Banking and Financial Market Law

Research paper 2021

Is the growth of crypto assets obscuring the AML directives?

Benozzi Filippo – Universitá Ca'Foscari – Venice

Summary

Introduction *3*

Blockchain, the technology behind the crypto assets *5*

Risks and opportunity of crypto assets *11*

The effort of the legislators with the AML directives *15*

Is AML threatening the crypto assets or the opposite? *18*

Bibliography and Sitography *21*

Introduction

From early 2000, the increasing spread of technology and internet has affected our behavior our habits in several ways from human relationships to the way we do business, payments, etc.
The economic and financial fields had a big technological revolution, in the last two decades, just think about the process of making a banking transfer in early 2000 compare to now.
The era of digitalization has affected in positive ways the banking system. This new medium between us and the banking services implies new directives and regulations that help make the banking system secure and transparent for both players.
The advent of crypto assets and cryptocurrency with the born of the fin-tech industries provoke a big revolution and potentially a disruptive revolution in finance.
This revolution brought new improvement in the financial system while at the same time opened the possibility of new ways of criminal activities such as money laundering or scam, undermining the transparency of the financial system.
These new virtual assets aim to remove the financial intermediaries such as bank and financial institution with the use of a decentralize technology called blockchain. This system has a lot of potential benefit for the final user such as a reduction of commission fees, the speed of the transaction, less bureaucracy in one side and a potential decrease of transparency on another.
In 2015 the 5th Anti-Money Laundering Directive was drafted in order to regulate the huge impact of the crypto assets in illegal operations with the aim of fighting money laundering and terrorist financing. In particular the directive tries to uncover what make the cryptocurrency so "special" for the malicious users: the anonymity of users and transactions.
Money laundering is one of the biggest issues that blockchain exchanges tend to face with the crypto assets. In fact, someone may think that crypto is considered to be a breeding ground for hackers, frauds and so called "black market".
Though cryptocurrency itself is secure and immutable. The danger grows from the cryptocurrency services, their vulnerability to hacks. Regardless of the kind of cryptocurrency, you cannot be guaranteed that your assets are safe (unless you have an insurance). Only in

Ethereum digital criminals stole $255 million in 2018, $1 billion is a total volume of money stolen from different exchanges in 2018. About $480 billion were stolen from different exchanges in the first part of 2019.

This paper aim to analyze the risk associated to crypto assets transaction and indeed analyze the current directives of the EU and find ways to improve it.

Regulate the transparency and security of a new market develop in a decentralize way need directives that are disruptive and different from a system that is develop in a centralized way.

Firstly, the paper will analyze the technology behind the crypto assets the blockchain, in order to understand the possible points where the system need to be regulated.

Then we will analyze pros and cons of the Fifth Anti-Money Laundering Directive and the potential lack of legislation.

Finally, I will examine some potential solution that could implement the European Central Bank in order to monitor the transaction activity of the crypto assets.

Blockchain, the technology behind the crypto assets

Crypto assets are a broad term used to cover all the assets stored on distributed ledgers, using a technology called blockchain.

In 2009, Satoshi Nakamoto (the pseudonymous person or persons who developed Bitcoin and the first blockchain) introduced the world to Bitcoin. Satoshi described the use of blocks connected in a chain that was chronological and permanent. This technology behind is called blockchain. Blockchain aim to solve the double-spend[1] problem and allowed people do transaction and exchange money in a secure and irreversible system.

Blockchain is build on a distributed ledger technology (DLT) — It is an accounting system where the ledger (record of transactions) is distributed among a network of computers called nodes.

Since then, blockchain technology has evolved, not only It can be applicable to financial transactions, but also in other types of peer-to-peer transactions involving other types of objects and not only money. Anything that involves exchanging information, data or products can be verified and recorded on a blockchain.

Crypto assets are built upon different types of DLT and also all the transactions involving crypto assets are contained within a specific digital ledger. Typically, every person with access to the digital ledger can view the transactions recorded on it. Bitcoin's ledger[2], for instance, can be accessed through the protocol or a website which is open to the general public.

