MALMÖ UNIVERSITET
FAKULTETEN FÖR HÄLSA OCH SAMHÄLLE

“NOW YOU SEE IT. NOW YOU DON’T”

HOW CRYPTOCURRENCIES ENABLE MONEY LAUNDERING

MARIA MOITA GONÇALVES

Degree Project in Criminology
Master’s Programme (120 credits)
May 2019

Malmö University
Health and Society
205 06 Malmö

“NOW YOU SEE IT. NOW YOU DON’T”

HOW CRYPTOCURRENCIES ENABLE MONEY LAUNDERING

MARIA MOITA GONÇALVES

Moita Gonçalves, M. Now you see it. Now you don’t - How Cryptocurrencies Enable Money Laundering. *Degree project in Criminology 30 credits.* Malmö University: Faculty of Health and Society, Department of Criminology, 2019.

Money laundering is a non-violent crime, however when successfully executed it has a negative impact on society, as it tends to support other illicit activities, including terrorism. As was the case for other financial crimes, the internet opened the door for new tools that enable criminals to launder their illicit profits. One of these tools is cryptocurrency.
This paper takes the form of a literature review, in order to find the most relevant and important work within the research topic, and to identify central issues associated with laundering money through cryptocurrencies. It aims to explain the crypto-laundering process, methods and features that make cryptocurrencies tempting to criminals when searching tools to launder their illicit profits.
The findings of this literature review demonstrate that cryptocurrencies have more characteristics that appeal to launderers than deters them. The results also show the existence of different methods that are employed in crypto-laundering and how it mirrors traditional money laundering stages, making evident that crypto-laundering is a real threat. Due to these results, it is essential that the criminological community delve into financial crimes perpetrated in the online environment.

Keywords: cryptocurrencies; money laundering; cyber-crime; cyber-laundering; crypto-laundering.

ACKNOWLEDGEMENTS

I would like to express my gratitude for the people who supported me during the making of this master's thesis. I would first like to thank my thesis supervisor Robert Svensson, who allowed this paper to be my own work, but steered me in the right direction when needed.

I would also like to thank Athina for being a great study partner, that not only contributed with ideas, but also uplifted me; Sam for reviewing my English; and Katherina and Vasco for their support.

Finally, I must express my very profound gratitude to my mother Fátima and my grand-parents Manuel and Teresa for providing me with unfailing support and continuous encouragement through my years of study, and throughout my life. This accomplishment would not have been possible without them.

Thank you.
Maria Moita Gonçalves
24.05.2019

TABLE OF CONTENTS

1. INTRODUCTION

Money laundering is not a recent criminal phenomenon, however it is a permanently evolving one, with updated techniques and growing business models (Wegberg, Oerlemans, & Deventer, 2018). Money laundering has a myriad of typologies, nonetheless it is a relatively easy concept to define - it is the process used by criminals to cleanse the profits of their illicit activities (Stokes, 2012).

As it happened to other financial crimes, the internet opened the door for a safer environment and for new tools that enable criminals to launder their illicit profits. One of these tools is cryptocurrencies (Ajello, 2015; Gifari, Anggorojati, & Yazid, 2017; Stokes, 2012).

Crypto-laundering is still seen as a small share of the whole (The Economist, 2018), as for example, economically relevant countries, such as the UK, considered cryptocurrencies as a low risk threat in relation to money laundering (HM Treasury & Home Office, 2017). Nonetheless, this type of virtual currency presents characteristics that might be attractive to those who intend to go around the anti-money laundering (AML) rules (Brenig, Accorsi, & Müller, 2015). Said characteristics must be analysed to comprehend the extent of the problem.

Laundering money is theoretically a non-violent crime, however, successful money laundering has extremely damaging consequences, as it tends to support other illicit activities including terrorism (Ajello, 2015). Giving the possibility of cryptocurrencies as a vehicle for money laundering, it is important to conduct a criminological study on this subject. The analysis of knowledge, or lack thereof, on risk factors embedded to cryptocurrencies, how the crime of money laundering is being perpetrated nowadays and the extent of the problem is essential for both cyber and financial crime prevention.

1.1. Aim and Research Questions

The purpose of this study is to examine the available literature about cryptocurrencies being used to launder money (crypto-laundering), and what are the risk factors that make cryptocurrencies tempting to criminals when searching tools to launder their illicit profits. The aim is to question how the current knowledge about the problem explains what are the characteristics of cryptocurrencies that enable money laundering (ML) and how criminals abuse it.

This study is based on the following research questions:
1. What are the risk factors of cryptocurrencies that enable ML?
2. How are cryptocurrencies used to launder money?
3. Does crypto-laundering mirror traditional ML stages?

2. BACKGROUND

This section intends to guide the reader into understanding the complex taxonomy of digital and virtual currencies, in order to comprehend the cryptocurrency concept. A brief overview on ML and the cyber version of it is also drawn, to assist the connection of how cryptocurrencies enable ML.

2.1. Digital and Virtual Currencies

Cryptocurrencies are included in the wide range of both digital and virtual currencies (Möser, Böhme, & Breuker, 2013). It is necessary then to comprehend the concept of virtual currencies, so that one may have a better understanding of cryptocurrencies.

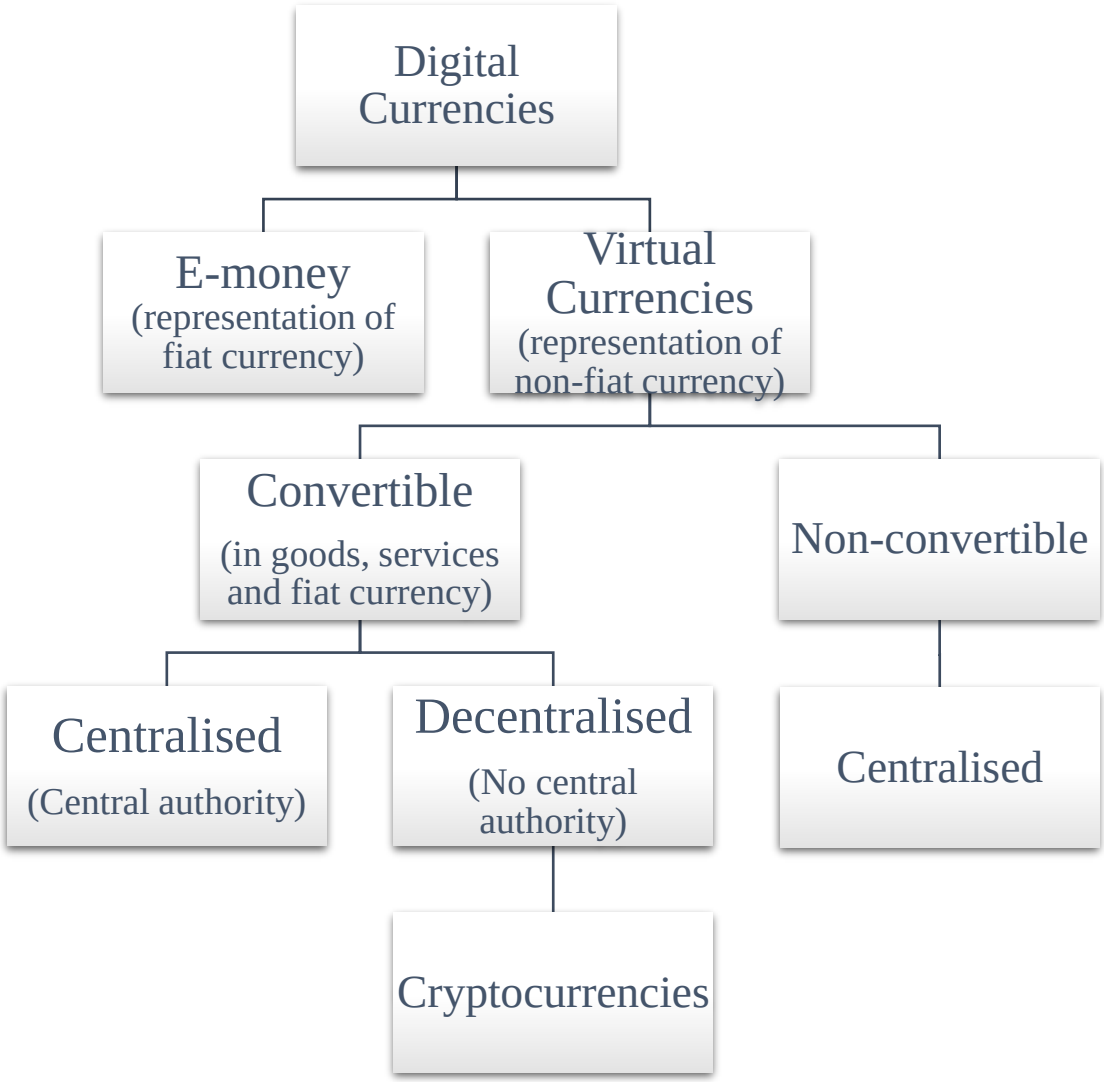


Figure 1. Taxonomy of Digital Currencies (FATF, 2014; He et al., 2016)

As one can observe on figure 1, digital currencies encompass two different digital representations: e-money, the online representation of "real currency" (from now on designated as fiat currency) and virtual currency, which stands for non-fiat currency in the online environment (FATF, 2014; He et al., 2016).

E-money allows online payments as a representative of fiat currency, generally via a digital transfer mechanism, e.g. PayPal (Bryans, 2014). In turn, virtual currencies are not controlled by any jurisdiction or financial institution, and are only valid in a context where the users validate the virtual currency as a representative of payment (Bryans, 2014; He et al., 2016).

According to the Financial Action Task Force, virtual currency may take two forms: convertible and non-convertible, meaning it can be exchanged to fiat currency or not (FATF, 2014). While all non-convertible virtual currencies are centralised (as they are issued by a central authority), convertible virtual currencies can be centralised or decentralised (ibid.).

Centralised virtual currencies have a single administrating authority, which means that a third party controls the system as it "issues the currency; establishes the rules for its use; maintains a central payment ledger; and has the authority to withdraw the currency from circulation" (FATF, 2014, p. 5). On the other hand, decentralised virtual currencies have no central administrating or monitoring authority (ibid.).

2.1.1. Cryptocurrencies

Cryptocurrency falls into the decentralised convertible virtual currency category (Figure 1), meaning that it allows online transactions and payments from one user to another (peer-to-peer), without the involvement or supervision of a financial institution (Nian & Chuen, 2015).

Nowadays, there is a myriad of different cryptocurrencies, such as Litecoin, Ethereum and Monero. To better understand the concept of cryptocurrency, without delving into the "computer" description of it, this paper will draw a short overview of Bitcoin – as it was the first decentralised convertible cryptocurrency, it dominates the virtual currency market and it is the one mostly analysed in the literature.

