The Internet of Money between Anonymity and Publicity: Legal Challenges of Distributed Ledger Technologies in the Crypto Financial Landscape*

Nadia Pocher[0000−0003−1472−2963]

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 project focuses on the impacts exerted by the tech schemes behind virtual currencies on the EU framework to prevent the misuse of the financial system and it aims to explore legal challenges posed in the IoM landscape by the double-edged nature of DLTs as both transparency and privacy-oriented. On the one hand, it plans to identify effective legislative and regulatory measures to ensure crypto accountability from an AML/CFT standpoint, as well as to assess the relevant role of pseudonymity. On the other hand, it pursues to discover innovative legal approaches to secure AML/CFT active cooperation in the crypto ecosystem(s), to the end of mitigating anonymity and traceability concerns while respecting both the value of publicity and transparency in the law and the conceptual origin of the crypto economy.

Keywords: Internet of Money · cryptocurrencies · DLT · blockchain · AML · CFT · pseudonymity · privacy · transparency · traceability.

1 State of the art

This research project is based on the following four preliminary pillars.

1.1 The crypto economy and the role of underlying technologies

To start with, it acknowledges transformations generated by the advent of the so-called crypto economy to the global financial landscape, as the latter is confronted with non-traditional forms of currencies in the wake of the Bitcoin launch in January 2009 as well as with industry-altering ideas such as Initial Coin Offerings (ICOs) or the recent Facebook-led Libra initiative. Conceptually, this

disruptive monetary ecosystem gave birth to the notion of Internet of Money (IoM) (Antonopoulos 2016, 2017b). It is profoundly influenced by inherent features of Distributed Ledger Technologies (DLTs) and, more specifically, of their blockchain-powered subset.

In short, blockchain technology (BT) is a cryptography-based peer-to-peer network system and it is the most common DLT scheme behind cryptocurrencies (Antonopoulos 2017a). Its properties responded to socio-economic queries pursuing decentralized and disintermediated structures that allow seamless transactions with no need of a trusted central party (Lischke and Fabian 2016), thus devising the concept of "the Internet of Value (IoV)".[1] Unprecedented degrees of verifiability, transparency, inalterability, trust and security stirred up interest in the most diverse fields and the pivotal role of BT among DLTs was highlighted within the European Commission's FinTech Action Plan (Arun, Cuomo, and Gaur 2019; Bambara and Allen 2018; Hacker et al. 2019). Nonetheless, projects such as IOTA wish to take these features to the next level by employing blockchain-unrelated DLTs.[2]

1.2 Illicit use of cryptocurrencies and the race to legislative and regulatory intervention

Secondly, though, cryptocurrencies and their anonymity-wise features were extensively argued to be vulnerable to large-scale exploitation for the most diverse illicit purposes[3] and to pose significant money laundering and terrorist financing risks (Directive (EU) 2018/843; Europol 2019). Consequently, a growing number of regulation attempts have been made, against the backdrop of a broader set of legislative actions targeting DLTs on the grounds that they often put the logic behind existing legal regimes to the test (Hacker et al. 2019; Maupin 2017; Paesano 2019). Essentially, the diversity of legal initiatives ranges from crypto-specific legislation to interpretative instances of existing legal frameworks in light of new technologies, thereby shifting between a pro-active and a reactive approach to regulatory scrutiny and intervention (Maupin 2017; Paesano 2019).

The Financial Action Task Force (FATF) has been issuing international Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) guidelines for virtual currencies (VCs) and assets (VAs) since 2014 and is currently working towards strengthening the application of its Recommendations (FATF 2019b) to DLTs. At the EU level, the 5th AML Directive (Directive (EU) 2018/843) targets VCs by labeling fiat/crypto exchanges and wallet service providers as reporting entities, thereby making them subject to Know Your Customer (KYC) and

1. The IoV was argued to be the next generation of Internet compared with the traditional Internet of Information (Chen et al. 2019).

2. More specifically, IOTA is designed for the Internet of Things (IoT) industry and employs a type of DLT called Directed Acyclic Graph, the Tangle

3. Such as transactions on the dark web, online gambling or financing of criminal and terrorist activities (Dion-Schwarz et al. 2019; Europol 2019)

Suspicious Transaction Reporting (STR) obligations. Even within blockchain-powered disintermediated ecosystems, the general tendency is to keep focusing on gateways to/from the traditional regulated financial system (FATF 2019a).

