Expertise
and insight
for the future

Thuy Thu Vo

Applying the Anti-Money Laundering regulations of virtual currency to build an effective internal control process

Case Study: Finland

Metropolia University of Applied Sciences

Bachelor of Business Administration

International Business & Logistics

Thesis

29 April 2020

Author(s) Title Number of Pages Date	Thuy Thu Vo Applying the Anti-Money Laundering regulations of virtual currency to build an effective internal control process Case Study: Finland 47 pages + 1 Appendix 29 April 2020
Degree	Bachelor of Business Administration
Degree Programme	International Business & Logistics
Specialisation option	Finance
Instructor(s)	Michael Keaney, Senior Lecturer

The growing adoption of virtual currency-related business activities has posed increasing challenges to law enforcement. Virtual currency offers a novel solution for both individuals and organisations to engage in money laundering activities and bypass the detection of law enforcement. Therefore, in the European context, the authority continuously introduces stricter regulations to the virtual currency service providers, creating pressure on the companies to meet the necessary legal requirements to avoid the reputational risk and ensure the existence of the business.

The objective of this thesis is to combine the literature and legislative texts related to virtual currency to create an AML internal process for a case company in the Finnish context. A qualitative approach featuring the case study was used because it is the most suitable approach to identify the business challenge and provide a solution to address the European regulation as transposed into law in Finland.

The outcome is the internal AML process proposal which was depicted as a swim lane chart detailing the company's departments and communication flow. The result would ensure agile AML execution and make the compliance process aligned with the company's strategy. The proposal would provide a preliminary means for the companies in constructing their AML program while complying to the stricter AML regulations.

Keywords	Anti-money laundering, virtual currency, regulation, AMLD5

Contents

Appendices

Appendix 1. Interview Questions for Case Company Personnel

List of Figures and Tables

List of Abbreviations

AML	Anti-Money Laundering
AMLD	Anti-Money Laudering Directive
CDD	Client Due Diligence
CWP	Custodian Wallet Provider
DLT	Distributed Ledger Technology
EDD	Enhanced Due Diligence
FATF	The Financial Action Task Force
FIN-FSA	Finnish Financial Supervisory Authority
FIU	Financial Intelligence Unit
ICO	Initial Coin Offering
IMF	International Monetary Fund
KYC	Know-Your-Customer
OTC	Over-The-Counter
P2P	Peer-to-peer
PEP	Politically Exposed Person
UBO	Ultimate Beneficial Owner
VASPs	Virtual Asset Service Providers
VC	Virtual Currency
VCEPs	Virtual Currency Exchange Providers

1 Introduction

1.1 Thesis' background and objectives

The activity of masking the origin of money obtained from criminal activities is indeed an old practice. This activity can be traced back to the 1920s when mafia families in the United States actively engaged in opening business "fronts" to launder their financial benefits derived from illegally lucrative businesses such as human trafficking, drugs, and arms (Levi & Reuter, 2006). The rapid globalisation process took place only after the second half of the 20th century has increased levels of transnational investment and technological transition across countries. As a result, criminal groups and terrorist organisations can now quickly move funds from one country to another while taking advantage of the discrepancy in the legislation of different states and territories.

A common dilemma is that, when criminals want to spend their illegally-earned money, this could potentially draw the attention of tax auditors or law enforcement authorities. As new financial instruments emerge into the global market, money launderers regularly adapt how and where they could convert and transfer the funds into other assets such as virtual currency ("VC") to circumvent the regulations enacted by the authority to identify and disrupt illegal activities. From the regulatory standpoint, the growing adoption of VC-related business activities have posed increasing challenges to not only the traditional banking system but also law enforcement, especially its compliance department and financial task force (Lastra & Allen, 2018)

VC asset offers a novel solution for both individuals and organisations engaging in criminal activities. According to expert's estimation, the total market capitalisation of VC once exceeded USD 600 billion during the bull run in the fourth quarter of 2017 and now being valued at USD 200 billion (CoinMarketCap, 2020). This growth has led to VCs and Initital Coin Offering ("ICOs") being an essential form of personal asset and VC-related businesses. These businesses consist of both direct business such as VC exchange or wallet custodian service provider and those supplementary business, including but not limited to, gaming, computing, and banking. Typically, VC is easily exploited by criminals amassing significant wealth from committing crimes such as human trafficking, Ponzi scheme, extortion, drug ring, and corruption. Illegal goods and services are now transferred quickly and largely anonymously on the so-called "dark-web" in exchange for VC. Chainanalysis, an industry leader in blockchain forensics, accounted that criminals

laundered $2.8 billion in Bitcoin to exchanges, up from $1 billion compared to 2018 (Robert, 2020). As VC offer greater obscurity than the traditional fiat currencies (such as EUR, USD, JPY), it is more challenging for the authority to connect the dots in investigating the crime proceeds. The hardest part is to link the laundered VC and its owner. AML risk presents severe threat to the integrity of the economy because it has effects on forming interest groups in specific sectors or industries, which in turns might corrupt large groups of people in the society.

As these engagements have continuously gained momentum, regulators and financial institutions are becoming more aware of the fact that decentralisation provides an ever-more powerful new tool for criminals and other sanctions-evaders to transfer or store illegal funds, and, as a result, create unique challenges in terms of money laundering risks to law enforcement.

As an attempt to address the problem, the author decided to write the Bachelor's thesis on the topic of " Applying the Anti-Money Laundering regulations of virtual currency to build an effective internal control process: Case study Finland". The research paper has three main objectives:

1. To display the current state of global AML regulation of virtual currency and its practical application in Finland;
2. To explore the money laundering activities in the virtual currency field;
3. To feature a case study and develop a comprehensive reference model in response to the AML risks.

1.2 Thesis' scope and structure

As a literature-based thesis, the scope is to apply the theoretical knowledge to develop an AML internal process for a case company in the Finnish context. This model shall identify the critical European legal requirements as transposed into practice in Finland.

This thesis consists of five main parts: introduction, literature review, analytical framework and methodology, and discussion on the findings.

The author organises this paper as follow: Chapter 1 outlines the thesis background, its significance, and objectives, which is helpful for readers to have a preliminary understanding of the thesis topic. Chapter 2 details the literature review, which consists

of three sub-sections providing the theoretical knowledge of the research topic. Section 2.1 would introduce the core definitions of VC and explain the growing importance of VC in today's world. Section 2.2 displays the sophisticated money laundering process conducted by the criminals, which leads to the analysis of the legal and regulatory challenges globally. This section also presents the existing AML legal & regulatory approach regarding virtual currency in both European and Finnish context. Section 2.3 detailed the potential AML risks from the regulatory standpoint, which are essential to construct an efficient AML internal process for the case company. Chapter 3 discusses the research methodology, data collection methods and data analysis of the study, which give insights to the case study and allow readers to develop their critical assessment of the study's reliability and validity. Chapter 4 encompasses the case study analysis, which consists of three sub-sections. The first sub-section is the current state analysis, which the author evaluates the current AML practice of the case company. Then, the author presents the AML reference model after identifying the critical AML challenges related to the existing practice. Afterwards, the author discusses the validation results of the AML reference model. The final Chapter 5 presents the summary and the assessment of the reliability and validity of the thesis.

2 Literature review

2.1 The strategic role of virtual currency in the global context

The virtual currency has undoubtedly gained popularity among the global financial market as a technological-advanced alternative for the traditional fiat currency. In less than a decade, virtual currency has gone from being a case of curiosity to the global phenomenon (Dabrowski & Janikowski, 2018). In order to comprehend the importance of AML risk controls in the virtual currency field, it is critical to understand fully what virtual currency is and how it is relevant to today's world.

2.1.1 Virtual Currency: Understanding the essence

The definition of the virtual currency tends to vary depending on the context. Virtual currency is defined as a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value but does not have legal tender status (FATF, 2014). Meanwhile, the European Central Bank explained virtual currency to be a type of unregulated, digital money, which

is issued and usually controlled by its developers and used and accepted among the members of a specific virtual community (ECB, 2012). According to Dibrova (2016), the definition provided by the ECB was too broad, which was revised again in 2015. In the new definition, the word “money” was removed because of the transaction volume of virtual currencies was too insignificant compared to other well-established payment solutions such as Visa or Mastercard. At the same time, the low acceptance rate of virtual currencies among online shops also contributed to the change in definition (ECB, 2015). Up until now, there is still no international agreement on how “virtual currency” should be defined, but people might find some overlapping terms such as “crypto-asset”, “crypto-token”, and “cryptocurrency” (ECB, 2019). The taxonomy of virtual currencies is detailed in the following figure:

Figure 1. Taxonomy of Virtual Currencies

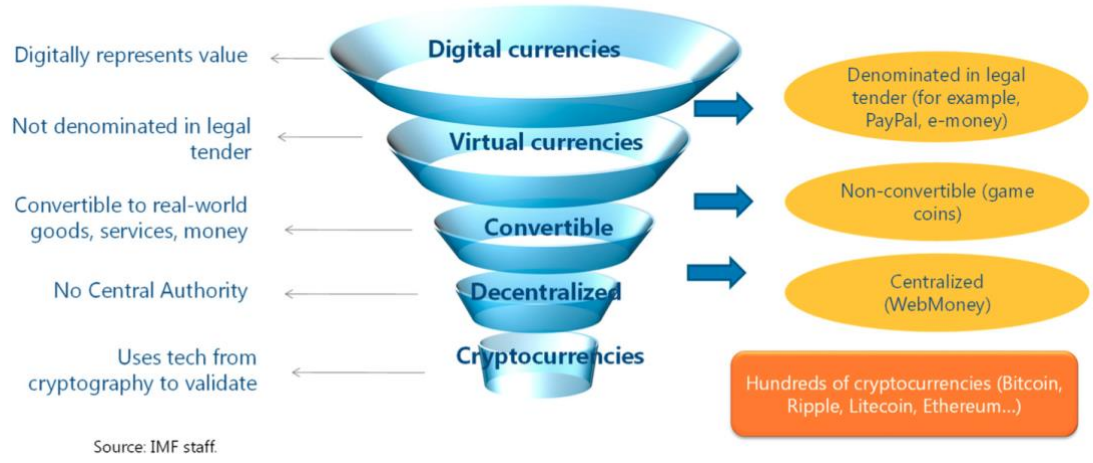


Figure 1. Taxonomy of Virtual Currencies, IMF (2016)

Dibrova (2016) argued that the development of definitions of virtual currencies in the European Union, including the continuation of finalised legislative base formation, had not been finalised. As a result, some people might find confusion in distinguishing VC from digital currency. Based on the IMF’s staff note, virtual currencies fall within a broader category of digital currencies (IMF, 2016). However, what sets them apart is that virtual currencies are not denominated in fiat currency and have their unit of account. For example, although electronic money (e-money) belongs to the digital currencies category, it is not classified as virtual currencies because it does not possess the legal status of currency or money. This confusion in definitions was further emphasised in the Fifth Anti-Money Laundering Directive (AMLD5) enacted by the European Parliament and of the Council in 2018 (European Union, 2018).

Virtual currencies consist of both centralised and decentralised currencies. The main difference between these two types is that decentralised VC does not need an administrator or trusted third-party ledger, but it can be exchanged for fiat currency. Meanwhile, both convertible and non-convertible centralised virtual currencies such as Web money or game coins require supervisory authority from an administrator. Although there is a discrepancy in how different organisations define what VC is, it is commonly agreed that VC is not classified as a financial instrument. Therefore, it does not represent financial liability or equity on any identifiable entity.

Distributed Ledger Technology (DLT)

In the wake of the continuous trend of banking disintermediation, the emergence of VC recently is further accelerated by a computing decentralisation mechanism called distributed ledger technology (DLT) (World Bank, 2017). Being the essence of virtual currencies, DLT is a novel and fast-evolving protocol which allows users to modify the records in a commonly-shared database (i.e. ledger) in a synchronised way, without needing to engage in a centralised system imposing either standards or processes (ECB, 2016). DLT has been linked to virtual currencies since its early days because DLT was invented as the technological foundation to the cryptocurrency Bitcoin. In 2008, Satoshi Nakamoto, an unidentified person using a pseudonym, published a landmark paper called “Bitcoin: A Peer-to-Peer Electronic Cash System”, which suggested a method of moving the funds in the form of Bitcoin based on the peer-to-peer (P2P) mechanism (Nakamoto, 2008). Although the terminology that Satoshi used in his paper is called “blockchain”, the idea of re-organising the records of assets in a P2P manner subsequently led to the new broader term “distributed ledger technology” (World Bank, 2017).

In the traditional banking system, the central bank facilitates the payment transactions by transferring the money from one account to another with a master ledger system. Therefore, the central banks hold the responsibility to validate the transaction on their central ledgers to ensure the accuracy of the data and safeguard them from being tampered by criminals. This standard transactional model is described on the right side of Figure 2.

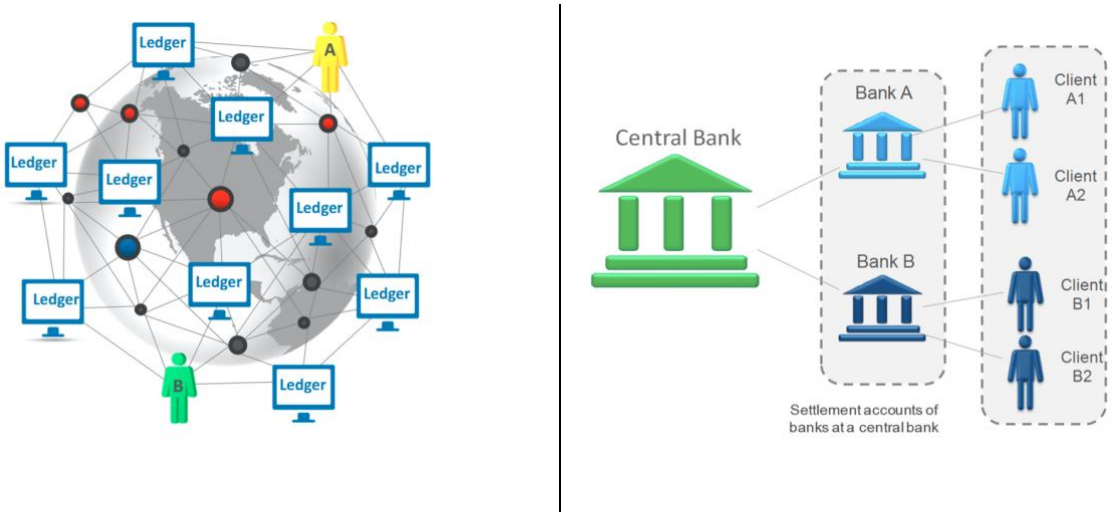


Figure 2. The mechanism of a blockchain-based DLT vs the centralised banking system. IMF (2016)

Meanwhile, the mechanism on the left side of Figure 2 depicts how the DLT-based infrastructure store, record, and exchange information digitally across different counterparties without the control of any centralise record-keeper. At the same time, the pre-defined algorithmic validation method of this mechanism guarantees there is no "double-spend". In plain words, it merely means that if a member A sent €1000 value of Bitcoin to member B, A cannot send that €1000 again to member C because other members would not verify the node containing that information. This distinctive feature of DLT led many industry experts to believe that DLT would revolutionise certain areas within the financial sector, especially in regulatory compliance. A case study by Accenture concluded that major investment banks could reduce the existing compliance cost by 30% to 50% if they can adequately combine DLT into the banking system (Accenture, 2017). As a result, in Dariusz Szostek's view (2019:142), the critical innovation of DLT may help to provide security and promote trust in a common ledger being maintained by a network of anonymous participants without the need of a centralised mediator or intermediary (Szostek, 2019).

