

Received Date: 21 April 2026**Accepted Date: 12 May 2026****Published Date: 1 June 2026**

Do blockchain-based crypto-assets facilitate the laundering of cryptocurrencies?

BOUNAR Amine ¹, BENNIS Laila ², MAZIZI Ikbal ³, Elmehdi BOUIRY ⁴

1. PhD student, National School of Commerce and Management, Kenitra, Ibn Tofail University – Morocco, Organisational Management Sciences Research Laboratory, amine.bounar13@gmail.com
2. Lecturer and Researcher, Kenitra National School of Commerce and Management, Ibn Tofail University – Morocco, Commerce and Management Research Laboratory, lailabennis30@gmail.com
3. PhD student, National School of Business and Management, Kenitra, Ibn Tofail University – Morocco, Commerce and Management Research Laboratory, maziziikbal@gmail.com
4. PhD, The Ain Chock Faculty of Legal, Economic and Social Sciences, Casablanca (FSJES Ain Chock) – Morocco, Business Intelligence, Organisational Governance, Finance and Financial Crime Laboratory (BIGOFCF), mehdibouiry43@gmail.com

Abstract

Cryptocurrency has become a hot topic in the financial world; given that its value rose sharply following the 2008 financial crisis, Bitcoin is the convertible virtual currency with the highest market capitalisation, having soared to new record highs. However, despite the success of cryptocurrencies, they have not been adopted by the public authorities in Morocco. Although there are legal and financial restrictions hindering the use of these cryptocurrencies and crypto-asset exchange platforms, known as ‘blockchain’, there are still proponents of illicit alternative investment who use cryptocurrencies for the purposes of corruption, fraud, terrorist financing and money laundering associated with the use of new technologies that guarantee security whilst avoiding the attention of regulatory authorities, hence the question of regulation is beginning to

arise. Consequently, very little research has been conducted into the use of cryptocurrencies in the context of money laundering or terrorist financing. An analysis of secondary data provides us with a presumptive certainty that the proceeds of criminal activities can be laundered through various dark web services; it also reveals that there are reputation-based services capable of processing transactions as part of a cash-out strategy (*‘Daniel Dupuis, Kimberly Gleason, 2020, p. 4’*). Therefore, the aim of this research is to answer the following questions:

How do money launderers use blockchain and cryptocurrencies for money laundering purposes? And how can the use of blockchain and cryptocurrencies for related financial offences be prevented?

Finally, the findings of our research are as follows:

- Criminals and professional money launderers are taking advantage of the rapid growth of cryptocurrencies and the anonymity they provide to facilitate the money laundering process;
- The blockchain is a suitable tool for uncovering fraudulent activities as it records all transactions carried out since its creation and makes it easier for central banks, including the bam, to prevent and detect illegal activities retrospectively.

To address these issues and for methodological reasons, this study will be structured around the following four areas:

- ❖ The first area will focus on blockchain as a technological innovation that facilitates cross-border transactions;
- ❖ The second area will focus on the regulation of cryptocurrency;
- ❖ The third area will outline the process of money laundering via cryptocurrencies;
- ❖ The fourth section will outline the regulatory guidelines relating to this new convertible virtual currency.

Keywords: Blockchain; Cryptocurrencies; Financial crime; Money laundering; Central banks.

1. Introduction

One area undergoing rapid change is that of digital technology, where recent developments include new payment transfer systems and new virtual and digital currencies (Mohammed Ahmad Naheem, 2019, p. 1).

The relentless evolution of technology and its growing global reach has transformed all strata of society, including the development of payment systems and forms of currency.

Admittedly, this fourth industrial revolution has had detrimental effects in terms of financial crime for countries with fragile infrastructure. This revolution provides an environment conducive to criminals and professional money launderers, enabling them to launder their illicit funds as easily as possible. However, it offers an opportunity for countries with robust infrastructure to promote international trade whilst fostering a sense of trust amongst traders.

Furthermore, crypto-assets are virtual assets that operate within decentralised systems based on blockchain technology. In contrast, government-issued fiat currencies are issued by central banks and are centralised, with all transactions recorded on a central server. As a result, customers generally trust this system as it is based on universally accepted rules and is appropriately regulated by legislation.

Thus, centralisation not only enables currencies and transactions to be regulated but also allows them to be monitored, so that Morocco's anti-money laundering framework – in this case, the Moroccan Law on Combating Money Laundering and the Financing of Terrorism (Law No. 43-05, which was amended and supplemented by the new Law No. 12-18°) complies with the 49 recommendations established by the Financial Action Task Force (FATF).

Indeed, traditional banks are required to carry out customer due diligence (CDD), which includes 'Know Your Customer' (KYC) and 'Anti-Money Laundering' (AML) procedures. These procedures involve identifying beneficial owners, the proposed business relationship, the source of funds and more.

Furthermore, the concept of cryptocurrency was first proposed in 1983 by the American cryptographer David CHAUM, who viewed cryptocurrency as a means of creating electronic money. Chaum's views on money and privacy led him to believe that, in order to trade securely, we needed a token-based currency that mimicked fiat currency but allowed for higher levels of confidentiality and security (*Angela S.M., Irwin, Adam B., Turner, 2018, p. 5*).

Then, Satoshi Nakamoto – a group of individuals whose identities remain unknown – put David Chaum's suggestion into practice by creating Bitcoin for the first time in 2009 "*Chad Albrecht, Kristopher McKay Duffin, Steven Hawkins, Victor Manuel Morales Rocha, 2019, p. 1*". From that point onwards, cryptocurrency transactions have been carried out securely and without the involvement of financial intermediaries. Moreover, cryptocurrencies have experienced exponential growth in terms of price, popularity and adoption by the general public.

