MAY 2019

FSBC Working Paper

Crypto Currencies as a New Challenge to Anti-Money Laundering Regulation and the Know-Your-Customer-Principle

Lutz Auffenberg

Crypto currencies and especially so-called privacy coins like Monero or Zcash expose the European legislators and regulators to critical systemic challenges when it comes to Anti-Money Laundering regulation. This paper shows the current regulatory approach of European regulators as well as upcoming legislation and critically assesses their appropriateness with regard to crypto currencies.

Current situation: the use of crypto currencies as a means of money laundering and criminal purposes

The presentation of the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" by Satoshi Nakamoto[1] in October 2008 was the first proposal of a fully-fledged and secure electronic payment system that does not require any trusted party as intermediary for the processing of payments. In Bitcoin, users can send monetary value directly to each other without a bank or financial institution involved, not hindered by any national borders and just within a few minutes.

The backbone of this electronic payment system is the blockchain, a distributed ledger of the full transaction history maintained by a peer-to-peer network which ensures that double-spending of a user's balance is not possible. The Bitcoin blockchain and with it the whole transaction history is available to everyone through the use of blockchain explorer tools[2]. User privacy shall be maintained by keeping the public keys of the users anonymous. Users are not required to provide any personal information for participating in the Bitcoin network. They only have to download and run

Frankfurt School Blockchain Center
www.fs-blockchain.de
contact@fs-blockchain.de

Follow us
www.twitter.com/fsblockchain
www.facebook.de/fsblockchain

**Frankfurt School of
Finance & Management gGmbH**
Adickesallee 32-34
60322 Frankfurt am Main
Germany

the open source and freely accessible Bitcoin client and generate a new Bitcoin address consisting of a public and a private key, where they can receive and send Bitcoins from and to. The Bitcoin addresses are represented by a chain of 26 to 35 characters and are not publicly linked to each owner.

Due to its ability to be used for fast and international transactions directly between sender and recipient, Bitcoin is not only used by honest users but also for transactions in the context of criminal activities. On former black market internet platforms like “Silk Road”, “Agora” or “Evolution”, where illegal goods or services were offered, Bitcoin was the only means of payment to be accepted.[3] On currently existing black market internet platforms like “Aero Market” or “Tochka”, the virtual currency “Monero” becomes more and more popular due to the fact that its technology has a stronger focus on privacy than Bitcoin. Shortly before it was shut down in July 2017 the black market internet-platform “AlphaBay” announced it would implement “Zcash” as a means of payment, another virtual currency with a very strong focus on the privacy of its users.[4]

These new decentralised peer-to-peer payment technologies provide serious challenges for financial regulators and criminal prosecution authorities since the existing money laundering and terrorist financing prevention rules are dependent on intermediaries with knowledge about the transactions of their customers. As soon as intermediaries are not necessary anymore for the transfer of monetary value, the existing rules become ineffective and must be questioned.

Administrative and institutional awareness. National regulators and regulatory institutions worldwide often pointed out that virtual currencies are being used as payment method for criminal activities and issued reports and warnings. In October 2012[5] and February 2015[6] the European Central Bank (ECB) issued papers on virtual currency schemes, including attempts to define virtual currencies and emphasizing that such payment units can be used by criminals, fraudsters and money launderers and may therefore represent a challenge to regulatory bodies. The European Banking Authority (EBA) published a warning to consumers on virtual currencies in December 2013[7] and expressed their opinion on virtual currencies in July 2014[8] pointing out the risks associated with the use of virtual currencies for Anti-Money Laundering (AML) regulation. In June 2014[9] the Financial Action Task Force (FATF) published a report on virtual currencies, also setting out the potential risks for AML regulation associated with their use. In June 2015[10] the FATF issued a guidance for national regulators and the private sector on how to deal with AML and Counter-Terrorist Financing (CTF) issues in the context of virtual currencies. The German Bundeskriminalamt (BKA) pointed out in its yearly report on cybercrime in 2016[11] that virtual currencies such as Bitcoin, Litecoin or Ethereum are very often used by criminals in connection with computer-based fraud, bribery, money laundering or financing of terrorist activities since their transfer does not necessarily involve any financial institutions and therefore grants a higher level of anonymity than usual payment methods.

