CRYPTOCURRENCIES: OPPORTUNITIES, RISKS AND CHALLENGES FOR ANTI-CORRUPTION COMPLIANCE SYSTEMS

CIUPA KATARZYNA
WARSAW SCHOOL OF ECONOMICS
katarzyna.ciupa@gmail.com

Key words: Corruption, Cryptocurrencies, Infrastructure, Blockchain, Compliance

Abstract

Since their inception in 2008, cryptocurrencies have attracted various groups of users. While some people considered them as an independent payment system without the need for a third party, others decided to invest their savings into this new phenomenon hoping for huge returns. Last, there were also players who found cryptocurrencies to be the long-awaited tool supporting their illicit practices. As a result, cryptocurrencies went from a niche innovation to become one of the hottest topics, calling for intervention from the international or national regulators. Due to the growing number of corruption issues involving cryptocurrencies, this global phenomenon can no longer be neglected and there is a need for a thorough analysis to identify anti-corruption measures.

The goal of this paper is thus to analyse which actions involving cryptocurrencies are especially at risk of corruption, and to propose preventive measures that can potentially reduce the illicit usage of cryptocurrencies.

This paper was submitted as part of a competitive call for papers on integrity and anti-corruption in the context of the 2019 OECD Global Anti-Corruption & Integrity Forum.

1. Introduction

The cryptocurrency concept was introduced 46 days after the bankruptcy of the Lehman Brothers, the event marking the beginning of the second biggest financial crisis in the human history (Friedman & Friedman, 2009; Knight, 2009; Partnoy, 2013), and it was for a long time either wrongly understood or completely ignored by the general public. During the time when many executives, law makers and managers were trying to define effective and preventive measures or practices to bring the economy back to the stable state, a small group of engineers decided to pursue the cryptocurrency idea further. Unfortunately, a group of bad players also emerged since they realised that there is a huge value proposition for illegal practices offered by the new concept.

Although the concept has been around since 2008 (Nakamoto, 2008), and thousands of new constructs have been created since, it is still a highly nascent and undiscovered area. The continuously growing complexity has not prevented new players from entering the market. This caused the popularity of cryptocurrencies to soar especially during the 2015-2017-time period, and pushed their prices to unimaginable levels, with Bitcoin price reaching almost USD 20k at the end of 2017 (Higgins, 2017).

Typical characteristics of cryptocurrencies such as decentralisation, their inherit global character, anonymous or pseudo-anonymous nature (Bonneau, Felten, Miller, & Narayanan, 2016; Clark & Narayanan, 2017; Pilkington, 2016), together with the initial lack of any regulations for their field of operation, have led to the situation in which cryptocurrencies started being considered as an interesting mechanism for those wishing to bypass the law and commit illicit actions such as money laundering, dark market payments or even terrorist financing (Houben & Snyers, 2018; Keatinge, Carlisle, & Keen, 2018; Keidar & Blemus, 2018). As a result, various governing bodies on national and international levels, added cryptocurrencies to their agendas, trying to define measures which should be undertaken in order to stop this illicit usage and to provide some guidelines, allowing for their sustainable and legal development. But while cryptocurrencies moved from garage laboratories to international conferences and board meetings, being discussed by representatives of private and public sectors as well as individuals, it still largely remains an open topic and not much clarity has been proposed so far.

The goal of the paper is thus to analyse which actions involving cryptocurrencies are especially at risk of corruption, and to propose preventive measures which, once implemented, might limit or at least hinder the illicit usage of cryptocurrencies. It uses the analysis of various documents published by founders, regulators and consulting companies as well as interviews conducted with compliance experts as a source (research method).

2. Cryptocurrencies and the role of blockchain technology

In order to be able to analyse cryptocurrencies' related opportunities, risks and challenges for anti-corruption compliance systems, it is essential to become familiar with the definitions, characteristics and key concepts that build their foundations.

Although cryptocurrencies' idea is already ten years old, cryptocurrencies are still lacking harmonized definitions and taxonomies according to which they can be categorized. Various international and national regulators propose different approaches classifying and thus defining cryptocurrencies either as a subclass of broader digital money or as a part of narrowly defined virtual currencies. The former definition is favoured by the Bank for International Settlements (2015) and the World Bank (2017). The latter approach is preferred by the European Banking Association (2014), the European Central Bank (2015), The European Securities and Markets Authority (2018) and the International Monetary Fund (2016) according to which all organisations agree that what distinguishes cryptocurrencies from other financial instruments is their independent issuance mechanism, not accepted by the official governing bodies. The definition published by the EU Parliament which could be regarded as a compromise solution considers cryptocurrencies as "a digital representation of value that (i) is intended to constitute a peer-to-peer ("P2P") alternative to government-issued legal tender, (ii) is used as a general-purpose medium of exchange (independent of any central bank), (iii) is secured by a mechanism known as cryptography and (iv) can be converted into legal tender and vice versa" (Houben & Snyers, 2018).