Bitcoin was based on Nakamoto's (2008) paper, and was launched in 2009. It is a virtual currency network, where the currency unit "bitcoins" are created, managed and transferred via peer-to-peer (P2P) (Stokes, 2012).

The software is open-source and can be downloaded for free by anyone. Once the software is downloaded the user has three ways to obtain bitcoins, namely through the purchase of the currency, through purchase/sale of goods or services (as with any fiat currency), or, finally, through the mining process, which will be explained further ahead (Plassaras, 2013).

Bitcoins transactions can be processed using a mobile app, computer software, or service provider that provides a bitcoin wallet (Nian & Chuen, 2015). The wallet generates an address that, although being similar to a bank account number, is in fact a unique alphanumeric sequence of characters (ibid.). Once said address is obtained, the user can start receiving bitcoins.

Bitcoin transactions are then verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain (Nakamoto, 2008) – this means that an encrypted algorithm is added to a public online history of previously agreed-upon P2P transactions (Möser et al., 2013). The use of encryption is to ensure both confidentiality (ensuring that only authorized persons can read the data) and authentication (ensuring that the data has not changed between source and destination) (Plassaras, 2013).

Mining is then essential to the Bitcoin network. Miners provide security and confirm Bitcoin transactions, as their role is to secure the network and to process

every Bitcoin transaction (Böhme, Christin, Edelman, & Moore, 2015). Miners accomplish this by solving a computational problem which allows them to chain together blocks of transactions, thus creating and securing the blockchain (ibid.). For this service, miners are rewarded with recently created Bitcoins or transaction fees (Reid & Harrigan, 2011).

One of the main advantages for the users of this virtual currency is, according to Böhme et al. (2015) the lack of imposition of a financial institution, payment processor, or other intermediary to validate the identity of the users. To create a bitcoin wallet, a new user must register using identification and contact information, but since there is no regulatory process or associated costs the information provided may not be real (Ajello, 2015; Stokes, 2012). Therefore, a single user can open as many wallets as he/she wants without ever providing their real identity (FATF, 2017).

Bitcoin is not supported or overviewed by any government or organisation, which means that there is no guarantor, supervision or control over the mining and transactions of bitcoins (Ajello, 2015; Gifari et al., 2017; Kethineni, Cao, & Dodge, 2018; Stokes, 2012). According to Stokes (2012) bitcoin acquires its value as a currency only through confidence, since users who make the transaction agree on its value and accept it as payment, again without the involvement of an institution to control bitcoin value.

In the carried-out transactions, there are no records regarding the names of users. Only a registry of public keys is necessary for the continuation of the mining process, making users able to send bitcoins electronically to anyone who accepts this currency, with a certain level of anonymity (Gifari et al., 2017). Adding to this, there is also the possibility of converting bitcoins into fiat currency, such as Euro, Pound or Dollar (Kethineni et al., 2018).

2.2. Money Laundering

Money laundering (ML) has numerous definitions. In its most simple way, ML is "the process of making illegally-gained proceeds (i.e. 'dirty money') appear legal (i.e. 'clean')" (Bryans, 2014, p. 442).

According to Schott (2006), most countries adopt the United Nation's ML definition: "the conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions" (p. 2)

This problem causes serious challenges to the global conjuncture, such as financing terrorists, spreading financial corruption or infiltrating politics (Bryans, 2014; Christopher, 2014; Gilmour, 2016a). Anti-money laundering (AML) laws were put in practice around the world exactly to prevent and punish those who engage in this crime (Bryans, 2014).

Money laundering follows different stages to finally release laundered funds into the legal financial system (Figure 2). The stages names might differ, depending on the author, but generally three main steps are considered – placement, layering (stratification or transformation), and finally integration (or investment of funds).

The typical money laundering scheme stages go as follows:

Placement In this initial stage, criminal actors or specialists (lawyers, accountants, etc.) will try to introduce illicitly acquired funds into the financial system (Brenig et al., 2015). A common method used by these actors is "smurfing", which is the division of a considerable amounts of money into smaller sums, so as to not raise the suspicions of financial organizations and/or authorities (Hunt, 2011).

Layering In the following stage, the funds typically are exchanged between several institutions and jurisdictions using, for example, the purchase/sale of investment instruments (bonds, stocks, cheques) or they are simply transferred between a series of accounts in several banks, especially to those with lax AML rules (Brenig et al., 2015). This juggling of transactions will obfuscate the origin of the funds, since, due to the large number of transactions carried out daily, the authorities will not be able to perceive it as ML strategy (Hunt, 2011).

Integration Finally, the last stage seeks to integrate the illicit funds into the legal economy through financial or commercial operations, to make it appear legit (Brenig et al., 2015). Money launderers usually use anonymous and/or false corporations or real estate investments to clean the ill-gotten gains (Hunt, 2011).

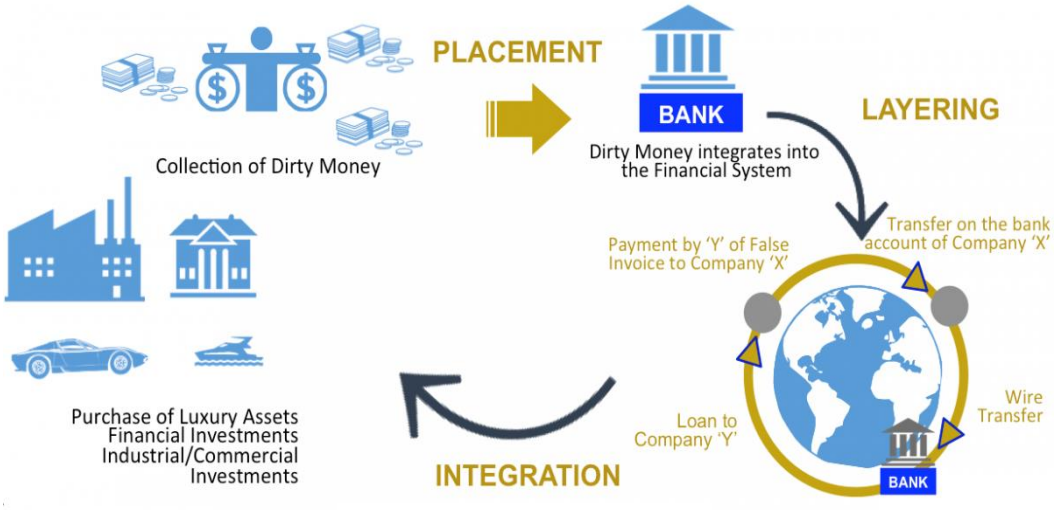


Figure 2: The traditional money laundering process (European Institute of Management & Finance, 2018).

The United Nations Office for Drugs and Crime (2018) estimates that the annual value of money laundered globally stands between 2% and 5% of global gross domestic product, meaning that between US$800 billion and US$2 trillion are laundered each year.

To combat illicit transactions, the global governance has strived to formulate regulations and AML directives (Bryans, 2014; Dostov & Shust, 2014). Several

methods were created to combat ML -"know your customer" policy (KYC) is considered to be an effective method (Möser et al., 2013). This policy aims to identify customers of financial institutions, such as banks (Brenig et al., 2015). Customers are required to present certain documents to enable identification, such as legal identification, proof of residency (addresses, nationality etc.) and a valid photograph (FATF, 2017).

2.3. Virtual Money Laundering

The internet opened before us a whole new reality, accessible with just one click. This internet reality also created a myriad of new possibilities for criminal activities (Filipkowski, 2008; Stokes, 2012; Tropina, 2015), served on a "jurisdictionless" plater. Money laundering is no exception (Tropina, 2015).

With technological progress and the internet's rapid evolution, soon came the possibility to use the online environment to turn ill-gotten funds into clean and untraceable money – this was defined as 'cyber laundering'(Stokes, 2012). The continued development of electronic and virtual money and payment technologies opened doors for 'virtual money laundering' (Filipkowski, 2008; Stokes, 2012).

Virtual laundering is the term that encompasses the different forms of performing money laundering in the online environment using virtual currency. According to several authors (Filipkowski, 2008; Stokes, 2012; Tropina, 2015), there are different ways to engage in virtual laundering, for example, exploiting online casinos, virtual worlds (such as Second Life), multiplayer online games (such as World of Warcraft), and more recently, cryptocurrencies.

2.3.1. Crypto-Laundering

At the same time that Bitcoin and other cryptocurrencies started to gain popularity, concerns arose regarding its potential to undermine the "real world" society, through tax evasion, ML and illegal transactions (Reid & Harrigan, 2011).

Criminal actors are cash rich, and their funds need to be transferred through different jurisdictions, to continue their criminal enterprises (Irwin & Milad, 2016). The new AML laws and regulations made the traditional corruption of the financial system increasingly harder to abuse (ibid.). However, cryptocurrencies have several characteristics that enable them to circumvent AML regulations (Dostov & Shust, 2014), becoming a viable solution for criminals, by allowing financial transactions to be made without being subject to scrutiny (Irwin & Milad, 2016).

Crypto-laundering is increasing extremely fast. While in 2017, $266 million was laundered using cryptocurrencies, by the second half of 2018 the estimated number was already at the $761 million mark (Crosman, 2018). These numbers only reflect on laundering of stolen funds and are not a complete estimate of all dark market transactions, leading to believe that the real number is higher.

This paper will later reflect more extensively on the subject of crypto-laundering, by analysing existing literature, in order to understand the risk factors that enable crypto-laundering, the way that crypto-laundering is conducted and its similarities with traditional ML methods.

3. THEORETICAL FRAMEWORK

Criminological theories are essential to answer one of the most complex of questions: why do people engage in criminal behaviour? (Gilmour, 2016b) However, this question was not posed enough regarding the virtual world.

Current literature has not yet delved into the use of virtual currency in money laundering and most criminological theories have not been tested for their application in explaining crimes related to cryptocurrencies or even in the cyber-world (Kethineni et al., 2018). Nonetheless, it was found that variables from self-control and social learning theories (e.g., low self-control, having deviant peers) predict involvement in some types of online deviance (see Louderback & Antonaccio, 2017, p. 641).

Although these theories, and others, have some power of explanation, this paper will base its theoretical grounds in the Rational Choice Theory (RCT). As the main focus of this thesis is to study the enabling factors of a specific crime, RCT can better support the analysis of the criminals' (perceived) benefits/costs of cryptocurrencies and crypto-laundering.

3.1. Rational Choice Theory

As a key criminological theory, RCT states that people generally act in their self-interest and make decisions to engage in criminal activities after a cost-benefit analysis, weighing the potential risks, including getting caught and punished, against the rewards that may come from their actions (Cornish & Clarke, 1987).

