Cryptocurrencies and financial crime: solutions from Liechtenstein

Fabian Maximilian Johannes Teichmann and Marie-Christin Falker
Teichmann International (Schweiz) AG, St. Gallen, Switzerland

Abstract

Purpose – The purpose of this paper is to illustrate how cryptocurrencies are being used as a vehicle for financial crime (such as money laundering, terrorist financing and corruption) and propose a more effective international standard for regulation that uses the Liechtenstein blockchain act as a benchmark.

Design/methodology/approach – This paper investigates how cryptocurrencies facilitate financial crime through a qualitative study consisting of interviews with 10 presumed providers of illegal financial services and 18 international compliance experts.

Findings – This study shows that cryptocurrencies are a highly suitable vehicle for money laundering, terrorist financing and corruption and that current compliance efforts in the cryptocurrency sector are ineffective.

Research limitations/implications – The presented findings illustrate that for a more effective combat of financial crime via cryptocurrency, an international standard for blockchain and cryptocurrency regulation must be created. This paper suggests that Liechtenstein's innovative and comprehensive blockchain act could be used as a basis for said standard. Practitioners should also consider cooperating transnationally when prosecuting financial crime via cryptocurrency.

Originality/value – The fact that cryptocurrencies facilitate financial crime is widely known. However, this study combines the perspectives of both compliance experts and presumed criminals to gain a comprehensive understanding of the techniques that money launderers, terrorist financiers and corrupt public officials use. This paper examines the potential for the innovative Liechtenstein blockchain act, which has, thus, far not received empirical attention, to set the benchmark for international regulations.

Keywords Corruption, Money laundering, Terrorist financing, Bitcoin, Blockchain, Corruption, Financial crime, Liechtenstein blockchain act, Cryptocurrency

Paper type Research paper

1. Introduction

As the launch of Bitcoin in 2008, cryptocurrencies have been criticized for allegedly facilitating financial crime. This claim has been substantiated by various studies and hard data such as trading volumes (Choo, 2015; Mabunda, 2018; Teichmann and Falker, 2020). Cryptocurrencies are not managed or overseen by a trusted third party and permit high anonymity. An additional challenge of innovative technologies is that they frequently evolve quicker than the appropriate legal framework that regulates them, meaning that it does not only take a long time to introduce adequate regulations but also that these regulations are in danger of becoming outdated soon after entering into force. For instance, Facebook's announced stablecoin Libra uses technologies that are highly different from Bitcoin (van Valkenburgh, 2019). When regulators create legal frameworks that relate to cryptocurrencies such as Bitcoin, by the time these legislations enter into force, new projects such as Libra may have emerged, which might require novel regulations.

Journal of Money Laundering Control

1368-5201
DOI 10.1108/JMLC-05-2020-0060

This article explains how cryptocurrencies function and details the risk factors that facilitate the financial criminal activities associated with them. To contribute to the existing literature on compliance concerns surrounding the digital currency, a qualitative study consisting of interviews with 10 presumed providers of illegal financial services and 18 compliance experts was conducted. In particular, the presumed criminals were interviewed informally within the scope of a pre-study that aimed to investigate how cryptocurrency could potentially facilitate financial crime based on the interview partners' expertise and experiences. Their statements were contrasted with those of compliance experts that were interviewed during the main study. The intention was to gain a comprehensive overview that considers both perspectives. This study found that cryptocurrencies continue to represent a risk factor for financial crime, which means that the current national regulations are rather ineffective. This article argues that only when an international standard is established can the dangers of cryptocurrency be mitigated and it proposes that the newly introduced Liechtenstein blockchain act (2019) can act as a potential benchmark for said international legal framework.

2. Literature review

2.1 Cryptocurrency

Cryptocurrencies are virtual currencies that operate in blockchain-based, decentralized systems. In contrast, governmental fiat currencies are issued by central banks and centralized, which means that all transactions conducted using fiat are recorded on a central server that ensures there is no double-spending. Customers usually trust this system because it is based on universally accepted rules and appropriately regulated by legislation. Centralization makes it possible not only to regulate currencies and transactions but also to monitor them so that compliance guidelines can be followed. Traditional banks are obligated to conduct customer due diligence (CDD), which includes know-your-customer (KYC) and anti-money laundering (AML) procedures. These procedures entail the identification of beneficial owners, the intended business relationship, the origin of funds and more.

Cryptocurrency transactions are conducted peer to peer (P2P) without the intervention of financial intermediaries (Nakamoto, 2008). Consequently, most crypto transactions are not subjected to KYC and AML procedures (Campbell-Verduyn, 2018). In addition, the values of state-issued currencies are usually rather stable, as they are controlled via monetary policy, whereas the values of cryptocurrencies like Bitcoin are often determined by supply and demand (Bitcoin Project,2009–2020), making them more volatile. Digital currencies that are supposed to be stable in value, so-called "stablecoins," are backed by gold, fiat or other assets. These stablecoins are usually powered by blockchain, but only certain entities have access to the network and control it (Memon, 2020).

"Traditional" decentralized cryptocurrencies such as Bitcoin are not controlled by a central entity (Government Office for Science, 2016). Instead, all transactions are recorded on the blockchain. It functions as a public ledger by making these records available for everyone to access (Grünewald, 2015). The blockchain consists of computers that can be located anywhere in the world. These so-called "nodes" download the blockchain either partially or fully. The nodes that download the entire blockchain validate transactions (Bheemaiah, 2015). This process is called "mining" and simultaneously creates new coins (Antonopoulos, 2015; Essebier and Wyss, 2017). Although regulations of cryptocurrency vary significantly between jurisdictions (Farell, 2015), mining operations are generally unconstrained by national borders (Hileman and Rauchs, 2017). To be eligible for mining, users must solve an extremely complex mathematical problem ("proof of work") that

requires significant, expensive computing power. Mining creates trust in the system because hackers are unlikely to undertake the effort of solving a proof of work, as it would likely be unprofitable (Tuwiner, 2019).