1.3 Crypto traceability, pseudonymity and money laundering: a multi-layered relationship

From a third standpoint, however, many actions were argued to insufficiently acknowledge crypto technical aspects; critics challenged both pinpointed reporting entities and the claimed level of anonymity and privacy. In spite of common misconceptions, major VCs such as Bitcoin and Ethereum are pseudonymous rather than anonymous and the same was suggested for Libra (Amsden et al. 2019; Lopp 2018; Wachsman 2019). Even if no real-world identities are involved, there are ways to link public addresses to real identities (Al Jawaheri et al. 2019; Dupont and Squicciarini 2015; Fleder, Kester, and Pillai 2015; Lischke and Fabian 2016);[4] parallelly, blockchain analysis techniques were enhanced over time and allow for a certain traceability of transaction flows (Airfoil 2019; Al Jawaheri et al. 2019; Paesano 2019; The Cryptocurrency Consultant 2019). Besides, the address used, the transferred amount and other metadata are permanently and publicly stored on the ledger (Wachsman 2019).

Nevertheless, sharpened intelligence methods also spawned the development of "privacy coins", such as Monero and Zcash, whose goal is to provide complete anonymity through privacy-enhancements such as embedded mixing/tumbling services. The latter are offered by other platforms to users of less-anonymous VCs, to obscure identifiability of tainted coins (Maupin 2017; Sun and Zhang Yi 2018a). Namely, the last topic highlights 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.[5]

1.4 The limits of conventional approaches to cryptocurrency regulation

Sections 1-3 highlight how some blockchain features that are praised functionality-wise give rise to thoroughly unpleasant scenarios. Concurrently, 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, which was imagined and created to keep intermediaries out of the picture and seem to inherently challenge conventional legal and accountability mechanisms. This friction emerges as of topical importance

4. As for Libra, the protocol does not link accounts to real-word identities; Calibra, however, seemingly requires AML/KYC (Amsden et al. 2019; Lopp 2018).

5. In the last case illicit proceeds are VAs themselves. The FATF itself acknowledged the entangling evolution of the VA sphere and the need for a common understanding of the content of the relevant risk-based approach (RBA) (FATF 2019a).

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 cryptographic innovations keep defying legislative attempts (Maupin 2017).

On a parallel level the same tech design of VCs arguably mismatches traditional approaches to AML/CFT regulation of financial transactions and payment systems. Another array of reasons causes unsatisfactory legal results: (a) distributed governance mechanisms of VCs and relevant accountability levels vary significantly,[6] (b) crypto transactions involve both traditional intermediaries and other actors, (c) their lifecycle features a multi-layered stakeholdership,[7] (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. Hence, authorities such as the European Banking Authority (EBA) put forward innovative approaches to the mitigation of crypto risks, namely a private/public co-regulation regime grounded on "regulated self-regulation", which would be implemented through the so-called "regulation-through-code" (EBA 2014; Hofert 2019). Besides, a "self-declaration" role of VC users is being assessed at the EU level (Directive (EU) 2018/843).

2 Research questions

In light of all the above, this research aims to provide an answer to the following main research questions:
1. Is any principle-wise aspect of the EU legal framework to prevent the misuse of the financial system called into question by cryptocurrencies being inherently influenced by the double-edged nature of DLTs as both transparency and privacy-oriented?
2. Is there an effective level and type of legislative and regulatory intervention to ensure crypto accountability from an Anti-Money Laundering standpoint, possibly leveraging on pseudonymity?
3. If not, what innovative legal approach(es) and concepts, such as regulation-through-code, may secure AML/CFT active cooperation in the crypto landscape and mitigate anonymity and traceability concerns while respecting the conceptual origin of crypto economy?

3 Description of the project

3.1 Setting a terminological and conceptual reference framework

The first part of this project is both technically and legally oriented and aims at laying out conceptual and definitional backbones to the end of providing the

6. Namely between the poles of fully public distributed ledgers and private ledgers (Hofert 2019).

7. Players involved, in fact, range from users to miners to exchanges to trading platforms, wallet providers, coin investors and offerors (Houben and Snyers 2018).

following sections with proper contextualization. It entails a preliminary analysis of the system of principles and values governing the evolution of DLTs and their payment-related implementations, in order to pursue other two specific goals: (a) clearly defining the object and scope of this project and (b) reviewing several features attached to these technologies in the context of the IoM, such as sector-specific notions of transparency, privacy and publicity.