There are currently more than 1,800 cryptocurrencies, whose market capitalisation exceeded 300 billion dollars in July 2018 — *Sean Foley, Jonathan R, Karlsen, Tālis J. Putniņš, 2019, p. 1798*". Furthermore, they are not subject to Know Your Customer (KYC) and Anti-Money Laundering (AML) procedures. This so-called innovative blockchain technology provides opportunities for criminals and professional money launderers. By contrast, the traditional banking system makes it easy for banking supervisory authorities and the National

Financial Intelligence Unit (ANRF) to prevent and detect suspicious transactions.

Very little research has been conducted into the use of cryptocurrencies in the context of money laundering or terrorist financing. An analysis of secondary data provides us with a presumptive certainty that the proceeds of criminal activities can be laundered through various dark web services; it also reveals that there are reputation-based services capable of processing transactions as part of a cash-out strategy (*'Daniel Dupuis, Kimberly Gleason, 2020, p. 4'*).

The banking sector has always been vulnerable to being used for illegal money laundering, which led supervisory and regulatory authorities to introduce legislation on banking secrecy for the first time in 1970.

As banks have continued to strengthen their anti-money laundering (AML) measures, criminals are simultaneously seeking to increase the complexity and sophistication of their money-laundering schemes (Mohammed Ahmad Naheem, 2019, p. 1).

Consequently, criminals and professional money launderers are colluding to circumvent existing banking regulations whilst taking advantage of the emergence of new decentralised technology, which may further facilitate the money laundering process.

The aim of this study is to answer the following questions:

How do money launderers use blockchain and cryptocurrencies for the purposes of money laundering? And how can the use of blockchain and cryptocurrencies for related financial offences be prevented?

To address this issue and for methodological reasons, this study will be structured around the following four areas:

- ❖ The first area will focus on the blockchain as a technological innovation that facilitates cross-border transactions;
- ❖ The second area will focus on the regulatory framework for cryptocurrencies;
- ❖ The third strand will outline the process of money laundering via cryptocurrencies;
- ❖ The fourth area will outline the regulatory guidelines relating to this new convertible virtual currency.

2. Blockchain as a technological innovation that facilitates cross-border transactions.

At first glance, digital currencies such as Bitcoin – the largest cryptocurrency, which accounts for around half of the total market capitalisation – stand out. The numerous online cryptocurrency markets and exchanges have a daily trading volume of around 50 billion dollars. More than 300 crypto funds have been established (speculative funds that invest solely in cryptocurrencies), attracting around \$10 billion in assets under management (*Sean Foley, Jonathan R Karlsen, Tālis J. Putniņš, 2019, p. 1799*). Bitcoin is a convertible electronic currency traded on a peer-to-peer (P2P) computer network based on the principle of cryptography to validate transactions (*"Alaoui Lalla Latifa, Saghrane Mohamed, Yassine, 2018, p. 2"*). This currency was created in 2009 by Satoshi Nakamoto, who utilised a technological system known as the blockchain, which is inseparable from Bitcoin. This anonymous platform enables the storage and transmission of information, transparency, decentralisation, security and anonymity, whilst also serving as a database containing the history of all transactions carried out between users. It also provides users with a unique, standardised identifier for each transaction, known as a hash. Each identifier is added to a block, which then places that transaction in a chain of other blocks. This acts as a chronological record, so that the value and sequence of transactions are recorded (*Mohammed Ahmad Naheem, 2018, p. 4*).

This innovative decentralised technology guarantees users:

- Anonymity;
- Professional secrecy, even vis-à-vis central supervisory authorities;
- The ability to carry out transactions in a fraction of a second;
- Facilitates international trade;
- Means of guaranteeing the delivery of a product;
- Facilitates money laundering, tax fraud and tax evasion.

Furthermore, Bitcoin miners are volunteers who work to solve the algorithm in exchange for a reward of 25 bitcoins for each function solved. Moreover, Table N 1 below shows the trend in the number of bitcoins in circulation, in millions.

Once consensus is reached on the algorithm, the block can be added to the chain. This verification and proof-of-work system ensures the security of the currency as it cannot be easily altered or manipulated and leaves a permanent record of transactions. Unlike other means of exchange such as art markets, which can fluctuate due to issues of trust *‘Mohammed Ahmad Naheem, 2019, p. 4’*. More specifically, the person selling a bitcoin is not necessarily involved in building the blockchain as this process is carried out solely and exclusively by bitcoin miners. Every transaction that takes place must be verified by the miners and recorded in the ledger, which requires solving the algorithm that constructs the next block *“Mohammed Ahmad Naheem, 2019, p. 3”*.

Table 1: The evolution of the number of bitcoins in circulation, in millions.

Date	Number of bitcoins in circulation (in millions)
Quarter 1 (Q1) 2011	5.8
Quarter 3 (Q3) 2011	7.38
Q1 2012	8.69
Q3 2012	10.06
Q1 2013	10.96
Q3 2013	11.77
Q1 2014	12.59
Q3 2014	13.33
Q1 2015	14
Q3 2015	14.67
Q1 2016	15.03
Q3 2016	15.72

Q1 2017	16.08
Q3 2017	16.42
Q1 2018	16.78
Q3 2018	17.12
Q1 2019	17.62
Q3 2019	17.79
Q1 2020	18.13
Q3 2020	18.42
Q1 2021	18.59
Q3 2021	18.75
Q1 2022	19

Source: Compiled by us; figures taken from the STATISTA website

This table shows the total number of Bitcoins in circulation worldwide, in millions, between the first quarter of 2011 and the start of the first quarter of 2022. It can be seen that the number of Bitcoins in circulation has risen astronomically, from 6 million in 2011 to 19 million in the first quarter of 2022.

