to comply with the Wwft yet. However, VBNL expected that regulations would follow in the future. VBNL members therefore tried to mitigate the risk of money laundering and financing of terrorism practices. Because of their proactive actions, they are already largely compliant with the upcoming Wwft.
The first measure that members of VBNL already implemented is the risk-assessment of clients. Clients are assessed on different factors. Is the country where the client was born a risk? Or the

current geographical location of the client? Is the client a politically exposed person? Which payment method is used? How is the transaction volume over time? Which IP-address(es) is/are used? Furthermore, a blockchain analysis is executed to find suspicious transaction behaviour. All these factors are combined to form a risk-assessment of the client.

Another implemented measure is due diligence. Every VBNL member applies its own due diligence measures. Some VBNL members developed their own KYC solutions and others outsourced it. Not every third party is fully reliable. It has happened more than once that VBNL discovered false identification documents during document verifications which were not detected by banks or companies that were specialized in KYC.

The last measure is the monitoring of transactions. The implementation of this measure also differs per VBNL member. Every member has their own implementation of transaction monitoring and developed this by themselves. A list of factors is here observed as well. The first factor is the transaction volume. Not only the transaction volume per transaction, but also the transaction volume over time is checked. The second factor is the used IP-address(es). When this changes every time, someone is probably trying to hide the real IP-address. Using a VPN, proxy or TOR can interfere with linking the crypto-address to an IP-address and therefore also the geographical location cannot be unraveled (Juhász et al., 2018). The third factor is the used payment method of the client. The last factor is the blockchain analysis, where suspicious patterns or transactions are tracked down.

Each member of VBNL decided for themselves which actions were required to comply with the new Wwft. VBNL members shared information with each other to make the application of the measures easier. Additionally, members of VBNL had contact with investigation services and other companies on a regular basis to see which needs arose from practice.

Necessity for wider AML measures

In theory the KYC, AML and anti-fraud measures of VBNL members are applicable to other crypto companies as well. But the question whether it is necessary to implement those measures at a broader scale into the crypto sector arises. Crypto exchanges and custodian wallet providers are the crypto companies that act between fiat currencies and cryptocurrencies, this cross-border acting brings along a certain amount of risk. Not all of the crypto companies in the crypto sector form a risk for money laundering or financing of terrorism.

4. Current situation

4.1. Responsibility

Smilo's business model is letting companies use their blockchain. To perform transactions on the blockchain, tokens are needed. Those tokens are called Smilo's (XSM). Smilo therefore owns virtual currencies. Virtual currencies should not be confused with electronic money (UNION & PARLIAMENT, Directive (EU) 2018/843 of the European Parliament and of the Council, 2018). The difference between the two is that electronic money does not change the value of fiat money (i.e. dollars, euros, etc.) and virtual currencies do not have the same value as any fiat currency. Smilo only owns virtual currencies, which means that Smilo is not an electronic money entity. That on its own implies that Smilo does not have a supervising authority like DNB or AFM, while there is no supervising authority for crypto companies in the Netherlands yet (September 2019). The first European guidelines to regulate crypto companies were published in AMLD5 (the fifth Anti-Money Laundering Directive) in June 2018. The European guidelines suggest that crypto exchanges and custodian wallet providers need to implement certain AML measures before the 10th of January 2020. The proposed Money Laundering and Terrorist Financing Act (Wwft) assigned DNB as supervisor for crypto exchanges and custodian wallet providers starting at 10th of January 2020.
Smilo is not a crypto exchange nor custodian wallet provider. This means that the Wwft is not applicable to Smilo. Therefore, Smilo will not be obliged to report suspicious transactions, monitor all their transactions nor are they required to exploit customer due diligence.

Although Smilo is not obligated yet and in the near future to report suspicious transactions, they want to become proactive in tackling money laundering practices and want to be prepared for stricter regulatory requirements.

4.2. Absence of AML policy

Presently, no actions are taken to prevent money laundering practices at Smilo. This is due to the lacking AML policy. Until recently, it was not one of Smilo's priorities to implement an AML policy and to take AML measures. At the moment there are no due diligence measures and there is not a specific model or program that can detect suspicious transactions on Smilo's blockchain. The current way of detecting suspicious transactions is by checking the transactions on Smilo's blockchain sometimes. This detection method is undoubtedly inefficient and can be improved by either implementing software or creating a method which is based on scientific literature.

5. AML improvement measures

5.1. Requirements

To find a solution to the research problem "*What measures can Smilo take to combat money laundering on their blockchain?"* requirements to this solution should be set first. The first requirement is an AML policy at Smilo. This AML policy should be based on the Wwft and AMLD5. The measures that are written down in this law and guideline should be implemented at Smilo in order to become effective in combating money laundering practices on the blockchain. As I mentioned in Chapter 3.5.3.1. crypto exchanges and custodian wallet providers need to:

- Draw up and note risk assessments (Brugman & Tonino, 2019).
- Conduct customer due diligence.
- Monitor customer transactions.
- Report suspicious transactions at the NFIU (Dutch Financial Intelligence Unit).
- Ensure that they have adequate policies to mitigate and control the risks of money laundering and the financing of terrorism.
- Register themselves at (at least one) supervising instance.