In order to make it more clear let's compare the virtual currency (as Bitcoin) with the "classical" electronic payment system. Imagine be in a clothes shop and you want to buy a jumper: the shop worker will provide through a POS the card details to the bank. The bank in an electronic and

[1] Double-spending is one of the most relevant concerns in using digital currencies: is the risk that a digital currency can be spent twice.

[2] Bitcoin ledger transaction database: *https://www.blockchain.com/btc/unconfirmed-transactions*

fast way will check and verify if the owner of the card has enough money to pay the item and provide a green light to the payment. While virtual currency such as Bitcoin will avoid the bank fees without checking in a centralized system, instead the network provides the validity of that fund by checking in the blockchain and authorize the transaction, if the validation pass. This is decentralized, fast technology of payment without any additional fees for both parties.

The tokens are the digital representation of the crypto assets. There are three main subcategories:

- Payment or exchange token: these are also known as cryptocurrency; an example of a payment tokens are: Bitcoin, Ethereum, Dogecoin etc.
- Security token: design for investment opportunity with the characteristics associated with traditional financial instruments. These tokens are either equity or debt token that claim to provide ownership rights. They are used as a sort of capital rising for start-up or projects. Unlike the payment token these cannot be use for further trade or means of payments.
- Utility / Access token: these tend to be tokens which entitle the contributor to use a function, product or service provided by a particular organization or business.

In the crypto assets chain, it is possible to identify various and different actors and intermediaries: miners, the issuer of the cryptocurrency that provide that exchange fiat money into virtual currencies, the wallet provider and tumbler services.

The miners are usually companies that runs cryptographic computation that allow new crypto assets to be posted on the specific DLT; an example could be made with Bitcoin, miners are rewarded with newly minted Bitcoins. One of the biggest miner company is for example Argo[3]. The cryptocurrency exchange platform are entities that exchange crypto assets, tokens and fiat currencies, such as Coinbase[4]. The wallet provider are entities that provide an online crypto-asset account service similar to a debit card offer by some financial institutions. Customers are

[3] Argo blockchain: *https://argoblockchain.com*

[4] Coinbase: *https://www.coinbase.com*

able to use their digital wallets to hold and store crypto assets and to transfer the crypto assets from one wallet to another. In some cases, custodian wallet providers have access to mainstream payment infrastructures through partnership with card issuer such as VISA or MasterCard[5].

The tumbler services are services that mix potentially identifiable cryptocurrency fund, in order to obscure the trail back to the originals funds sources. These kinds of services arisen in order to improve the anonymity of cryptocurrencies, since the blockchain of the specific currency provide a public ledger of all the transactions. When crypto assets have been processed through a mixer, the digital ledger shows that a transaction was sent by one of many possible payers to one of many possible payees. Mixers make possible for entities with 'tainted' crypto assets (for instance, the crypto asset proceeds of the sale of illegal goods online) to launder proceeds of crime by obscuring the original source of funds. This is one of the reasons why crypto assets are causing great curiosity across criminals and terrorist because they represent the best and easy way to launder money and finance terrorism thanks to their great anonymity.

The crypto assets system is so wide and so fast in technology improvement, with new players and new kind of tokens that arise every day that put the european legislator in alarm in order to fix these problems.

The first directive to combat money laundering was enacted in 1991, the European Union is still updating with subsequence measure to fight against this phenomenon. In the 2018 the trouble and the mediatic "boom" of crypto assets and the necessity to regulate the phenomenon of scam and money laundering was seriously taken into account by Directive 2018/843 also known as AML5. The main purpose with this directive is the prevention of illegal activity related to crypto assets such as money laundering and financing of terrorism. In addition, this directive defines a first definition of cryptocurrency improving the transparency.

[5] Crypto (https://crypto.com) is a company that made a partnership with VISA and allow the customer to use and spend cryptocurrency through a "classical" debit card.

