Legal Technology Transformation

A Practical Assessment

Edited by

Andrea Caligiuri

Editoriale Scientifica

2020

Legal Technology Transformation
A Practical Assessment

Edited by
Andrea Caligiuri

Editoriale Scientifica

2020

Via San Biagio dei Librai, 39 – 80138 Napoli
www.editorialescientifica.com – info@editorialescientifica.com

ISBN 978-88-9391-985-2

Scientific Committee

TABLE OF CONTENTS

PART III
ARTIFICIAL INTELLIGENCE AND SMART CITIES

PART IV
LEGAL RAMIFICATIONS OF BLOCKCHAIN TECHNOLOGY

SECTION I
BLOCKCHAIN AND CRYPTOCURRENCIES

BLOCKCHAIN AND CRIMINAL RISK

ROBERTO ACQUAROLI

SUMMARY: 1. Why criminal law has dealt with blockchain. – 2. Criminal alarm for the use of cryptocurrencies. – 3. Anonymity as a crime? – 4. Conclusions.

1. *Why criminal law has dealt with blockchain*

In the last decade, also criminal law had to deal with the world of virtual currencies, more precisely, cryptocurrencies that exploit the technology and the potentialities offered by Blockchain. Blockchain is a protocol capable of certifying the chronological order of a series of operations, using a single chain of blocks or algorithms in which each subsequent transaction or operation is indelibly and irreversibly linked to the previous operations. In particular, the characteristic of this technology, from which the problematic nature of the "classic" criminal law approach derives, consists in the presence of a linked series of blocks, which record, for each operation, the identity of the payer, the amount transferred and the identity of the beneficiary: "Each block contains information related to transactions carried out consecutively over a period of ten minutes, as well as a reference to the previous block. In this way, the Blockchain provides a complete and updated representation of all the transactions that have taken place since the system was started up to that moment".[1]

Starting from the last decade, a series of decentralized and convertible crypto currencies have been triggered on this technology, among which the most famous is Bitcoin, which represent a sort of realization of an unprecedented perspective, as regards the traditional monetary system. In fact, Bitcoin creates a sort of "financial democracy", characterized by the absence of intermediaries and state control, which would have, as its objective, the creation of an economy and a "totally free market, whose regulation is exclusively delegated to individual participating users of the system".

The same philosophy which animates the creation and dissemination of virtual currencies, therefore, appears to be in contrast with the existing system of order in matters of governance of the currency and financial markets. In fact, it expresses its *raison d'être* "in the equality of conditions among all individuals", which excludes the presence of a *super partes* body that controls its work, in the absence of rules that slow down the deliberately rapid and left to the exclusive decisions of individual actors. It is therefore an economic dimension that theorizes the trust that the individual user places in the other operators of the blockchain, whom we do not know the name, but only the encrypted code. This is a particularly delicate issue with regard to virtual currencies, such as bitcoin, in which "each person holding a bitcoin account is

[1] F. Di Vizio, 'Le cinte daziarie del diritto penale alla prova delle valute virtuali degli internauti' (2018) Diritto penale contemporaneo 21 <https://archiviodpc.dirittopenaleuomo.org/d/6224-le-cinte-daziarie-del-diritto-penale-alla-prova-delle-valute-virtuali-degli-internauti>.

guaranteed total confidentiality about her/his identity, so that the user can preserve both privacy from state control relating to his own person, as well as that relating to the object of her/his own sales”.[2] It should also be noted that, in this regard, it is more appropriate to speak of “pseudo anonymity” since each transaction, which took place in crypto currency, is actually recorded in a sort of digital ledger (distributed ledger) in the public domain, accessible by anyone, from which it is possible to trace part of the operation carried out in the blockchain to the accounts.