The latter point is not applicable to Smilo, while only custodian wallet providers and crypto exchanges can register themselves at DNB. The other bullet points should be seen as requirements for Smilo's AML policy, to effectively tackle money laundering practices.

Smilo's risk assessment

It is important to know in which ways Smilo is exposed to risks. In which ways can Smilo's network be misused for illegal activities like money laundering? What are the types of customers Smilo serves? Where are these customers geographically located? Which products and services are offered? The biggest risk of Smilo's network being misused is by people who get Smilo tokens via a partnered crypto exchange or custodian wallet provider. People can only get access to Smilo's blockchain when they possess Smilo tokens themselves. This means that Smilo tokens must be sent from an exchange or custodian wallet provider to a Smilo wallet to make use of Smilo's blockchain, while Smilo tokens on exchanges and custodian wallet providers are managed by the exchange's wallet or custodian wallet provider's wallet. In other words, if you own coins on an exchange or custodian wallet provider, those coins are in reality possessed by the exchange's wallet or custodian wallet provider's wallet. From the moment you send the coins to a Smilo wallet, the coins are owned by you. Once that state is reached, Smilo's blockchain can be used for money laundering and other criminal activities. At this moment, unlimited amounts of Smilo wallets can be generated anonymously. This decision was made by Smilo to increase the privacy of their users. This has also a downside, while criminals can also act anonymously on Smilo's blockchain. The most evident solution to this problem is to implement customer due diligence methods.

Requirements for the risk assessment:

- Identify the ways Smilo's network can be misused.
- Determine customer types.
- Determine geographical location of customers.
- Determine which products and services are offered.

Customer due diligence

The first question in specifying the requirements for customer due diligence is; which customers does Smilo want to identify and verify? In other words, which customers need to perform KYC steps? All the customers with a certain risk profile or all the customers? Due to the higher risk of money laundering with cryptocurrencies, crypto exchanges and custodian wallet providers need to conduct

enhanced customer due diligence (AFM, 2018). Additionally, the safest method is to identify all customers, while even the customers which are assessed as no risk, can be involved in criminal activities. This can be due to false positive assessments or sophisticated criminal operations.

The next question is: what are proper enhanced customer due diligence requirements? The first requirement of enhanced customer due diligence is customer identity verification. When a new customer wants to register, Smilo needs to know whether the person is really who he claims that he is. An extra check can be added by checking the place of residence. Furthermore, the KYC methods should also be able to verify customers from outside the Netherlands. An important requirement is that fake ID's, blacklisted customers from Smilo and other crypto companies can be recognised. In this way you prevent criminals from misusing the Smilo blockchain.

An extra risk assessment can be built in the enhanced customer due diligence. There are a few signs which can indicate less or extra risk. When a user and device are often seen together, it makes the user less risky, but when devices are shared with multiple users this seems riskier. Higher risk also appears when a user adds new devices.

Requirements for proper customer due diligence:

- ID or passport verification.
- Extra customer verification (e.g. place of residence check).
- KYC methods should be able to identify and verify customers from outside the Netherlands as well.
- Fake ID's and blacklisted customers should be recognized.
- Enhanced customer due diligence risk signs.

Transaction monitoring

In which way do we want to monitor transactions? It is hard to make a distinction between transactions, while there are no personal details linked to Smilo wallets yet. A customer-based risk approach seems therefore hard to deploy. Although it might be possible to cluster wallets with the same transaction behaviour. In this way you can only monitor the transactions of the high-risk wallets, but this method is not optimal in recognizing illicit wallets while outliers from low risk wallets are not detected in this way.
However, if the KYC solutions are implemented before transaction monitoring, a risk-based approach can be used to monitor transactions because personal details can be linked to Smilo wallet addresses and their transactions. In this way, customers will be monitored based on their risk profile.

Other than the customer due diligence, it is hard to find software for transaction monitoring on Smilo's blockchain, because Smilo uses a custom token protocol and not the industry wide one. This means that Smilo must create their own transaction algorithm or work together with a company to create one together.

Also at transaction monitoring it is crucial to blacklist Smilo addresses which are used for criminal activities. In this way other potential criminal addresses connected to the blacklisted address can be identified as well.

Requirements for transaction monitoring:

- Determine features for a transaction monitoring algorithm (see Chapter 5.3.).
- Blacklist Smilo addresses which are used for criminal activities.

Report to the FIU
Every suspicious transaction should be reported to the FIU. For FIU's investigation into the case, it is essential to deliver as much details about the transaction as possible. This means that at least the suspected wallet address, transaction data and receiving wallet address should be send to the FIU. When more information around the suspicious transaction is available, this should certainly also be sent with the other details.

Requirements for reporting to the FIU:

- Make a standard template or program which can easily be used to report suspicious transactions to the FIU.
- Report every suspicious transaction to the FIU.

