The open legal challenges of pursuing AML/CFT accountability within privacy-enhanced IoM ecosystems*

Nadia Pocher

PhD Candidate
Universitat Autònoma de Barcelona • K.U. Leuven • Università di Bologna
Law, Science and Technology: Rights of Internet of Everything Joint Doctorate
LaST-JD-RIoE MSCA ITN EJD n. 814177
nadia.pocher@uab.cat

Abstract

This research paper focuses on the interconnections between traditional and cutting-edge technological features of virtual currencies and the EU legal framework to prevent the misuse of the financial system for money laundering and terrorist financing purposes. It highlights a set of Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT) challenges brought about in the Internet of Money (IoM) landscape by the double-edged nature of Distributed Ledger Technologies (DLTs) as both transparency and privacy oriented. Special attention is paid to inferences from concepts such as pseudonymity and traceability; this contribution explores these notions by relating them to privacy enhancing mechanisms and blockchain intelligence strategies, while heeding both core elements of the present AML/CFT obliged entities' framework and possible new conceptualizations. Finally, it identifies key controversies and open questions as to the actual feasibility of effectively applying the "active cooperation" AML/CFT approach to the crypto ecosystems.

1 The Internet of Money and underlying technologies

The onset and subsequent development of the so-called "crypto economy" significantly and ubiquitously transformed the global financial landscape. The latter has been extensively confronted with non-traditional forms of currencies since the Bitcoin launch in January 2009. Relevant industry-altering effects, both ongoing and prospective, have been outlined more clearly by ideas such as Initial Coin Offerings (ICOs) or the recently unveiled Facebook-led Libra initiative. On a conceptual level, this disruptive[1] monetary ecosystem gave birth to the notion of Internet of Money (IoM) as a way to depict a new decentralized financial system. From a functional perspective, it is significantly influenced by inherent technical features of Distributed Ledger Technologies (DLTs) and, more specifically, of their blockchain-powered subset.

[*] This work has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie ITN EJD grant agreement No. 814177.

[1] Reference is to the definition of "disruptive technologies" as *"those that fundamentally alter the way we live, work, and relate to one another"* [27].

Blockchain technology (BT), in fact, is the most common DLT scheme behind cryptocurrencies [5][2] and its structural role within the topic at hand revolves around it being at the core of the Bitcoin ecosystem, which can be seen as a pathfinder in the crypto sphere. Indeed, it is widely recognized that BT's properties responded to socio-economic queries that were pursuing decentralized and disintermediated structures that could allow transactions to be performed with no need of a trusted central party [43].

The relevant algorithm-based "consensus protocol" was described as leading to crowd-sourced functions of validation and auditing, which led several European institutions to acknowledge its disintermediation-wise worth [62]. BT's unprecedented, albeit partly disputable, degrees of verifiability, transparency, inalterability, trust and security stirred up interest in the most diverse fields and appealed governments and stakeholders from all over the world [9, 19, 40]. Parallelly, however, projects such as IOTA most interestingly wish to take these features to the next level by employing blockchain-unrelated DLTs – e.g. a type of DLT called Directed Acyclic Graph, the Tangle – to the end of appropriately targeting the Internet of Things (IoT) industry by pursuing secure data monetization from connected devices [51].

The deep conceptual and architectural impact of these innovations was underlined by crafting a broader notion: the "Internet of Value(s) (IoV)". The IoV comprises cryptocurrencies and purportedly labels the infrastructure of the next generation of Internet, compared with the more traditional "Internet of Information" [59].[3] Whereas the latter enables people to directly send information to one another, the IoV removes any fences to the direct participation of everyone to the global (digital) economy by embedding an economic layer in the Web [16, 41].

2 Crypto monetary ecosystems and relevant misuse risks

On the one hand, this innovative way of processing payments catered for the need to find alternative solutions to traditional financial institutions. One of the main purported goals behind this monetary (r)evolution, in fact, was the opening of financial opportunities to the unbanked and non-traditional investors by mitigating their troubles in accessing the ordinary banking system because of its risk-averting principles and consequent de-risking approach.[4] Accordingly, crypto ecosystems were praised as conductive to financial inclusion and at a lower regulatory cost [59, 68].

From a risk perspective, however, it cannot come as a surprise that the very same lower - and possibly non-existent - degree of access control causes these instruments and their anonymity-wise features to be perceived as highly vulnerable to be exploited for most diverse and large-scale illicit purposes. Generic references may encompass transactions on the dark web, scams, ransomware, malware, hacking and identity theft, market manipulation and fraud, Ponzi schemes, online gambling, financing of criminal and terrorist activities, etc [19, 27, 35, 37, 68]. Some of these aspects were brought into the spotlight by the widely known and well-publicized Silk Road case; the subsequent increased crypto-risk awareness arguably played a role in the shutdown of Darknet markets such as Alphabay, Valhalla and Wall Street Market.

[2] From a technical and definitional standpoint, "virtual currency" and "cryptocurrency" are not synonyms. However, despite the paramount need for conceptual clarity in the crypto realm, for the sake of the narrative they are used interchangeably in this paper. In compliance with the EU regulatory approach, local and complementary currencies fall outside the scope of this work.

[3] The notion of IoV is argued to depict the Internet as a space to transfer and store any conceivable value; blockchain would make it possible by ensuring the security, decentralization, efficiency and transparency of such storage [59].

[4] De-risking refers to the reduction in the provision of banking (and related) services to people and places that are perceived as too risky by relevant institutions [16].

Over and beyond, Virtual Currencies (VCs) were found to generate significant money laundering and terrorist financing risks [21, 27]; the primary concern is the extent to which they can be easily resorted to in order to engage in these illicit practices. For this reason, a growing number of domain-specific regulation attempts was spurred, against the backdrop of a broader set of legislative and regulatory actions targeting DLTs from a technology-based perspective, on the grounds that they often put the logic behind existing legal regimes to the test [45, 49].

