Check for updates

Received: 24 February 2021 | Accepted: 23 October 2021

DOI: 10.1111/ecno.12195

ORIGINAL ARTICLE

WILEY

Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry?

Giulio Soana[1,2]

[1]Department of Criminal Law and Criminology, KU Leuven University, Leuven, Belgium

[2]Department of Criminal Law, Luiss Guido Carli University, Rome, Italy

Correspondence
Giulio Soana, Department of Criminal Law and Criminology, KU Leuven University, Leuven 00199, Belgium.
Email: gsoana@luiss.it

Abstract

The rise of cryptocurrencies during the last decade has caused growing concerns among national and international regulators. One of the risks identified is that these instruments may constitute an innovative tool for criminals when laundering money. This risk has been confirmed by numerous recent cases which have underlined the criminogenic potential of cryptocurrencies. Through the V antimoney laundering (AML) Directive, the European legislator has first regulated this emerging issue. This legislation extends the AML duties to two players of the cryptocurrencies market: exchangers and wallet providers. This choice, however, does not exploit the opportunities offered by cryptocurrencies and fails to provide a customized regulatory framework. By maintaining a traditional regulatory approach centered on intermediaries it misses the key innovation of blockchain technology: disintermediation. Compared with traditional online money flows, intermediaries are not necessary nor fundamental in the cryptocurrencies environment. Failing to adapt to this reality, the Directive is employing chivalry to fight a trench war. To guarantee the integrity of this market, the policymaker has to abandon the traditional intermediary-centred approach in favor of a strategy that seizes the new opportunities offered by blockchain. This paper advocates for a shift from an individual-centered approach to financial crime control to a transaction-centered one.

This is an open access article under the terms of the Creative Commons Attribution-NonCommercial-NoDerivs License, which permits use and distribution in any medium, provided the original work is properly cited, the use is non-commercial and no modifications or adaptations are made.
© 2021 The Authors. *Economic Notes* published by John Wiley & Sons Ltd.

KEYWORDS
antimoney laundering, blockchain, cryptocurrencies

1 | INTRODUCTION

Roused from the ashes of 2008s financial crisis (Forgang, 2019, p. 4), cryptocurrencies bear the promise of a democratic, egalitarian currency market free from the control of Central Banks and financial institutions (Brown, 2016; Di Vizio, 2018, p. 86). Rooted in the anarcho-libertarian philosophy that characterizes a certain part of online players[1], this innovative form of currency[2] has gained an increasingly central role in the public debate.

Twelve years after its conception there is one certainty: a new phenomenon has affirmed globally. Namely, if in the beginning there was only the bitcoin, now a myriad of cryptocurrencies has developed globally with different success and characteristics. This growth has also encouraged the development of a prosperous ancillary market that offers support services to the cryptocurrencies' functioning: mining farms, wallet providers, and exchangers have grown into remunerative industries[3].

True revolution and reason of cryptocurrency's success is the underlying technology: the blockchain. This technology, when applied to cryptocurrencies, allows users to transact with each other without availing of third parties (peer to peer [P2P]), as banks (Pérez López, 2017; Razzante, 2018, p. 9).

The absence of an intermediary, while ensuring advantages to users, creates problems in terms of control of illicit financial flows. Indeed, financial intermediaries are a key element in the prevention and repression of financial crimes (Accorsi et al., 2015, p. 4); as, through a system of diffused policing, these intermediaries enable the reduction of the information asymmetry that characterizes these crimes (Accorsi et al., 2015, pp. 2–3).

Cryptocurrencies bypass this system enabling users to send money directly from their wallet to their receiver's, in a fashion similar to cash adding the advantages related to their immateriality.

Subject of special attention has been the possibility that cryptocurrencies may be used as an innovative tool to launder money (Cryptoassets Taskforce, 2018; European Banking Authority, 2019; Europol, 2018). This is a crime that has caused an increasing alarm between the regulators: both for its distortive effects on the legal market, and as a crucial phase in the remuneration of crime (Accorsi et al., 2015, p. 1; Mabunda, 2018, p. 2); this alarm has led to growing attention and stringent regulations.

Currently, money laundering is developing along three directives: globalization, dematerialization, and anonymization of transactions. Cryptocurrencies offer transactions that perfectly match these trends[4]. In particular, compared with traditional online payment services, cryptocurrencies guarantee a higher level of anonymity, both in terms of absence of intermediaries and parties' identity (Barone & Masciandaro, 2019, p. 9; Carlisle, 2017, pp. 9–11).

On the other hand, blockchain offers interesting opportunities in terms of traceability and transparency (Möser et al., 2013, p. 1; Paesano, 2019). Indeed, this technology is based on a public ledger, formed by unmodifiable consequential blocks, where each transaction ever performed is registered (Jakubenko Goriacheva, Pogodina, & Silnov, 2018). The storage of this ledger is not entrusted to a central entity but to the whole users' community: this means that anyone can access a copy of all the transactions pursued within the system (De Vido, 2019). Even though the parties of the single transactions are only recorded through an alphanumeric code—the public key—once

[1]So-called cypherpunk Carlisle (2017, p. 1); on this movement see also Dyntu and Dykyi (2019, p. 77).
[2]Even though its characterization as a currency constitutes matter of debate. The European Central Bank has adopted the definition of crypto-asset.
[3]Zohar (2015, p. 21), for an analysis of the crypto market see Blandine et al. (2020, p. 17).
[4]As affirmed by Carlisle (2017, p. V) "they offer rapid international transaction settlement and a greater degree of anonymity around users' identities than many other established electronic payment methods; and they do so without involving banks or other powerful intermediaries in payment processing. A payment method that affords secrecy, operates outside the established financial system and facilitates speedy international payments provides obvious attractions to global criminals."