AML policy
In order to conduct and maintain customer due diligence, transactions monitoring and the reporting to the FIU, an AML policy is needed. The policy must clearly outline what is expected from the employees regarding customer due diligence, transaction monitoring and reporting to the FIU. This policy should be shared internally.
Furthermore, it is important that Smilo's employees are aware of money laundering and its consequences, while this makes them more attentive on what can happen when the AML policy is not complied with. The awareness is important for getting employees on the same line about money laundering.

To raise the awareness of Smilo's proactive position in tackling money laundering, Smilo can also create a public AML policy. This policy should be in line with internally shared one but should not contain information that can be used by criminals. Think about procedures employees need to conduct when suspicious transactions are found or what kind of features are triggers for suspicious transactions.

Requirements for the AML policy:

- Create an internal AML policy and clearly outline per topic (i.e. customer due diligence, transaction monitoring, reporting) what is expected from the employees.
- Inform employees about the consequences from money laundering.
- Create a public AML policy.

5.2. Available methods

5.2.1. All-in-one solution

IdentityMind delivers an all-in-one AML solution. They partnered up with multiple other companies to provide a complete platform. This platform offers KYC solutions, transaction monitoring and virtual currency risk assessment (VCRA). VCRA is an important method to prevent criminals from using the Smilo blockchain. This method analyses transactions with machine learning algorithms to determine whether the addresses of customers have a low or high risk of criminal activities by scanning their transactions. VCRA may be compatible with Smilo's network, but CipherTrace (partner of IdentityMind) has to make some changes to integrate their platform. The question is if they are willing to do this. Otherwise, only the KYC solutions of IdentityMind are available for usage.

Another company which delivers customer due diligence- and transaction monitoring solutions is Chainalysis.

5.2.2. Risk assessment

DNB advises companies to use SIRA (Systematic Integrity Risk Assessment) in order to assess the risk in their company.
SIRA has 4 different steps (De Nederlandsche Bank, 2015) which I recommend using as requirements for a risk assessment:

1. **Risk identification.**
   This step is all about the identification of risk on different points. Risk is assessed based on country of origin, origin of clients, services/products, employees and third parties.

2. **Risk analysis.**
   Risk analysis is about assessing what the chance is that a certain risk appears and what its impact is.

3. **Risk controlling**
   Risk controlling focusses on designing policies and procedures based on the results of the risk identification and the risk analysis.

4. **Risk monitoring and review**
   Risk monitoring is about the monitoring of the risks that are stated in the policies. This step also includes reviewing the policies and procedures that were designed.

A platform that offers help designing a basic AML policy for free is KYC2020.

5.2.3. KYC companies

There are multiple companies that offer customer due diligence for blockchain companies like Smilo. Examples are Mitek, Sum&Substance, KYC3, Crypto-KYC. More KYC companies are available in the market.

5.3. Features for a future transaction monitoring algorithm

Using other companies for implementing AML solutions can be expensive, especially when algorithms must be adjusted in order to work. This is the case with most of the transaction monitoring algorithms from companies, while most of them are created for the Bitcoin blockchain or Ethereum blockchain and the Smilo blockchain is only based on the Ethereum blockchain. Therefore, it might be wise to create a new algorithm to monitor transactions and give alerts when a transaction is suspicious. At least the following points should be taken into account when creating an algorithm:

- If a transaction is worth more than 10.000 euro. The amount of Smilo tokens in a transaction must be converted to the value in euros. This may be done by getting an up to date market price. However, this method might not be ideal when prices fluctuate extremely. In this case the 7-day average can be used.
- Transactions together surpassing 10.000 euro per 24 hours.
- Alert when inactive accounts suddenly receive large amounts of money (Rao & Kanchana, 2018).
- Blacklist Smilo addresses that are linked to illicit activities.
- Scaling, there are not so many transactions yet, but this might change in the future.
- Preferably real time monitoring. This is desirable while transactions can directly be followed and suspicious transactions can directly be reported to the FIU.

In Chapter 3.3. I described the blackhole and volcano principle which is used in the classical financial money laundering detection system. The same principle can be used for Smilo's blockchain. It can be that the blackhole is an address on an exchange, but it can also be on Smilo's blockchain.

Magomedov (2018) assumed that a blackhole has no outgoing transactions, but this was just assumed to simplify the definition. Li Z. et al. (2010) stated that the incoming transactions divided by the outgoing transactions (T_{in}/T_{out}) give a very large value (L). Volcanoes on the other hand have a very large value (L) for the outgoing transactions divided by the incoming transactions (T_{out}/T_{in}). How big L needs to be in both cases needs to be defined by analysing Smilo's blockchain.

- Detect blackhole and volcano patterns.
- Determine the value for L.

Larik and Haider (2011) created a clustering algorithm to detect anomalous transactions using Principal Component Analysis (PCA) and k-means. Their method combined distance- and density-based clustering together with statistical methods to detect suspicious transactions. Clustering methods bring customers with a similar transaction history together. In distance-based clustering identifies points that lie far from the cluster as suspicious, while density-based clustering declares areas with less customers as anomalous.

- Cluster customers with the help of PCA and k-means.