The wide world behind crypto assets makes difficult to define what they are. The European Union as said in the 5th Anti-Money Laundering Directive (5AMLD) tried to define a suited definition. The 5AMLD tried to cover all the potential uses and measure of the virtual currencies underling what they are not (art.10): "*Virtual currencies should not to be confused with electronic money…nor with in-games currencies, that can be used exclusively within a specific game environment…*".

While the 18 Amendment to Directive 2015/849 declares virtual currencies 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 it is accepted by natural or legal persons as a medium of exchange and which can be transferred, stored and traded electronically*".

These definitions they are underling some aspect of the cryptocurrency, but they are far from well defying all the types of crypto asset.

Crypto assets look as one of the quickest and most transparent mediums of exchange, but they also have drawbacks. In fact, all the transaction are recorded permanently, which means that they are irreversible, no matter the reason. This implies that operational risk represents a very concrete part of the usage of virtual currencies, with for example erroneous transaction that cannot be reversed. In addition, even with a decentralized system that help securing transaction, attacks again cryptocurrency are still present.

The European Commission is still struggling regulating virtual currencies. Cryptocurrencies ledger are completely open for the public to view, what they lack is the openly available identity data where all the transactions are conducted between unique wallet addresses. Therefore, once two owner's wallet account identity are revealed, according to virtual currencies transparency feature, it is possible to potentially reveal all transaction history between those two owners. However, the possibility to trace back the identity of the wallet are not negligible.

This is a strength point behind the increasing importance of virtual currencies among criminals, who have in this way the possibility to clean money or hide illicit origin of their funds, this as logic consequence will favor money laundering and terrorist financing.

It's highly likely that new types of cryptocurrencies will emerge in the years to come. Right now, is how this decade is shaping up to be the era where mainstream adoption of crypto assets is achieved. PayPal[6] is gearing up to allow cryptocurrencies to be used for purchases with millions of merchants, and China is trying to make its digital yuan[7] available to its population.

Overall, there are little doubt that the coronavirus pandemic has transformed our relationship with money forever[8]. Cash was already beginning to lose popularity, but banknotes are now being used even less considering there were concerns they could cause infections to spread, especially in this pandemic period.

There will be challenges that lie ahead. The whole notion of decentralized finance, meaning that there isn't a single person in charge and may not sit well with all the directive that EU is introducing.

It also remains to be seen whether central bank digital currencies can peacefully co-exist alongside cryptocurrencies such as Bitcoin.

[6] Paypal one of the biggest payment service provider is enabling user to buy, hold and sell cryptocurrency and use as a mean of payment *https://newsroom.paypal-corp.com/2020-10-21-PayPal-Launches-New-Service-Enabling-Users-to-Buy-Hold-and-Sell-Cryptocurrency*

[7] China create Its own digital currency *https://www.wsj.com/articles/china-creates-its-own-digital-currency-a-first-for-major-economy-11617634118*

[8] The Coronavirus Crisis has changed money forever https://www.forbes.com/sites/billybambrough/2020/04/06/the-coronavirus-covid-19-crisis-has-changed-money-forever/

Given there are concerns that private digital asset like Libra[9] could undermine the financial sovereignty of traditional fiat currencies, there may be greater levels of regulatory pushback in the 2020s.

Crypto asset exchanges are coming under increasing pressure to ensure that they perform *Know Your Customer*[10] checks before allowing people to make transactions – preventing digital currencies from being used for money laundering and the financing of terrorism.

[9] Japan central banker warns Facebook libra may undermine monetary policy *https://www.reuters.com/article/us-japan-facebook-libra-idUSKCN1US0SK*

[10] This refers to all the AML directives that the EU published.

Risks and opportunity of crypto assets

The new crypto assets scenario has some potential benefits, like for example the speed of the transaction and the lower cost of them since there are no intermediaries. Nevertheless, this technology is the same and available worldwide making it an effective and reliable payment system in countries underdeveloped or where systems like the European payment system are not develop or not reliable in monetary policy. These are some of the potential benefits but despite these a number of risks and implications in financial system are associated to the crypto assets.

A decentralize system could be perfect if all the player act legitimately, but unfortunately as the statics said a lot of illicit activities arise after the introduction of the crypto assets.