Level of privacy in Bitcoin. The author of the Bitcoin whitepaper was aware of the fact that the electronic cash system he has offered does not grant full anonymity to the users. The publicly available Bitcoin blockchain sets out a full history of all Bitcoin transactions validated so far as well as the Bitcoin addresses of sender and recipient, the transferred Bitcoin amount and the time of the transaction. It can be inferred that the level of privacy in Bitcoin is rather pseudonymous than anonymous, since users are represented on the Bitcoin blockchain as public Bitcoin addresses. Satoshi Nakamoto therefore emphasized in his whitepaper that generating a new Bitcoin address for every transaction is recommended to keep transactions from being linked to a common sender or recipient.[12] Several researchers have shown that a sophisticated analysis of the Bitcoin blockchain enables investigators to link specific Bitcoin addresses to specific users.[13] Whenever a Bitcoin address can be linked to a specific person, e.g. in the case of companies publishing their Bitcoin address on their website or in the case of an unforced disclosure of a private or institutional Bitcoin address for the purpose of receiving donations or alike, a reference point for such analysis is made. In many cases it is also possible to conclude that different Bitcoin addresses belong to the same person, for example by exploiting the properties of generally used Bitcoin clients as well as a behaviour-based analysis of the Bitcoin addresses. The not necessarily illegal need of the users for privacy has brought so-called Bitcoin mixers[14] into existence, services obfuscating Bitcoin transactions for users by receiving bitcoins and then sending them to a determined Bitcoin address in accordance with the client's order. Such services, of course, lead to a centralization of the Bitcoin system since the user of a mixing service must trust the service provider. Furthermore, the linkability of transactions that have been mixed may be more difficult but still generally possible through a blockchain analysis as explained above.

The level of privacy in Bitcoin is rather pseudonymous than anonymous, since users are represented on the Bitcoin blockchain as public Bitcoin addresses.

Level of privacy in Monero. Monero is a crypto currency with a strong focus on the privacy of its users. Technically it is based on the CryptoNote[15] protocol which suggests the use of ring signatures instead of single private key signatures for the signature of transactions. When creating a Monero transaction the sender's Monero address is grouped with other randomly chosen Monero addresses which additionally appear in the transaction as possible senders of the transaction. As a result, it is not possible to exactly determine the true sender of a Monero transaction. For investigators, it is, however, possible to determine that a specific person is part of a group of possible senders. Therefore, the level of privacy of a Monero transaction is reliant on the size of the group of possible senders, the so-called "mix-in level". According to the hiding-in-the-crowd-principle, the level of privacy increases, the higher the mix-in level is. The current default number of group members is six. It is possible for a Monero sender to choose a higher mix-in level by offering a higher fee to his transaction.

When sending Monero units to a recipient's public Monero address, a one-time address is automatically created by the system where the funds are actually sent to, a so-called "stealth address". Only this stealth address and not the public address appears in the public Monero blockchain which is why neither the sender nor any other investigator is able to infer from the public address of the recipient how much funds the respective public address is currently holding and in which other transactions it has been involved. The recipient of the transaction has a secret view key which allows him to allocate the stealth address on the Monero blockchain and to see his funds.

In addition to that, a sender can create a transaction view key which can be disclosed to a person for proving that a Monero transaction has been made.

Level of privacy in Zcash. Another crypto currency with a strong focus on privacy is Zcash. Originally it was meant to be an update to the Bitcoin protocol for enhancing privacy. Since the idea did not get enough support in the Bitcoin community, the developers created an autonomous crypto currency in the form of Zcash. The project has been massively criticized in the past for several reasons.[16] For the purpose of this article the focus will be set on the privacy-related features of Zcash.