Weber et al. (2019) used a variety of methods to classify Bitcoin transactions as illicit or not with the Elliptic data set. Local information and neighbour information are used to fuel their algorithms with data. Local information is information that is available about a certain transaction (central node), while neighbour information is the information from a transaction one hop backward/forward from the central node. Based on the paper's conclusions, neighbour information and calculating node embeddings improves the performance of the algorithm. Taking this conclusion in account, I would recommend using the following features:

- Local information: time stamp, transaction fee, output volume and aggregated figures such as average Smilo received (spent) by the inputs/outputs and average number of incoming (outgoing) transactions associated with the inputs/outputs.
- Information from neighbours: aggregated features like minimum, maximum, standard deviation, correlation coefficients of the neighbour transactions for the same information data (transaction fee, transaction value, time stamp, etc.)

Weber et al. also concluded that non-graph-based classification models (i.e. Logistic Regression, Random Forest, Multilayer Perceptrons) increased performance when features of Graph Convolutional Networks (GCN) embeddings were used.
Furthermore, Random Forest and GCN had the best outcome on the Elliptic data set. Therefore, they recommend finding a solution to combine those two methods.

6. Conclusion

6.1. The conclusion

Money laundering through cryptocurrencies is a growing problem. Being associated with money launderers on your blockchain can harm a firm's business. That is why Smilo wanted to keep the money launderers out of their own blockchain. The research question for this paper is:

What measures can Smilo take to combat money laundering on their blockchain?

In order to come to an answer, I created a theoretical framework where the blockchain and the transactions on it were explained. A blockchain is an ever growing decentral distributed ledger which supports transactions as well as data storage. The most important characteristics of the blockchain are transparency and immutability.

Subsequently, I outlined the classical money laundering system and what is being done to prevent this type of money laundering. Money laundering contains three basic steps, namely; placement, layering and integration. There are two levels of preventing classical money laundering; via laws and regulations (e.g. the BSA, Wwft, AMLD), and algorithms which detect suspicious transactions.

Thereafter, I investigated money laundering through cryptocurrencies and the measures that exists for the 'new' money laundering system. The 'new' way of money laundering also sticks to the three basic steps (i.e. placement, layering and integration). The money laundering process with cryptocurrencies can be found in Figure 9.
The measures for money laundering on the blockchain are just like the measures for the classical system divided in legislation and algorithms. However, there has not been as much research on effective real time transaction monitoring algorithms as is available for the classical money laundering system. This is due to the relative novelty of the field. The first regulations about cryptocurrencies formed in 2014 in New York, whereas the first regulations about cryptocurrencies will become active in the Netherlands at the 10th of January 2020. This implicates why there is not much research available about transaction monitoring on the blockchain.

After that, I described Smilo's current situation in terms of responsibility. It turned out that Smilo is not obliged to comply with the new upcoming regulations (i.e. AMLD5 and Wwft) for crypto companies, while these regulations only hold for crypto exchanges or custodian wallet providers. However, this does not mean that Smilo does not want to prevent money launderers from their blockchain. The reason that no action is taken regarding AML is because of a lacking AML policy at Smilo.

To improve the current situation, I set up requirements. These requirements comprised risk assessment, customer due diligence, transaction monitoring and reporting to the FIU. Thenceforth, I presented the available methods which met the requirements. However, Smilo's uniquely designed blockchain delivered a hurdle. Transaction monitoring software is now only available for regular blockchains (i.e. bitcoin blockchain, Ethereum blockchain, etc.). However, this software is not available yet for custom made blockchains. This means that Smilo must create its own transaction monitoring algorithm, when they want to be proactive in tackling money laundering. Based on AML algorithms used for the classical money laundering system, I wrote down features for Smilo's transaction monitoring algorithm.

During the research I gained insights on what measures Smilo can take to prevent money laundering on their system. The recommendations in the next section provide the answer to the research question.