According to United Nation estimates[11], between $800 billion and $2 trillion are being laundered every year across the globe, representing the 2-5% of the global gross domestic product. Out of this, more than 90% goes undetected. The exact volume of crypto laundering is yet to be ascertained. The report says that crypto thefts, hacks, and frauds totaled $1.36 billion in the first five months of 2020, compared to 2019's US$4.5 billion. According to another report[12] from MIT, criminals laundered US$2.8 billion through crypto exchanges in 2019, compared to US$1 billion in 2018. As of 2019, total Bitcoin spending on the dark web[13] was US$829 million, representing 0.5% of all Bitcoin transactions in the same period. A separate study[14], analyzing more than 800 market maker exchanges, found that 56% of all crypto exchanges worldwide have weak KYC[15] identification protocols, with exchanges in Europe, the US and the UK among the

[11] Money laundering statistic from UN *https://www.unodc.org/unodc/en/money-laundering/overview.html*

[12] Report from MIT about Criminal Launder in 2019 *http://technologyreview.com/2020/01/16/130843/cryptocurrency-money-laundering-exchanges/*

[13] Bitcoin money laundering: how criminals use crypto *https://www.elliptic.co/blog/bitcoin-money-laundering*

[14] More than half of all crypto exchanges have weak or no ID verification *https://cointelegraph.com/news/more-than-half-of-all-crypto-exchanges-have-weak-or-no-id-verification*

[15] The know your customer or know your client (KYC) guidelines.

worst offenders. The study noted that 60% of European Virtual Asset Service Providers have deficient KYC practices.

In October 2020, the Europol announced[16] that an unprecedented international law enforcement operation involving 16 countries had resulted in the arrest of 20 individuals who attempted to launder tens of millions of euros since 2016 on behalf of the world's foremost cybercriminals. Operated by the notorious QQAAZZ network, the scheme involved the conversion of stolen funds into cryptocurrency using tumbling services that help hide the source of funds. In yet another incident[17], a man from New Zealand was arrested on money laundering, worth thousands of dollars, involving cryptocurrency.

Crypto assets risks are rooted in three main pillars: by nature, the lack of underlying claim, their unregulated nature and the absence of a formal legislator or government structure. The deficiency and the lack of a central authority has made the crypto assets extremely suitable for illegal actions. The lack of a central control has benefits but also many drawbacks, this made the crypto assets subject to high volatility. This behavior of the asset could create also quite often price bubble. One of this case happened in February 2021 with Tesla[18-19] that bought $1.5 billion in Bitcoin and by the end of March it was worth $2.5 billion with the price of exchange[20] of Bitcoin with US dollar around $20000 in January and reach around $53000 in mid-April 2021.

[16] 20 arrests in QQAAZZ multi-million money laundering case
https://www.europol.europa.eu/newsroom/news/20-arrests-in-qqaazz-multi-million-money-laundering-case

[17] Auckland raids: Man facing money laundering charges granted name suppression
https://www.nzherald.co.nz/nz/auckland-raids-man-facing-money-laundering-charges-granted-name-suppression/2GAPJQQ6SOJX4BHLIRKJ77KQIY/

[18] Tesla, Bitcoin, GameStop Bubbles All Have Roots In Tokyo
https://www.forbes.com/sites/williampesek/2021/03/24/tesla-bitcoin-gamestop-bubbles-all-have-roots-in-tokyo/

[19] Tesla bought $1.5 billion in bitcoin early this year. By the end of March, it was worth $2.5 billion
https://edition.cnn.com/2021/04/28/investing/tesla-bitcoin/index.html

[20] The prices of the Bitcoin exchange are taken from *https://www.investing.com/crypto/bitcoin/btc-usd*

Or again, the depreciation[21] that happen between December 2017 and February/March 2018 where the exchange rate fell from $19435 to $6858.

