Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

October 2018

National Risk Assessment (NRA):

Risk of money laundering and terrorist financing posed by crypto assets and crowdfunding

Report of the interdepartemental coordinating group on combating money laundering and the financing of terrorism (CGMF)

Contents

Executive summary

To date, the Swiss authorities have not identified a single case of terrorist financing using crypto assets or online crowdfunding and have recorded only a few cases of money laundering using these new technologies. Consequently, the real risk of money laundering and terrorist financing associated with them cannot be precisely assessed. Nevertheless, this report concludes that the risks posed by these technologies and the vulnerabilities of Switzerland in this area are considerable, with not only Switzerland being affected, but all countries.

The threat posed by crypto assets results from the anonymity of token transactions, particularly concerning the beneficial owner of the assets, and from the fact that a large proportion of these transactions is carried out directly without a financial intermediary and they are thus beyond any control. The threat is reflected both in the criminal exploitation of design errors in cryptocurrencies and in investor fraud, particularly in the case of ICOs and the use of cryptocurrencies for ransomware payments. However, the use of cryptocurrencies poses a threat also in other crime patterns: terrorist financing, laundering of funds from the sale of illegal services and products, phishing scams or drug trafficking, especially by criminal organisations. Cryptocurrencies are particularly well suited for money laundering because of their anonymity.

Just like other countries, Switzerland is vulnerable to this danger because it is complicated for both financial intermediaries and prosecution authorities to establish the identity of the beneficial owner of certain assets. In most cases, the technology underlying crypto assets is responsible for the fact that this identity cannot be established. Only when cryptocurrencies are bought or sold for fiat money can the identity of the beneficial owners of the assets involved be established. But even this does not provide comprehensive fraud protection for the online exchange offices that carry out such transactions. They have no means of verifying the identity of the beneficial owners of the wallets to which they credit assets on behalf of their customers. Moreover, it is extremely difficult to prove the criminal origin of the assets involved in a crypto transaction.

This new technology is a major challenge for prosecution authorities too. Not only is it difficult to identify the beneficial owners of crypto assets and to detect the criminal background to a transaction involving such assets, but it is also technically impossible to confiscate the assets deposited in a wallet without having the corresponding private key. Moreover, because crypto transactions are usually cross-border, international police cooperation or international mutual assistance requests are necessary in order to punish the associated white-collar crime. Consequently, prosecution authorities are often taken by surprise by the speed and mobility of crypto transactions, and there are often problems in terms of the competent jurisdiction.

However, international police administrative assistance and judicial mutual assistance are currently the most efficient instrument for combating money laundering and terrorist financing using crypto assets. They have been responsible for the biggest successes in suppressing white-collar crime in connection with cryptocurrencies. This also shows that an answer to this type of transnational threat must be worked out at the international level.

In this respect, Switzerland's commitment within the FATF to greater harmonisation of national regulations to combat money laundering and terrorist financing using crypto assets is an appropriate response. It is supplemented by efforts to train prosecution authorities in the field of cybercrime and by the creation in summer 2018 of a national platform for judicial and police cooperation, the Cyberboard, which specialises in this type of white-collar crime.

Moreover, the AMLA already applies in Switzerland to a particularly wide range of services relating to trading and transactions involving crypto assets, although certain clarifications on the scope of this law are currently being examined.[1]

The report concludes that, thanks to these various measures, Switzerland has developed the best possible regulatory mechanism to combat the significant threat posed by crypto assets, even if this does not eliminate all vulnerabilities, which are likewise significant and which can be considerably reduced only by means of an international solution.

In the case of crowdfunding, the greatest risk is terrorist financing, although not a single such case has yet been recorded in Switzerland. The danger with this new technology for raising capital arises from the anonymity of the donors, but also from the fact that certain online crowdfunding platforms are not subject to the AMLA. In order to reduce this risk, the report recommends examining whether it would be appropriate to include such platforms in the Ordinance of 11 November 2015 on Combating Money Laundering and Terrorist Financing (OMLTF, SR 955.01).

[1] See recommendations in the *Federal Council report on legal framework for distributed ledger technology and blockchain in Switzerland*, 14 December 2018, https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf.

List of abbreviations used

AMLA: Federal Act of 10 October 1997 on Combating Money Laundering and the Financing of Terrorism in the Financial Sector

CCJPD: Conference of Cantonal Justice and Police Directors

CCPCS: Conference of Cantonal Police Commanders of Switzerland

CGMF: Interdepartmental coordinating group on combating money laundering and the financing of terrorism

CSPP: Conference of Swiss Public Prosecutors

DLT: Distributed ledger technology

FATF: Financial Action Task Force

FGB: Federal Gaming Board

FINMA: Swiss Financial Market Supervisory Authority

FIS: Federal Intelligence Service

FITSU: Federal IT Steering Unit

FOJ: Federal Office of Justice

ICO: Initial coin offering

MELANI: Reporting and Analysis Centre for Information Assurance

MROS: Money Laundering Reporting Office Switzerland

NRA: National Risk Assessment

OAG: Office of the Attorney General of Switzerland

SCP: Swiss Crime Prevention

SIF: State Secretariat for International Finance

SSN: Swiss Security Network

Index

Asymmetric encryption: Asymmetric encryption is an encryption technique that distinguishes between public and private keys, the latter of which actually allow the data transmitted to be decrypted. This

technique is used in the crypto area to carry out secure transactions between two wallets. Each wallet thus has both a public key and a private key. In order to carry out a transaction for a wallet, the person commissioning it must have the public key to enable the crypto assets to be transferred to a particular wallet and not to another. The private key, which only the owner of this wallet has, is the actual access code with which the owner can access the credited assets. However, certain cryptocurrencies also use other encryption techniques to secure transactions between two wallets.

Bitcoin: Bitcoin is the oldest and most popular cryptocurrency, which was created in 2009 in response to the financial crisis.

Blockchain: Blockchain is a computer technology for storing and transferring data without a central control body. In a broader sense, this term also refers to the database containing the history of all transactions carried out with this technology. Blockchain is used mainly in the area of crypto assets. It is the technical basis for numerous cryptocurrencies, including bitcoin and ether, where it enables the readability of all transactions. To record on the blockchain, several transactions are chronologically grouped in a block, which is then appended to the previous block after the transactions have been validated by miners. These check whether the individual who commissioned the transaction actually has the assets or data he wants to transmit. Such validation is performed by solving a mathematical problem. After the transactions are recorded on the blockchain, they can be deleted only by a person or group of people with more than 51% of the processing power required to validate transactions throughout the blockchain.

Crypto asset: A crypto asset is commonly understood to be a digital representation of a value that can be digitally traded on a blockchain and can be used for the purpose of payment (payment function), use (usage function) or investment (investment function).

Cryptocurrency: Synonym for "virtual currency". See below.

Darknet: The term darknet refers to networks on the internet that use access protocols that allow their users to remain anonymous, especially by hiding the IP addresses of connections. Darknets are located on the deep web, i.e. those parts of the internet to which conventional browsers have no access and of which there are several. The most famous of these networks is TOR (the onion router), for which there are special browsers. Anonymous networks host legal websites which are used in particular for the exchange of confidential data, but also numerous websites for the sale of illegal products and services. These so-called dark markets mainly offer drugs, child pornography, weapons or stolen credit cards. Content that exists on darknets is called darkweb.

DLT (distributed ledger technology): DLT is generally understood to mean technologies that allow individual participants (nodes) within a system to propose operations in a secure manner, validate them and store them in a synchronised data set (ledger) that is distributed across all nodes in the system.

Ether: Ether or ethereum, introduced in 2015, is the second most important cryptocurrency after bitcoin.

Fiat money: Fiat money is issued by a state whose central bank sets and controls the legal rate.

ICO: ICOs are a way of raising capital. With an ICO, investors transfer funds (usually in the form of cryptocurrencies) to an ICO organiser. In return, they receive blockchain-based "coins" or "tokens", which are created either on a newly developed blockchain or on an existing blockchain by means of a so-called smart contract and stored in a decentralised manner.

Miner: Miners are responsible for the validation of transactions. Miners (i.e. validating nodes) check whether the individual who commissions a transaction actually has the assets or data he wants to transmit. Such validation is performed by solving mathematical problems. They combine transactions into a block and send this to the network for verification. The nodes accept a block only if the transactions

it contains are valid. Miners are compensated with newly created bitcoins ("mining") and transaction fees.

Public key/private key: Public keys (or addresses) correspond to identities of cryptocurrency users. A cryptocurrency user can send a message (or transaction) from his address by signing it with his private key. The private key is thus the signature key and the public key the verification key. The private key must be kept secret; the verification key is typically made public.

Smart contract: Smart contracts are computer protocols that automatically execute the terms of a contract based on algorithms that determine when which decision has to be made. Smart contracts were originally developed by the Ethereum Foundation, whose cryptocurrency ether was the first to enable the use of such protocols. They allow the execution of contracts and the monitoring of transactions on the blockchain they generate, while at the same time suppressing the risks of arbitrariness associated with human action – the principle is that one cannot deviate from the smart contract protocol, which is absolutely rational and fair to all and thus becomes the law of those who use this technology ("The code is the law").

Token: In the context of a blockchain, a token is a unit that either contains an intrinsic value or represents another asset or a usage function. Blockchain-based tokens are usually fungible and can be exchanged between network participants.

Virtual currency: A virtual currency is an electronic representation of a value that is tradable online and can be used as a means of payment for real goods and services. It has its own denomination, but is usually not accepted as legal tender. A virtual currency is merely a digital code and has no physical counterpart, e.g. in the form of coins or notes.

Wallet: A wallet is a piece of software that uses an interface to manage cryptographic tokens.

Introduction

The Federal Council acknowledged the first report on the national evaluation of the risks of money laundering and terrorist financing in Switzerland in June 2015. The national risk assessment (NRA) report is the first cross-sector assessment of money laundering and terrorist financing risks in Switzerland. It shows that Switzerland is not spared financial crime and that the proceeds of crime, most of which is committed abroad, are laundered in Switzerland too. With the publication of the NRA, the Federal Council is implementing the revised recommendations 1 and 2 of the Financial Action Task Force (FATF). The recommendations of the intergovernmental organisation encourage countries to introduce a mechanism to combat money laundering and terrorist financing efficiently. The NRA report is part of this mechanism insofar as it aims to identify money laundering and terrorist financing risks in Switzerland, to initiate targeted countermeasures and to review their efficiency at regular intervals (identify and assess their money laundering and terrorist financing risk on an ongoing basis).[2] The publication of the NRA report does not mark the end of the national risk assessment process. The NRA is a continuous process. In order to comply with the FATF recommendations in the longer term and to adapt the effectiveness of Switzerland's anti-money laundering and terrorist financing system to the new threats, further risk analyses will be prepared.

This report on money laundering and terrorist financing risk in connection with two of the most important forms of fintech application – crypto assets and crowdfunding – is to be understood as one of these further risk analyses of a sectoral nature. It first deals with the risk associated with crypto assets and then, in a somewhat shorter form, with the risk associated with online crowdfunding.

Crypto assets are any form of virtual asset stored on an electronic medium that allows a community of users who accept them as means of payment to execute transactions in such assets without using a legal currency. Although the term "crypto asset" covers a broader range than "virtual currency" or "cryptocurrency" (see above), they are used synonymously in this report.

At the end of 2017, the spectacular surge of the bitcoin exchange rate drew the attention of the public and the media to crypto assets. The bitcoin cryptocurrency, developed in response to the global financial crisis of 2008, is the oldest of these crypto assets that can bypass the traditional banking system by choosing an anonymous, fully decentralised and thus unregulated transaction form that is processed over the internet. Very early on, the lack of control and the anonymity of bitcoins led the authorities to address the potential risks of fraud, money laundering and terrorist financing associated with them. The Financial Action Task Force (FATF) drew its members' attention to these dangers as early as 2014 and 2015, and drew up initial guidance for the development of a risk-based approach to assessing the dangers of money laundering or terrorist financing associated with cryptocurrencies.[3] Several parliamentary procedural requests and postulates on this subject have been submitted in Switzerland since 2013, prompting the Federal Council to publish a report on virtual currencies[4] in 2014. It concluded that the risk was still low and that no special measures were required in the immediate future. Since then, however, new economic uses of crypto assets have been added, the number of such currencies has increased – currently there are more than 2,000 – and the technologies underlying these currencies have evolved. These factors, as well as the recent public enthusiasm for virtual currencies triggered by the surge in the bitcoin exchange rate, have prompted national and international bodies to examine whether a reassessment of the associated money laundering or even terrorist financing risks is necessary. The FATF is planning to draw up an in-depth strategy on this subject[5], several countries,

---

2 FATF, *National Money Laundering and Terrorist Financing Risk Assessment*, 2013, p. 6, http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

3 FATF, *Virtual currencies. Key definitions and potential AML/CFT risks*, June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf; id, *Virtual currencies. Guidance for a risk-based approach*, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

4 *Federal Council report of 25 June 2014 on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates*, https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf.

5 FATF, *FATF Fintech & RegTech Initiative*, http://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc(fatf_releasedate).

and the European Union in particular, are in the process of amending their legislation as regards the risks[6] associated with cryptocurrencies, and the number of reports on this subject drawn up by various authorities and organisations is constantly increasing.[7]

Such a reassessment is particularly important for Switzerland, which positions itself as a crypto-friendly state. The canton of Zug, for example, attracts many companies in this sector and is often referred to as the Swiss "Crypto Valley", while the canton of Geneva, which wants to emulate it, also encourages the establishment of such companies on its territory and the development of the crypto sector in its banks. The innovative potential of crypto assets and their impact on civil and financial market law are the subject of a separate report by the Federal Council[8], which this report seeks to supplement with an analysis of the money laundering and terrorist financing risks associated with crypto assets.

In contrast to other money laundering and terrorist financing risks, those associated with cryptocurrencies are novel and there are not yet many sources that allow an assessment. In particular, the Money Laundering Reporting Office Switzerland (MROS) has received only a few suspicious activity reports and no reliable statistical information can yet be derived from them. Although the suspicious activity reports received by MROS were used for analysis as far as possible, it was still necessary to use other sources and take a qualitative rather than a quantitative approach. The specialist literature on the subject together with press articles and reports from foreign authorities thus form the basis for this report, which was supplemented by consultations with several Swiss police and judicial authorities and the private sector. We would like to take this opportunity to thank them for their availability.

The first part of this report is devoted to the definition of terms and concepts in the field of crypto assets and their technology, and is deliberately kept short. For more information, please refer to the Federal Council's report which will be published by the end of 2018 and will cover this aspect in more detail.[9] The second chapter deals with the description of the most important services used in token transactions and their legal qualifications. Specifically, initial coin offerings (ICOs) are presented and defined. Their number has multiplied in Switzerland in just over a year, making them a particular problem for legislators and the business sector. The actual risk assessment follows in the third chapter. It is based on the experience of the competent Swiss authorities and trends from abroad, and is divided into a review of the threats and a presentation of the vulnerabilities. It is stressed, however, that neither one nor the other is specific to Switzerland, but must be regarded as global. A risk assessment is carried out at the end of this chapter. Then, the fourth chapter lists the factors that make it possible to reduce the money laundering and terrorist financing risks associated with cryptocurrencies. The most important of these factors is having the various companies active in the token business comprehensively subject to the Anti-Money Laundering Act (AMLA; SR 955.0). Nevertheless, other regulatory and operational instruments are likewise taken into account.

Finally, the fifth chapter of the report deals with online crowdfunding and the associated money laundering and terrorist financing risks. This area, which, like crypto assets, is linked to the development of fintech, is also at the centre of the national and international political agenda, as several cases of terrorist financing using such fundraising procedures have been detected abroad.[10] It would seem sensible to analyse whether Switzerland is equipped to deal with this threat, which was pointed out by the FATF already in 2015.[11]

---

6 http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0178+0+DOC+PDF+V0//DE.

7 EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017; FANUSIE YAYA and ROBINSON TOM, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance and ELLIPTIC, 12 January 2018; European Parliament, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, May 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

8 *Federal Council report on legal framework for distributed ledger technology and blockchain in Switzerland*, 14 December 2018, https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf.