Broadly speaking, the blockchain – which is inextricably linked to cryptocurrencies – allows users to operate anonymously and commit a related financial offence known as crypto, without attracting the attention of commercial banks, central banks, financial intelligence units and the Financial Action Task Force (FATF), as this digital currency is undetectable and uncontrollable.

3. Regulation of cryptocurrency

Several countries recognised the risks inherent in this new form of currency at an early stage and set up teams to thoroughly analyse the risks intrinsically linked to cryptocurrencies, as well as the associated benefits. Among these countries, the following can be cited:

3.1. Morocco

Morocco has banned transactions in bitcoins and cryptocurrencies since 20 November 2017 (*Zakaria Bziker, 2021, p. 2*). In fact, this ban has not caused any unrest within the Moroccan community, except amongst a minority who use cryptocurrencies for financial crime.

Furthermore, in a joint press release issued on Tuesday 21 November 2017 by the Moroccan Ministry of Economy and Finance, Bank al Maghrib (BAM) and the Moroccan Capital Markets Authority (AMMC), it was announced that Morocco would accept digital exchange platforms for the bitcoin as a means of payment for the purchase of goods and services.

Following this joint statement, convertible virtual currency, or cryptocurrency, is regarded as a decentralised unit of account, created not by a state or a monetary union but by a group of individuals or legal entities, based on the existence of a ledger containing all transactions, which is kept up to date across all nodes of the network (blockchain technology).

Furthermore, virtual currency is traded exclusively online and therefore does not exist in the form of coins or banknotes. There are now more than 5,000 such currencies, of which Bitcoin is the most established.

As this is an unregulated activity, the Ministry of Economy and Finance, the BAM (which established a new institutional committee in 2017 to assess the risks and benefits of cryptocurrencies for the national economy) and the AMMC are drawing the public's attention to the risks associated with the use of virtual currencies, chief among which are:

- The lack of regulatory protection to cover losses in the event of exchange platform failure;
- The lack of a specific legal framework to protect users of these currencies in relation to transactions carried out, particularly in the event of theft or misappropriation;
- The volatility of the exchange rate of these virtual currencies against a legal tender (rates that can fluctuate sharply, both upwards and downwards,

within a very short period of time and in an unpredictable manner);

- The use of these currencies for illicit or criminal purposes, in particular money laundering and the financing of terrorism.

On 23 March 2021, the Wali of Bank Al-Maghrib (BAM) stated during his press briefing that Morocco was part of a global debate surrounding cryptocurrencies, as the COVID-19 crisis had clearly demonstrated that digital technology is set to become increasingly important both in the areas of trade and commerce and in monetary matters. He also added that Morocco was taking part in various discussions with international stakeholders on the subject to draw on their experiences, with a view to opting for a gradual evolution of the legal framework and the way in which it will oversee and regulate this convertible digital currency (MNC).

The Governor of the BAM was quick to quote the Chair of the US Federal Reserve System (Fed): "Cryptocurrency is not a currency; it may be an asset, but it is speculative." He also emphasised the risk of money laundering associated with the use of this convertible digital currency (CDC), whilst taking into account the guidelines on the risk-based approach to virtual assets and virtual asset service providers published by the Financial Action Task Force (FATF).

The anonymity of blockchain-based cryptocurrencies is the key issue driving central banks – in this case, the BAM – to regulate or prohibit the use of crypto-assets in Morocco. Although cryptocurrencies are banned in Morocco, their use cannot be stopped. There is no practical way for a government to enforce the ban as long as people have smartphones and internet access. Anyone can participate in public cryptocurrency ledgers, as there is no need to identify oneself or register, unlike with traditional banks, which have a 'Know Your Customer' (KYC) process in place from the outset of a banking relationship.

Indeed, a Moroccan citizen was accused of trading cryptocurrency – specifically Bitcoin (which is not recognised as a currency under Moroccan law) – on a Finnish blockchain platform, where he had been buying and reselling Bitcoin on behalf of his clients in return for commissions ranging from 3 per cent to 8 per cent, from 2016 until his arrest in March 2020. The investigation also identified nearly 1,000 clients, 99 per cent of whom are Moroccans.

The Court of Appeal had in fact sentenced the offender to eighteen months' imprisonment, plus financial penalties

ranging from 11.2 million dirhams to 2.2 million dirhams payable to the customs authorities.

As they are unable to monitor cryptocurrency transactions, digital currency provides an opportunity for money launderers to refine their techniques for money laundering and the financing of terrorism.

3.2. European Union (EU)

The Fifth Anti-Money Laundering Directive (5AMLD) is currently the European Union's main piece of legislation governing cryptocurrencies.

It should be noted that EU directives and regulations have different legal characteristics. Whilst an EU regulation is a directly applicable legal act, which does not require transposition into national law, a directive is an indirect legal act. This means that the competent authorities of the European Union have set a specific deadline for Member States to transpose the directive into their national law, whilst national authorities are free to choose the means and methods to achieve the intended objective. Thus, Member States were required to implement the directive's provisions by 10 January 2020.