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

a user is associated with a specific key it is possible to rebuild the entire money trail[5]. This characteristic may greatly facilitate financial investigation on transnational entities, overcoming problems related to banking secrecy and legal systems' differences.

These characteristics of cryptocurrencies have not passed unnoticed. After a 2014 report by the FATF launched a wake-up call (Financial Action Task Force, 2019), an array of other authorities have issued reports where they highlighted the risks related to cryptocurrencies, causing various regulatory responses.

At the Union level, the European Union has recently introduced the directive 2018/843 (V Anti Money Laundering Directive)—amending the previous directive 2015/849—including cryptocurrencies in the pre-existing AML framework; the Directive extends the AML compliance duties to two players of the cryptocurrency market: exchangers and custodial wallet providers.

2 | THE V ANTI MONEY LAUNDERING DIRECTIVE: *RATIO* AND PURPOSES

The V Directive extends the AML compliance duties to two players of the cryptocurrency market: exchangers and custodial wallet providers. Both of these players are, therefore, deemed wardens of this new market: they will have to identify and monitor their users so to break that pseudonymity which menaces the efficient prosecution of crimes. While the choice of including wallet providers is a novelty introduced by the European legislator, the regulation of the exchangers is a "classic" of the sectorial policy (De Vido, 2019).

The *ratio* of this focus towards the exchangers is their supposed function of bottleneck between the traditional and the crypto market (Di Vizio, 2018, p. 87; Meiklejohn et al., 2016, p. 91). The underlying idea of this regulatory approach is that the crypto market does not have an autonomous existence separated from that of fiat currencies, and that, therefore, the cryptocurrencies market simply represents a stage of the *iter criminis*. If this assumption is correct, sooner or later the criminal will need to convert his cryptocurrencies in euro or vice versa, and in that moment he will need to use an exchanger. If the exchanger is subject to the AML compliance duties, the incoming or outcoming transaction will be identified and from there, through the blockchain ledger, it will be possible to rebuild the whole money trail.

Through this approach, the legislator does not act directly on the crypto market, rather it fences the market and tries to avoid that its malign results can spill over and pollute the traditional market.

It is as if, when faced with a high-crime area, the policymaker, rather than acting in the area by augmenting police presence, simply builds a wall around it and puts soldiers at the gates to avoid that criminals enter or exit.

This approach is questionable not only from a criminal policy standpoint it is also of arguable efficacy: indeed, as maintained in the following chapters, the representation of the exchangers as a bottleneck between the crypto and the traditional markets is debatable.

When it comes to the wallet providers the choice is probably due to their structural similarity with banks. Also in this case the equation is quite frail or at least it is in modern terms: wallet providers offer a service similar to the one offered by banks when it comes to cash and not to online transactions[6]. Namely, the user, who does not want to guard his savings under the mattress (e.g., in an online or offline private wallet) for reasons of safety or convenience, can use these services. These are, therefore, non-necessary players of the cryptocurrencies market, differently from banks when it comes to online transactions.

[5]As stated by forensic expert Meiklejohn "If you catch a dealer with drugs and cash on the street, you've caught them committing one crime but if you catch people using something like Silk Road, you've uncovered their whole criminal history (…) it's like discovering their books", see Bohannon (2016).
[6]Carlisle (2017, p. 24), Wallet providers activity "appear similar to deposit taking. However, this is not generally an accurate characterization (…) The digital currency is simply stored in the customer's name in a secure facility usually on-premises, rather like a digital safety deposit box … safekeeping digital currency credentials is something new that falls between traditional custodial key escrow services and fiduciary trust services."

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Notwithstanding these weaknesses, the choice of the European legislator to provide a framework on the matter is for sure commendable.

In primis, as it delivers a first definition of cryptocurrencies and of the players that operate in this market. The lack of defined and stable terminology is a crucial problem in this ambit and has a detrimental effect in terms of communication and progress. Having a stable definition in the European legislation is an element of efficiency and clarity both in terms of regulatory and doctrinal debate.

In secundis, as it sends a precise signal to the Member States and the players both of the crypto and the traditional market: cryptocurrencies are a theme of the European agenda and their regulation is indispensable. This is of particular importance as cryptocurrencies do not only constitute a risk factor but are also an opportunity in terms of economic growth. It is, therefore, necessary to safeguard and guarantee their controlled evolution; a situation of complete deregulation bears the risk that these currencies are absorbed by the criminal market, scaring investors and users, eventually hampering their development[7]. Careful regulation is, therefore, necessary De Vido (2019).

In tertiis, as, in this area, a national approach is insufficient. Dealing with a completely decentralized and dematerialized market, the possibility for service providers to migrate towards more complacent jurisdictions is apparent (Pérez López, 2019, p. 168). An approach the more territorially extended possible is necessary to avoid grey areas and exercise an influence that can actively modify the decision-making process of the players involved (Carlisle, 2017, p. 28). Acting at a national level, especially for States territorially small as the European ones, risks to yeald limited results. In this sense the European Union, even though its dimension is still limited compared to the global landscape, can assert a territorial and economic influence comparable with that of other international players, as the United States and China.

3 | THE DEFINITION OF CRYPTOCURRENCIES

Defining cryptocurrencies is anything but an easy task. This is a relatively young market that is experiencing a dizzying development: suffice it to say that, as of this writing, more than 6000 types of cryptocurrencies exist[8], and each one of those has different features and aims. Also the power relations in the market are extremely flexible: the bitcoin, which in 27 represented nearly 90% of the market (Carlisle, 2017), saw its share declining to 54% in just 2 years (European Central Bank, 2019), making any hypothesis regarding a "standard model," stable over time, quite frail. Finally, cryptocurrencies' characteristics are technology-specific; this means that their core features are mainly rooted in the limits and potentials of the underlying technology. Therefore, as technology advances and increasingly surpasses these limits, also the characteristics of cryptocurrencies are bound to consequently evolve.