9 *Ibid*.

10 See for example: TRACFIN, *Tendances et analyse de risques de blanchiment de capitaux et de financement du terrorisme en 2015*, 2015, p. 64 et seq., https://www.economie.gouv.fr/tracfin/tendances-et-analyse-des-risques-en-2015.

11 FATF, *Emerging Terrorist Financing Risks*, October 2015, p. 6 and p. 31 et seq., http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf.

1. Virtual currencies

1.1. Definition

A virtual currency is an electronic representation of a value that is tradable online and can be used as a means of payment for real goods and services. It has its own denomination, but is usually not accepted as legal tender. A virtual currency is merely digital code and has no physical counterpart, e.g. in the form of coins or notes.[12] The term "virtual currencies" is used synonymously for "cryptocurrencies" below.

For this risk analysis, the money laundering and terrorist financing risk of decentralised virtual currencies and thus of cryptocurrencies is analysed, and this term is also used below.

1.2. Developments since 2014

The Federal Council published the report on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates in 2014.[13] Bitcoin was already the largest virtual currency at the time. On 5 January 2014, a bitcoin[14] was worth less than USD 1,000 and the market capitalisation was USD 10.5 billion (rounded). On 9 October 2018, the value of a bitcoin was USD 6,644 and the market capitalisation was USD 115 billion (rounded), corresponding to a market share of 52% with 2,047 cryptocurrencies.[15] Both the value of a bitcoin and the total value of the bitcoins in circulation have soared. Many other virtual currencies, e.g. ripple and litecoin, have also increased massively in value relative to 2014. This makes virtual currencies attractive for both investors and criminals.

1.3. Typologies of virtual currencies

Virtual currencies can basically be categorised according to two characteristics: exchangeable vs. non-exchangeable virtual currencies, and centralised vs. decentralised virtual currencies.

1.3.1. Exchangeable vs. non-exchangeable virtual currencies

Exchangeable virtual currencies can be exchanged into official currencies, e.g. bitcoin, ether, etc. Non-exchangeable virtual currencies can only be used within a closed system to pay for virtual or real goods and cannot be exchanged for official currencies, e.g. Amazon coin, which can only be used for Amazon's website and has the function of a voucher.[16]

1.3.2. Centralised vs. decentralised virtual currencies

All non-exchangeable virtual currencies are centralised currencies. Exchangeable virtual currencies can be centralised or decentralised. Centralised virtual currencies have a central administrator who issues the currency, regulates usage and controls the system. The administrator can also take the currency out of circulation. Examples of centralised virtual currencies include World of Warcraft gold and Second Life Linden dollars. Decentralised currencies are always exchangeable virtual currencies and do not have a central administrator who can control the system. Currencies of this type are based on a network

---

12 See also the definition in the Federal Council report of 25 June 2014 on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates, p. 7, https://www.news.admin.ch/NSBSubscriber/message/attachments/35355.pdf.

13 SANSONETTI RICCARDO, "Bitcoin: Virtuelle Währungen mit Chancen und Risiken", in Die Volkswirtschaft, 9-2014, pp. 44-46.

14 See https://www.coindesk.com/bitcoin-price-2014-year-review/ (last visited on 14.05.2018).

15 See https://coinmarketcap.com (last visited on 09.10.2018).

16 SERAINA GRÜNEWALD, "Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen", in: Rolf H. Weber et al.(ed.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, ZIK vol. 61, Zurich/Basel/Geneva 2015, p. 95.

of computers solving a mathematical calculation and are also called cryptocurrencies. Examples include bitcoin, ripple and litecoin.[17]

1.3.3. How the technology works

Something new was created with the implementation of bitcoin at the start of 2009: bitcoin enables joint accounting with participants who do not trust each other, do not know each other and do not know how many other participants are in the system. The technology that makes this possible is called blockchain and it allows a new data management model. The term blockchain refers to the fact that transactions are grouped into blocks and confirmed together. The confirmation in turn links the block with the new transactions to a chain of previous blocks and thus incrementally builds up a transaction history.

The variety of systems developed in practice goes beyond the term blockchain, which is why the broader term distributed ledger technology (DLT) was introduced.

The decentralised nature of distributed ledger technology enables transactions to be processed directly between the parties without intermediaries such as banks or payment service providers (peer-to-peer). The transactions are stored in a decentralised register. The participants thus have to agree on (1) the valid transactions and (2) a valid register (distributed consensus) for the organisation and storage of the data structure.

In the case of transactions, validity is generally determined by the participants agreeing which transactions are "genuine" and are to be added to the valid register. With today's DLT models, the voting power of the voting participants can be determined mainly in two ways, whereby a mixture of systems can also occur:[18]

- *Proof of work (mining)*: Some systems use the proof-of-work mechanism for consensus building when creating blocks. Cryptographic functions are executed until the result has certain properties. We speak of a valid proof of work if the property sought is fulfilled. The cryptographic function makes it impossible to check the validity of the proof of work without actually executing the function. But checking its validity is trivial with a valid input. This forces the participant to guess a valid input with repeated testing (work). Bitcoin uses a one-way function (specifically a SHA-256 hash function) until the output has a certain prefix (specifically, several 0 digits).

- *Proof of stake*: A participant is selected by an algorithm to validate the transaction. Participants with a high credit balance and/or a long holding period are preferred. With this concept, tokens are usually created only at the beginning and their number is not subsequently increased. Compensation is thus via transaction fees.

Since the register, i.e. the data structure, is decentralised, a copy is stored for each or several participants and these are continuously compared with each other according to the protocol rules.[19] The version which is in turn confirmed as true by the majority of the data structure keepers, the so-called full (blockchain) nodes[20], is considered true.[21]

---

[17] FATF Report – Virtual Currencies, Key Definitions and Potential AML/CFT Risks, June 2014, p. 5, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

[18] LUZIUS MEISSER, Kryptowährungen: Geschichte, Funktionsweise, Potential, in: Rolf H. Weber et al. (ed.), Rechtliche Herausforderung durch webbasierte und mobile Zahlungssysteme, ZIK vol. 61, Zurich/Basel/Geneva 2015, 82 et seq.

[19] LUZIUS MEISSER, loc. cit., 83 et seq.

[20] Keepers of the blockchain protocol (including the "register" of transactions). The full blockchain nodes constantly compare the blockchain protocol with each other and thus ensure that no false transactions can take place. In addition, transactions take place via the full blockchain nodes.

[21] MARTIN HESS/PATRICK SPIELMANN, Cryptocurrencies, Blockchain. Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht, in: Reutter, Thomas U. / Werlen, Thomas (Hrsg.): Kapitalmarkt – Recht und Transaktionen XII. Zurich: Schulthess 2017, p. 154.

2. Cryptocurrencies in practice

2.1 Cryptocurrencies as a funding instrument

There has been a significant increase in initial coin offerings (ICOs) carried out or offered in Switzerland since 2017. There are currently no definitions for ICOs established in law or doctrine, but this can generally be understood as the creation of a token and its first offer to the public.[22] The ICO organiser generally uses the ICO to disseminate the tokens and raise capital for business purposes; this is carried out exclusively via distributed ledger or blockchain technology. With an ICO, the investors participate in a blockchain-based project of the ICO organiser. The investors transfer funds to the ICO organiser and receive blockchain-based tokens in return. These are created either on a newly developed blockchain or on an existing blockchain by means of a so-called smart contract and stored in a decentralised manner. This is ultimately a form of crowdfunding without an intermediate platform (see section 2 below). "Token sale" and "token generating event" are also used as synonyms. Participants in an ICO often invest in project facilities or business ideas and hope for successful project implementation. As a result, ICOs are very similar to traditional financing rounds or private placements. The financial resources received via the issued tokens can generally be of an equity or debt nature. Generally speaking, however, the token holders should become neither shareholders nor creditors of the company. In these cases, elaborate documentation (e.g. the obligation to publish a prospectus) can often be avoided during the issue.[23] Transparency requirements for legal entities are likewise circumvented. In cases where the tokens are issued with the intention of creating cryptographic shares, fundamental corporate law questions arise as to the extent to which a shareholder position can be established in this way.

ICOs are usually designed in such a way that investors can acquire the newly issued token by transferring ethers (ETH) or bitcoins (BTC) to a blockchain address (e.g. a smart contract) belonging to the ICO organiser. In some cases, ICO organisers also accept payments in fiat money. In order to participate in an ICO, participants regularly have to register in advance (partly with identification) on the ICO organiser's website, although there are still virtually no uniform standards with regard to customer onboarding.

The ICO may be preceded by a private placement of the tokens at preferential conditions with selected investors in the form of a pre-sale. In the context of ICOs, tokens are sometimes not issued in the case of pre-financing and pre-sales; instead only (conditional)[24] claims to a token still to be created are distributed.

The following chart[25] illustrates the significant increase in ICO projects globally:

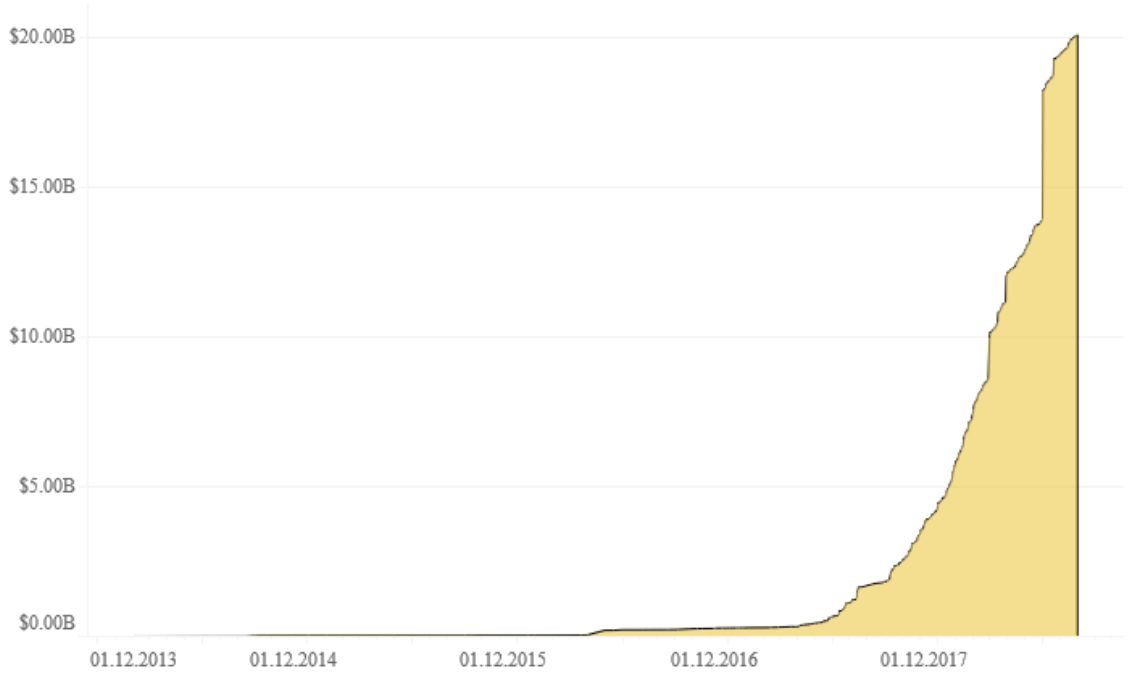
---

22 ICOs often take place in various phases. Public ICOs aimed at the general public are usually preceded by so-called pre-sales or private sales, in which only a limited number of participants can participate.

23 An exception to this is the requirement to draw up a bond prospectus when issuing bonds in accordance with Article 1156 of the Swiss Code of Obligations.

24 For example, the "terms of token sale" stipulate that there is no entitlement to corresponding tokens if the project does not materialise.

25 The chart was taken from https://www.coindesk.com/ico-tracker/ ("All-time Cumulative ICO Funding"; last visited on 27 July 2018).



Uniform data on the number of ICOs worldwide and the volumes collected cannot be accurately determined. According to a study by PwC Switzerland, 450 ICOs took place worldwide last year, bringing in investments of around CHF 4.6 billion. The volumes collected were almost twenty times more than in 2016. In Switzerland alone, the 70 ICOs carried out totalled CHF 1 billion.[26] These figures illustrate the significance of the Swiss financial centre in the ICO market. Switzerland is a global centre for ICOs. Especially in the case of ICOs that took place in 2017, the foundation form was often used (see also table below). In 2018, however, there was an increase in the ICOs organised by companies limited by shares or limited liability companies (GmbHs). Against the background of the surge in ICOs in Switzerland, FINMA published guidelines[27] on how it applies existing financial market legislation to classify ICOs in terms of supervisory law.

The concrete structure of ICOs differs greatly in individual cases from a technical, functional and economic point of view, with the result that a generally applicable classification is not possible. Some ICOs, for example, see the creation of tokens that are intended to assume the functions of money and are thus suitable for qualifying as a means of payment within the meaning of the Anti-Money Laundering Act (AMLA). In this context, it is planned that the Federal Council's blockchain/ICO working group[28] will deal in greater detail with the various constellations and legal implications of the different token models.

Means of payment are instruments that enable third parties to transfer assets.[29] A uniform definition of the term does not exist in Swiss law. Nevertheless, the issuance of means of payment constitutes an activity subject to the AMLA. The act lists credit cards and travellers cheques as examples of means of payment (Art. 2 para. 3 lit. b of the AMLA). The list of examples shows that a broad definition of means of payment can be assumed for regulatory purposes.

A token issued as part of an ICO qualifies as a means of payment within the meaning of the Anti-Money Laundering Act if it is actually to be used or is intended to be used by the issuer as a means of payment

---

26 See https://www.srf.ch/news/wirtschaft/finanzierung-mit-digitalgeld-millionen-generieren-mit-bitcoin-und-co; with reference to the PwC study (last visited on 27 March 2018). For example, USD 228,590,404 was collected with the TEZOS ICO (ended on 14 July 2017).

27 See https://www.finma.ch/de/news/2018/02/20180216-mm-ico-wegleitung/ (last visited on 29 March 2018).

28 Federal Council, *Federal Council report of 14 December 2018 on legal framework for distributed ledger technology and blockchain in Switzerland*, https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf.

29 See FINMA Circular 2011/1 "Financial Intermediation under the Anti-Money Laundering Act", para. 55.

for the purchase of goods or services. Unlike coins or banknotes and sight deposits with the SNB, cryptocurrencies are not accepted as legal tender and are not denominated in Swiss francs (e.g. BTC, ETH). Unlike e-money, cryptocurrencies are not necessarily a claim against the issuer. They exist only as digital code and there is no material counterpart in the form of coins or notes. Some tokens evolve to become a cryptocurrency only over time as soon as they are accepted as a means of payment. However, a cryptocurrency may exist already at the time of the ICO if the creation of a means of payment is intended.

Payment processing typically follows the following (somewhat simplified) pattern:

(1) The debtor enters the recipient address of the creditor and the number of tokens to be sent either directly via his account or via an account with a trading platform (see letter d below).

(2) The information is sent to the blockchain network.

(3) Based on the consensus mechanism in the respective protocol, the blockchain network confirms the validity of the transaction and the credit to the creditor's address.

Despite huge price fluctuations, an increasing number of traders (especially in online trading and service providers in the IT field) accept cryptocurrencies as a means of payment.[30]

According to Coinmarketcap, there are currently 2,094 cryptocurrencies worldwide.[31] Among the top 40 or so cryptocurrencies with a market capitalisation of over USD 300 million (as of 08.11.2018), the following companies in particular are connected to Switzerland:

Ranking	***Name***	***Market cap. (USD bn)***	***Swiss connection***
# 2	Ethereum (ETH)	21.7	Ethereum Foundation, Zug
# 8	Cardano (ADA)	1.9	Cardano Foundation, Zug
# 18	Tezos (XTZ)	0.78	Tezos Foundation, Zug
# 29	Lisk (LSK)	0.3	Lisk Foundation, Zug
# 37	Icon (ICX)	0.2	Icon Foundation, Zug

2.2 Wallet providers

A cryptographic key pair is required to carry out transactions via DLT. This consists of a public key (PUK), which serves as an address (a kind of account number), and a private key (PIK), which gives full access to the address (similar to a PIN). The PIK is the decisive element for initiating a transaction. Only with this can a transaction be validly signed and thus triggered. If the PIK is lost, the power of disposal over the cryptocurrency is also lost. Accordingly, it is important to store the PIK safely. This can be done

[30] The most widespread is probably still bitcoin. Examples in Switzerland include the residents' register office of the city of Zug and the Zug commercial register office. See also https://bitcoin-stores.ch/ (last visited on 29 March 2018); this site has a Swiss bitcoin shop directory and bitcoin e-shopping business directory, and lists only businesses and online shops in Switzerland that accept bitcoins as a means of payment.