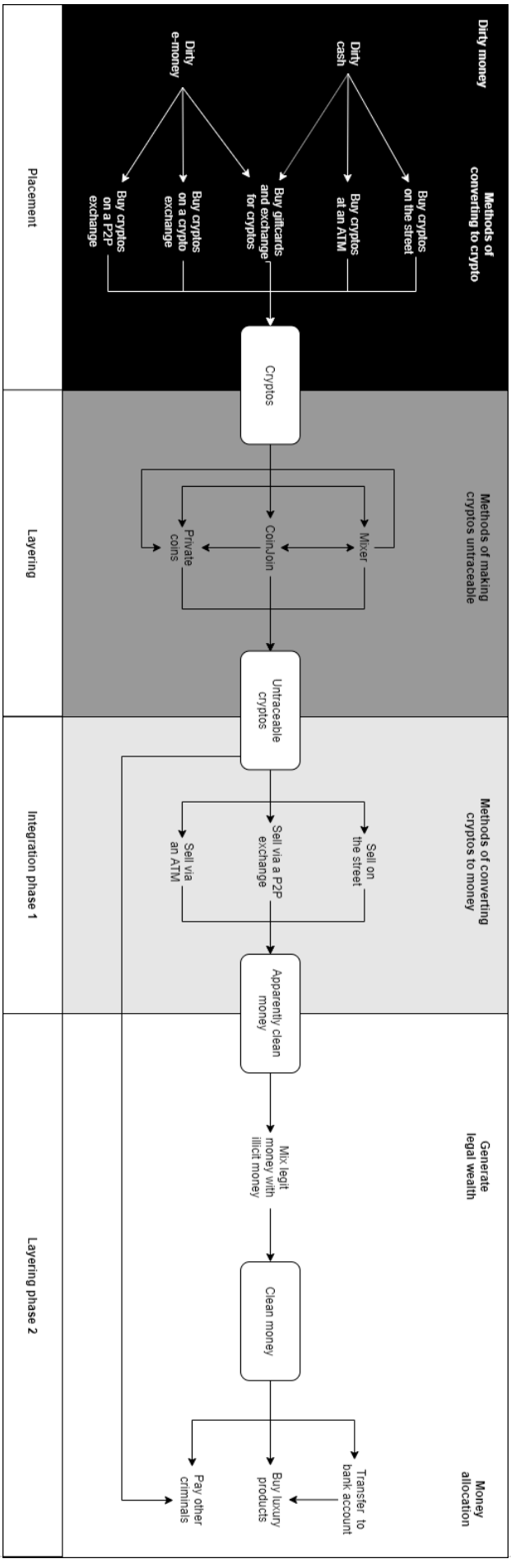

Figure 9: Money laundering with cryptocurrencies

6.2. Recommendations

1. Only partner with exchanges that implement KYC measures into their company in order to avoid criminals from easily accessing the Smilo token and thereby Smilo's blockchain. This prevents criminals from changing another cryptocurrency into Smilo tokens without verification.
2. Create a solid AML policy and publish it internally and externally. Furthermore, keep this policy up-to-date and obey this policy. Acquiring or selecting a compliance officer to conduct these steps might be a good idea.
3. I recommend to annually conduct SIRA. In this way Smilo can estimate the risk of their network being misused by criminals. This can help in creating an appropriate AML policy (and in designing a suiting solution).
4. Implement KYC measures. These are very important in preventing money launderers on Smilo's blockchain, while illegal activity can directly be linked to an identity. I would recommend using IdentityMind for implementing KYC measures, while they have a big partner ecosystem. This means that customer due diligence consists of multiple companies working together, which is advantageous in information sharing. Blacklists, fake ID recognition and other information can be shared through the consortium.
   First implement KYC methods, then transaction monitoring, because risk based transaction monitoring can be conducted in that way.
5. There seems no third-party solution for transaction monitoring yet, because Smilo does not use an ERC-20 protocol for their tokens, but a custom one. I recommend creating an own transaction monitoring algorithm, which takes the recommended features mentioned in Chapter 5.3. into account.
   Smilo's blockchain is completely open source. I recommend to not publish the transaction monitoring algorithm, because money launderers can easily read which actions trigger an alarm in the algorithm.
6. Report every suspicious transaction/account to the FIU with as much evidence as possible. Provide customer details: Smilo address, Smilo balance, (suspicious) transactions, Identification (passport, ID, driver license), living address, etc.
7. Stay in contact with other crypto companies that implemented AML practices (e.g. VBNL members). Every AML solution is company specific, but they all comply with the upcoming legislation. Sharing AML information on the blockchain is valuable in the fight against money laundering practices. AML policies can be shared, and AML solutions can be discussed.
8. I also recommend joining the InnovationHub from DNB & AFM. Together with other companies Smilo can talk about how to implement the newest regulations into the crypto sector and their own company.
9. Once a complete solution that complies with the Wwft- and AMLD5 requirements is implemented, I recommend keeping up to date with the FATF guidelines, as those will almost certainly be translated in national laws.
10. As I mentioned earlier, Smilo does not fall under the term VASP, but I recommend Smilo's legal person to investigate whether Smilo will fall under this term when tokens are sent to partner companies in the future. When Smilo will fall under the term VASP in the future, they **must** comply with AMLD5 and the Wwft. Which implicates that they need to register themselves at DNB, conduct a risk assessment, conduct enhanced customer due diligence, perform transaction monitoring and to report to the FIU.

7. Discussion

7.1. Exploratory research

This research is conducted on new and volatile ground with rapidly changing technologies and standards (guidelines, laws, rules). Because of this reason, researches like this can become outdated quite quickly. However, this does not mean that the scientific relevance becomes less meaningful. It is important to create clarity for crypto companies that do not (yet) have to comply with AML regulations. In this way, those crypto companies have the opportunity to slowly integrate AML solutions. It is hard for crypto companies to keep up with the latest rules and guidelines, because of continuously changing rules and guidelines, but also the implementation costs can be a bottleneck.

7.2. Further research

I recommend researchers to investigate the AML possibilities on the Ethereum blockchain. Bitcoin is the market leader of cryptocurrencies, but Ethereum is the foundation of smart contracts. While smart contracts are of significant relevance for the blockchain industry, I do not expect scientific research on the Ethereum blockchain to become irrelevant.