A criminal's rational choice may differ from crime to crime, but the reward concept is subjective to the criminal – this creates a myriad of decision-making scenarios (Gilmour, 2016b). When one decides to act upon one of these scenarios, even if not acting completely rationally, the decision is always "rational from the perspective of the offender" (Tierney, 2009, p. 13).

Gilmour (2016b) argues that RCT can explain money laundering. According to the author, the choices made in ML "are based upon a definable rational assessment of various factors associated with the scenario, as well as indirectly relevant factors" (p. 11). In this type of offence the criminal is aware that the risks associated are higher and failure will cause great losses (Gilmour, 2016b). With a rational decision-making process, criminals who engage in ML seek to lessen risks and efforts and increase rewards by "adopting a reversal of situational preventative techniques" (Gilmour, 2016b, p. 11).

Cybercrime presents a different reality from street crime: offenders in the online space show a varied set of behaviours and skills, and, the environment itself is different, especially considering the level of anonymity one can obtain in the internet (Kethineni et al., 2018). Characteristics of the internet have a bearing regarding rational choice theory. For instance, the lack of time and space barriers, the range of potential victims and the possibility of obtaining higher profits, influence the criminal into rationalizing the benefits of the offence as higher (Louderback & Antonaccio, 2017). Adding to this, criminals perceive costs and possibility of arrest as lower, due to the element of anonymity and the lack of physical contact with victims (ibid.).

4. METHODOLOGY

For this study to be set for replication, this section of the paper will outline the overall process followed within the chosen methodological model - systematic literature review. The aim of the chosen method will be explained, as the criteria for search, inclusion and exclusion of the data. This section will also include an analysis description and an overview on validity and reliability.

4.1. Systematic Literature Review

A systematic literature review is, as the name suggests, "a systematic way of collecting, critically evaluating, integrating, and presenting findings" (Pati & Lorusso, 2018, p. 15) from several research studies on a certain topic. This method was chosen to produce unbiased and comprehensive results of the reviewed literature, in order to better understand how money can be laundered using cryptocurrencies. To reach this understanding it is necessary to select, filter and evaluate the studies that are supposed to be included, as it is fundamental to disregard inadequate studies from further consideration (Harris, Quatman, Manring, Siston, & Flanigan, 2013).

4.1.1. Search Criteria

Since the selected method of data collection was a systematic literature review, it was essential to guarantee that the data would be collected in a systematic manner and with transparency, in order to identify the relevant research within the field of "Crypto-laundering". The first criteria for searching the chosen resources (studies, journals, articles and reports) was that they needed to have been peer-reviewed. However, "grey literature" was also considered, as it is important to look into field-specific articles and investigative reports to have a better understanding of the crypto-laundering phenomena (Pati & Lorusso, 2018).

To retrieve the most relevant journals, studies, and articles related to crypto-laundering, seven databases were used: The Malmö University's electronic library, the database of SAGE journals, JSTOR, ProQuest, Emerald, ScienceDirect and Google Scholar. These specific databases were selected as they are well-known and recommended by several scholars and librarians (Williams, n.d.). The search was conducted using the following "keywords": "crypto laundering"; "cyber laundering"; "virtual laundering"; "money laundering" AND "online" OR "cyber"; "money laundering" AND "cryptocurrencies" OR "bitcoin"; "money laundering" OR "cyber laundering" AND "cryptocurrencies" OR "bitcoin" OR "virtual currencies". Using the same databases, portuguese "keywords" were also searched: "criptolavagem"; "lavagem de dinheiro virtual"; "criptomoeda,"AND "lavagem de dinheiro" OR "branqueamento de capitais"; "lavagem de dinheiro" OR "branqueamento de capitais" AND "criptomoeda" OR "bitcoin" OR "moeda virtual". Moreover, only peer-reviewed articles were selected during the research procedure, to reassure scientific quality, as mention before.

Adding to peer-reviewed scientific articles, reports were also searched, in field specific websites, such as Europol, Financial Action Task Force, CipherTrace, UK National Crime Agency and Center of Sanctions and Illicit Finance. The reports were mainly retrieved from the websites "publications" or "documents" sections – no specific keywords were utilized when the search was performed.

4.1.2. Inclusion and Exclusion Criteria

There is a certain difficulty following new trends and tools criminal actors use for laundering illicit money. Cryptocurrencies were first considered as a tool for money laundering in 2012 (Federal Bureau of Investigation, 2012), hence a certain lack of literature on the subject. Nevertheless, a considerable number of articles were found using the search criteria mentioned above.

The major inclusion criterion is the reference of both money laundering and cryptocurrencies. Articles discussing crypto-laundering but with a focus on the legislation problematic, which does not concern this study, were excluded. Another exclusion criterion used relates to the taxonomy of digital currencies – articles that analyse any other currency besides cryptography protected, decentralised, convertible virtual currency (as explained in the background section), were not deemed relevant to this study. In addition, articles or reports that analysed money laundering or theft in crypto markets were excluded, as most do not portray cryptocurrencies as the main money laundering tool.

In order to assure that the articles included in the study were current, a time frame was implemented, thus only articles and reports from between 2012 and 2019 were considered. This time frame was selected, as it begins after the conceptual creation of Bitcoin in 2008 (Nakamoto, 2008), and in the same year that the FBI reported evidence of money laundering using cryptocurrencies (Federal Bureau of Investigation, 2012). Resources published before 2012 were used in this study to support the background and the theoretical sections.

Lastly, no geographical exclusion criterion was imposed, as crypto-laundering is a global phenomenon. However, articles and other literature written in other languages than English or Portuguese were excluded from this study, as an unbiased translation of the results cannot be guaranteed from articles who are written in languages that the author is not proficient in.

4.2. Analysis

"Analysis is the job of systematically breaking down something into its constituent parts and describing how they relate to each other" (Hart, 1998, p. 110). This systematic literature review will be analysed based on a method described by Cronin, Ryan, & Coughian (2008): First, summary or abstracts of the articles will be read, to understand if they fit the inclusion criteria, also in this phase a list of type of source, methodology and results will be produced. The next step will consist on reading and analysing the literature, this time using a more systematic and critical review of the content. The literature must be read several times to create familiarity and the PQRS (preview, question, read, summarize) process shall be included, as it will facilitate the identification and collection of material from the reviewed publications (Cronin et al., 2008). The third step in the analysis process will be to identify different themes in the articles, according to the different research questions. All articles will be compiled to enable an overview of the main points of the study. This procedure will allow and simplify integration of theoretical and empirical knowledge (Cronin et al., 2008). The last step is to formulate a text were the different articles main points are presented by theme, within the research questions.

4.3. Validity and Reliability

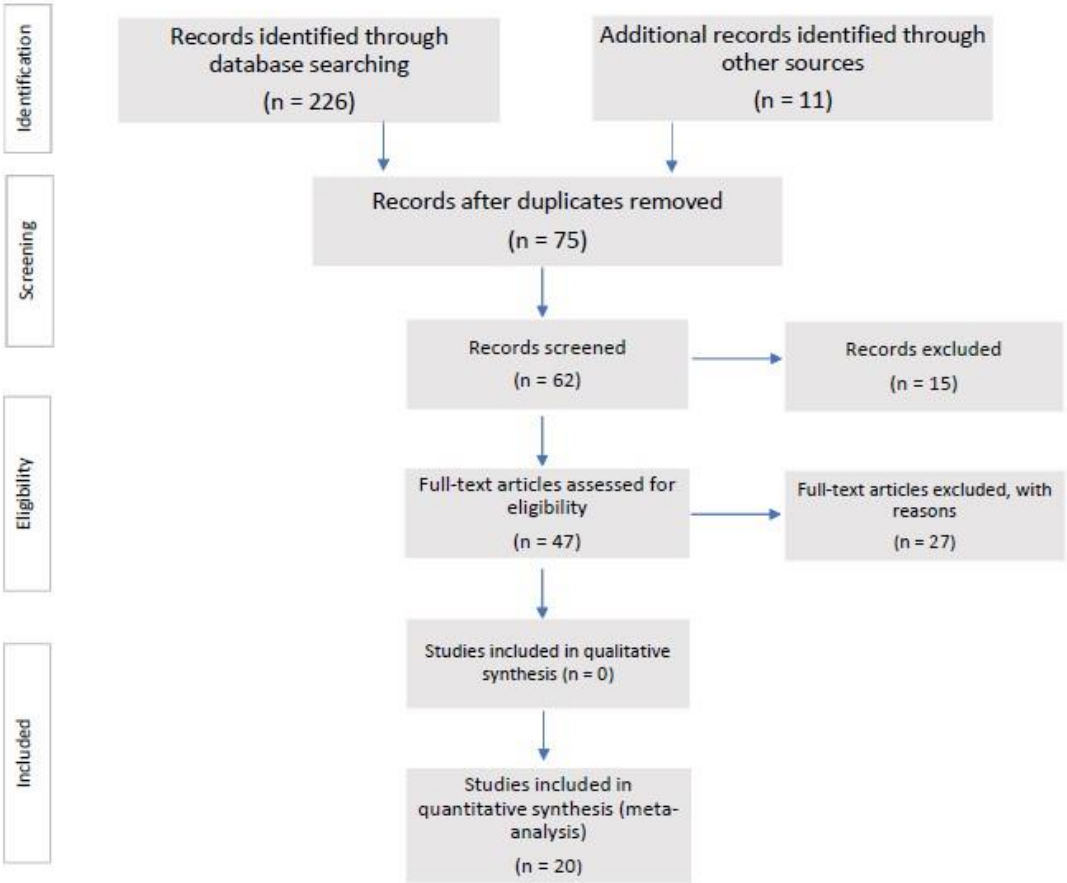
A high validity can be reached by forming a clear aim, clear research questions, and search for relevant sources to include in the study (Harris et al., 2013). The data should also be peer-reviewed to assure the study's quality, which in this case might be affected by the fact of inclusion of "grey literature". Validity and reliability can be obtained by setting limits, boundaries or inclusion and exclusion criteria (Cronin et al., 2008; Pati & Lorusso, 2018). To certify that this study would gain higher trust, these criteria was formulated in the beginning of the process.

A well described literature review search criteria will gain a high replicability (Pati & Lorusso, 2018), meaning that the study selection process should be drawn according with screening of findings, eligibility, and an assessment of the articles included in the review, in order for other researchers to repeat the study and get similar results. To make sure that the replicability remains high, a flow diagram (section 4.5.) and results table (appendix 1) will be included.

4.4. Ethics

This master's thesis was not subjected to an ethical approval from the Malmö University's academic committee, since the methodology followed is a systematic literature review and no one's integrity would be risked, no one would need to give their informed consent to participate in the study, no classified documents would be handled and the data used would be already published. Also, when doing a literature review, sources must be cited and referred in a proper way to facilitate others on finding the literature included in the thesis and to simplify the revision of the statements made. Therefore, a reference list will be provided.