The diffusion of crypto currencies could not fail to draw attention to their possible use for illegal purposes, given the purely economic nature of the transactions carried out; and, above all, the connotations that characterize it. In particular, there are three features of the blockchain system that have repeatedly drawn attention to the risk of its use for illegal purposes namely:

a) the anonymity or pseudo anonymity of users of cryptocurrencies;

b) the virtual environment in which crypto currency develops and feeds a very dense series of exchanges: the network, in fact, allows transactions to be carried out in a very short time at an international and transnational level, exploiting, precisely, the possibilities offered by the web, on a par with what happens for any other form of economic and financial relationship of the so-called legal economy;

c) the singular and complex structure of the blockchain, which feeds the suspicion of illegal operations;

d) the absence, or better, the choice to avoid any form of regulation and control by the authority. The feature is considered both as an obstacle to the prevention of economic and financial crime phenomena, connected not only to white-collar crime, but also to organized crime and international terrorism; both as an indication of suspicion of illegal conduct, aimed not only at hiding the movements of money, but rather at the use of virtual money, once converted into real money, in illegal transactions.

2. *Criminal alarm for the use of cryptocurrencies*

Criminal literature has for some time highlighted the risk that cryptocurrency is a suitable, if not privileged, instrument for operations of an illicit nature, especially in relation to money laundering phenomena, attributable to cyberlaundering, i.e. the use of the Internet and new technologies to accomplish the cleaning of dirty money. In this regard, it is emphasized that “the offensive potential of cyberlaundering emerges, in particular, with regard to telematic transactions involving virtual currencies, on the basis of which it is possible to carry out transactions, from one part of the world to the other, at an instant speed, without barriers to entry, in total anonymity and in the absence of control by supervisory institutions”.[3] The author goes on to underline how “cyberspace allows the offender to benefit, in addition to the ‘dematerialization’ of the resources linked to the digital content of money, the dispersion due to the difficulty of identifying the perpetrator, also of a delocalization of the user who, operating on the

[2] L. Sturzo, ‘Bitcoin e riciclaggio 2.0’ (2018) Diritto penale contemporaneo 19 <https://archiviodpc.dirittopenaleuomo.org/d/6006-bitcoin-e-riciclaggio-20>, 20.

[3] F. Pomes, Le valute virtuali e gli ontologici rischi di riciclaggio’ (2018) Diritto penale contemporaneo 159 <http://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_pomes.pdf>, 165.

network, can be present in several IT 'spaces' at the same time".[4] An alarming observation, which, however, highlights not the criminal potential of the blockchain, but the now consolidated new scenario in which the entire economy and global finance moves, with respect to which the internet is an indispensable pillar for survival itself.

However, it is undeniable how, with respect to consolidated IT systems and electronic money, which has long found citizenship in legal economies and related sector disciplines, the spread of cryptocurrencies raises some questions about its actual danger, linked to the structure of IT protocols, and to the same philosophy that is at its origin. In particular, it was asked whether they constitute a new and more insidious risk for the legal economy or whether, they fall within the boundaries already drawn up for the criminal protection of assets and the economy, especially as regards the phenomenon of money laundering, despite the suggestions related to the characteristics of the blockchain.

3. *Bitcoins as a constituent element of money laundering crimes*

The debate on the relationship between bitcoin and money laundering crimes helps to better grasp the risks of a hasty judgment on the alleged danger of the blockchain. In fact, many scholars have highlighted how the operations carried out using bitcoins can be attributed to the constituent elements of the crimes of money laundering (648 *bis* of the Criminal Code) and self-laundering (648 *ter* of the Criminal Code), cases that are not limited to punishing the simple substitution or money laundering of illicit origin, requiring instead a *quid pluris*, that is, in the case of money laundering, that the conduct implemented is capable of hindering the identification of the criminal origin; while in self-laundering, the conduct must be further characterized by an effective, i.e. concrete, suitability to make the identification of the criminal origin more difficult. In this regard, it has been highlighted that "the probability that the Bitcoin system is transformed into a system for cleaning up international illicit proceeds will be directly proportional to the ability it will show to make it difficult to ascertain the origin of that value. Although it is undeniable that the blockchain mechanism represents a valid tool for the traceability of transactions carried out on the network via bitcoin, it is in any case demonstrated how this chain ends up coinciding with a pure mathematical matrix algorithm, not only of complex resolution, but often difficult to trace back to a well-identified natural or legal person", so that "in the case of virtual currencies, the link between the addresses of the transactions and the identity of those who actually control them is not insured". In other words, it would be anonymity to establish the essential characteristic of money laundering crimes, namely the ability to hinder the identification of the criminal origin: the pseudonym, that is the bitcoin account represented by a series of numbers and letters, which, however, once traced by the police it does not allow to go back further, in fact continuing to conceal the real physical identity of the owner of the identified account".[5]

[4] Idem, 166.
[5] Sturzo (n 2), 22.