[31] See https://coinmarketcap.com/all/views/all/ (last visited on 27 November 2018).

with a wallet. Generally speaking, this can be understood as software that allows cryptographic tokens to be managed via an interface.

Wallets can be designed differently by corresponding wallet app developers: a distinction can generally be made between decentralised wallet applications and custody wallet providers. The former are typically decentralised open source projects that cannot necessarily be assigned to individual companies. The corresponding software applications are often provided free of charge as freeware (e.g. Mycelium, Electrum, etc.; also referred to as non-custodian wallets, private wallets or self-hosted wallets). Such wallets allow users to manage their own key pairs (to be distinguished from so-called crypto custodians or custody wallet providers), i.e. the developer usually has no knowledge or access to the app users' generated key pairs. In contrast, custody wallet providers often maintain a lasting customer relationship and for this purpose also manage the corresponding key pairs (i.e. particularly customers' private keys).

Based on a 2017 study by the University of Cambridge[32], the following rough estimate can be made concerning the wallet provider market:

- It is estimated that the number of wallets rose from 8.2 million in 2013 to almost 35 million in 2016.
- An estimated 5.8 to 11.5 million wallets were active last year.
- Approximately 80% of the wallet providers are domiciled either in North America or Europe, whereas only 60% of the users also come from these regions.
- About 73% of the wallets do not control PIKs (private wallets), 15% are custodian wallets, and the user can determine access to the PIK in 12% of wallets.
- Just under 40% of wallets support multiple cryptocurrencies.
- Mobile wallet apps are the most common (65%), followed by desktop wallets (42%) and internet wallets (38%).
- The distinction between wallets and trading platforms is becoming increasingly blurred. Approximately half of the wallets allegedly have an exchange functionality too (see section 4.1. below).
- Approximately 24% of wallet providers hold a state licence. All of these wallet providers support the exchange of cryptocurrency vs. fiat money. However, only 75% of the wallet providers who enable the exchange of cryptocurrency vs. fiat money hold a state licence.

On 30 May 2018, the European Parliament and the Council of the EU adopted an amendment to the 4th Anti-Money Laundering Directive.[33] Among other things, it now provides for the scope of the directive to be extended to platforms for exchanging virtual currencies and to custodian wallet providers in order to make it easier to identify users of virtual currencies.

The FATF follows the topics of virtual currencies and DLT within the framework of the "Risk, Trends and Methods Group" (RTMG) and develops recommendations. In a Virtual Currencies Update (October 2017) by RTMG, the group addressed the role of hosted wallet providers, which also allow technically illiterate users to easily transfer virtual currencies, as well as ICOs. These topics are referred to as future challenges and topics for discussion.

---

[32] The estimates are based on the 2017 Global Cryptocurrency Benchmarking Study by Garrick Hileman & Michel Rauchs, Cambridge Centre for Alternative Finance, University of Cambridge, Judge Business School (last visited on 28 March 2018).

[33] See Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, OJ L 156 of 19.06.2018, p.43.

2.3 Exchange offices and centralised/decentralised trading platforms

A distinction can generally be made between online exchange offices and (centralised and decentralised) trading platforms. In the case of exchange transactions, changers offer the purchase and sale of cryptocurrencies directly from their own holdings. They do not act as an intermediary agency or marketplace between buyers and sellers of cryptocurrencies, but rather in the sense of an exchange office (bipartite relationship). Exchange transactions with cryptocurrencies qualify as financial intermediary activities within the meaning of the AMLA.

Like traditional trading venues, centralised trading platforms have an order book, matching rules and order types. What is special is that users trade directly on the platform (non-intermediated access) instead of via a regulated financial intermediary (e.g. bank or securities dealer). The user either deposits his tokens with the platform or uses a wallet to which the platform has access. The transactions are carried out via the platform and the tokens can usually be accessed by the platform (private keys) until the user has the tokens transferred to another wallet. These trading platforms differ from changers in that they assume an intermediary function and there is thus a tripartite relationship. The traders accept funds or cryptocurrencies from customers and forward them to other users. Consequently, they function like a foreign exchange market where supply and demand meet and the exchange takes place at the negotiated exchange rate. Such trading platforms qualify as so-called money transmitters and are subject to the AMLA. Aside from this activity, many trading platforms also offer the purchase and sale of cryptocurrencies from their own holdings and function in this respect like a traditional exchange office. In this regard, this report concentrates on issues in the area of anti-money laundering legislation. Typically, however, centralised trading platforms in Switzerland additionally require FINMA licences.[34] There is currently no approved trading platform for cryptocurrencies in Switzerland.

The exchange sector for cryptocurrencies is the most significant market and has the largest population of companies operating in this sector. According to Coinmarketcap figures, 2094 cryptocurrencies were traded worldwide on a total of 15,840 "markets" as at 12 November 2018.[35] The same website has a ranking of 207 trading platforms with the largest daily trading volumes.[36] The five largest trading platforms in terms of bitcoin trading volumes are currently Bifinex (Hong Kong), OKEx (Belize/Hong Kong), Binance (Hong Kong), Huobi (Beijing) and Bitflyer (Japan). Corresponding trading platforms are currently in the planning and implementation phase in Switzerland. In the secondary market, in contrast, some brokers (namely Bitcoin Suisse[37] and Bity[38]) are already active in the exchange business. According to applicable law, these brokers must have an SRO affiliation or authorisation from FINMA as a directly subordinated financial intermediary (DSFI), unless their activities already require another form of authorisation under financial market legislation.

In guidance issued in June 2015[39], the FATF highlighted in particular the risks involved in exchanging cryptocurrencies for fiat money and the need to regulate VC exchanges. This is in application of FATF Recommendations 14, 16 and 26.

2.4 Decentralised trading platforms

Like centralised trading platforms, decentralised trading platforms also maintain a customary order book, but they do not control the customers' token wallet. In other words, the platform does not have the private keys. The tokens are held in a decentralised manner in the customers' wallets and are not pooled by

---

34 When trading tokens that qualify as securities under financial market infrastructure legislation, particularly authorisation as a multilateral trading facility or a licence as a securities dealer (with or without authorisation to operate an organised trading facility) comes into consideration. Bank authorisation is also conceivable, depending on the activities of the platform.

35 See https://coinmarketcap.com/ (last visited on 12 November 2018).

36 See https://coinmarketcap.com/exchanges/volume/24-hour/all/ (last visited on 28 March 2018).

37 See https://www.bitcoinsuisse.ch/ (last visited on 13 March 2018).

38 See https://bity.com/ (last visited on 13 March 2018).

39 FATF Virtual Currencies – Guidance for a risk-based approach 6/2015.

the platform, which should reduce the risk of hacking. Settlement takes place directly on the blockchain using a smart contract. Even decentralised platforms often allow their private customers to participate directly.

In contrast to bilateral trading platforms or exchange offices, a fully decentralised platform never becomes a counterparty to a trade and, unlike centralised trading platforms, the processing of merged orders (after release / confirmation of trade) on the blockchain takes place directly between the platform users. Since a transfer of assets ultimately takes place with the help of the trading platform, the question arises as to whether the platform provides a financial intermediary service within the meaning of the AMLA.[40]

2.5 Off-chain payment systems

Due to the low transaction speeds via the blockchain, scaling efforts have been under way for some time. Providers of so-called "off-chain payment systems"[41] promise a solution to this problem. This is a network where users can make payments to other network users online (but off-chain). The payment system is decentralised and has no access to users' assets.

2.6 Crypto funds

Aside from the possibility of investing directly in cryptocurrencies, efforts are also under way to meet the demand for indirect investment opportunities. Various players intend to launch a crypto fund. Crypto funds are generally understood to mean collective investment schemes that invest their fund assets predominantly or exclusively in cryptocurrencies or other crypto assets. They are not treated differently from other collective investment schemes in terms of anti-money laundering law, i.e. they are regarded as financial intermediaries if they are authorised as a fund management company, SICAV, limited partnership for collective investment or SICAF.[42] No approved Swiss crypto fund exists at present.

3. Risk analysis

Parallel to the spectacular development of crypto assets since the invention of bitcoin in 2009, the risks of criminal use have also increased. While economists and regulatory authorities are constantly drawing attention to the speculative risks to which investors are exposed with investments in cryptocurrencies, and particularly in ICOs[43], several national and international authorities are highlighting the dangers of money laundering and terrorist financing in connection with cryptocurrencies.[44] The Federal Council had already stressed this risk in its 2014 report in response to the Schwaab (13.3687) and Weibel (13.4070) postulates.[45] Although the number of cryptocurrencies has soared in recent years and their use is becoming more and more significant, the trends currently shaping money laundering and terrorist financing risks can be better identified thanks to the experience gained by the authorities responsible for preventing and suppressing white-collar crime. The assessment of this risk is based on both the threats that cryptocurrencies pose to the integrity of the financial system and the vulnerabilities that characterise this system. Among the threats, a distinction has to be made between those that are

---

40 Federal Council, *Federal Council report of 14 December 2018 on legal framework for distributed ledger technology and blockchain in Switzerland*, https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf, pp. 131-142.

41 See for example the Liquidity Network solution (last visited on 12 July 2018).

42 Art. 2 para. 2 lit. b and lit. b^{bis} of the AMLA

43 See for example the numerous warnings published by the US *Securities and Exchange Commission* since 2014: https://www.sec.gov/news/statements.

44 FATF, *Virtual currencies. Key definitions and potential AML/CFT risks*, June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

45 Federal Council report of 25 June 2014 on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates, https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf.

inextricably linked to cryptocurrency technologies and those related to their possible use for white-collar crimes for which fiat money could also be used but which are even more dangerous with the use of cryptocurrencies. Switzerland's weaknesses with regard to the risk of money laundering and terrorist financing using crypto assets, which will be discussed later, are the same as those of most other countries, which are likewise confronted with this new and growing risk.

3.1. Threats associated with crypto assets

3.1.1. Threats inherent in the technology for crypto assets

a. Transaction anonymity and difficult identification of beneficial owners

The biggest threat posed by crypto assets results from the anonymity which is associated with related transactions.

To process crypto transactions, all you need is an electronic wallet, which can be set up easily and free of charge thanks to numerous online programs. Except in the case of a wallet managed by a specialised company (custodian wallet), the procedure for setting up an electronic wallet is usually anonymous. In order to carry out a transaction, the wallet holder simply orders a transfer to another address of the same type using his private key or discloses his public address to another user who wishes to debit the wallet, e.g. to pay for a purchase or service. With cryptocurrencies such as bitcoin, whose technology is based on a combination of asymmetric encryption and blockchain, the transactions are either confirmed or not confirmed by miners based on the assets actually in the wallet concerned. The transactions are visible to all users of this cryptocurrency. The transactions can thus be fully traced, but the actual identity of the person associated with the wallet remains unknown to the other users. Moreover, although this system allows the identification of all transactions that originate from or are directed to a specific address, most wallet programs automatically generate several addresses for the same wallet and a user can own several wallets and use a different one for each transaction, with the result that it becomes virtually impossible to associate a physical person with the transactions he initiates.

Blockchain technology has also been further developed since it was created to introduce bitcoin, and it now provides even more anonymity to certain cryptocurrencies. This is true for currencies such as bytecoin or its successor monero, for example, which are based on CryptoNote technology: a cryptographic process that is based on the so-called "ring signature" and differs from that of bitcoins and ethers. This technology allows users to be grouped: if one of them orders a transaction, it is impossible to know which member of the group did so. Furthermore, the history of the transactions can be completely hidden with the CryptoNote algorithm, unlike with the bitcoin blockchain, where the entire chain of transactions can be viewed by any user who wants to. Finally, CryptoNote enables the splitting of the sums transmitted in a transaction via third-party accounts, with the result that the actual total amount becomes invisible and cannot be traced.

Such splitting can also be carried out by "mixed services", also known as mixers or tumblers, in order to increase the anonymity of transactions in cryptocurrencies which, like bitcoin, use blockchain technology. The cryptocurrencies are sent to a platform that first divides the amount into many smaller sums and transfers them to other addresses before the total sum is sent to the recipient's address. While such mixed services are offered by external servers particularly in the case of bitcoin, certain recently developed crypto assets such as dash have integrated them directly into their protocol, further enhancing the anonymity associated with token transactions. However, anonymity is already very high with the other cryptocurrencies, which is why they are all particularly appealing to criminals.

Last but not least, newly developed technologies for the use of cryptocurrencies also make it possible to boost this anonymity. This applies to prepaid debit cards in crypto assets and crypto banknotes, for example, which were recently launched by a Zug-based company that also has a branch in Singapore.[46]

In terms of anonymity, cash is associated with a similar risk to cryptocurrencies.[47] However, the threat posed by cryptocurrencies is exacerbated by the technological speed and mobility of transactions. In contrast to cash, enormous cryptocurrency sums can be moved from one electronic account to another within seconds without knowing who is carrying out the transactions. The amounts involved can thus be made available almost immediately to anonymous users anywhere in the world. In addition, a wallet holder can pass on the private key at will, thereby granting a third party completely anonymous access to his electronic wallet. This practice too can be compared to passing cash from hand to hand, but because cryptocurrencies can be passed on completely anonymously via the internet, the associated risk increases. The risk of money laundering arising from cryptocurrencies is thus due to the combination of anonymity, speed and mobility.

b. Security vulnerabilities in the underlying cryptocurrency technologies

The technologies underlying crypto assets – particularly blockchain and its successor technologies, as well as asymmetric encryption – were developed to fully secure transactions while ensuring anonymity. Thanks to miners' collective control, such transactions can be executed only by users who actually have the cryptocurrency balance in their wallet that they want to spend. Moreover, thanks to asymmetric encryption, only the actual owner of the wallet can access the assets credited to it in order to carry out transactions. When a transaction has finally been validated by the miners, it is registered on the blockchain and is considered irrevocable. Such an entry can be deleted only if the entire blockchain is changed. However, this would require more than half of the mining power (hash rate) for the blockchain in question. For the bitcoin blockchain, this would require computing power that is estimated to be over 50 times greater than that of a company like Google.

Nevertheless, these technologies are not infallible. As more and more proof-of-work calculations are required, mining can no longer be carried out by a single miner using his computer, as was the case in the early days of cryptocurrencies; instead, it requires the pooling of resources and the creation of mining pools whose members share the revenue. However, such a pooling of resources also runs the risk of more than 50% of the hash rate of a blockchain being concentrated in the hands of a single mining pool, which could then modify the blockchain at will, delete transaction data or have fictitious transactions confirmed by its own miners.[48] In this respect, the development of ever more powerful processors constitutes a danger. These machines, which are generally developed for industrial or administrative purposes and not for mining cryptocurrencies, are increasingly being targeted by hackers, who want to divert their computing power for mining. In other cases, it is the legitimate users of these computers themselves who use them for mining. This was the case in February 2018, for example, when scientists from the Russian Federal Nuclear Center in Sarov were arrested by the Russian Federal Security Service (FSB) when they attempted to connect the centre's IT system – one of the world's most powerful computers – to the internet in order to mine bitcoins.[49] Moreover, mining revenue is so high that it is quite conceivable that criminals will invest massively in the purchase of computers to launder their revenue from illegal activities and use them to build mining farms. Such examples show that the danger

---

46 EMMANUEL GARESSUS, "Une société suisse veut émettre des billets de bitcoins", in *Le Temps*, 8 May 2018, https://www.letemps.ch/economie/une-societe-suisse-veut-emettre-billets-bitcoins; "Singapour: les premiers billets Bitcoins visent à favoriser l'adoption de l'actif", in *Crypto-France.com*, https://www.crypto-france.com/singapour-premiers-billets-bitcoin/.