Being aware of the definition's challenge, it is worth to elaborate on cryptocurrencies' characteristics which might partially explain the complexity of the terminology. First of all, it has to be pointed out that cryptocurrencies are just one (albeit the first) out of many constructs called cryptoassets, that have been created with the usage of blockchain technology[1]. They are also a key element in a three-dimensional structure introduced by Satoshi Nakamoto, calling it "a peer to peer electronic cash system" (2008). Such a system consists of (i) the universal value representative[2] (e.g. Bitcoin), (ii) infrastructure essential for its issuance, settlement and audit trial (e.g. Bitcoin blockchain[3]) and (iii) the rules governing money supply and transaction related processes (e.g. Proof of Work). Despite the fact that the system is organisationally decentralised meaning that there is no central entity governing the cryptocurrency supply, it has a very centralised logic with all the rules being predefined and dictated by the open-source algorithm.

Cryptocurrencies also proved to be very successful use case for blockchain technology. Most cryptocurrencies are built on public-permissionless blockchains (Hileman & Rauchs, 2017), as these constructs minimize the information asymmetry (Tabarrok & Cowen, 2015) related to the transaction process and allow everybody to

[1] The term cryptoassets was invented as a consequence of continuous development of the blockchain technology which resulted in the creation of completely new constructs with their value proposition being often too far away from the one delivered by the initial construct. The topics discussed in the paper are related to cryptocurrencies and in case the aspects concern also cryptoassets, it is clearly stated in the paper.

[2] The term is introduced by the author in order to describe the nature of the cryptocurrency which is, as indicated the universal value representation making it similar to the concept of money.

[3] Interestingly, the author of the paper, has not used the term "blockchain" even once in its publication.

become both a member of the system and a holder of the same copy of a database[4]. The novel technology also allowed for a value exchange between two conflicting parties without the need of a middleman that is responsible for proper transaction validation and settlement (Gupta, 2017; Moore & Christin, 2013; Tapscott & Tapscott, 2016). Blockchain provides a transaction ledger, where each entry is supposed to be correct, verified, and immutable. Cryptocurrencies rely on blockchain also to solve the 'double spending' problem: being able to spend a unit of the currency more than once because no accurate transaction record can be kept (Budish, 2018; Efanov & Roschin, 2018).

Cryptocurrencies have a global character and could circulate freely across borders and they are also pretty easy to use, as only the software installation is required instead of many administrative steps present in regular financial ecosystem and almost all of them are traded electronically, which additionally facilitates their adoption. Many have a predefined and often fixed currency supply, but their initial issuance process varies considerably with some coins being released (e.g. Bitcoin[5]), others (e.g. Ethereum[6]) being distributed through ICO[7] and yet a few being fully (e.g. Stellar) or partially pre-mined and given to the public either for free or in the form of ICO. A very important feature is also their anonymous (e.g. Monero[8], Zcash[9]) or pseudo-anonymous (e.g. Bitcoin) nature. This aspect is hugely attractive for an illicit user, wishing to take advantage of the innovative technology, which is proven through many examples presented in the further part of the paper.

Another aspect which often proves to be the main field of potential wrongdoings, is the cryptocurrency ecosystem. It is a quite diverse infrastructure consisting of users, potential investors or speculators, miners, wallet providers, exchange and trading platforms and entrepreneurs. Users drive the demand and are interested either in short-term speculation, long-term investing or are simply the trend-followers who decided to jump on the cryptocurrency bandwagon. Miners are responsible for system security and are in charge of transaction validation, block creation and in general act as system stability guards. Wallet providers offer the platforms in which cryptocurrencies are kept, and finally exchange and trading platforms[10] allow for a smooth exchange between fiat money[11] and cryptocurrencies and thus offer a secondary market on which cryptocurrencies could be traded.

3. Risk and challenges for anti-corruption compliance

Cryptocurrencies, both intriguing and attractive, unfortunately proved to be often involved in illegal practices. Even though the new concept opened an amazing opportunity to create a medium able to serve the digital economy, with users interacting on peer-to-peer basis, it was often utilized by illicit players who realized that committing a crime has become much easier since the invention of the new phenomenon.