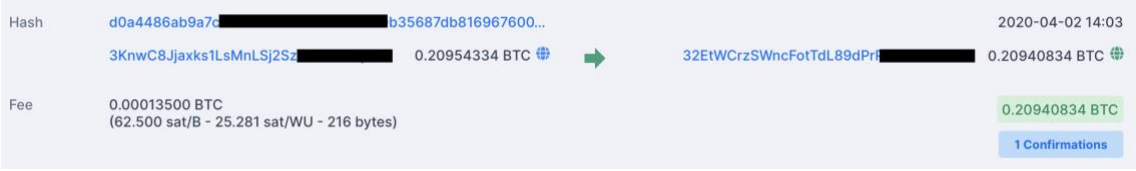


Figure 3. Bitcoin transaction. Blockchain.com (2020)

The blockchain-based DLT is described as pseudo-anonymous (Luu & Imwinkelried, 2015). Brito & Castillo (2013) classified the blockchain as a parties-unknown/transaction-known model, a hybrid of the cash payment and intermediary's system. The transaction of Bitcoin in Figure 3 illustrates the anonymity of the blockchain. It may be noted that two parties participating in the transaction are coded by a blockchain addresses, which can be created without providing personal information. On the other hand, people can easily find the information about the transactions on the ledger from public record such as blockchain.com, depending on the VC types. Therefore, the blockchain is not considered entirely private. Nevertheless, some users complicate this pseudonymity by employing a variety of techniques to conceal the connection between the blockchain address and the actual transacting person, making it highly challenging for the authority to attribute the address to specific people. How the characteristics of blockchain make VC appealing to the money launderers and increasing the complexity the forensics to the authority shall be discussed in part 2.3.1.

2.1.2 Increasing relevance of virtual currency & AML risk

In recent years, the rapid development and growing adoption of VC-related business activities have gained the public eye. From the regulatory perspective, the increasing relevance of virtual currencies and its AML risk might (i) reshape the financial market structurally, (ii) compel the authority to adopt more sophisticated measures to deal with elevated AML risks.

The mass adoption of virtual currency among institutions and countries might reduce the reliance on fiat currency and revolutionise the way people or institutions transfer funds. When discussing the impact of VC in the global context, Susan Athey, a Stanford University professor, emphasised on how virtual currencies could become a "convenient and safe form of payment in countries where most citizens do not have bank accounts", "particularly in high-inflation countries" (Athey, 2015). Indeed, in some countries, people have started using VCs such as Bitcoin as a second currency because it is much better than the existing options. Joe Waltman, GiveCrypto's executive director, notes that virtual currency "has the highest likelihood of being helpful to people in places where the money is broken … and there is probably a no better example of broken money right now than Venezuela." Under President Nicolas Maduro's regime, the country's bolivar recorded hyperinflation reaching above a million percentage (Grinspan, 2019). While the Venezuelan civilians turned to cryptocurrency as their vital source of income, their

government has used Bitcoin to get around the economic sanctions imposed by the U.S. As a result, Venezuela finds itself ranked fourth in the world in terms of Bitcoin trade, with an estimation of $3.7 billion in Bitcoin remittances in 2019 (Aguilar, 2019). MIT Technology Review (2019) argued that Bitcoin provided the Venezuelan state with a way to deviate money around the world when the country was isolated from the global financial system.

Some critics indicate that the astonishing growth of Internet users has driven acceptance of VC (Klumov, 2020). In recent years, the global economy is undoubtedly moving towards digital solutions and eco-system. According to Internet World Stats, the number of worldwide internet users in 2000 was 361 million, whereas, by 2019, this figure reached 4.5 billion. Research from (Deutsche Bank, n.d) indicated that the growth of cryptocurrency and the internet is directly proportional to each other with a positive gradient. It can be observed from Figure 4 that the growth pattern of these two variables bears a strong resemblance to each other.

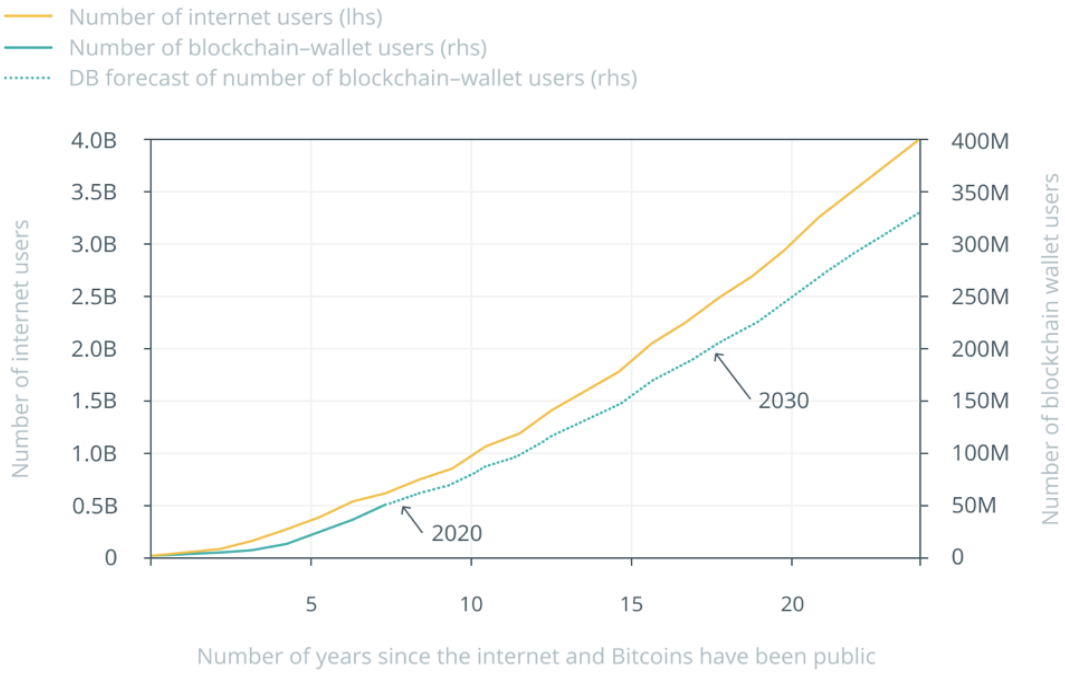


Figure 4. Adoption rates of cryptocurrencies & Internet. Deutsche Bank (n.d.)

Another factor worth considering how VCs might reshape the financial market structurally is the increasing participation of the financial sector into the VC space. Kauflin, (2019) noted the substantial investment from individuals and corporations seeking to build advanced decentralised peer-to-peer networks since the cryptocurrency bull run in 2017.

A notable case is a partnership between Ripple (XRP) and the Bill & Melinda Gates Foundation in October 2017 to create a new interoperable system called Mojaloop that would “help unbanked people around the world access digital financial services.” (Wintermeyer, 2018). Technology moguls and traditional banks are also in the race of getting involved into VC as well. When Facebook announced its plan to launch a new token “Libra”, it is clear that this might shake up the global financial system (Paul, 2019). JP Morgan Chase, despite having plan to launch their token “JPM Coin”, declined Facebook’s invitation to develop Libra over concerns that Libra might be used to violate money laundering and sanctions law (Andriotis, et al., 2019). As the Federal Reserve Chairman Jay Powell noted "The size of Facebook's network means it could be, essentially, immediately systemically important.", it clearly shows that Libra has raised awareness of the long-term VC adoption and emphasised the need for more sophisticated AML implementation as well as new technologies to enhance compliance procedure (Kiernan, 2019).

2.2 A glance at money laundering of virtual currency

2.2.1 Money laundering – key definitions and background

Before the case of the U.S. versus $4,255,625.39 in 1982, the term “money laundering” had never appeared in a Judicial or legal context (Ferguson, n.d.). Sharman (2008) describes money laundering as a practice of concealing the illegal origins of the money obtained from criminal activities. In the legal context, this expression is defined in several ways. Majority of the nations adhere to the money laundering concepts adopted by the United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (UNODC, n.d). It implied money laundering as the conversion or transfer of the asset, which is derived from any drug trafficking offences, to hide the illegal origin of such asset. While the said definition set by the Vienna Convention was limited to only drug trafficking offences, FATF and other international organisations have expanded the definition to include 20 additional designated categories of offences. For example, the list of money laundering criminal offences also contains murder, environmental crime, robbery, migrant trafficking, and participation in an organised crime group. (FATF, n.d)

In the Finnish context, money laundering was defined in the Finnish Criminal Code, chapter 32, section 6 (Ministry of Justice, Finland, 2015). According to the section, a person is guilty of money laundering if he/she:

> "(1) receives, uses, converts, conveys, transfers or transmits or possesses property acquired through an offence, the proceeds of crime or property replacing such property in order to obtain benefit for himself or herself or for another or to conceal or obliterate the illegal origin of such proceeds or property or in order to assist the offender in evading the legal consequences of the offence; or
>
> (2) conceals or obliterates the true nature, origin, location or disposition of, or rights to, property acquired through an offence, the proceeds of an offence or property replacing such property or assists another in such concealment or obliteration." (Ministry of Justice Finland, 2015).

Regardless of the varying definitions, the essence of this term indicates the process of turning the illegally-obtained property into the lawful property with the following purposes: (i) to obscure the origin of criminal property, and (ii) to erase and eliminate the trail leading to the crime. Despite the fact that the surface of money laundering might be simple to define on paperwork, Buchanan (2004) notes that it is incredibly challenging to investigate and prosecute the criminal activities.

From the expert's point of view, the money laundering phenomenon can have a substantial impact on the worldwide economy on multiple aspects (McDowell, 2001). First, it encourages criminal financing and corruption, which eventually increases the crime rate and disrupt social stability. Second, it might turn a country into a money-laundering haven. Having this reputation is considered a significant disadvantage to any countries because the economy of such countries is less attractive to foreign investors. In specific, those countries often face more scrutiny in terms of financial transactions and more limited access to the global financial market, which endorses transparency. Typically, havens for money laundering tend to have weak AML regime, little enforcement of AML provisions, and insignificant penalties. For developing countries, reduced access to world markets, especially to the capital market, might intensify the poverty situation. Third, money laundering can damage the solidity of the financial institutions because it exposes those organisations to reputational, operational, and legal risks. Basel Committee on Banking Supervision (2001) discusses that the trade-offs of engaging in money laundering include termination of banking infrastructures, liquidity issues, declines in stock value, declines in the stock value, and asset confiscation. For instance, regarding the reputational risk, an organisation might lose confidence in its soundness and integrity from its major stakeholder. Needless to say, money laundering is critical concern towards financial institutions where there are multiple complex

counterparty relationships and connections. Finally, money laundering can disrupt and compromise the private sector. When criminals use “front stores” to legitimise their illegal business, they can form interest groups and monopolise different parts of the private sector, leading to the monetary and economic instability (McDowell, 2001).

AML legal & regulatory approach regarding virtual currency

The fight against money laundering is undoubtedly a vital priority of international organisations. It is widely perceived that money laundering practices often occur transnationally ; therefore, domestic measures are often insufficient to address this issue (Borliini, 2012). The FATF’s standards (also known as the FATF Recommendations) were drafted in February 1990, amended in 1996, in 2003, in 2012 and most recently in 2019 are the cornerstone of the existing AML paradigm (Nance, 2018). Endorsed by over 180 countries through different regional affiliated bodies, the FATF’s Standards require all nations to formulate effective measures to address and prevent the money laundering issue. Regarding the AML measures, FATF outlined the policies and coordination between nationally and internationally, confiscation, preventive measures, transparency and beneficial ownership, and powers and responsibilities of relevant authorities. In legal terms, FATF Recommendations are not considered legally binding, but the Member States and affiliated bodies committed to incorporate them into their local and regional legislation (Salas, 2005). FATF also partners with the World Bank and IMF to draft the methodology for assessing the AML compliance system as well. Therefore, despite the limited partnership of the FATF, they remain one of the standard setters regarding money laundering penal and regulatory framework.