Crypto transactions are highly anonymous. Paradoxically, they are also transparent (Ponsford, 2015). For each transaction, the time, date, value and usernames ("public key") of the transacting peers are recorded (Schmid and Schmid, 2012). The public key functions as the address to which other peers send coins. Peers have a second key, a "private key," which allows them to authorize transactions and access their coins. These coins are stored in a software program called an "e-wallet." As all transaction details are recorded in a block, this provides transparency. However, most cryptocurrency purchases do not require identification. Therefore, it is only possible to connect public keys to their beneficial owners if the owner uses them to purchase something in the analog world.

2.1.1 Risks and abuses of cryptocurrency. The blockchain's risk-enhancing features mainly pertain to its global nature, the general lack of regulation and the high anonymity of crypto transactions. Anonymity in particular is likely the most widely criticized feature of cryptocurrencies (Dostov and Shust, 2014). Dostov and Shust (2014) differentiate between "anonymity as privacy" and "anonymity as hidden identity" (p. 258). While users that appreciate cryptocurrencies for their privacy intend to minimize intrusions into their personal life, criminals require anonymity to conceal their identity to avoid tracking by the authorities (Dostov and Shust, 2014). Cryptocurrency's overall reputation has largely been shaped by criminals' "embrace of the technology" (Chainalysis Team, 2020, p. 5).

A criminal prosecution of money laundering or terrorism financing can be significantly complicated by transfers of funds across multiple jurisdictions. The fact that criminals using cryptocurrency are unconstrained by geographical boundaries facilitates the establishment of digital accounts and identities worldwide (Houben and Snyers, 2018). That is why it is so important to introduce international regulatory standards. It is estimated that between 2009 and 2018, around US$2.5bn was laundered via Bitcoin alone (Canellis, 2018). However, data on illicit activity via cryptocurrency are not reliable and one can assume that a large number of cases go undetected because they involve false identities or unregistered businesses (Foley *et al.*, 2018; Hutchings and Holt, 2017).

In its 2020 crypto crime report, blockchain analysis company chainalysis defined three common threads that link all categories of crypto crime:

(1) crypto crime is becoming increasingly similar to white-collar crime with the majority of incriminated cryptocurrency ending up in the hands of a "small but powerful segment of criminals" (Chainalysis Team, 2020, p. 7);

(2) money laundering is the common denominator behind all crypto crime; and

(3) scams represented the highest-earning category of crypto crime in 2019.

One of the most popular destinations for incriminated Bitcoins are exchanges. In particular, US$2.8bn in Bitcoin were transferred from criminal entities to exchanges during 2019 (Chainalysis Team, 2020).

Chainalysis Team (2020) finds that many illicit Bitcoin transactions are facilitated by over-the-counter (OTC) brokers. OTC brokers facilitate trades between individual sellers and buyers who do not want to transact on an open exchange. They typically operate individually while being associated with a certain exchange. Traders frequently use OTC brokers to trade large amounts of cryptocurrency at a fixed price. According to Chainalysis Team (2020), some of these OTC brokers specialize in the provision of money laundering services by offering much lower KYC requirements than exchanges. One popular method

that is used by OTC brokers to launder money is the exchange of cryptocurrency into a stable intermediary currency such as Tether, before exchanging the funds into fiat. These money laundering structures driven by OTC brokers enable nearly every other form of crypto crime (Chainalysis Team, 2020). When it comes to risks for the money launderer, the main issues include potential loss of assets from scams, law enforcement actions or scams (Lavorgna, 2015) and cryptocurrencies' volatility (Sovbetov, 2018).

Although terrorist financing via cryptocurrency is in its early stages, it is advancing quickly (Chainalysis Team, 2020). Because of the decentralized nature of cryptocurrencies, it is difficult for law enforcement agencies to shut down crypto addresses belonging to terrorist financiers. Chainalysis reports that especially worrying "[. . .] are the advancements in technical sophistication that have enabled successful terrorism financing campaigns" (2020, p. 70). In one case, the Mujahideen Shura Council (MSC) (a Gaza-based, pro-Islamic State, jihadist group) launched a public crowdfunding campaign called "equip us" that asked donors to send cryptocurrency so the group could purchase weapons. The campaign ran between June 2016 and 2018 (Chainalysis Team, 2020) and was promoted by MSC's media wing, Ibn taymiyya media center (ITMC), via social networks such as Twitter, Telegram and YouTube (Solomon, 2016). The ITMC posted a Bitcoin address to which donors could send funds. At least 27 other addresses were associated with the address. Donors mostly used P2P exchanges, mixers or regulated exchanges to send donations to intermediary private wallets that eventually reached the ITMC address (Chainalysis Team, 2020). Mixers are services that divide coins and send them to different darknet addresses to make connecting the funds to the original address difficult (Canellis, 2018). The process is also popular for money laundering. Across over 50 individual donations, ITMC was able to procure cryptocurrency worth US$10,000 (Chainalysis Team, 2020).