[4] Nevertheless, different concepts utilize various kinds of blockchain such as private-permissioned or public-permissioned setups.
[5] https://bitcoin.org/en/
[6] https://www.ethereum.org/
[7] Topic of ICO (Initial Coin Offering) is discussed in chapter 3.1
[8] https://www.getmonero.org/
[9] https://z.cash/
[10] The latter are different from the former, in that they do not hold the currencies on behalf of their users but only provide an infrastructure that matches the opposite orders of the clients, which makes them similar to over the counter (OTC) trading platforms, where users exchange with one another.
[11] Term "fiat money" is often used to describe officially accepted financial instruments

3.1 Scams and Market Abuse Practices

ICO, or Initial Coin Offering, has become a highly popular mechanism for cryptocurrencies' or cryptoassets' distribution, attracting both potential investors and entrepreneurs who exchanged billions of dollars in order to finance and thus invest in entrepreneurial blockchain-based activity (Abraham, 2018; FabricVentures & TokenData, 2018; Fisch, 2019; Howell, Niessner, & Yermack, 2018). ICO started as a brilliant idea aiming to revolutionize, or rather democratize start-ups' funding.

Unfortunately, the new mechanism turned out not to be as perfect as initially planned. On the one hand, start-ups quickly realized that the possibility of raising real money without offering anything meaningful in exchange and without preparing any complex documentations[12] has not only become a reality but it proved to be a very successful practice. As a result, new ideas wishing to get funding, emerged, including various scam practices with impossible or illogical value propositions such as Pincoin (collected USD 660mn) (Suberg, 2018), AriseBank (collected USD 600mn) (Khatri, 2018) or Savedroid (collected USD 50mn) (Esteves, 2018). Other "entrepreneurs" decided to utilize further practices known as "Ponzi/Pyramid Scheme" with Optioment (collected USD 115mn) (Groendahl, 2018) being a broadly known example. In general, citing the results of the latest research, in 2017 around 78% of the projects, collecting a total of USD 1,34bn, ended up being scams (Alexandre, 2018).

On the other hand, people hoping for quick and considerable returns, decided to "invest" their savings into projects, following market news, influencers' advice (Smith, 2018) or other players' moves, and often not even being aware of what their "investment" is about.[13] This new kind of social rush fuelled by the "fear of missing out" (Gantori et al., 2017; Johnson, 2018), was vastly facilitated by the emergence of exchange and trading platforms. New and liquid secondary markets where the reason why many players did not even consult the whitepaper prior to their buying decision, as they were given a chance to smoothly liquidate their position, often at a much higher than initially offered price. This led to a "crypto rush" or "crypto bubble" at the end of 2017 (Adriano, 2018; Benedetti & Kostovetsky, 2018), which was the result of mostly speculative actions with many illicit users wishing to utilize practices well-known and forbidden on regular capital markets.

As a consequence, various abusive mechanisms have been discovered, with an increasing number of "Pump and Dump" groups trying to manipulate the market (Hamrick et al., 2018; Xu & Livshits, 2018). These are especially successful in case of cryptoassets with low market capitalisation and low circulating supply as such characteristics considerably increase the ease of abusive practice and thus lead to the best results. Groups communicate via various messaging channels (e.g. Telegram) and sometimes even offer a kind of "affiliation program", encouraging the existing users to invite new members (Martineau, 2018). Some popular examples of cryptocurrencies which were abused include Bancor[14], Cloackcoin and Agrello (Shifflett & Vigna, 2018)

[12] Only one document, known as "whitepaper" was required, acting more like a vision rather than business plan
[13] One example is the project named "Useless Ethereum Token", which in a very transparent manner informed users about its useless concept and still was able to collect about USD 200k in the ICO phase.
[14] https://pumpdump.coincheckup.com/pump/bancor-2018-04-23-19-02-01/

3.2 Ransom ware attacks

Cryptocurrencies have become popular also among hackers who started requesting them as a new form of bribery in case of ransom ware attacks. According to FBI statistics in 2017, more than USD 58,3mn was stolen in cyber ransom situations, when after blocking the access to the files, attackers asked for payment in cryptocurrencies, mostly in Bitcoin, Ethereum or Bitcoin Cash (CipherTrace, 2018). One example of such a practice was the WannaCry virus in which payment in Bitcoin was required (Browne, 2017; Memoria, 2018).

The motives behind requesting cryptocurrencies instead of regular financial instruments result from their attractive characteristics such as a global character which implies that hacker does not have to cover high transaction costs related to currency exchange or international transfer, and also their anonymous or pseudo-anonymous nature thanks to which hacker could more effectively hide his real identity. Above mentioned coins were preferred as these were the least volatile and thus allowed for more stable gain's prediction.