47 CGMF, *Report on the use of cash and its risks of abuse for money laundering and financing of terrorism in Switzerland*, October 2018, https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73465.html.

48 DE PREUX PASCAL and TRAJILOVIC DANIEL, "Blockchain et lutte contre le blanchiment d'argent. Le nouveau paradoxe ?", in *Resolution LP*, https://resolution-lp.ch/wp-content/uploads/2018/02/064_L_14_De_Preux_Trajilovic.pdf.

49 "Ils minaient des bitcoins dans un centre nucléaire", in *La Tribune de Genève*, 10 February 2018, https://www.tdg.ch/faits-divers/Ils-minaient-des-bitcoins-dans-un-centre-nucleaire/story/30448246.

of more than 50% of the hash rate of a blockchain being concentrated in one place is not purely theoretical. Although the most important cryptocurrencies are likely to be too highly developed to be victims of such a 51% attack, this has already been the case with newer virtual currencies. Recent examples include verge, monacoin and bitcoin gold. In the case of bitcoin gold, a miner managed to take control of the blockchain. He amortised the high cost of the operations to gather the required computing power by stealing bitcoin gold, exchanging it for other cryptocurrencies and then deleting the transactions, thereby recovering the already exchanged bitcoin gold.[50]

In addition to this threat, the blockchain and asymmetric encryption technologies have a certain susceptibility to hacker attacks that is greater than their developers could ever have imagined. Clever hackers can take control of the private keys of third parties' wallets in order to carry out transactions on them at will. Since 2011, several hacker attacks have been reported on cryptocurrency trading and storage platforms, often with tens of millions of dollars' worth of assets being stolen.[51] In the first quarter of 2018 alone, the total amount of cryptocurrencies stolen during hacker attacks reached the equivalent of USD 670 million.[52] All cryptocurrencies are vulnerable, and although most reported cases relate to bitcoin, the record theft was carried out in January 2018 on another cryptocurrency, when hackers succeeded in taking more than XEM 500 million (the cryptocurrency of the NEM network) from the Coincheck platform based in Japan, equivalent to about USD 530 million.[53] However, this problem does not affect only virtual currency trading and storage platforms. Wallets of simple private individuals that are managed without an e-wallet provider can also be hacked and the losses can be high. In 2014, the Swiss authorities became aware of such a case, which cost the injured party almost CHF 100,000.[54]

Similarly, certain cryptocurrencies such as ether – but not bitcoin – are vulnerable to the diversion and subsequent laundering of funds because they allow smart contract technology. This technology originated from a further development of the blockchain designed for bitcoin and was originally developed by Ethereum. It is based on the formulation of protocols that automatically execute contract provisions. The decisive factors are computer algorithms, which determine under which conditions which decision has to be made. In this way, contracts can be executed and transactions on the blockchain they generate can be monitored, while at the same time suppressing the risks of arbitrariness associated with human action – the principle is that one cannot deviate from the smart contract protocol, which is absolutely rational and fair to all and thus becomes the law of those who use this technology ("The code is the law"). However, the example of the DAO project shows that such protocols which are considered infallible are also prone to certain design flaws. The DAO model, which was intended to put into concrete terms the utopia of a fully decentralised and democratic economy, was founded on the Ethereum blockchain in 2016. It was managed from Switzerland by DAI.LINK Sàrl and can be defined as a sort of decentralised and automated investment fund. Users could vote on projects and approve or reject financing, while the subsequent payments were made automatically via a smart contract. But due to a programming error in this smart contract, a user could use the terms of the contract for his own purposes without changing the contract itself. In this way, the user was able to divert tokens worth a total of USD 53 million in compliance with the protocol. To fill this gap, it was necessary to find users who agreed to change the blockchain and delete all transactions that had been made from the time of the improper forwarding of the tokens. Although this is contrary to the very principles of blockchain, this decision was supported by the majority of users. However, the resistance of the minority led to a hard fork and thus to a split in the Ethereum blockchain. Consequently, despite all the precautions taken by their developers, smart contracts can serve as an instrument for the misappropriation of cryptocurrencies,

---

50 "Bitcoin Gold: une attaque double dépense fait perdre plusieurs millions de dollars à des plateformes d'échanges", published on the Crypto-France website. https://www.crypto-france.com/bitcoin-gold-attaque-double-depense-pertes-millions-dollars-plateformes-echange/.

51 LOUBIRE PAUL, "La très longue liste de vols de bitcoins par des hackers", in *Challenges*, 08.12.2017, https://www.challenges.fr/finance-et-marche/la-tres-longue-liste-de-vols-de-bitcoins-par-des-hackers_518541.

52 "670 millions de dollars de crypto-monnaies ont été dérobés au cours du premier trimestre 2018", in *Crypto-France.com*, April 2018, https://www.crypto-france.com/670-millions-dollars-crypto-monnaies-voles-premier-trimestre-2018/.

53 "Cryptomonnaie: la plateforme japonaise Coincheck victime d'un vol record", 29 January 2018, http://www.rfi.fr/economie/20180129-coincheck-vol-cryptomonnaie-injonction-japon.

54 *Federal Council report of 25 June 2014 on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates*, https://www.news.admin.ch/NSBSubscriber/message/attachments/35361.pdf, cit., p. 22.

which – once syphoned off – can be laundered thanks to the anonymity of blockchain transactions. To date, the only way to counter this is to change the blockchain itself.

c. Threats in connection with the novelty effect and users' inexperience

The third money laundering risk associated with cryptocurrency technologies stems from the new enthusiasm for this type of currency and the lack of monitoring of those who use it, who are often unfamiliar with the minimum precautions to be observed in this area. Due to their relative novelty and multiple uses, cryptocurrencies have an appeal that sometimes leads to rash actions and increases vulnerability to fraud. The most common risk factor is negligence when storing the private keys that give access to wallets. If these keys are not stored in sufficiently secure locations, they can easily be stolen and used by third parties without hacking. But aside from this banal beginner's mistake, there are also more sophisticated fraud methods directly linked to the growing prevalence of cryptocurrencies, and their main victims are inexperienced users tempted by the novelty and enormous profits they hope to make from these virtual currencies.

The number of cryptocurrencies is constantly rising and currently stands at around 2,000, about half of which are no longer used. Some of them quite simply involve fraud. This mostly concerns cryptocurrencies that are based on blockchain technology but are not decentralised. In such cases, their promoters – actually fraudsters – do not disclose the code base and first collect all or most of the tokens, and they then manage their exchange value themselves. If such cryptocurrencies are managed by clearly identifiable and well-controlled institutions, they can offer concrete advantages in the fight against financial crime, as the promoters can easily identify their customers and, if necessary, inform the financial supervisory authorities or prosecution authorities. But in many cases they are scams along the lines of a Ponzi or snowball system, against which people can in fact protect themselves with cryptocurrencies that are actually decentralised. MROS has received several suspicious activity reports in connection with cryptocurrencies that apparently belong to this fraud category. In all cases, customers were blinded by the fixed high returns promised by the promoters and bought tokens of these currencies. They were then immediately asked to recruit new buyers from their circle of friends. However, there is every indication that the revenue paid out to existing customers in all of these cases registered by MROS was financed by the money of new investors, even though the pyramid has not yet collapsed. Nevertheless, the authorities of several countries, including Germany, Italy and Bulgaria, have already banned trading in one of these currencies. In Switzerland, FINMA likewise ordered the legal liquidation in September 2017 of companies that offered and managed e-coin, which is presumably based on such a crime pattern.[55]

A similar risk of fraud could exist for investors with ICOs. The recent enthusiasm for this way of raising capital on the part of investors who are dazzled by the high profits that seem to characterise fintech, as well as start-ups that want to raise money for projects and would probably not be supported by conventional investment institutions, actually opens the door for many possibilities of fraud. A frequent and typical example concerns false ICOs, where the alleged developers of a project launch calls for investment without really having started the development of any project. MROS recently learned of such a case.

False ICO

An online exchange office reported a case to MROS after one of its customers fell victim to a rip-off and drew their attention to it. The customer in question had invested in an ICO project organised by a company registered in another European country. The project concerned the development of a physical wallet, similar to a debit card. The customer wanted to invest in this seemingly innovative project and transferred a bitcoin sum to the financial intermediary. This was first to be exchanged for

[55] FINMA press release of 19 September 2017, https://www.finma.ch/de/news/2017/09/20170919-mm-coin-anbieter/.

ether and then credited to the recipient's wallet, which was hosted by a platform under foreign law. However, it soon became apparent that this ICO project was a scam. The competent prosecution authorities to which the case was referred nonetheless refused to intervene and argued that the competent place of jurisdiction could not be in Switzerland due solely to the financial intermediary's domicile.

A second threat related to ICOs arises from the withdrawal of promoters from a project that exceeds their capacity. The promoters might prefer to file for bankruptcy, later set up new companies and resort again to ICOs to finance them, rather than stick to the implementation of the project for which they launched the original ICO.

Another potentially criminal pattern associated with ICOs is the manipulation of the prices of tokens issued by ICO organisers. One such suspicion concerns Zug-based envion AG, which launched an ICO to develop mobile mining farms to reduce the ecological footprint of mining. According to several publicly available sources, the director who was in charge of implementing this ICO, which raised over USD 100 million, is said to have issued illegally generated tokens and sold them to crypto exchanges to take control of the company. The price of the tokens issued collapsed as a result of these suspicions, and investors risk losing almost all their deposits. FINMA has initiated proceedings against the issuers of these ICOs, focusing on possible violations of banking law resulting from any unauthorised acceptance of public funds in connection with this ICO.[56]

As the tokens received by investors in return for their investments are not treated as company shares in many ICOs, but rather as priority rights of use, the funds invested could be irrevocably lost in the event of fraud, except for the ICO organisers. Since the sums involved in ICOs which have recently become known are often astronomical, such fraud scams constitute a major threat. According to some studies, two thirds of the ICOs launched have failed or turned out to be a fraud, with more than USD 12 billion apparently raised worldwide by ICOs in the first five months of 2018 alone.[57]

d. Malware and ransomware

The anonymity of the tokens and their electronic media make them a privileged instrument for hackers, especially in connection with ransomware. There are numerous examples of this at home and abroad: hackers attack computers of third parties, usually companies, encrypt the files on them with malware and demand a ransom in cryptocurrency for their release. After the payment has been made, these ransoms are transferred to wallets that are registered in other countries and from which they can be forwarded or exchanged, making it impossible to prosecute such extortion in most cases. A famous example of such ransomware is WannaCry, which was used in May 2017 to encrypt the data of over 300,000 computers in more than 150 countries. A ransom was demanded in bitcoins for decryption, and was also paid by some of the companies involved. The extorted money was then apparently exchanged into monero in small tranches via trading platforms – including a platform domiciled in Zug. As that is neither a centralised trading platform with access to the wallets of its users nor a decentralised platform with power of disposal, it is not subject to the AMLA. Consequently, it did not carry out any checks which would have made it possible to identify the criminal origin of the money exchanged. Nevertheless, the platform in question worked with the prosecution authorities to block the money laundering after the first indications.[58]

---

56 FARINE MATHILDE, "La FINMA enquête sur une ICO à 100 millions de francs", in *Le Temps*, 26 July 2018, https://www.letemps.ch/economie/finma-enquete-une-ico-100-millions-francs; FINMA, press release of 26 July 2018, https://www.finma.ch/de/news/2018/07/20180726-mm-envion/.

57 FARINE MATHILDE, "Comment investir dans les cryptomonnaies", in *Le Temps*, 22 July 2018, https://www.letemps.ch/economie/investir-cryptomonnaies; FAUCETTE JAMES, GRASECK BETSY and SHAH SHEENA, *Update: Bitcoin, Cryptocurrencies and Blockchain*, Morgan Stanley, 1 June 2018, p. 35, https://www.macrobusiness.com.au/wp-content/uploads/2018/06/82012860.pdf.

58 SUBERG WILLIAM, "Bitcoin exchange ShapeShift helps police as WannaCry attacker converts to monero", in https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero; EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017, p. 11.

e. Laundering of illegally acquired crypto assets

Due to their intrinsic properties and above all the anonymity they provide, cryptographic technologies can be misused in many ways to launder illegally acquired tokens. Nonetheless, it should be noted that, in certain cases, it is not established beyond doubt whether the illegal acquisition of crypto assets is to be equated with an offence and thus a predicate offence to money laundering. Due to the lack of legal precedent on this issue, it is not clear whether token diversion via smart contracts or 51% attacks are themselves relevant under criminal law, as in both cases the initiators of these actions only use the possibilities of the blockchain and smart contract technologies that are available to all users. In contrast, the theft or extortion of tokens, as well as their acquisition through investor fraud, are clearly economic crimes and predicate offences to money laundering.

Money laundering activities depend on criminals' IT skills. The system of peer-to-peer transaction validation offers a certain guarantee of self-monitoring. Wallets to which diverted sums are credited can be blacklisted and the associated transactions rejected by the user community, with the result that the stolen assets often cannot be used. In order for a wallet to be blacklisted, however, the members of the user community must first determine the criminal origin of the assets credited to it, which rarely happens according to police information.

In order to launder illegally acquired crypto assets, criminals often use darknets, where tokens of criminal origin can be sold at sometimes undervalued prices on decentralised trading platforms hosted there. This type of money laundering was apparently used in the case of the XEM stolen from the Coincheck crypto exchange: it was possible for more than 40% of the stolen XEM to be exchanged for bitcoins on such platforms and thus sold quickly.[59] Mixed services likewise constitute a major obstacle for the identification of illegally acquired bitcoins, which is why criminals who wish to cover up the dishonest origin of their cryptocurrencies very often resort to them. But exchanging cryptocurrencies for other cryptocurrencies, withdrawing money from crypto ATMs and playing games in online casinos are also ways of laundering illegally acquired crypto assets.[60] Another money laundering technique involves opening wallets with recognised providers of electronic wallets in the name of so-called money mules, which are equipped with false documents. From there, the assets are transferred to bank accounts that have been opened in the name of money mules too, but over which the criminals also have control thanks to false documents.[61]

3.1.2. Threats of fraudulent use of cryptocurrencies

Cryptocurrencies are associated with great threats not only due to their technology. They can also be used for white-collar crime activities that are not specifically aimed at cryptocurrencies, but for which such currencies are of particular interest due to their anonymity, transaction speed and the absence of financial intermediaries in transaction processing.

a. Terrorist financing using cryptocurrencies

To date, only a few cases of terrorist financing using cryptocurrencies have been reported worldwide. Terrorist organisations and their supporters appear to prefer other forms of financing and other means

[59] "Coincheck: les pirates servaient déjà parvenus à blanchir 40% des 500 millions de XEMs dérobés", https://www.crypto-france.com/coincheck-pirates-blanchiment-xems/.

[60] FANUSIE YAYA and ROBINSON TOM, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance and ELLIPTIC, 12 January 2018.