The goal sub (a) addresses the need for terminological clarity in legal research and discourse, not to mention legislation and regulation, especially when innovative frameworks are concerned. A proper investigation of the issue at hand requires to go beyond the misleading interchangeability amongst concepts such as "cryptocurrencies", "VCs", "VAs", "blockchain", "Bitcoin blockchain", "DLTs", "non blockchain-based DLTs", "stablecoins", "altcoins", "convertible and non-convertible VCs", "centralized vs. decentralized VCs", "VASPs". The preceding labels are not just words, they shape the bottom line of relevant ecosystems and stakeholders; referring to them inaccurately means misinterpreting their essence as well as legal and accountability impacts. Initiatives such as Libra and IOTA highlight the topicality of this preliminary issue.

As to the (b) section, reviewing the notions of "privacy" and "transparency" in the realm of cryptocurrencies calls for re-tracing the socio-economic ideology that spurred their advent, in order to assess (1) what "privacy" means for these instruments, (2) its relationship with concepts such as secrecy, traceability and pseudonymity, and (3) whether it is currently and prospectively inherent to VCs (Sun and Zhang Yi 2018a).[8] Different examples of the latter are scrutinized in a case-study fashion, with reference to their technical aspects as they evolved beyond shared traits such as distributed consensus, transaction transparency and party entity abstraction.[9] As for blockchain-based VCs, crypto-related "privacy" and "publicity" are confronted by breaking the issue down to pieces of blockchain-embedded information as to determine whether they are private or public; three aspects are relevant in this regard: a) privacy of identity or user-identity privacy;[10] b) privacy of transaction data/information;[11] c) privacy of

8. Studies have tackled privacy impacts of Bitcoin implementations and underlined the difference between activity unlinkability and profile indistinguishability (Androulaki et al. 2013)

9. Distributed consensus means they feature no central point of failure or control. Trans. transparency stems from ledger entries being retraceable and tamper-resistant

10. Privacy of identity relates to the concept of anonymity; 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" (Sun and Zhang Yi 2018a)

11. Privacy of transaction data is a mutable concept; 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. There is no binary (public vs. anonymous) solution and there is a need for a flexible and structured approach to the "anonymity set" of different blockchains (Monero's anonymity set is arguably significantly larger than Bitcoin's) (Sun and Zhang Yi 2018a)

the total blockchain state.[12] A parallel assessment shall be carried out for non-blockchain-based cryptocurrencies.

3.2 Pseudonymity in cryptocurrencies between privacy enhancement and blockchain intelligence

The second section builds on findings pertaining degrees of "privacy" and "transparency" featured by the diverse array of cryptocurrencies, to the end of tackling pseudonymity and transaction traceability in the IoM landscape. It features a two-fold approach, as it focuses on (a) the multi-layered topic of intelligence strategies and (b) the concept of privacy-enhanced VCs and relevant ever-evolving techniques. The end is to contextualize crypto pseudonymity by determining whether (1) all types of cryptocurrencies are pseudonymous, (2) the notion always holds the same meaning, and (3) there is a future for this concept. Technical aspects[13] that may exert influence in this realm are assessed, as well as the role of forensics in ensuring accountability.

The part sub (a) focuses on blockchain and crypto-forensics and on relevant achievable results against the backdrop of privacy-boosting strategies; it entails references 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 Airfoil 2019; Paesano 2019; The Cryptocurrency Consultant 2019. 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 are taken into account.[14] Reference is not limited to Bitcoin forensics; data-exploitation strategies were deployed also on the Ethereum blockchain and discussions are ongoing for non BT-based DLTs.[15]

The topic sub (b) targets anonymity-enhanced VCs and takes a case-study and AML-oriented approach, leveraging on experiences such as Monero and Zcash.[16] It is grounded on three methods that have been identified to obfus-

12. It was argued that different attributes of the total blockchain state can be private to different extents (Sun and Zhang Yi 2018a)

13. Such as blockchain internal governance and types of consensus algorithm

14. On transaction-graph analysis:(Fleder, Kester, and Pillai 2015; Ober, Katzenbeisser, and Hamacher 2013); On user activities clustering:(Neudecker and Hartenstein 2017); On clustering heuristics (Androulaki et al. 2013; Lischke and Fabian 2016; Reid and Harrigan 2013); On transaction fingerprinting using p.a. information:(Fleder, Kester, and Pillai 2015); On using off-network information:(Lischke and Fabian 2016; Reid and Harrigan 2013); On web-scraping and OSINT tools:(Airfoil 2019).