Furthermore, I recommend Smilo to develop an algorithm to monitor all transactions on their blockchain. This may require more investigation on their own blockchain, while no Ethereum blockchain research regarding this topic is available yet. Therefore, it seems logical to let a Smilo employee with understanding of their blockchain investigate how to develop a transaction monitoring algorithm. This employee can be assisted by a researcher or other crypto companies that already implemented a transaction monitoring algorithm.

When Smilo decides to not conduct customer due diligence at every customer, they should investigate other ways to identify customers. Narrowing down the customer's geographical location through IP-addresses is not a solid way. As Patrick van der Meijde described, IP-addresses can easily be hidden through TOR networks or VPNs. Customers can also use Tails (The amnestic incognito live system) a system which was created to enhance privacy, to mask their IP-address and other information that can be linked to their identity. While such systems make it hard to gain any information of a customer, I highly recommend conducting customer due diligence at every customer.

7.3. Scientific relevance

This research is completely based on the Bitcoin blockchain. Smilo's custom blockchain is based on the Ethereum blockchain. Not that much Ethereum blockchain research is available, especially not regarding the AML topic. That is why this research should be seen as an exploratory research.

In Chapter 3.5.3. I outlined the conversations with experts from DNB and VBNL. The findings of conversations that are outlined in this research are limited to the perspectives of those people.

In Chapter 5.3. I recommended clustering customers in combination with statistical methods as a feature for the transaction monitoring algorithm. However, clustering algorithms use an unsupervised learning technique; therefore, it is hard to determine the accuracy of the algorithm. This should be taken into account when the algorithm will be created.

The last point of consideration is the robustness of the transaction monitoring algorithm that might be build. The methods used in Weber's et al. (2019) failed to perform accurately after a sudden shutdown of illicit nodes. The designer of Smilo's transaction monitoring algorithm should think about ways to prevent decrease in performance when sudden shutdowns or other unexpected events happen.

7.4. Generalization

This research and its recommendations are especially applicable to Dutch custodian wallet providers and crypto exchanges that did not implement any AML-measures yet. This research gives a foundation for those companies in knowing how to comply with the Wwft. It also gives an insight at what the Wwft asks from Dutch custodian wallet providers and crypto exchanges.

However, not only Dutch custodian wallet providers and crypto exchanges can gain knowledge from this research. Also blockchain companies which are located in the EU that want to be proactive in fighting money laundering can learn which steps they need to perform in order to comply with AMLD5.

Furthermore, blockchain companies that did already implement AML-measures can see the recommendations as a guideline. Blockchain companies that are located in a FATF member states might not be aware where their national laws come from. This research can make them aware of the fact that FATF recommendations are almost certainly translated into national laws. This can help them to anticipate on cryptocurrency laws that might be coming and gives them extra time to comply with upcoming laws.

Not all the recommendations in my research are relevant for every blockchain company. The fifth and the tenth recommendation are not suitable for every company.
The fifth recommendation is only useful for companies that do not have a transaction monitoring system and are not using ERC-20 tokens or Bitcoin. Ready-made transaction monitoring systems are available for companies that use ERC-20 tokens or Bitcoin.
The tenth recommendation is company specific. I would recommend companies to clearly outline why they are a VASP or not. It is important for their business to evaluate this regularly, because a change has consequences for the company's regulation.

Appendix

A. Questions DNB

1. *What is DNB's point of view on cryptocurrencies?*

2. *What methods (software/algorithms/mathematical models) will be used to supervise crypto exchanges and wallet providers to safeguard the Wwft?*

3. *With which organizations does DNB collaborate to supervise the Wwft? What are the different roles within the collaboration?*

4. *At the beginning of January 2019, DNB wrote a joint advice together with AFM to create a national licensing system for crypto exchanges and crypto wallet providers. What is the idea behind a national licensing system? How will the exchanges and wallet providers be tested on reliability? Which requirements should be fulfilled in order to obtain a license?*

5. *Are there crypto companies that already have a solution to detect money laundering transactions?*

6. *Are there money laundering detection methods from the regular financial system which can also be applied on the blockchain?*

7. *What is expected from companies like Smilo to comply with the Wwft?*
   How are companies that are not listed under the Wwft stimulated to tackle money laundering practices?

8. *What do you advise crypto companies that not fall under Wwft to tackle money laundering practices?*

9. *Are there plans for stricter regulations for crypto companies in the future?*

10. *How big is the crypto money laundering problem?*

B. OECD's money laundering typologies for cryptocurrencies

Indicators

Unusual transactions

- Trading or having coins available from mining without relevant equipment or electricity costs to show for
- Accepting, trading or having coins available with a history on the dark web
- Withdrawal of large amounts of cash from the bank account shortly after having received money from cryptocurrency exchanges
- Paying high fees for converting (selling) cryptocurrency in exchange for cash
- Large deposits of cash into personal accounts, followed by purchases of cryptocurrencies from commercial/regulated exchanges
- Use of a debit card fuelled by cryptocurrencies
- Large cash deposits and large cash withdrawals via coin ATMs
- Cryptocurrency transactions for the purchases of luxury items that seem not in line with the buyers reported income
- Unexpected amounts of cryptocurrency in the business (sales or loans)