3.3 Exchange Platforms' Thefts

Exchange and trading platforms play a crucial role in the ecosystem. They allow for the exchange between fiat money and cryptocurrencies, and therefore facilitate the growth of the network. Nevertheless, their operating model is prone to various risks, with thefts being one of the most prominent examples. Exchange platforms, due to the fact that they hold large amounts of cryptocurrencies on behalf of their customers are often considered to be "honey pots" attracting bad actors to commit theft. Such structures make the attack especially easy since the hacker could break or bypass the security mechanism of an exchange in order to get the access to thousands, if not millions, of cryptocurrencies' accounts stored there. Common misconception has labelled such attacks as being made possible because of blockchain vulnerabilities. It is important to correct these fallacies since it is not about the blockchain's weakness: exchange wallets are kept off chain and in case of theft, no interaction with blockchain takes place. The reason why such attacks could happen is often the absence of a strong security mechanism, or the presence of a very naive system, making it very easy to manipulate the exchange construct and thus steal collected cryptocurrencies.

According to the statistics published by the CipherTrace, during the period 2016-2018 cryptocurrencies worth around USD 1,3bn were stolen. Nevertheless, such a practice is not new and it has been present on cryptocurrencies' market since the origins of exchange platforms. One of the most spectacular events was the bankruptcy of Tokyo based Mt.Gox exchange, where around 750.000 of its clients' Bitcoins have been lost. Youbit, a South-Korean based exchange, could be named as another example, as this platform filed for bankruptcy after losing around 17% of its holdings. There were also some exchanges that managed to survive the attacks including Japan-based exchange platform Coincheck.Inc which in January 2018 lost around USD 530mn worth XEM (NEM) (Cheng, 2018). However, the illicit procedure considerably hurt their reputation.

3.4 Money Laundering

Money laundering is an old and well-known practice exercised across borders and involving various financial instruments. Estimates of the amount of money laundered worldwide range from USD 500bn to a USD 1tn and such a procedure is not the problem of only a few nations: citing Basel AML Index, around 64% of countries have been classified as having a significant risk of money laundering[15] with only 4% of countries able to improve their ranking comparing to their last year's results (2018). Since 2008 the illicit users have another tool, namely cryptocurrencies, which started to become a very promising mechanism for players wishing to engage in money laundering.

These cryptocurrencies could come from various sources. They could be collected as ransom ware payments, stolen from cryptocurrency exchanges, gathered through scams. In addition, also "clean", both fiat money and cryptocurrencies may fuel the process. After the funds are collected, the laundering practice starts with the so called "layering" step in which inputs are mixed in order to break the initial link with their dirty origins. In case of cryptocurrencies this process could have various forms and thus it either (i) involves the usage of a dedicated infrastructure such as mixers, tumblers, foggers, offered by for example BestMixer[16], BitBlender[17] or CoinMixer[18], (ii) happens on the newly created gambling sites[19] and crypto-casinos which are not required to follow any rules and regulations and thus allow for a very efficient laundering procedure or (iii) relates to many repetitive exchange processes until there is no sign of illegal connections, with privacy coins such as Zcash[20] or Monero[21], being often utilized.

Once the "layering" is finished, the "integration" phase starts, with its goal being to integrate cleaned instruments into the regular financial system. This practice is however not trivial and depositing large amounts of money into bank account without any well documented history of their origins is definitely not an easy task. Nevertheless, creative illicit users utilize for example the practice known as "micro laundering", in which small chunks of cryptocurrencies are exchanged for fiat and later deposited into regular accounts, causing them to look less suspicious. This practice was utilized for example by the cocaine cartel and allowed European dealers to pay for the Columbian cocaine (The Economist, 2018).

According to Europol statistics, around 3-4% of the Europe's annual criminal taking is crypto-laundered (around USD 4,2-5,6bn), which in comparison to the overall money laundering practices accounting for 2-5% of GDP (around USD 800bn-2tn), could be considered as still a minor problem (The Economist, 2018). Nevertheless, various experts predict that this probably will change in the future and thus these practices cannot be ignored.

[15] The results consider both money laundering and terrorist financing
[16] https://bestmixer.io/en
[17] https://bitblender.io/
[18] https://coinmixer.io/
[19] The list of potential gambling sites could be found here: https://www.gamblingsites.com/cryptocurrency/sites/
[20] https://z.cash/
[21] https://www.getmonero.org/

3.5 Financing of illicit purposes

Since their inception, cryptocurrencies have also attracted many dark market users. The anonymous or pseudo anonymous character, irreversibility of transaction, process efficiency and lack of regulations caused cryptocurrencies to become a highly popular means of payment integrated into dark market platforms, with their role being often compared to the role of PayPal in eBay's development (Foley, Karlsen, & Putniņš, 2018).