Therefore, the obstacle does not concern the traceability of virtual money as such, but the identification of the author: this represents, however, an extensive reading of the two criminal cases, in which, instead, the criminal relevance concerns exclusively the methods of implementation of the conduct put in place by the offender. On the other hand, bitcoins are anonymous as banknotes are anonymous, the use of which may possibly constitute an indication of suspicion over their illicit origin, but certainly not a relevant conduct such as money laundering.

Conversely, it seems quite substantiated the concern of those who believe that the purchase of bitcoins with real currencies and the subsequent use of the same through a virtual wallet (so-called e-wallet), connected to the blockchain, which stores all the monetary movements attributable to each wallet, can hide an operation to clean up money of illicit origin. In this case, it would be assumed that the implementation of a replacement conduct, suitable to hinder the traceability of dirty money, which is completed with the subsequent transformation of the virtual value in one's possession into legal tender currency through the subsequent crediting of the sums of money to the current account, once converted, similarly to what happens with normal means of payment. Consider, in this regard, the presentation of a check of illicit origin at an institute of credit, with the consequent replacement of the value represented by the credit security with "clean" money, an operation deemed suitable for supplementing the money laundering conduct. Obviously, it will be necessary to ascertain, in addition to the existence of the conduct, the author's *mens rea*: an assessment that cannot be limited to a presumption, determined by the use of an operational tool – bitcoin, in fact – which has a peculiar operating complexity.

4. *Anonymity as a crime?*

Therefore, anonymity remains as an element around which the criminogenic potential of cryptocurrencies is built. This conclusion, widely shared in the doctrine,[6] does not appear entirely correct. First of all, because it doesn't seem to be true. As noted, "Bitcoins are not anonymous but pseudonyms. This means that each user is connected to a certain nickname, consisting of a long set of numerical digits that make up the address to which a particular wallet is connected. It follows that it is possible to identify the holder of the deposit, starting from the nickname use".[7] Perhaps an optimistic statement, since the pseudonym, that is the bitcoin account represented by a series of numbers and letters, once traced by the police, would not allow, however, to go back further, continuing in fact to conceal the real physical identity of the owner of the identified account.[8] More precisely, "cryptocurrencies guarantee a much higher level of anonymity than ordinary banking transactions, not only because their operating protocol does not require the identification or verification of the real identity of the holders of electronic wallets, but because [...] there are numerous tools

[6] G. P. Accinni, 'Profili di rilevanza penale delle criptovalute (nella riforma della disciplina antiriciclaggio del 2017' (2017) Archivio penale <http://www.archiviopenale.it/profili-di-rilevanza-penale-delle-criptovalute-(nella-riforma-della-disciplina-antiriciclaggio-del-2017)/articoli/15332>, 12.

[7] J. Sicignano, 'L'acquisto di bitcoin con denaro di provenienza illecita' (2020) Archivio penale <http://www.archiviopenale.it/lacquisto-di-bitcoin-con-denaro-di-provenienza-illecita/articoli/24907>, 13.

[8] Sturzo (n 2), 31.

that allow you to maximize the privacy of users and virtual currencies […] which are completely anonymous. The owner of an e-wallet fed with proceeds of illicit activity could therefore well dispose of it in a confidential manner, using the provision for the purchase of goods and services without leaving a trace of his actual personal details. It has also already been shown that the virtual currency system has now reached global scale, so that Bitcoin and other cryptocurrencies are easily used to make transfers at a supranational level, allowing interested parties to transfer large capital in many countries of the world. often lacking any anti-money laundering system”.[9]