In the European Union (EU), the Anti-Money Laundering Directive developed by the EU, which is in line with FATF Recommendations, acts as a legislative act regarding the AML matter. However, it must be noted that the directive is considered a common goal for all Member States to obtain. It means that member states have to devise its own legal and regulatory framework to achieve the directive’s goal. The European Commission (EC) developed its first Anti-Money Laundering Directive in 1991 (“AMLD1”) to coordinate the regulations and measures across all Member States and ensure the financial stability of the region. The second amendment came into effect afterwards, leading to the second Anti-Money Laundering Directive (*AMLD2”) in 2001, which extended the recommendations to include the fight against terrorist financing (Salas, 2005). This decision was triggered by the 9/11 terrorist attack and by the disagreement in the

definition of serious crimes laid out in the first directive. In February 2012, when FATF published their revised recommendations, the EC subsequently modified their term coverage to include lawyers, accountants, real estate agencies, and casinos to be aligned with the FATF Recommendations. A decade later, fourth Anti-Money Laundering Directive ("AMLD4") came into effect and resolved the ambiguities in the previous directive. Although it provided a more rigorous risk-based approach to make the fight against money laundering effective, it did not explicitly recognise the VC in its terms. As a result, the fifth Anti-Money Laundering Directive ("AMLD5" or "Directive (EU) 2018/843") introduced in June 2018, outlined new requirements regarding virtual currencies. This directive must be transposed into law by the Member States by January 10, 2020. The key amendments regarding VC are displayed as follow:

1. AML scope extension to VC	The EC now identifies any VC-related businesses as "obliged entities". As a result, the scope is extended to include two new types of VC-related service providers: virtual currency exchange providers (VCEPs) and custodian wallet providers (CWPs). VCEPs are VC exchanges which convert traditional fiat currency (e.g. USD, EUR, JPY) from their clients and exchange them into VC (Bitcoin, Litecoin). Meanwhile, CWPs are custodian wallet service providers which safeguard the clients' virtual asset funds. These service providers must be registered with the local authorised financial supervisory (e.g. Germany's Federal Financial Supervisory Authority BaFin, Finland's Financial Supervisory Authority FIN-FSA).
2. Transparency on the Ultimate Beneficial Owners (UBO) and Politically-Exposed Persons (PEPs)	Under the AMLD5, the registration of Ultimate Beneficial Owner of European businesses would be made publicly available. The public access also includes the affiliated interconnection of the national registration record. The information of the UBOs comprises of name, birth date, nationality, country of residence, and beneficial interest. At

	the same time, during the AML screening process, consulting the beneficial ownership register is compulsory. The national PEPs would be put under the same examination level as the foreign PEPs and the high-level officials of international organisations. Simultaneously, Member States must establish public offices or functions to help companies identìying the PEPs.
3. Rigorous due diligence measures to implement transparency	VC service providers are now subject to the same AML and KYC requirements of any traditional financial institutions. For the KYC purposes, all obliged entities must use the electronic identification technology that complies with the eiDAS regulation for the customer's identity verification purpose. Entities now have to determine the Client Due Diligence (CDD) level depending on different circumstances. In a generic situation, CDD is sufficient. However, in those particular situations outlined in the directive where additional measures are specifically required, entities must conduct Enhanced Due Diligence (EDD). For example, European organisations having business relationships or transacting with high-risk third countries must conduct EDD. This process requires entities to acquire information regarding the source of wealth, ownership structure, and reasons for doing transactions.
4. More intense transactions monitoring and suspicious activity reporting	Any financial flows to and from high-risk countries relating to money laundering subject to stricter due diligence practice. Notably, any transactions of complex nature or conducted in an unusual flow shall be must be monitored regularly and reported to the governmental entities where applicable.

Table 1. AMLD5 amendments

How does Finland comply with the AMLD5?

The Act on Virtual Currency Providers (572/2019) entered into force on May 1st, 2019. The FIN-FSA has also published its Regulations and Guidelines, which entails the primary obligations for virtual asset service providers (VASPs). VASPs must be officially registered with the FIN-FSA. The obliged entities of this Act comprise of VC exchange services, custodian wallet providers, and issuers of virtual currencies. The scope of FIN-FSA's definition concerning exchange services include the VAs to VAs exchanges as well.

For those VASPs who had already provided services before the effective date must be registered by November 1st, 2019 (FIN-FSA, 2019). By the end of 2019, there are five regulated VASPs in Finland. The main requirements that entities must comply for this registration include:

- Basic and fit proper check: To ensure the validity of the entity;
- Customers' fund management: To examine the technical compliance level (e.g. client's fund segregation, security practice);
- Marketing of services: To guarantee the appropriateness of the marketing materials displayed to the public;
- AML regulation compliance: To review the AML policy and risk assessment of the entity as required by the regulation

It must be noted that this new regulation does not change the characteristics of VCs or the risks associated with VC-related investments. However, regulated entities are responsible for assessing whether the VC is deemed as a financial instrument, as cited in the Investment Services Act (747/2012/chapter 1, section 14) (FIN-FSA, 2020). FATF (2019) describes the attitude of the VASPs toward the FIN-FSA regulation as a "total turn". In the past, VASPs did not want to be regulated, but nowadays, they are keen on being regulated. One reason contributing to this significant change might come from the limited access to the banking system as VASPs have faced difficulties in opening a bank account.

A gap in global AML enforcement regarding VC

From a macro perspective, the global AML enforcement regarding VC transactions varies widely, from the strict regulations in the U.S. to nearly non-existent practices in countries such as Russia and Mexico. Even within the EU, the regulations between the Member States vary widely as well. In some instances, the legal status of those is considered enigmatic depending on the development of the legislation. For example, from 2013 to 2018, the Netherlands did not formally extend their AML regulation to address the VC activities. The salient gaps in these regulations present opportunities for money launderers to exploit.

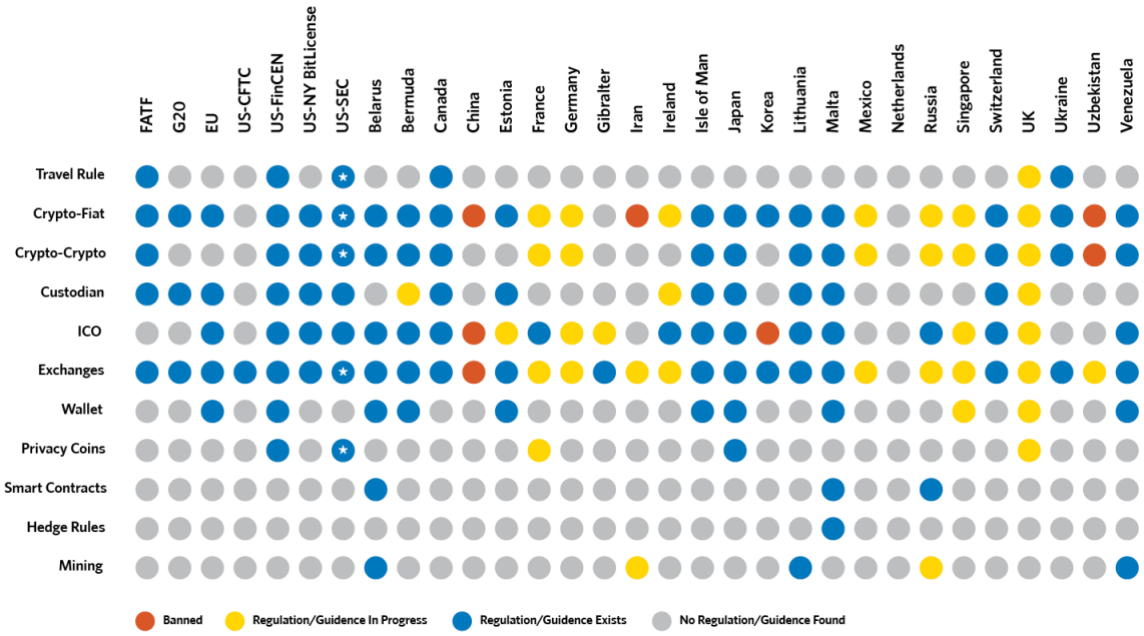


Figure 5. The current implementation of VC AML/CFT regulations globally. Cipher Trace (2019)

Regulations have been tighter for VC business for the past two years. As discussed above, international organisations have stepped up implementing stricter rules and regulations concerning VC. VASPs are acting fast to meet up with tight restrictions from the authority to avoid being shut out of lucrative markets. However, the challenges towards comprehensive AML/CTF control remain significant. These difficulties include the complication in linking transactions to its ultimate beneficial owners, the discrepancy between the regulations and the companies' AML capacity, and the lack of technological understanding from the regulatory.

2.2.2 The money laundering processes and methods

Initially, concerns over money laundering back in the 80s under Reaganomics mainly focused on the “war on drugs” (Verhage, 2008:11). Nowadays, the illegal gains are generated from a wide range of lucrative criminal engagements. The size and amount depend on the nature of the adopted illicit means. For example, in terms of operations, a Mexican drug cartel is estimated to generate hundreds of millions to billions of dollars in annual revenue. Needless to say, this asset cannot be lawfully deposited into established financial institutions because it would trigger the suspicious transaction monitoring and blacklisting process, leading to a criminal investigation operated by the police and authority. As a result, most scholars argue that money launders would try to launder the illicit money following three primary phases: placement, layering and integration (UNODC, 2009; Buchanan, 2004). This section shall describe the money laundering process both in theory and in the VC sector.

Figure 6. A typical money laundering scheme. Delna (2018)

Phase 1: Placement

In the initial phase of this scheme, criminals deposit the bulk cash obtained from illicit activities into the mainstream financial system. Typically, the majority of illegal activities generate cash profits, which might be inconvenient and troublesome to conceal in large amounts. Therefore, the money launderer has to find an alternative solution to transfer large masses of cash into a legitimate set up to display to the financial institutions. The most common method is to establish front companies and businesses and record the money as legal instruments such as sale orders and cashiers' checks. Thus, this step is considered the most vulnerable phase for law enforcement to detect the proceeds' origins (Bachus, 2004). However, it has to be noted that placement is only relevant when the money is transferred into the financial system. In certain circumstances, the funds can be used for contraband activities or pay the salary to the illegal immigrants working in the front business. In this case, the criminal would not start with placement.

In the VC sector, virtual currencies can be easily purchased with cash through buy/sell platforms or exchanges. Different exchanges or VASPs have different levels of compliance regarding identity verification and source of funds declaration. This occurrence is because of the wide gap in VC regulations worldwide. On exchanges that are negligent to the regulations or are not required to be AML compliant, money launderers can anonymously open an account and convert the illegitimate money into VCs such as Bitcoin or Ethereum.

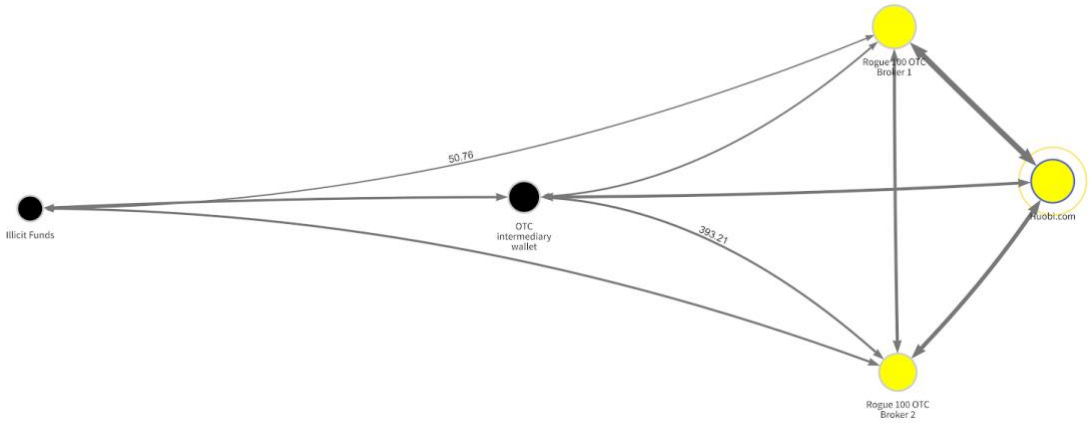


Figure 7. Placement via VC OTC desk. Chainanalysis (2019)

Another path that money launderers use is through over-the-counter (OTC) broker. Figure 7 depicts the flow that money launderers used to transfer illicit funds to the Huobi exchange. In the traditional financial market, OTC desk often mediates the transactions of securities that are not listed on formal exchanges, such as the New York Stock

Exchange (NYSE) (Murphy, 2020). OTC brokers tend to deal with the buyers and sellers directly and subject to less regulation. It is reported that OTC desk has emerged as a "lynchpin of a new type of money laundering" that criminals resort to (Roberts, 2020). While exchanges might take days or weeks to process the funds, OTC desks can settle the transactions within 24 hours. As a result, when the OTC desk does not conduct rigorous Know-Your-Customer (KYC) protocols, money launderers can exploit this channel to consolidate illicit cash (Chainanalysis, 2020).

Phase 2: Layering

When the illicit fund is successfully placed into the financial system, the second phase called "layering" takes place. The ultimate goal of this stage is to obscure the money trail and camouflage the original crime (Bachus, 2001; Buchanan, 2004). This process refers to the creation of a highly complex and sophisticated web of financial transactions that imitates the nature of the legitimate financial activity. From Figure 7, it can be noted that offshore financial centres are an essential linchpin in this stage. To evade scrutiny by law enforcement and regulators, criminals often wire the funds into the financial system via any offshore banks. Cox (2014:17) claims that:

> "The money launderer will move the funds between a number of accounts in a number of different jurisdictions and through a series of companies to ensure that the trail is as complicated as possible. This will essentially obscure the audit trail and sever the link with the original criminal proceeds. The funds can actually 'spin up' to ten times prior to being integrated into the banking system." Cox (2014:17)

VC could serve as a vehicle to transit the funds transnationally because criminals can utilise an anonymising service to obscure the fund's source. In April 2018, the Europol exposed a money-laundering operation that was facilitated via a Finnish exchange (Europol, 2018). The Spain-based criminals initially split the illicit cash into hundreds of third bank accounts. Afterwards, they created a highly complex layering network to transfer the money obtained from drug trafficking to Colombia and Panama. Other tactics to exploit VCs is to participate in an Initial Coin Offering (ICO), where money launderers can exchange one type of VCs for another. The Monetary Authority of Singapore (MAS) noted that ICOs are "vulnerable to money laundering and terrorist financing risks due to the anonymous nature of the transactions, and the ease with which large sums of monies may be raised in a short period of time." (Leong, 2017)

Phase 3: Integration

The final phase of the money laundering scheme is known as integration whereby the cleansed funds reintegrated into the economy under a legitimate shell. It is highly demanding for law enforcement to distinguish the illegal proceeds and legal ones from the integrated affluence. Money launderers usually transformed the money into different forms, such as the purchase of assets, such as real estate, financial assets and securities, and luxury assets (Bachus, 2001; Buchanan, 2004).