Dark market users until the emergence of cryptocurrencies had to rely on the traditional money transfers coming from untrusted users. Since 2008, they have been given a tool providing a trust-free, efficient and immutable solution for this already highly risky setup. Various studies have proved that financing of illegal activities, mainly purchases of illicit products, has been one of the most popular use cases of cryptocurrencies. Some researchers even tried to define patterns characterising typical illicit actors. According to one study, these actors treat Bitcoin as a payment system and are not interested in holding it as a long-term investment or speculative asset. As a result, they transact quite often but the transactions amounts are considerably smaller. Additionally, the actor prefers to transacts with a given counterparty who proved to be trustworthy in order to minimise the risk of entering into a potentially risky business relation. Finally, these actors hold less Bitcoin in a fear of seizure and try to have only the amount needed for purchases, which additionally confirms the non-investment character of discussed practice. Interestingly, such users are also more active during the time when (i) many marketplaces operate, (ii) there is a small hype or mainstream interest, or (iii) directly after seizures and scams often in a fear of losing the source of the illegal products essential for their existence. The research shows also another shocking statistic, namely it was proven that around 25% of all Bitcoin users and around 44% of all Bitcoin transactions are associated with illegal practices; about 38% of Bitcoin addresses are hold by illegal users and more than 50% of all Bitcoins were associated with illicit practices through the analysed time period. Bitcoin worth around USD 72bn are supposed to be involved in illicit activities every year. Equally interesting is the declining proportion of Bitcoins being used for dark market purchases, with the size of this market continuously increasing, and thus implying the growing popularity of other cryptocurrencies now more often utilized for this purpose (Foley et al., 2018).

Regulators have been actively trying to terminate illicit practices and seize the dirty cryptocurrencies. The FBI terminated Silk Road, one of the most famous dark marketplaces accepting cryptocurrencies and confiscated about 144.000 Bitcoins (Wikipedia, 2019). Moreover, the joint initiative of Europol, FBI, DEA and the Dutch National Policy regulators was successful in taking down two biggest dark marketplaces, namely AlphaBay and HANSA in 2017 (FBI 2017; Memoria, 2017)

3.6 Terrorist financing

Cryptocurrencies as a tool for terrorist financing is, comparing to previously discussed examples, still in a very nascent stage. Potential users value the cryptocurrencies' characteristics such as anonymity or pseudo-anonymity, lack of regulations, high speed and irreversibility of transactions. Nevertheless, their high volatility acts as a limiting factor for terrorist financing as this procedure requires reliable source of considerably large sums of funds, which cryptocurrencies with their constantly changing prices could not fulfil. Moreover, the acceptance of cryptocurrencies is rather limited, which additionally hinders their attractiveness for terrorist

financing. Nevertheless, they are not completely out of interest among terrorist groups, as cryptocurrencies offer, for example, fast international transfers or allow for collection of donations from all over the world. Such practices have been already utilised by the Islamic state of Iraq and Syria (Higgins, 2014) or al-Sadaqah (Keatinge et al., 2018), that recommended Bitcoin as anonymous and secure payment mechanism.

3.7 Tax evasion and accounting challenges

Resulting from the lack of a harmonized approach and no clarity with regard to tax rules, cryptocurrencies, since their inception, started attracting players searching for tax-evasion solutions. In the early days, cryptocurrencies, with their considerably low market capitalisation and little mainstream adoption, were not considered as a potential risk by various regulators and as a result there was not much work undertaken aiming to define the harmonized tax regulations. In 2017 however, this situation changed considerably, with many new investors exercising extremely high returns, forcing tax regulators to rethink their rules and approaches.

There were many new questions arising regarding tax issues, such as for example how to differentiate between cryptocurrencies' trading and spending, mainly due to the lack of a clear definition and because of their constantly evolving nature. As a consequence, defining and agreeing on proper taxation has become a huge challenge with various countries trying to define national rules, and hoping for more stabilisation but often only contributing to already massive complexity of the system.

Similar challenges, stemming from the global and constantly evolving nature of cryptocurrencies, exist with regard to accounting rules. Various regulators, such as the International Accounting Standards Board, Financial Accounting Standards Board, Accounting Standards Board of Japan and Australian Accounting Standards Board have started their cryptocurrencies' assessments in order to define the proper classification. However, according to their latest announcement, the topic requires further investigation in order to compile a recommended set of actions (EY, 2018; PwC, 2018). Question whether a new asset class should be established is also under discussion with no final answer being given yet.

4. Anti-Corruption Compliance Agenda

Based on the examples presented in preceding paragraphs, it could be concluded that cryptocurrencies have always been challenging with regard to anti-corruption measures and due to the fact that the new phenomenon has been attracting more and more, often very creative, users, and already a high number of abusive practices has been discovered, it is no longer feasible to postpone the discussion on anti-corruption measures.

First of all, it is important to realise that with regard to corruptive behaviours discussed in the paper, no new techniques were utilized but rather those that have a long history on regular markets. Moreover, the presented negative outcomes happened not due to technical failures of the blockchain technology but they resulted from the behaviour of the people and often took place outside the three dimensional structure. As a result, taking the ICO mechanism as an example, despite its technical novelty, compliance experts could take advantage of

their knowledge about all past abusive behaviours in order to define preventive measures and implement procedures that could limit attractiveness of illicit practices.