Zcash uses “Succinct Non-interactive Arguments of Knowledge” proofs, so-called zk-SNARK proofs, for encrypting shielded transactions on the Zcash blockchain. Although zk-SNARK-encrypted, Zcash transactions can still be verified as valid according to the consensus rules used in Zcash. Using zk-SNARK proofs enables a party to prove to another party within only a few milliseconds that a certain piece of information is known without revealing the information itself.[17] Therefore, this technology makes it possible to verify the validity of a transaction without knowing who the sender or the recipient is and what the value of the Zcash transaction is.

In Zcash, users can choose between using transparent or private Zcash addresses. While transparent addresses and balances held on them are visible on the Zcash blockchain, private addresses do not show the account address, nor the value held or received. Users can therefore choose whether they want their transaction to be public or private by using a transparent or private Zcash address. As a consequence, four different types of transactions may occur in the Zcash blockchain: fully public transactions when two public addresses are used, shielding transactions where a transparent address transfers Zcash units to a private address, deshielding transactions where a private address sends Zcash units to a public address and private transactions where only private addresses are involved. The value of a shielding or deshielding transaction will not be visible on the Zcash blockchain as it will not be determinable how many addresses are involved on the private side of the transaction.

Status quo of AML regulation in the European Union and Germany

AML regulation in the European Union. In the European Union AML regulation has been harmonized since 1991 when the first AML directive (EG/91/308) obligated the member states to ensure that their national laws provide some regulatory minimum standards in relation to money laundering and terrorist financing prevention. The currently effective fourth AML directive (EU/2015/849) had to be transposed into the national law of the member states by June 26, 2017.

The approach of the AML directive is to impose specific monitoring and verification obligations on certain persons and companies with a typically higher risk of being involved in money laundering or terrorist financing activities. Such obliged entities are generally banks, insurance companies and other financial institutions but also non-financial entities such as, for example, audit companies, notaries, trusts and fiduciaries as well as gambling services, estate agents or other persons trading in goods to the extent that payments are made or received cumulatively amounting to 10,000 euros or more. An exclusive catalogue of obliged entities is set out in art. 2 of the fourth AML directive. Therefore, the systemic starting point of the AML regulation according to the fourth AML directive are always the obliged parties.

Under the regime of the fourth AML directive obliged entities must conduct a specific customer due diligence every time before establishing a new business relationship with customers. In addition to that, they must apply or even repeat the due diligence measures in case of occasional transactions exceeding a total of 15,000 euros. Besides, in case of suspicious transactions, where there are any indications of money laundering or terrorist financing, the obliged entities must apply the due diligence measures. In the case of traders of goods, the due diligence obligation is already triggered by a transaction of 10,000 euros or more. For gambling services this threshold is even stricter since they must conduct the due diligence obligations when there is a transaction of 2,000 euros or more. Furthermore, obliged entities must install an effective risk management for avoiding money laundering and terrorist financing.

The most important part of the customer due diligence is the obligation to identify the customer, the so-called Know-Your-Customer-principle (KYC-principle). Obliged entities have to ask customers for their name, address, date of birth and nationality as well as the purpose of the business relationship or the transaction and identify the beneficial owner. If the customer is not a private person but a legal entity, the obliged entities must additionally ask about its legal form, company register number and names of the representatives and shareholders of the legal entity. After collecting the information, obliged entities must review and check the information collected, e.g. by reviewing the passport of a private person or by verifying the information obtained with the company register.

Whenever an obliged entity has any evidence or indication that monies derive from criminal activities, it must immediately inform the national Financial Intelligence Unit (FIU) - a central authority established by each member state for this purpose. Besides, it has to follow its further instructions in order not to endanger necessary investigations.

Neither crypto currencies nor its users or businesses related to them are explicitly mentioned in the fourth AML directive. The regulatory customer due diligence duties and further obligations are therefore generally not imposed on persons or companies dealing with or offering services in relation to crypto currencies. However, the fourth AML directive may be applicable in crypto currency-related cases.

Firstly, money laundering is defined in art. 1 para. 3 of the directive as the "conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation of such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of that person's action". "Property" in this sense means, according to art. 3 para. 3 of the directive, any "asset of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form, including electronic or digital, evidencing title to or an interest in such assets". Crypto currencies as incorporeal digital assets may insofar be subject to money laundering activities. Consequently, an obliged entity receiving notice of a criminal activity in connection with a crypto currency transaction will be obliged to give immediate notice to the national FIU.