Furthermore, the military wing of Hamas, Izz ad-Din al-Qassam Brigades (AQB), began soliciting Bitcoin donations in early 2019. Chainalysis calls the event "one of the largest and most sophisticated cryptocurrency-based terrorism financing campaigns ever seen" (2020, p. 73). The AQB used different types of wallet infrastructures to receive donations and ultimately settled on a system that generated new addresses for every donor to send cryptocurrency to. During the first sub-campaign, the AQB website invited users to "donate to the jihad" via a quick response (QR) code that led to a Bitcoin address associated with an anonymous regulated US exchange. After law enforcement alerted said exchange, the account was frozen and investigations were initiated. In the second sub-campaign, the AQB published an address linked to a private, non-custodial wallet. Crypto analysts were again able to trace these transactions. Then, the third and most advanced sub-campaign was launched by AQB. The organization used a Bitcoin wallet that was integrated into its website and generated a new receiving address for each donor. The AQB published an explanatory video detailing how to donate. The AQB managed to raise over US$17,000 through these sub-campaigns (Chainalysis Team, 2020).

Moreover, cryptocurrencies offer discreet and secure avenues for online payment within the scope of dark web marketplace and online black-market transactions (Desmond *et al.*, 2019). The steady growth of e-commerce required a payment method that is equally as trustworthy, anonymous and portable as cash while at the same time allowing international transfers (Drainville, 2012; Merlonghi, 2010). According to Goldman *et al.* (2017), cryptocurrencies can be used to both conceal traditional criminal proceeds and foster an increase in money laundering platforms. Researchers find that cryptocurrencies have been fully integrated into the conventional money-laundering procedure (Ajello, 2014; Desmond *et al.*, 2019; van Wegberg *et al.*, 2018). Bitcoin continues to be the most commonly used

cryptocurrency for both legal and illicit transactions (Davidian, 2017; Reynolds and Irwin, 2017).

3. Methodological approach

This paper's methodological approach can be broken down into several stages. Within the scope of a pre-study, interviews were conducted with 10 presumed providers of illegal financial services from Russia, Italy, Switzerland, the United Arab Emirates, Kazakhstan, Germany, Liechtenstein, Monaco and Ukraine, all of whom have presumably facilitated financial crimes. Because of concerns regarding the potential for criminal prosecution, such individuals are not usually willing to be recorded while sharing their extensive knowledge with researchers. Therefore, the pre-study consisted of guided interviews that were not recorded with these 10 interview partners. The intention was to investigate how cryptocurrency can be used to facilitate financial crime. The interview partners were selected based on their expertize and personal experiences.

Because of the fact that financial crime is often international, interview partners from different jurisdictions were selected. To maintain their anonymity, the authors cannot provide any of their personal information. The interviews were held in a conversational, open manner via video chat or in-person and recorded via handwritten notes. Naturally, this form of record tends to be incomplete or distorted, which represents a limitation of the pre-study. However, because of the abovementioned reasons, the selected approach was deemed most suitable. One can assume that the persons interviewed in the pre-study have direct experience with illegal financial services or at least have profound knowledge of them. However, the conversations were not centered around the participants' past offenses; rather, they focused on hypothetical actions that hypothetical intelligent offenders might take. All interview partners were informed of this study's intention and asked not to discuss concrete offenses or divulge any personal information.

Although the pre-study served as the basis for the planning of the main study, the findings were not detailed enough to serve as a foundation for a hypothesis, especially, as the pre-study interviews could not be recorded. To explore the findings of the pre-study more deeply and compensate for weaknesses in the research methodology, 18 exploratory interviews were conducted with compliance experts from Germany, Austria, Liechtenstein and Switzerland. Suitable interview partners were identified via a literature review and online research (Bogner *et al.*, 2014) and selected based on their expertize in the area of financial crime. Others were recruited via the authors' personal networks based on previous empirical research projects.

A careful selection of experts is essential to gaining profound insight. In particular, the experts' knowledge should ideally extend beyond the knowledge presented in the existing literature and draw on a current, systematic and practical knowledge of criminals' concrete approaches to financial crime. Thus, a great emphasis was placed on selecting experts with sufficient practical and empirical knowledge so that they would be able to meaningfully structure the field of action and address concrete problem areas (Bogner *et al.*, 2014). To gain diverse perspectives, experts working in financial services and for consulting companies, investigative authorities and regulating authorities were questioned. The intention of this study was to gain the firsthand insights into a new field and to specify certain processes to solve the research problem.

Because of the qualitative nature of the study, the questions were adjusted throughout the interviews and open-ended, meaning that the interviews were semi-standardized. The comparability of the interviews was not impaired by this (Bogner *et al.*, 2014). In particular, the order of the questions asked changed based on the interview so that the conversations

would flow as naturally as possible. The interview partners' responses were recorded with their consent and subsequently transcribed (Creswell, 2013). Their answers were anonymized as some of the interview partners occupy highly exposed positions. Theoretical saturation was achieved after seven interviews, which is why it was determined that a sufficient volume of data was reached.

In the next step, the collected information was analyzed via qualitative content analysis following Mayring (2010). This type of analysis is centered around categories and offers a means of systematically processing large amounts of text (Mayring, 2010). First, analysis entities are defined. Next, paraphrases are generalized and similar paraphrases are deleted. Then, the statements are reduced and categorized. The category system was created inductively based on the interviews. In particular, topics that the interview partners mentioned often were highlighted and then categorized. General statements were put into their own category. Throughout the analysis, an emphasis was placed on remaining open to new information. It was also important that the interview partners' statements were not distorted during the analysis (Creswell, 2013).