Unusual behaviours

- Unable to justify the economic or business benefit of transactions involving cryptocurrency
- Transactions in cryptocurrencies which have at least two of the following features:
    a) The seller or purchaser offers their services via demand and supply sites on the internet
    b) The parties do not establish each other's identity
    c) The seller or purchaser protects their identity
    d) Cryptocurrencies are paid for in cash
    e) The exchange fee is unusually high
    f) The transaction is conducted in a (public) place where a lot of people are present, which decreases the safety risks for the seller and purchaser
    g) A legal economic explanation for the way the exchange was made is not likely
    h) The scope of the purchased virtual currencies is unlikely in relation to the average private use
    i) The exchanger is unknown to the Chamber of Commerce and the Tax Administration
- The purchaser and/or seller make(s) use of a so-called mixer or tumbler

Figure 10: Money laundering indicators. OECD, (2019).

References

AFM. (n.d.). Retrieved from https://www.afm.nl/en/professionals/nieuws/2019/jan/adviesrapport-crypto

AFM. (2018). *Toepasbaarheid Wwft op (beheerders van) beleggingsinstellingen in crypto's.* AFM.

AMLC. (2017). The Bitcoin trader, a facilitating role in the cash out of criminal proceeds. (August).

AMLC. (2017). Witwasindicatoren. *1017*, (p. 1-6).

Bitcoin Wiki. (n.d.). Retrieved from https://en.bitcoin.it/wiki/CoinJoin

Brave New Coin. (n.d.). Retrieved from https://bravenewcoin.com/insights/mass-exodus-of-bitcoin-exchanges-from-new-york-state-triggered-by-bitlicense-deadline

Brugman, J., & Tonino, H. (2019). Nieuwe anti-witwas- en terrorismefinancieringregeling van toepassing op Nederlandse crypto-omwissel platforms en crypto-bewaarportemonnees. *Estate planning, 2019/2*, (p. 1-3).

Bryman, A., & Bell, E. (2011). Ethics in business research. In A. Bryman, & E. Bell, *Business Research Methods* (p. 2-26). Oxford University Press.

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change, 69*, (p. 283-305).

Choo, K. (2015). Cryptocurrency and Virtual Currency: Corruption and Money Laundering/Terrorism Financing Risks? In K. Choo, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (p. 283-307).

CipherTrace. (2019). *Cryptocurrency anti-money laundering report.*

Coin ATM Radar. (n.d.). Retrieved from https://coinatmradar.com/bitcoin-atm-near-me/

Coin ATM Radar. (n.d.). Retrieved from https://coinatmradar.com/blog/how-to-use-printed-paper-wallet-on-receipt-from-a-bitcoin-atm/

Cooper, D., & Schindler, P. (2014). *Business Research Methods, 12th Edition.* 1221 Avenue of the Americas, New York, NY, 10020: McGraw-Hill Education.

CypherTrace. (2019). Cryptocurrency Anti-Money Laundering. (July), (p. 1-52).

de Balthasar, T., & Hernandez-Castro, J. (2017). An Analysis of Bitcoin Laundry Services BT - Secure IT Systems. In H. Lipmaa, A. Mitrokotsa, & R. Matulevičius (Eds.). (p. 297-312). Cham: Springer International Publishing.

De Nederlandsche Bank. (2015). De integriteitrisicoanalyse.

Department of Financial Services. (n.d.). Retrieved from https://www.dfs.ny.gov/search/site?search=bitlicense&page=0

Dyntu, V., & Dykyi, O. (2019, 2 11). Cryptocurrencies in the System of Money Laundering. *Baltic Journal of Economic Studies, 4*, (p. 75-81).

Ehrhart, C., & Gupta, A. (2017). Explained: Blockchain. *Delivered. The Global Logistics Magazine*(03), (p. 25).

European Commission. (n.d.). Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering_en

European Commission. (n.d.). *Money laundering*. Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering_en

European Institute of Management and Finance. (n.d.). Retrieved from https://eimf.eu/understanding_money_laundering/

European Union Law. (n.d.). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018L0843&from=EN

F. Xavier Olleros, M. (2016). *Research Handbook on Digital Transformations.* Edward Elgar Pub.

FATF. (n.d.). Retrieved from https://www.fatf-gafi.org/about/

FATF. (n.d.). Retrieved from https://www.fatf-gafi.org/glossary/u-z/

FATF. (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. (p. 6-59). FATF/OECD.

FinCEN. (n.d.). Retrieved from https://www.fincen.gov/history-anti-money-laundering-laws

FIU-Nederland. (2019). *FIU-Nederland Jaaroverzicht 2018.* FIU-Nederland, Zoetermeer.

Forbes. (n.d.). Retrieved from https://www.forbes.com/sites/michaeldelcastillo/2019/07/16/cryptocurrency-crimefighter-chainalysis-joins-next-billion-dollar-startups/#29c2141aace0

Fortune. (n.d.). Retrieved from http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/

Friedman, J. (1997). Data Mining and Statistics: What's the Connection? *Proceedings of the 29th Symposium on the Interface Between Computer Science and Statistics*, (p. 1-7).