Providing a stable definition in this situation is a complex exercise as the risk is, on one hand, to deliver a definition too narrow and to leave blind spots; on the other hand, to establish a definition so broad that would make cryptocurrencies a "black box" of heterogeneous instruments.

This has caused relevant terminological confusion. Scanning through the reports of international authorities the terms used include virtual asset, crypto asset, cryptocurrencies, e-money, and digital currencies. The main problem of this variety is the consequent difficulty in understanding if these terms all refer to the same phenomenon or different variants of it (Houben & Snyers, 2018, pp. 20–23).

Art. 1.2.d of the Directive steps in this semantic dispute choosing the term "virtual currencies," refusing, therefore, the definition of "virtual asset." This is an interesting choice, as it highlights how the EU legislator

[7]See Möser et al. (2013), who explain how the development of the first ATMs in the '30s was hampered by the fact that these machines were mainly used by those individuals who did not want to face the cashier, as prostitutes and pimps.

[8]While this number is difficult to calculate also as it changes fast see the data provided by https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

considers these instruments as genuine currencies which have, therefore, the potential of being used in a way similar to fiat currencies.

Moving to the content of the definition, virtual currencies are "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"[9].

The core features of cryptocurrencies are, according to this definition.

First, absence of a public issuer and only potential relation with a fiat currency. The subjective characteristics of the issuer are, therefore, not positively defined; this leaves room to a wide pool of private issuers; as well as the possibility to encompass, in the scope of this policy, both centralized currencies - meaning those issued and managed by a central authority[10]—and decentralized ones—rooted in algorithmic regulation and consensus[11].

Second, general medium of exchange. The Directive requires that cryptocurrencies are apt to carry out the primordial function of currencies[12]. Even though the function of medium of exchange plays a crucial role when it comes to traditional currencies, at the moment cryptocurrencies witness a pre-eminence in the investment and speculative function Pérez López (2017, p. 26); mainly due to their limited acceptance as a retail means of payment and to their price volatility (Hileman & Rauchs, 2017, p. 2).

Where cryptocurrencies play a fundamental function of means of exchange is in the criminal market (HM Treasury, 2017, p. 40; Vandezande, 2017, p. 343). Cryptocurrencies, in particular Bitcoin, not only are the predilect means of payment in the dark web (Barone & Masciandaro, 2019, p. 235) they are also the elective means of remuneration when it comes to cybercrime[13].

Third, the possibility to transfer, store, and trade. This last part of the definition is aimed at excluding from the ambit of the Directive any asset that has a function of mere investment[14]. From this last section of the definition, it is possible to imply that, according to the EU legislator, cryptocurrencies are essentially currencies and that the means of exchange function is a characteristic that, even if not necessarily prevalent, has to always be present.

Analyzing the definition proposed by the Directive, it is easy to understand how this is extremely wide as it encompasses a broad range of virtual currencies that have different features and functions. Even if the *ratio* is probably avoiding the early obsolescence of the policy, it has to be underlined that there are some structural differences between virtual currencies that have a direct influence in terms of regulation that should have been considered by the Directive.

Among all, two aspects can be mentioned that should have been certainly taken into account by the European policymaker.

First, the above-mentioned difference between centralized and decentralized currencies. Indeed, in centralized virtual currencies, the presence of a governing body that controls the currency allows the regulation of the latter—for example, by imposing on it AML/CFT duties. This is not a viable option when it comes to decentralized currencies, as the lack of an identified governance body and the shifting power relations impairs the possibility of identifying a regulatory point of pressure.

[9]Both the choice of the term virtual-currencies and its definition are in line with the definition proposed by Financial Action Task Force (2014).

[10]See as an example Liberty Reserve as described in Trautman (2014).

[11]The latter are usually defined cryptocurrencies see De Vido (2019, p. 61), that defines them as "open-source, math-based peer-to-peer virtual currencies that have no central administrating authority, and no central monitoring or oversight". For a definition of the two types of currencies see Financial Action Task Force (2014, p. 5).

[12]In line with the interpretation of Haffke et al. (2019, p. 8) "only tokens that are accepted by natural and legal persons as an intermediary asset in trade without their traders' own interest in their use or consumption are virtual currencies within the meaning of AMLD5."

[13]Europol (2018, p. 16, 2020, p. 17), "Reliability, irreversibility of transactions and a perceived degree of anonymity have made cryptocurrencies the default payment method for victim-to-criminal payments in ransomware and other extortion schemes, as well as criminal-to-criminal payments on the Darkweb."

[14]For a differentiation see European Banking Authority (2019, 7).

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Second, the different structure of the transactions: the insidiousness of currencies that use a P2P system cannot be equated with that of currencies that employ an intermediated transaction strategy. Namely, the latter permits the perpetuation of the intermediary-centered policy model; contrarily, P2P currencies circumvent intermediaries and, therefore, call for a policy approach that does not simply rely on them.

The sensation is, therefore, that to prevent blind spots, the Directive has assimilated extremely different instruments. It would have probably been better to provide for customized policies for each instrument, so as to better exploit the specific features and mitigate the specific risks.

4 | THE SUBJECTS OF THE V DIRECTIVE: EXCHANGERS AND WALLET PROVIDERS. BETWEEN ADVANTAGES AND BLIND SPOTS

The principal subjects of the extension operated by the V Directive are the exchangers.

These are defined as "providers engaged in exchange services between virtual currencies and fiat currencies". Regardless of the opportunity of this extension, two definitory matters need to be addressed.