Essentially, the diversity of relevant legal initiatives ranges from crypto-specific legislation to interpretative instances of existing legal frameworks in light of new technologies; hence, the state-of-the-art highlights a bipartite scenario comprising both a pro-active and a reactive approach to regulatory scrutiny and intervention [40, 49]. The latter distinction may arguably play a significant role in paving a way forward for a more suitable and effective attitude to any discussion concerning the regulation of crypto stakeholders.

3 AML/CFT legislative and regulatory initiatives

The Financial Action Task Force (FATF)[5] is the most prominent international organization in the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) landscape and has been issuing specific guidelines for VCs and Virtual Assets (VAs)[6] since 2014; it is currently working towards strengthening the application of its Recommendations to DLTs.

More specifically, in October 2018 financial activities involving VAs were explicitly included in the scope of the FATF Recommendations and in June 2019 an Interpretive Note to Recommendation 15 (”New Technologies”) provided some further clarifications [28, 30]. On the same occasion, the experts drafted an update of relevant guidelines concerning the Risk-Based Approach (RBA)[7] to VCs, whereby emphasis was put on examples of risk indicators concerning transaction obfuscation and relevant inability to perform customer identification [28].

Within this framework of measures, crypto regulatory efforts target a set of entities labelled as “Virtual Asset Service Providers (VASPs)”. Interestingly, according to the FATF Glossary, a VASP is *“any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i) exchange between virtual assets and fiat currencies, ii) exchange between one or more forms of virtual assets, iii) transfer of virtual assets, iv) safekeeping, and/or administration of virtual assets or instruments enabling control over virtual assets; and v) participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset”*. Most notably, therefore, pursuant to ii), crypto-to-crypto exchanges are included in the scope of FATF provisions.

As far as the supranational level is concerned, the frequently mentioned European Union 5th AML Directive [21] addresses VCs and mandates Member States to regulate them. More

[5] The FATF is an intergovernmental organization and it is both a policy making and enforcement body. It addresses national competent authorities and sets international standards seeking to combat money laundering, terrorist financing and other threats to the international financial system. Notably, its Recommendations outline a comprehensive framework of measures whose implementation is called for in order to combat money laundering and terrorist financing.

[6] The FATF Glossary defines a ”virtual asset” as *”a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.”*

[7] The RBA is a pivotal concept in the AML/CFT realm; it requires relevant preventive and mitigatory measures to be commensurate with the risks identified. Consequently, all stakeholders involved (e.g. the EU commission, national authorities, supervisory authorities, obliged entities, etc) are demanded to carry out preliminary risk assessments.

specifically, it labels "fiat-to-crypto exchanges" and "custodian wallet service providers"[8] as reporting/obliged entities, by listing them amongst other more traditional regulated categories like financial institutions and professionals.

Indeed, even if Article 3(18) of the consolidated version of the AML Directive defines VCs 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"*, Article 2(3)(g) limits its scope to *"providers engaged in exchange services between virtual currencies and fiat currencies"*.

All in all, by enclosing these new set of "institutions" as "reporting entities" the Directive makes them subject to AML/CFT obligations. Given the nature of a directive as a EU legal instrument, relevant provisions may to some extent be tailored by Member States during relevant transposition processes. Nevertheless, relevant duties encompass, *inter alia*, appropriate registration and/or licensing procedures, Know Your Customer (KYC), Customer Due Diligence (CDD), up-to-date record-retention, internal procedures, ongoing monitoring - e.g. transaction scrutiny - and Suspicious Transaction Reporting (STR). Relevant mechanisms of monitoring, supervision and sanctions are also outlined by the abovementioned frameworks.

In a nutshell, obliged entities are preliminarily requested to conduct individualized risk assessments, which require to take into consideration a plethora of elements, such as targeted customers, offered products and services, geographical areas involved. Subsequently, in light and on the basis of the development of a comprehensive risk profile, they must implement and maintain consistent controls and monitoring efforts [68].

STR, on the other hand, is an instance of the well-known "active cooperation" duties, as a possible outcome of prior assessment and supervision tasks, which overall comprise both "active" and "passive" provisions. Also in the crypto context, CDD requires to identify - and take reasonable measures to verify the identity of - transaction parties and counterparties, such as customers (or any person purportedly acting on their behalf) and beneficial owners, as well as to assess purpose and intended nature of the business relationship [49].[9] More specifically, from a data analytics perspective, AML/CFT transaction monitoring controls include aggregation requirements and detection of structuring payments [35].

4 Possible pitfalls of conventional approaches

A conclusion may already be drawn; even within blockchain-powered disintermediated ecosystems, and despite inherent crypto-specific socio-financial goals, the general tendency is to keep focusing on gateways and gatekeepers to/from the traditional regulated financial system, the so-called "chokepoints" [28]. The explicit goal of the 5th AML Directive, for instance, is to allow competent authorities to monitor the use of VCs through relevant obliged entities [21], albeit it is concurrently acknowledged that their inclusion in the AML/CFT compliance sphere is not sufficient to enforce supervision on all crypto transactions [21]. In a nutshell, in fact, at least two sets of arguments may possibly challenge this approach.

First, a massive tension can be detected between the need for financial transactions to comply with originator/beneficiary information-related regulations and the nature of VCs as a privacy-oriented instrument. It is widely acknowledged that cryptocurrencies were imagined and created to keep intermediaries out of the picture; thus, the conceptual origin of the

[8] Article 3(19) of the Directive defines "custodian wallet provider" as *"an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies"*.

[9] Tracing the customer's IP address may be arguably demanded when Enhanced CDD is required [28].

crypto economy is seemingly and empirically at odds with identifying middlemen to be held accountable in the area of ensuring transparency of financial transactions. Interestingly, it has been straightforwardly argued that there is a structural incompatibility between the concept of transparency within non-centralized systems and financial regulatory transparency rules, since the latter oppose any opaqueness concerning the origins of funds, reasons for operations and relevant beneficial owners [51]. This friction appears as of topical importance because next generation DLTs are foreseen to take the ongoing revolution beyond peer-to-peer computer networks up to potentially including every Internet of Things (IoT)-connected device, while ever-evolving payment-related innovations keep defying legislative attempts [45].