This directive also sets out certain requirements for Member States to regulate this area:

- Empowering national financial supervisory authorities to obtain the addresses and identification details of digital currency owners;
- The obligation for cryptocurrency exchanges and wallets to register with the competent authorities in their country of establishment;
- The obligation for platforms providing cryptocurrency services to submit suspicious activity reports (SARs) and carry out customer due diligence (CDD).

European Union countries are implementing both digital technologies and the 5th AMLD at breakneck speed. Among the most active jurisdictions in this field, Malta and Estonia are leading the way.

3.3. Germany

The Federal Republic of Germany ranks 33rd globally for cryptocurrency adoption and 9th in the 2020 Global Innovation Index. Nevertheless, the EU's largest economy is often seen as lagging behind by other members of the bloc, so the German authorities' stance on cryptocurrencies appears

particularly significant. As for taxation, bitcoins are recognised as assets and are subject to capital gains tax.

According to regulations issued by the German Ministry of Finance, Bitcoin has been classified as a means of payment, meaning that the purchase of goods or payment for services using digital currency is subject solely to VAT.

Consequently, from January 2020, German banks have been authorised to hold and trade in bitcoins and other cryptocurrencies; furthermore, the law stipulates that online banking services involving transactions in shares, bonds and cryptocurrencies, will only be available to German financial institutions; specifically, 40 banks have expressed an interest in obtaining a licence for cryptocurrency services, which has been issued by the Federal Financial Supervisory Authority (BaFin), *'Evgheni Florealorea, Elena S. Pustelnik, 2021, pp. 74, 75 and 76'*.

3.4. The United Kingdom

The country openly supports businesses operating in the field of digital currencies, which often choose it because of the availability of all the necessary infrastructure to conduct business comfortably within a well-developed banking and financial sector. Nevertheless, the legal framework governing cryptocurrency activities has not yet been developed. From a legal perspective, cryptocurrencies are regarded as 'private money' in the United Kingdom *'Evgheni Florealorea, Elena S. Pustelnik, 2021, pp. 74, 75'*.

In general, the UK is moving towards regulating the sector in a similar way to traditional financial services.

3.5. Switzerland

Switzerland is regarded as a global financial centre that is reluctant to join the EU of its own accord in order to avoid collective pressure on its banking system. Traditional finance is not Switzerland's only strength. According to the Global Innovation Index 2020, the country ranks first in the world for the second consecutive year in terms of innovation development, ahead of Sweden, the United States and the United Kingdom. In early 2020, the Swiss Ministry of Finance began discussing regulations that would establish a legal framework to regulate the blockchain and cryptocurrency industry at national level. Furthermore, although the process had not yet been finalised by August 2021, most cryptocurrency-related activities are subject to general financial market regulations. Previously, the Swiss government had refused to create a separate legal framework to regulate the blockchain and cryptocurrency industry. The authorities decided to amend only certain laws governing

various areas ranging from corporate insolvency to securities trading 'Evgheni Florealorea, Elena S. Pustelnik, 2021, p. 70'.

3.6. United States of America

At first glance, the United States has adopted a more sceptical official stance towards the launch of central bank digital currencies (CBDCs), whilst carefully studying the implications of digital currency. Researchers, both at the Federal Reserve Board of Governors in Washington, DC, and at the regional Federal Reserve Banks, also began to take an interest in digital currencies, publishing research on Bitcoin and related topics as global interest in cryptocurrencies soared in 2013 (Martin Chorzempa, 2021, p. 106).

Furthermore, in early 2016, a working group focused on fintech was looking in particular at distributed ledger technology and digital currencies. At that time, observers outside the government proposed the idea of a 'Fed Coin' issued by the Federal Reserve, but the idea found no traction within the Fed or the US government. The crypto community also harbours certain hopes regarding the new US president (Martin Chorzempa, 2021, p. 106). In particular, the new president has decided to put on hold the implementation of certain executive orders issued by his predecessor, Donald Trump. This has also affected the proposal to collect personal information on contracting parties and customer transactions carried out by cryptocurrency firms, which was to be implemented by the Financial Crimes Enforcement Network (FinCEN). Many representatives of the crypto industry viewed this initiative by the previous president extremely negatively, considering it 'ruinous' for the digital currency sector (Evgheni Florea, 2021, p. 77).

3.7. China

The Asian cryptocurrency market is the largest in the world. According to the crypto-analytics firm Chainalysis, 31 per cent of all cryptocurrency transactions in 2020 (amounting to \$107 billion) took place in East Asia, which is 77 per cent more than in the second-largest region (Western and Northern Europe). China alone accounts for 65 per cent of the world's bitcoin mining capacity. More specifically, China dominates the cryptocurrency market, but this dominance did not last long.

However, a series of government decisions were taken by central government bodies (the People's Bank of China (PBOC), the Cyberspace Administration of China, the Ministry of Industry and Information Technology, the State Administration for Industry and Commerce, and the Banking

Regulatory Commission) issued a joint announcement on the prevention of financial risks associated with initial coin offerings. According to the document, virtual coin offerings are considered unauthorised investment solicitations.

Indeed, the Chinese government effectively banned Initial Coin Offerings (ICOs) in the country in January 2020, when the country's cryptocurrency law came into force to formalise the official creation of China's centralised digital currency (Hui Deng, Robin Hui Huang, Qingran Wu, 2018, pp. 468–490), (Evgheni Florealorea, Elena S. Pustelnik, 2021, pp. 77, 78).