4.5. Flow Diagram



5. RESULTS

This section will focus on the results obtained after having conducted a systematic literature review on crypto-laundering, which will be laid out based on the research questions that were set at the beginning of this paper. A table with the articles reviewed, including methodology and results, is presented on appendix 1.

5.1. Cryptocurrencies risk factors that enable ML

The literature referenced on appendix 1 mentions a variety of factors and characteristics that make cryptocurrencies directly or indirectly a risk for ML. These risk factors will be presented below.

Anonymity

This inherent characteristic of cryptocurrencies was the most referenced in the literature as being a high risk for ML. According to Stokes (2012) anonymity in transferring value is in fact a core ML risk associated with Bitcoin, as it obstructs viable audit by authorities, when following the money trail. Brenig et al. (2015) found that the pseudonymous nature of cryptocurrencies provides positive incentives to money launderers. Other studies (Ajello, 2015; Andrade, 2017; Brown, 2016; Choo, 2015; Christopher, 2014; Mabunda & Sobukwe, 2018; Wegberg et al., 2018) also indicate that the anonymous and near-untraceable nature of cryptocurrencies have an appeal for criminals, presenting a risk for ML.

Some authors (Möser et al., 2013; Reynolds & Irwin, 2017) discuss that anonymity is not entirely covered by the Bitcoin network, as although being far more complicated to uncover the identity of criminals than, for example, in banks, it is not impossible. Ergo, the term pseudonymous describes better the actual anonymity achieved by the system (Reynolds & Irwin, 2017).

Having this in mind, the literature provides evidence that cryptocurrencies still hold a high level of anonymity, which explains its popularity amongst criminals (Wegberg et al., 2018). For instance, even though all Bitcoin transactions are registered in a public blockchain, the "only data which is available is the amount of the transfer and the public addresses involved (…) and there are no records linking any public address to an individual or organisation." (Stokes, 2012, p. 225). Moreover, one can create for free an infinity number of Bitcoin wallets, resulting in increased anonymity (Christopher, 2014; Dyntu & Dykyi, 2018; Reynolds & Irwin, 2017) and due to lack of Know Your Costumer measures, the information necessary to open said wallets might be fictitious, which creates a problem when trying to trace back transactions (Christopher, 2014; Wegberg et al., 2018).

Adding to this, Möser et al. (2013), Wegberg et al. (2018) and Irwin & Turner (2018) shed light on the existence of services that anonymize the relation between users over a Bitcoin transaction - Bitcoin mixers. The way said services work to launder cryptocurrencies will be explored in the next segment (section 5.2.). For now, the fact that, on top of an already pseudonymous network such as Bitcoin, one can further eliminate traces of transactions, offers a higher level of attraction for money launderers.

Finally, Choo (2015) determined that anonymity is a risk factor present on all of the three stages of ML: the placement phase is facilitated by the possibility that cryptocurrencies wallets can be created by criminals (since there is no KYC meausures); the layering stage is potentiated by the possibility of opening accounts under fictitious information and the last stage, integration, benefits from the anonymous nature of cryptocurrencies by allowing the cashing out of criminal profits at automated teller machines (ATMs), or by transferring anonymously "to individuals who are the (true) beneficial owners and whose names do not appear on the account" (p. 303).

Speed and Portability

Peer-to-peer Bitcoin transactions occur instantaneously (Christopher, 2014), and so, the speed and ease at which Bitcoin transactions can be performed is seen by some authors (Ajello, 2015; Brenig et al., 2015; Stokes, 2012) as an advantage to criminal actors wanting to engage in ML, as it makes monitoring of accounts and transactions extremely difficult. Brenig et al. (2015) concluded that the transaction speed within cryptocurrencies "has an indirect effect on the execution of the ML process, providing positive incentives for money launderers" (p. 8).

Choo (2015) includes real-time transaction characteristic of bitcoins as a risk for ML, as in the placement phase illicit funds can be rapidly transferred to a different account or to fiat currency. As transactions are processed in real-time, the layering phase occurs with little chance of being perceived by authorities (ibid.). And finally, the integration phase is facilitated by the fact that illicit funds can be sent quickly through the system and withdrawn into fiat currency in a different part of the world (ibid.).

Stokes (2012), Christopher (2014), Ajello (2015) and Brenig et al. (2015) also observed that cryptocurrencies can be advantageous to ML due to their portability. These studies compared cryptocurrencies (mainly Bitcoin) with a more traditional anonymous ML vehicle (cash) and found that Bitcoin avoids certain limitations such as the physical transportation across international borders.

In his study, Brenig et al. (2015) suggest that portability has both a direct and indirect effect on the ML process, which provides positive incentives to whom might want to use cryptocurrencies as a ML channel.

Decentralization

The decentralization nature of cryptocurrencies is an intrinsic risk for laundering money (Ajello, 2015; Andrade, 2017; Brenig et al., 2015; Christopher, 2014; Dostov & Shust, 2014; Mabunda & Sobukwe, 2018). The administration system of cryptocurrencies functions without the intervention of a third-party, such as banks or other financial institutions (Ajello, 2015; Dyntu & Dykyi, 2018). With this comes the challenge of applying AML measures, such as KYC, as it is difficult to record and control information on every user (Dostov & Shust, 2014). Without these measures there is no proper protection against ML or reporting of suspicious activities, which is attractive to criminals (Ajello, 2015).

Brenig et al. (2015) also explain that these low barriers make cryptocurrencies a suitable instrument for high risk individuals searching for other channels to launder money. The same study found that the lack of a central authority provides positive incentives to ML.

Flexibility and Low transactions costs
The flexibility of creation of accounts and operation transactions in the Bitcoin network (Andrade, 2017; Brenig et al., 2015; Choo, 2015) and the low cost of said transactions (Brenig et al., 2015; Christopher, 2014) provide positive incentives for ML.

The placement stage is then easy to achieve, as criminals can divide their illicit funds into multiple wallets or into multiple cryptocurrencies – this will avoid triggering reporting requirements (Choo, 2015). Again, the flexibility of the cryptocurrency networks enables performing multiple transactions to obscure the money trail, which is utilized in the layering stage of ML (Andrade, 2017; Choo, 2015).

This flexibility is empowered by the low to no cost of transactions. The Bitcoin network "enables transfers directly between accounts, the only transaction costs of cryptocurrencies are the operating costs for authorization and verification of payments" (Brenig et al., 2015, p. 10). This renders a Bitcoin address as something disposable (Christopher, 2014), meaning that criminals can use a Bitcoin address once and then create multiple ones, which will favour, for example, smurfing.

Brenig et al. (2015) state that criminals ponder on transaction costs associated with ML activities, and logically, "the lower the costs for conducting these transactions are, the higher the revenue of ML" (p. 11). Cryptocurrencies provide then a more cost-efficient ML channel than traditional financial ones.

Lack of regulation
Some authors (Brown, 2016; Choo, 2015; Dyntu & Dykyi, 2018; Irwin & Turner, 2018) reviewed the lack of global, efficient and uniform virtual currency regulation as increasing the possibility of cryptocurrencies being exploited for ML.

Cryptocurrencies do not bear legal status, nor are they controlled by any government or country (Choo, 2015). According to Andrade (2017), most countries have no regulation whatsoever regarding virtual currencies (which include cryptocurrencies), while some are only now starting to create AML measures that comprise the digital environment.

This lack of consistent cryptocurrency regulation at a global level enables ML (Irwin & Turner, 2018), as criminals can send the illicit funds to countries with lax AML regulation, again obscuring the money trail (Gifari et al., 2017).

Irrevocability
Cryptocurrency transactions are irrevocable, for example, in the case of Bitcoin, once the network confirms the transaction, there is no process to have the transferred funds charged back (Brenig et al., 2015; Christopher, 2014; Mabunda & Sobukwe, 2018).

According to Brenig et al.'s (2015) analysis, this property of cryptocurrencies has simultaneously a direct and an indirect effect on ML. With irrevocability the risk of payment fraud is lower, which provides positive incentives to criminals who

want to use cryptocurrencies for ML. Besides, irrevocability has an indirect effect, also providing positive incentives, since it is impossible for authorities to reverse transactions, after these being confirmed by the network (ibid.).

Convertibility
As seen before, cryptocurrencies are convertible into fiat currency, and/or vice-versa. This characteristic enables the abuse of cryptocurrencies for ML (Brown, 2016; Choo, 2015; Wegberg et al., 2018).

Convertibility allows criminals to exchange illicit-funds gained through cyber-crime into fiat currency, since they can be withdrawn from another account in a different country, facilitating the integration phase (Choo, 2015). However, the inverse situation also might occur. According to Wegberg et al. (2018) criminals can use bitcoin as a solid cash-out strategy, meaning that their proceeds exist in form of fiat currency and by converting them into bitcoins, the illicit funds will be layered, thus obfuscating the money trail.

Acceptability and Price Volatility
Although these two features were mentioned, they did not yield as risk factors for ML, in fact, they were deemed a deterrent factor for criminals (Brenig et al., 2015; Choo, 2015; Christopher, 2014; Dostov & Shust, 2014).

Brenig et al. (2015) identified limited acceptance and high price volatility of cryptocurrencies as "the only factors in their study considered to provide negative incentives" (p.11) to ML.

Cryptocurrencies are very volatile and can easily devalue, for example, over a security incident, such as the bitcoin theft on Mt Gox (Choo, 2015). Since cryptocurrencies pose such a significant risk as a store of value, they might not be desirable as a ML channel (Christopher, 2014; Mabunda & Sobukwe, 2018).

Money laundering is frequently conducted by purchasing of commodities and services. Once most cryptocurrencies, including bitcoin, are not widely accepted, it becomes complicated for a money launderer to convert, move and integrate illicit funds using solely cryptocurrencies (Brenig et al., 2015).

5.2. How are cryptocurrencies used in ML?
One of the most common ways to launder money is through the purchase of commodities and services, however, due to limited acceptability of cryptocurrencies, other methods are utilized for crypto-laundering: Mixers, Darknet markets, exchange services and gambling/online game sites.

Anonymizer Services
As discussed before, the anonymity level presented by cryptocurrencies might be insufficient to launder money and evade authorities. Consequently, anonymizer services were created. These services are known as mixers, blenders or tumblers, and their function is to anonymize the relationship between sender and recipient of bitcoins (Custers, Pool, & Cornelisse, 2018; Möser et al., 2013).