Secondly, the same tech design of VCs arguably mismatches traditional approaches to AML/CFT regulation. Unsatisfactory legal results are caused by a diverse array of reasons, such as: (a) distributed governance mechanisms of VCs and relevant accountability levels vary significantly,[10] (b) crypto transactions involve both traditional intermediaries and other actors, (c) their lifecycle features a multi-layered stakeholdership,[11] (d) it is difficult to assess which innovative ecosystems properly belong to the financial services sphere, (e) their cross-border nature and structures lead to major jurisdictional issues.

One of the main controversies tainting the current approach is that it arguably does not consistently address the issue of crypto-to-crypto exchanges often being under a different regulatory framework than crypto-to-fiat ones [35].[12]

In light of these inconsistencies, institutions such as the European Banking Authority (EBA) put forward – albeit incidentally – innovative approaches to the mitigation of crypto risks, namely a private/public co-regulation regime grounded on “regulated self-regulation” [23, 42]. The latter is to be implemented through the so-called “regulation-through-code” mechanism, along the lines of the concept of “regulation by design”. Besides, an AML/CFT “self-declaration” role of the same crypto users and market participants was suggested, and is being assessed at the EU level [21].

In general terms, it is arguably incorrect to take for granted that disruptive technology equals disrupted law [34]. Nevertheless, a commonly agreed upon feature of BTs is to implement tasks that are traditionally performed by law and legal institutions [46], as well as to carry an alternative vision of the economic system [40]. These elements give rise to foresee principle-wise alterations grounded on the transposition of socio-economic interactions to a virtual, potentially horizontally-structured and hyper-connected world. Similarly, the inherent structure of these tech solutions seemingly leads to a deep power shift amongst stakeholders and possibly to a so-called “emergent technocracy” [40], thereby ostensibly challenging legislative frameworks and relevant accountability schemes.

5 Pseudonymity, traceability and blockchain intelligence

Many crypto-related legislative and regulatory actions were argued to insufficiently acknowledge context-specific technical aspects. Besides some comments on traditional approaches possibly being unreasonable in the crypto landscape [41], other critics challenged both the choice of which entities to include in the scope of AML/CFT obligations and the claimed level of anonymity and

[10] Namely, internal governance mechanisms range between the poles of fully public distributed ledgers and private ledgers [42].

[11] Players involved, in fact, range from users to miners to exchanges to trading platforms, wallet providers, coin investors and offerors [25].

[12] As recently underlined, however, under the FATF framework virtual-to-virtual and virtual-to-fiat transactions are supposedly both covered by the relevant Standards [28].

privacy of DLT-based financial applications. In spite of common misconceptions, in fact, major VCs such as Bitcoin and Ether are pseudonymous rather than anonymous and the same was suggested for Libra [3, 44, 66]. Even if no real-world identities are involved, there are ways to link public addresses to real identities [2, 22, 33, 43].[13] Concurrently, blockchain analysis techniques were enhanced over time and allow for a certain traceability of transaction flows; transacting in most popular VCs was found to leak information that can be used for de-anonymization purposes [2, 49].[14] Besides, the address used – i.e. the public key –, the transferred amount and other metadata are permanently and publicly stored on the ledger [66].

From a traceability and accountability standpoint, pseudonymity needs to be contextualized within the framework of results that are achievable by crypto/blockchain forensics. The issue at hand entails reference to the set of tools aimed at definitively or statistically matching actual users to transactions performed by crypto-IDs and possibly spotting unique identifiers to individuals [1, 49, 58]. Forensic experts, in fact, can extract data from a transaction, receive the history of a specific address and use this information to engage in "follow the money" activities, to the end of possibly detecting the use of VCs by analyzing the retrieved data [37]. The conceptual and explainability-related impacts of these intelligence strategies may only be grasped by delving into how specific techniques – such as transaction-graph analysis, user activities/address clustering, clustering heuristics, transaction fingerprinting by leveraging publicly available and off-network information, web-scraping and OSINT tools - have been developed and refined to this end.[15] Reference is not limited to Bitcoin forensics; data-exploitation strategies were deployed also on the Ethereum blockchain – notably to detect smart Ponzi schemes [14, 17] – and discussions are ongoing for non BT-based DLTs [57].

Moreover and most interestingly, studies were presented to assess the feasibility of using publicly available information and machine learning techniques to map Bitcoin transactions, model the difference between licit and illicit ones from an AML screening standpoint, and possibly predict which transactions are legal and illegal [60, 68].[16] From a legal standpoint, it is thought-provoking to notice how such analyses, e.g. their data collection and evaluation phases, were challenged from a privacy violation perspective, while at the same time they were defended by leveraging on the fact that they would actually make AML compliance easier and cheaper by exploiting BT's abovementioned features [60].

These arguments show a compelling paradox generated by the way (non-privacy-enhanced) DLTs relate to the financial sphere. On the one hand, their pseudonymous nature provides the opportunity of engaging in illicit activities while hiding in plain sight. On the other hand, however, their very same data tech schemes and subsequent public availability allow for law enforcement experts to successfully deploy more effective, and also possibly crowdsourced, forensic analysis techniques [68]. This ambiguity is arguably enrooted in the basic features of BTs, giving rise to even more conflicting and counter-intuitive scenarios. From an AML compliance perspective, in fact, the use of such distributed systems is parallelly deemed to provide degrees of traceability and credibility for a reliable registration of AML information [67].

[13] As for Libra, the protocol does not link accounts to real-word identities; the Calibra wallet, however, seemingly requires AML/KYC [3, 44].