4. The process of money laundering via cryptocurrencies

4.1. Traditional money laundering

Firstly, money laundering has become a real threat at both national and international levels as a result of several factors, notably changes affecting global markets. It is therefore a complex phenomenon in that it risks having adverse effects on the stability of financial institutions and, consequently, undermines economic stability.

Furthermore, the Moroccan Penal Code and Law 43-05 on combating money laundering and the financing of terrorism, as amended and supplemented by Law 12-18, provide a definition of money laundering, specifically in Article 574-1.

According to Eric Vernier (2018), money laundering is defined as a process used to conceal the origin of funds derived from criminal activities (such as drug trafficking, arms trafficking, corruption, etc.); its ultimate aim is to create the impression that illegally acquired funds have a lawful source and to integrate them into the economic sphere. Svetlana Nikolosk (2012) defined money laundering as a procedure for concealing illegal proceeds and for their use or legalisation. Fraud lies at the heart of the entire money laundering process, serving to falsely represent the origin of the assets of the institutions concerned.

According to Dionysios S. Demetis (2018), money laundering is a process that involves concealing funds derived from an illicit source (such as drug trafficking, human trafficking, fraud, extortion and kidnapping for ransom).

In 2021, money laundering was defined by Sergij S. Vitvitskiy et al. and Arjan Premti et al. as a process involving the concealment of funds derived from an illicit source, and that money from an illicit source destabilises economically stable countries.

Consequently, an examination of the extensive literature on money laundering has enabled the authors of this article to propose their own definition:

“Money laundering can be defined as a related economic and financial offence involving the concealment of core offences, cybercrimes and cryptocurrency offences underpinned by blockchain technology, committed by financial criminals in order to give the appearance of legitimacy to these core offences whilst reinvesting part of the illicit proceeds in unlawful projects, the other part into the underground economy, and the remainder into less profitable projects (the visible tip of the iceberg) in order to justify the legitimacy of their money obtained illegally and fraudulently”. (BENNIS Laila, BOUNAR Amine)

Having outlined the various definitions of money laundering and those of the perpetrators, the traditional money laundering process comprises the following three phases:

- The first phase (placement stage – integration stage), where the money is placed into the financial system;
- In the second phase (layering), the money enters the financial system or passes through it via numerous transactions;
- And the third phase (integration), where the money is integrated into the financial system, primarily with the aim of laundering it.

Finally, financial investigators – more specifically cashiers, head cashiers, account managers and compliance analysts – are expected to be imaginative, empathetic and have a keen instinct to prevent and detect money laundering at an early stage, whilst protecting our economy from the harmful effects caused by this financial crime, as criminals and professional money launderers are always seeking to disguise their money-laundering processes through crypto-laundering supported by the blockchain, which we detail below.

4.2. Crypto-money laundering

As with conventional money laundering involving fiat currency, cryptocurrency laundering similarly follows the three stages of money laundering:

Placement: this involves concealing funds from an illicit source whilst converting fiat currencies into cryptocurrencies via an exchange;

Layering: this involves multiplying cross-border transactions between users on the decentralised blockchain platform;

And integration: the movement of assets in a way that allows the money to be reintegrated into the economy and benefits the criminal ‘*Dennis B Desmond, David Lacey, Paul Salmon, 2019, p. 6*’.

Furthermore, to illustrate the practical process of money laundering, we will provide further clarification to help better understand this scheme:

At first glance, cryptocurrencies lend themselves to the placement and layering of illicit funds. During the placement stage, most of the evidence that would enable supervisory authorities and law enforcement agencies to trace the funds back to their source is eliminated. That is to say, when placing illicit funds on a decentralised platform that guarantees anonymity – such as the blockchain – the money launderer could purchase cryptocurrencies via exchanges (whether regulated or unregulated), P2P exchanges and cryptocurrency ATMs (DABs) still do not require identification.

Subsequently, during the layering stage, the money launderer exchanges the cryptocurrencies for several other digital currencies and transfers them between several different addresses in a process known as ‘hops’.

For this process, unregulated exchanges appear to be popular as they generally do not apply anti-money laundering measures or know-your-customer checks.

As for integration, on the one hand, money launderers attempt to acquire tangible or intangible assets on the blockchain platform whilst channelling funds from an illicit source into the legal economy; and on the other hand, the illicit funds that were first placed on the blockchain and transferred repeatedly during the ‘ ’ phase, they will be invested in the legitimate economy whilst converting the convertible digital currency (Bitcoin) into fiat currency such as the dirham.

Money launderers may also use mixers to render the money laundering process undetectable, whilst using anonymous browsers such as Tor or networks that give the impression they are located in another country. Once the process is complete, the coins are pooled again and held as assets or exchanged for fiat currency.

Finally, the interviewees reiterated the importance for money launderers to use only public networks and to remove all incriminating evidence – such as laptops containing digital traces of their illicit activities – from their homes, so that law enforcement agencies are unable to link their cryptocurrencies to their cryptographic addresses in the event of a property search ‘*Fabian Maximilian Johannes Teichmann, Marie-Christin Falker, 2021, pp. 775–788*’.

A – Methods of operation for money laundering using cryptography

In a money-laundering operation, an agent means concealing the origin of funds derived from criminal activity to make them appear, so that they can be used without attracting the attention of the authorities. Laundering money from cryptocurrency is technically straightforward for anyone who is comfortable using the internet (1). Whilst the use of digital tokens requires an extra step in the money-laundering process, it remains widely accessible from a and imposes few constraints from a practical perspective (2).