Secondly, it is of course possible that a bank or another financial institution which is professionally dealing with crypto currencies is involved in a suspicious transaction with a customer or business partner. This bank or financial institution is obliged to inform the national FIU about any suspicious facts in connection with the transaction because of its status as obliged entity. In this context it is important to emphasise that crypto currency exchanges, professional crypto currency traders or other crypto currency related businesses are not automatically considered as banks or financial institutions in the sense of the AML directive. They only are considered as such if they conduct banking activities or financial services which are subject to public financial supervision.[18]

AML regulation in Germany. The AML regulatory situation in Germany is special. Like all other member states Germany had to transpose the standards from the fourth AML directive into national law until June 26, 2017. While the general rules from the fourth AML directive are therefore harmonized in the form of the German AML Act with the rules in the other European member states, the German financial supervision authority BaFin qualified crypto currencies such as Bitcoin, Litecoin or comparable clones officially as "units of account" and therefore as financial instruments in the sense of the German Banking Act (KWG).[19] BaFin did not make a sophisticated differentiation between the different technologies behind crypto currencies at that time but rather stated generally that "Bitcoins and comparable clones" are financial instruments under German regulatory law. In May 2018 BaFin again confirmed its view on crypto currencies as financial instruments by stating that, according to its administrative practice, it qualifies "crypto tokens" as units of account and therefore as financial instruments.[20] According to BaFin, the term "units of account" covers all means of payment created under private law which are intended to be used in computer networks as an alternative currency and therefore as a synthetic alternative to legal tender.[21] This general approach which has not been tested by the German courts so far means that all crypto currencies and blockchain tokens which are intended to be used as a means of payment are likely to be classified as financial instruments by BaFin under the KWG.

The consequence of this qualification is that the KWG is applicable to companies with business models based on crypto currencies. As soon as the service offered is qualified as a banking activity or financial service in the sense of the KWG, the respective company will be regarded as a "credit institution" or "financial institution" and must obtain permission from BaFin prior to starting the business and will then be subject to the ongoing supervision of the authority to the extent of the regulated business.

According to sec. 25h KWG institutions must install stricter risk management systems than usual obliged entities in the sense of the German AML Act. While obliged entities must install processes for the determination, analysis and mitigation of money laundering and terrorist financing risks associated with their business and customers in general, institutions have to extend these systems additionally to criminal activity risks for their own properties in order to avoid systematic failure with negative market effects. Furthermore, according to sec. 25h para. 3 of the German Banking Act, institutions must investigate all transactions in relation to usual transactions being extraordinarily high or complex, unusual or not appearing in any obvious economic context.

Both sec. 6 para. 2 no. 4 of the German AML Act as well as sec. 25h para 1 KWG oblige companies to continuously implement and develop effective measures to enhance their risk management systems in order to effectively avoid the misuse of new innovative financial instruments and technologies for the purpose of money laundering and terrorist financing or the obfuscation of business relationships or transactions. Such financial instruments or technologies may of course be crypto currencies and distributed ledger technologies. German institutions therefore have to extend and enhance their risk management systems as soon as they come in contact with crypto currency-related transactions which can happen easily, e.g. when a customer uses a bank account of the institution for a cash-out-transaction from a crypto currency exchange.

Sec. 25k KWG obliges institutions to conduct a full customer due diligence in accordance with the AML Act in the case of accepting cash. The minimum thresholds of the AML Act are not applicable to institutions in these cases.

Current legislative approaches for an appropriate AML regulation

Even before the rules of the fourth AML directive needed to be transposed into national law of the EU member states the European Commission proposed an amendment of the fourth AML directive on 5 July 2016 as a reaction to the terrorist attacks in Paris in November 2015 and Brussels in March 2016 as well as the so-called "Panama papers" leak.[22] The proposal was the result of a politically motivated action plan of the European Commission published on February 2, 2016.[23] On December 15, 2017 the European Commission, the European Parliament and the European Council agreed on a final text version for an amending directive to the fourth AML directive which has finally come into effect on May 30, 2018. This amending directive is often referred to as the fifth AML directive. Member states now have to transpose the new rules into national law until January 20, 2020.