According to Möser et al. (2013), mixers can be considered a money laundering tool, as they mask the origin of bitcoins. On their study on Bitcoin laundering, Fanusie & Robinson (2018) found that mixers have a "higher propensity to being

used for laundering bitcoins" (p.7). Other studies reflect the same idea (Custers et al., 2018; Dyntu & Dykyi, 2018; Gifari et al., 2017; Irwin & Turner, 2018; Kethineni et al., 2018; Sat et al., 2016; Wegberg et al., 2018).

Currently, several different mixing services exist, and most have somewhat suggestive names such as "BitLaundry" (Möser et al., 2013). Mixers combine transactions into several accounts owned by the service provider, so anyone inspecting the transactions will not be able to distinguish whose coins went where (Gifari et al., 2017; Irwin & Turner, 2018; Kethineni et al., 2018). According to Gifari et al. (2017), there are two main bitcoin mixing schemes. Criminals can choose a *traditional mixing scheme* that combines cryptocurrencies into a single communal pot, and then connects to several bitcoin addresses. There is also the option of using a *conjoin scheme*, which manipulates the blockchain into displaying several transactions as only one transaction.

Möser et al. (2013) found that not all mixers guarantee the same level of anonymity, for example, in their study "BitLaundry" was assessed as not providing anonymity, whilst others such as "BitFog" and "Blockchain.info" made it impossible to discover any direct connections in the blockchain.

It was observed, in Kethineni et al. (2018) study, that criminals use their illicit funds to directly purchases bitcoins via bitcoin exchanges, then utilize mixers to further cover the source of the funds. When a criminal successfully uses a bitcoin mixer and an underground bitcoin exchange, only process mistakes will lift the veil of anonymity (Wegberg et al., 2018).

Darknet Markets

The anonymous nature of the darknet (see appendix 2) is associated to illicit activities like drug trafficking and child pornography (Ajello, 2015). In this part of the internet one can find a multiplicity of markets that provide all kinds of services and products. One of the most famous markets was, the now extinct, Silk Road (Ajello, 2015; Fanusie & Robinson, 2018; Sat et al., 2016).

Since one of the most used ML methods is to spend the illicit proceeds on products and/or services (Custers et al., 2018), criminals soon discovered that darknet marketplaces such as Silk Road would be ideal to do so. Dyntu & Dykyi (2018) point out that "Silk Road was functioning as a somewhat of a Bitcoin's bank" (p. 79), as to make purchases one had to have a bitcoin address attached to his account on the website.

Fanusie & Robinson (2018) found that darknet marketplaces such as Silk Road and, later, AlphaBay, were the major source for most of the illicit bitcoins laundered. The same study observed that in 2016, a rise in bitcoins laundered in the darknet markets came from ransom and Ponzi schemes, signalling an increase in this type of cyber-crimes that continued into 2017.

Exchange Services

Exchange services provide currency exchange from fiat currency to cryptocurrency and vice-versa (Gifari et al., 2017). As mentioned previously (section 5.1.), this very factor of convertibility is favourable to ML. Due to its cash-out possibilities, exchange services enable this exact problem (Brown, 2016; Gifari et al., 2017).

Christopher (2014) theorized how exchange services (Mt. Gox and Liberty Reserve) would be a channel for ML, especially in the placement stage. In their study of crypto-laundering in Thailand, Gifari et al. (2017) saw the same pattern: first, there is an exchange of Indonesian Rupiahs (IDR) into bitcoins via the exchange service, then generally by using mixers and/or smurfing the founds are layered, and the integration stage is accomplished by selling again the bitcoins in a bitcoin exchange to get back IDR and withdrawing the money in a bitcoin ATM.

Also, Brown (2016) explained how easy the process is to convert fiat currency into bitcoins using electronic payment consoles in Bucharest, which only requires an e-mail address that can obviously be fictitious.

Both Fanusie & Robinson (2018) and the CipherTrace (2018) report found that Bitcoin exchanges account for the main share of total Bitcoin volume laundered. CipherTrace (2018) added that just regarding top exchanges, around 380.000 bitcoins were laundered, which at the time of the making of the report meant a value of 2.5 billion USD.

Gambling sites/ online gaming sites

Just like mixing services, gambling sites and online gaming sites provide a safe space to launder money. They facilitate all stages of ML. For instance, online gambling sites, such as Satoshi DICE, were considered by Irwin & Turner (2018) as "an ideal mechanism for crypto-laundering" (p. 302), for facilitating the placement phase, just as in land-based casinos. Also, according to Brown (2016) online gambling services and the purchasing of tokens in online games using cryptocurrencies is a way to "rehabilitate criminal proceeds" (p. 333).

Christopher (2014) explained how the process can be done in an online game, using the example of Second Life: credit cards can be used to buying Linden Dollars (the currency used in the game). Linden Dollars can then be sold (frequently using digital currency exchangers) for bitcoins, which will hinder the money trail.

Fanusie & Robinson (2018) concluded that mixers and online gambling sites "have a bitcoin laundering problem" (p. 10). They process a high proportion of dirty bitcoins, making them a significant concern for crypto-laundering (ibid.). The same study also identified that just three gambling services account for nearly half of all Bitcoin laundering.

5.3. Does crypto-laundering mirror traditional ML stages?

As one could observed in the last two sections, most characteristics enable one or more traditional ML stages, and most crypto-laundering methods go through the traditional process of placement, layering and integration (Andrade, 2017; Brenig et al., 2015; Choo, 2015; Christopher, 2014; Custers et al., 2018; Gifari et al., 2017; Mabunda & Sobukwe, 2018).

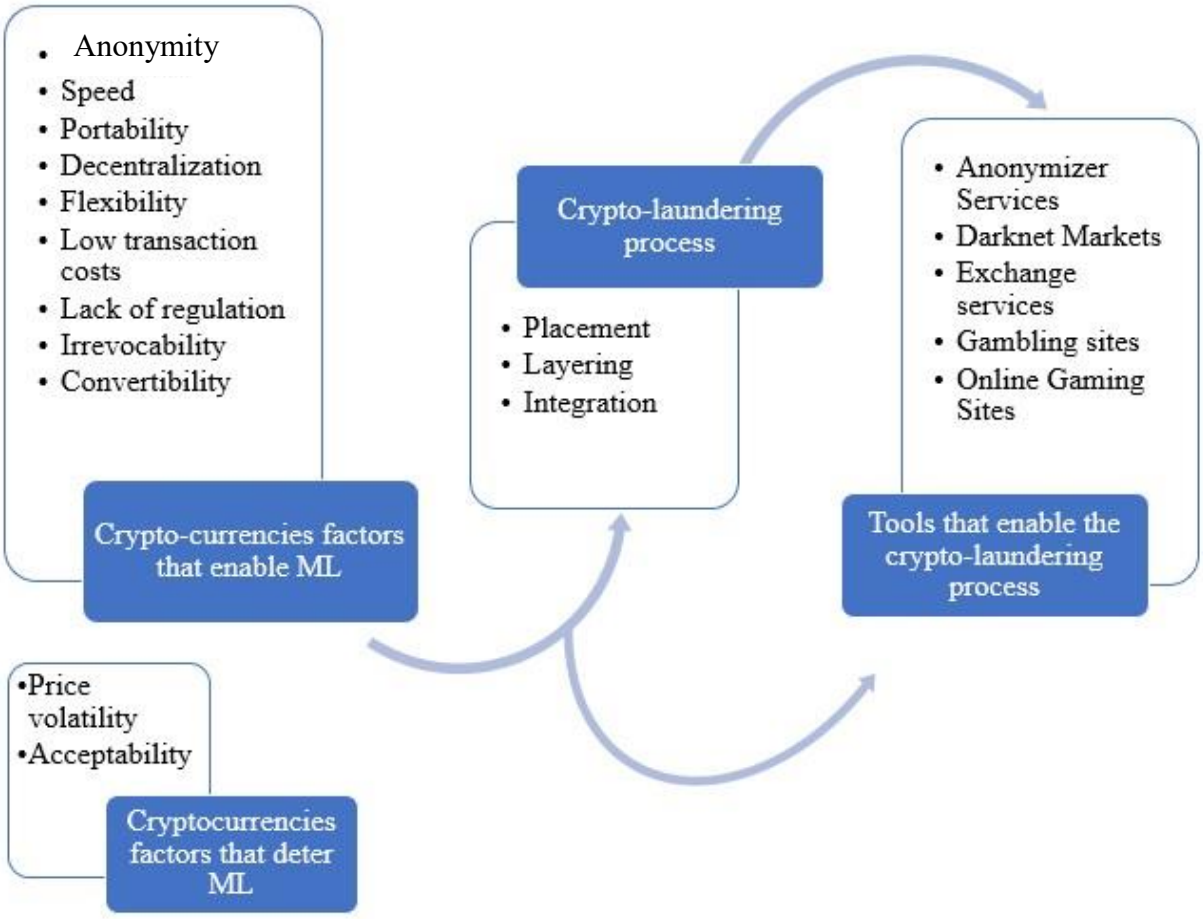
Money laundering is always preceded by a crime, and in the case of crypto-laundering the preceded crimes might also be committed online (ransomware, malware, etc.), nevertheless, the laundering process still shares several characteristics with "real-world" ML (Custers et al., 2018; Mabunda & Sobukwe, 2018)

According to Christopher (2014), the placement stage of the ML scheme is accomplished by quickly and cheaply converting illicit-funds into bitcoins, generally using exchange services. The second step, layering, is carried out by transferring bitcoins between wallets of one or more users. Since Bitcoin wallets contain little to no identifying data about the user, and users can have a countless number of wallets, such layering transactions will erase any record of ownership (ibid.). Finally, in the integration stage, the reverse of placement occurs, ergo the now clean funds are incorporated in the legitimate financial sector (ibid.).

On his study on bribery and corruption, Choo (2015) observed the same process: in the placement stage, the launderer introduces corruption earnings by acquiring cryptocurrencies. Once the proceeds are on the system, the layering stage is accomplished by transferring said cryptocurrencies to different accounts, often resorting to mixing services (ibid.). The integration happens when the funds are converted back into fiat currency, appearing to have been legally earned (ibid.).

As already mentioned, Gifari et al. (2017) found that crypto-laundering in Thailand follows the traditional stages of ML - for better understanding and visualization, a flow chart composed by the authors will be presented on the appendix 3. Adding to this, Custers et al. (2018) describe the same method for laundering illicit funds obtained from banking malware: converting stolen funds into bitcoins, dividing them into different bitcoin addresses and finally, integrating them by buying goods or converting back into fiat currency.

5.4. Summary of Results



6. DISCUSSION

The aim with this literature review was to understand which characteristics of cryptocurrencies enable money laundering and how criminals abuse such currencies. In the following section the results are going to be analysed and discussed. A discussion on limitations and implications for future studies will also be included.