[14] This was also demonstrated by the arrests concerning the Wall Street Market [1, 58]

[15] On transaction-graph analysis:[33, 48]; On user activities clustering:[47]; On clustering heuristics [4, 43, 53]; On transaction fingerprinting using p.a. information:[33]; On using off-network information:[43, 53]; On web-scraping and OSINT tools:[1]. For a more comprehensive outlook:[37].

[16] The licit or illicit nature of each transaction was assessed through heuristic processes if no other data points were available [68].

6 VC-related privacy, anonymity enhancements and obfuscation of financial flows

On a broader level, the issue of VC-related “privacy” is far from straightforward, just as its relationship with adjacent concepts such as secrecy, traceability and pseudonymity. Studies have tackled privacy impacts of Bitcoin implementations, where an important difference was underlined between activity unlinkability and profile indistinguishability [4]. In order to draw a comprehensive picture of the crypto monetary landscape from the standpoint at hand, different cryptocurrencies should be scrutinized in light of how their technical aspects evolved beyond shared - albeit differently textured - traits such as distributed consensus, transaction transparency and party entity abstraction. Because the relevant focus has generally been on blockchain-based VCs, the issue is usually confronted by breaking the issue down to pieces of blockchain-embedded information as to determine whether they are private or public.

More specifically, three aspects were deemed relevant in this regard: (a) *privacy of identity or user-identity privacy*: it relates to the concept of anonymity and it entails assessing the link to a real-world identity, drawing a parallel between “public and private keys” of Bitcoin-like virtual currencies and the concepts of “username and password” [4]; (b) *privacy of transaction data/information*: it is a mutable concept and relates to the fact that data is represented differently in different blockchains, different aspects may be private from a third-party observer, different types of information can be private to different extents [4]; (c) *privacy of the total blockchain state*: different attributes of the total blockchain state can be private to different extents [4].

Moreover, two sets of elements - a) sharpened intelligence methods, and b) concerns expressed by crypto-privacy advocates - spawned the development of the so-called “privacy coins”. The most popular examples may be Monero and Zcash; the underlying goal is to provide true anonymity by embedding privacy-enhancing mechanisms. The need for heightened anonymity was interestingly contextualized within the conceptual pursuit of true fungibility amongst VCs, a feature that could otherwise be tarnished by the immutability of relevant records [16]. Hence, unlike what happens on the Bitcoin blockchain, these secrecy-reinforced instruments do not keep unencrypted records of data such as wallet addresses and transactions amounts.

From a categorization perspective, three main methods have been identified to obfuscate financial flows: (a) *mixing/tumbling-based approaches*; (b) *zero-knowledge based privacy*; (c) *user best practices* [63, 64, 65]. As far as embedded enhancements are concerned, Zcash reaches a high degree of privacy by making use of “zero-knowledge proofs” – namely, the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, or zk-SNARK –, whereas Monero is slightly less anonymous but implements more intensively tested techniques of ring signatures.

Interestingly enough, the “Zero Knowledge Proof” method, and the relevant possibility to preserve confidentiality on selected data (so-called “shielded” operations), was argued to pursue the union between two underlying objectives of many blockchains: to provide both user anonymity and transparency of operations [51]. As much as such a junction may seem counterintuitive and definitely dangerous from an AML and illegal transactions perspective - not to mention radically challenging relevant legal and regulatory frameworks in the financial transparency sphere, as previously mentioned -, its existence must be acknowledged and addressed.

Parallelly, Zcash offers selective transparency of transactions and it was originally defined as follows: *“Bitcoin is like HTTP for money, Zcash is HTTPS”*. Besides, another cryptocurrency, DASH, might also be arguably labelled as a “privacy coin”. As for non-blockchain-based currencies, the possibility of enhancing IOTA’s privacy protocols notwithstanding its quantum resilient hash-based signatures is being closely investigated [54, 57].

These arguments show how there is in fact no binary - public vs. anonymous - solution, which highlights the need to apply a flexible and structured legal reasoning while confronting the "anonymity set" of different blockchains. For instance, it can be argued that Monero's anonymity set is significantly larger than Bitcoin's [4]. In any case, a parallel assessment can be carried out as far as non-blockchain-based cryptocurrencies are concerned, where the analysis potentially holds significant differences.[17]

On top of the possibility to enhance the degree of anonymity at an infrastructural level, relevant users were also found to resort to so-called ”best practices”. The latter entail the use of anonymizers, such as The Onion Router (TOR), proxies and VPNs, the Invisible Internet Protocol (I2P) or Dark Wallet to hide the origin of the transaction or employing a new address for every payment [37, 63]. Concurrently, in the wake of Silk Road's takedown, darknet markets themselves started deploying more sophisticated techniques to make it more difficult for authorities to effectively intervene [45].

7 Virtual currencies and money laundering: a multi-layered relationship

A first way to look at the relationship between VCs and money laundering is most empirical. ML is traditionally defined as involving three different stages: a) *placement*: dirty money needs to be placed into the financial system, if not already in it; b) *layering*: its illegal origin needs to be concealed through as many complex transactions as possible; c) *integration*: funds need to be integrated in the financial system as cleaned. It is possible to analyze how crypto monetary instruments may be efficiently employed in all of these steps.

Namely, a crypto-based *placement* phase may be eased by the low-risk opportunity to rapidly open and access VC accounts, thereby pseudo-anonymously engaging in the relevant conversion and consolidation of illicit proceeds. Furthermore, the cross-border nature of these instruments facilitates *layering* across multiple exchanges, especially in the context of trade-based ML. As far as the *integration* stage is concerned, relevant risks are argued to expand in relation to the growing variety of goods that can be purchased with VCs; this phase is also aided by resorting to hardware wallets. The interconnection with unregulated and crypto-to-crypto traded ICOs further increases the overall risk; naturally, in fact, all these financial hazards are seemingly more serious in the context of unregulated areas of the crypto ecosystems [35].