The fifth AML directive of the European Union. As a reaction to the rapidly growing importance and adoption of crypto currencies the fifth AML directive sets out a definition of virtual currencies. Furthermore, the amending directive extends the catalogue of obliged entities by “providers engaged in exchange services between virtual currencies and fiat currencies” and “custodian wallet providers”.

As a reaction to the rapidly growing importance and adoption of crypto currencies the fifth AML directive sets out a definition of virtual currencies.

According to the wording of the amending directive, virtual currencies will be defined as “a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically”. The wording is an advancement of previous institutional proposals for definitions of virtual currencies, as for example by the ECB in 2012[24] and 2014[25]. It is important to notice that the definition does not explicitly contain any reference to any form of distributed ledger technology which is why it may also include centralized payment schemes not based on blockchain technology. Examples are computer game currencies such as Linden Dollars (Second Life) or Warcraft Gold (World of Warcraft), issued by a private company as the game platform operator.

The inclusion of providers engaged in exchange services between virtual currencies and fiat currencies into the catalogue of obliged entities will impose the discussed obligations from the fourth AML directive on these service providers, especially the identification and verification of customers as well as the surveillance of the transactions executed through their services. Not only will online virtual currency exchange platforms in the form of multilateral trading facilities be affected but also traders offering the direct sale and purchase of virtual currencies from their own stocks to customers, as long as the conversion of virtual currency into fiat currency is offered, that is to say central bank issued currency with legal tender status. In contrast to that, exchange service providers only converting virtual currencies into other virtual currencies will not be covered by the wording of the provision since a conversion of fiat currency is not involved in their services. The European Commission emphasized in its proposal, dated July 5, 2016, that the inclusion into the catalogue of such gateways, acting as the needle eye between virtual currencies and broadly accepted fiat currency, is a necessary and appropriate measure for ensuring that the AML competent authorities of the member states receive sufficient information about virtual currency-based transactions for the purpose of AML prevention which they do not have in the current system of the fourth AML directive.

The amending directive provides a definition for custodian wallet providers which shall also be included in the catalogue of obliged entities. According to the definition in the amending directive, a custodian wallet provider is “an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies”. It is remarkable that custodian wallet providers shall be qualified as obliged entities even if they are not at all involved in a conversion of virtual currency to fiat currency or vice versa. The European Commission justifies the inclusion of custodian wallet providers with the argument that they act as gatekeepers giving the public access to virtual currencies. The definition of wallet providers is limited to providers safeguarding private keys required to access and transfer virtual currencies. Service providers only offering software programs which enable users to save cryptographic private keys on local devices therefore do not fall under the definition.

Approach of the German legislator. So far, the German legislator has been reluctant to set up codified laws on crypto currencies or other blockchain-related issues. As can be seen from the 2018 coalition contract of the governing parties CDU/CSU and SPD, this approach will not be changed in the near future. It is remarkable that the parties have mentioned the word “blockchain” in the contract in five sections. However, it seems that the parties do not intend to pass any national laws but rather to campaign for a consolidated blockchain strategy as well as an adequate legal framework for the trade of crypto currencies and tokens at the European and international level.[26] The coalition contract is a guideline for the 19th legislative period and only sets out general positions instead of going into detail. AML regulation in the context of crypto currencies is therefore not explicitly mentioned in the contract. Apart from that, the position of BaFin to classify crypto currencies as financial instruments, with the consequence that many market participants with blockchain-related business models already fall under the currently applicable AML regulation in Germany, might have the effect that the German legislator does not consider the current regulatory situation to be inadequate.