In primis, this legislation only encompasses the exchanger services between crypto and fiat currencies. Therefore, the exchangers that only provide crypto-to-crypto conversions are out of the scope of this legislation. This choice is in line with the abovementioned "fencing" approach that adopts a laissez faire attitude towards the functioning of the crypto market per se. Notwithstanding this teleologic coherence, this choice seems inefficient. Indeed, on one hand, this choice stems from the idea that cryptocurrencies will never constitute an autonomous market; if this is currently correct, given the limited acceptance of cryptocurrencies by traditional sellers, this is not a given for the future. On the other hand, the crypto-to-crypto exchange activity already constitutes a risk factor in terms of money laundering[15]; indeed, by exchanging a sum into different cryptocurrencies it is possible to drastically reduce the traceability of the transactions. This behavior, known as "chain hopping", is extremely effective, as it allows to pass the transactions through different blockchains, that usually have different characteristics (Forgang, 2019, p. 12). The exclusion of this type of exchangers constitutes, therefore, a relevant blind spot of the Directive.

In secundis, the Directive only mentions those entities that provide exchange services. However, the market of the exchangers is extremely varied when it comes to cryptocurrencies: together with services that directly carry out exchange activities—so-called centralized exchangers—there are services that simply enable the matching of supply and demand—so-called decentralized exchangers (Hileman, & Rauchs, 2017, p. 34). The latter are usually structured as online bulletin boards where individuals that want to sell or buy cryptocurrencies post a message and then carry out the transaction privately; even though some of these websites do charge a commission this is not the rule. Some commentators believe decentralized exchangers can be included within the scope of the Directive through an extensive interpretation (Haffke et al., 2019, p. 10). However, this extension is not automatic, especially when such platforms perform this bulletin board activity not only for cryptocurrencies but for a wide array of goods. It is also questionable whether it is correct to burden such basilar services with demanding duties as those provided by the anti-money laundering legislation.

The other main category targeted by the extension operated by the Directive is that of the custodian wallet providers. These are defined by art. 1.2.d, as "entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies".

Leaving aside the opportunity of the extension operated by the Directive, this definition bears a relevant flaw: only a part of wallet providers safeguards the private keys of their users, whereas many others simply provide for instruments to safeguard the key without actually storing it[16]. The law could, therefore, provoke a migration of the

[15]European Banking Authority (2019, p. 21); see also Yousaf et al. (2019, pp. 837–850).

[16]Of the sample analyzed by Hileman and Rauchs (2017), only 27% of the wallet providers managed the private keys of the users.

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

wallet providers towards the noncustodial option. Indeed, it would be enough for a platform, instead of memorizing the private key, to require the user to insert it manually at each access to avoid the onerous duties imposed by the antimoney laundering legislation. On the other hand, a user who would like to avoid such identification duties could simply choose a noncustodial wallet provider (Haffke et al., 2019, p. 11). Having to type a password at each access, even if a complex one—as is the case with cryptocurrencies—does not seem to be an excessive effort if compared with the stringent identification requirements provided by the AML legislation, especially for a clientele looking for privacy. Also this formulation seems, therefore, to suffer a relevant blind spot.

5 | EXCHANGERS, WALLET PROVIDERS, AND FINANCIAL INSTITUTIONS A HASTY EQUATION?

From the point of view of the AML compliance duties, the Directive does not prescribe any customized duty for the newly regulated entities: exchangers and wallet providers are subject to the same obligations in terms of identification and reporting as traditional financial institutions.

To better understand the problems related to this choice of the obliged entities by the European Legislator, it is appropriate to do a premise on the analyzed technology. Even though the definition of virtual currencies, as provided by the Directive, encompasses a wide array of instruments, when it comes to money laundering one of the hottest topics is related to those currencies that use blockchain technology, enabling users to carry out P2P transactions[17]. *Punctum dolens*, as above mentioned, of these instruments is the possibility for users to transact without availing of intermediaries that act as a filter (Brown, 2016, p. 328), as Banks or other financial institutions. It is, therefore, coessential to the system that any intermediary is only eventual: this is true for the exchangers and even more for the wallet providers. If this was not to be true, the main innovation introduced by cryptocurrencies would be denied, namely the liberation of the users from the tyranny of the intermediaries.

Consequently nor the exchanger nor the wallet providers, even though to a different extent, are forced checkpoints for the users of the cryptocurrency market and can be compared to Financial Institutions in traditional online transactions.

Exchangers undoubtedly play a fundamental role in intermediating the crypto and traditional market (Meiklejohn et al., 2016, p. 91). As underlined by recent investigations[18], criminals frequently use these services as a way in the cryptocurrency market, and their collaboration has proven vital in several criminal investigations. However, there will always be the possibility, for sufficiently motivated users to directly access the crypto market, by dealing with individuals willing to sell cryptocurrencies (Pérez López, 2017, p. 27). These kind of transactions are more laborious than simply using an exchanger service, especially when purchasing large sums; however, this laboriousness does not imply an impossibility. Another element that has to be taken into account is the globality and immateriality of the crypto market, which entails that there will always be the possibility for users to address individuals that operate outside of the European control, in more complacent jurisdictions (Pérez López, 2017, p. 46).

When it comes to the wallet provider, the above-mentioned problem is even more accentuated. A cryptocurrencies wallet can be stored in various forms, with varying levels of convenience and safety (Brown, 2016, p. 331; Hileman & Rauchs, 2017, p. 49), using a custodial wallet provider is just one of the many options available; indeed an individual willing to use cryptocurrencies for illicit purposes could, simply, privately store his key and avoid this way any control.

[17]These are the more diffused currencies as Bitcoin, Ethereum, and Monero.