From a strict AML/CFT legal perspective, however, a further step is very significant; most notably, crypto mixing/tumbling services are a key element in this sphere, to the extent that the advent of Bitcoin mixing shaped the notion of ”cryptocurrency laundering” or ”crypto-cleansing” from a conceptual standpoint [1].[18] This privacy-enhancing technique leverages on the fungibility of VCs and consists of combining inputs and outputs of different transactions into a larger one, in order to sever the links between addresses of senders and recipients [63]. Hence, they make use of temporary false crypto wallet addresses to re-route transactions and obfuscate the traceability chain [36].

These services cannot only be found in the online world as embedded features of "privacy coins"; rather, other platforms offer them as-a-service, to the end of enabling users of less-anonymous VCs to obscure identifiability of tainted coins [63]. In recent times, a more advanced type of exchanges provide their services without requiring any login or verification [36].

[17] With reference to IOTA: [57]

[18] Common mixing services providers: Bitmixer.io, SharedCoin, Blockchain.info, Bitcoin Laundery, Bitlaunder, Easycoin [32].

Furthermore, Fig.1 shows how it is concurrently possible to convert Bitcoins into less trackable altcoins via an AML/CFT *unregulated* crypto-to-crypto mixer after obtaining them via a *regulated* fiat-to-crypto exchange. Subsequently, anonymity-enhanced cryptocurrencies (AECs) may be used to buy illicit goods on the Dark Web, possibly through the deployment of user best practices and precautions such as resorting to the TOR browser or VPNs, using encrypted email services, setting up anonymous e-wallets, parceling out the total amount of owned cryptocurrencies to several different wallets.

Thus, studies have highlighted different phases of the so-called crypto-cleansing, which both state and non-state actors were deemed to engage into: (1) from fiat currency to primary VC (through a basic exchange via traditional bank accounts or by cash through VC ATMs); (2) mixing from primary coins to privacy-enhanced altcoins (through an advanced exchange); (3) layering tactics through multiple AECs, exchanges and addresses; (4) integration, withdrawing the cleansed funds from the crypto world, possibly through a hardware crypto wallet [36].

However, the money flow may actually go in the opposite direction as well, and this is another idea behind virtual-to-virtual layering schemes, that are unfortunately getting a foothold in recent years [28].

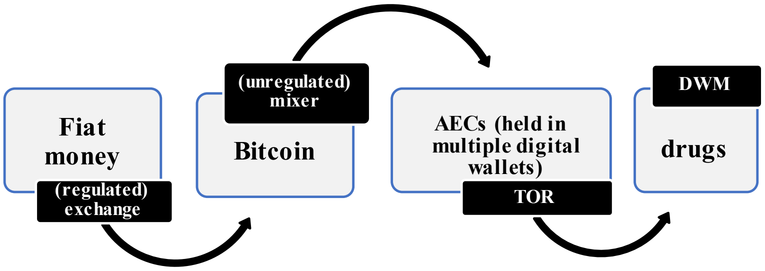

Figure 1: *Illicit use of cryptocurrencies and virtual-to-virtual layering schemes*

Namely, mixing/tumbling approaches highlight the two-fold relationship between cryptocurrencies and ML: (a) “traditional” schemes perpetrated by resorting to VCs in the placement, layering and integration stages of ML, and (b) cryptocurrencies laundering, i.e. tumbling ill-gotten VAs. In the last case illicit proceeds to be laundered are VAs themselves. Not surprisingly, the FATF acknowledged the entangling evolution of the VA sphere and the need for a common understanding of the content of the relevant RBA. Relevant authorities, in fact, deemed this ecosystem to be increasingly permeated by AECs, mixing/tumbling service providers, decentralized platforms and exchanges, as well as other products and services acting as enablers for a reduction in transparency and an increase in the obfuscation of financial flows [28].

8 Open conceptual accountability issues

Recent years have shown how blockchain space and legal order feature numerous interconnections, as well as how the transformative character of DLTs causes significant and extensive points of friction with incumbent legal systems. As far as the payment sphere is concerned, efforts are being expended to encourage evolution while trying to mitigate the risk of destabilizing the banking and financial sector. State-of-the-art legal instruments to safeguard the latter transparency-wise, in fact, empirically emerge as challenged by transformations brought about by crypto tools; this research paper highlighted how some technical features that are praised functionality-wise give rise to thoroughly unpleasant scenarios.

Arguably, the feasibility of anonymity-enhanced ecosystems complying with state-of-the-art AML/CFT regulations appears as rather weak. Recent FATF guidelines on how to apply relevant Recommendations may be referred to as a prime example of this. Furthermore, it is to be noted that the same organization has called for participating jurisdictions to forbid VASPs from engaging in activities that involve anonymity-enhancing technologies if unable to manage and mitigate relevant risks [28], which means their so-called ”obligation to abstain” from undertaking the operation is triggered.

At the same time, inherent features of the IoM seem to ideologically mismatch legal objectives aiming at anticipating changes in criminal activities [27], giving rise to major controversies. It was argued that AML/KYC requirements could go to the detriment of opportunities offered to the unbanked or non-traditional investors [66].

Concurrently, while the current AML/CFT framework relies on the “active cooperation” of the so-called “obliged entities”, the IoM is definitely developing beyond gateways and gatekeepers. Relevant transfers do not always involve regulated third parties or beneficiaries, and recent regulatory efforts have targeted not only VAs that are convertible to fiat money but also VAs that are convertible to another VA [28, 49]. The actual role and accountability attached to entities included in the scope of the 5th AML Directive, together with the effectiveness of this choice, need further scrutiny.[19] Consistently, scholars and authorities have started discussing the actual feasibility of forcing the crypto-world into a system of “approved parties” [49].