[61] EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017, p. 8.

of payment.[62] Therefore, the United Kingdom considers the actual risk of terrorist financing using cryptocurrencies to be low.[63] However, the extent of the threat is illustrated by numerous discussions on the use of cryptocurrencies held by international followers of the Islamic State (IS) on social networks, where the most experienced among them offer actual training on the use of crypto assets.[64] In this context, cryptocurrency donations have also been called for to finance the IS, underlining the particular threat of token crowdfunding in terms of terrorist financing.[65] It appears that a Salafi Palestinian terrorist organisation used this technique to secure financing.[66] Although no evidence has been provided to date, several journalists, including the anti-terror organisation Ghost Security Group, claim that bitcoin wallets contributed to the financing of the recent terrorist attacks in France and Indonesia, and that the Islamic State has several such wallets to which assets amounting to several million US dollars are credited.[67] The simplicity and anonymity of crypto transactions, which allow assets to be moved quickly from one place in the world to another, thus pose a major threat regarding terrorist financing, even if this risk is currently proven more in theory than in practice. A similar threat which has not yet been confirmed could come from ICOs, whose profits could be used to finance terrorism. However, extreme right wing organisations, which are often suspicious of traditional financial institutions, which they believe are controlled by Jews, are increasingly resorting to cryptocurrencies, especially in the United States, and particularly to raising capital in cryptocurrencies. In this way, they can bypass traditional payment systems, from which they are often excluded because of their activities. Nevertheless, there is still no evidence that such organisations have ever used crypto assets to finance terrorism.[68]

Not a single case of terrorist financing using cryptocurrencies has been reported in Switzerland. Nonetheless, MROS received information about such suspicious cases from a foreign counterpart. Bank transactions in fiat money from various European countries, including Switzerland, were credited to an account in the country whose FIU had notified MROS. After the money was transferred to this account, it was exchanged for bitcoins and apparently used to finance terrorist activities. Since there is no legal basis for requesting information from financial intermediaries in response to a request from a foreign FIU, MROS was unable to carry out any further investigations in this case. But the mere reporting of such a suspicion shows the major threat of terrorist financing posed by crypto assets. They potentially facilitate the rapid and anonymous transfer of large sums of money intended for the financing of terrorist organisations, but can also be used by simple supporters of such organisations who wish to carry out terrorist attacks. In this respect, they are particularly dangerous in that they can be used to illegally purchase the necessary material on the darknet.

b. Cryptocurrencies as a means of payment for illegal goods and services

Digital platforms that offer illegal goods and services for sale or purchase and can be found on darknets prefer to use cryptocurrencies. Bitcoin was the most widely used currency on such platforms for a long time. Meanwhile, however, the significance of monero, which guarantees greater anonymity and non-traceability of transactions, appears to be increasing. Crypto assets are the main means of payment on darknets, where criminals can stock up on prohibited pornographic material, primarily child pornography, weapons, stolen credit card numbers and particularly drugs. Drugs are increasingly being traded via

---

62 European Parliament, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, May 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

63 HM Treasury and Home Office, *National risk assessment of money laundering and terrorist financing 2017*, London, 2017, p. 38, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.

64 BRANTLY AARON, "Financing Terror Bit by Bit", in *CTC Sentinel*, vol. 7, no. 10, October 2014, p. 4, https://ctc.usma.edu/financing-terror-bit-by-bit/.

65 WILE ROB, "Supporter of extremist group ISIS explains how bitcoin could be used to fund Jihad", in *Business Insider Australia*, 8 July 2014, https://www.businessinsider.com.au/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7.

66 European Parliament, *Virtual currencies and terrorist financing*…, cit., p. 29.

67 IRWIN ANGELA S.M. and MILAD GEORGE, "The use of crypto-currencies in funding violent jihad", in *Journal of Money Laundering Control*, vol. 19, no. 4, 2016, p. 410-411.

68 European Parliament, *Virtual currencies and terrorist financing*…, cit., p. 30.

such illegal digital platforms, although police sources say that much drug trafficking is still carried out in cash.[69]

Darknet transactions are difficult to trace. On the one hand, networks such as TOR, which provide darknet access, use different servers (nodes) and thus different IP addresses, which makes it extremely difficult to identify the actual IP address of a user. On the other hand, darknet transactions are carried out via mixed services between the seller and the buyer of the illegal goods or services, which is an additional obstacle to the identification of both. Finally, a wallet can be blacklisted because it received assets that originated from illegal trading on darknets. However, it is not evident on the blockchain whether a transaction took place on the darknet or off it. As a matter of fact, a user currently has to make a mistake and publish his encrypted address or other personal data on a third-party site on the internet in order for the anonymity of darknet transactions to be lost. In such cases, prosecution authorities can assign various crypto transactions to the wallets of a particular user and sometimes to an identified person with patient comparisons.[70]

Although darknets do not exclusively serve criminal activities, the danger of terrorist financing posed by crypto assets is increased by the possibility of buying weapons, other war material or instructions for producing explosive devices under the protective cover of anonymity that is difficult to penetrate. However, no such case has yet been proven in Switzerland. With regard to money laundering, in contrast, the risk is linked to the fact that proceeds from illegal sales in cryptocurrencies are fed back into the legal circuit. Several such cases have been reported in Switzerland. Sellers of illegal products on the darknet mostly use online exchange offices – sometimes those based in Switzerland – to exchange their cryptocurrencies for fiat money. If they are simple casual traders, the sums involved are often small. But the sums can also be considerable, e.g. when organisers of trafficking in drugs or arms or administrators of an illegal online trading platform are involved, as shown by the following case dealt with by MORS in 2017.

Laundering money from illegal online trade using cryptocurrencies

An online exchange office reported a suspicion concerning one of its customers to MROS. The customer was named in the press and reported to be the administrator of an illegal online trading platform who had been tracked down thanks to cooperation between the federal police of two North American states and an Asian country. The man, who had been living in this Asian country for several years and was arrested there, had amassed considerable wealth selling illegal products, especially weapons and drugs, on the platform he operated on a darknet. He had used the online exchange office to launder the profits he had made in bitcoins, and the office had finally reported this. The office had given him fiat money for his bitcoins, and he had mainly invested this in real estate in several countries and in luxury products. It was no longer possible to analyse the transactions and determine the criminal origin of the sums exchanged because of the mixed services used on darknets. Nonetheless, the foreign authorities that had initiated criminal proceedings against him were able to seize and confiscate assets worth tens of millions of US dollars in cryptocurrency thanks to the information obtained from analysing his computers.

This case shows that even if the identity of the person who exchanged cryptocurrencies for fiat money is known, and even if the cryptocurrency in question is bitcoin, where all transactions can be traced, it is almost impossible to identify the criminal origin of the assets because of the anonymity surrounding wallets.

---

69 See also HAEDERLI ALEXANDRE and STÄUBLE MARIO, "De la drogue livrée en courrier A. Comment fonctionne le marché des stupéfiants sur le Darknet", in *La Tribune de Genève*, 02.05.2018, https://www.tdg.ch/extern/interactive_wch/darknet/.

70 AL JAWAHERI HUSAM, AL SABAH MASHAEL, BOSHMAF YAZAN and ERBAD AIMAN, "When a small leak sinks a great ship: deanonymizing Tor hidden service users throught bitcoin transactions analysis", in *arXiv*: 1801.07501v2, April 2018, https://arxiv.org/abs/1801.07501.

c. Cryptocurrency use for phishing

Crypto assets are increasingly involved in the numerous scams that belong in the category of computer fraud. Although the vast majority of such cases are still operated with fiat money, a review of the suspicious activity reports sent to MROS shows that cryptocurrencies are increasingly used for this predicate offence to money laundering. Two main variants of this type of crime show how tokens are used to launder fraudulently obtained assets. In the first variant, criminals use hacked electronic access data for third-party bank accounts to transfer fiat money to accounts of individuals who want to sell cryptocurrencies. Once these individuals have received the amount in fiat money, they transfer the cryptocurrencies thus purchased to a wallet indicated to them. However, this wallet does not belong to the beneficial owners of the accounts to which the fiat money was improperly debited. As a rule, however, the beneficial owners of the wallet to which the assets were credited cannot be identified by the prosecution authorities due to the anonymity associated with it, with the result that the criminal proceedings initiated against them have to be discontinued. With the second, more sophisticated variant a money mule is used, and the assets taken from hacked business relationships are transferred to his account. Money mules are usually lured by a false employment contract or other fraudulent pretexts, and they then buy cryptocurrencies on behalf of criminals and credit them to the wallets indicated to them. With both variants, classical crime patterns can be perfected using cryptocurrencies: the paper trail is obscured thanks to the anonymity of crypto wallet holders, who are usually registered in countries other than Switzerland, which makes prosecution even more difficult in such cases than in traditional phishing cases.

d. Investment of funds of criminal origin in crypto assets

The anonymity of crypto assets and the money laundering opportunities offered by crypto transactions and the exchange of such currencies are making them increasingly popular with criminals who want to invest their illegally acquired funds and thereby launder them.[71] The increasing frequency with which crypto assets are used to launder funds from online scams illustrates this trend. Nevertheless, revenue from all possible predicate offences can be used to purchase crypto assets. In this respect, ICOs are exposed to a similar risk and it cannot be ruled out that funds of criminal origin may be invested in them. An indication of this is the high number of suspicious activity reports sent to MROS by ICO organisers who discovered that their customers had used stolen or forged identity papers to initiate the business relationship. At present, however, the predicate offence whose profits are most often laundered by purchasing crypto assets appears to be drug trafficking controlled by criminal organisations. Criminal networks active in this field are using cryptocurrencies not only to sell drugs on darknets, but increasingly also to return their illegally obtained revenue from Europe to exporting regions. This shows how easy it is to transfer tokens quickly and extensively across borders with these systems, as demonstrated by a case dealt with by Europol recently. Members of a criminal network selling cocaine imported from Colombia in Europe hired money mules to exchange cash from drug trafficking at bitcoin ATMs. These bitcoins were then to be transferred to wallets likewise controlled by money mules, who were in turn working for drug exporters in Colombia.[72] The American authorities have also seen growing use of cryptocurrencies by criminal organisations active in the drug trade in the United States, Europe and Australia, which invest their revenue from this illegal trade in the purchase of bitcoins.[73] Although no such case has yet been discovered in Switzerland, the occurrence of such a case cannot be ruled out.

---

71 EUROPOL, 2017 *Virtual Currencies Money Laundering Typologies*, 2017, p. 12; FANUSIE YAYA and ROBINSON TOM, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance and ELLIPTIC, 12 January 2018, p. 5.

72 KOOS COUVÉE, "European traffickers pay Colombian cartels through bitcoin ATMs: Europol Official", in ACAMS Moneylaundering.com, 28 February 2018, https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/.

73 U.S. Department of Justice and Drug Enforcement Administration, *2017 National Drug Threat Assessment*, October 2017, p. 130; TZANETAKIS MEROPI, "Comparing cryptomarkets for drugs: a characterisation of sellers and buyers over time", in *International Journal of Drug Policy*, vol. 56, June 2018, p. 176-186.

In this context, the growing use of bitcoin ATMs could pose a threat in that criminals active in areas other than drug trafficking could also use them for their own purposes.

3.2. Switzerland's vulnerability to money laundering and terrorist financing via cryptocurrencies

The aspects presented so far demonstrate the great danger that cryptocurrencies pose in the area of money laundering and terrorist financing. Although this threat has not yet been reflected in a large number of proven cases, that does not mean that the risk is low. The financial system's vulnerability to this danger is considerable and not specific to Switzerland. Nevertheless, this does not include the legal qualification of crypto assets: in Switzerland, crypto assets are generally treated by prosecution authorities as one of several types of assets that can contribute to money laundering. This view also corresponds to that of FINMA, which is responsible for financial market supervision.

3.2.1. Vulnerabilities of financial intermediaries that carry out crypto transactions

In FINMA's view, all types of financial intermediaries in Switzerland that carry out crypto transactions are subject to the AMLA. This applies to online exchange offices that exchange cryptocurrencies for fiat money, centralised trading platforms for various crypto assets – none of which is registered in Switzerland – providers of custodian wallets, decentralised trading platforms for various crypto assets that can intervene in their customers' transactions, and companies that launch ICOs and issue tokens that can serve as means of payment.

However, due to the decentralised nature of the technology underlying most cryptocurrencies, users can often carry out transactions without financial intermediaries, which is a major vulnerability in the anti-money laundering system. For example, providers of non-custodian wallets and decentralised trading platforms for cryptocurrencies which cannot intervene in the transactions arranged by their customers are not subject to regulation. In actual fact, companies that offer such services do not intervene at any time in the transactions carried out by users and therefore do not carry out any financial intermediary activity. This applies in particular to decentralised trading platforms for cryptocurrencies.[74] This vulnerability is illustrated by the example given above, in which such a Swiss company had exchanged bitcoins procured with the ransomware WannaCry for moneros without recognising the originators of the transactions or the criminal origin of the exchanged tokens. Consequently, there is no control whatsoever for a large proportion of crypto transactions.[75]

Moreover, not all financial intermediaries involved in crypto transactions seem to be equally aware that they are subject to the AMLA and the related due diligence obligations. They also do not always fulfil these obligations in an appropriate manner, do not always know their customers precisely and, despite their willingness to cooperate with the prosecution authorities, are not in a position to provide information on the identity of their customers or the origin of the tokens with which they trade. Nonetheless, the growing number of suspicious activity reports received by MROS from companies specialising in cryptocurrency trading indicates that these financial intermediaries are becoming increasingly aware of their due diligence obligations. In February 2018, FINMA also published guidelines on IOCs which define the conditions under which companies that use this way of raising capital in cryptocurrency are regarded as financial intermediaries. MROS has found that more suspicious activity reports have been received from such companies since the publication of these guidelines.

---

74 See section 4.1.4.

75 "76% of incorporated wallet providers do not have a license", HILEMAN GARRICK and RAUCHS MICHEL, *Global Cryptocurrency Benchmarking Study*, Cambridge, Centre for Alternative Finance/University of Cambridge, 2017, p. 62.

But even if all financial intermediaries were aware of their due diligence obligations, the effectiveness of these precautionary measures would inevitably remain limited, as crypto transactions are transnational and run through service companies registered in a great many countries. For example, online exchange offices registered in Switzerland are often instructed to exchange cryptocurrencies by foreign custodian wallet providers acting on behalf of their customers. In such cases, the Swiss platform has no access to the KYC data of the customer of the foreign platform for which it is carrying out the exchange and therefore does not know the identity of the customer. Similarly and because of the anonymity of crypto transactions, financial intermediaries which carry out such transactions on behalf of their customers have no way of checking whether the persons indicated by their customers actually own the wallets from which the securities they trade originate or to which they make transfers. In order to reduce this vulnerability, certain financial intermediaries concentrate on the management of their customers' assets and do not carry out payment transactions for the benefit of third parties. Moreover, they accept anonymous cryptocurrencies only after extremely precise clarifications and only for customers they know well.

Such efforts are particularly valuable, as the only crypto transactions that allow the beneficial owners of the assets involved to be identified are those involving cryptocurrencies being bought or sold for fiat money. Online exchange offices that carry out such transactions are aware of their due diligence obligations, comply with them and, if necessary, supply the information available to them to the prosecution authorities just like all conventional financial intermediaries. According to the competent police and judicial authorities, such online exchange offices are the only financial intermediaries involved in crypto transactions that can provide them with precise information on the identity of the beneficial owners of the assets in question. But this does not provide them with comprehensive protection against fraud. They have no way of verifying the identity of the beneficial owners of wallets to which they credit amounts on behalf of their customers. Moreover, if a customer wants to sell his tokens for fiat money, the financial intermediary has only limited means available to prove the possible criminal origin of these tokens. With cryptocurrencies such as bitcoin, where all transactions can be traced, the financial intermediary can use chain analysis to check whether the customer's wallet actually contains the bitcoins he wants to sell and possibly identify whether the assets in question went through a mixed service or – more rarely – a blocked wallet. In contrast, the financial intermediary cannot find out whether it is the customer himself who used this mixed service or blocked wallet, or whether he legally acquired the tokens concerned only after these suspicious stages.

In addition, the account opening procedures of online exchange offices often provide a certain amount of leeway for criminals who want to launder illegally obtained money with the help of tokens. MROS is aware of cases in which such Swiss financial intermediaries filed a suspicious activity report concerning money laundering because business relationships had been initiated using stolen identity documents. Since the procedure for opening an account is often carried out online, such identity theft could not have been detected beforehand. A similar vulnerability also concerns companies that offer ICOs and are considered financial intermediaries. All previous reports from such companies to MROS were based on the suspicion that forged documents were involved in the initiation of business relations. For example, a company that ran an ICO reported to MROS over 100 business relationships with investors willing to invest who had presented forged identity papers. This increased the suspicion that the sums invested in the ICO could be of criminal origin.