[18]See between the others the Operaciòn Tulipan Blanca pursued by Europol where the collaboration of a Finnish exchanger has been crucial to identify the suspects. For further information see https://www.europol.europa.eu/newsroom/news/illegal-network-used-cryptocurrencies-and-credit-cards-to-launder-more-eur-8-million-drug-trafficking

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

This is recognized by the Directive itself that at recital nine states "the inclusion of providers engaged in exchange services between virtual currencies and fiat currencies and custodian wallet providers will not entirely address the issue of anonymity attached to virtual currency transactions, as a large part of the virtual currency environment will remain anonymous because users can also transact without such providers."

A further difficulty is given by the temporariness of the measures adopted. The system examined, especially when it comes to the regulation of the exchanger, is rooted in the assumption that the crypto market is dependent on the fiat currency market. However, this assumption remains valid as long as the possibility to use cryptocurrencies as a retail means of payment is limited (Accorsi et al., 2015, p. 8); even though this assumption is presently valid, the situation may well change soon (Carlisle, 2017, p. 14).

Indeed, cryptocurrencies aim at replacing or at least at supplementing fiat currencies; to reach this goal cryptocurrencies must become a widely accepted means of payment. If this was to happen, the whole framework of the Directive would lose its function. Namely, a criminal that was to obtain the proceeds of his activity in cryptocurrencies, could then directly reinvest them without having to pass by any of the checkpoints put in place by the Directive. This risk is even more acute given the current absence of duties of identification for crypto-to-crypto exchangers.

Notwithstanding the abovementioned problems, the Directive performs an important policing function: on one hand, it sends a clear message to those that are, at the moment, the most important actors of the cryptocurrency market. On the other hand, it promotes a capacity-building effort in this industry when it comes to money laundering prevention. To enable the healthy growth of cryptocurrencies, it is fundamental for them to shake off the criminal label to which they are usually associated in the public discourse. To obtain that, a normalization of the actors involved in this market through their classification in the legislative framework is for sure an obliged passage.

6 | THE IDENTIFICATION AND REPORTING REQUIREMENTS: CRITICAL ASPECTS AND NEW OPPORTUNITIES

The perception, when analyzing the content of the Directive, is that the legislator is using the cavalry to fight a trench war.

Cryptocurrencies, notwithstanding the semantic similarity with fiat currencies, are an essentially different instrument from these: new challenges require new answers (Carlisle, 2017, p. 29).

To this end, part of the literature is proposing a change of approach to tackle this issue. Following the old motto "when life gives you lemons, make lemonade," it is proposed to shift the regulatory focus from the users to the transactions.[19] Indeed, if cryptocurrencies only guarantee an imperfect knowledge of users' identity, on the other hand, they guarantee a perfect knowledge of the transaction ledger. When a suspicious transaction is identified, it will be possible to follow the money wherever it goes (Zohar, 2015, p. 111): it would be conceivable, this way, to frustrate the possibility for the criminal to achieve any form of profit by using cryptocurrencies.

From this perspective there are three possible directives along which the legislation in this sphere could be developed.

First, transaction analysis. Blockchain technology provides a precious instrument to investigators and supervisors: a public ledger where all the transactions ever carried out with a specific currency are registered. Even though this ledger does not bear the names of the users the information present is still useful (Bohannon, 2016, p. 1145). As underlined by part of the literature, criminal transactions do follow specific pathways (Berggren & Asplund, 2016, 1/44); if this specialty were to be proved, there would be the possibility to codify a software that

[19]"The lesson for cybercrime fighters is: AML in Bitcoin has to deal with imperfect knowledge of identities, but may exploit perfect knowledge of all transactions" Möser et al. (2013, p. 12); Accorsi et al. (2015, p. 12) "could imply a paradigm shift in AML controls, where monitoring of actual transactions gains more relevance compared to ex-ante customer identification procedures"

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

could continuously monitor the ledger looking for suspect transactions or accounts. Once launched, this program would benefit from the possibility of continuously learning from the results obtained, sharpening the knowledge of the pathways[20]. This solution would enable the supervisor to bypass the players of the cryptocurrency market and the financial institutions[21] – as the supervisors would directly access the ledger. Also, this system would create a form of diffused and continuous worldwide police system.

The FAFT itself in its 12-month review on virtual assets (Financial Action Task Force, 2021), published in 2021, underlined the potential of ledger analysis as a tool to prevent money laundering and to fill the regulatory gap with regard to P2P transactions. Stating "it is also important that jurisdictions understand the ML/TF risks and the potential of ledger analysis as a tool to prevent money laundering and to fill the regulatory gap (…) and the potential to use analytic tools to mitigate risks associated with the P2P sector, the extent to which P2P transactions occur in their jurisdiction and potential blockchain native AML/CFT solutions."

Institutionalizing ledger control at a policy level would transition it from an investigative activity to a policy/supervisory measure. The use, functioning, and effects of blockchain crawlers should be directly provided by the AML regulation and act in pair with intermediaries regulation. Such a regulation would have the merit of spelling a policy that harnesses the differences between the fiat and crypto world to ameliorate control. Instead of perpetrating a policy approach—the one based on intermediaries—which is no longer sustainable in a blockchain environment.

Furthermore, policy-mandated measures to guarantee ledger analysis and control are not new in AML/CFT. Namely, in a sense, this measure would translate the requirement spelled by the FATF Recommendation number 10 lett. c to monitor "transactions undertaken throughout the course of that relationship" into the cryptocurrency world. Indeed, while digital transactions of fiat currencies are stored in centralized ledgers held by every single intermediary, cryptocurrencies' transactions are all stored in a common public ledger. Through this policy approach, harnessing the different storage system of blockchain, the transaction monitoring function, required by Recommendation 10, would be implemented directly by the public supervisor—for example, the FIU—on the public ledger in a fashion similar to what intermediaries do with their ledgers.