In any case, even if we try to abide by the traditional principles informing the AML/CFT framework(s) and especially when we take into consideration the recent FATF RBA guidelines, it seems pivotal to understand what may be the best prospective regulatory approaches to crypto-to-crypto mixers and advanced exchanges. These platforms, in fact, seemingly pose the most significant money laundering and terrorist financing risks; even though they have the possibility to access their own trades and wallets balances, however, imposing any specific regulatory burden on them would likely involve huge jurisdiction-wise controversies [36].

9 Considerations on bridging the gap between law as-we-know-it and crypto ecosystems

When assessing the inherent (in)compatibility between current approaches and changes set forth by blockchain-based payment and its most recent transparency and privacy-wise evolutions, it seems desirable to take into account the need for legislative actions to focus on individual cases rather than merely being technology-based. Due to the diversity of DLT-based or even blockchain-based utilities, in fact, it was noted that legal efforts ought to be grounded on the concrete function of each specific tool. On a parallel level, it is worth mentioning that all crypto-related open questions actually relate to a broader issue: the very same role and nature of regulation in the Internet landscape has always been far from straightforward [41].

More specifically, however, scholars have identified three categories blockchain-based implementations may belong to with respect to their legal impacts: (a) recycle box; (b) dark box; (c) sandbox [45]. The first set of instruments are usually implemented by AML/CFT-regulated actors and are overall compatible with existing legal frameworks, hence requiring only minor

[19] It is also interesting to resort to blockchain analytic service providers to validate source of wealth and obtain a risk rating when performing Enhanced CDD [49].

adaptations;[20] at the opposite side, the dark box category features use cases whose objectives are fundamentally illegal.[21] In between, a set of transformative innovations defy existing legal schemes because compliance would destroy the specific implementation; their objective is not illegal, but they involve risks that ought to be regulated.[22] Consistently, regulatory sandbox for blockchain was argued to call for four distinctive features: global reach, cross-sectoral flexibility, start-up friendly operating structure, use of case-tailored parameter-setting practices [45]. This categorization may provide a useful tool to apply the case-based legislation approach in a sensitive manner. The comprehensive or piecemeal outlawing option is also to be taken into account, as well as critics underlining that the only way to perform it would be to shut down the Internet altogether.

With reference to innovative legal approaches, it seems advisable to carry out a comprehensive analysis of the underlying ratio behind the EBA's idea of creating a "scheme governance authority". This entity would ensure accountability to regulators and supervisors; its setup would be mandatory for VC schemes wishing to be regulated as a financial service and interact with regulated financial services [23]. The idea might be contextualized within the broader discussion on self-regulation, co-regulation and code-based regulation as ways to provide appropriate domain-specific legal solutions to the Internet sphere [41]. Nonetheless, as compliance with such a requirement could challenge the very same existence and conceptual origin of VCs, as well as it could run the risk of destroying the whole structure, compatibility needs to be carefully assessed. The bedrock of the "regulation-through-code" reasoning, which makes it potentially relevant to the IoM landscape, is that assessed tools belong to the cyberspace landscape, which was argued to be a realm where code complements or even substitutes law from a normative order standpoint [40].

Consistently, a similar review should target the feasibility, advantages and disadvantages of involving cryptocurrency users and market participants in AML/CFT compliance, to the end of mitigating relevant risks by establishing themselves as governance authorities [25, 42].

All in all, the analysis at hand is definitively aiming at a moving target. This element cannot be overlooked and was convincingly argued to cause the so-called "risk of overfitting", i.e. the risk that rules may be technologically outdated when they enter into force. The actual dangers daunting the crypto world, in fact, largely relate to the specific use criminals make of virtual currencies, which in turns empirically depends on their ever-evolving anonymity features, relevant degrees of blockchain-embedded privacy, and on regulation and law enforcement strategies [27, 49, 40]. On an additional but parallel level, the same concept of "legal overfitting" may give rise to thoroughly inefficient rules if they were to be too specifically tailored to the needs of individual cases to be foreseeably applied to ever-evolving technologies. Thus, (too specific) case-based legislation may be burdened by its own set of risks.

As a final note, since the financial sector has arguably been the first area of systematic application of BTs [40], focusing on the anonymity and transparency aspects of the IoM and cryptocurrencies may provide impactful legislative and regulatory insights also with broader reference to the so-called "Blockchain 2.0" implementations such as smart contracts and blockchain-based organizations. The broader framework of such disruption relates to how BT, among other ideas, was argued to be structurally informing the so-called "Internet 3.0" phase [16].

[20] For instance, blockchain-based interbank settlement systems such as the Ripple network and the so-called "blockchain banking" [45].

[21] Such as the abovementioned online drugs or weapons markets, human trafficking, money laundering, terrorist financing, tax evasion, etc [45].

[22] For instance because they bypass regulated entities, such as in the DAO case [45].

10 Acronyms

AEC	Anonymity-Enhanced Cryptocurrency
AML	Anti-Money Laundering
BT	Blockchain Technology
CDD	Customer Due Diligence
CTF	Counter-Terrorist Financing
DLT	Distributed Ledger Technology
EBA	European Banking Authority
EC	European Commission
EU	European Union
FATF	Financial Action Task Force
I2P	Invisible Internet Project
IoM	Internet of Money
IoT	Internet of Things
IoV	Internet of Value(s)
KYC	Know Your Customer
ML	Money Laundering
OSINT	Open-Source Intelligence
RBA	Risk-Based Approach
STR	Suspicious Transaction Report
TOR	The Onion Router
VA	Virtual Asset
VC	Virtual Currency
VASP	Virtual Asset Service Provider

References

[1] Airfoil (2019): De-Anonymizing Anonymous Crypto Services. Data Driven Investor. Medium.com. Retrieved from: https://medium.com

[2] Al Jawaheri, H., Al Sabah, M., Boshmaf, F., Erbad, A. (2017): Deanonymizing Tor hidden service users through Bitcoin transaction analysis.
Retrieved from: https://arxiv.org/pdf/1801.07501.pdf