With regard to theft, from an anti-corruption compliance perspective, it is not the emergence of theft that is the most interesting, but rather the way these stolen cryptocurrencies could be spent and which kinds of actions could they finance. The larger amounts are lifted, the more illicit activities they can fund and thus cause even more severe problems. Compliance officers are however well aware of the various techniques which could be used in order to both increase the security of the users' deposits and curtain the number of attacks. Again, the novelty of the cryptocurrencies is not a challenge, as the wrongdoings happen not inside the blockchain but in the accompanying infrastructure, thus previous security expertise might prove to be very helpful. As a result, it might be worth imposing both high security standards with regard to all exchange and trading platforms and introduce recurring audits or other control mechanisms in order to limit the scale of attacks and thus the size of potential corruption.

In case of decentralised trading platforms, the potential anti-corruptive measures might be tougher to implement. Due to the over the counter nature of these constructs, it could be much harder to define players responsible for security standards' implementation which as a consequence could encourage even more illicit users to undertake these actions. Therefore, in case of these structures, compliance officers have a more complex challenge to solve and should consider innovative mechanisms that could effectively diminish the chances of such risks. It might be useful for example to define a new standard on how such over the counter trading could take place which on the one hand would be more attractive for the users and still allow for expected return, and on the other hand could make the illicit practice simply no longer appealing.

An interesting approach, namely reframing (Jong & Dijk, 2015) has generated a vivid interest among managers. Reframing might be also worth considering when defining anti-corruption compliance agenda. The concept asks for (i) definition of key beliefs driving business practices or business models, (ii) deciding what is their underlying driver or notion and then (iii) turning such a notion on its head. The power of out of the box thinking has to be mentioned as well. It is very important to utilise the new way of thinking about preventive measures with regard to novel technology. Cryptocurrencies are a global, open-source and constantly evolving phenomenon, often called even disruptive, and as such it has to be approached in an innovative manner. As formulated by the famous expert, Professor Christensen (Bower & Christensen, 1995; Christensen, Raynor, & McDonald, 2015), the best way to attack a disrupter is to disrupt him, which might be also a useful advice for compliance officers.

The definition of a proper anti-corruption agenda also requires a holistic approach, meaning that when setting such practices, all areas which could potentially be at risk, should be addressed. It is, for example, not enough to regulate the cryptocurrency exchange platforms, as the illegal practice could happen on peer-to-peer exchanges or elsewhere. Due to the fact that the emergence of cryptocurrencies could encourage more users to commit crimes such as ransom ware attacks, it is essential for compliance experts to put themselves in bad actors' shoes in order to define measures which could discourage these players from undertaking illicit

practices at all. It is also essential to build teams in which experts have backgrounds in various fields e.g. in order to define proper tax regulation both taxation and cryptocurrencies experts are required.

As an inherent part of a cryptocurrency, blockchain technology also offers lots of opportunities for anti-corruption compliance. Manipulation of the ledger is almost impossible due to high costs and its distributed nature. Immutable audit trail delivers detailed data sets enabling a profound analysis of all past actions, making the whole analysis process smoother and more efficient (Pilkington, 2016; Tapscott & Tapscott, 2016). Thanks to the public nature of blockchain it has become a lot easier to trace all moves and therefore define the patterns allowing for more promising corruption prevention. Moreover, the irreversible history of all past actions makes it much easier to prove illicit practices in case such a proof is needed. The idea of smart contracts, programs running on top of the blockchain that are self-executing, offers another advantage (Bartoletti & Pompianu, 2017). Smart contracts could facilitate the work of compliance officers and also, once rolled out, improve the security of various practices. For example, in case the instruction given by a hacker as a consequence of a ransom ware attack is required to have a smart contract form. One cannot prevent such attacks from happening, but at least it would be certain that once the instruction is followed and bribery is paid, the access to files or other promises would be executed.

Moreover, cryptocurrencies are constantly evolving and open-source innovations, implying the need for a coordinated and international approach in defining worldwide harmonized regulations. This could prevent corruptive practices and still stimulate the development of innovative ideas. In case uncoordinated actions are undertaken, anti-corruption measures might be less successful as illegal activities, characterised by their global character, would move around the world in search for a more friendly environment, and thus considerably diminishing the success rate of preventive measures.

Finally, it is highly important to define the proper level of regulation and standardization. Innovations and entrepreneurial thinking are principal for the economic growth, and therefore it is important to impose rules which on the one hand would be warmly welcomed by the good players supporting the proliferation of their businesses, and on the other hand discourage bad actors from abusing cryptocurrencies.