6.1. Results Discussion

The literature reviewed provided answers to the research questions posed in this study. The summary of results (section 5.4.) shows that said answers are in fact entwined with each other. When analysing the results, it is visible that the ML risk factors of cryptocurrencies influence the crypto-laundering process and its tools. Adding to this, by finding that the crypto-laundering process follows the same stages as traditional ML it became clear that the tools involved were used to provide aid in the different steps. These relations between risk factors, process and tools, demonstrates that crypto-laundering is not only a complex and functional method, but also a real threat to AML.

Due to the extreme importance of knowing the risk factors that enable ML in order to prevent, protect, and fight against it (Stokes, 2012), this study first started by gathering information on said factors. By reviewing and analysing the literature, a set of characteristics - anonymity, speed, portability, decentralization, flexibility, low transaction costs, lack of regulation, irrevocability and convertibility – were found to have direct and/or indirect ML risks. This review only found two features of cryptocurrencies – price volatility and acceptability - as being a deterrent to their use as a laundering channel. These results reveal that cryptocurrencies have more attractive characteristics to criminals who want to engage in ML, than characteristics that would discourage them. Although one cannot know at this point if the two deterrence factors trump the enabling factors in the choice of pursuing crypto-laundering, it is worrying and worth investigating the fact that most characteristics of this currency are ML risk factors.

Most of the literature analysed mentions the element of anonymity, the possibility to convert fiat currency into cryptocurrency (and vice-versa) and the decentralized nature of cryptocurrencies as a direct ML risk. These characteristics attract criminals, which can be analysed according to the Rational Choice Theory. Thus, if criminals seek to lessen risks and increase rewards (Kethineni et al., 2018; Louderback & Antonaccio, 2017) and cryptocurrencies offer the possibility of laundering money in an anonymous, un-regulated space, with a cash-out solution, then crypto-laundering will be perceived as an extremely appealing choice. Higgins (2007) found that the more criminals perceive benefits of pirating online content, the more probability of cyber offending – since there is no research specific to crypto-laundering and RCT, one can only theorize that the same applies in the case of crypto-laundering, meaning that the more cryptocurrencies characteristics benefit criminals, the more the chance of engaging in crypto-laundering.

The second question intended to find an explanation to how cryptocurrencies are used to launder money. When looking to the results, different methods and channels are used to accomplish successful crypto-laundering. This paper only

analyses anonymizer services, darknet markets, exchange services, gambling and online gaming sites as crypto-laundering channels, however, there is a myriad of other channels, many of them unknown to researchers and authorities. The online environment is an ever evolving one, and constantly new ways to offend are being created or adapted, which generates a greater problem – the impossibility to prevent the unknown.

Again, the risk factor anonymity is intertwined, since the methods/channels analysed in this paper – especially anonymizer services – provide an extra layer of "smoke", which authorities and researchers have not yet the tools to study or deconstruct. This might be the reason why most National Risk Assessments (BCFT, 2015; HM Treasury & Home Office, 2017; Statsadvokaten, 2015; van der Veen & Heuts, 2017) classify the risk of crypto-laundering as low, or do not even mention the problematic. In fact, Brown (2016) explains that although cryptocurrencies are being used extensively for crime, they are not yet entirely on the authorities' radar, due to the complexity of investigative implications or, simply, they are not even considered.

Finally, the third question aimed to determine if crypto-laundering mirror traditional ML stages. One can observe that, according to the results, crypto-laundering also follows a "placement, layering and integration" structure.

According to Mabunda & Sobukwe (2018), the crypto-laundering process is similar to the traditional one, and so are its consequences. A worrying aftermath of traditional ML is the investment of funds in other illegal activities, and crypto-laundering presents the same problem, especially online, where the funds may be used to acquire child pornography, trafficking of drugs, trafficking of guns, and/or to invest in tools to perpetrate other types of cyber-crime (e.g., malware).

By mirroring the same structure, crypto-laundering also opens the door for terrorism financing. According to Irwin & Milad (2016) terrorist groups use the same type of techniques as money launderers to elude authorities and omit the identity of sponsors and beneficiaries of funds. Therefore, crypto-laundering becomes an ideal instrument for terrorist organizations as it warrants a great level of anonymity, and financing becomes faster and borderless, without attracting attention of authorities (Hunt, 2011; Irwin & Milad, 2016; Sat et al., 2016; Teichmann, 2018; Whyte, 2019).

6.2. Limitations

The study must be seen in light of some limitations. Firstly, literature reviews have inherent limitations, as the author has to rely on previously published research, the availability of these studies, and the appropriateness of these studies regarding the inclusion and exclusion criteria (section 4.1.2.).

Secondly, there was a need to resort to grey literature (e.g. official and field-specific reports) to better understand the global knowledge within the subject. The decision to include such literature might affect the validity of the study, as "grey literature does not have to meet the criteria of peer-reviewed publications" (Pappas & Williams, 2011, p. 229).

Cryptocurrencies are a recent phenomenon, created ten years ago, making crypto-laundering a new and under researched topic. This creates limited resources of

information and scientific studies on the subject, especially within the field of criminology (Kethineni et al., 2018; Willison & Lowry, 2018). Adding to this problematic, most articles reviewed focused solely on Bitcoins, which limits the knowledge on cryptocurrencies in general.

Finally, some of the literature here reviewed were partly or entirely literature reviews. Although the author controlled for not overlapping studies, there was no control regarding if the information used were from articles older than 2012, which was the limit stipulated on section 4.1.2. The use of literature reviews is then a major limitation of this paper, and it most be taken in consideration when analysed.

6.3. Practical and Future Implications

The criminological field must start delving into the cybercrime arena. The lack of knowledge, research and applicability of criminological theories into subjects such as crypto-laundering might be producing a proliferation of crime in the online environment.

It is a pressing matter that criminology joins forces with other fields and explores crime in the virtual world, especially to investigate if the existent theories of crime can be applied in the online environment, or if it is necessary to create a separate theory. A few steps have already been made in that direction, as for example, Louderback & Antonaccio (2017) confirmed that TRDM, an innovative concept with roots on RCT, is a significant predictor of cyber deviance involvement. It would be of interest to study if this concept could be applied to crypto-laundering.

This literature review demonstrates that cryptocurrencies have more characteristics that appeal to launderers than deters them. Thus, it is necessary to conduct further studies on different aspects of this crime, such as process, methods, channels. Similarly of interest, would be to identify who engages in crypto-laundering (is it part of the organized crime sphere? is it a new generation of criminals who operate only online?) or trying to understand which types of crimes generally precede crypto-laundering (traditional crime or cyber-crime).

It was also observable that crypto-laundering leads to serious consequences, such as terrorism financing. This is of extreme importance to analyse further, especially to identify how terrorist or other criminals abuse, protect and invest their funds using cryptocurrencies.

7. CONCLUSIONS

This paper aimed to explain how cryptocurrencies enable money laundering, and by analysing literature on the subject it was possible to conclude a variety of characteristics that do so, methods that are employed in crypto-laundering and how it mirrors traditional money laundering stages.

The results showed that the anonymity of transactions, decentralization, convertibility associated with the lack of specific regulations regarding cryptocurrencies, is related to the expansion and specialization of money

laundering. Adding to this, there is a collection of services online that also potentiate crypto-laundering, such as mixers and darknet markets.

The transfer of traditional crime into the virtual world must become a major concern to the criminological community, which in turn, needs to start exploring the (not so) new world of cyber-crime.

REFERENCES

Ajello, N. J. (2015). Fitting a Square Peg in a Round Hole: Bitcoin, Money Laundering, and the Fifth Amendment Privilege Against Self-Incrimination. *Brooklyn Law Review*, *80*(2), 435–461.

Andrade, M. (2017). Legal treatment of crypto-coins: the dynamics of bitcoins and the crime of money laundering. *Brazilian Journal of Public Policy*, *7*(3), 44–59.

BCFT. (2015). *National risk assessment of money laundering and financing of terrorism*. >http://www.portalbcft.pt/sites/default/files/anexos/pt_nra_synthesis.pdf < (Retrieved 22 Apr 2019)

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

Brenig, C., Accorsi, R., & Müller, G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. In *ECIS 2015 Completed Research Papers* (pp. 1–18).

Brown, S. D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. *The Police Journal: Theory, Practice and Principles*, *89*(4), 327–339.

Bryans, D. (2014). Bitcoin and Money Laundering: Mining for an Effective Solution. *Indiana Law Journal*, *89*(441), 441–472.

Choo, K. R. (2015). Cryptocurrency and Virtual Currency: Corruption and Money Laundering/ Terrorism Financing Risks? In D. Chuen (Ed.), *The Handbook of Digital Currency* (1st ed., pp. 283–306). Elsevier Inc.

Christopher, C. M. (2014). Whack-a-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Money Laundering. *Lewis and Clark Law Review*, *18*(1), 1–36.

CipherTrace. (2018). *Cryptocurrency Anti-Money Laundering Report 2018 Q3*. >https://ciphertrace.com/crypto-aml-report-2018q3.pdf < (Retrieved 22 Feb 2019)

Cornish, D. B., & Clarke, R. V. (1987). Understanding crime displacement: an application of rational choice theory. *Criminology*, *25*(4), 933–948.

Cronin, P., Ryan, F., & Coughian, M. (2008). Undertaking A Literature Review: A Step-by-Step Approach. *British Journal of Nursing*, *17*(1), 38–44.

Crosman, P. (2018). Crypto money laundering up threefold in 2018: Report. *American Banker*, *183*(128), 1.

Custers, B. H. M., Pool, R. L. D., & Cornelisse, R. (2018). Banking malware and the laundering of its profits. *European Journal of Criminology*, *00*(0), 1–18.

Dostov, V., & Shust, P. (2014). Cryptocurrencies : an unconventional challenge to the AML / CFT regulators ? *Journal of Financial Crime*, *21*(3), 249–263.

Dyntu, V., & Dykyi, O. (2018). Cryptocurrency in the System of Money Laundering. *Baltic Journal of Economic Studies*, *4*(5), 75.

European Institute of Management & Finance. (2018). *Understanding Money Laundering*. >https://eimf.eu/understanding_money_laundering/ < (Retrieved 5 Apr 2019)

Fanusie, Y. J., & Robinson, T. (2018). *Bitcoin Laundering : An Analysis of Illicit Flows into Digital Currency Services*. >https://s3.us-east-2.amazonaws.com/defenddemocracy/uploads/documents/MEMO_Bitcoin_Laundering.pdf < (Retrieved 15 Feb 2019)

FATF. (2014). *Virtual Currencies - Key Definitions and Potential AML / CFT Risks*. >https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf < (Retrieved 15 Feb 2019)

FATF. (2017). *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion With a Supplement on Customer Due Diligence*. >http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf < (Retrieved 15 Feb 2019)

Federal Bureau of Investigation. (2012). *Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity*. >https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf < (Retrieved 15 Feb 2019)

Filipkowski, W. (2008). Cyber Laundering : An Analysis of Typology and Techniques. *International Journal of Criminal Justice Sciences*, *3*(1), 15–27.