15. Notably to detect smart Ponzi schemes on Ethereum (Chen et al. 2019); as for IOTA: (Tennant 2017).

16. Unlike the Bitcoin blockchain, "privacy coins" do not keep unencrypted records of data such as wallet addresses and transactions amounts. Zcash reaches a high degree of privacy by making use of "zero-knowledge proofs", whereas Monero is slightly less anonymous but implements more intensively tested techniques of ring signatures. Zcash offers selective transparency of transactions and it originally defined itself as "Bitcoin

cate financial flows: (x) mixing-/tumbling-based approaches; (y) zero-knowledge based privacy; (z) user best practices (Sun and Zhang Yi 2018b, 2018a; Zhang and Sun 2019).[17] Within the (b) issue, and ultimately going beyond it, a subsection is dedicated to currency mixing/tumbling in the crypto world, in view of its pivotal role in the ML/TF landscape.[18] Bitcoin mixing services originated the notion of cryptocurrency laundering (Airfoil 2019). Some "privacy coins" embed this system, but it is also possible to convert Bitcoins into less trackable VCs via crypto-to-crypto mixers after obtaining them via a regulated fiat-to-crypto exchange; this is the reason why recent years have seen the rise of virtual-to-virtual layering schemes (FATF 2019a, 2019c).

3.3 Legislative and regulatory approaches to cryptocurrencies within an "active cooperation"-based AML/CFT framework

From a third point of view, this project focuses on the observed legal and regulatory impacts exerted by VCs on the EU financial ecosystem, and most notably on the AML/CFT framework. This part is divided into three subsections and assesses: (a) relevant AML/CFT initiatives targeting cryptocurrencies and VAs, (b) perceived peculiarities of VCs from an AML/CFT risk perspective and (c) specificities related to the feasibility of crypto-related "obliged entities" and relevant advantages and disadvantages.

The topic sub (a) is tackled by addressing most relevant principles, concepts, actors and obligations in this realm. Hence, this first subsection entails reference to preventive measures such as Customer Due Diligence (CDD), KYC, recordkeeping, STR, internal controls, as well as sanctions, enforcement, licensing and/or registration of gatekeeper-like entities. Also in the crypto context, CDD requires to identify (and verify the identity of) transaction counterparties, such as customers and beneficial owners, and to assess purpose and intended nature of the business relationship (Paesano 2019).[19] The analysis starts out from international guidelines and delves into the legislative approach taken at the EU level, as enshrined by the 5th AML Directive, and into elements arisen from transposition procedures brought about by Member States and relevant enforcement data. Yet, the scope of the comparative analysis may encompass

is like HTTP for money, Zcash is HTTPS". DASH might also be arguably labelled as a "privacy coin". The possibility of enhancing IOTA's privacy protocols despite its quantum resilient hash-based signatures is under assessment (Sarfraz et al. 2019; Tennant 2017).

17. The latter entails the use of anonymizers such as The Onion Router (TOR), Invisible Internet Protocol (I2P) or Dark Wallet to hide the origin of the transaction or employing a new address for every payment (Sun and Zhang Yi 2018a).

18. The concept leverages on the fungibility of cryptocurrencies 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 (Sun and Zhang Yi 2018a).

19. Tracing the IP address may be demanded when Enhanced CDD is required (FATF 2019a).

non-EU jurisdictions whose experiences may provide useful insights to the goal of this research.

Subsection (b) wishes to identify the main risks posed by VCs in the area of ML and financing of criminal activities, as well as to determine which implementations are more dangerous from a concrete perspective. It accounts for the distinction between centralized and decentralized VAs-related services. The approach is strengthened by analyzing the difference between cryptocurrencies and other means that can be used to engage in non-face-to-face business relationships and to rapidly move funds globally, against the backdrop of the evolving landscape of digital payments; a data-based approach may highlight whether and how crypto-transactions are actually more dangerous than the ones performed using regular fiat money. Reference is based on the abovementioned multi-layered relationship between VCs and the concept of ML.