In addition, just like conventional exchange offices, online exchange offices involved in crypto asset trading are required to apply their due diligence obligations to customers' exchange transactions only if the amount exceeds CHF 5,000 (Art. 51 para. 1 no. 1 of the AMLO-FINMA, SR 955.033.0). This leaves scope for numerous, completely anonymous exchange transactions below this threshold. The growing use of crypto ATMs increases this vulnerability, as confirmed by several suspicious activity reports received by MROS.

Breakdown of sums in the case of cryptocurrency purchases

A platform for payment services that accepts payments in crypto assets sent a suspicious activity report to MROS stating that the same wallet had been credited with bitcoin sums purchased within a short period of time through eleven withdrawals from ATMs, with the maximum permitted amount being withdrawn each time. The reporting platform did not know the beneficial owners of the credited wallet – suggesting that financial intermediaries that carry out crypto transactions without an exchange into fiat money are often unaware of their due diligence obligations. To identify the person(s) who carried out these exchange transactions, MROS had only the Swiss mobile phone number. Mobile network operators that issue such telephone numbers are legally obliged to identify their customers under the Federal Act on the Surveillance of Postal and Telecommunications Traffic (SPTA, SR 780.1). In this case, however, they had not fulfilled their duty and the telephone numbers were registered under imaginary names such as Donald Duck. Since the SPTA does not provide for any criminal sanctions for such failures by mobile network operators, they could not be prosecuted. Consequently, MROS had no way of tracing the owners of these telephones. Since it also lacked information on the origin of the assets that had been exchanged for bitcoins, it had to cease investigations. In this case, the financial intermediary did indeed recognise the suspicious transactions and duly reported them to MROS. However, because there were no means of identifying the owner of the wallet to which the amounts were credited, the investigations could not be pursued. The amendment to the SPTA which came into force on 1 January 2018 and provides for criminal sanctions for such violations of mobile network operators' obligation to identify customers was intended to put an end to the total anonymity of transactions still possible in this case. However, it cannot prevent a mobile phone from being used for criminal purposes by someone other than the legitimate owner, e.g. a thief.

Financial intermediaries involved in crypto asset transactions are thus highly vulnerable to the risks of money laundering and terrorist financing. Moreover, the vulnerability of the Swiss financial centre is further aggravated by the limited number of such financial intermediaries, but this also applies to other countries. The fact that there are only a few companies active in the field of financial intermediation for cryptocurrencies implies that countless transactions take place directly between users. They use platforms that only provide programs that users can use without their intervention and are therefore not considered financial intermediaries. With a few exceptions, e.g. the United States, Japan and, more recently, Malaysia, providers of custodian wallets are not yet subject to anti-money laundering legislation in most countries. This makes it easy for Swiss users to use the services of financial intermediaries registered in other countries where anti-money laundering laws do not apply to them or are rarely applied for crypto transactions and potentially money laundering as well. In this respect, the fact that the traditional boundaries of criminal jurisdiction are blurred on the internet is one of the key elements hampering the suppression of token financial crime.

3.2.2. The difficult suppression of money laundering and terrorist financing using cryptocurrencies

The police and judicial authorities charged with the suppression of cybercrime and, in particular, money laundering and terrorist financing using crypto assets are confronted with numerous obstacles, which are not specifically related to the Swiss financial centre but apply to all countries. Due to the anonymity surrounding token transactions, it is extremely difficult to identify suspicious transactions and the beneficial owners of the wallets involved. In this respect, chain analysis offers only very limited assistance. On the one hand, such analysis is possible only for cryptocurrencies where the transactions on their blockchain are traceable, and it cannot be carried out at all for completely anonymous tokens such as monero or verge. On the other hand, the paper trail is definitively interrupted by an intermediate mixed service even with traceable cryptocurrencies such as bitcoin. And even if the assets concerned can be traced using chain analysis, the problem is not solved: this analysis does not say anything about

the beneficial owners of the wallets involved in the transactions, about the possibly criminal nature of a transaction in connection with a money laundering operation or about the IP addresses of the computers used for the transactions. With certain chain analysis programs, however, the transactions carried out between different wallets can be compared relatively accurately, making it possible to determine with a very high degree of probability whether their beneficial owner is always the same. Moreover, these programs can also indicate if one of the wallets used for the transactions was blacklisted for any reason, e.g. because someone transferred assets from the sale of illegal goods or services on the darknet.

In the absence of such an indication, however, there is no difference in a chain analysis between a legal transaction and an illegal transaction or one carried out on the darknet. In order to be able to identify a transaction that could have been used to launder money from darknet sales, police authorities are also usually forced to infiltrate these illegal markets, locate the criminals' pseudonyms and hope that they make a mistake that can break their anonymity. An example of such a mistake would be if they disclose information on a public website that can be matched with the result that their identity and control over a particular wallet can be determined. It is even more difficult to detect fraudulent token transactions that do not originate from a darknet, as the prosecution authorities do not know *a priori* on which area to focus their investigations. However, MROS receives reports from financial intermediaries that encounter the same difficulties as the prosecution authorities when analysing transactions. In most cases, they report fraud because one of their customers has been a victim of fraud and has therefore filed criminal charges or a complaint, or because stolen or forged identity documents were used when the business relationship was initiated.

The beneficial owner of the associated assets must be identified as soon as a suspicious transaction has been detected. According to the judicial authorities consulted, this identification is possible with information provided by financial intermediaries. However, it is possible for a dubious transaction to have been carried out without a financial intermediary or, if a financial intermediary was involved, that the financial intermediary did not have any information about it. Finally, suspicious transactions are often carried out mainly by crypto asset trading platforms that are not registered in Switzerland. In such situations, the prosecution authorities can only hope that the suspected criminal will make a mistake that will allow the veil of anonymity to be lifted, or that the exchange of information between the police and the judiciary and their foreign counterparts will prove productive. While international mutual assistance is undoubtedly one of the most effective instruments for suppressing crime in connection with cryptocurrencies, it is often knocked out by the speed of cross-border transactions. Moreover, even if wallets with assets of suspicious origin and their beneficial owners are identified, the assets deposited in them can be confiscated only if the prosecution authorities have the private keys to these wallets. With a little luck, a cooperative custodian wallet provider will have this key and hand it over to the judiciary. From the viewpoint of the Swiss authorities, however, this provider must be registered in Switzerland, which is very rarely the case. Similarly, a criminal against whom criminal proceedings have already been initiated can disclose the private key of his wallet and thus clear the way for the seizure and confiscation of the assets deposited in it. However, if none of these cases occurs, the proceeds from money laundering using cryptocurrencies are irrevocably lost for the prosecution authorities, at least with the current state of technology.

In most cases, the police and judicial authorities also fail to break the anonymity of crypto transactions and the wallets in which the virtual funds are deposited. Similarly, it is not easy to determine whether the launch of a new cryptocurrency or an ICO is simply based on a scam. There may be corresponding suspicions, but often nothing can be proved. Finally, the unclear boundaries of criminal jurisdiction on the internet likewise lead to considerable problems regarding the place of jurisdiction, and these are compounded by the inertia of the international mutual assistance process. This creates numerous obstacles for the prosecution of money laundering and terrorist financing using cryptocurrencies, which explain why in many suspected cases of money laundering using cryptocurrencies forwarded by MROS to a public prosecutor's office, a no-proceedings order was issued. The most common reason cited was that, after the preliminary investigations had been completed, it was not possible to identify the beneficial owners of the wallets containing cryptocurrencies of suspicious origin.

3.3. Risk analysis summary

Although the number of suspected cases of money laundering using cryptocurrencies reported to the Swiss authorities has increased, it is still so small that it is difficult to evaluate the associated risk. The few cases could reflect a real but ultimately low risk arising from an expanding but still new technology that is very rarely used for the criminal purposes of money laundering or terrorist financing. The low number of reports could also be due to weaknesses in the clarification of suspicions and the identification of money laundering and terrorist financing cases using tokens. Be that as it may, the major threat posed by cryptocurrencies has been confirmed and Switzerland's vulnerabilities in this area are considerable, even if all countries are affected. In this respect, it should be noted that the unclear boundaries of criminal jurisdiction on the internet pose a particularly high risk, without it being possible to say that this is a specifically Swiss phenomenon. A user who wishes to remain anonymous in order to carry out transactions in connection with a crime pattern, for example, can easily fall back on crypto service providers registered in a country where they are not subject to anti-money laundering legislation or where it is not effectively applied, even if he himself is operating from a country where very strict anti-money laundering regulations apply.

4. Risk mitigating factors

Although the threat posed by cryptocurrencies is high and the vulnerabilities are considerable, there are several risk mitigating factors. Some of these have already been mentioned and are related to the technologies underlying cryptocurrencies. When tokens are stolen or fraudulently diverted, users can identify the wallets to which these assets are transferred and blacklist them, thus preventing any money laundering. Similarly, rookie mistakes made by honest users can also thwart criminals. According to the competent prosecution authorities, the best way to prevent the use of cryptocurrencies for money laundering is for the perpetrators of such crimes to make mistakes that allow them to be identified and, if possible, put out of action. Aside from these factors, which help to reduce the technology-related risks, the Swiss authorities are also striving to develop instruments that are as efficient as possible in order to curb the money laundering and terrorist financing risks associated with cryptocurrencies. Despite the limitations of the national regulation of this transnational problem, these include primarily the particularly far-reaching subjection of financial intermediaries active in the crypto business in Switzerland to the AMLA, although this does not prevent crypto transactions from being conducted predominantly via services that do not come under financial intermediation. Examples include providers of non-custody wallets or decentralised trading platforms that are not subject to the AMLA or are registered abroad.

4.1. Classification of crypto application cases under supervisory law

4.1.1. Initial coin offerings

If tokens issued within the framework of an ICO[76] are actually or are intended to be accepted by the organiser as means of payment for the purchase of goods or services and/or are intended to serve the transfer of money and assets, this constitutes, under anti-money laundering law, the issuance of means of payment subject to such legislation pursuant to Article 2 paragraph 3 letter b of the AMLA in conjunction with Article 4 paragraph 1 letter b of the AMLO.

The AMLA entails various due diligence obligations and the obligation either to join an SRO or to submit themselves to direct AMLA supervision by FINMA. According to FINMA practice, this obligation is deemed to have been complied with if the funds are received by a financial intermediary subject to the AMLA in Switzerland and this financial intermediary complies with the due diligence obligations.

[76] FINMA announced its practice on the classification of ICOs under supervisory law in the guidelines for enquiries about the applicability of regulation regarding initial coin offerings (ICOs) dated 16 February 2018.

The duty to identify the contracting party pursuant to Article 3 of the AMLA is a fundamental principle of money laundering prevention. In principle, the duty to identify applies from CHF 0. However, the AMLO-FINMA, CDB 16 and SRO regulations provide for a complete waiver or simplified identification in a risk-oriented manner for certain transactions and up to certain amount thresholds. For the issuance of means of payment within the framework of an ICO, FINMA provides for the possibility of simplified identification in the case of an investment amount of CHF 0 to CHF 3,000 (simple copy of identity document).[77] Full identification is required only for transactions in excess of CHF 3,000. This simplification is justified by the risks inherent in an ICO. The greatest risk in the case of an ICO is that it is a scam or that the ICO organiser will use the funds to finance terrorism.[78] Another risk is the possibility that funds of criminal origin can be invested in an ICO.[79] By subjecting ICOs in which payment tokens are issued, the AMLA risk is adequately addressed.

It is generally found that ICOs are very similar to traditional financing rounds or private placements by legal entities. However, as token holders generally do not become shareholders or creditors of the company, time consuming and costly documentation (e.g. the obligation to publish a prospectus) and transparency requirements for legal entities can be circumvented upon issuance.

4.1.2. Wallet providers

A wallet provider that holds the customer's private key (custody wallet provider) enables cryptocurrencies to be sent and received and thus provides a service subject to the legislation for payment transactions within the meaning of the AMLA (Art. 2 para. 3 lit. b of the AMLA in conjunction with Art. 4 para. 1 lit. a of the AMLO). The function and risk situation are similar to those of money transmitters. In particular, cryptocurrencies can be used to send assets around the globe quickly and easily. There is a risk that sanctions could thereby be circumvented and terrorists financed.

Corresponding wallet providers must either join an SRO or submit themselves to direct AMLA supervision by FINMA. As wallet providers cannot restrict transactions geographically, there is a general identification duty from CHF 0 according to FINMA practice, like in the case of foreign transfers by money transmitters. Due to the analogy with new payment methods, simplified identification (simple copy of identity document) is also permissible for wallet providers if the wallet provider limits the transaction volume to CHF 500 per month and CHF 3,000 per calendar year.

The subjection of custody wallet providers only partially takes account of the AMLA risks.[80] Most wallet providers do not control customers' private keys (non-custody wallet providers, see section 2.2. above). With the prevailing legal situation, subjection would be possible only with extensive interpretation of Article 4 paragraph 1 letter a of the AMLA, according to which a service related to payment transactions exists if the financial intermediary "orders" the transfer of liquid financial assets in the name and on behalf of the contracting party. FINMA reviewed a corresponding interpretation and concluded that it is incompatible with the classification of the AMLA and the concept of financial intermediation, which refers to the power of disposal over third-party assets.

4.1.3. Exchange offices and centralised trading platforms

In the case of exchange transactions, changers offer the purchase and sale of cryptocurrencies directly from their own holdings. Exchange transactions with cryptocurrencies qualify as financial intermediary activities within the meaning of the AMLA (see Art. 2 para. 3 lit. c of the AMLA in conjunction with Art. 5 para. 1 lit. a of the AMLO).

---

77 In analogous application of Art. 12 para. 2 lit. d of the AMLO-FINMA.

78 See section 3.1.1.c above.

79 See section 3.2.1 above.

80 See MROS case in section 3.2.1, which could not be pursued due to the lack of an identification duty on the part of the wallet provider.

The AMLA risk in the case of cryptobased changers is similar to that in the case of conventional exchange transactions, i.e. lower than in the case of payment transactions, as the assets are only exchanged with the customer and not transferred to third parties. Against this backdrop, FINMA applies the existing identification duty threshold of CHF 5,000 for changers also in the crypto area. Nevertheless, the differentiation between exchange transactions (with the complete waiver of identification up to CHF 5,000 per transaction) and payment transaction services is a challenge in the crypto business. With a conventional exchange transaction at a counter, the financial intermediary can be sure that it is genuinely an exchange transaction, as he sees the person to whom he is handing over the exchange amount directly in front of him. On the internet, in contrast, the changer does not know whether the recipient wallet specified by the customer also belongs to him or whether it is the wallet of a third party (which would result in a transfer, i.e. riskier payment transaction). The cryptobased changer therefore has to take appropriate measures to ensure that there is only a two-party relationship in order to benefit from the higher threshold of CHF 5,000. It is up to the changer to decide how this requirement is implemented.

Unlike exchange offices, centralised trading platforms act as intermediaries between the users of the platform. The traders accept funds or cryptocurrencies from customers and forward them to other users. Such trading platforms qualify as money transmitters and are thus subject to the AMLA. According to FINMA practice, the same threshold applies for trading platforms as for custody wallet providers (see section 4.1.2 above).

4.1.4. Decentralised trading platforms

Unlike centralised trading platforms, decentralised trading platforms allow the processing of pooled orders (after release/confirmation of the trade) on the blockchain directly between the users of the platform.[81] Since a transfer of assets ultimately takes place with the help of the trading platform, the question arises as to whether the platform provides a financial intermediary service for payment transactions within the meaning of the AMLA.

For such a trading platform to be subject to the AMLA, the decisive factor is whether or not the platform operator acquires power of disposal over the cryptocurrencies traded. This is often the case in principle, as the platform has to confirm the orders (in whatever form) or release them for execution in order to ensure orderly trading or has the possibility to block them. In order to ensure that all completed trades can be settled properly, the operator often additionally reserves the right to intervene and not to release user requested repayments of cryptocurrencies held within the framework of the settlement smart contract. According to FINMA practice, decentralised trading platforms are generally subject to the AMLA.