Gifari, A., Anggorojati, B., & Yazid, S. (2017). On Preventing Bitcoin Transaction from Money Laundering in Indonesia: Analysis and Recommendation on Regulations. In *2017 International Workshop on Big Data and Information Security (IWBIS)* (pp. 143–148).

Gilmour, N. (2016a). Preventing money laundering: a test of situational crime prevention theory. *Journal of Money Laundering Control*, *19*(4), 376–396.

Gilmour, N. (2016b). Understanding the practices behind money laundering - A rational choice interpretation. *International Journal of Law, Crime and Justice*, *44*, 1–13.

Harris, J. D., Quatman, C. E., Manring, M. M., Siston, R. A., & Flanigan, D. C. (2013). How to Write a Systematic Review. *The American Journal of Sports Medicine*, *42*(11), 2761–2768.

Hart, C. (1998). *Doing a literature review: Releasing the social science research imagination* (2nd Editio). London: SAGE Publications, Inc.

He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M.,

Stetsenko, N. (2016). *Virtual Currencies and Beyond: Initial Considerations*. >https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf < (Retrieved 18 Feb 2019)

Higgins, G. E. (2007). Digital Piracy, Self-control Theory, and Rational Choice: An Examination of the Role of Value. *International Journal of Cyber Criminology*, *1*, 33–55.

HM Treasury, & Home Office. (2017). *National risk assessment of money laundering and terrorist financing 2017*. >https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf < (Retrieved 15 Apr 2019).

Hunt, J. (2011). The new frontier of money laundering: How terrorist organizations use cyberlaundering to fund their activities, and how governments are trying to stop them to stop them. *Information and Communications Technology Law*, *20*(2), 133–152.

Irwin, A. S. M., & Milad, G. (2016). The use of crypto-currencies in funding violent jihad. *Journal of Money Laundering Control*, *19*(4), 407–425.

Irwin, A. S. M., & Turner, A. B. (2018). Illicit Bitcoin transactions: challenges in getting to the who, what, when and where. *Journal of Money Laundering Control*, *21*(3), 297–313.

Kethineni, S., Cao, Y., & Dodge, C. (2018). Use of Bitcoin in Darknet Markets : Examining Facilitative Factors on Bitcoin-Related Crimes. *American Journal of Criminal Justice*, *43*, 141–157.

Louderback, E. R., & Antonaccio, O. (2017). Exploring Cognitive Decision-making Processes, Computer-focused Cyber Deviance Involvement and Victimization: The Role of Thoughtfully Reflective Decision-making. *Journal of Research in Crime and Delinquency*, *54*(5), 639–679.

Mabunda, S., & Sobukwe, R. (2018). Cryptocurrency : The New Face of Cyber Money Laundering. In *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)* (pp. 1–6). IEEE.

Möser, M., Böhme, R., & Breuker, D. (2013). An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. In *2013 APWG ECrime Researchers Summit, ECrime Researchers Summit (ECRS)*.

Nakamoto, S. (2008). *Bitcoin : A Peer-to-Peer Electronic Cash System*. >https://bitcoin.org/bitcoin.pdf < (Retrieved 15 Feb 2019)

Nian, L., & Chuen, D. (2015). Introduction to Bitcoin. In D. Chuen (Ed.), *The Handbook of Digital Currency* (1st ed., pp. 6–29). Elsevier Inc.

Pappas, C., & Williams, I. (2011). Grey literature: Its Emerging Importance. *Journal of Hospital Librarianship*, *11*(3), 228–234.

Pati, D., & Lorusso, L. N. (2018). How to Write a Systematic Review of the Literature. *Health Environments Research & Design Journal*, *11*(1), 15–30.

Plassaras, N. A. (2013). Regulating digital currencies: bringing bitcoin within the reach of IMF. *Chicago Journal of International Law*, *14*(1), 307–407.

Protek Support. (2018). *Is Your Business Exposed to the Dark Web? - Protek Support*. >https://proteksupport.com/is-your-business-exposed-to-the-dark-web/ < (Retrieved 6 May 2019).

Reid, F., & Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System. In *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing* (pp. 1318–1326). IEEE.

Reynolds, P., & Irwin, A. S. M. (2017). Tracking digital footprints: anonymity within the bitcoin system. *Journal of Money Laundering Control*, *20*(2), 172–189.

Sat, D. M., Krylov, G. O., Evgenyevich, K., Bezverbnyi, Kasatkin, A. B., & Kornev, I. A. (2016). Investigation of Money Laundering Methods Through Cryptocurrency. *Journal of Theoretical and Applied Information Technology*, *83*(2), 244–254.

Schott, P. A. (2006). *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism*. >http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf < (Retrieved 22 Mar 2019).

Statsadvokaten. (2015). *Money Laundering in Denmark - National Risk Assessment 2015*. >https://anklagemyndigheden.dk/sites/default/files/Documents/Money Laundering Secretariat - National Risk Assessment 2015.pdf < (Retrieved 12 Apr 2019).

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

Teichmann, F. (2018). Financing terrorism through cryptocurrencies – a danger for Europe? *Journal of Money Laundering Control*, *21*(4), 513–519.

The Economist. (2018). Crypto money-laundering: Digital detergent. *The Economist (UK)*, *414(9086)*, 68.

Tierney, J. (2009). *Key Perspectives in Criminology*. Berkshire, GBR: Open University Press.

Tropina, T. (2015). Fighting money laundering in the age of online banking, virtual currencies and internet gambling. *ERA Forum*, *15*(1), 69–84.

United Nations Office on Drugs and Crime. (2018). *Money-Laundering and Globalization*. >https://www.unodc.org/unodc/en/money-laundering/globalization.html < (Retrieved 5 Apr 2019)

Van der Veen, H. C. J., & Heuts, L. F. (2017). *National Risk Assessment on Money Laundering for the Netherlands.* >https://www.wodc.nl/binaries/Cahier 2017-13a_2689c_Full text_tcm28-328683.pdf < (Retrieved 23 Apr 2019).

Wegberg, R. Van, Oerlemans, J.-J., & Deventer, O. Van. (2018). Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, *25*(2), 419–435.

Whyte, C. (2019). Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise. *Studies in Conflict & Terrorism*, 1–24.

Williams, B. (n.d.). *Criminology, Law and Society: Criminology Databases*. >https://guides.lib.uci.edu/criminology/crim/databases < (Retrieved 5 Apr 2019).

Willison, R., & Lowry, P. B. (2018). Disentangling the Motivations for Organizational Insider Computer Abuse through the Rational Choice and Life Course Perspectives. *Data Base for Advances in Information Systems*, *49*(s1), 81–102.

APPENDIX 1

Results from the articles used in the systematic literature review:

Author and Publication year	Type	Methodology	Results
Stokes (2012)	Original Article	This paper reviewed literature and presented an analysis of the ML risks of both Linden dollar and Bitcoin.	Bitcoin has potential for ML, especially due to anonymity, speed and decentralised nature. The author also demonstrates that at the time of research bitcoin had ML utility but was still unsuitable for laundering on a large scale.
Möser, Böhme and Breuker (2013)	Conference Article	Several experiments were conducted, using reverse-engineering methods, to understand the operation mode of three different mixers and try to trace anonymized transactions back to the probe accounts.	The authors concluded that not all mixing services provide the same level of anonymity. While BitcoinFog and Blockchain.info successfully anonymize the test transactions, BitLaundry was still traceable.
Dostov and Shust (2014)	Original Article	Descriptive analysis of Digicash and Bitcoin and comparison to cash and cashless payments. "Bundle of attributes" was also analysed, to understand their attractiveness to criminals.	Cryptocurrencies characteristics are unlikely to make them widespread, as demand for anonymity seems to be overvalued. It is also shown that there is ML risk in cryptocurrencies, due to the decentralized and anonymous nature.
Christopher (2014)	Original Article	This article addresses the crime of money laundering and its related criminal activities. Only part II was considered for this literature review as it presents a descriptive analysis of Bitcoin as a ML vehicle.	The paper explains how anonymity and convertibility in the Bitcoin system play a part in ML. The author also alludes to how currency exchangers are used in the crypto-laundering process.
Choo (2015)	Original Article	The article offers a literature review to explain cryptocurrency and corruption, and provides a descriptive analysis of Bitcoin's characteristics and how these traits increase the risk of laundering corruption funds.	Near anonymity, elusiveness, high negotiability, real-time transaction, utility and withdrawal of funds were concluded to be ML and terrorism financing risk factors regarding the three money laundering stages.