In VC, criminals can legitimise the illicit fund by directly or indirectly convert the VCs into fiat currency. Nowadays, there is an ever-growing list of goods and services that accepts VAs as payment method. Additionally, similar to how an offshore bank operates in Figure 7, online companies can transform dirty VAs into luxurious items as well. For instance, Vaultoro is a popular Berlin-based trading platform allowing people to trade between cryptocurrency and physical gold (Bloomberg, 2019). Alternatively, ICOs with below-average compliance control might be abused by money launderers seeking to convert their illegal-gained VAs into other types of VAs. Afterwards, the criminals can exit the whole money laundering process by selling them when the new VC become listed on the exchange.

2.3 Key AML risks from regulatory standpoint

As mentioned in the first section, VC is a novel resolution for both individuals and entities engaging in criminal activities. The potential risks do not only emerge from the nature of the blockchain itself but also the environment circulating the service providers as well. As the underlying technology behind VC becomes more evolving and advanced, the law enforcement and authority finds it more challenging to tackle the money laundering issue. In general, the potential risks linked to VC arise from the following factors: (i) anonymity and pseudonymity, (ii) P2P cross-border transaction, and (iii) decentralisation. (Keating, et al., 2018)

2.3.1 Anonymity and pseudonymity

Keating et al. (2018) emphasised that describing decentralised virtual currencies such as Bitcoin as “anonymous” or “untraceable” was insufficient. Instead, it is better to describe them as “**pseudonymous”.** In the VC industry, the ultimate beneficial ownership can only be confirmed on customer accounts because the VC transactions

stored on the blockchain are from one numbered account to another (Houben & Snyers, 2018) (Houben & Snyers, 2018). However, it has to be noted that if the law enforcement put enough efforts to deploy the proper data-driven techniques, such as quantum computing, it is still possible for the authority to detect the users' identities (Houben and Snyers 2018 cited in Dupont 2012:44). Although the information concerning the user's identity cannot be found on the blockchain, other vital information such as transaction date, transaction value, counterparties' deposit addresses, are displayed publicly on different blockchain explorer websites. Several private blockchain forensic companies have developed tools to de-anonymising VC transactions and scrutinise the illegal activities related to those (Wan, 2020). These companies have worked closely with law enforcement and VCEPs to analyse the users' transaction pattern. Therefore, theoretically speaking, law enforcement can trace the identity of criminals. Still, investigating the personal identities following this approach can be costly and time-consuming. In some cases, it might not lead to any fruitful results.

As discussed in the first section, some individuals employ different techniques to add another layer of anonymity to obscure the connection between the blockchain address and the actual transacting person. Some key techniques that money launderers can utilise are:

- *Anonymising tool*

This term refers to tools and services which camouflage the VC transactions, such as Tor (darknet). The default P2P protocol of some virtual currencies does not hide the Internet Protocol (IP) of people participating in the transaction. Therefore, law enforcement can easily follow the IP address to track down the identities of associated individuals. Money launderers use this tool because it is an open-source communication network which disguises the IP address (Genkin, et al., 2018:78-82).

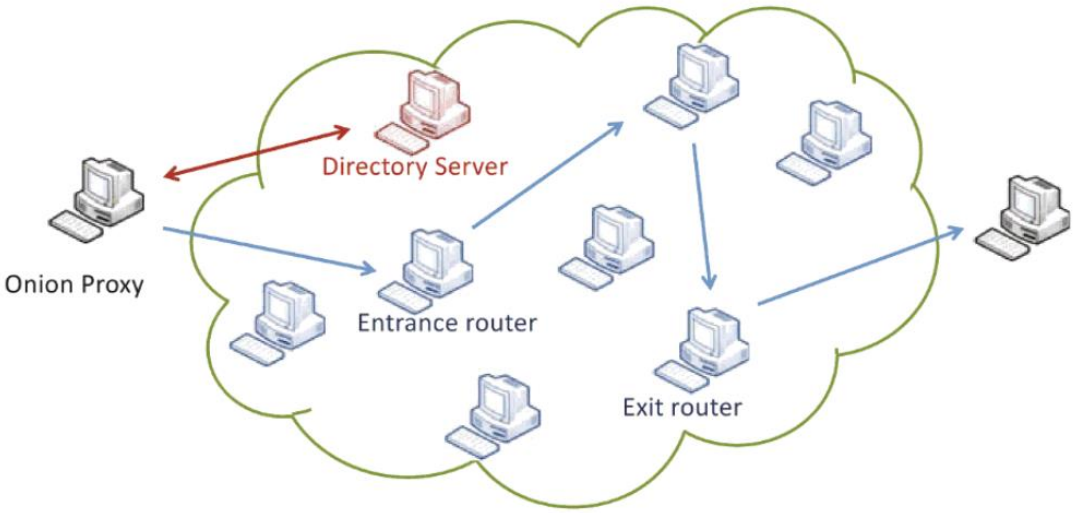


Figure 8. Tor-Onion router communication. Traffic Monitoring and Analysis: Third International Workshop (2011)

As described in Figure 8, this tool routes the communications/transactions through different worldwide computers and forwards through an established circuit wrapped in highly-complex encryption algorithm (Domingo-Pascual, et al., 2011:113). Therefore, this tool confuses law enforcement seeking to locate the computer hosting of the users who initiated the transaction. Some criminals even couple Tor with a Virtual Private Network (VPN) then combine some mixer tools to disguise and entangle the whole money laundering process.

- *Mixer (tumbler) service*

This service combines all involved VC transactions into a mutual address then produces output through a semi-random mechanism, making it difficult to link any VC address to any specific transaction (Genkin et al., 2018:78-82).The tumbler service provider often takes a cut on the transaction fee, usually between 1% and 3% of the total transaction value (Allison, 2015). There are various mixing methods, such as centralised solutions, peer-to-peer mixing, and decentralised mixing. The mixing mechanism depends on different types of service providers. Figure 9 illustrates the most common form of VC tumbling. In early 2020, an Ohio-based man was arrested by the Federal Bureau Investigation FBI's Washington Office for operating a VC tumbler service which laundered over $300 Million (The U.S. Department of Justice, 2020). This case clearly shows that law enforcements are continuously keeping a tab on this illegal practice of money laundering.

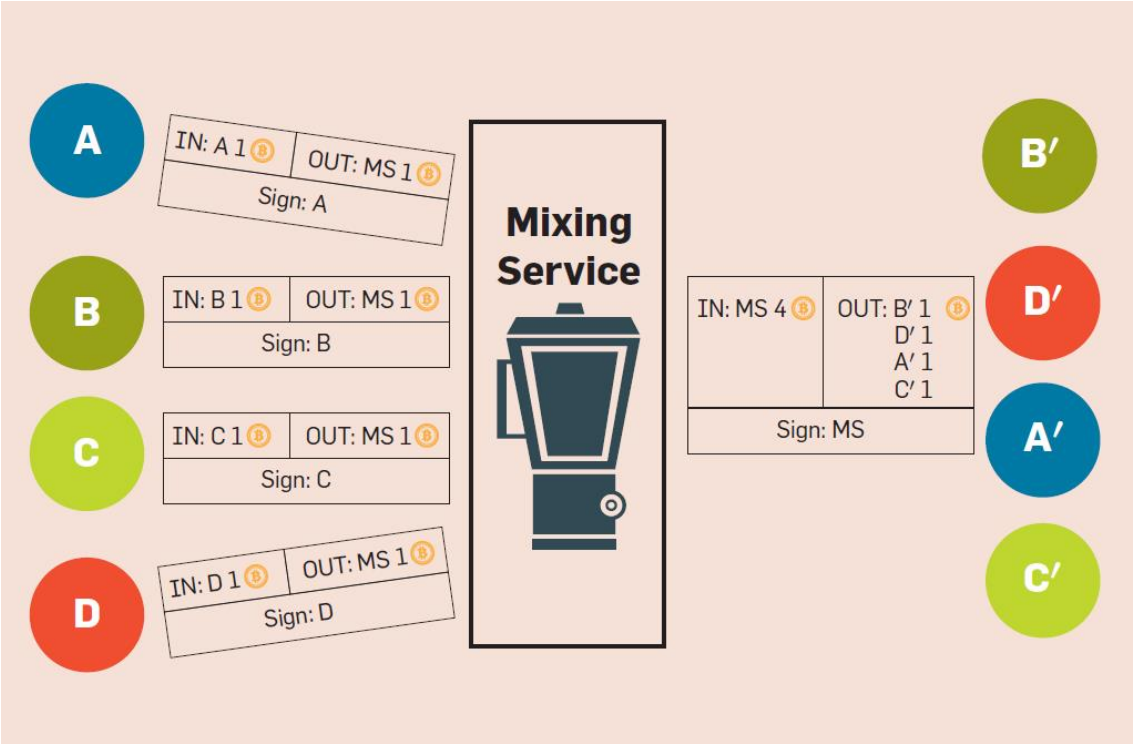


Figure 9. Example of the centralised mixing service. Source: Association for Computing Machinery 2018

There are a handful of virtual currencies developed to be completely anonymous, such as Monero and Zcash. These are known as “privacy coins” because the information on transactions is not made public. Their masking of transaction data makes it hard for law enforcement to trace the original sender because the blockchain does not reflect any personal information (Kumar, et al., 2017). Needless to say, these coins might hold some appeal for money laundering actors due to its private nature.

2.3.2 Cross-border transaction

Another characteristic of virtual currency that elevates the AML risk is the cross-border transaction. Without any regulated intermediaries, the money launderers can transfer the virtual asset internationally (Keatinge, 2018:36). This feature has attracted criminals such as ransomware hackers, drug traffickers, and extortionist. These groups usually receive payments in virtual currency from different worldwide locations. The situation becomes more complicated because those criminals could take advantage of the gap in the AML regulations among different nations or the political conflicts between countries to thread their way through the detection of law enforcement. In early 2019, CiPherTrace reported a 46% increase in the number of cross-border transactions from American

virtual currency exchanges to offshore exchanges (Huillet, 2019). Indeed, this increase is alarming to the authorities as the domestic regulation might shield these transactions.

The existence of worldwide Bitcoin ATMs further accelerates the money laundering activities. There are nearly 7000 Bitcoin ATMs placed in different locations worldwide, with the highest concentration in the U.S. and Europe (Pirus, 2020). The Colombian drug cartel was detected to use Bitcoin ATM to launder their illicit funds across Europe in 2019. The whole operation was estimated to have cleaned around €9 million before it was busted by Spain's Guardia Civil (Aguilar, 2019). This case proves that the use of virtual currency to facilitate cross-border transactions makes it more difficult for law enforcement to trace to the illicit origin.

2.3.3 Decentralisation

This factor does not concern the centralised virtual currency such as a game coin or Webmoney. However, it must be noted that the majority of virtual currency are decentralised. This feature makes virtual currency risky from the regulatory perspective because there is no central authority that can prohibit any individuals from getting access to the virtual currency network or penalise or suspend it. Keatings (2018) describes this characteristic as "censorship-resistant" because it enables people who seek unrestricted access to virtual asset fundraising and allocation. On Figure 10, it can be seen that while the transactions of centralised currency circulate around one central authority, the transactions on the decentralised side have multiple sub-authorities, known as the intermediaries. In reality, the decentralised networks have multiple of centralised intermediates such as virtual currency exchanges, custodian wallets or atomic swaps (Wright & Filippi, 2015). New users who want to access the virtual currency network for the first time typically convert their fiat currency into virtual currency on the exchanges. If they're going to execute large trading blocks, they can do so via the OTC trading desk of those exchanges as well.

On exchanges that are regulated and fully compliant to the AML regulations, if law enforcement wants to trace a transaction on those exchanges, the information regarding users' identities should be available. Such exchanges often have well-defined AML policy detailing specific AML process, rigorous identity verification procedure, meticulous risk assessment framework, and effective transaction monitoring. Some major exchanges, such as Coinbase, Kraken, and Gemini are considered the financial institutions of the virtual currency field (Fitzpatrick, 2019). They typically place deposit or withdrawal

limitations, depending on the account verification level. For example, on Coinbase, a user has to reach the Pro-level of verification to withdraw up to USD 10 000 per day. Besides, virtual currency exchanges can restrict or ban user access to the service depending on the geographical locations from IP address or violation of Terms and Conditions. Therefore, practically speaking, money launderers still face restraints from exchanges that comply fully with the AML regulations.

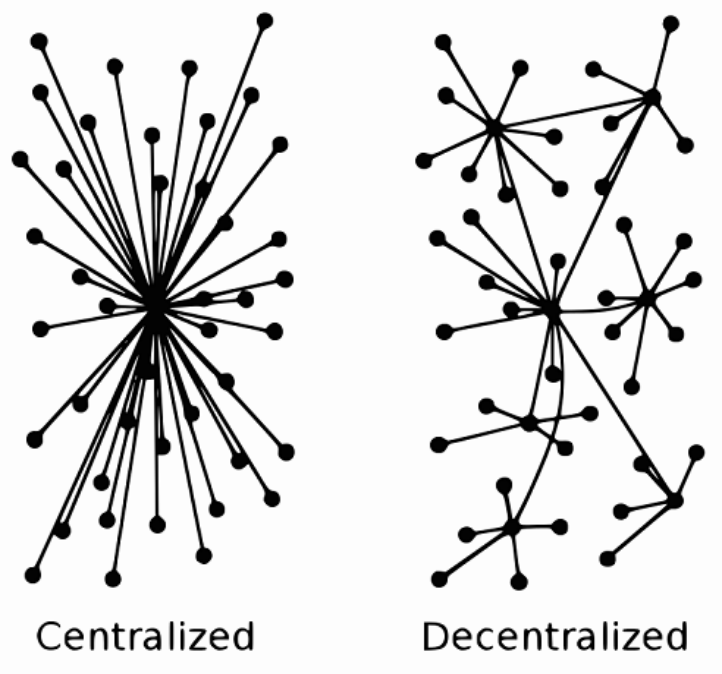


Figure 10. Centralised vs Decentralised. Source: Wright & Filippi, 2015

However, the elevated risk lies on exchanges and OTC desks that do not adhere strictly to the AML regulation or do not need to be AML compliant due to lack of local legislation (Chain analysis, 2020). Apart from the centralised exchanges mentioned in the previous paragraph, there are also decentralised exchanges (DEXs) which facilitate P2P transactions among their users using a unique exchange method known as an atomic swap. These swaps establish automated contracts that operate based on predetermined rules zero-fee trading. This decentralised nature can be considered a vulnerable money laundering point to law enforcement because some of these exchanges do not implement KYC control. A notable name is "bisq" (formerly Bitsquare), a DEX which only requires no name, no ID documents but just an email to register an account on its platform. Indeed, zero-KYC action intensifies the money laundering risks.