The second leg of this policy proposal would consist in account banning. This second leg would be aimed at providing an enforcement weapon to the first leg—that is, ledger analysis. Indeed, when it comes to P2P transactions one of the main problems is that there is nearly no way to coercively enforce a decision—as a seizure or freezing order—within a public, permissionless blockchain. Without an intermediary—that is, a custodial wallet provider—to compel, the State has no one to turn to. Therefore, the risk is that transaction analysis alone becomes a blunt weapon: in other words, an alarm system without a corresponding enforcement mechanism.

This is precisely the role account banning could play. Eminently, once a suspect transaction was to be identified by the crawler, it would be necessary to block the cryptocurrencies associated with the latter. What is interesting on this matter is the proposal of recent literature, according to which it would be possible to use with cryptocurrencies a system similar to the one adopted with marked bills (Möser et al., 2013, p. 11). In particular, the proposal is to create a black-list, where all the serial numbers of suspect cryptocurrencies are reported, that would prohibit to the market participants to accept those bills (Carlisle et al., 2017, pp. 30–33). The mechanism of black-listing would constitute a form of *de facto* seizure, which, while not guaranteeing the apprehension of the criminal, would frustrate its activity.

From a legal perspective, this black-listing mechanism may be modeled on the technique used by tax law in the field of presumptions and the corresponding reversal of the burden of proof. When a certain transaction would receive a hit by the crawler, the corresponding coin would be blacklisted. It would then be to the owner of the coins to contact the AML supervisor and give proof of the legitimacy of the transaction. This system would substitute

[20]See the functioning of the software Reactor developed by Chain Analysis; https://www.chainalysis.com/

[21]Which, as demonstrated by recent enquires, is all but obvious.

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

ex-ante identification—under the traditional compliance model—with ex-post one. Such a model would better fit the structure of cryptocurrency by focusing on the information blockchain provides—that is, transaction transparency.

The third leg of this renewed policy approach should be based on controlling the actions aimed at obscuring the transaction ledger. Given the abovementioned regulatory proposal, it is evident how maintaining the publicity of the transactions is a fundamental moment to contrast money laundering through cryptocurrencies. It would, therefore, be appropriate to garrison all those actions that permit to hinder this transparency: think about the crypto-to-crypto exchange activity or to the use of Tumblers[22].

Regarding the use of Tumblers, the latter is for sure the notable absentee of the Directive: these services allow to augment the privacy of the users by obscuring the trail of one or more transactions (Berggren & Asplund, 2016, p. 21). Their use for money laundering purposes is widely demonstrated by recent cases and by several reports. While some ask for their complete ban (Carlisle, 2017, 26), it would have been at least desirable to have a regulation similar to the one provided for wallet providers (Haffke et al. 2019, pp. 12–14). The European policymaker is, however, inexplicably silent on this topic.

Finally, it is worth mentioning the development that the cryptocurrency market is experiencing: bitcoin is giving way to new instruments that aim to perfect its structure (Hileman & Rauchs, 2017). In particular, a field where developers are active is the reduction of the publicity and transparency of the blockchain ledger[23], striking example of this development is Monero, which uses an opaque blockchain (Forgang, 2019, p. 11). Given the importance, in terms of crime identification and repression, of the possibility to access the transaction ledger, it would be appropriate for the policymaker to intervene so that this new generation of cryptocurrencies, while guaranteeing the privacy of the transactions from the control of the *quivis de populo*, still ensures the accessibility to the ledger for public actors.

7 | A NEW DEVELOPMENT: THE VIRTUAL ASSET'S GUIDANCE OF THE FATF

Following the V AML Directive the FATF has adjourned, in 2018, its recommendations and published a new guidance on "virtual assets and virtual asset service providers," in 2019 (Financial Action Task Force, 2019). Through these new policy instruments, the FATF has partially revolutionized the approach adopted in the previous reports and fully embraced by the Directive of 2018.

The crux of this revolution is a significant extension of the obliged entities—the so-called Virtual Asset Service Providers (VASP)—to intra-market players. Namely, following this last recommendation any natural or legal person who conducts as a business one or more of several specified activities[24] or operations for or on behalf of a customer is to be considered a VASP. Tellingly, the recommendation specifies that the "FATF definition includes both virtual-to-virtual and virtual-to-fiat transactions or financial activities or operations".

While the new FATF's recommendations and guidelines provide for further innovative and useful clarification in terms of VASPs duties, risk identification, and management, these are not of central relevance for our analysis which deems to evaluate the overall policy approach to cryptocurrencies financial flows control.

In this perspective, the abovementioned extension certainly represents an evolution of cryptocurrencies regulation. Indeed, it signifies the desertion of the above-criticized fencing approach in favor of a more active role of

[22]These software also known as Mixers enable the user to obscure the connection between two transactions. In particular by filtering and randomly reallocating a group of transaction these software drastically reduce the possibility to associate the incoming transaction with the outgoing one. For an analysis regarding the functioning of these software's and their efficacy see Möser et al. (2013) and Jakubenko Goriacheva et al. (2018, p. 48).
[23]Bohannon (2016, p. 1146). See the Zero proof technology as described by Mari (2016).
[24]These activities are: exchange between one or more forms of virtual assets; Transfer of virtual assets; Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

the regulator within the cryptocurrencies market and not only at its borders. Indeed, by imposing KYC and reporting duties also to intra-market transactions the regulator for the first time recognizes the need of intervening in the market.

While this change of perspective is for sure welcome it is only a partial one and certainly not resolutive as it does not address the crucial difference existing between fiat currencies and cryptocurrencies: disintermediation.

The new FATF guidance simply expands the number of regulated entities, however, it does not purport a new policy approach. The sole focus is still on intermediaries and no attention is paid to the ledger. Increasing the number of regulated entities will not change the fact that cryptocurrencies permit P2P transactions and, therefore, that no intermediary will ever have that function of compulsory bottleneck it has in the fiat market. Trying to adapt the legacy regulatory approach to a new instrument can only yield partial and ultimately unsatisfactory results.