Critical statement on the crypto currency-related part of the fifth AML directive

The amending directive to the fourth European AML directive in its current form shall extend the catalogue of obliged entities by virtual currency exchange service providers and custodian wallet providers and additionally provide a definition of virtual currencies for legal certainty. The general systematic approach of obligating intermediaries involved in transactions shall not be changed. Apparently, for the time being, the European legislator holds the opinion that an identification and verification of customers together with a surveillance of transactions and, in the event of suspicious facts, a notification obligation of involved service providers is sufficient for an effective and adequate AML regulation in the European Union. However, the technical construction of blockchain-based payment systems may require a more tailored approach since intermediaries are not necessarily involved in transactions performed with crypto currencies. Maybe the most innovative achievement of crypto currencies and blockchain technology is the fact that a transfer of value can be accomplished *without* an intermediary that processes the transaction. This decentralization of crypto currency schemes enables users to transfer units of monetary value directly via a peer-to-peer system to a recipient. In the context of AML regulation this means that criminals performing transactions for the purpose of money laundering, terrorist financing or other criminal activities are not dependent on any intermediary for the transfer of value.

The technical construction of blockchain-based payment systems may require a more tailored approach since intermediaries are not necessarily involved in transactions performed with crypto currencies.

The European Commission justified the extension of the catalogue of obliged entities in its proposal for the amending directive with the argument that exchange service providers are the connection between crypto currencies and fiat money and therefore necessary intermediaries for crypto currency users. The same argument was used in regard to custodian wallet providers who give people access to crypto currencies and therefore occupy a central position. The arguments, however, are only partially valid as long as crypto currencies are not broadly or at least widely accepted by people as a means of payment. This is due to the fact that exchange services would no longer be necessary in these scenarios for withdrawing the monetary value from crypto currencies. Even if crypto currencies are not broadly accepted as a means of payment nowadays, the represented monetary value can rapidly and internationally be transferred. As soon as a criminal finds any person willing to purchase crypto currency directly from him without the involvement of an intermediary, a conversion of crypto currency to fiat money can be performed anywhere in the world in only a few minutes.

The KYC procedures, surveillance and notification obligations of the obliged entities of the current fourth AML directive are therefore not effective with regard to the prevention and intervention of money laundering, terrorist financing and criminal transactions. In addition to that, they cause enormous administrative burdens on exchange service providers and custodian wallet providers as they must implement complex risk management systems and surveillance mechanisms. Furthermore, the KYC procedures will affect legal users to the greatest extent because criminal users will most probably avoid using service providers that are obliged entities under the fourth AML directive.

Another criticism of the approach of the amending directive is the fact that the possibilities of obliged entities to monitor the transactions of their customers are limited. Firstly, the use of new crypto currency addresses for each new transaction has already been recommended in the Bitcoin whitepaper in 2008 for the (legitimate) purpose of transaction data protection and financial privacy. Secondly, many wallet software programs automatically generate new addresses for each transaction. Thirdly, in crypto currency systems with a stronger focus on privacy such as Monero or Zcash or in case of the involvement of a Bitcoin mixing service, crypto currency addresses and transactions may not even be publicly visible. These facts make it impossible (or at least harder) for investigators to assess whether a crypto currency user is acting in a suspicious way which may justify a further assessment or notification to the competent FIU. A sophisticated blockchain analysis[27] may be possible but far too complex to possibly impose such a burden on obliged entities.

As the use of intermediaries can be avoided in crypto currency transactions, a more effective approach for AML regulation in the context of crypto currencies would be preferable. If in such an approach the intermediaries would not be the reference point for regulatory measures, another group of systematically necessary participants would have to be addressed. Since not all crypto currencies work on the basis of the proof-of-work mechanism as explained in the Bitcoin whitepaper, miners do not exist in all crypto currency schemes which is why they cannot be an adequate addressee for AML regulatory obligations. The developers of crypto currencies often stay anonymous[28] and therefore cannot be adequate addressees of regulation. Imposing regulatory obligations on users of a crypto currency in general would also be problematic because criminal users would simply not obey such rules. Therefore, such an approach would be ineffective.