3 Methodology and analytical framework

3.1 Methodology

The study applies a case study approach which involves qualitative analysis. Yin, (2003:13) defines a case study as “an empirical inquiry that investigates a contemporary phenomenon in depth and within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident”. Unlike quantitative research which mainly consists of statistical generalisations (Jackson, 2008), the qualitative analysis focuses more on understanding the fundamental nature of the research problem (Strauss & Corbin, 1994). As the case study provides “the holistic and meaningful characteristics of real-life events” and answers the how or why question, it is aligned with the study’s objectives (Tellis, 1997:4). As addressed in section 1, the author aims at developing an AML internal process in a Finnish case company. Therefore, the case study is the most suitable approach to identify the business challenge and provide solution to match the European regulation as transposed into law in Finland.

The thesis research design is displayed in Figure 11 below. Before starting the research, the author decides the general details such as case study objective, case selection, research timeline and interview location, and determines the required skills and techniques. The case study’s goal is to reinforce the current AML internal process of the case company to comply with the regulatory requirements from the FIN-FSA. In the first phase, the author discusses the existing compliance challenges in the case company. To do so, the author prepares the data, identifies the criterion sampling, and conducts the relevant interviews with the company’s personnel. Afterwards, combing the internal documentation, the author revises the AML internal process based on the current state analysis, focusing on strengthening the case company’s AML program. Lastly, the author validates the process by acquiring feedbacks from a compliance consultant associated with the case company.

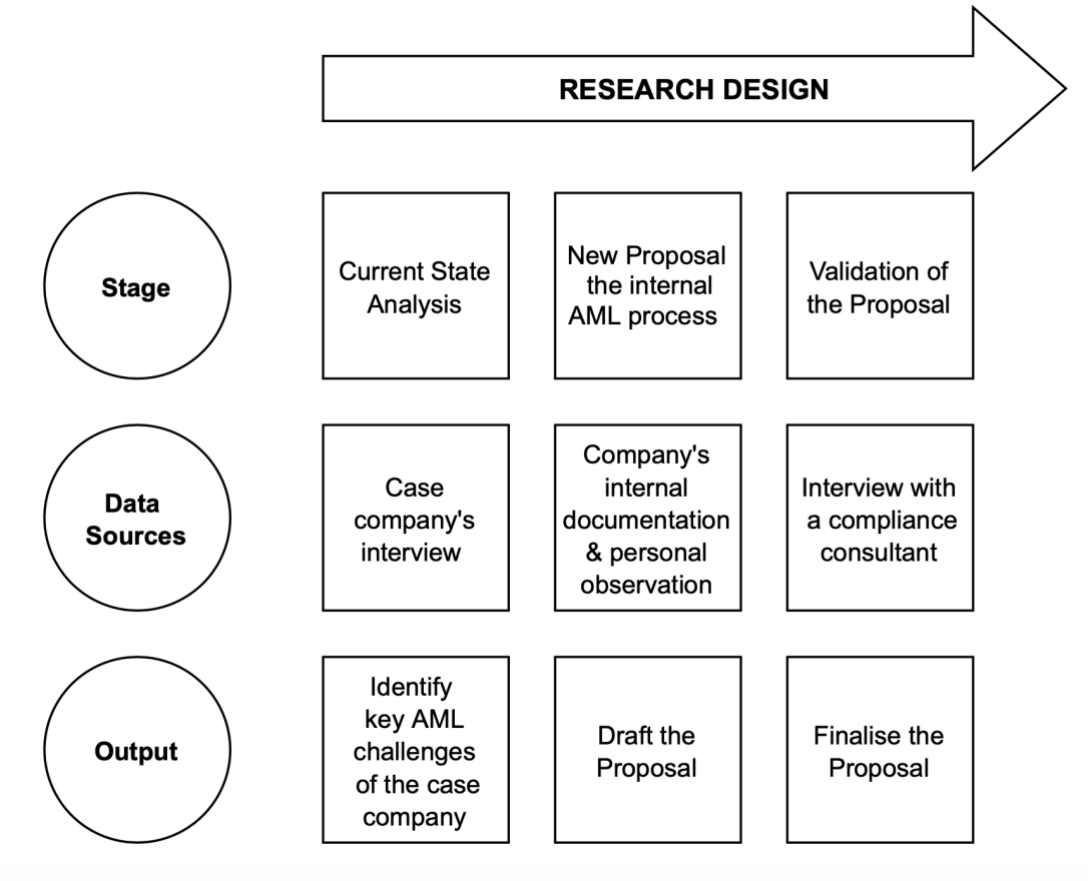


Figure 11. Research design

When designing the case study, the author decides whether the case is a good one based on recommendations from Kardos & Smith (1979). Firstly, a good case is the one taken from real life, although the real identities can be concealed. Secondly, the case should consist of many parts, and each part typically ends with problems and points for discussion. Thirdly, the case should include sufficient information for the readers to treat the issues. Finally, it should be believable for the reader.

3.2 Data Collection & Data Analysis

The qualitative data for this thesis was collected from three different stages to make sure that it is valid and reliable. The primary data was acquired through in-depth interviews. The use of qualitative data is prioritised in this thesis because it is insightful and allow access to the case (Yin, 1984:80).

The three data stages are displayed in Table 2 below.

Data Stage	*Data Source*	*Data Type*	*Period*	*Content*
1. Current State Analysis	Case company's personnels	Face-to-face interview	11/2019	Conducting interview about the current AML implementation status and challenges of the company
2. New proposal regarding the internal AML process	Personal Observation	Field notes	08/2019 - 02/2020	Observing the AML process (e.g. KYC, Transaction Monitoring, compliance technology, etc)
	Company's internal documentation	Documentation	08/2019 - 02/2020	Reviewing the case company's internal guidelines and revising the AML model
3. Validation of the Proposal	The compliance consultant	Face-to-face interview	03/2020	Conducting interview to validate and evaluate the AML reference model

Table 2. Data dollection methods

The first data stage was collected from the face-to-face interviews and the author's observation to conduct the current state analysis. The company's COO was chosen as the respondent because that person has the most knowledge of compliance issues in the case company. The interviews were conducted in English on a regular conversational basis. This author tried to create a pleasant atmosphere to help the respondent to openly share the opinions and insights precisely the way he means it. This approach is considered attractive because it involves little cost, which makes people feel familiar with their everyday conversations (Denscombe, 2010). The data from this interview was recorded by a recording device and inscribed on the author's field notes. Also, the author's observation over the six months was used in this stage to gain direct insight into the case company's actual AML practice.

The next data stage was compiled from the case company's internal documentation, including documents such as AML policy and documents detailing the IT infrastructure for blockchain analytics. The key findings of this phase would be combined with the data from the first phase to design an enhanced AML reference model aiming at improving the existing AML program. The details of the documentation are displayed in Table 3 below:

	Name of the document	***Number of Pages***	***Description***
1	Anti-Money Laundering and Counter Terrorist Financing Policy ("AML/CTF Policy")	17	Description of the fundamental AML principles of the case company to prevent and mitigate the AML risks
2	CDD/KYC Application form for Individuals and Corporate Clients	2	The standard KYC form for general clients and counterparties
3	EDD/KYC Application form for Individuals and Corporate Clients	2	The standard KYC form for high-risk clients abd counterparties
4	Identification Verification Process	3	Description of the process and technology employed to verify the identity of the clients and counterparties
5	Legal Documents	35	All legal documents related to the registration of the case company to the authority
6	Guidelines from the Finnish police	15	Presentation slides from the Finnish police detailing the sufficient AML measures

Table 3. Internal documentation details

The last data stage is to evaluate and validate the AML reference model by interviewing with a local compliance consultant. The selection of the respondent was decided based on the level of expertise in the compliance field. The critical requirement is that the person should have a high level of understanding to both compliance and the virtual currency sector. The author first approached the compliance consultant via email and scheduled a video call in March 2020.

4 Case study

4.1 Current State Analysis

About the case company

The case company of this thesis is a small company operating as a registered virtual asset service provider founded in Finland. The company's vision is to build an investment service that supports the growing adoption of virtual currency in the near future. Backed by reputable equity investors and venture capitalists with a proven track record, the company provides tailored asset management services to different customer segments. The team members of the company have a blend of deep expertise in traditional finance, blockchain, software development, and regulation, having worked at Tier-1 financial institutions around the world. After a period of operation, the business model of the case company is confirmed to be scalable with positive growth indicators. The revenue of the company was estimated to grow 120% in Q3 2019 and projected to continue this growth until Q3 2020.

The business challenges

As virtual currency spread across the world, the regulations become more and more developed to govern them. It is noted in the literature review that the regulatory landscape of VC is continuously evolving, especially in the European Union. From the company's point of view, the legal risk coming from lack of awareness or misunderstanding of the law related to the business might result in detrimental damages, including financial and reputational loss. The registration of the company with the local FSA has shown the company's determination to be fully compliant with the legal requirements. The Directors at the case company fully understands the importance of an efficient AML internal process to the existence of the business. The first reason is to

establish the legitimacy of the business toward not only law enforcement but also the company's counterparties as well. As the virtual currency is considered an evolutionary field yet utterly new to the traditional finance world, it has long faced restricted access and doubts from the investors' network. In the growth strategy of the company, developing a partnership relationship is crucial in scaling the business model. To do so, having a comprehensive AML program is considered a significant advantage in gaining trust from different counterparties and VASPs. Indeed, significant VASPs around the world have stepped up to endorse transparency in the field. As a result, a positive reputation in compliance comes in as a key to establish the reputation and legitimacy to ensure the stability and growth of the business model. The second reason is that the company needs a competent model that would save up time in the execution process. In the AML staff training, having a clear process chart will make it easier to assign the tasks to the correct departments, thus, removing the redundant stages. At the same time, the case company acknowledges the risk of having weak AML implementation. The AML approach of the company critically identifies the following factors:

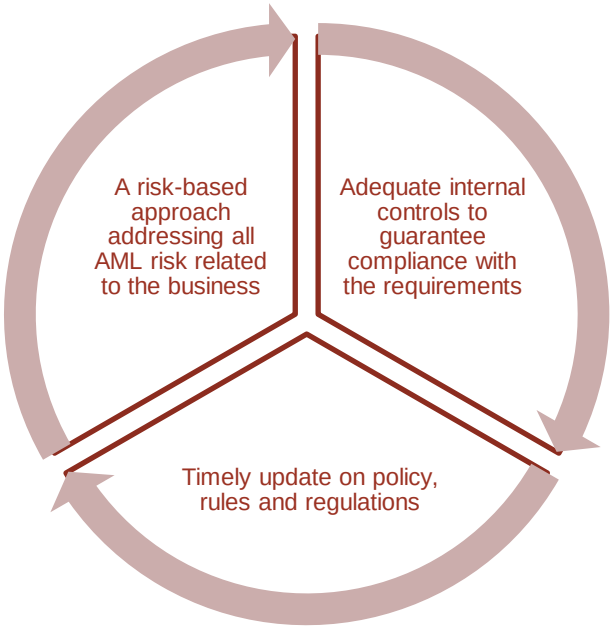


Figure 12. Case company AML approach

The company seeks to monitor closely and regularly update the AML Policy and internal procedure to ensure the most efficient compliance practice possible. The list of interview questions can be found in Appendix 1.

From the discussion between the author and the company's key compliance personnel, there are currently two key issues that the company needs to address:

(i) At the moment, the Compliance Officer is the only personnel duly authorised to guarantee the effective implementation and enforcement of the AML/KYC procedure as well as supervise all AML aspects related to the business. At the same time, at the impressive growth rate of the business, the company needs to hire new sales and customer representatives to engage more with the customers and drive in more sales pipelines. This situation has left the company to question whether the compliance department can coordinate with the Sales and the Technology team to make the current internal AML process better and more effective. In this case, the company **needs to structure an efficient internal AML process** to address this possible new change.

(ii) Along with the mentioned change and considering the operational risk, the company **needs better internal AML information and communication flow.** The company wants to explore whether there is any better communication flow than the existing one, given that the AML process will have multiple information points in the scenario above. This internal validity is needed before implementing the changes expected to occur in Q4 2020.