Due to this unregulated crypto asset nature, the final customers have not protection in terms of security of the assets and legality. This nature and fluctuation make crypto assets very attractable for final users as a speculative financial investment but at the same time create an easy field for criminals to create scam or to steal money from customers that does not know very well how the system works, without any legal protection. An example of big international scam about cryptocurrency is the one from a company called OneCoin[22].

Thanks to the ledger technology, crypto assets provide almost anonymous and decentralized financial flows. In the first case the user addresses cannot be directly associated to the individual identity and mixing mechanisms can hide the true source of the fund making difficult to individuate the real owner of the wallet and the origin of the fund in it. In the second case the lack of centralized institution like for example the EBC or simply the banks institution makes more complicated to report suspected transaction form money-laundering or terrorism financing or even to impose AML directives.

Criminals use a number of methods involving cryptocurrencies to hide the illicit origin of funds. All these methods make use of some or the other vulnerabilities of cryptocurrencies such as their inherent pseudonymity, easy cross-border transactions and decentralized payments. As in the case of cash-based money laundering, there are three main stages in money laundering using cryptos: placement, layering and integration.

In the placement step, illicit funds are brought into the financial system through intermediaries such as financial institutions, exchanges, shops and casinos, where one type of cryptocurrency

[21] Down More than 70% in 2018, Bitcoin Closes Its Worst Year on Record *https://www.coindesk.com/down-more-than-70-in-2018-bitcoin-closes-its-worst-year-on-record*

[22] Cryptoqueen: How this woman scammed the world, then vanished *https://www.bbc.com/news/stories-50435014*

can be bought with cash or other cryptocurrencies. It can be done through online cryptocurrency exchanges. Criminals often use exchanges with less levels of compliance with AML directives for the purpose.

After that in the layering phase criminals obscure the illegal source of funds through structure transactions. This makes the trail of illegal funds difficult to decode. Using crypto exchanges, criminals can convert one cryptocurrency into another or can take part in an Initial Coin Offering where payment for one type of digital currency is done with another type. Criminals can also move their crypto holdings to another country.

In the last stage, illegal money is put back to the economy with a clean status. One of the most common techniques of criminals is the use of over the counter (OTC) brokers who act as intermediaries between buyers and sellers of cryptocurrencies. Many OTC brokers specialize in providing money laundering services and they get very high commission rates for the same.

The complicated chain of intermediaries and providers make it complicated to extract information about the origin of the tokens, so perhaps criminals who get illicit money by means of cryptocurrencies could clean up dirty money of financing terrorism anonymously.

The choice of the country with a low measure of 5th Anti-Money Laundering directives are key for criminals. There are countries like Italy where the 5th Anti-Money Laundering directives are a legal instrument in national law and others like Argentina or South Africa that not specifically regulate crypto assets, these are perfect for criminals.

Owning various wallets cross country give to the criminals the possibility to do all money laundering procedures in every country, increasing the level of protection and security.

The effort of the legislators with the AML directives

In order to counter the increasing money laundering and finance terrorism threads related to crypto assets, regulators across the globe and in particular the European legislators have come up with rules and recommendations for firms and governments dealing with crypto assets.

In 2019 the global AML watchdog the Financial Action Task Force published its guidance the "*Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*[23]" for virtual assets and virtual assets service providers. In particular the guidance says that: "*The FATF strengthened its standards to clarify the application of anti-money laundering and counter-terrorist financing requirements on virtual assets and virtual asset service providers. Countries are now required to assess and mitigate their risks associated with virtual asset financial activities and providers; license or register providers and subject them to supervision or monitoring by competent national authorities*".

The European Union (EU) has recently adopted the 5th Anti-Money Laundering Directive (AML5), with the focus of expand the 4th Anti-Money Laundering Directive in order to integrate crypto assets into the new directives. The main focus of this directive is obligation of crypto exchanges and custodial service providers to register with their local regulator and be compliant with thoroughgoing know-your-customer (KYC) and anti-money laundering AML procedures.