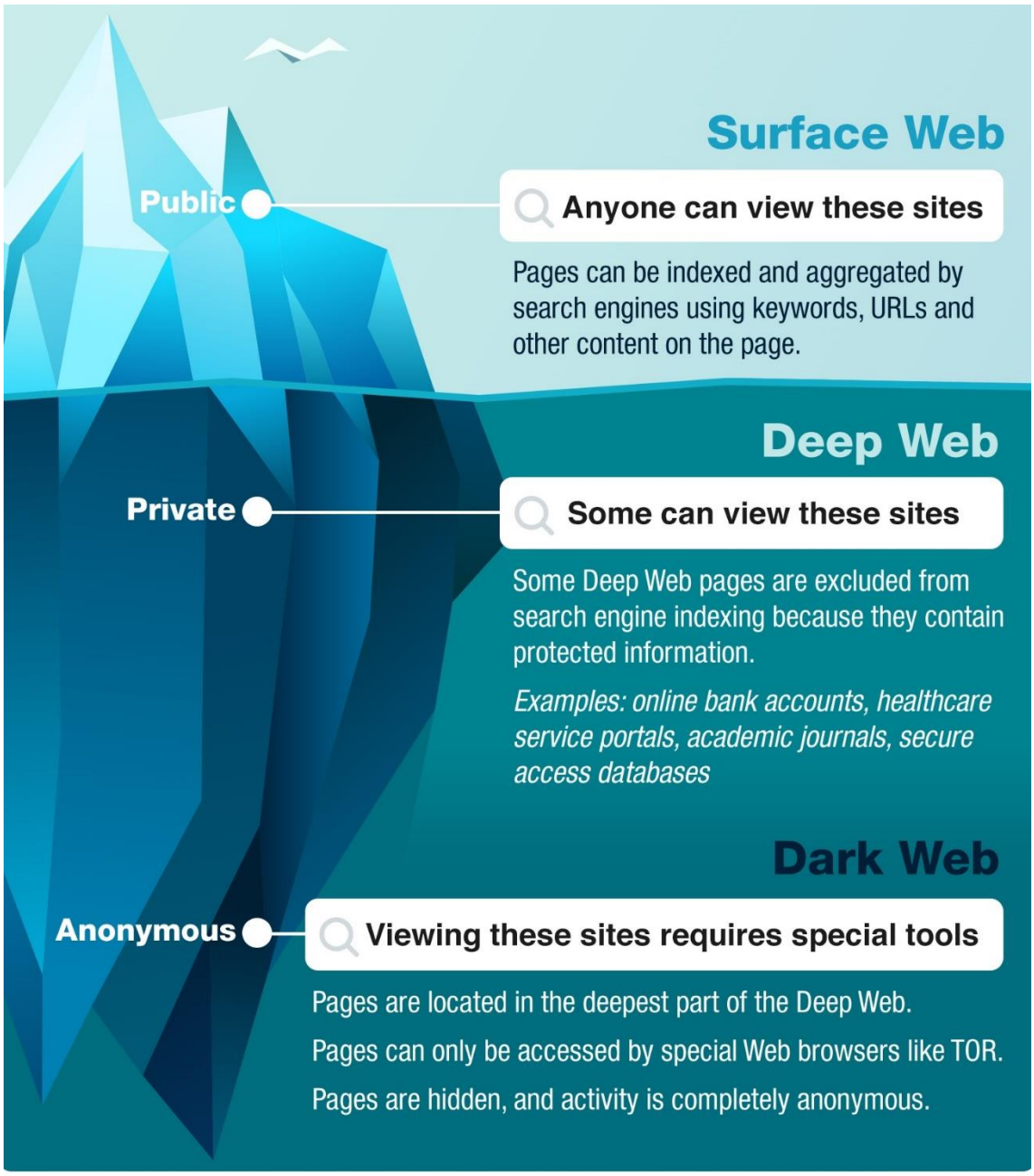
Brenig, Accorsi and Müller (2015)	Conference Article	This paper addresses if cryptocurrencies are a ML risk, by conducting an analysis on contextual and transactional factors influencing the incentives of criminals. To identify said factors literature of organizations responsible for AML and academic and online literature on cryptocurrency's vulnerabilities were reviewed.	Contextual factors identified: acceptability, administration, authentication level and price volatility. Transactional factors identified: Flexibility, irrevocability, payment processing, portability, rapidity and transactions costs. Acceptability and price volatility were the only factors considered to provide negative incentives to ML.
Ajello (2015)	Original Article	The article is divided in four different parts, being the first part a literature review to explain Bitcoin's traits and use and how these traits increase the risk of money laundering. The other sections of the article focus on regulation, which does not concern this paper.	Bitcoin as a vehicle for ML due to decentralized nature, anonymous trait and speed and ease with which Bitcoin transactions are executed.
Brown (2016)	Original Article	The article explores Bitcoin, as the currency of criminals, by reviewing literature and study cases on its use in different types of crimes, including ML.	The article explains that anonymity, decentralization and convertibility are risks for ML. Regarding the latter, the article provides an analysis on currency converters and electronic payment consoles.
Sat, Krylov, et al. (2016)	Original Article	The article investigates crypto-laundering methods, by performing a bitcoin transaction data analysis (using cluster and principal component analysis methods). A relational database was designed and implemented for storage and processing.	The hypothesis of the existence of signs of identification of crypto-laundering was verified. Mixing-services, anonymous altcoins and darknet markets were considered methods of crypto-laundering.

Gifari, Anggorojati and Yazid (2017)	Conference Article	A qualitative approach is used in this research for data collection and analysis. Interview with two experts representing bitcoin exchange company and legal consultant was conducted in data collection. The study was conducted in Indonesia.	The paper concludes that the misuse of bitcoin is due to exploitation of its pseudonymous nature. The authors were also able to describe how ML is processed in Indonesia using cryptocurrencies, and how mixing services and exchange services aid said offense.
Andrade (2017)	Original Article	The article uses a qualitative approach, with support in literature review and descriptive analysis of ML with cryptocurrencies.	The authors determined that it is not possible to directly associate the use of bitcoins as the only variable of weight in relation to the illicit practice of ML. Lack of specific regulation for cryptocurrencies with decentralization and anonymity of transactions is related to the expansion and specialization of ML.
Reinolds and Irwin (2017)	Original Article	The article contains a literature review on anonymity of users and the potential ability to track transactions through the blockchain and an experiment on four different Bitcoin exchange services to determine whether information provided at the sign-up stage is sufficiently verified and reliable.	It may be possible to recognise criminal actors through the analysis of transaction histories by tracing them back to an interaction with a Bitcoin exchange. However, the compliance of AML rules are inadequately implemented within some exchange services, thus criminals are able to evade identification controls and continue to transact anonymously.
Wegberg, Oerlemans and Deventer (2018)	Original Article	This paper presents a cash-out experiment in which five mixing and five exchange services are analysed, having an especial focus on service-percentages and reputation-mechanisms in underground bitcoin laundering services.	Some of the examined services provide an excellent, professional and well-reviewed service at competitive cost. Whereas others turned out to be frauds, accepting bitcoin without return.

Mabunda (2018)	Conference Article	Literature review and comparative analysis between Bitcoin and liberty reserve, regarding ML.	This article reveals that ML with cryptocurrency shares a lot of common characteristics with the archetypal ML, as the process is the same and so is the consequences of thereof. It is the cryptocurrency properties - anonymity, security, irreversibility and decentralisation - that enable ML.
CipherTrace (2018)	Report	Intelligence report on cryptocurrencies and AML. Quantitative analyses of 45 million transactions at the 20 top cryptocurrency exchanges globally.	Main results: 97% of direct criminal bitcoin payments are sent to unregulated exchanges; 36 times more criminal bitcoin is received by cryptocurrency exchanges in countries with lax AML regulation; cryptocurrency ML on top exchanges involves a significant amount of bitcoin (some 380,000 bitcoins or $2.5 billion at today's prices).
Kethineni, Cao and Dodge (2018)	Original Article	The article explores Bitcoin-related offenses, including ML. The research utilized 3 online sources (LexisNexis, Google, and PACER) to identify 12 criminal cases involving bitcoins. Content analysis is used to assess what factors contribute to Bitcoin-related offenses.	Four factors were found to facilitate crypto-laundering in darknet markets: identity and flexibility, dissociative anonymity, ease of associating in cyberspace, and lack of deterrence.
Irwin and Turner (2018)	Original Article	A literature review was conducted to understand the main law enforcement challenges of anonymity and attribution. The paper also reviewed research and projects that aim to identify illicit transactions involving cryptocurrencies and the darknet.	Cryptocurrencies are defined as an ideal mechanism, which facilitate the laundering of criminal proceeds via mixers and gambling sites. Anonymity is seen as risk factor.

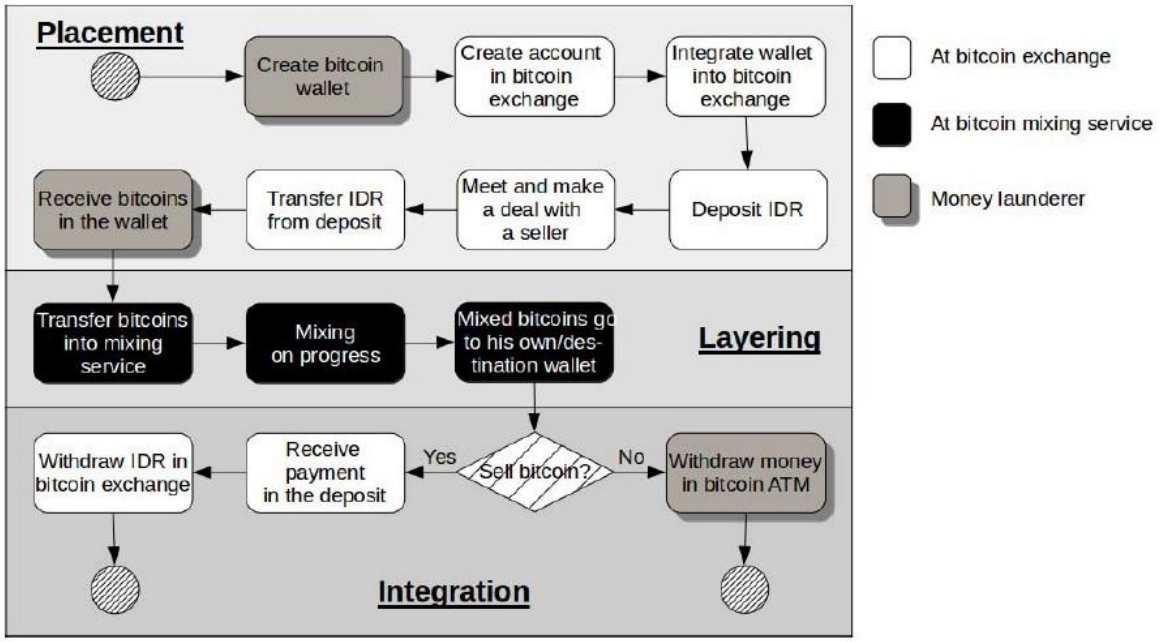
Fanusie and Robinson (2018)	Report	The report used a forensic analysis tool, which combines public blockchain data with a proprietary dataset of Bitcoin addresses associated with known entities, to show who is transacting with whom in Bitcoin and to identify bitcoins moving from illicit entities to conversion services. The transaction data reviewed comprised the years between 2013 and 2016.	Two types of services – mixers and online gambling services – receive a high proportion of illicit bitcoins and thus, are substantial concerns for Bitcoin laundering. Also, services which appear to hide their location have high rates of Bitcoin laundering activity.
Custers, Pool and Cornelisse (2018)	Original Article	To describes how profits of banking malware are laundered, different methodologies were used: a literature review; 20 semi-structured interviews were conducted; and a total of four police files with criminal cases were investigated. The research was carried out in 2016, in the Netherlands.	Banking malware profits that are exchanged into bitcoins may simply be put in a bitcoin wallet, which serves as a savings account. The article also mentions that cybercriminals will use anonymization software such as Tor or mixing services, to improve the level of anonymity.
Dyntu and Dykyi (2018)	Original Article	The research is based on an analysis of historical stages of cryptocurrency creation. Moreover, there were analysed cases of money laundering where criminals who used cryptocurrency have been identified and press charged. In addition, the comparative methods were used to collate different positions regarding cryptocurrency all over the world and inside Ukraine.	Cryptocurrency is a convenient tool for ML due to: relative anonymity; decentralized nature; and the user can have more than one account and conduct transactions from different places at the same time.

APPENDIX 2



Iceberg Diagram on the different Internet anonymity stages (Protek Support, 2018)

APPENDIX 3



Bitcoin money laundering flow in Thailand (Gifari et al., 2017, p. 146).