Heerkens, J., & van Winden, A. (2012). *Geen probleem, een aanpak voor alle bedrijfskundige vragen en mysteries.* Buren: Business School Nederland.

Hoekstra, W. (2019). Aanbiedingsbrief implementatiewet wijziging vierde anti-witwasrichtlijn. (p. 1-6).

Huang, D., Mu, D., Yang, L., & Cai, X. (2018). CoDetect: Financial Fraud Detection with Anomaly Feature Detection. *IEEE Access, 6*, (p. 19161-19174).

Jayasree, V., & Siva Balan, R. (2015). Money laundering identification on banking data using probabilistic relational audit sequential pattern. *Asian Journal of Applied Sciences, 8*(3), (p. 173-184).

Juhász, P., Stéger, J., Kondor, D., & Vattay, G. (2018). A Bayesian approach to identify Bitcoin users. *PLoS ONE, 13*, (p. 1-21).

Larik, A., & Haider, S. (2011). Clustering based anomalous transaction reporting. *Procedia Computer Science*, *3*, (p. 606-610).

Magomedov, S., Pavelyev, S., Ivanova, I., Dobrotvorsky, A., Khrestina, M., & Yusubaliev, T. (2018). Anomaly detection with machine learning and graph databases in fraud management. *International Journal of Advanced Computer Science and Applications, 9*, (p. 33-38).

Maksutov, A., Alexeev, M., Fedorova, N., & Andreev, D. (2019). Detection of blockchain transactions used in blockchain mixer of coin join type. *Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2019*, (p. 274-277).

Medium. (n.d.). Retrieved from https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373

NOS. (2019, September 26). Retrieved from https://nos.nl/artikel/2303385-om-onderzoekt-abn-amro-vanwege-witwassen.html

Odinot, G., Verhoeven, M., Pool, R., & Poot, C. d. (2017). Organised Cybercrime in the Netherlands. *The WODC (Research and Documentation Centre) of the Ministry of Security and Justice*, (p. 1-87).

OECD. (2019). *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors.* Paris: OECD.

Oerlemans, J., Custers, B., Pool, R., & Cornelisse, R. (2016). *Cybercrime en witwassen.* Meppel: Boom.

Public Statement on Virtual Assets and Related Providers. (n.d.).

Pulakkazhy, S., & Balan, R. (2013). Data mining in banking and its applications- A review. *Journal of Computer Science, 9*, (p. 1252-1259).

Rao, A., & Kanchana, V. (2018). Dynamic approach for detection of suspicious transactions in money laundering. *International Journal of Engineering and Technology, 7*, (p. 10-13).

Ravenda, D., Valencia-Silva, M., Argiles-Bosch, J., & García-Blandón, J. (2019). Money laundering through the strategic management of accounting transactions. *Critical Perspectives on Accounting, 60*, (p. 65-85).

Raza, S., & Haider, S. (2011). Suspicious activity reporting using Dynamic Bayesian Networks. *Procedia Computer Science*, *3*, (p. 987-991).

Russell, S., & Norvig, P. (2010). *Artificial Intelligence: A Modern Approach.* Upper Saddle River, New Jersey 07458: Pearson Education, Inc.

Smilo. (n.d.). Retrieved from https://smilo.io/

Soudijn, M. (2012, 9). Removing excuses in money laundering. *Trends in Organized Crime, 15*, (p. 146-163).

UNION, (1991). Council Directive 91/308/EEC of 10 June 1991 on prevention of the use of the financial system for the purpose of money laundering. *Official Journal of the European Communities, L166/77*, (p. 77 – 83).

UNION & PARLIAMENT, (2018). Directive (EU) 2018/843 of the European Parliament and of the Council. *Official Journal of the European Union, L 156/43*(19.6.2018).

UNODC. (n.d.). *United Nations Office on Drugs and Crime*. Retrieved from https://www.unodc.org/unodc/en/money-laundering/globalization.html

Vallerand, R., Pelletier, L., Blais, M., Briere, N., Senecal, C., & Vallieres, E. (1992). The Academic Motivation Scale: A Measure of Intrinsic, Extrinsic, and Amotivation in Education. *Educational and Psychological Measurement, 52*(4), (p. 1004-1009).

van de Poel, I., & Royakkers, L. (2011). *Ethics, Technology, and Engineering An Introduction.* New York, NY: McGraw-Hill/Irwin.

van Wegberg, R., Oerlemans, J.-J., & van Deventer, O. (2018). Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime, 25*, (p. 419-435).

Weber, M., Domeniconi, G., Chen, J., Daniel Karl I. Weidele, C., Robinson, T., & Leiserson, C. (2019). Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. (p. 1-7).

Worldbank. (n.d.). Retrieved from https://data.worldbank.org/indicator/ny.gdp.mktp.cd?name_desc=false

Yin, H., Langenheldt, K., Harlev, M., Mukkamala, R., & Vatrapu, R. (2019). Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain. *Journal of Management Information Systems, 36*, (p. 37-73).

Zhongmou Li, Hui Xiong, & Yanchi Liu. (2010). Detecting Blackholes and Volcanoes in Directed Networks. *ArXiv, abs/1005.2179*, (p. 1-4).