4. Empirical findings

The pre-study and main study investigated the methods that are currently being used to launder money, finance terrorist organizations or perpetuate corruption via cryptocurrency. The empirical findings aim to give legislators, compliance officers and law enforcement an insight into the concrete methods used by offenders. Research on financial crime usually seem to focus on either the prevention perspective or the offender's perspective. This study uses both perspectives to gain a comprehensive overview of the issue. The findings of the main study can be used to gain a profound theoretical understanding of financial crime via cryptocurrency, which could serve as the basis for more effective crime prevention. The methods used to engage in financial crime that were reconstructed based on the interview partners' statements are illustrated in the following sections.

4.1 General statements

The pre-study finds that because of its strict regulations, actors engaging in financial crime prefer to use sectors other than the financial sector. To circumvent CDD guidelines, terrorist financiers, money launderers and corrupt public officials relocate to non-regulated sectors such as cryptocurrency. Even when cryptocurrencies are regulated in a particular jurisdiction, it is difficult for law enforcement there to trace transactions back to their beneficial owners. Therefore, the interview partners argued that cryptocurrencies represent an alternative to wire transfers.

The interview partners also emphasized that anonymity is an advantage of cryptocurrencies. In addition, the interviewees mentioned that storing cryptocurrency can be less risky than the storage of other assets and they stated that it can be used for darknet transactions. One disadvantage that was discussed is that cryptocurrency cannot be used in most retail transactions. Compliance experts added that cryptocurrency can hardly be traced back to the beneficial owner, which represents a challenge for law enforcement. They also stated that they perceive international cryptocurrency transfers to be cheaper and quicker than regular transfers.

4.2 Terrorist financing

Terrorist financiers use both legal and illegal sources of income to finance terrorist organizations. The interview partners identified personal transfers, hawala transfers (parallel banking systems), transfers to Turkey and cryptocurrency as vehicles for the

transfer of funds. Thus, the hypothesis that cryptocurrency is a popular vehicle for terrorist financing was confirmed. Within the scope of the pre-study, the interview partners argued that because cryptocurrencies are hardly regulated or monitored, they represent an alternative to regular transfers, which is why financial institutions might not necessarily come into contact with terrorist financiers. A public terrorist financing scandal would have immensely negative consequences for a bank. Therefore, compliance efforts have increased significantly in recent years – the names of suspected terrorist financiers are being blacklisted, transactions with suspicious references are being blocked and frozen and detailed KYC investigations are being conducted. By contrast, cryptocurrencies present terrorist financiers with few obstacles that cannot be compared to the compliance measures in place in the financial sector. In addition, cryptocurrencies can also reach regions that do not have a regular banking system. Terrorists merely need an internet connection to access their funding.

Like the interview partners in the pre-study, the compliance experts stressed that most cryptocurrencies lack transparency, are highly anonymous and can easily be hidden, which makes it difficult for prosecutors to establish a connection between potential terrorist financiers and incriminated transactions. To use cryptocurrencies for terrorist financing, the interview partners stated that they would need to have access to an e-wallet. To remain undetected, they explained they would regularly exchange their computers and use several e-wallets. To access the internet, terrorist financiers would likely only use public network. They would use either cash or assets to purchase cryptocurrency. For this purpose, they would need to find a private exchange partner or an exchanger.

Once the funds have been transferred, the terrorist organization can use the cryptocurrency to purchase Compliance experts stated that from the criminal's perspective, a significant advantage of cryptocurrency is probably that the authorities are not usually up to date with the technology. The same is true for the regulations surrounding the technology. One disadvantage for the criminal that the interview partners identified is that cryptocurrencies leave digital trails, which can be used to track criminals' online activity once their cryptocurrency address has been identified.

4.3 Money laundering

Cryptocurrencies are suitable for the placement and layering of incriminated funds. During placement, most evidence that would enable supervisory authorities and law enforcement to trace incriminated funds back to their origin are eliminated. During layering, a plausible background story for the origin of the funds is created.

To place incriminated funds, the money launderer could purchase cryptocurrency. Popular methods for purchasing cryptocurrency are the use of exchanges (either regulated or unregulated), P2P exchanges and crypto automatic teller machines (ATMs). From the launderer's perspective, both unregulated exchanges and P2P exchanges offer the advantage that they do not always require identification. In addition, other peers frequently accept cash. However, these methods require some expertize and in the case of P2P exchanges, they require a peer that is willing to exchange money for cryptocurrency. Of the three, crypto ATMs seem to be the simplest method as they do not require much expertize and ATMs can be found in nearly every country (Coin ATM Radar, 2019). Some ATMs do not even require identification. If they do, however, the interview partners suggested that money launderers could send straw people that would use their own passports to make the purchase. If the launderer does not have an electronic wallet, the ATM will create one for them. The receipt recording the transaction can be discarded and no other paper trail is created.

Subsequently, during layering, the launderer would exchange the crypto coins into multiple other digital currencies and transfer them between several different addresses during so-called "hops." For this process, unregulated exchanges seem to be popular as they usually do not enforce AML or KYC measures. However, they can be difficult to use. Alternatively, the money launderer can use mixers. To further complicate a potential prosecution, money launderers often use anonymizing browsers such as Tor or virtual private networks that make it seem as though they are located in a different country. After the process is complete, the coins are pooled again and either held as an asset or exchanged back into fiat. The interview partners again stressed that it would be important for the launderer to only use public networks and eliminate all incriminating evidence such as laptops with digital traces of their illicit activities, from their home so that law enforcement would not be able to connect their crypto address to them in the event of a property search.