There have been proposals suggesting a crypto currency-related AML regulation on the basis of blacklisting or whitelisting models.[29] In a whitelisting model, legitimate users could, for example, publish their crypto currency addresses and so self-verify. The legislator could additionally oblige users of the crypto currency to limit their transactions only to verified addresses set out on the whitelist. In contrast to that, in a blacklisting model, crypto currency addresses that have been involved in criminal transactions could be set out on a publicly available list. The legislator could additionally prohibit users of the crypto currency from performing any transactions with the addresses set out on the blacklist. It would also be possible to set out criminal transactions instead of addresses on blacklists in order to avoid a criminal simply generating a new address not yet listed.

The listing approach also causes several problems which in the case of regulatory implementation would lead to ineffectiveness. Firstly, a list would have to be operated and updated for every crypto currency in existence, preferably by an official institution. Lists of different crypto currency systems would furthermore have to be linked to each other in order to determine connected transactions performed in various crypto currency schemes. Secondly, list models would not be effective in crypto currency schemes where mixing services, ring signatures or zero-knowledge proofs for the obfuscation of transactions and addresses are used. Stealth addresses, for example, are not publicly visible on the Monero blockchain, neither are private transactions in Zcash with shielded inputs and outputs visible on the Zcash blockchain.

Another problem with listing models is the fact that they can only be effective when flanked by a legislative prohibition of interaction with listed and/or unlisted addresses because peer-to-peer transactions in crypto currency systems are definite and cannot be revoked. This could lead to situations where legal users unintentionally interact with prohibited addresses. Crypto currency units involved in such transactions would then be "infected" and the addresses where they are deposited would have to be listed and/or delisted to the effect that the units would lose their market value. The result would be a total loss of monetary value on the side of the legal user accidentally interacting with a prohibited address.

Neither the approach of the amending directive to the fourth AML directive, nor alternative listing models are fully effective approaches for an adequate AML regulation. The innovative characteristics of blockchain technology and the amending features of advancements with a stronger focus on privacy demand innovative approaches from regulators for an effective and adequate AML regulation.

Conclusion

As discussed above, the current approach of the European legislator to apply the rules of the AML directive to virtual currency exchange services and custodian wallet providers raises several severe doubts with respect to its effectiveness and adequacy because crypto currency transactions do not necessarily involve a payment provider or any other intermediary. However, a better approach to AML regulation for crypto currencies has not been found yet and must therefore be subject to further research and political discussions in the future. Nevertheless, the application of the traditional AML regulatory rules to virtual currency service providers should not necessarily be regarded as a first step in the right direction because the chosen direction - that is to say the application of the traditional rules - might be the wrong one and a step back will have to follow.

Lutz Auffenberg is German Attorney at Law and founder of FIN LAW, a Frankfurt-based law firm with a strong focus on the law of blockchain and DLTs, virtual currencies and security token offerings. You can contact him via e-mail (l.auffenberg@fin-law.de) or LinkedIn (www.linkedin.com/in/lutz-auffenberg-llm).

[1] *Satoshi Nakamoto,* Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.

[2] Examples for such tools are available at https://blockchain.info or https://blockexplorer.com.

[3] *Jessica Roy*, Everything You Need to Know About Silk Road, the Online Black Market Raided by the FBI (Time), http://nation.time.com/2013/10/04/a-simple-guide-to-silk-road-the-online-black-market-raided-by-the-fbi/.

[4] *Joshua Althauser*, Dark Web Market AlphaBay Shut Down by US Authorities (Cointelegraph), https://cointelegraph.com/news/dark-web-market-alphabay-shut-down-by-us-authorities.

[5] ECB, Virtual Currency Schemes, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[6] ECB, Virtual Currency Schemes – a Further Analysis, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[7] EBA, Warning to Consumers on Virtual Currencies, https://www.eba.europa.eu/documents/10180/598344/EBA+Warning+on+Virtual+Currencies.pdf.

[8] EBA, Opinion on ‚Virtual Currencies', EBA/Op/2014/08, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf.

[9] FATF, Virtual Currencies – Key Definitions and Potential AML/CTF Risks, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

[10] FATF, Guidance for a Risk-Based Approach to Virtual Currencies, http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html.