A decentralised trading platform is not subject to the AMLA only if it has no intervention possibility whatsoever regarding the settlement of the trades concluded (e.g. mere provision of an escrow smart contract necessary for settlement without intervention possibilities for the platform). As is the case with non-custody wallet providers, FINMA does not see any possibility of subjecting such trading platforms to the AMLA with the current legal situation.

4.1.5. Mining

In Switzerland, cryptocurrency mining is not subject to authorisation under financial market legislation. With regard to the sale of the cryptocurrencies obtained through mining, there may be a trading activity that is relevant under anti-money laundering law, particularly if trading is carried out on behalf of third parties.

---

[81] The transfer may also be carried out by means of off-chain payment systems. In this case, the payment system or the operator has no power of disposal over the users' assets. The users transfer cryptocurrencies among one another with the help of the payment system infrastructure.

4.1.6. Table showing an overview of the various types of crypto asset services and their subjection to the AMLA

Category of services	Subject to the AMLA	Not subject to the AMLA	Subject to the AMLA under certain conditions
ICOs			Subject to the AMLA when tokens that can be equated to means of payment (payment tokens) are issued during the ICO
Custodian wallet providers	Subject to the AMLA in any case		
Non-custodian wallet providers		Not subject to the AMLA	
Online exchange offices	Subject to the AMLA just like conventional exchange offices		
Centralised trading platforms	Subject to the AMLA in any case		
Decentralised trading platforms			Subject to the AMLA if they have the possibility of intervening in the transactions of their users, e.g. to block a transaction
Miners		Not subject to the AMLA	

4.2. International cooperation

As already mentioned, the Swiss prosecution authorities are relatively powerless against financial crime using cryptocurrencies and, above all, against the danger that these could be used for money laundering and terrorist financing. Criminals always seem to be one step ahead in this area. However, prosecutors can use traditional and very useful instruments, particularly cooperation with their European partners.

The police and judicial authorities agree that international police and judicial mutual assistance is just as effective in prosecuting financial crime using cryptocurrencies as it is in other areas. Thanks to this type of international cooperation, in which the Swiss judiciary and police are extensively involved, the greatest successes have been achieved internationally in the suppression of financial crime using cryptocurrencies and, above all, in the fight against money laundering.[82] These include in particular the closure of the largest illegal marketplaces on darknets such as Silkroad, Hansa and Alpha Bay. The local judicial and police authorities are often involved in these extensive operations, which sometimes lead to convictions in Switzerland.

Conviction of a cybercriminal active on the darknet in Switzerland

As part of coordinated operations by several countries' police and judicial authorities against the online black market Silk Road 2, Switzerland received an international request for mutual assistance regarding a website managed from Switzerland for this illegal market accessible via a darknet. As part of their investigations, foreign police authorities identified the IP address, and the competent cantonal prosecutor initiated criminal proceedings. Finally, internationally coordinated house searches were carried out in several countries at the same time. In Switzerland, it was possible for the server being sought to be confiscated in the apartment where the identified connection was located, and for the developer and webmaster of the website for illegal sales to be identified. The police investigations also revealed that he had offered fictitious illegal goods for sale. In just a few months, he had collected around USD 125,000 in bitcoins, which he had almost completely lost while playing online poker. But he still had around 20 bitcoins from his criminal activity on a wallet. The accused was willing to cooperate with the judiciary and handed over the private key to this wallet, with the result that the amount on it could be confiscated. The accused was then convicted of fraud.

Aside from the provisions of the Federal Act on International Mutual Assistance in Criminal Matters (IMAC, SR 351.1), the Council of Europe Convention on Cybercrime, approved by the Federal Assembly and implemented by federal decree of 18 March 2011[83], provides an important legal basis for regulating judicial and police cooperation in this area. In particular, it allows the police of the various signatory states to contact foreign companies directly in order to obtain the data necessary for their investigations (Art. 32). The requested companies are not obliged to respond to such requests, but according to the competent police authorities, several of them are actively working on such procedures, provided that the national legislation to which they are subject permits this. Moreover, thanks to this legal instrument, the requested companies can be obliged to keep the data that was the subject of the request extra carefully with a view to a proper request for mutual assistance even in the event of refusal to provide information. According to the competent police authorities, this instrument has proved to be extremely important. Furthermore, practice has shown that the requested companies can send suspicious activity reports to their FIU based on such requests if they are financial intermediaries. This information can then be spontaneously transmitted to MROS.

The opposite also applies: Swiss intermediaries contacted by foreign police forces under Article 32 of the Council of Europe Convention on Cybercrime do not always respond directly, but always provide the requested information to MROS, which forwards it to its foreign partners. Furthermore, MROS sends its foreign partners requests for information and unsolicited information on suspected cases of money laundering using cryptocurrencies. At present, however, it is still too early to evaluate the results.

---

82 "Significant law enforcement actions", in European Parliament, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, May 2018, p. 85, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

83 https://www.admin.ch/opc/de/official-compilation/2011/6293.pdf.

4.3 Technological progress in favour of prosecution authorities

With the current state of technology, chain analysis tools are only of partial assistance for investigators tracking money laundering and terrorist financing using cryptocurrencies. But this could change quickly. Several research projects are giving rise to hopes that significant progress will be made in this area in the near future. For example, several companies are currently developing IT tools to reconstruct the paper trail of crypto transactions using mixer/tumbler services. At the international level, Switzerland is also participating in the TITANIUM project (Tools for the Investigation of Transactions in Underground Markets), in which computer researchers and prosecution authorities from several countries are working together under the leadership of INTERPOL. The aim of this project is to develop a tool to improve the transparency of crypto transactions on darknet markets. In particular, a simultaneous analysis of blockchains of different cryptocurrencies is to be used in order to break the anonymity of their users.[84]

4.4 Miscellaneous

In addition to the measures mentioned above, several authorities have taken various initiatives to combat financial crime using cryptocurrencies and, above all, money laundering and terrorist financing more effectively. These include efforts to train the authorities concerned, for example. As a result, public prosecutors, police officers and MROS financial analysts are becoming increasingly aware of the problem of cryptocurrencies and the associated potential crime. Police officer training includes cybercrime courses offered by the Swiss Police Institute. Such an approach is particularly important, not only because comprehensive expertise in this area is essential to understand the technical possibilities of cryptocurrency technologies for money laundering and terrorist financing, but also for suppressing them. These approaches, which are still in their infancy, should be systematised and deepened. In this respect, the establishment of brigades specialising in cybercrime in the various cantonal police forces is an important step forward.

Another example of an initiative in the fight against money laundering and terrorist financing risks in connection with cryptocurrencies is the formation of a working group on this topic within the Office of the Attorney General of Switzerland. Several cantonal public prosecutor offices have also set up pools of public prosecutors specialising in such issues.

All these initiatives culminated in the creation of a national platform for judicial and police cooperation – the Cyberboard – in the summer of 2018, to which representatives of the most important players in the fight against cybercrime in Switzerland belong: CCJPD, CCPCS, Conference of Swiss Public Prosecutors (CSPP), fedpol, Office of the Attorney General of Switzerland, Swiss Crime Prevention (SCP), SSN, FIS and FITSU. The modular platform is intended to enable these players to work together and coordinate their actions in order to combat cybercrime more efficiently. For example, the first module, Cyber CASE, brings together public prosecutors and cantonal and federal police officers specialising in cybercrime, as well as representatives of MELANI. This module, which has been active since 6 July 2018, has the task of ensuring coordination in operational cases between public prosecutor offices and the federal and cantonal police as well as the exchange of experience and knowledge.

The Federal Gaming Board (FGB) is likewise keeping an eye on the problem of money laundering using crypto assets, as it could affect casinos. This hitherto non-existent threat could emerge with the lifting of the ban on online gaming, which the Swiss people approved on 10 June 2018 with their approval of the new Federal Act on Gambling. Within the framework of the FGB's supervision of such online games, it will become clear whether specific measures need to be taken against any misuse of cryptocurrencies in this area. Under Article 76 paragraph 2 of the draft Gambling Ordinance (GamblO), which is currently under consultation with a view to its approval by Parliament, the FGB has the power to prohibit certain means of payment. The FGB is thus reserving the right to make use of this for certain cryptocurrencies should it prove necessary.

---

[84] https://www.interpol.int/News-and-media/News/2017/N2017-069.

5. Crowdfunding platforms

5.1. Types

Even before the advent of ICOs, money was collected on the internet via crowdfunding platforms. The term crowdfunding refers to the financing of a project by a large number of donors. The aim is to have the masses finance projects, which borrowers usually post on the internet on a crowdfunding platform. A crowdfunding platform is basically responsible for operating the crowdfunding website and enabling the associated project posting, coordination and bringing together of donors and borrowers. Depending on the business model, the platforms perform various (further) activities. Many platforms accept funds and pass them on, for example. In some cases, this does not happen until a certain total sum has been reached within a certain period of time. If the total sum is not reached by the deadline, the platforms usually have an obligation to return the money to the donors. There are different forms of support provided through crowdfunding (definitions and terms vary or other terms may be used):

a) Crowddonating: Donors make a certain amount available to borrowers as a donation without consideration. The money provided is not expected to be refunded.

b) Crowdsupporting: Donors make a certain amount available to borrowers as a donation for non-material or only minor consideration (e.g. a signed copy of the CD produced). The money provided is generally not expected to be refunded.

c) Crowdlending (participation in debt capital): In this form, both the refund of the transferred money and regular interest payments are agreed. Under private law, these are loan agreements.

d) Crowdinvesting (provision of equity capital): This is a form of company financing where participation rights are promised in return for the transfer of the money and, if applicable, a share in the success.

The more recent appearance of ICOs is also basically crowdfunding. In practice, the differences lie in the fact that there is usually a platform (intermediary) between donors and borrowers with classical crowdfunding, and the funds are transferred in fiat money. In the case of ICOs, a platform is not usually used as an intermediary, and instead the donors pay directly to the borrower. In addition, the sum of money is often – but by no means always – accepted in cryptocurrencies.

5.2. Risk analysis

Like with crypto assets, it is currently difficult to evaluate the risk of money laundering and terrorist financing with online crowdfunding platforms, as the number of cases recorded by the Swiss authorities is very small. Nevertheless, the threats of such platforms are evident. They result from anonymity, which is exacerbated by the fact that these platforms operate on the internet. Crowdfunding platforms enable participation in projects beyond national borders.[85] The threats posed by crowddonating are especially pronounced. Funds can be raised by fraudulent non-profit organisations through social media or formal crowddonating platforms under the guise of humanitarian aid. As shown by several reports to MROS, such fundraising can be tantamount to investor fraud, just like ICOs, if the project allegedly to be financed is not implemented at all and the organisers keep the donations for themselves. The main threat,

[85] ADVANCED FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Financial Institutions and Crowdfunding*, K.M. Veldhuizen-Koeman, 2016, p. 6 et seq., http://files.acams.org/pdfs/2016/Financial_Institutions_and_Crowdfunding_K_Veldhuizen.pdf).

however, is that the money raised can be used as material support for foreign terrorist fighters (for airline tickets, mobile communications, etc.) or as funds for carrying out terrorist attacks.[86]

The FATF report on Emerging Terrorist Financing Risks states that donors are often unaware of what the money they donate through social media (including crowdfunding platforms) is ultimately used for, which is a risk that terrorist organisations can exploit.[87] The threat of terrorist financing is likely to increase in the short term as the popularity of these systems grows and they become more widely used. While transactions may be traceable, identifying the actual end user or beneficiary is difficult if the crowdfunding platform does not perform KYC duties. According to the FATF, the extent to which terrorist groups and their supporters exploit these technologies is currently unclear. The use of organised crowdfunding techniques constitutes an emerging terrorist financing risk. Crowdfunding runs the risk of being used for illegal purposes, even in cases where a false purpose is stated for a funding campaign. Individuals and organisations that wish to raise funds in support of terrorism and extremism may claim to be engaged in legitimate charitable or humanitarian activities and establish non-profit organisations for this purpose. The FATF shows in a case study that the Canadian FIU has examples that individuals investigated in connection with terrorist crimes attempted to leave the country for terrorist purposes and used crowdfunding websites beforehand to do so.

The French Tracfin points to the considerable risks of terrorist financing using crowddonating. It also describes a case where the analysis of a crowddonating platform revealed that certain cash flows came from sensitive geographical areas and that the total amount was donated unusually rapidly relative to the nature of the project financed. Some of the projects on this platform appeared to have links with radical Islamists.[88] With the entry into force of the "Ordonnance n°2016-1635 du 1er décembre 2016 renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme" at the end of 2016, the status as "intermédiaire en financement participatif" is no longer optional, and is instead mandatory for so-called "plateformes de dons", i.e. crowddonating platforms. These now have to comply with the rules on combating money laundering and terrorist financing.[89]

Furthermore, the Association of Certified Anti-Money Laundering Specialists ACAMS reported on a case in which two people of a French charity campaign were accused of terrorist financing in Syria. The campaign site collected money for Syrian children, among others. Although food and medical supplies were delivered to Syria, many of these supplies were also used to provide funds to jihadist groups. According to ACAMS, the number of reports of illegal activities related to crowdfunding sent to the US agency FinCEN is still low, but it is steadily increasing. The review and analysis of these reports shows that crowdsupporting platforms in particular are used for money laundering purposes.[90]

There are no known cases of crowdfunding platform abuse in Switzerland to date. MROS has not received any corresponding reports. However, this could also be due to the fact that many platforms are not currently subject to the AMLA and are unable to submit reports. Some major crowddonating and crowdsupporting platforms not subject to the AMLA active on the market nevertheless subject the registered projects and the borrowers to a prior examination. These aspects constitute a real vulnerability for Switzerland in this area.

---

86 See on terrorist financing: FATF, *Emerging Terrorist Financing Risks*, October 2015 (http://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf).

87 *Ibid.*, p. 6, 31 et seq.

88 TRACFIN, *Tendances et analyse de risques de blanchiment de capitaux et de financement du terrorisme en 2015*, 2015, https://www.economie.gouv.fr/tracfin/tendances-et-analyse-des-risques-en-2015.

89 See Art. L548-2, II and Art. L561-2, 4° of the Monetary and Financial Code, https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026.

90 ADVANCING FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Crowdfunding: The New Face of Financial Crime?*, Financial Institutions and Crowdfunding, 2017, p. 14 et seq., http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf.

5.3. Risk mitigating factors

The subjection obligation under the AMLA is regulated, inter alia, in Article 2 paragraph 3 of the AMLA and in the Anti-Money Laundering Ordinance (AMLO; SR 955.01). This includes persons who on a professional basis accept or hold on deposit assets belonging to others or who assist in the investment or transfer of such assets; they include in particular persons who provide services related to payment transactions (Art. 2 para. 3 lit. b of the AMLA). A service related to payment transactions exists in particular if the financial intermediary transfers liquid financial assets to a third party on behalf of the financial intermediary's contracting party and thereby physically takes possession of these assets, has them credited to the financial intermediary's own account or orders the transfer of the assets in the name and on behalf of the contracting party, or if the financial intermediary carries out the money or asset transfer transaction (Art. 2 para. 3 lit. b of the AMLA in conjunction with Art. 4 of the AMLO; see also FINMA Circular 2011/1, para. 58). If there is a service related to payment transactions and if the financial intermediary is operating on a professional basis (Art. 7 of the AMLO), the financial intermediary must comply with the due diligence obligations under Articles 3 to 7 of the AMLA.

Collection activities are not regarded as financial intermediation. Collection is based on a bilateral or multilateral legal transaction in which the collection agent is generally not involved. The person entrusted with collection collects due receivables on behalf of the creditor. The agent acts either as a direct representative of the creditor or in his own name vis-à-vis the debtor. Making the collection activity subject to the AMLA would generally be largely pointless, as collection firms could not be obliged to identify the debtors in accordance with Article 3 of the AMLA due to the lack of a contractual relationship with them.[91] Exceptionally, the agent has contractual relationships with both the creditor of the receivable and the debtor. According to FINMA Circular 2011/1 paragraph 9, collection activity may nevertheless exist in such cases. The decisive factor is on whose behalf the transfer or forwarding is carried out, and this has to be ascertained based on indications. The service is typically paid for by the instructing party.