4.4 Corruption

Individuals engaging in corruption can use cryptocurrency to send or receive bribes. Generally, corruption can be defined as the abuse of public office (Sun, 2001). Bribery in particular is defined as an act in which one party intentionally abuses their entrusted power for private gain (Teichmann, 2017). This means that the party in power receives a (monetary) consideration for acting in the interest of the other party, who is the briber. For a transaction, both parties would require a wallet and a certain amount of cryptocurrency. The briber would then simply transfer the intended amount to the individual that is being bribed, who could be a public official or an otherwise politically exposed person. To remain undetected, the recipient of the bribe would need to ensure that their e-wallet cannot be accessed by others. If they do not want to hold the cryptocurrency as an asset, they could conduct a number of transfers between different wallets or use a mixer or OTC broker to launder the funds and then exchange them back into fiat.

5. Discussion

As detailed in Section 4 above, cryptocurrencies facilitate various types of financial crime. Based on this study's findings, it was concluded that currently used local regulations seem to have little effect because of the decentralized, transnational nature of most cryptocurrencies. Hence, this article argues that regulations should be aligned on an international level so that a standardized legal framework for blockchain can be created. If all jurisdictions apply the same due diligence measures, virtual asset providers that do not want to comply with these standards will be prevented from simply relocating to other jurisdictions.

In terms of blockchain regulation, most jurisdictions focus mainly on regulating cryptocurrency. Bitcoin has been banned in 10 jurisdictions including Bolivia, Saudi Arabia and Vietnam. In other jurisdictions, cryptocurrency is "restricted," which means that it cannot be traded or used for payment in countries such as China and India, which essentially has the same effect as a ban. In at least 24 other jurisdictions, Bitcoin is neither legal nor illegal (Cryptonews, 2020). For peers operating in this legal gray zone, using cryptocurrency for private or business-related reasons can become dangerous. Scams in particular are one of the major concerns associated with cryptocurrency use (Chainalysis Team, 2020). Naturally, the inconsistency in international standards pertaining to both the status of cryptocurrencies and their regulation creates gaps that criminals may exploit (Davidian, 2017; Houben and Snyers, 2018). For money launderers or terrorist financiers, legal uncertainty can be advantageous because they can refer back to the lack of adequate regulation if and when their actions are investigated by the authorities. Furthermore,

trading volumes illustrate that citizens in nations where Bitcoin is banned or restricted continue to trade the cryptocurrency (see e.g. Coin.Dance for trading volumes), which confirms the hypothesis that cryptocurrency transactions can hardly be blocked.

In the European Union (EU), the 5th anti-money laundering directive (AMLD5) entered into force on January 10 2020. The AMLD5 subjects all service providers offering the exchange of digital currency for fiat and wallet providers to due diligence regulations. These regulations entail strict KYC guidelines and registration with local authorities. In addition, service providers in both areas must monitor transactions and report any suspicious activities (Baydakova and De, 2019). In response to the AMLD5, multiple cryptocurrency service providers, including Dutch Bitcoin trading platform Deribit, UK-based Bitcoin payments provider Bottle Pay and KyberSwap, the second-largest non-custodial cryptocurrency exchange by market share have either left the market entirely or relocated to jurisdictions with less strict regulations, blaming the AMLD5 and its regulations for being too strict to allow them to continue operations (McIntosh, 2020). In response to the AMLD5, Bottle Pay announced:

> [. . .] the amount and type of extra personal information we would be required to collect from our users would alter the current user experience so radically, and so negatively, that we are not willing to force this onto our community (Bottle Pay, 2019).

In addition, the financial action task force, which coordinates international efforts in the fight against money laundering, published new guidelines for virtual asset providers such as cryptocurrency exchanges or wallet providers in June 2019. These include that virtual asset providers must forward information about their customers who transfer funds between two corporations. This information must include the sender's name, birthdate, bank account number and more.

In the USA, virtual currencies were first regulated in 2007, when the government prosecuted e-gold, a virtual currency backed by gold that was found to have been used for money laundering and other illegal activities (Albrecht *et al.*, 2019). Because of the fact that e-gold required a central entity to approve transactions, the government was able to source records and track payments. According to Albrecht *et al.* (2019), this case set the standard for governmental dealings with virtual currencies and cryptocurrencies. The main issue with decentralized cryptocurrencies, however, is that unlike e-gold, they cannot easily be investigated or prosecuted. As a result, most governments have only just begun to discuss appropriate legislation (Albrecht *et al.*, 2019).

Some jurisdictions, including China and Venezuela, have either begun to plan or have already implemented their own cryptocurrencies. Facebook's planned launch Libra seems to have motivated governments to look into the possibility of creating governmental cryptocurrencies, even though the European Central Bank, for instance, had announced in 2018 that there were no plans for a digital euro (Palmer, 2018). It can be expected that the digital euro will be introduced in the near future (Sandner and Groß, 2020). Facebook's announcement of Libra caused an international outcry from both politicians and central bankers who publicly criticized Facebook's unreliability when it comes to data security and argued that currencies should not be issued by private entities (Schulze, 2019). Nonetheless, the announcement seems to have made it clear to central banks worldwide that for the financial sector, digital money is one of the main priorities of 2020.