[11] BKA, Cybercrime Bundeslagebild 2016, p. 10, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.html?nn=28110.

[12] *Satoshi Nakamoto*, Bitcoin: A Peer-to-Peer Electronic Cash System, p. 6.

[13] *Elli Androulaki et al.,* Evaluating User Privacy in Bitcoin, in: Shadegi (Hrsg.), Financial Cryptograhy and Data Security. 17th International Conference, FC 2013, Revised selected Papers, 2013, p. 34 – 51; as to assessment techniques also *Dorit Ron and Adi Shamir*, Quantitative Analysis of the Full Bitcoin Transaction Graph, in: Sadeghi (Hrsg.) Financial Cryptography and Data Security, 17th International Conference, FC 2013, Revised Selected Papers, 2013, p. 6 – 24.

[14] Bitcoin-mixing services are available e.g. at https://coinmixer.se or https://cryptomixer.io.

[15] *Nicolas van Saberhagen,* CryptoNote v. 2.0, https://cryptonote.org/whitepaper.pdf.

[16] An example is the critique that Zcash is run by the for-profit company “Zerocoin Electric Coin Company” which by design of Zcash earns ten percent of all mining-rewards.

[17] *Eli Ben Sasson et al.*, Zerocash: Decentralized Anonymous Payments from Bitcoin, http://zerocash-project.org/media/pdf/zerocash-extended-20140518.pdf.

[18] Examples of banking activities are deposit business and credit business, financial services are activities like investment brokerage, investment advisory or proprietary trading.

[19] *Münzer, Jens,* Bitcoins: Supervisory assessment and risks to users, https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Fachartikel/2014/fa_bj_1401_bitcoins_en.html.

[20] BaFin Yearly Report 2017, Kryptotoken, https://www.bafin.de/DE/PublikationenDaten/Jahresbericht/Jahresbericht2017/Kapitel2/Kapitel2_7/Kapitel2_7_3/kapitel2_7_3_artikel.html.

[21] BaFin, Advisory letter on the classification of tokens as financial instruments, https://www.bafin.de/SharedDocs/Downloads/EN/Merkblatt/WA/dl_hinweisschreiben_einordnung_ICOs_en.html.

[22] Proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC, 2016/0208 (COD).

[23] EU Commission Action Plan to strengthen the fight against terrorist financing, press release,
http://europa.eu/rapid/press-release_IP-16-202_en.htm.

[24] ECB, Virtual Currency Schemes, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[25] ECB, Virtual Currency Schemes – a Further Analysis, https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf.

[26] coalition contract between CDU/CSU and SPD dated 12 March 2018, pp. 41, 44, 70, https://www.cdu.de/system/tdf/media/dokumente/koalitionsvertrag_2018.pdf?file=1.

[27] *Elli Androulaki et al.,* Evaluating User Privacy in Bitcoin, in: Shadegi (Hrsg.), Financial Cryptograhy and Data Security. 17th International Conference, FC 2013, Revised selected Papers, 2013, p. 34 – 51; as to assessment techniques also *Dorit Ron and Adi Shamir*, Quantitative Analysis of the Full Bitcoin Transaction Graph, in: Sadeghi (Hrsg.) Financial Cryptography and Data Security, 17th International Conference, FC 2013, Revised Selected Papers, 2013, p. 6 – 24.; *Malte Möser et al.*, (2018), An Empirical Analysis of Traceability in the Monero Blockchain, Proceedings on Privacy Enhancing Technologies, 2018(3), 143-163, https://doi.org/10.1515/popets-2018-0025.

[28] The author of the Bitcoin-whitepaper writing as “Satoshi Nakamoto” has still not been identified. The author of the CyberNote-whitepaper who published under the pseudonym “Nicolas van Saberhagen” has also still not been identified.

[29] *Rainer Böhme et al.*, Bitcoin and Alt-Coin Crime Prevention, Project BITCRIME, https://www.bitcrime.de/presse-publikationen/pdf/BITCRIME-RegulRep.pdf.