The 5th Anti-Money Laundering Directive also, as said in the previous chapter introduce the first definition of the term virtual currency. The importance of this definition is the separation between the electronic money and the virtual currency; where the first is a digital representation of the fiat money and behind the request of the electronic money holder, it should be guarantee

[23] Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers *https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html*

that electronic money issuers pay off the monetary value. Although some cryptocurrencies can be convertible into fiat money, but they are not ensured by any public authorities or central bank. For this reason, cryptocurrency also define as virtual currency cannot be incorporated into the definition of electronic money.

Crypto assets represent one of the main trend topics at the moment. The blockchain technology is expanding with time by including a lot of new applications. One example of this is the increasing interest into NFT[24], non-fungible token that in the first months of 2021 generated a lot of media interest. These kinds of crypto assets give property rights in form of ownership, with a ledger database that certificate the property of the digital asset. This process transforms the perception of tokens not limiting its function to mere mean of payment.

This fast evolution of crypto assets and application link to the blockchain technology could make outdated the 5th Anti-Money Laundering directive due to the fact that the definition of the virtual currency by defining as "*mean of exchange*" this no longer include all type of crypto assets, since NFT are not further tradable. The AML5 tries to face this problem with the recital 10: "*Although virtual currencies can frequently be used as a means of payment, they could also be used for other purposes and find broader applications such as means of exchange, investment, store-of-value products or use in online casinos.*". The EU legislators tried to guarantee that all crypto assets fall within the scope of the 5th Anti-Money Laundering Directive.

An important introduction is AML architecture concerns the identification and the definition of the obliged entities. The fist entity is defined by the amendment of Directive 2015/849 Art. 2 that said: "*providers engaged in exchange services between virtual currencies and fiat currencies*" these are representing by the natural or legal person that practice the profession by providing the

[24] The Untold Story of the NFT Boom *https://www.nytimes.com/2021/05/12/magazine/nft-art-crypto.html*

exchange service between virtual currency and fiat money, an example could be Coinbase[25] or Revolut[26].

The second entity are the wallet providers the Art. 3(19) of AML5: "*custodian wallet provider*" means an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies. But this article is not complete since there is the lack of all the hardware providers and software solution that facilitate the transfer of crypto assets between users. All the entities that sell physical instrument as USB stick and provider of app that store offline the tokens on different devices are not covered by the 5th Anti-Money Laundering Directive, and this could potentially generate an opportunity for people who conduct criminal activities.

Another important insertion of the AML5 is: "*Member States shall ensure that providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, are registered…".* This article underlines that EU legislator must ensure more control over the field of cryptocurrency. The providers still have a lot of power and freedom to action since they only need to register the national authorities.

Which are the possible practical solutions that the ECB can activate in order to control and regulate the crypto assets?

[25] Coinbase a popular exchanging platform for crypto *https://www.coinbase.com*

[26] Revolut, a financial technology company that offers banking services introduce the possibility to exchange cryptocurrencies *https://www.revolut.com/en-IT/go-from-cash-to-crypto-instantly*

Is AML threatening the crypto assets or the opposite?

Open a bank account today and you will almost certainly be subject to identity and background checks, as well as ongoing monitoring of your activities. This is because with policies adopted by the financial institution, they are able to identify "dirty" money resulting from illicit or criminal activities. This as result, provide more security to the final user against scam or potential frauds.
To counter this the European Institution adopted over the years strong policies known as AML, these generate strong control every time a new bank account is created or when large deposits are made, so banks and other financial institution are unlikely to accept them if there is no legitimate explanation of where deposits come from.
Cryptocurrencies like for example Bitcoin have been consider as money laundering dream, by enabling fast transfer with pseudonymous, bypassing all the "traditional" financial institution that usually trust and apply strong AML controls. When this phenomenon started to grow the focus of the European financial institution became clear: how can we regulate a business handling Bitcoin made with a decentralized technology, with the AML directives made for a centralized system? How can we determine the real source of the funds?
The real source of the funds could be straightforward with blockchain technology since all the transactions are register in public ledger database, and so a business can demonstrate that the funds may come from an AML compliance source with a verifiable receipt. The solution is to trace the transaction between the addresses, and this could be applied to every kind of crypto assets not only cryptocurrency since the technology behind is the same. In the previous chapter we said that identities are not recorded, actually studies[27] has shown that by performing an analysis of the ledger database of the blockchain and mixing that with external data, some identities can be

[27] An Analysis of Anonymity in the Bitcoin System, Fergal Reid, Martin Harrigan *https://arxiv.org/abs/1107.4524*

determine. We, therefore, have the potential solution of tracking crypto assets transaction and finding the source, of course mixing services can help to obscure the source but at least we will know if the transaction was legitimate or not.