[3] Amsden, Z., Arora, R., Bano, S., Baudet, M. et al. (rev. 2019): The Libra Blockchain. The Libra Association.
Retrieved from: https://developers.libra.org/docs/assets/papers/the-libra-blockchain.pdf

[4] Androulaki, E., Karame, G.O., Roeschlin, M., Scherer, T., Capkun, S. (2012): Evaluating User Privacy in Bitcoin.
Retrieved from: https://eprint.iacr.org/2012/596.pdf

[5] Antonopoulos, A.M. (2017): Mastering Bitcoin. Programming the open blockchain. 2nd Edition. O'Reilly

[6] Antonopoulos, A.M. (2016): The Internet of Money. A collection of talks. Volume One. Merkle Bloom LLC

[7] Antonopoulos, A.M. (2017): The Internet of Money. A collection of talks. Volume Two. Merkle Bloom LLC

[8] Arner, W.D, Zetsche, D.A., Buckley, R.P., Barberis, J.N. (2019):The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities. European Business Organization Law Review. Asser Press.

[9] Arun, J.S., Cuomo, J., Gaur N. (2019): Blockchain for business. Discover how blockchain networks are transforming companies, driving growth, and creating new business models. Pearson Education.

[10] Athanassiou P.L. (2019): Tokens and the Regulation of Distributed Ledger Technologies: Where Europe Stood in the Last Quarter of 2018. Journal of International Banking Law and Regulation, Volume 34, Issue 3, pgg. 105-114. Thomson Reuters and Contributors

[11] Avgouleas, E., Chiu, I.H-Y., Schammo, P. (2019): Editorial. European Business Organization Law Review. Asser Press.

[12] Bambara J.J., Allen P.R. (2018): Blockchain. A practical guide to developing business, law, and technology solutions. McGraw Hill Education

[13] Barone, R., Masciandaro, D. (2019): Cryptocurrency or usury? Crime and alternative money laundering techniques. European Journal of Law and Economics. Springer

[14] Bartoletti, M., Carta, S., Cimoli, T., Saia, R. (2019): Dissecting Ponzi schemes on Ethereum: identification, analysis, and impact. Future Generation Computer System.
Retrieved from: https://arxiv.org/pdf/1703.03779.pdf

[15] Casey, M., Crane, J., Gensler, G., Johnson, S., Narula, N. (2018): The Impact of Blockchain Technology on Finance: A Catalyst for Change. International Center for Monetary and Banking Studies.

[16] Casey, M.J., Vigna P. (2018): The Truth Machine: the Blockchain and the Future of Everything. St. Martin's Press.

[17] Chen, W., Zheng, Z., Ngai, E.C., Zheng, P., Zhou, Y. (2019): Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum. IEEE Access.
Retrieved from: https://www.semanticscholar.org

[18] Danzmann, M. (2019): Why State Currencies Will Not Be Replaced by Cryptocurrencies. Journal of International Banking Law and Regulation, Volume 34, Issue 8, pgg. 272-278. Thomson Reuters and Contributors.

[19] Dion-Schwarz, C., Manheim, D., Johnston, P.B. (2019): Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats. Rand Corporation.
Retrieved from: https://www.rand.org/

[20] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

[21] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU

[22] Dupont, J., Squicciarini, A.C. (2015): Towards De-Anonymizing Bitcoin by Mapping Users Location. Retrieved from: https://dl.acm.org/citation.cfm?id=2699128

[23] European Banking Authority (July 2014): EBA Opinion on "Virtual Currencies".
Retrieved from: https://eba.europa.eu

[24] European Banking Authority (January 2019): Report with advice for the European Commission on crypto-assets. Retrieved from: https://eba.europa.eu

[25] European Parliament (July 2018): Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion.
Retrieved from: http://www.europarl.europa.eu

[26] European Securities and Market Authority (January 2019): Advice. Initial Coin Offerings and

Crypto-Assets. Retrieved from: https://www.esma.europa.eu

[27] Europol (2019): Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement. European Union Agency for Law Enforcement Cooperation. Retrieved from: https://www.europol.europa.eu

[28] FATF (June 2019): Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers. Retrieved from: https://www.fatf-gafi.org

[29] FATF (June 2015): Guidance for a Risk-Based Approach: Virtual Currencies. Retrieved from: https://www.fatf-gafi.org

[30] FATF (rev. June 2019): International Standards on Combating Money Laundering and the Financing of Terrorism and Proliferation. The FATF Recommendations. Retrieved from: http://www.fatf-gafi.org

[31] FATF (June 2019): Public Statement on Virtual Assets and Related Providers. Retrieved from: http://www.fatf-gafi.org

[32] FATF (June 2014): Virtual Currencies: Key Definitions and Potential AML/CFT Risks. Retrieved from: https://www.fatf-gafi.org

[33] Fleder, M., Kester, M.S., Pillai, S.U. (2015): Bitcoin Transaction Graph Analysis. Retrieved from: https://arxiv.org/pdf/1502.01657.pdf

[34] Fradera, F. (2018): Conference Report on 'Digital Revolution: Data Protection, Artificial Intelligence, Smart Products, Blockchain Technology and Virtual Currencies. Challenges for Law in Practice'. European Review of Private Law, 5-2018: 707-712.

[35] French, T., Stettner, B. (2019): Anti-Money Laundering Regulation of Cryptocurrency: U.S. and Global Approaches. The International Comparative Legal Guide to: Anti-Money Laundering 2019. Allen Overy. Retrieved from: https://www.allenovery.com

[36] Fruth, J. (2018): Crypto-cleansing: strategies to fight digital money laundering and sanctions evasion. Financial Regulatory Forum. Reuters. Retrieved from: https://www.reuters.com

[37] Furneaux, N. (2018): Investigating Cryptocurrencies. Understanding, extracting, and analyzing blockchain evidence. Wiley.

[38] Girasa, R. (2018): Regulation of cryptocurrencies and blockchain technologies. National and international perspectives. Palgrave Studies in Financial Services Technology. Palgrave Macmillan.