Section 2.1 above illustrates that OTC brokers and other services operating on exchanges are a source of opacity and money laundering risks. Therefore, exchanges should increase due diligence measures. They must also extend KYC scrutiny that is required by law to OTC desks. However, as demonstrated above, regulating cryptocurrency continues to be

extremely difficult. The AMLD5 has especially proven that strict cryptocurrency regulations can cause innovators, entrepreneurs and startups to relocate or leave the market, thus driving innovation out of the respective country. These developments could ultimately lead to a decline in economic growth. In addition, many users prefer cryptocurrencies because they provide anonymity. Increasing regulation has already led to the creation of new digital currencies that are even more private than the previous generations. It could, therefore, be possible that the market will simply come up with new technologies that will be even more difficult to trace or regulate.

In contrast to the previously outlined regulations that have shaken up the crypto market, the Liechtenstein government decided to introduce a more general legal framework that targets all possible applications of blockchain rather than only focusing on cryptocurrency. The tokens and TT Service Providers Act (German: Token- und VT-Dienstleister-Gesetz; TVTG) represents a comprehensive legal framework that was designed to keep pace with future innovations. It is difficult to regulate innovative technologies because they are constantly evolving. The TVTG calls blockchain-based technologies "TT systems (transaction systems based on trustworthy technologies)" to warrant its broad applicability (Government of Liechtenstein, 2019). Liechtenstein addresses the due diligence concerns associated with cryptocurrency in the Due Diligence Act (2008) (German: Sorgfaltspflichtgesetz; SPG). Exchange offices that exchange regular currencies for cryptocurrency have been regulated by the SPG, as September 1 2017 and all transactions of 1,000 francs or more have been subject to due diligence regulations (Art. 3 SPG). The TVTG also implements a registration system for TT service providers (Government of Liechtenstein, 2019).

The importance of blockchain for different sectors has been acknowledged by countless experts (Ganne, 2019; Underwood, 2016; Crosby *et al.*, 2015). However, businesses and private actors alike can only begin to implement the technology when sufficient legislation is in place to protect them. By introducing a comprehensive blockchain act, Liechtenstein has become a legislative pioneer. Countries that follow Liechtenstein's example could gain competitive advantages over countries that do not regulate blockchain. When it comes to financial crime, the introduction of appropriate due diligence measures is of particular importance. The intention of due diligence is not to restrict legitimate providers of cryptocurrency services; rather, due diligence measures target suspicious transactions that could potentially involve incriminated funds or illegal activity. Consequently, innovative cryptocurrency startups should not be opposed to the implementation of KYC as long as they have nothing to hide. The Liechtenstein government claims that the due diligence duties defined in the TVTG go beyond the scope of other regulations and that constant, careful supervision is required (Government of Liechtenstein, 2019).

Because of its comprehensiveness and farsightedness, the TVTG could serve as a benchmark and set an example for a potential international standardized framework. This article mainly focused on Liechtenstein's legislation because instead of concentrating on cryptocurrency, the TVTG considers all possible applications of blockchain. By implementing the law, Liechtenstein's legislators will not likely need to revisit the legislation in the near future and amend it based on new innovations because the TVTG already considers the possibility of new developments taking place, which gives it a strategic advantage over other existing legal frameworks.

6. Conclusion

Based on the literature review, it was determined that cryptocurrencies continue to represent a feasible vehicle for financial crimes. However, previous research usually focuses mainly on

one perspective – that of regulators, law enforcement and compliance officials. This research gap is closed by the present study, which investigated the issue from both perspectives. In particular, both alleged criminals and prevention experts were asked to detail based on their personal experiences and expertize how they believe criminals would use cryptocurrency to conduct financial crime without attracting the attention of law enforcement authorities. Both groups identified the decentralized, multinational nature of cryptocurrencies and their high level of anonymity as the main risk factors for financial crime. Therefore, it was concluded that only an international regulatory standard could have the desired effect of eliminating financial crime via cryptocurrency.

This paper suggests that based on its comprehensiveness and innovation, the Liechtenstein blockchain act could serve as a benchmark for legislators aiming to regulate blockchain more effectively. In particular, the TVTG could be used as a basis for the proposed international legal framework. The main advantage of the TVTG is that it does not concentrate solely on cryptocurrency like most other regulations do. Instead, it uses abstract terms to refer to blockchain-powered technologies that include but are not limited to cryptocurrency. By doing so, the Liechtenstein government ensures that the TVTG will continue to remain relevant as time goes on and new technological innovations emerge. By regulating the concept of blockchain itself, rather than focusing on smaller details such as cryptocurrency, legislators can break this repetitious regulatory pattern and create long-lasting, effective regulations that benefit individual cryptocurrency users, companies and law enforcement alike. In addition, national law enforcement agencies should cooperate more frequently when prosecuting cryptocurrency-related crimes.

References

Ajello, N. (2014), "Fitting a square peg in a round hole: bitcoin, money laundering, and the Fifth Amendment privilege against self-incrimination", *Brook. Law Review*, Vol. 80, p. 435.

Albrecht, C., McKay Duffin, K., Hawkins, S. and Morales Rocha, V.M. (2019), "The use of cryptocurrencies in the money laundering process", *Journal of Money Laundering Control*, Vol. 22 No. 2, pp. 210-2016.

Antonopoulos, A.M. (2015), *Mastering Bitcoin – Unlocking Digital Cryptocurrencies*, O'Reilly, Sebastopol.

Baydakova, A. and De, N. (2019), "All crypto exchanges must share customer data, FATF rules", available at: www.coindesk.com/fatf-crypto-travel-rule (accessed 12 November 2019).

Bheemaiah, K. (2015), "Block chain 2.0: the renaissance of money", available at: www.wired.com/insights/2015/01/block-chain-2-0/ (accessed 23 October 2019).