The analysis sub (c) builds on the acknowledgement that while the AML/CFT framework relies on the active cooperation of the so-called "obliged entities", the IoM is developing beyond gateways and gatekeepers and transfers do not always involve regulated third parties or beneficiaries, as well as that recent regulatory efforts have targeted not only VAs that are convertible to fiat money but also VAs that are convertible to another VA (FATF 2019a; Paesano 2019). The actual role and accountability attached to entities included in the scope of the 5th AML Directive, as well as the effectiveness of this choice, need further scrutiny.[20]

3.4 The IoM between anonymity and publicity: legal and AML/CFT impacts of the double-edged nature of DLTs

The fourth part strives to integrate previous results and to (a) assess whether the double-edged nature of DLTs as both transparency and privacy-oriented may be reconciled to allow for crypto payments to comply with state-of-the-art principles informing legislation targeting financial transactions, and (b) understand whether it is possible to determine a suitable level of legislative intervention to mitigate secrecy-related concerns while enabling crypto-specific socio-economical and cross-border financial goals.

This section plans to honor 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. More specifically, 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 (Maupin 2017). 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 adaptations;[21] at the opposite side,

20. It is also interesting to resort to blockchain analytic service providers to validate source of wealth and obtain a risk rating for Enhanced CDD (Paesano 2019).

21. For instance, blockchain-based interbank settlement systems such as the Ripple network and the so-called "blockchain banking" (Maupin 2017).

the dark box category features use cases whose objectives are fundamentally illegal. 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]

The goal is to understand whether the current EU AML/CFT framework is inherently compatible with changes set forth by the advent of blockchain-based payment and its most recent transparency- and privacy-wise evolutions, which leads to topic sub (b). The comprehensive or piecemeal outlawing option is taken into account, as well as critics underlining that the only way to perform it would be to shut down the Internet altogether. Parallelly, it is to be noted that (1) the FATF 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, as well as (2) scholars and authorities have started discussing the actual feasibility of forcing the crypto-world into the abovementioned system of "approved parties" (FATF 2019a; Paesano 2019).

3.5 Bridging the gaps between law as-we-know-it and the crypto ecosystem: innovative legal approaches and regulation-through-code

The final section of this research projects aims to (a) come to terms with those specificities of cryptocurrencies that may clash with existing legislative, regulatory and supervisory schemes and, most importantly, concepts, in order to (b) understand what fences innovative AML/CFT solutions ought to mend and (c) put forward possible ideas from an evolutionary perspective. Preceding sections are bound to highlight topical issues to be borne in mind, as well as suggest elements to shape an innovative and efficient solution or part thereof. The bedrock of this reasoning 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 (Hacker et al. 2019).

Consistently, the topic sub (b) elaborates on technical features of stakeholders and actors involved in crypto transactions and is coupled with an analysis of the underlying ratio of the abovementioned idea of creating a "scheme governance authority" that would ensure accountability to regulators and supervisors and whose setup would be mandatory for VC schemes wishing to be regulated as a financial service and interact with regulated financial services. As compliance with such a requirement could challenge the very same existence and conceptual origin of VCs and runs the risk of destroying the whole structure, compatibility needs to be assessed. This is why in order to tackle subsection (c) a parallel aspect will be taken into consideration, consistently with findings of the preceding steps of this research, namely the role of cryptocurrency users and market participants in complying with AML/CFT obligations, mitigating relevant risks

22. for instance because they bypass regulated entities, such as in the DAO case. (Maupin 2017).

and establishing themselves as governance authorities (EBA 2014; Houben and Snyers 2018; Hofert 2019).

4 Methodological remarks

The abovementioned subsections feature different, albeit ultimately convergent, methodological approaches. The main reason lies in the concurrent presence of legal, technical and socio-economic aspects, which need to be scrutinized in a way that both reflects their specificities and is consistent with the overall structure of this project and its intended innovation-oriented objectives. Hence, relevant methodologies are foreseen to range from deductive, to inductive, to abductive and speculative reasonings. Multiple approaches will not cause inconsistencies, as reasons will be clarified, and each specific finding contextualized.