5. Conclusion

Innovation always comes with two promises: one which offers huge opportunities for existing practices, for example by making them more efficient, inclusive or safer, and the other that relates to potential risks and challenges that this new proposition could bring. The same holds true for cryptocurrencies, which introduce a solution able to fulfil the role of fiat money but in constantly growing digital economy. However, as the examples prove, such a novel solution is not problem-free. Cryptocurrencies attract both good and bad players, with the latter deciding to utilize the new tool for illicit practices. Many examples of corruptive behaviours involving cryptocurrencies have been identified such as scams, market abuses, exchanges' thefts, ransom ware attacks, dark market transactions and terrorist financing. Cryptocurrencies have become also very popular for those wishing to avoid taxes, who for a long time benefited from the lack of proper tax regulation.

As a result, from being a niche topic, cryptocurrencies have moved up to the top headlines, being discussed on national and international levels. Regulators from all over the world agree that there is a need for harmonized approach towards cryptocurrencies, nevertheless no details on its implementation have been provided so far. Anti-corruption compliance agendas have to be extended in order to cover new risks and challenges related to cryptocurrencies, as in case of the full ignorance, the preliminary blessing could become a serious curse. Compliance officers should concentrate on preventive measures which require an innovative approach and out of the box thinking. Blockchain technology offers a huge advantage as it provides an immutable audit trail based on which some illicit behavioural patterns could be defined.

Introduced almost ten years ago, cryptocurrencies are still in an early stage of their development, lacking taxonomies, standards, regulations or even harmonized definitions. Due to their very complex nature, they require a thorough analysis and versatile exploration in order to define their true potential, possible risks and proper measures which could prevent corruption practices and still contribute to sustainable development of the cryptocurrencies' innovations.

Bibliography

Abraham, C. (2018, October 13). The Origin Story of the Initial Coin Offering (ICO) Token Sale History

Adriano, A. (2018, June). Crypto Bubble? An Historical Analysis of Financial Crises. *IMF F&D Magazine*, *55*(2)

Alexandre, A. (2018). New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams.

Bank für Internationalen Zahlungsausgleich, & Committee on Payments and Market Infrastructures. (2015). *Digital currencies*. Basel

Bartoletti, M., & Pompianu, L. (2017). *An empirical analysis of smart contracts: platforms, applications, and design patterns*.

Basel Institute on Governance. (2018). Basel AML Index 2018 Report.

Benedetti, H., & Kostovetsky, L. (2018). *Digital Tulips? Returns to Investors in Initial Coin Offerings* (SSRN Scholarly Paper No. ID 3182169). Rochester, NY: Social Science Research Network.

Bonneau, J., Felten, E., Miller, A., & Narayanan, A. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton: Princeton University Press.

Bower, J. L., & Christensen, C. M. (1995). Disruptive Technologies: Catching the Wave.

Browne, R. (2017). Hackers withdraw $143,000 from bitcoin wallets tied to WannaCry ransomware.

Budish, E. (2018). The Economic Limits of Bitcoin and the Blockchain, 23.

Chanson, M., Gjoen, J., Risius, M., & Wortmann, F. (2018). Initial Coin Offerings (ICOs): The role of Social Media for Organizational Legitimacy and Underpricing, 17.

Cheng, E. (2018). Japanese cryptocurrency exchange loses more than $500 million to hackers.

Christensen, C. M., Raynor, M. E., & McDonald, R. (2015). What Is Disruptive Innovation? *Harvard Business Review*

CipherTrace. (2018). Cryptocurrency Anti-Money Laundering report Q2.

Clark, J., & Narayanan, A. (2017), Bitcoin's Academic Pedigree. *Communication of the ACM*, *60*(12), 36–45.

EBA. (2014). EBA Opinion on Virtual Currencies.

Efanov, D., & Roschin, P. (2018). The All-Pervasiveness of the Blockchain Technology. In *The All-Pervasiveness of the Blockchain Technology* (Vol. 123, pp. 116–121). Procedia Computer Science

Esteves, R. (2018). Savedroid Fakes $50 Million ICO Exit Scam, Community Outraged.

European Central Bank. (2015). *Virtual currency schemes: a further analysis.* Frankfurt am Main: European Central Bank

EY. (2018). IFRS: Accounting for crypto-assets

FabricVentures, & TokenData. (2018). *The State of the Token Market Final2.pdf*.

Federal Bureau of Investigation. (2017). AlphaBay Takedown

Fisch, C. (2019). Initial coin offerings (ICOs) to finance new ventures. *Journal of Business Venturing*, *34*(1), 1–22.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2018). *Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?* (SSRN Scholarly Paper No. ID 3102645)

Friedman, H. H., & Friedman, L. W. (2009). *The Global Financial Crisis of 2008: What Went Wrong?* (SSRN Scholarly Paper No. ID 1356193)

Fry, J., & Cheah, E.-T. (2016). Negative bubbles and shocks in cryptocurrency markets. *International Review of Financial Analysis*, *47*, 343–352.