Bitcoin Project (2009-2020), "FAQ", available at: https://bitcoin.org/en/faq#what-is-bitcoin (accessed 9 April 2020).

Bogner, A., Littig, B. and Menz, W. (2014), *Interviews Mit Experten: eine Praxisorientierte Einführung*, [in German], Springer-Verlag, Wiesbaden.

Bottle Pay (2019), "Official announcement on the shutdown of Bottle pay", available at: https://bottlepay.helpscoutdocs.com/article/40-official-announcement-on-the-shutdown-of-bottle-pay (accessed 24 April 2020).

Campbell-Verduyn, M. (2018), "Bitcoin, crypto-coins and global anti-money laundering governance", *Crime, Law and Social Change*, Vol. 69 No. 2, pp. 283-305.

Canellis, D. (2018), "Here's how criminals use Bitcoin to launder dirty money", available at: https://thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2/ (accessed 3 April 2020).

Chainalysis Team (2020), "The 2020 state of Crypto crime", available at: https://blog.chainalysis.com/reports/cryptocurrency-crime-2020-report (downloaded 31 January 2020).

Choo, K.K.R. (2015), "Cryptocurrency and virtual currency: corruption and money laundering/terrorism financing risks?", in Chuen, D.L.K. (Ed.), *Handbook of Digital Currency*, Elsevier, Amsterdam, pp. 283-307, available at: https://doi.org/10.1016/B978-0-12-802117-0.00015-1 (accessed 9 April 2020).

Coin ATM Radar (2019), "Bitcoin ATM map", available at: https://coinatmradar.com/ (accessed 15 November 2019).

Creswell, J.W. (2013), *Research Design: qualitative, Quantitative, and Mixed Methods Approaches*, Sage Publications, Thousand Oaks, CA.

Crosby, M. Pattanayak, P. Verma, S. and Kalyanaraman, V. (2015), "BlockChain technology, beyond Bitcoin", available at: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf (accessed 7 November 2019).

Cryptonews (2020), "Countries where Bitcoin is banned or legal in 2020", available at: https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm (accessed April 24, 2020).

Davidian, R. (2017), "Anti-money laundering laws for Bitcoin exchanges", *American Criminal Law Review*, Vol. 36, pp. 26-41.

Desmond, D.B., Lacey, D. and Salmon, P. (2019), "Evaluating cryptocurrency laundering as a complex socio-technical system: a systematic literature review", *Journal of Money Laundering Control*, Vol. 22 No. 3, pp. 480-497.

Dostov, V. and Shust, P. (2014), "Cryptocurrencies: an unconventional challenge to the AML/CFT regulators?", *Journal of Financial Crime*, Vol. 21 No. 3, pp. 249-253.

Drainville, D. (2012), *An Analysis of the Bitcoin Electronic Cash System*, University Waterloo, Waterloo, ON.

Essebier, J. and Wyss, D.A. (2017), "Von der blockchain zu smart contracts [in German]", Jusletter, 24 April, available at: https://jusletter.weblaw.ch/juslissues/2017/889/von-der-blockchain-z_5bd3b52a43.html__ONCE&login=false (accessed 25 November 2019).

Farell, R. (2015), *An Analysis of the Cryptocurrency Industry*, Wharton Research Scholars, University of PA, p. 123.

Foley, S., Karlsen, J. and Putninš, T. (2018), *Sex, Drugs, and Bitcoin: How Much Illegal Activity is Financed through Cryptocurrencies*?, University of Sydney Business School, Sydney.

Ganne, E. (2019), *Can Blockchain Revolutionize International Trade*?, WTO Publications, Geneva.

Goldman, Z., Maruyama, E., Rosenberg, E. and Saravalle, E.A.S.-S.J. (2017), Terrorist Use of Virtual Currencies, Center for a New American Security, Washington, DC.

Government of Liechtenstein (2019), Report and application of the government to the parliament of the Principality of Liechtenstein concerning the creation of a law on tokens and TT service providers (Tokens and TT Service Providers Act, TVTG) and the amendment of other laws, (No. 54/2019).

Government Office for Science (2016), "Distributed ledger technology: beyond block chain", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (accessed 31 October 2019).

Grünewald, S. (2015), "Währungs- und geldwäscherechtliche Fragen bei virtuellen Währungen [in German]", *ZIK – Publikationen Aus Dem Zentrum Für Informations- Und Kommunikationsrecht Der Universität Zürich*, Vol. 61, pp. 93-112.

Hileman, G. and Rauchs, M. (2017), "Global Cryptocurrency benchmarking study", available at: www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf (accessed 22 May 2020).

Houben, R. and Snyers, A. (2018), "Cryptocurrencies and blockchain – legal context and implications for financial crime, money laundering and tax evasion", available at: www.europarl.europa.eu/

cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (accessed 22 May 2020).

Hutchings, A. and Holt, T.J. (2017), "The online stolen data market: disruption and intervention approaches", *Global Crime*, Vol. 18 No. 1, pp. 11-30.

Lavorgna, A. (2015), "Organised crime goes online: realities and challenges", *Journal of Money Laundering Control*, Vol. 18 No. 2, pp. 153-168.

McIntosh, R. (2020), "Is 5AMLD causing crypto companies to shut down and relocate?", available at: www.financemagnates.com/cryptocurrency/news/is-5amld-causing-crypto-companies-to-shut-down-relocate/ (accessed 9 April 2020).