[39] Giuliano, M. (2018): La Blockchain e gli Smart Contracts nell'innovazione del diritto nel terzo millennio". Il diritto dell'informazione e dell'informatica. Year XXXIV, n. 6, pgg. 989-1039. Giuffrè

[40] Hacker, P., Lianos, I., Dimitropoulos, G., Eich, S. (2019): Regulating Blockchain: Techno-Social and Legal Challenges – An introduction. Forthcoming. Oxford University Press. Retrieved from: https://papers.ssrn.com

[41] Herian, R. (2019): Regulating Blockchain: Critical Perspectives in Law and Technology. Routledge.

[42] Hofert, E. (2019): Regulating Virtual Currencies: Shortcomings of the EU Framework. Computer Law Review International. 1:2019 pgg. 10-15. OttoSchmidt

[43] Lischke, M., Fabian, B. (2016): Analyzing the Bitcoin Network: the First Four Years. Future Internet. MDPI. Retrieved from: https://www.semanticscholar.org

[44] Lopp, J. (2019): How Will Facebook's Libra "Blockchain" Really Work? One Zero. Medium.com. Retrieved from: https://onezero.medium.com

[45] Maupin, J.A. (2017): Mapping the Global Legal Landscape of Blockchain and other Distributed Ledger Technologies. Forthcoming in CIGI Academic Paper Series. Retrieved from: https://papers.ssrn.com

[46] Möslein, F. (2018): Conflicts of Laws and Codes: Defining the Boundaries of Digital Jurisdictions. Retrieved from: https://papers.ssrn.com

[47] Neudecker, T., Hartenstein, H. (2017): Could Network Information Facilitate Address Clustering in Bitcoin? Retrieved from: https://fc17.ifca.ai

[48] Ober, M., Katzenbeisser, S., Hamacher, K. (2013): Structure and Anonymity of the Bitcoin Transaction Graph. Retrieved from: https://www.mdpi.com/1999-5903/5/2/237/htm

[49] Paesano, F. (2019): Working Paper 28. Regulating cryptocurrencies: challenges considerations. Basel Institute on Governance. Retrieved from: https://www.baselgovernance.org

[50] Perugini, M.L., Spada, M.C. (2018): Distributed Ledger Technologies e Sistemi di Blockchain. Diritto dell'Informatica e delle Nuove Tecnologie. DirICTo. Cendon / Book. Key Editore.

[51] Quiniou, M. (2019): The Advent of Disintermediation. ISTE and Wiley.

[52] Rahmatian, A. (2019): Electronic Money and Cryptocurrencies (Bitcoin): Suggestions for Definitions. Journal of International Banking Law and Regulation, Volume 34, Issue 3, pgg. 115-121. Thomson Reuters and Contributors.

[53] Reid, F., Harrigan, M. (2012): An Analysis of Anonymity in the Bitcoin System.
Retrieved from: https://arxiv.org/pdf/1107.4524.pdf

[54] Sarfraz, U., Alam, M.M., Zeadally, S., Khan, A. (2018): Privacy Aware IOTA Ledger: Decentralized Mixing and Unlinkable IOTA Transactions. Computer Networks.
Abstract retrieved from: https://www.researchgate.net

[55] Sarzana di S. Ippolito, F., Nicotra, M. (2018): Diritto della Blockchain, Intelligenza Artificiale e IoT. Wolters Kluwer

[56] Sotiropulou, A., Ligot S. (2019): Legal Challenges of Cryptocurrencies: Isn't It Time to Regulate the Intermediaries? European Company and Financial Law Review 5/2019: 652-675.

[57] Tennant, L. (2017): Improving the Anonymity of the IOTA Cryptocurrency.
Retrieved from: https://laurencetennant.com/papers/anonymity-iota.pdf

[58] The Cryptocurrency Consultant (2019): Crypto Forensics. How the Blockchain convicts criminals. The Startup. Medium.com. Retrieved from: https://medium.com

[59] The Cryptocurrency Consultant (2019): What is the Internet of Values? A story of the Web 3.0 and cryptocurrencies. The Startup. Medium.com. Retrieved from: https://medium.com

[60] The Cryptocurrency Consultant (2019): Analyzing Money Laundering on the Bitcoin Blockchain. The Startup. Medium.com. Retrieved from: https://medium.com

[61] The Law Society (2017): "Blockchain: The Legal Implications of Distributed Systems". Horizon Scanning.

[62] Yermack, D. (2017): Corporate Governance and Blockchains. Oxford Review of Finance, 2017: 7-31.

[63] Yi, S., Zhang, Y. (2018): Privacy in Cryptocurrencies: An Overview. Medium.com. Retrieved from: https://medium.com

[64] Yi, S., Zhang, Y. (2018): Privacy in Cryptocurrencies: Mixing-based Approaches. Medium.com. Retrieved from: https://medium.com

[65] Yi, S., Zhang, Y. (2019): Privacy in Cryptocurrencies: Zero-Knowledge and zk-SNARKs. Medium.com. Retrieved from: https://medium.com

[66] Wachsman (2019): Answering One of Blockchain's Biggest Questions: Anonymity or Pseudonymity? Medium.com. Retrieved from: https://medium.com

[67] Wang, H., Ma, S., Dai, H.N., Imran, M., Wang, T. (2019): Blockchain-based data privacy management with Nudge theory in open banking. Future Generation Computer Systems.
Retrieved from: https://doi.org/10.1016/j.future.2019.09.010

[68] Weber, M., Domeniconi, G., Chen, J., Weidele, D.K.I., Bellei, C., Robinson, T., Leiserson, C. (2019): Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics. KDD '19 Workshop on Anomaly Detection in Finance. Retrieved from: https://arxiv.org/pdf/1908.02591.pdf

[69] Zetzsche, D.A., Buckley R.P., Arner D.W.: The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. University of New South Wales Law Research Series. Retrieved from: http://www5.austlii.edu.au