1 – Example of money laundering using a cryptocurrency

A classic example is that of a drug trafficker in possession a large sum of money from criminal sources, which they wish to invest in the legitimate economy. For example, he wishes to buy a property in a European capital, such as Paris. In order to launder the funds in question, the trafficker buys assets in one or more cryptocurrencies of his choice, via a platform exchange hosted in any country in the world. The purchase is made bank transfer, using an account into which from criminal activities criminal activities. As a precaution, this account does not reveal the trafficker's name but is linked to a shell or a front man. The sum invested in cryptocurrency is then converted back into euros and transferred to the bank account of a French company which shows no identifying features to the previous account. Behind the French company, the main shareholder is the trafficker, either as a natural person or a legal entity, which has itself as its main shareholder the trafficker or a front man. Thus, the mere act of converting a currency into cryptocurrency(ies) and then converting the cryptocurrency assets back into the currency in circulation in the country chosen for the final investment is a highly effective way of concealing the of the funds.

2 – Example of money laundering using a non-monetary

With regard to fundraising via crypto - (Initial Coin Offering or 'ICO'), gaining investor status enables the investor to become a holder of tokens. Once the investment transaction has actually taken place, verification of the source of the funds relates to this successful investment in a project financed by the fundraising. The analysis of suspicious activity reports relating to crypto-assets reveals predominantly cases of fraud – whether straightforward, such as fictitious blockchains, or more subtle, such as price manipulation schemes or Ponzi schemes. This is why TRACFIN concludes that 'in this sense, blockchains do not truly new methods of fraud, but offer a new scope for tried-and-tested methods that have already been tried and tested'?

3 – Regulatory guidelines on virtual currencies:

In order to prevent the misuse of cryptocurrencies by criminals and professional money launderers, several guidelines have been published, including those from the FATF and the European Union, which we will attempt to outline below.

4.3. Financial Action Task Force (FATF) Guidelines

In these guidelines (2014), the FATF identifies convertible virtual currencies, including Bitcoin and Zincoin, as posing a higher risk of money laundering, although this may be a more practical approach in terms of managing anti-money laundering regulations (it is not necessarily the case that non-convertible currencies pose a significantly lower risk).

The FATF's guidelines on virtual currencies are merely standard risk-based AML/CFT warning signs, applied at the points where fiat currency is introduced into the money laundering process. In other words, through virtual currency exchanges.

4.4. The European Union's Fifth Anti-Money Laundering Directive (5MLD) 2018/843

The Fifth Directive 2018/843 of 30 May 2018, amending European Union (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, introduces the following measures to prevent the use of cryptocurrencies for money laundering purposes:

- A legal definition of cryptocurrency can generally be regarded as a digital representation of value that can be stored, transferred and converted into fiat currency;
- Cryptocurrencies and cryptocurrency exchanges are subject to the same AML/CFT regulations. This entails a duty of customer due diligence (CDD) and a 'know your customer' (KYC) obligation;
- The Fifth Directive 2018/843 granted financial intelligence units (FIUs) the power to obtain the addresses and identities of virtual currency owners, thereby combating anonymity;
- The 5MLD also introduces regulations for providers of exchanges, cryptocurrency wallets, and virtual currency exchange offices that convert virtual currency into fiat currency.

5. Conclusion

To answer the first question, *'How do money launderers use blockchain and cryptocurrencies for money laundering purposes?'*, criminals and professional money launderers are exploiting the rapid growth of cryptocurrencies and the anonymity they provide to facilitate the money laundering process via the blockchain, whilst employing the methods of placement, layering and integration (see section 4). As for the second question, *'How can we prevent the use of cryptocurrency blockchains for money laundering purposes?'* The blockchain is a suitable tool for uncovering fraudulent activities, as it records all transactions carried out since its creation and makes it easier for central banks, including the BAM, to prevent and detect illegal activities retrospectively. More specifically, the FBI's shutdown in 2013 of the illegal marketplaces known as 'Silk Road', which had been launched in 2011 *'Sean Foley, Jonathan R. Karlsen, Tālis J. Putniņš, 2019, p. 1806'*.

5.1. Recommendations to public policymakers

To enable Morocco to monitor and control the use of blockchain and cryptocurrencies by money launderers, the following recommendations are put forward to the professional community in order to prevent and detect crypto-money laundering retrospectively:

- Prohibit the informal use of cryptocurrencies by blockchain service providers, currency exchange bureaux and the stock exchange;
- Grant licences through the Moroccan central bank to blockchain service providers and currency exchange bureaux that convert convertible virtual currency into fiat currencies, in this case the dirham;
- Grant a licence to the digital stock exchange by the Moroccan capital markets authority;
- Create a digital currency through the bam;
- Create a centralised and decentralised blockchain platform;
- Work closely with central banks that have created their own digital currencies and other financial intelligence units to prevent the use of cryptocurrencies for money laundering and terrorist financing;

- Assist other countries in creating their own digital currencies so that the economy is not affected by money laundering;
- Identify unlicensed providers, currency exchange bureaux and exchanges through the spontaneous exchange of information between financial intelligence units (fius) at international level;
- Adherence to professional ethics and standards in order to carry out these tasks with complete objectivity;
- Tax cryptocurrencies on entry and exit;
- Central and commercial banks to set up their own blockchain with authorised or semi-private access.