Mabunda, S. (2018), "Cryptocurrency: the new face of cyber money laundering", *2018 International conference on advances in big data, computing and data communication systems (icABCD) proceedings of the international conference in Durban, South Africa, IEEE, Piscataway*, pp. 1-6, available at: https://doi.org/10.1109/ICABCD.2018.8465467 (accessed 9 April 2020).

Mayring, P. (2010), *Qualitative Inhaltsanalyse: Grundlagen Und Techniken [in German]*, Beltz, Weinheim.

Memon, B. (2020), "Guide to stablecoin: types of stablecoin and its importance", available at: https://masterthecrypto.com/guide-to-stablecoin-types-of-stablecoins/ (accessed 8 April 2020).

Merlonghi, G. (2010), "Fighting financial crime in the age of electronic money: opportunities and limitations", *Journal of Money Laundering Control*, Vol. 13 No. 3, pp. 202-214.

Nakamoto, S. (2008), "Bitcoin P2P e-cash paper", The Cryptography Mailing List, 1 November, available at: www.mail-archive.com/cryptography@metzdowd.com/msg09959.html (accessed 22 October 2019).

Palmer, D. (2018), "ECB has 'no plans' to issue a digital Euro, says Mario Draghi", available at: www.coindesk.com/ecb-has-no-plans-to-issue-a-digital-euro-says-mario-draghi (accessed 9 April 2020).

Ponsford, M.P. (2015), "A comparative analysis of bitcoin and other decentralised virtual currencies: legal regulation in the People's Republic Of China, Canada, and the United States", *Hong Kong Journal of Legal Studies*, Vol. 9, pp. 29-50.

Reynolds, P. and Irwin, A.S. (2017), "Tracking digital footprints: anonymity within the Bitcoin system", *Journal of Money Laundering Control*, Vol. 20 No. 2, pp. 172-189.

Sandner, P. and Groß, J. (2020), "Warum wir den digitalen Euro brauchen [in German]", available at: www.manager-magazin.de/finanzen/artikel/digitaler-euro-auf-blockchain-basis-europa-braucht-eine-kryptowaehrung-a-1304537.html (accessed 9 April 2020).

Schmid, J.D. and Schmid, A. (2012), "Bitcoin – eine einführung in die funktionsweise sowie eine auslegeordnung und erste analyse möglicher rechtlicher fragestellungen [in German]", Jusletter, 4 June, available at: www.epartners.ch/assets/images/publications/1338882576_Bitcoin.pdf (accessed 22 April 2020).

Schulze, E. (2019), "Facebook's Libra plans are under fire again – this time from global privacy regulators", available at: www.cnbc.com/2019/08/06/facebook-libra-crypto-plans-under-fire-from-privacy-regulators.html (accessed 9 April 2020).

Solomon, A.B. (2016), "Gaza-based pro-ISI group urges Muslims on social media to donate for weapons", available at: www.jpost.com/middle-east/isis-threat/gaza-based-pro-isis-group-urges-muslims-on-social-media-to-donate-for-weapons-457680 (accessed 8 April 2020).

Sovbetov, Y. (2018), "Factors influencing cryptocurrency prices: evidence from bitcoin, Ethereum, Dash, Litcoin, and Monero", *Journal of Economics and Financial Analysis*, Vol. 2 No. 2, pp. 1-27.

Sun, Y. (2001), "The politics of conceptualizing corruption in reform China", *Crime, Law and Social Change*, Vol. 35, pp. 245-270, available at: www.researchgate.net/profile/Yan_Sun77/publication/227158676_The_Politics_of_Conceptualizing_Corruption_in_Reform_China/links/

568146d908ae1975838f7237/The-Politics-of-Conceptualizing-Corruption-in-Reform-China.pdf (accessed 31 March 2020).

Teichmann, F. (2017), *Anti-Bribery Compliance Incentives*, Kassel University Press, Kassel.

Teichmann, F. and Falker, M.C. (2020), "Money laundering through cryptocurrencies", in Popkova, E.G. and Sergi, B.S. (Eds), *Artificial Intelligence: Anthropogenic Nature vs Social Origin, ISC Conference*, Volograd, pp. 500-511.

Tuwiner, J. (2019), "What is Bitcoin mining and how does it work?", available at: www.buybitcoinworldwide.com/mining/ (accessed 22 April 2020).

Underwood, S. (2016), "Blockchain beyond Bitcoin", *Communications of the ACM*, Vol. 59 No. 11, pp. 15-17.

van Valkenburgh (2019), "The differences between Bitcoin and Libra should matter to policymakers", available at: the-differences-between-bitcoin-and-libra-should-matter-to-policymakers (accessed 23 April 2020).

van Wegberg, R., Oerlemans, J. and van Deventer, O. (2018), "Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using Bitcoin", *Journal of Financial Crime*, Vol. 25 No. 2, pp. 419-435.

Further reading

Coin.Dance (2020), "LocalBitcoins volume (China) – updated weekly", available at: https://coin.dance/volume/localbitcoins/CNY (accessed 9 April 2020).

Fortney, L. (2019), "Blockchain explained", available at: www.investopedia.com/terms/b/blockchain.asp (accessed 7 November 2019).

Government of Liechtenstein (2008), "Gesetz vom 11 Dezember 2008 über berufliche Sorgfaltspflichten zur Bekämpfung von Geldwäscherei, organisierter Kriminalität und Terrorismusfinanzierung (Sorgfaltspflichtgesetz, SPG) [in German]", available at: www.gesetze.li/konso/2009.047 (accessed April 9 2020).

Corresponding author

Marie-Christin Falker can be contacted at: falker@teichmann-law.ch