Gantori, S., Donovan, P., Ganesh, K., DeMichiel, M., Dennean, K., Trussari, F., & Klien, M. (2017). *Cryptocurrencies Beneath the Bubble*

Groendahl, B. (2018). Austrian Bitcoin 'Scam' Triggers Police Search Across Europe - Bloomberg.

Gupta, V. (2017, March 6). The Promise of Blockchain Is a World Without Middlemen.

Hacker, P., & Thomale, C. (2017). *Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law* (SSRN Scholarly Paper No. ID 3075820)

Hamrick, J. T., Rouhi, F., Mukherjee, A., Feder, A., Gandal, N., Moore, T., & Vasek, M. (2018). *The Economics of Cryptocurrency Pump and Dump Schemes* (SSRN Scholarly Paper No. ID 3303365)

Higgins, S. (2014, July 7). ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide

Higgins, S. (2017). From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited.

Hileman, G., & Rauchs, M. (2017). *2017 Global Blockchain Benchmarking Study* (SSRN Scholarly Paper No. ID 3040224)

Houben, D. R., & Snyers, A. (2018). Cryptocurrencies and blockchain, 103.

Howell, S. T., Niessner, M., & Yermack, D. (2018). *Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales* (No. w24774). National Bureau of Economic Research

IMF Staff Team. (2016). Virtual Currencies and Beyond: Initial Considerations. *Staff Discussion Notes*, *16*(03), 1

Johnson, S. (2018, January 16). Beyond the Bitcoin Bubble. *The New York Times Magazine*

Jong, M. de, & Dijk, M. van. (2015). Disrupting beliefs: A new approach to business-model innovation | McKinsey

Keatinge, T., Carlisle, D., & Keen, F. (2018). Virtual Currencies and terrorist financing: assessing the risks and evaluating responses

Keidar, R., & Blemus, S. (2018). *Cryptocurrencies and Market Abuse Risks: It's Time for Self-Regulation* (SSRN Scholarly Paper No. ID 3123881). Rochester, NY: Social Science Research Network

Khatri, Y. (2018). FBI Arrests AriseBank CEO Over $4 Million Crypto Fraud

Knight, K. B. and J. (2009, September 16). Lehman's Three Big Mistakes

Martineau, P. (2018). Inside the group chats where people pump and dump cryptocurrency

Memoria, F. (2017). Tracing Ethereum and Bitcoin? Darknet's Two Biggest Marketplaces are Busted

Memoria, F. (2018). First Bitcoin Cash Ransomware Makes It Impossible to Decrypt Files

Moore, T., & Christin, N. (2013). Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In A.-R. Sadeghi (Ed.), *Financial Cryptography and Data Security* (Vol. 7859, pp. 25–33). Berlin, Heidelberg: Springer Berlin Heidelberg

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System

Partnoy, F. (2013, September 16). Five Years After Lehman's Collapse, Bankers Still Haven't Confronted Their Biases

Pilkington, M. (2016). *Blockchain Technology: Principles and Applications*. France: University of Burgundy.

PwC. (2018). Cryptocurrency-bitcoin-accounting

Securities and Markets Stakeholder Group. (2018). Own Initiative Report on Initial Coin Offerings and Crypto-Assets

Shifflett, S., & Vigna, P. (2018). Some Traders Are Talking Up Cryptocurrencies, Then Dumping Them, Costing Others Millions

Smith, B. (2018). What would you have made if you held McAfee's "Coin of the Day" to date?

Suberg, W. (2018). Vietnam: Pincoin, Ifan ICOs Exposed As Scams That Allegedly Stole $660 Million

Tabarrok, A., & Cowen, T. (2015, April 6). The End of Asymmetric Information.

Tapscott, D., & Tapscott, A. (2016, May 10). The Impact of the Blockchain Goes Beyond Financial Services

The Economist. (2018, April 26). Crypto money-laundering

The Law Library of Congress. (2018, June). Regulation of Cryptocurrency Around the World

US Confiscates Millions in Cryptocurrencies in Alphabay Forfeiture Case. (2018)

Wikipedia. (2019). Silk Road (marketplace)

Williams-Grut, O. (2018, January 31). Startups raised $5.6 billion through ICOs in 2017 - Business Insider Deutschland

World Bank Group. (2017). *Distributed Ledger Technology (DLT) and Blockchain* (FinTech Note, No. 1). Washington, US

Xu, J., & Livshits, B. (2018). The Anatomy of a Cryptocurrency Pump-and-Dump Scheme