By perpetuating an intermediary-based control the regulator fails to customize the regulation to the technology and forces an extension that is incompatible with the blockchain structure. Such extension symbolizes an erroneous regulatory strategy that does not start from a thorough understanding of the technology around which a regulation is built to harness the opportunity it offers. Rather it is based on a blind adaptation of obsolete regulatory schemes to new, incompatible instruments.

While unsatisfactory, these new guidelines could provide an opportunity for the European policymaker to innovate its regulatory framework in the field of virtual currencies. Namely, for the time being, the applicable legislation within the European Union is still the V AML Directive as the FATF guidelines do not have direct effect in the European Union.

This means that the EU will have to update its regulation in the field of virtual currencies in the short/medium term. Such an update could constitute a good opportunity to propose a change of approach which goes beyond the FATF guidelines. By customizing the regulation to the characteristics of blockchain technology, shifting the focus from the intermediaries towards the ledger, there would not only be a relevant amelioration in the effectiveness of control there would also be an economic effect. Indeed, the expansion of the regulated entities under the FATF guidelines entails that a whole set of nascent players will need to build the capacity to guarantee compliance with the AML legislation. This implies a relevant burden on any new venture in the cryptocurrency market and, therefore, a strong check to the market development.

The European Union, by introducing a legislation that harnesses the opportunities of blockchain's ledger in terms of financial integrity and reduces the pressure on intermediaries could become an attractive market for blockchain ventures. A favorable, while fair, regulation is a key factor for the development of a market. In this sense, the EU could become a global standard-setter in this field while also creating a favorable regulatory environment for cryptocurrencies' related start-ups.

Unfortunately, the EU does not seem inclined to seize this opportunity. Indeed, based on the proposal presented by the Commission on July 2021[25] on a new regulatory package on AML/CFT, the Commission simply aims at adapting to the new FATF guidelines, this way perpetuating this incomplete policy approach.

8 | CONCLUSION

Cryptocurrencies, and the underlying blockchain technology, constitute one of the main innovations of the XXI century. They promise to revolutionize the terms of the fiduciary relationship and the transparency of the currency market.

In the face of such an innovation, the legislator cannot afford to remain on the fence. Especially when it comes to criminal law, the potential of these technologies has to be closely monitored: while avoiding over-regulation that

[25]European Commission, Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, 2021, 5

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

could provoke the fossilization of the market, the policymaker has to act to avoid an unchecked growth that would end up in a far west situation. The cryptocurrency market itself could benefit from these interventions that could help in filling that reputational gap that afflicts these instruments at the moment.

The Directive tries to operate this difficult trade-off by intervening for the first time, at the European level, on the relation existing between money laundering and cryptocurrencies. Even though the intention is correct, the impression is that the legislator could have aimed at more innovative and bespoke solutions: cryptocurrencies are essentially different instruments from the fiat currencies and ask for customized solutions, not for simple extensions of a pre-existing policy.

In a similar fashion, the new FATF guidance, by simply extending the number of obliged entities does not capture the fundamental revolution purported by blockchain: disintermediation. Focusing on intermediaries when regulating a technology that makes of disintermediation its flagship innovation seems a contradictory choice and extending the number of intermediaries will not solve this fundamental underlying problem.

On the contrary, the legislator should start focusing on what blockchain does offer. The relative transparency and accessibility of its ledger and the development of analysis tools call for a new approach to financial integrity regulation. One that shifts the focus from the individual to the transaction. This shift requires extensive reforms of the control system to guarantee the effectiveness of this new policy approach. However, if correctly implemented this new model would reduce the burden on market participants while enhancing controls' effectiveness and tackling the borderless nature of cryptocurrencies.

It is not only up to technologists and scientists to innovate; lawyers and policymakers need to face the new challenges with an open-minded approach that allows them to go beyond the legacy system. The policymaker needs to embrace technological evolution and find creative solutions that are firmly rooted in the understanding of the technology.

ACKNOWLEDGMENTS

Open access funding provided by Libera Universita Internazionale degli Studi Sociali Guido Carli within the CRUI-CARE Agreement.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no data sets were generated or analysed during the current study.

ETHICS STATEMENT

The authors have followed the required ethical standard.

REFERENCES

Accorsi, C., Brening, R., & Müller, G. (2015). Economic analysis of cryptocurrency backed money laundering. In *Twenty-Third European Conference on Information Systems (ECIS)*, pp. 1–18.

Barone, R., & Masciandaro, D. (2019). Cryptocurrency or usury? Crime and alternative money laundering techniques. *European Journal of Law and Economics*, *47*(2), 233–254.

Berggren, C., & Asplund, J. (2016). Identifying and analyzing digital payment flows regarding illegal purposes on the Internet: I samarbete med CGI OCH Finanskoalitionen.

Blandine, A., Pieters, G., Wu, Y., Eisermann, T., Dek, A., Taylor, S., & Njoki, D. (2020). 3rd global cryptoasset benchmarking study, Cambridge Center for Alternative Finance. Retrieved August 19, 2021 from, https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/3rd-global-cryptoasset-benchmarking-study

Bohannon, J. (2016). The bitcoin bust. *Science*, *351*(6278), 1144–1146.

Brown, S. D. (2016). Cryptocurrency and criminality: The bitcoin opportunity. *The Police Journal: Theory, Practice and Principles*, *89*(4), 327–339.