Consistently, parts that are legally oriented from a state-of-the-art perspective are based on a comparative documentary analysis of systems of values and concepts as primarily enshrined by EU legal sources and policy instruments, in conjunction with international guidelines and MS-level transposition and implementation of legal, regulatory and operational measures. They mainly feature a deductive approach. Sections wishing to go beyond established approaches by conceptualizing findings draw from a deductive approach but are grounded on inductive and speculative reasoning from both a normative and a non-normative perspective; inherently, they are also bound to take an evaluative stand. The employment of abductive reasoning cannot be ruled out, as a pragmatical standpoint is foreseen as pivotal in tackling the complexities of the issues at hand.

All sections deal or are somehow confronted with technical aspects of information technology, albeit are still placed within the setting of legal arguments. Consequently, they draw from both doctrinal and empirical analyses; they will involve documentary research based on legal and technical sources, and they will feature an inductive approach to impacts on principles and systems of values. Meanwhile, insofar as they also focus on the perspective of relevant crypto stakeholders and socio-legal aspects, they may also infer from field research and interviews. Inherently technical parts will also feature a descriptive approach, built on the abovementioned documentary analyses which will be enhanced by the participation in conferences, events, secondments and trainings.

5 Expected results

This research is bound to identify friction points between transformations brought about by DLT-based tools, notably blockchain-based, and traditional principles underlying legislative approaches to financial transactions. The extent to which these changes diverge from those generated by other instances of digitalization and the globalization process should be further investigated, as well as impacts on the system of values informing the EU AML/CTF landscape. Arguably, the feasibility of anonymity-enhanced ecosystems complying with state-of-the-art regulations appears as rather weak. Recent FATF guidelines on how to apply

relevant Recommendations may be referred to as a prime example of this. At the same time, inherent features of the IoM seem to mismatch legal objectives aiming at anticipating changes in criminal activities (Europol 2019), 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 (Wachsman 2019).

The analysis is definitively aiming at a moving target, which causes the risk of overfitting, as the actual risk behind cryptocurrencies largely relies on the relevant use by criminals, which in turns depends on anonymity features, blockchain-embedded privacy, regulation and law enforcement (Paesano 2019).[23] The proposed study does not take for granted that disruptive technology equals disrupted law (Fradera 2018). Nevertheless, a feature of BTs is to implement tasks traditionally performed by law and legal institutions (Möslein 2018), as well as to carry an alternative vision of the economic system (Hacker et al. 2019), which gives rise to foresee principle-wise alterations grounded on the transposition of interactions pertaining to a specific social and economic environment 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, possibly giving rise to a so-called "emergent technocracy" (Hacker et al. 2019).

This proposal plans to reach an assessment of the scope of possible innovation-suited reforms, built on cross-jurisdictional cooperation via an integrated approach and possibly on the concepts of regulation by design and regulation-through-code (EBA 2014; Hofert 2019). As the financial sector has arguably been the first area of systematic application of BTs (Hacker et al. 2019), focusing on the anonymity and publicity aspects of the IoM and cryptocurrencies may provide impactful legislative and regulatory insights also with reference to the so-called "Blockchain 2.0" implementations such as smart contracts and blockchain-based organizations.

6 Acknowledgement

This project 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.

References

Airfoil. 2019. *De-Anonymizing Anonymous Crypto Services.* `https://medium.com/datadriveninvestor/`.

23. As for the risk of overfitting, it was argued that rules might be technologically outdated when they enter into force (Europol 2019; Hacker et al. 2019).

Al Jawaheri, Husam, Mashael Al Sabah, Yazan Boshmaf, and Aiman Erbad. 2019. "Deanonymizing Tor hidden service users through Bitcoin transactions analysis." *Computers & Security* 89. arXiv: 1801.07501.

Amsden, Zachary, Ramnik Arora, Shehar Bano, Mathieu Baudet, Sam Blackshear, Abhay Bothra, and George Cabrera. 2019. "The Libra Blockchain - White Paper": 1–29.

Androulaki, Elli, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. 2013. "Evaluating user privacy in Bitcoin." *Lecture Notes in Computer Science* 7859:34–51. doi:10.1007/978-3-642-39884-1_4.

Antonopoulos, Andreas M. 2016. *The Internet of Money - Volume One.* Merkle Boom LLC.

———. 2017a. *Mastering Bitcoin, 2nd Edition.* O'Reilly Media, Inc.

———. 2017b. *The Internet of Money - Volume Two.* Merkle Boom LLC.