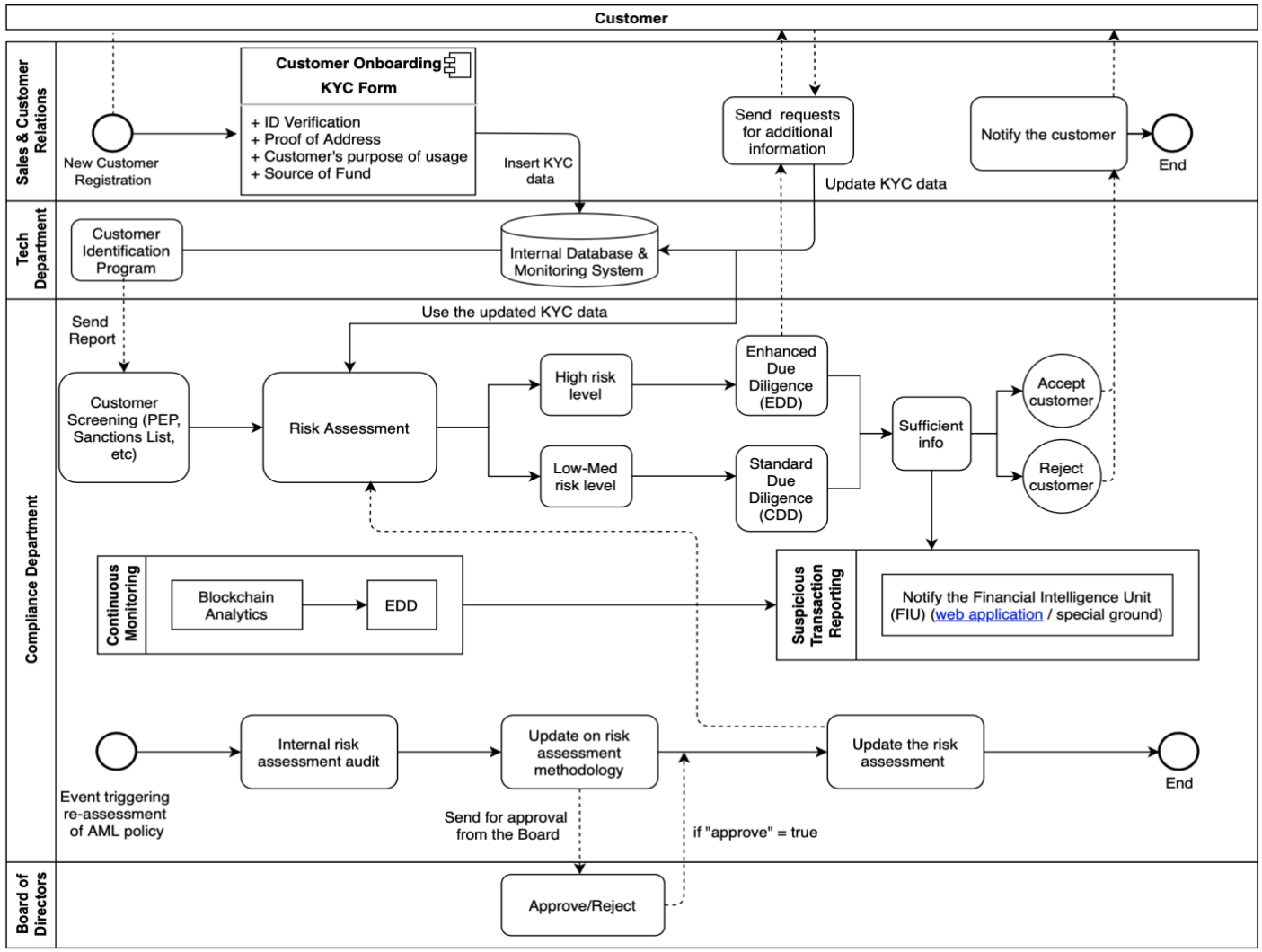
4.2 Build the Proposal

This section develops a proposal to improve the internal AML process (Figure 13) after considering the business challenges. The conceptual process has been created based on in-depth interviews, author's observation, the company's internal documentation, and literature review materials. This process shall provide guidelines and address the relevant AML mitigation controls.

The AML process involves four internal components in the case company: sales and customer relations, IT, Compliance department, and Board of Directors. It is triggered when a customer registers an account and enters the relationship with the case company.

From the figure below, the arrow indicates the sequential flow of the process, while the dashed arrow implies the communication and information flow.

Figure 13. AML Internal Process Proposal



As the case company provide virtual currency-related financial offerings, the AML process is attached to the daily operations such as account management and database monitoring. The AML process above is divided into four correlative activities: Customer Onboarding, Continuous Monitoring, Suspicious Transaction Reporting, and Audit AML Risk Assessment. First, the Customer Onboarding process includes KYC, customer identification program, customer screening, and AML risk assessment. After approving the customer to open an account, the compliance officer has to run all transactions through continuous monitoring to mitigate the AML risk during the process further. During the establishment of the customer relationship or when conducting the virtual currency transactions, if the company suspects that transaction is related to money laundering schemes, then the company shall immediately report a suspicious transaction to the FIU via an electronic form or on the special ground if necessary. On special occasions that trigger the Audit AML Risk Assessment, the Compliance Department has to assign an officer to analyse the AML program as a whole. The Board of Directors must approve the final decision to update the risk assessment before implementation.

4.2.1 Customer Onboarding Process

Upon entering the customer relationship with the company, the customer has to fill in a mandatory KYC form initially. As required in section 14, subsection 1 of the Act on Virtual Currency Providers (572/2019), the process of assessing the risk level of each customer begins with verifying the customer's identity and collecting other relevant data (Valtiovarainministeriö, 2019). Examples are such as proof of residential address, government identification number, general information on the source of fund, PEP status declaration and purpose of service usage. In this KYC form, the customer must review and agree to the Terms of Service and confirm the responsibility to provide accurate information.

The essence of this process is for the case company to (i) establish the customer identity, and (ii) obtain the preliminary understanding of the potential AML risks possibly linked to the customer. This process produces the first input data for the compliance team to conduct the risk assessment later. Customer profiles that have deficient or incomplete KYC information fail to sufficiently represent the customer and might lead to inaccurate risk rating. Therefore, the sales and customer representatives are responsible for diligently collecting the most accurate data possible and inserting this data into the internal database and monitoring system. During this phase, the company has to keep

the KYC information on entries in the register for five years from the date ending the customer relationship as required by section 10 of the Act on Virtual Currency Providers (572/2019). If a customer registers a corporate account, the identity of the authorised representative should be verified. According to the main change regarding UBO mentioned in Table 1, the company should identify the UBOs on a case-by-case basis. However, based on Directive 2004/39/EC, the corporate customer does not have to disclose the UBOs information and identity if it is a publicly listed company on regulated exchanges in one or several European Economic Area (EEA) region. This exemption also includes credit institutions if they have UBOs information available on request (FIN-FSA, 2018). If the company cannot identify the customer or perform the KYC actions, it should refuse to enter the customer relationship or conducting VC transactions. This case should be reported to the FIU depending on a case-by-case basis.

The proof of residential/business address can be a utility bill, bank statements, tax documents of the customers within the past three months.

Customer Identification Program

Once the customer verification data enters the internal database, the IT Department is responsible for verifying the customer's identity using the existing technological techniques or outsourcing to the third party. If the IT Department outsources this process to the third party, the company has to ensure that the third party vendor must comply with the guidelines on customer identification. However, the identification data must be stored in the database throughout the data retention period defined by section 10 of the Act on Virtual Currency Providers (572/2019). Afterwards, the IT officer has to send an identification report to the Compliance Department to proceed forward to customer screening.

The identity of any natural person should be verifiable based on a valid official identification document. If the company suspects the authenticity of the ID document, it should reserve the right to send a request for additional identity information to the customer. All ID documents have to contain the customer's picture and the validity period. According to the Standard 2.4 Customer Due Diligence of FIN-FSA, the company should accept the following ID documents:

- Valid documents issued by the Finnish authorities:

  - A driving license;
  - National identification card;
  - Passport, diplomatic passport;
  - Alien's passport, refugee travel document;
  - SII card containing photo (SII card is no longer issued since October 2008)
- Valid documents issued by the foreign authorities:
  - National passport issued by the foreign authority;
  - ID card accepted as a valid travel document.

The scan of these documents should be an original and high-resolution scan without being altered by photoshop. If the customer submits the passport scan, the MRZ graphical format must be visible so that the validity of the document is confirmed. If the ID document and proof of address are in the non-Latin format (e.g. Thai, Hebrew, Chinese), a notarised translation copy should be attached in the KYC form as well.

Customer Screening

Customer Screening is an crucial stage in the Customer Onboarding process. The Compliance Department is responsible for screening the customer data against the relevant external and internal PEP and sanction list databases. The Compliance Officer has to pay attention to not only the PEP but also to immediate family members and close associates of PEPs. They might enter the business relationship with the company. Likewise, the sanction lists in terms of persons, companies and commodities imposed by the United Nations Security Council (UNSC) and the EU should also be examined. An example of an entity belongs to the UNSC consolidated list is Islamic Republic of Iran Shipping Lines and Pyongyang-based Kwangson Banking Corporations.

According to the FATF Guidance on PEPs (FATF, 2013), the company should consider the following relevant points:

- Ensure the customer's PEP status is up-to-date: The Compliance Officer has to regularly check the PEP status of customers because sometimes they can become a PEP after entering the business relationship with the company;
- Use the Internet and media searches: Internet searches can help locating relevant information, but the reliability of the data should be considered;

- Use of commercial databases and third-party agent: The Compliance Officer should be cautious when using such databases because they have limitations regarding the accuracy level and the requirement by the authority. The PEP definitions of those databases and services should be verified to be aligned with the definition adopted in Finland. The most common databases are Office of Foreign Assets Controls (OFAC) and World-Check by Thomson Reuters;
- Use of general information publicised by competent authorities: This is useful to determine whether a PEP tries to abuse the financial system or not, depending on the corruption level;
- Use of in-house databases and information sharing within the industry or the country;
- Use of government-issued PEP lists;

AML Risk Assessment

Once the KYC, CIP and screening data enters the internal database and monitoring system, the Compliance Officer conducts the AML risk assessment to evaluate the risk factors and control environment. In a small company, the responsibility to oversee this process lies in the Compliance Officer. However, if the company plans to expand the business, the Compliance Department can hire more risk analysts to execute this process, given that sufficient staff training is provided. When evaluating the risks related to the business, it is essential to define the scope of the assessment. It should cover all inherent money laundering risk factors to classify and assign an individual risk level to the customer. In the case company context, the AML risk profile is important to formulate the total risk level related to the customer. In this section, the author applies the three risk assessment phases by the The Wolfsberg Group (2015) to the case company as follow

1. to identify the inherent risk factors and vulnerabilities,
2. to assess the risk controls,
3. to derive the residual risk level and assign the risk level to the customer.

Phase 1: Define the inherent risk factors

Inherent risk is defined as the current risk exposure of the company to the money laundering activities before implementing the mitigation controls (ECA, 2013).The author

divides the inherent risk factors to four risk categories which are relevant to the virtual currency service providers.

The current AML inherent risk factors related to the case company are displayed in Figure 14. The list is neither binding nor exhaustive.

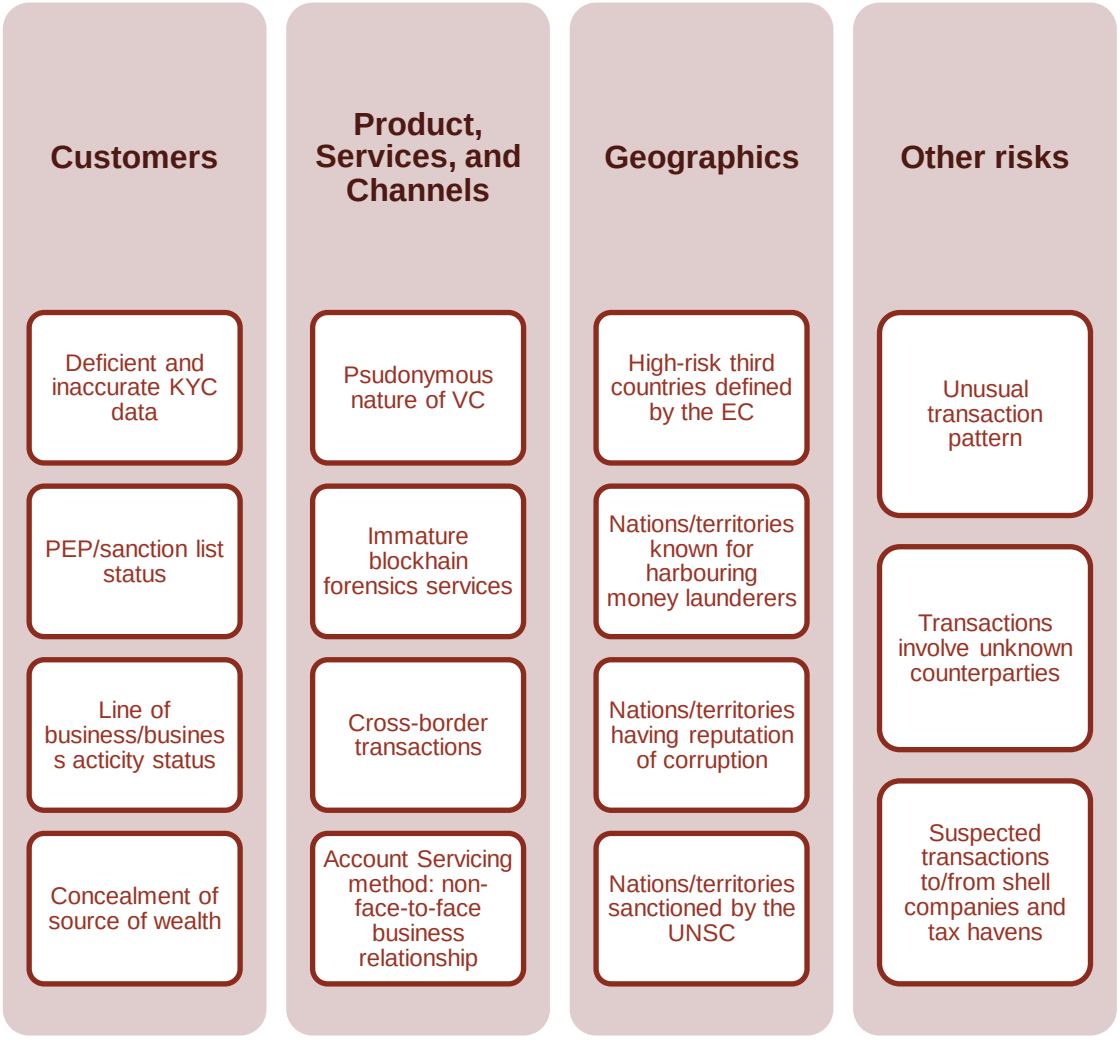


Figure 14. Inherent AML risk factor consideration

Upon examining the inherent risk factors, the Compliance Department should weigh these components to a risk category rating. A quantitative risk rating can be scored into a 5-tier rating scale, ranging from 0 to 100. The fewer the point is, the lower money laundering risk is associated with the company. This risk rating should be updated frequently to keep the assessment as accurate as possible.

- 0 - 20 : Low risk

- 21 - 40: Low-Med risk
- 41 - 60: Medium risk
- 61 - 80: Med-High risk
- 81 - 100: High risk

When using the quantitative rating scale, the Compliance Department has to ensure the risk rating scale reflects the risk categories realistically and objectively.

Phase 2: Assess the risk controls

Once the inherent risk factors are examined, the Compliance Officer has to analyse the operating efficiency of the internal AML risk controls. Here are the aspects to consider:

- KYC, CDD, and EDD process:
  - whether the KYC procedure adequately addresses the AML risk related to the inherent risks;
- Data Retention and Record-Keeping:
  - whether the customer's profiles are complete and accurate;
  - whether the internal database is up-to-date and available in case of reporting to FIU;
- Continuous Monitoring and Controls:
  - whether the level of reliance on the third-party service is acceptable;
  - whether the detection of unusual transactions is accurate;
  - whether the technological capacity is appropriate;
- Staff Training:
  - whether the employees receive proper AML training to ensure the AML competence level in operations;
- AML Policy and the company's governance:
  - whether the AML governance and policies address the AML risk adequately;
  - whether the AML training is frequently organised to update on any regulatory changes;
- Suspicious Transactions Reporting:
  - whether the existing information exchange and cooperation channel between the case company and the relevant authority is smooth;
  - whether the suspicious transaction is reported on time to the authority.