Since crowdfunding platforms generally accept third-party funds and pass them on to the projects to be financed, there is basically a service for payment transactions subject to the legislation (see Art. 2 para. 3 lit. b of the AMLA in conjunction with Art. 4 para. 1 lit. a of the AMLO). In the current legal environment, however, it is possible to operate crowddonating platforms without authorisation. In particular, operators of crowddonating and crowdsupporting platforms can claim the collection exception pursuant to Article 2 paragraph 2 letter a number 2 of the AMLO. In Switzerland, therefore, only crowdlending and crowdinvesting platforms (i.e. donors receive interest or dividends) have generally been subject to the Anti-Money Laundering Act (Art. 2 para. 3 of the AMLA), as the money on these platforms flows in both directions between donor and borrower, and thus there can be no collection order from the donor alone. The other platforms are generally designed in such a way (particularly concerning their general terms and conditions and cash flows) that they can make use of the collection exception pursuant to Article 2 paragraph 2 letter a number 2 of the AMLO.

On 1 August 2017, simplifications for financial market participants were included in the Banking Ordinance and crowdfunding can benefit greatly from these too.[92] However, the amendments have no impact on the applicability of the AMLA to crowdfunding platforms.[93]

---

91 See FINMA Circular 2011/1, para. 8; practice of the Anti-Money Laundering Control Authority regarding Art. 2 para. 3 of the AMLA of 29 October 2008, para. 4.1, p. 31 (https://www.finma.ch/FinmaArchiv/gwg/d/dokumentationen/publikationen/gwg_auslegung/pdf/59402.pdf), which served as the basis for the PFIO; BGE 2A.62/2007, ext. 8.

92 "If a crowdfunding platform operator accepts funds on a commercial basis and, rather than forwarding them to the project developer within 60 days (prior to 1 August 2017 the maximum period allowed in practice was 7 working days), holds them for some time (in order, for instance, to ensure that the amount is available at the end of a lengthy collection period), a licence under the Banking Act must be obtained prior to taking up business. From 1 August 2017, a licence is no longer required in such cases if the funds accepted for forwarding do not exceed CHF 1 million, as this is no longer regarded as commercial activity. However, before transferring the funds to the platform, project financers must be made aware that the platform is not supervised by FINMA and their deposits are not protected." (FINMA crowdfunding factsheet, as at 1 August 2017).

93 Explanations on the amendment of the Banking Ordinance (Fintech) of the Federal Department of Finance (FDF) of 5 July 2017, section 1.1.3.

6. Conclusions/recommendations

6.1. Conclusions from the analysis of the risks posed by crypto assets

The threat of money laundering and terrorist financing using crypto assets is high, even though the number of proven cases in Switzerland has been limited so far. It is based on the anonymity of token transactions and is reflected both in the criminal exploitation of design errors in cryptocurrencies and in investor fraud, particularly in the case of ICOs and the use of cryptocurrencies for ransomware payments. However, the use of cryptocurrencies poses a threat also in other crime patterns: terrorist financing, laundering of funds from the sale of illegal services and products, phishing scams or drug trafficking, especially by criminal organisations. Cryptocurrencies are particularly well suited for money laundering because of their anonymity.

In Switzerland, the number of cases in which tokens were demonstrably used for money laundering is not very high and even zero in the area of terrorist financing. The risk associated with cryptocurrencies is thus difficult to evaluate, but Switzerland's vulnerability to this threat is considerable, even if it is not specific to the Swiss financial centre.

Due to the anonymity of crypto transactions, the identification of tokens of criminal origin and their beneficial owners is extremely complicated for prosecution authorities and financial intermediaries dealing with them. The decentralised structure of cryptocurrency technologies means that a great many transactions are not subject to any control: these technologies allow for anonymous cryptocurrency trading and exchange without financial intermediaries and often without it being possible to determine from which country the transactions were ordered. This underlines the crucial responsibility of platforms for exchanging fiat money and crypto assets: at present, they appear to be the only financial intermediaries able to exercise their due diligence obligations towards their customers, even if these precautionary measures have only a limited effect.

While legal adjustments to reduce the risk of money laundering and terrorist financing associated with cryptocurrencies could be considered[94], the Swiss authorities have been able to adapt the instruments already available to them under existing legislation. Thus, all companies offering financial intermediary services in the token area are subject to the AMLA, even the providers of custodian wallets, decentralised trading platforms that can intervene in transactions ordered by their customers, and certain ICOs that do not come under financial intermediation in other countries. Nonetheless, the providers of non-custodian wallets and decentralised platforms which are unable to intervene in their customers' transactions escape the anti-money laundering system. Moreover, not all financial intermediaries subject to the AMLA are equally aware of their due diligence obligations.

The prosecution authorities are also striving to punish crime in connection with cryptocurrencies with the means at their disposal. International cooperation and judicial and police mutual assistance with their foreign counterparts are undoubtedly among the most important instruments. However the speed of transactions, which allow tokens of criminal origin to be moved from one place in the world to another within seconds and with just a few clicks without the initiators having to get up from their computers, often makes this cooperation futile.

Due to the transnational nature of the dangers of money laundering and terrorist financing using cryptocurrencies, the most important measures to reduce the associated risk must be coordinated at the international level, even if the extent of this risk has been difficult to evaluate so far. Switzerland's commitment within the FATF to the international harmonisation of regulations for companies involved in crypto asset trading and transactions is an appropriate response to this challenge. Without such harmonisation, any request for mutual assistance abroad would run the risk of being pointless. In

[94] See recommendations in the *Federal Council report on legal framework for distributed ledger technology and blockchain in Switzerland*, 14 December 2018, https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf.

addition, any tightening of Swiss legislation could be counterproductive and simply lead to new activities subject to new due diligence requirements leaving Switzerland and moving to another country.

Aside from Switzerland's involvement on the international stage, several national and cantonal initiatives are also helping to reduce the risk of money laundering and terrorist financing using crypto assets as far as possible. The most important is the creation of the Cyberboard in June 2018: a national platform for judicial and police cooperation in the field of cybercrime. However, the training of Swiss police officers in the field of economic cybercrime, the creation of a specialised working group within the OAG and the cantonal police forces' brigades specialising in financial cybercrime are also important steps forward. Combined with the close judicial, police and administrative cooperation between Switzerland and foreign states, they are the strongest weapons in the fight against the increased threat posed by crypto assets in the area of money laundering and terrorist financing.

6.2. Conclusions and recommendations regarding the analysis of the risks posed by crowdfunding platforms

The risk associated with online crowdfunding relates mainly to terrorist financing. The Swiss authorities have not recorded any such cases to date, but Switzerland has weaknesses in this area that would be worth remedying.

The current regulations do not take adequate account of the risks identified. An adjustment at regulatory level has to be examined. The explicit subjection of crowddonating and crowdsupporting platforms to the AMLA is at the forefront here. Without such an adjustment, platforms that collect money (intermediaries), unlike crowdlending and crowdinvesting platforms, would be exempt from the AMLA, while those that collect money for themselves (ICOs) may already be subject to the AMLA under certain circumstances (issue of a payment token). In its design, however, the AMLA is linked to the control of cash flows involving intermediaries. Moreover, this would not prevent the risk of misappropriation and misuse of the funds collected.

7. Bibliography

ADVANCED FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Financial Institutions and Crowdfunding*, K.M. Veldhuizen-Koeman, 2016, http://files.acams.org/pdfs/2016/Financial_Institutions_and_Crowdfunding_K_Veldhuizen.pdf).

ADVANCING FINANCIAL CRIME PROFESSIONALS WORLDWIDE (ACAMS), *Crowdfunding: The New Face of Financial Crime?*, Financial Institutions and Crowdfunding, 2017, p. 14 *et seq*., http://files.acams.org/pdfs/2017/Crowdfunding_The_New_Face_of_Financial_Crimes_S.Sessoms.pdf.

AL JAWAHERI Husam, AL SABAH Mashael, BOSHMAF Yazan and ERBAD Aiman, "When a small leak sinks a great ship: deanonymizing Tor hidden service users through bitcoin transactions analysis", in *arXiv*: 1801.07501v2, April 2018, https://arxiv.org/abs/1801.07501.

ANONYMOUS, "Singapour: les premiers billets Bitcoins visent à favoriser l'adoption de l'actif", in *Crypto-France.com*, https://www.crypto-france.com/singapour-premiers-billets-bitcoin/.

ANONYMOUS, "Ils minaient des bitcoins dans un centre nucléaire", in *La Tribune de Genève*, 10 February 2018, https://www.tdg.ch/faits-divers/Ils-minaient-des-bitcoins-dans-un-centre-nucleaire/story/30448246.

ANONYMOUS, "Bitcoin Gold: une attaque double dépense fait perdre plusieurs millions de dollars à des plateformes d'échanges", in Crypto-France, https://www.crypto-france.com/bitcoin-gold-attaque-double-depense-pertes-millions-dollars-plateformes-echange/.

ANONYMOUS, "670 millions de dollars de crypto-monnaies ont été dérobés au cours du premier trimestre 2018", in *Crypto-France.com*, April 2018, https://www.crypto-france.com/670-millions-dollars-crypto-monnaies-voles-premier-trimestre-2018/.

ANONYMOUS, "Cryptomonnaie: la plateforme japonaise Coincheck victime d'un vol record", 29 January 2018, http://www.rfi.fr/economie/20180129-coincheck-vol-cryptomonnaie-injonction-japon.

ANONYMOUS, "Coincheck: les pirates servaient déjà parvenus à blanchir 40% des 500 millions de XEMs dérobés", https://www.crypto-france.com/coincheck-pirates-blanchiment-xems/.

BRANTLY Aaron, "Financing Terror Bit by Bit", in *CTC Sentinel*, vol. 7, no. 10, October 2014, p. 4, https://ctc.usma.edu/financing-terror-bit-by-bit/.

CGMF, *Report on the use of cash and its risks of abuse for money laundering and financing of terrorism in Switzerland,* October 2018, https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73465.html

DE PREUX Pascal and TRAJILOVIC Daniel, "Blockchain et lutte contre le blanchiment d'argent. Le nouveau paradoxe ?", in *Resolution LP*, https://resolution-lp.ch/wp-content/uploads/2018/02/064_L_14_De_Preux_Trajilovic.pdf.

European Parliament, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, May 2018, http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf.

EUROPOL, *2017 Virtual Currencies Money Laundering Typologies*, 2017.

FANUSIE Yaya and ROBINSON Tom, *Bitcoin laundering: an analysis of illicit flows into digital currency services*, Center on Sanctions & Illicit Finance et ELLIPTIC, 12 January 2018.

FARINE Mathilde, "Comment investir dans les cryptomonnaies", in *Le Temps*, 22 July 2018, https://www.letemps.ch/economie/investir-cryptomonnaies.

FARINE Mathilde, "La FINMA enquête sur une ICO à 100 millions de francs", in *Le Temps*, 26 July 2018, https://www.letemps.ch/economie/finma-enquete-une-ico-100-millions-francs.

FAUCETTE James, GRASECK Betsy and SHAH Sheena, *Update: Bitcoin, Cryptocurrencies and Blockchain*, Morgan Stanley, 1 June 2018, p. 35, https://www.macrobusiness.com.au/wp-content/uploads/2018/06/82012860.pdf.

FATF, *National Money Laundering and Terrorist Financing Risk Assessment*, 2013, http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf.

FATF, *Virtual currencies. Key definitions and potential AML/CFT risks*, June 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

FATF, *Virtual currencies. Guidance for a risk-based approach*, 2015, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

FATF, *FATF Fintech & RegTech Initiative*, http://www.fatf-gafi.org/fintech-regtech/?hf=10&b=0&s=desc(fatf_releasedate).

Federal Council, *Federal Council report of 25 June 2014 on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates*, https://www.news.admin.ch/NSBSubscriber/message/attachments/35353.pdf.

Federal Council, *Federal Council report of 14 December 2018 on legal framework for distributed ledger technology and blockchain in Switzerland*, https://www.newsd.admin.ch/newsd/message/attachments/55153.pdf

FINMA, Press release of 19 September 2017, https://www.finma.ch/fr/news/2017/09/20170919-mm-coin-anbieter/.

FINMA, Press release of 26 July 2018, https://www.finma.ch/fr/news/2018/07/20180726-mm-envion/?pk_campaign=News-Service&pk_kwd=La%20FINMA%20ouvre%20une%20proc%C3%A9dure%20%C3%A0%20l%27encontre%20d%27un%20%C3%A9metteur%20d%27ICO.

GARESSUS Emmanuel, "Une société suisse veut émettre des billets de bitcoins", in *Le Temps*, 8 May 2018, https://www.letemps.ch/economie/une-societe-suisse-veut-emettre-billets-bitcoins.

GRÜNEWALD Seraina, "Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen", in Rolf H. Weber et al. (ed.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, ZIK vol. 61, Zurich/Basel/Geneva 2015.

HAEDERLI Alexandre and STÄUBLE Mario, "De la drogue livrée en courrier A. Comment fonctionne le marché des trupéfiants sur le Darknet", in *La Tribune de Genève*, 02.05.2018, https://www.tdg.ch/extern/interactive_wch/darknet/.

HESS Martin and SPIELMANN Patrick, "Crypocurrencies, Blockchain. Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht", in: Reutter, Thomas U. / Werlen, Thomas (Hrsg.): Kapitalmarkt – Recht und Transaktionen XII. Zurich: Schulthess 2017, p. 154.

HILEMAN Garrick and RAUCHS Michel, *Global Cryptocurrency Benchmarking Study*, Cambridge, Centre for Alternative Finance/University of Cambridge, 2017.

HM Treasury and Home Office, *National risk assessment of money laundering and terrorist financing 2017*, London, 2017, p. 38, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.

IRWIN Angela S.M. and MILAD George, "The use of crypto-currencies in funding violent jihad", in *Journal of Money Laundering Control*, vol. 19, no. 4, 2016, pp. 410-411.

Koos Couvée, "European traffickers pay Colombian cartels through bitcoin ATMs: Europol Official", in ACAMS Moneylaundering.com, 28 February 2018, https://www.moneylaundering.com/news/european-traffickers-pay-colombian-cartels-through-bitcoin-atms-europol-official/.

LOUBIRE Paul, "La très longue liste de vols de bitcoins par des hackers", in *Challenges*, 08.12.2017, https://www.challenges.fr/finance-et-marche/la-tres-longue-liste-de-vols-de-bitcoins-par-des-hackers_518541.

MEISSER Luzius, "Kryptowährungen: Geschichte, Funktionsweise, Potential", in WEBEER Rolf H. *et al.* (ed.), Rechtliche Herausforderung durch webbasierte und mobile Zahlungssysteme, ZIK vol. 61, Zurich/Basel/Geneva 2015.

Monetary and Financial Code, consolidated version of 1 October 2018, https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006072026.

SANSONETTI Riccardo, "Bitcoin: Virtuelle Währungen mit Chancen und Risiken", in Die Volkswirtschaft, 9-2014, pp. 44-46.

SUBERG William, "Bitcoin exchange ShapeShift helps police as WannaCry attacker converts to monero", in https://cointelegraph.com/news/bitcoin-exchange-shapeshift-helps-police-as-wannacry-attacker-converts-to-monero.

TRACFIN, *Tendances et analyse de risques de blanchiment de capitaux et de financement du terrorisme en 2015*, 2015, https://www.economie.gouv.fr/tracfin/tendances-et-analyse-des-risques-en-2015.

TZANETAKIS Meropi, “Comparing cryptomarkets for drugs: a characterisation of sellers and buyers over time”, in *International Journal of Drug Policy*, vol. 56, June 2018, pp. 176-186.

U.S. Department of Justice and Drug Enforcement Administration, *2017 National Drug Threat Assessment*, October 2017.

US Securities and Exchange Commission, https://www.sec.gov/news/statements.

WILE Rob, "Supporter of extremist group ISIS explains how bitcoin could be used to fund Jihad", in *Business Insider Australia*, 8 July 2014, https://www.businessinsider.com.au/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7.