Arner, Douglas W., Dirk A. Zetzsche, Ross P. Buckley, and Janos N. Barberis. 2019. "The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities." *European Business Organization Law Review* 20 (1): 55–80. doi:10.1007/s40804-019-00135-1.

Arun, Jai Singh, Jerry Cuomo, and Nitin Gaur. 2019. *Blockchain for Business.* Pearson Education.

Athanassiou, Phoebus 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* 34 (3): 105–114.

Avgouleas, Emilios, Iris H.Y. Chiu, and Pierre Schammo. 2019. "Editorial." *European Business Organization Law Review* 20 (1): 1–4. doi:10.1007/s40804-019-00140-4.

Bambara, Joseph J., and Paul R. Allen. 2018. *Blockchain. Practical Guide to Developing Business, Law, and Technology Solutions.* McGraw-Hill.

Barone, Raffaella, and Donato Masciandaro. 2019. "Cryptocurrency or usury? Crime and alternative money laundering techniques." *European Journal of Law and Economics* 47 (2): 233–254. doi:10.1007/s10657-019-09609-6.

Chen, Weili, Zibin Zheng, Edith C.H. Ngai, Peilin Zheng, and Yuren Zhou. 2019. "Exploiting Blockchain Data to Detect Smart Ponzi Schemes on Ethereum." *IEEE Access* 7 (c): 37575–37586. doi:10.1109/ACCESS.2019.2905769.

Danzmann, Max. 2019. "Why State Currencies Will Not Be Replaced by Cryptocurrencies." *Journal of International Banking Law and Regulation* 34 (8): 272–278.

Dion-Schwarz, Cynthia, David Manheim, Patrick B. Johnston, and Rand Corporation. 2019. *Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats.* Rand.

Directive (EU) 2015/849. *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.*

Directive (EU) 2018/843. *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.*

Dupont, Jules, and Anna Cinzia Squicciarini. 2015. "Toward De-Anonymizing Bitcoin by Mapping Users Location." In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy,* 139–141. Association for Computing Machinery. doi:10.1145/2699026.2699128.

EBA. 2014. *EBA Opinion on virtual currencies.* Technical report July. https://eba.europa.eu/.

———. 2019. *Report with advice for the European Commission on crypto-assets.* Technical report January. https://eba.europa.eu/.

ESMA. 2019. *Advice - Initial Coin Offerings and Crypto-Assets.* Technical report January. https://www.esma.europa.eu/.

Europol. 2019. *Do Criminals Dream of Electric Sheep? How Technology shapes the future of crime and law enforcement.* https://www.europol.europa.eu/.

FATF. 2014. *Virtual currencies – Key Definitions and Potential AML/CFT Risks.* Technical report June. http://www.fatf-gafi.org/.

———. 2015. *Guidance for a Risk-Based Approach: Virtual Currencies.* Technical report June. http://www.fatf-gafi.org/.

———. 2019a. *Guidance for a risk-based approach: virtual assets and virtual asset service providers.* Technical report June. Paris: FATF. http://www.fatf-gafi.org/.

———. 2019b. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations.* Technical report. Paris: FATF. whttp://www.fatf-gafi.org/.

———. 2019c. *Public Statement on Virtual Assets and Related Providers.*

Fleder, Michael, Michael S. Kester, and Sudeep Pillai. 2015. "Bitcoin Transaction Graph Analysis" (February). arXiv: 1502.01657.

Fradera, Francesc. 2018. "Conference Report on 'Digital Revolution: Data Protection, Artificial Intelligence, Smart Products, BlockchainTechnology and Virtual Currencies. Challenges for Law in Practice'." *European Review of Private Law* 26 (5): 707–712.

Girasa, Rosario. 2018. *Regulation of Cryptocurrencies and Blockchain Technologies.* Palgrave Macmillan. doi:10.1007/978-3-319-78509-7.

Giuliano, Massimo. 2018. "La Blockchain e gli Smart Contracts nell'Innovazione del Diritto nel Terzo Millennio." *Il diritto dell'informazione e dell'informatica* 34 (6): 989–1039.

Hacker, Philipp, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich. 2019. "Regulating Blockchain: Techno-Social and Legal Challenges – An Introduction." *Regulating Blockchain. Techno-Social and Legal Challenges.* https://papers.ssrn.com/.

Hofert, Eduard. 2019. "Regulating Virtual Currencies: Shortcomings of the EU Framework." *Computer Law Review International* 20 (1). doi:10.9785/cri-2019-200103.