Each of the area mentioned above should be scrutinised meticulously. Each of the categories above should be rated based on the weighting factor. If the mitigation controls are found deficient, the Compliance Department is responsible for conducting the internal audit AML assessment and sending the proposal to the Board of Directors for approval. Once the Board accepts the changes, the Compliance has to update the risk assessment framework duly and organise the staff training to ensure the synchronisation in AML operation across all departments.

Phase 3: Derive the residual risk level and assign the risk level to the customer.

The final phase of AML risk assessment is to calculate the residual risk after considering the mitigation controls (The Wolfsberg Group, 2015). The residual risk calculation is the subtraction of the inherent risk level to the mitigation control. After determining the residual risk level, the Compliance Department would assign the due diligence action depending on the risk level. If the risk rating ranges from 0 to 60, the Compliance shall apply the standard Due Diligence process. If the risk rating ranges from 61 to 100, the Compliance shall proceed to the Enhanced Due Diligence procedure.

Below is an illustrative example of a risk assessment (this example does not represent any real cases):

	Inherent Risk Level				**Mitigation Controls**	**Residual Risk Level**	**Due Diligence Action**
	Customers	**Product**	**Geographics**	**Other risks**			
Customer X	5	10	8	9	5	**27** (Low-Med)	**Standard CDD**
Customer Z	15	25	20	18	3	**75** (Med-High)	**Enhanced DD**

Customer…	-	-	-	-	-	-	-

Table 4. AML risk assessment example

Enhanced Due Diligence

Once the Compliance Department assigns the EDD to the customer, the Customer Representative shall send the customer request for additional information. To comply with the Customer Due Diligence Code of Conduct of FIN-FSA (2010), the EDD process should be applied in the following cases:

- Customer or UBO who has a link to the high-risk third countries outlined by the European Commission;
- Customer who is a PEP;
- non-face-to-face identification;
- The residual risk level is medium to high;
- When the blockchain analytics implies the unusual transaction pattern or when the blockchain address links to the money laundering practice.

However, it should be noted that the EDD process has to address the level of risk on a case-by-case basis realistically. For example, if a customer declares on the KYC form that the source of wealth is from employment income, the Compliance Officer can ask the customer to provide the identity of the employer, latest accounts or tax declaration, recent payslip, etc. When the customer delivers the request document or information, the Customer Representative has to enter the data into the internal database. The Compliance Department then assesses if the information is sufficient to determine whether the company accepts or rejects the establishment of the customer relationship.

4.2.2 Continuous Monitoring & Suspicious Transaction Reporting

Ongoing monitoring is required to guarantee those suspicious transactions are duly detected and reported to the law enforcement. In some instances, the Compliance Department can initiate the EDD to request the customer to provide additional documents and information. At the same time, the Compliance Department can

immediately suspend the customer's account if it is suspected to engage in money laundering activities.

Examples of suspicious transaction activities include but not limited to:

- The VC transactions are not compatible with the characteristics of the business activity declared by the customers;
- The customer is suspected of falsifying the documents or refuses to disclose the required information;
- The blockchain analytics detects the blockchain address of the customer for having a connection with the money laundering activities.

During the Customer Onboarding or the Continuous Monitoring process, if the Compliance Department detects such cases, it shall notify and file in an electronic report to the Financial Intelligence Unit with detailed instructions.

4.3 Validation of the Proposal

In this stage, the author validates the proposal to examine whether the AML internal process would realistically address the business challenges provided by the case company.

The validation process was conducted through an in-depth interview with a local compliance consultant ("Informant X") who has substantial experience in both the virtual currency industry and legal framework. The author discussed with the informant about the AML Internal Process Proposal to (i) evaluate the feasibility of the proposal regarding the business challenge, and (ii) assess whether the process adequately covers the legal requirements imposed by the law enforcement in the Finnish context.

The overall evaluation of the proposal was positive. Informant X noted that having an AML internal process would provide the company with an advantage to deal with the AML risk. The most inherent benefit is that the process would reduce the company's resources spent on coordinating the compliance matter, thus, save the cost. By implementing the process, the company can allocate the resources to other departments and projects, such as research and development. Another considerable gain is communication flow. According to the feedback, a swimlane process chart details the

responsibility of each department precisely, therefore, saves time during the execution process.

> "Some parts of this process are sufficient to be put into operation: The Customer Onboarding process, Suspicious Transaction Activity, responsibility division, and the information flow." (Informant X)

However, informant X also emphasised that there were still areas of improvement before implementing the process model. First, regarding the AML risk assessment, informant X noted the importance of the human factor, which was not mentioned in the proposal. According to Informant X, if the company plans to expand the team members and recruit more sales representatives, it is crucial to notice the possible human error during the process.

> "There should be a section in the chart addressing the underlying human factor to ensure the occurrence of human error." (Informant X)

Second, informant X discussed that the process needs a complete data structure because it determines the strength of the AML regime. Notably, the risk rating mentioned in the AML risk assessment proposal should be evaluated carefully. This evaluation is because some qualitative risk factors cannot be reflected in a quantifying rating scale. Informant X articulated that the risk rating needs long-term testing at the case company to ensure the validity of the data.

The interview concluded that the proposal is functional but not adequate to put into implementation immediately concerning the timeline provided by the case company. Although the overall process still needs more development, the proposal was seen as a good fundamental foundation to create a more detailed and tailored AML internal process for future references. Some sub-activities of the process can be enforced based on the timeline outlined by the company.

5 Discussion and Conclusion

5.1 Summary

The objective of this thesis is to combine the literature and legal framework related to virtual currency to create an AML internal process for a case company in the Finnish context.

In the present, as detailed in the literature review, money launderers and criminals are continuously utilising sophisticated technology to bypass the detection of law enforcement. Consequently, the authority is tightening the regulations given the widespread growth of VC. In the European context, the introduction of AMLD5 in 2018 has changed the stance and business landscape of virtual currency service providers. Companies have strived to meet the necessary legal requirements to hedge the reputational risk and ensure the existence of the business. However, companies find it highly difficult when applying the lengthy legal framework to the actual implementation. Having an efficient AML internal process is seen as an advantage to reinforce the AML program. Companies having a positive reputation regarding the compliance practice shows the integrity in dealing with the elevated money laundering risks considering the high level of complexity in this field.

The study features a qualitative case study in the Finnish context. The fundamental of the case study derives from the increasing complexity of the AML offences, the growth of VC in the modern context, and the vast global AML gap concerning regulation and actual practice. The company is a Finnish VASP aiming at building an investment service that supports the growing adoption of virtual currency in the near future. The study started with the current state analysis of the company to determine critical business challenges. The first data from the interview revealed that the case company aimed at exploring a new AML internal process to establish the legitimacy of the business and improve the internal communication flow, given a possible change in personnel speculated to happen in the future. More importantly, it must be noted that the process has to take into consideration the AML risks and the legal requirements outlined in the literature review.

Against this background, the proposal was built and tailored to the case company through in-depth interviews, company's documentation, legislative materials and

author's observation. The output was a swim lane chart, which specifically detailed both sequence flow and information flow in the company. This process was found to be a feasible solution to agile compliance execution, which is aligned with the case company's AML approach:

1. A risk-based approach addressing all AML risks related to the business
2. Adequate internal controls to ensure compliance with the legal requirements
3. The timely update on policy, rules, and regulations

The process is divided into four correlative activities, namely: (i) Customer Onboarding Process, (ii) Continuous Monitoring, (iii) Suspicious Transaction Reporting, and (iv) Audit AML Risk Assessment. The idea behind this proposal is to help to define the AML risk mitigation controls correspondent to the legal requirements while always having an internal audit. The proposal also makes sure that each department is fully aware of the responsibility to avoid wasting time and resources, given that the AML process would be repetitive and continuous in real-life scenarios.

Lastly, the proposal was evaluated and validated through an in-depth interview between the author and the local compliance consultant. In general, the proposal was seen as a feasible solution. Certain parts of the process (e.g. Customer Onboarding, information flow) adequately address the business challenges. However, it was recommended by the consultant that the whole process should not be put into implementation according to the scenario drafted by the company because it needs more testing, especially the risk rating and risk criteria in AML risk assessment.

5.2 Reliability and Validity

Patton (2002) argued that the reliability and validity of research are essential concerns for any qualitative researcher designing a study, analysing the results, and determining the quality of the study. The author assesses the thesis reliability based on the four criteria: credibility (internal validity), transferability (external validity), dependability (reliability), and confirmability (objectivity) (Lincoln & Guba, 1985).

Credibility (Internal Validity)

This criterion is also known as internal validity, which answers to the question “How congruent are the findings with reality? (Shenton cited in Merriam, 2004:64). The credibility can be assessed by adopting the well-established research methods, developing an early familiarity with the culture of a participating organisation, performing triangulation, conducting reflective commentary. In this thesis, the author ensures the credibility of the study by engaging in the case company to gain an adequate understanding of the business challenge and establish the mutual trust with the company’s personnel before conducting the research. This strategy would ensure the collection of honest feedback and review from the informant.

Moreover, the author combines different methods and data sources, from the in-depth interview and internal documentation to personal observation. The supporting documents obtained from the case company provided comprehensive information regarding policy and governance. At the same time, the five-month period of personal inspection supported the author in understanding the compliance in practice. Meanwhile, another angle of triangulation was utilised as the author involve different informants for each research phases. The individual standpoint and experiences of each informant would enrich the research outcome.

Transferability (External Validity)

The transferability of research is “concerned with the extent to which the findings of one study can be applied to other situations” (Shenton cited in Merriam, 2004:69). In other words, the primary concern is whether the result of this study can be applied to a broader sample. In the case study, the process was constructed based on the legal requirements outlined by FATF and the EU, along with the theoretical framework of compliance. However, it must be noted that the author’s proposal was tailored to address the specific business challenge of the company in the Finnish context. Therefore, the author emphasised that some process details might not apply to other institutions due to the different nature of business. Readers are recommended to critically analyse whether the proposal is pertinent on a case by case basis, given that this research only involves a single sample company in thousands of virtual currency businesses around the world.

Dependability

The author has to assess whether the result remains the same if the work were repeated using the same method and in the same context to determine the dependability of the research (Shenton, 2004:71). Reliability of a study can be achieved through thorough research design, meticulous operational detail, and reflective appraisal of the paper. In the thesis paper, the research design, data collection methods, and internal documentation were reported in detail. However, the data from the interviews might be exposed to the bias, which is unavoidable, given that the respondent might not want to reveal the company's internal problem wholly. To mitigate bias, the author tried to create a comfortable environment and draft the appropriate interview questions. The fact that the case company agreed to show the author the confidential documents and involve her in high-level compliance discussion clearly shows their determination in disclosing the actual practice. However, the author insists that virtual currency is still a relatively new field with not many academic papers available. Therefore, the author had to feature multiple figures from Medium blogs as an illustration mean. However, the core theoretical and legal framework was obtained from the official regulations and structure of reputable organisations.

Confirmability

This criterion indicates the level of the author's influence on the research, including the investigator bias. While doing the case study, the author emphasised on the fact that she spent a year working at the case company. Therefore, she knows the company's actual AML practice. The author tends to reduce the impact of her personal belief by displaying the methodological description and reaffirming the reflective commentary. During the research period, the author tried to confirm her understanding of the issue with the compliance consultant to avoid bias.

6 References

Accenture, 2017. *Banking on blockchain a value analysis for investment banks.* [Online] Available at: https://www.accenture.com/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/consulting/accenture-banking-on-blockchain.pdf [Accessed 1 March 2020].

Aguilar, D., 2019. *Venezuelan Migrants Are Using Bitcoin for Remittances, But There's a Catch.* [Online] Available at: https://www.coindesk.com/venezuelan-migrants-are-using-bitcoin-for-remittances-but-theres-a-catch [Accessed 1 March 2020].

Allison, I., 2015. *Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering.* [Online] Available at: https://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480 [Accessed 24 March 2020].

Andriotis, A. M., Rudegeair, P. & Hoffman, L., 2019. *Inside Facebook's Botched Attempt to Start a New Cryptocurrency.* [Online] Available at: https://www.wsj.com/articles/facebook-wanted-to-create-a-new-currency-it-wasnt-ready-for-the-backlash-11571242795 [Accessed 1 March 2020].

Athey, S., 2015. *5 ways digital currencies will change the world.* [Online] Available at: https://www.weforum.org/agenda/2015/01/5-ways-digital-currencies-will-change-the-world/ [Accessed 1 March 2020].

Bachus, A., 2004. From Drugs to Terrorism: The Focus Shifts in the international fight against money laundering after September 11, 2001. *Arizona Journal of Internation & Comparative Law,* Issue 842.

Basel Committee on Banking Supervision, 2001. *Customer due diligence for banks.* [Online] Available at: https://www.bis.org/publ/bcbs85.pdf [Accessed 3 March 2020].

Borliini, L., 2012. *EU Anti-Money Laundering Regime: An Assessment within International and National Scenarios.* [Online] Available at: DOI:10.2139/ssrn.2144122 [Accessed 12 March 2020].

Brito, J. & Castillo, A., 2013. *Bitcoin: A Primer for Policymakers.* [Online] Available at: https://www.researchgate.net/publication/269707314_Bitcoin_A_Primer_for_Policymakers [Accessed 15 February 2020].

Buchanan, B., 2004. Money laundering—a global obstacle. *Research in International Business and Finance ,* Volume 18, pp. 115-127.

Chainanalysis, 2020. *Money Laundering in Cryptocurrency: How Criminals Moved Billions in 2019.* [Online] Available at: https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019 [Accessed 18 March 2020].

CoinMarketCap, 2020. *Top 100 Cryptocurrencies by Market Capitalization.* [Online] Available at: https://coinmarketcap.com [Accessed 29 January 2020].