5.3. Outlook

This research, specifically the literature review, has led us to formulate the following outlooks:

- To measure crypto-money laundering by future researchers, using a quantitative method (questionnaire) and examining the evolution of blockchain platform use for the purpose of laundering funds derived from major financial offences;
- To explore this field within the scientific community retrospectively, using a qualitative method (interviews), in order to gain a deeper understanding of the subject of money laundering and its relationship with cryptocurrency;
- To broaden the scope of discussion for the scientific community whilst preparing a paper entitled 'The positive impacts of blockchain on international trade'.
- To examine the conversion of cryptocurrencies into central bank money, and to address the following question: 'How do central banks oversee cryptocurrency transactions?'.

Bibliography

- Alaoui Lalla Latifa, Saghrane Mohamed, Yassine, 2018, 'THE DIGITAL REVOLUTION OF CRYPTOCURRENCY: WHAT FUTURE FOR BITCOIN AND BLOCKCHAIN?', *Public and Non-profit Management Review*, Volume 3, Issue 1, pp. 1–14;
- Amaury-Perrin, 2019, 'BITCOIN AND THE LAW: ISSUES OF CLASSIFICATION', *Public Management and Finance*, Volume 1, Issue 1, pp. 84–93;
- Angela Samantha Maitland Irwin, Adam Turner, (2018), 'Bitcoin transactions: a digital discovery of illicit activity on the blockchain', **Journal of Financial Crime**, Volume 25, Issue 1, pp. 109–130;
- Angela S.M. Irwin, Adam B. Turner, (2018), 'Illicit Bitcoin transactions: challenges in getting to the who, what, when and where', **Journal of Money Laundering Control**, Volume 21, Issue 3, pp. 297–313;
- Anushree Tandon, Puneet Kaur, Matti Mäntymäki, Aman Deep Dhir, (2021), 'Blockchain applications in management: A bibliometric analysis and literature review', *Technological Forecasting and Social Change*, Volume 166, pp. 1–19;
- Bart Custers, Jan-Jaap Oerlemans, Ronald Pool, (2020), 'Laundering the Profits of Ransomware: Money Laundering Methods for Vouchers and Cryptocurrencies', *European Journal of Crime, Criminal Law and Criminal Justice*, Volume 28, Issue 1, pp. 121–152;
- Bianca Linis, Bianca Linis, (2021), 'Digital and Blockchain-based Legal Regimes: An EEA Case Study Based on Innovative Legislation – Comparison of French and Liechtenstein Domestic Regulations', **Financial Law Review**, pp. 1–17;
- Brigitte Unger, Joras Ferwerda, Melissa van den Broek, Ioana Deleanu, (2014), 'Definitions of money laundering in practice', in **The Economic and Legal Effectiveness of the European Union's Anti-Money Laundering Policy**, pp. 87–96;
- Chad Albrecht, Kristopher McKay Duffin, Steven Hawkins, Victor Manuel Morales Rocha, (2019), 'The use of cryptocurrencies in the money laundering process', *Journal of Money Laundering Control*, Volume 22, Issue 2, pp. 210–216;
- Christian Brenig, Rafael Accorsi, Gunter Muller, (2015), 'Economic Analysis of Cryptocurrency-Backed Money Laundering', *Association for Information Systems Electronic Library (AIS eL)*, pp. 1–19;
- Daniel Dupuis, Kimberly Gleason, (2020), 'Money laundering with cryptocurrency: open doors and the regulatory dialectic', *Journal of Financial Crime*, Volume 28, Issue 1, pp. 60–74;
- Dennis B. Desmond, David Lacey, Paul Salmon, (2019), 'Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review', **Journal of Money Laundering Control**, Volume 22, Issue 3, pp. 480–497;
- Dionysios S. Demetis, (2018), 'Fighting money laundering with technology: A case study of Bank X in the UK', **Journal of Decision Support Systems**, pp. 96–107;
- Esman Kurum, (2020), 'RegTech solutions and AML compliance: what future for financial crime?', *Journal of Financial Crime*, pp. 1–19;
- Evgheni Florea, Elena S. Pustelnik, (2021), 'On the regulation of cryptocurrency: international experience', *Supremacy of Law*, pp. 69–83;
- Fabian Maximilian Johannes Teichmann, Marie-Christin Falker, (2021), 'Cryptocurrencies and financial crime: solutions from Liechtenstein', *Journal of Money Laundering Control*, Volume 24, Issue 4, pp. 775–788;
- Fabian Maximilian Johannes Teichmann, Marie-Christin Falker, (2020), 'Money laundering via cryptocurrencies – potential solutions from Liechtenstein', **Journal of Money Laundering Control**, Volume 24, Issue 1, pp. 91–101;
- Hayder Albayati, SukK young Kim, Jae Jeung Rho, (2020), 'Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach', **Technology in Society**, Volume 62, pp. 1–14;
- Hui Deng, Robin Hui Huang, Qingran Wu, (2018), 'The Regulation of Initial Coin Offerings in China:

- Problems, Prognoses and Prospects’, *European Business Organisation Law Review*, Volume 19, Issue 3, pp. 465–502;
- Isaiah ADELEKE, Umaru Mustapha ZUBAIRU, Bilkisu ABUBAKAR, Faiza MAITALA, Yakub MUSTAPHA, Ekanem EDIUKU, (2019), A SYSTEMATIC REVIEW OF CRYPTOCURRENCY SCHOLARSHIP, *International Journal of Commerce and Finance*, Vol. 5, pp. 63–75;
 - Malcolm Campbell-Verduyn, (2018), ‘Bitcoin, crypto-coins, and global anti-money laundering governance’, **Crime, Law and Social Change**, Volume 69, Issue 2, pp. 283–305;
 - Martin Chorzempa, (2021), ‘China, the United States, and central bank digital currencies: how important is it to be first?’, *China Economic Journal*, Vol. 14, No. 1, pp. 102–115;
 - Mohammed Ahmad Naheem, (2019), ‘Exploring the links between AML, digital currencies and blockchain technology’, *Journal of Money Laundering Control*, Volume 22, Issue 3, pp. 515–526;
 - Mohammed Ahmad Naheem, 2018, ‘Regulating virtual currencies – the challenges of applying fiat currency laws to digital technology services’, *Journal of Financial Crime*, Volume 25, Issue 2, pp. 562–575;
 - Mohammed Ahmad Naheem, (2018), ‘Regulating virtual currencies – the challenges of applying fiat currency laws to digital technology services’, **Journal of Financial Crime**, Volume 25, Issue 2, pp. 562–575;
 - Marianne Verdier, 2018, ‘Blockchain and financial intermediation’, *Revue d’économie financière*, Volume 129, Issue 1, pp. 67–87
 - Beaudemoulin, N., Warzée, D. and Bedoin, T. (2017). ‘The challenges of blockchain for the Banque de France and the Autorité de Contrôle Prudentiel et de Résolution (ACPR)’, Volume 5, Issue 3, pp. 29–33
 - Niels Vandezande, 2017, ‘Virtual currencies under EU anti-money laundering law’, **Computer Law & Security Review**, Volume 33, Issue 3, pp. 341–353;
 - Nicola Borri, Kirill Shakhnov, (2019), ‘Regulatory spillovers across cryptocurrency markets’, **Finance Research Letters**, Volume 36, pp. 1–6, DOI:10.1016/j.frl.2019.101333;
 - Patrick Waelbroeck, 2017, ‘The Economic Implications of Blockchain’, *Annales des Mines – Réalités industrielles*, Volume 2017, Issue 3, pp. 1–10;
 - Raffaella Barone, Donato Masciandaro, (2019), ‘Cryptocurrency or Usury? Crime and Alternative Money-Laundering Techniques’, **European Journal of Law and Economics**, Volume 47, Issue 2, pp. 233–254;
 - Sean Foley, Jonathan R Karlsen, Tālis J. Putniņš, (2019), ‘Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?’, *The Review of Financial Studies*, Volume 32, Issue 5, pp. 1798–1853;
 - Sergij S. Vitvitskiy, Oleksandr N. Kurakin, Pavlo S. Pokataev, Oleksii M. Skriabin, Dmytro B. Sanakoiev, (2021), Formation of a new paradigm of anti-money laundering: The experience of Ukraine, *Problems and Perspectives in Management*, Volume 19, Issue 1, pp. 354–363;
 - Svetlana Nikolosk, Ivica Simonovski, ‘The role of banks as entities in the system for the prevention of money laundering in Macedonia’, (2012), **Procedia – Social and Behavioural Sciences**, pp. 453–459;
 - Solène Clément, Juliette Lelieur, 2021, ‘Anti-money laundering compliance in relation to crypto-assets’, *Journal of Criminology and Comparative Criminal Law*, 1(1), 15–24
 - Tadas Limba, Kestutis Driaunys, Andris Stankevicius, (2020), ‘CRYPTOCURRENCY AND NATIONAL SECURITY: PECULIARITIES OF INTERACTION’, **Transformations in Business and Economics**, Volume 19, pp. 138–158;
 - Victor Dostov, Pavel Shust, (2014), ‘Cryptocurrencies: an unconventional challenge to AML/CFT regulators?’, *Journal of Financial Crime*, Volume 21, Issue 3, pp. 249–263;
 - Zakaria Bziker, (2021), The status of cryptocurrency in Morocco, *Research in Globalisation*, Issue 3, pp. doi:1–8.

- Reports:
- Guidelines on the risk-based approach to virtual assets and service providers dealing with virtual assets, 2019;
- European Union Directive 2018/8435MLD;
- FATF Report: Virtual Currencies – Key Definitions and Potential AML/CFT Risks, June 2014.
- Books:
- Xavier Vamparys, 2018, Blockchain in Finance: Legal Framework and Practical Applications, Edition RB, France, Paris, 165 pages;
- Didier Geiben, Olivier Jeain-Marie, Thiboult Verbiest, Jean François Vilotte, 2016, *Bitcoin and Blockchain: Towards a New Paradigm of Digital Trust? *, Edition RB, France, Paris, 122 pages;
- Eric VERNIER, 2017, “Money Laundering Techniques and Countermeasures”, fourth edition, DUNOP, Paris, 295 pages;
- Philippe Herlin, 2021, Bitcoin: Understanding and Investing – A Practical Guide to Cryptocurrencies: Bitcoin, Ethereum, Blockchain, Decentralised Finance, NFTs, etc., Eyrollez, France, Paris, 203 pages;
- Stéphane PREVOST, Erwan ROYER, 2020, *Blockchain*, DALLOZ, France, Paris, 225 pages;
- Philippe Herlin, 2018, I’m Buying Bitcoin: A Practical Guide to Investing in New Assets – Bitcoin, Ethereum, Tokens, ICOs, Eyrollez, France, Paris, 143 pages;
- Jean Guillaume DUMAS, Pascal LAFOURCADE, Ariane TICHIT and Sébastien VARRETTE, 2019, *Blockchains in 50 Questions: Understanding How This Innovative Technology Works and the Issues at Stake*, DUNOP, France, Paris, 279 pages.