Carlisle, D. (2017) Virtual currencies and financial crime: Challenges and opportunities. Royal United Services Institute for Defence and Security Studies. Retrieved August 19, 2021 from, https://rusi.org/explore-our-research/publications/occasional-papers/virtual-currencies-and-financial-crime-challenges-and-opportunities

Cryptoassets Taskforce. (2018) Final report. Retrieved August 19, 2021 from, https://www.gov.uk/government/publications/cryptoassets-taskforce

De Vido, S. (2019). All that glitters is not gold: The regulation of virtual currencies in the new eu v anti-money laundering directive. *DPCE Online*, *38*(1), 59–76.

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Di Vizio, F. (2018). Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti. *Diritto Penale Contemporaneo*, *10*, 21–81.

Dyntu, V., & Dykyi, O. (2019). Cryptocurrency in the system of money laundering. *Baltic Journal of Economic Studies*, *4*(5), 75–81.

European Banking Authority. (2019). Report on Crypto-Assets. Retrieved August 19, 2021 from, https://www.eba.europa.eu/eba-reports-on-crypto-assets

European Central Bank. (2019). Crypto-assets: Implications for financial stability, monetary policy, and payments and market infrastructures. Retrieved August 19, 2021 from, https://www.ecb.europa.eu › pub › pdf › scpops

Europol. (2018). Internet organised crime threat assessment. Retrieved August 19, 2021 from, https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

Europol. (2020). Internet organised crime threat assessment. Retrieved August 19, 2021 from, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Financial Action Task Force. (2014). Virtual currencies: key definitions and potential AML/CFT risks. Retrieved August 19, 2021 from, http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html

Financial Action Task Force. (2019). Virtual asset and virtual asset service providers: Guidance for a risk-based approach. Retrieved August 19, 2021 from, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

Financial Action Task Force. (2021). Second 12-month review of the eevised FATF Standards on Virtual Assets/VASPs. Retrieved August 19, 2021 from, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/second-12-month-review-virtual-assets-vasps.html

Forgang, G. (2019). Money laundering through cryptocurrencies. *Economic Crime Forensics Capstones 4.0*, 1–25.

Haffke, L., Fromberger, M., & Zimmermann, P. (2019). Cryptocurrencies and anti-money laundering: The shortcomings of the fifth aml directive (EU) and how to address them. *Journal of Banking Regulation*, *21*(2), 125–138.

Hileman, G., & Rauchs, M. (2017). Global cryptocurrency benchmarking study, Cambridge Centre for Alternative Finance. Retrieved August 19, 2021 from, https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-04-20-global-cryptocurrency-benchmarking-study.pdf?ref=hackernoon.com

HM Treasury. (2017) National risk assessment of money laundering and terrorist financing. Retrieved August 19, 2021 from, https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2017

Houben, R., & Snyers, A. (2018). Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion, European Parliament. Retrieved August 19, 2021 from, https://op.europa.eu/en/publication-detail/-/publication/631f847c-b4aa-11e8-99ee-01aa75ed71a1/language-en/format-PDF/source-76403102

Jakubenko Goriacheva, N., Pogodina, O., & Silnov, D. (2018). Anonymization technologies of cryptocurrency transactions as money laundering instrument. *KnE Social Sciences*, *3*(2), 46–53.

Mabunda, S. (2018). Cryptocurrency: The new face of cyber money laundering. international conference on advances in big data computing and data communication systems (icABCD). IEEE, pp. 1–6.

Mari, J. (2016). When blockchain, cryptocurrencies, and Aml Meet. Banking Exchange. https://m.bankingexchange.com/news-feed/item/6547-when-blockchain-cryptocurrencies-and-aml-meet

Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G. M., & Savage, S. (2016). A fistful of bitcoins: Characterizing payments among men with no names. *Communications of the ACM*, *59*(4), 127–140.

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the bitcoin ecosystem. 2013 APWG eCrime Researchers Summit, pp. 1–14.

Paesano, F. (2019). Regulating cryptocurrencies: Challenges & considerations. Basel Institute on Governance. Retrieved August 19, 2021 from, https://baselgovernance.org/publications/working-paper-28-regulating-cryptocurrencies-challenges-and-considerations

Pérez López, X. (2017). Las Criptomonedas: Consideraciones Generales Y Empleo De Las Criptomonedas Como Instrumento De Blanqueo De Capitales En La Unión Europea Y En España. *Revista de Derecho Penal y Criminología*, *18*, 141–187.

Pérez López, X. (2019). *Blanqueo De Capitales Y Tic: Marco Jurídico Nacional Y Europeo, Modus Operandi y Cripto*monendas. Editorial Aranzadi.

Razzante, R. (2018). *Bitcoin E Criptovalute, Profili Fiscali, Giuridici E Finanziari*. Santarcangelo in Romagna.

Trautman, L. J. (2014). Virtual currencies; Bitcoin & what now after Liberty Reserve, Silk Road, and Mt. Gox? *Richmond Journal of Law and Technology*, *20*(4), 1–108.

Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. *Computer Law & Security Review*, *33*(3), 341–353.

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License

Yousaf, H., Kappos, G., & Meiklejohn, S. (2019). Tracing transactions across cryptocurrency ledgers. In *28th {USENIX} Security Symposium*, pp. 837–850.

Zohar, A. (2015). Bitcoin: Under the hood. *Communications of the ACM*, *58*(9), 104–113.

How to cite this article: Soana, G. (2022). Regulating cryptocurrencies checkpoints: fighting a trench war with cavalry? *Economic Notes*, 51, e12195. https://doi.org/10.1111/ecno.12195

14680300, 2022, 1, Downloaded from https://onlinelibrary.wiley.com/doi/10.1111/ecno.12195 by Luiss Lib University Degli Stu, Wiley Online Library on [14/03/2024]. See the Terms and Conditions (https://onlinelibrary.wiley.com/terms-and-conditions) on Wiley Online Library for rules of use; OA articles are governed by the applicable Creative Commons License