Consider then an automated AML service provided by the European Central Bank that verify the source and evaluate a transaction and the fund link to it with a "risk score" based on the history ascertained through block chain analysis. As result the transaction will be classified as "higher risk" if it comes from a mixing services, verified or known criminals or thefts. It would be classified with a "lower risk" if a clear link to trusted institutions or trusted services like Coinbase could be made, more in general if a clear link to the origin of the funds could be establish. Researcher at University of Munster in Germany[28] tried to describe a system like that.

But what are the consequence of risk scoring for the crypto assets? This issue of mark blacklist certain assets is really controversial: can for example cryptocurrency work as proper currencies if it is fungible, where some coins are worth more than others because of their provenance? Probably not, especially because an analysis like that on the blockchain will require time and the funds could be already to someone else. Imagine for example a criminal may be reported as guilty after days. By then the funds may be gone to innocent people, and when the blacklist took effect, the guiltless person will find that the assets that they have, have been devaluated. Who would use such a currency with that risk?

It seems inevitable that when there is a "history" associated to every asset, "dirty" units of assets will exist. One possible solution is doomed every crypto unit. Extension of cryptocurrency such as Zerocoin protocol[29] do exactly that: make impossible to link transaction to its origin by transforming crypto asset more like cash currency. It does that by implementing a mixing services

[28] Towards Risk Scoring of Bitcoin Transactions, Malte Moser, Rainer Bohme, and Dominic Breuker *http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_15.pdf*

[29] Zerocoin project *http://zerocoin.org*

at protocol level. But system like that could become heaven for money launders and be automatically rejected by a regulated AML business.

The AML directives currently active were strongly develop after the 9/11 by implementing directives aim to trace and fight illicit founds used for financing terrorism and after the financial crisis, when virtual currency and crypto assets born. This results in a very huge responsibility for banks and other financial institution that are still struggling to keep the pace with these new technology and directives.

The rise of the blockchain technology must provide an impetus to rethink the role and efficacy of AML directives design with a centralized mind, in order to create system that are able to operate in a decentralized context.

Bibliography and Sitography

- AML5 *https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843*
- Anti-money laundering and counter terrorist financing *https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terrorist-financing_en*
- Money laundering *https://medium.com/blockchain-highlights/money-laundering-b2c1bda2fc88*
- Virtual Currency (including cryptocurrency, virtual assets, and "value that substitutes for currency") *https://johnbandler.medium.com/virtual-currency-including-cryptocurrency-252d1173bf25*
- Blockchain Technology Explained *https://medium.com/swlh/a-simple-guide-to-blockchain-technology-4589971e6d03*
- Blockchain Needs Selfless People *https://medium.com/swlh/what-blockchain-needs-is-selflessness-5286501c9d4a*
- Legal context and implications for financial crime, money laundering and tax evasion *https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf*
- Cryptocurrency Crime and Anti-Money Laundering Report, February 2021 *https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/*
- Cryptoassets – Believing the money laundering impact *https://www.incegd.com/en/news-insights/cryptoassets-believing-money-laundering-impact*

- The risks of cryptoassets from a financial crime, money laundering and terrorist financing perspective *https://www.lexisnexis.co.uk/legal/guidance/the-risks-of-cryptoassets-from-a-financial-crime-money-laundering-terrorist-financing-perspective*
- Towards Risk Scoring of Bitcoin Transactions, Malte Moser, Rainer Bohme, and Dominic Breuker *http://fc14.ifca.ai/bitcoin/papers/bitcoin14_submission_15.pdf*