Horizon Scanning. 2017. *Blockchain: the Legal Implications of Distributed Systems.* Technical report 3. doi:10.1108/17506200710779521.

Houben, Robby, and Alexander Snyers. 2018. *Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion.* Technical report July. European Parliament. https://www.europarl.europa.eu/.

Lischke, Matthias, and Benjamin Fabian. 2016. "Analyzing the bitcoin network: The First Four Years." *Future Internet* 8 (1). doi:10.3390/fi8010007.

Lopp, Jameson. 2018. *How Will Facebook's Libra "Blockchain" Really Work?* https://medium.com/.

Maupin, Julie A. 2017. *Mapping the Global Legal Landscape of Blockchain Technologies.* Technical report October. CIGI. https://www.cigionline.org/.

Möslein, Florian. 2018. "Conflicts of Laws and Codes: Defining the Boundaries of Digital Jurisdictions." *SSRN Electronic Journal,* no. May. doi:10.2139/ssrn.3174823.

Neudecker, Till, and Hannes Hartenstein. 2017. "Could network information facilitate address clustering in bitcoin?" *Lecture Notes in Computer Science* 10323 LNCS:155–169. doi:10.1007/978-3-319-70278-0_9.

Ober, Micha, Stefan Katzenbeisser, and Kay Hamacher. 2013. "Structure and anonymity of the bitcoin transaction graph." *Future Internet* 5 (2): 237–250. doi:10.3390/fi5020237.

Paesano, Federico. 2019. *Working Paper 28 Regulating cryptocurrencies: challenges & considerations.* Technical report. Basel Institute on Governance. https://www.baselgovernance.org/.

Perugini, Maria Letizia, and Marco Carlo Spada. 2018. *Distributed Ledger Technologies e Sistemi di Blockchain.* Diritto Dell'Informatica E Delle Nuove Tecnologie, Key Editore.

Rahmatian, Andreas. 2019. "Electronic money and cryptocurrencies (Bitcoin): Suggestions for definitions." *Journal of International Banking Law and Regulation* 34 (2): 115–121.

Reid, Fergal, and Martin Harrigan. 2013. "An Analysis of Anonymity in the Bitcoin System." In *Security and Privacy in Social Networks.*

Sarfraz, Umair, Masoom Alam, Sherali Zeadally, and Abid Khan. 2019. "Privacy aware IOTA ledger: Decentralized mixing and unlinkable IOTA transactions." *Computer Networks* 148 (January): 361–372. doi:10.1016/j.comnet.2018.11.019.

Sarzana di S.Ippolito, Fulvio, and Massimiliano Nicotra. 2018. *Diritto della Block-chain, Intelligenza Artificiale e IoT.* Ipsoa.

Sotiropoulou, Anastasia, and Stéphanie Ligot. 2019. "Legal Challenges of Cryptocurrencies: Isn't It Time to Regulate the Intermediaries?" *European Company and Financial Law Review* 16 (5): 652–676.

Sun, Yi, and Yan Zhang Yi. 2018a. *Privacy in Cryptocurrencies: An Overview.* https://medium.com/@yi.sun/.

———. 2018b. *Privacy in Cryptocurrencies: Mixing-based Approaches.* https://medium.com/@yi.sun/.

Tennant, Laurence. 2017. "Improving the Anonymity of the IOTA Cryptocurrency": 1–20. https://laurencetennant.com/.

The Cryptocurrency Consultant. 2019. *Crypto Forensics: how the blockchain convicts criminals.* https://medium.com/swlh/.

Wachsman. 2019. *Answering One of Blockchain's Biggest Questions: Anonymity or Pseudonymity?* https://medium.com/@Wachsman/.

Yermack, David. 2017. "Corporate governance and blockchains." *Review of Finance* 21 (1): 7–31. doi:10.1093/rof/rfw074.

Zetzsche, Dirk A, Ross P Buckley, Douglas W Arner, Katharine Kemp, Jessica Chapman, Tsany Ratna Dewi, Paul Friedrich, et al. 2017. "The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain." *University of New South Wales Law Research Series.*

Zhang, Yan, and Yi Sun. 2019. *Privacy in Cryptocurrencies : Zero-Knowledge and zk-SNARKs (1/2).* https://medium.com/@krzhang/.