Therefore, this is not true anonymity, but rather a failure to identify the real user of the operation. In this regard, it could be observed that, in the world of the real economy, this circumstance occurs in a plurality of cases, all of which can be traced back to traditional forms of transactions and commercial relationships. However, the main objection, relating to the issue of anonymity, is another. The fact that the user is anonymous does not, in itself, determine the integration of money laundering conducts, at least in the forms described by the cases currently provided for in Italian law. A different conclusion can be reached in a perspective exclusively of preventive control, based on the type of perpetrator, rather than on the danger of the conduct, according to the consolidated regulatory framework that animates the entire anti-money laundering discipline, provided for by Legislative Decree No. 231 of 2007, as amended by Legislatives Decrees No. 90 of 2017 and No. 125 of 2019.[10] On the level more strictly related to criminal law, the enhancement of anonymity as a constitutive element of the conduct of re-laundering raises many doubts in relation to Art. 25 of Italian Constitution and seems to be dictated by a strong suggestion exerted by the reference to the need to combat infiltration phenomena of illicit economies in the legal fabric, as well as by the alarm raised in relation to international public order, by the continuous references to the methods of financing terrorism through cryptocurrencies.[11]

In this perspective, the hypothesis on which the alarm for the possible criminal relevance of the conduct is based is that such technologies are even conceived and developed to pursue intrinsically illegal purposes, for the sole fact of being non-compliant with established mechanisms. of exchanges and transactions and, more generally, to the general rules on the tracing of financial transactions. The context in which cryptocurrencies and the blockchain were born and have increased their consent from users is thus distorted. Their original perimeter is entirely internal to the

[9] Accinni (n 5), 20.

[10] Decreto Legislativo 25 maggio 2017, n. 90 – *Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo e recante modifica delle direttive 2005/60/CE e 2006/70/CE e attuazione del regolamento (UE) n. 2015/847 riguardante i dati informativi che accompagnano i trasferimenti di fondi e che abroga il regolamento (CE) n. 1781/2006* <https://www.gazzettaufficiale.it/eli/id/2017/06/19/17G00104/sg>. See C. Ingrao, ‘Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio’ (2019) Diritto penale contemporaneo 148 <https://dpc-rivista-trimestrale.criminaljusticenetwork.eu/pdf/DPC_Riv_Trim_2_2019_ingrao.pdf>; G. P. Accinni, ‘Cybersecurity e criptovalute. Profili di rilevanza penale dopo la quinta direttiva’ (2019) Sistema penale 209 <https://www.sistemapenale.it/it/articolo/cybersecurity-e-criptovalute-rilevanza-penale-dopo-quinta-direttiva>.

[11] Ibid., 149-150.

legal economy, as an expression of a cultural model that does not recognize the need for intermediation and constant control in financial transactions and operations, by credit institutions and public control agencies, in the name of a perhaps questionable and perhaps unrealistic democratization of the global economy, based, according to the approach of the supporters of such a scenario, on trust among operators, rather than on institutional control.[12]

5. *Conclusions*

The value of danger formulated with regard to bitcoins seems, therefore, strongly conditioned by a prejudice of a cultural nature, which pushes to identify the area of criminal risk regardless of the real detrimental suitability of the instrument as such. Above all, the element of anonymity is confused, which in any case affects the figure of the author, or rather his immediate identifiability, with the constitutive elements of the cases of money laundering, which do not include the intentional concealment of the perpetrator of the conduct Illicit: not all obstacle activities are punishable by way of money laundering or self-laundering, but only those that concern exclusively the reconstruction of the illicit origin of the goods or utilities that the subject intends to clean up. On the contrary, in virtual currencies, the only dissimulatory operation concerns the possible holder of the virtual currency, who would be covered by a pseudo anonymity. From a material point of view, the asset does not undergo any camouflage, resulting in perfectly traceable and visible bitcoin transactions.[13]

Therefore, if it is compatible with a criminal system centred on introducing control mechanisms in a preventive function intended to bring out the identity of the virtual user, an analogical interpretation of the types of money laundering provided for in the code system, which punishes the same only because you do not collaborate with the authority in revealing your own identity.

[12] Sturzo (n 2), 20.
[13] Sicignano (n 6), 15.