Cox, D., 2014. *Handbook of Anti-Money Laundering.* s.l.:John Wiley & Sons.

Dabrowski, M. & Janikowski, L., 2018. *Virtual currencies and their potential impact on financial markets and monetary policy.* [Online] Available at: https://case-research.eu/files/?id_plik=5708 [Accessed 1 February 2020].

Denscombe, M., 2010. *The Good Research Guide for Small-Scale Research Projects.* 4th Edition ed. Beverly Hills, CA: Open University Press.

Deutsche Bank, n.d. *Imagine 2030 The decade ahead.* [Online] Available at: https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000503196/Imagine_2030.PDF [Accessed 17 February 2020].

Dibrova, A., 2016. *Virtual Currency: New Step in Monetary Development.* [Online] Available at: https://www.researchgate.net/publication/308003035_Virtual_Currency_New_Step_in_Monetary_Development> [Accessed 3 February 2020].

Domingo-Pascual, J., Shavitt, Y. & Uhlig, S., 2011. Traffic Monitoring and Analysis. *Third International Workshop,* p. 113.

ECA, 2013. *Risk assessment in performance audits.* [Online] Available at: https://www.eca.europa.eu/Lists/ecadocuments/GUIDELINE_RISK_102013/GUIDELINE_RISK_102013_EN.pdf [Accessed 11 April 2020].

ECB, 2012. *Virtual currency schemes.* [Online] Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf [Accessed 3 February 2020].

ECB, 2015. *Virtual currency schemes – a further analysis.* [Online] Available at: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf [Accessed 14 February 2020].

ECB, 2016. *Occasional Paper Series Distributed ledger technologies in securities post-trading.* [Online] Available at: https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf [Accessed 9 February 2020].

ECB, 2019. *Crypto-assets – trends and implications.* [Online] Available at: https://www.ecb.europa.eu/paym/intro/mip-online/2019/html/1906_crypto_assets.en.html [Accessed 1 March 2020].

European Union, 2018. *Directive (eu) 2018/843 of the european parliament and of the council.* [Online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?Uri=CELEX:32018L0843 [Accessed 10 February 2020].

Europol, 2018. *Illegal network used cryptocurrencies and credit cards to launder more than eur 8 million from drug trafficking.* [Online] Available at: https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking [Accessed 17 March 2020].

FATF, 2013. *politically exposed persons (recommendations 12 and 22).* [Online] Available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-PEP-Rec12-22.pdf [Accessed 11 April 2020].

FATF, 2014. *Virtual Currencies Key Definitions and Potential AML/CFT Risks.* [Online] Available at: <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> [Accessed 2 February 2020].

FATF, n.d. *Designated categories of offences.* [Online] Available at: https://www.fatf-gafi.org/glossary/d-i/ [Accessed 2 March 2020].

Ferguson, A., n.d. *Money Laundering.* Trinidad, CICAD-OAS.

FIN-FSA, 2018. *Customer due diligence; Prevention of money laundering and terrorist financing.* [Online] Available at: https://www.finanssivalvonta.fi/en/regulation/FIN-FSA-regulations/organisation-of-supervised-entities-operations/2.4/ [Accessed 10 April 2020].

FIN-FSA, 2019. *FIN-FSA regulations and guidelines 4/2019 concerning virtual currency providers enter into force on 1 July 2019.* [Online] Available at: https://www.finanssivalvonta.fi/en/publications-and-press-releases/supervision-releases/2019/fin-fsa-regulations-and-guidelines-42019-concerning-virtual-currency-providers-enter-into-force-on-1-july-2019/ [Accessed 16 March 2020].

FIN-FSA, 2019. *Virtual currency providers to be covered by supervision of anti-money laundering – Supervision will not extend investor protection to virtual currencies.* [Online] Available at: https://www.finanssivalvonta.fi/en/publications-and-press-releases/Press-release/2019/Virtual-currency-providers/ [Accessed 17 March 2020].

FIN-FSA, 2020. *Frequently asked questions on virtual currencies and their issuance (Initial Coin Offering).* [Online] Available at: https://www.finanssivalvonta.fi/en/banks/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/frequently-asked-questions-on-virtual-currencies-and-their-issuance-initial-coin-offering/ [Accessed 17 March 2020].

Genkin, D., Papadopoulos, D. & Papamanthou, C., 2018. Privacy in Decentralized Cryptocurrencies. *Communications of the ACM,* 61(6), pp. 78-88.

Grinspan, L., 2019. *Want to help people in Venezuela? Your best bet might be bitcoin..* [Online] Available at: https://www.vox.com/future-perfect/2019/7/10/18700235/cryptocurrency-venezuela-humanitarian-aid-maduro-bitcoin [Accessed 4 March 2020].

Houben, R. & Snyers, A., 2018. *Cryptocurrencies and blockchain.* [Online] Available at: http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf [Accessed 19 March 2020].

Huillet, M., 2019. *CipherTrace Detects Major Uptick in Cross-Border Payments to Offshore Crypto Exchanges.* [Online] Available at: https://cointelegraph.com/news/ciphertrace-detects-major-uptick-in-cross-border-payments-to-offshore-crypto-exchanges [Accessed 19 March 2020].

IMF, 2016. *Virtual Currencies and Beyond: Initial Considerations.* [Online] Available at: https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf [Accessed 1 March 2020].

Kardos, G. & Smith, o., 1979. On writing engineering cases.. *Proceedings of the American Society for Engineering Education National Conference on Engineering Case Studies.*

Kauflin, J., 2019. *Why Everyone In Crypto Is Talking About DeFi.* [Online] Available at: https://www.forbes.com/sites/jeffkauflin/2019/04/26/why-everyone-in-crypto-is-talking-about-defi/#47c021f2723f [Accessed 5 February 2020].

Keating, T., Carlisle, D. & Keen, F., 2018. *Virtual currencies and terrorist financing: assessing the risks and evaluating responses.* [Online] Available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)6 [Accessed 19 March 2020].

Kiernan, P., 2019. *Fed's Powell Says Facebook's Libra Raises 'Serious Concerns'.* [Online] Available at: https://www.wsj.com/articles/feds-jerome-powell-faces-senators-after-rate-cut-signal-11562837403 [Accessed 10 March 2020].

Klumov, G., 2020. *https://cointelegraph.com/news/why-internet-growth-is-a-prime-cryptocurrency-adoption-driver.* [Online] Available at: https://cointelegraph.com/news/why-internet-growth-is-a-prime-cryptocurrency-adoption-driver [Accessed 29 March 2020].

Kumar, A., Fishcer, C. & Saxena, A., 2017. *A Traceability Analysis of Monero's Blockchain.* [Online] Available at: https://eprint.iacr.org/2017/338.pdf [Accessed 24 March 2020].

Lastra, R. & Allen, J., 2018. *Virtual currencies in the Eurosystem: challenges ahead.* [Online] Available at: https://www.europarl.europa.eu/cmsdata/150541/DIW_FINAL%20publication.pdf [Accessed 20 January 2020].

Leong, G., 2017. *MAS clarifies position on regulation of digital token offers.* [Online] Available at: https://www.straitstimes.com/business/companies-markets/mas-clarifies-position-on-regulation-of-digital-token-offers [Accessed 18 March 2020].

Levi, M. & Reuter, P., 2006. *The University off Chicago.* [Online] Available at: https://www.tni.org/files/publication-downloads/money_laundering_levi_and_reuter.pdf [Accessed 15 January 2020].

Lincoln, Y. & Guba, E., 1985. *Naturalistic inquiry.* Beverly Hills, CA: Sage.

Luu, J. & Imwinkelried, E., 2015. The Challenge of Bitcoin Psuedo-Anonymity To Computer Forensics. *UC Davis Legal Studies Research Paper Series*

McDowell, J., 2001. The consequences of money laundering and financial crime. *An Electronic Journal of the U.S. Department of State ,* 6(2).

Ministry of Justice, Finland, 2015. *The Criminal Code of Finland.* [Online] Available at: https://www.finlex.fi/en/laki/kaannokset/1889/en18890039.pdf [Accessed 4 March 2020].

MIT Technology Review, 2019. *Venezuela may be turning to Bitcoin to get around sanctions.* [Online] Available at: https://www.technologyreview.com/2019/09/27/75405/venezuela-may-be-turning-to-bitcoin-to-get-around-sanctions/ [Accessed 17 February 2020].

Murphy, C., 2020. *Over-The-Counter (OTC).* [Online] Available at: https://www.investopedia.com/terms/o/otc.asp [Accessed 17 March 2020].

Nakamoto, S., 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System.* [Online]. Available at: https://bitcoin.org/bitcoin.pdf [Accessed 1 March 2020].

Nance, M., 2018. The regime that FATF built: an introduction to the Financial Action Task Forc. *Crime Law Soc Change,* Issue 69, pp. 109-129.

Patton, M., 2002. *Qualitative evaluation and research methods.* 3rd Edition ed. CA: Sage Publication.

Paul, K., 2019. *Libra: Facebook launches cryptocurrency in bid to shake up global finance.* [Online] Available at: https://www.theguardian.com/technology/2019/jun/18/libra-facebook-cryptocurrency-new-digital-money-transactions [Accessed 1 March 2020].

Pirus, B., 2020. *There Are Now Over 7,000 Cryptocurrency ATMs Worldwide.* [Online] Available at: https://cointelegraph.com/news/there-are-now-over-7-000-cryptocurrency-atms-worldwide [Accessed 27 March 2020].

Robert, J. J., 2020. *How shadowy brokers allegedly launder billions for crypto criminals.* [Online] Available at: https://fortune.com/2020/01/15/crypto-criminals-brokers-launder-billions/ [Accessed 29 January 2020].

Roberts, J., 2020. *How shadowy brokers allegedly launder billions for crypto criminals.* [Online] Available at: https://fortune.com/2020/01/15/crypto-criminals-brokers-launder-billions/ [Accessed 18 March 2020].

Salas, M., 2005. *The third anti-money laundering directive and the legal profession.* [Accessed 16 March 2020].

Sharman, J., 2008. Power and Discourse in Policy Diffusion: Anti-Money Laundering in Developing States. *International Studies Quarterly ,* Volume 52, pp. 635-656.

Shenton, A., 2004. *Strategies for Ensuring Trustworthiness in Qualitative Research Projects.* [Online] Available at: https://www.researchgate.net/publication/228708239_Strategies_for_Ensuring_Trustworthiness_in_Qualitative_Research_Projects [Accessed 20 April 2020].

Strauss, A. & Corbin, J., 1994. *Grounded theory methodology..* s.l.:SAGE.

Szostek, D., 2019. *Blockchain and the Law.* 1st Edition ed. s.l.:Nomos Verlagsgesellschaft.

Tellis, W., 1997. Introduction to Case Study. *CAHSS,* 3(2), pp. 1-14.

The U.S. Department of Justice, 2020. *Ohio Resident Charged with Operating Darknet-Based Bitcoin "Mixer," which Laundered Over $300 Million.* [Online] Available at:

https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million [Accessed 20 March 2020].

The Wolfsberg Group, 2015. *Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption.* [Online] Available at: https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/faqs/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf [Accessed 11 April 2020].

UNODC, 2009. *Money laundering and financing of terrorism.* [Online] Available at: https://www.unodc.org/documents/southeastasiaandpacific/2009/02/TOCAMLO/07-CHAPTER_II.pdf [Accessed 16 March 2020].

UNODC, n.d. *Money Laundering And The Financing Of Terrorism: The United Nations Response.* [Online] Available at: https://www.imolin.org/pdf/imolin/UNres03e.pdf [Accessed 10 March 2020].

Valtiovarainministeriö, 2019. *Eduskunnan vastaus hallituksen esitykseen VM/2018/157.* [Online] Available at: https://vm.fi/paatos?decisionId=0900908f8062bd8c [Accessed 29 March 2020].

Verhage, A., 2008. Between the hammer and the anvil? The anti-money laundering-complex and its interactions with the compliance industry. *Crime, Law and Social Change,* Issue 52, pp. 9-32.

Wan, C., 2020. *Chainalysis traced $2.8 billion in bitcoin being sent to crypto exchanges by criminals last year.* [Online] Available at: https://finance.yahoo.com/news/chainalysis-traced-2-8-billion-221124730.html [Accessed 19 March 2020].

Wintermeyer, L., 2018. *The Role Of Cryptocurrencies In Future Society.* [Online] Available at: https://www.forbes.com/sites/lawrencewintermeyer/2018/10/26/the-role-of-cryptocurrencies-in-future-society/#900e6e3787d1 [Accessed 1 March 2020].

World Bank, 2017. *Distributed Ledger Technology (DLT) and Blockchain.* [Online] Available at: http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf [Accessed 2 March 2020].

Wright, A. & Filippi, P., 2015. *DECENTRALIZED BLOCKCHAIN TECHNOLOGY AND THE RISE OF LEX CRYPTOGRAPHIA.* [Online] Available at: https://www.intgovforum.org/cms/wks2015/uploads/proposal_background_paper/SSRN-id2580664.pdf [Accessed 27 March 2020].

Yin, R., 1984. *Case Study Research: Design and Methods.* Beverly Hills, California: SAGE.

Yin, R., 2003. *Case Study Research: Design and Methods.* s.l.:SAGE.

Appendix 1. Interview Questions for Case Company Personnel

Topic	Questions
1. General Compliance Background	- What is the company's overall AML strategy? - How relevant is the compliance issue to the business? - Who is responsible for designing the AML Program? - Can you walk me through the worst pain of your AML program from your point of view? - What are the possible changes in the business environment that might affect the compliance decisions?
2. Customer Onboarding Process	- Can you describe the general customer onboarding process? - What are the required documents of individual/corporate customers? - How do you store the customer's data? - How do you communicate with the customers? - How do you transfer the information internally?
3. AML Risk Assessment	- Who is in charge of auditing the AML Risk Assessment? - We already discussed this topic, but can you confirm again with me the risk criteria of the company? - What is the basis of your risk rating? - What is the rationale behind dividing the customer into CDD & EDD?
4. Continuous Monitoring & Suspicious Transaction Activity	- Who is responsible for monitoring the transactions? - To whom do you report if there is suspicious transaction? What happens afterwards? - How do you detect suspicious activities? - How do you guarantee up-to-date database? - What kind of technological tool do you use for blockchain analytics?