Money Laundering using Cryptocurrency: The Case of Bitcoin!

By Gaspare Jucan Sicignano *

The bitcoin, one of the most discussed topics in recent years, is a virtual currency with enormous potential and can be used almost immediately with no intervention from financial institutions. It has spread rapidly over the last few years, and all financial and governmental institutions have warned of the risk of its use for money laundering. The paper focuses on this aspect in order to understand if any purchases of bitcoins, using illicit money, can come under the anti-money laundering criminal law.

Keywords: Bitcoin; Money laundering; Italian law; Cryptocurrency.

Introduction

The bitcoin\(^1\) is a virtual, decentralised and partially anonymous currency based on cryptography and peer-to-peer technology\(^2\). With bitcoins it is possible to buy any type of good or service securely and rapidly. Transactions need not be authorised by a central entity; rather, they are validated by all users of the platform. The system is totally secure, since it is practically impossible to hack the protocol\(^3\).

Bitcoin has been much criticised over the last few years; it has quickly become public enemy number one for everything from financing terrorism to drug dealing to money laundering. It has also recently been said that bitcoin would pollute the planet due to the resources required for mining\(^4\).

This paper will attempt to analyse in depth the relationship between the bitcoin and money laundering in Italian law. It will analyse the warnings issued by authorities in various sectors, as well as the opinions expressed in Italian legal literature regarding the possibility of committing money laundering and self-laundering crimes in various operations carried out using virtual currency. Finally, it will compare the accusations levelled against Bitcoin today with those levelled against the Internet in the early 2000s.

---

\(^1\)PhD Researcher in Criminal Law, Faculty of Law, Suor Orsola Benincasa Univerisity, Naples (Italy). Email: gaspare.sicignano@unisob.na.it.

\(^*\) Ph.D. Researcher in criminal law, Faculty of Law, Suor Orsola Benincasa Univerisity, Naples (Italy). Email: gaspare.sicignano@unisob.na.it

\(^1\)By convention, the word “bitcoin”, written in lower case, denotes the virtual currency, while the term "Bitcoin", with the initial capitalised, indicates the protocol, i.e. the technology and network used to generate and transfer money.

\(^2\)Antonopoulos (2017) at 3; Wiseman (2016).

\(^3\)Sicignano (2019).

The Risk of Money Laundering

According to many commentators, the primary risk associated with the use of bitcoins is money laundering.

In the 2013 Report of the Financial Intelligence Unit of Italy (UIF), the Bank of Italy announced that investigations were ongoing regarding the potential risk of money laundering and financing terrorism via Bitcoin. In particular, the Director of the UIF stated that the urgency of further investigations was confirmed by several reports of suspicious anomalous international transactions.

The European Banking Authority (EBA), together with the European Central Bank (ECB) and the European Securities and Markets Authority (ESMA), also emphasised the risks of virtual currencies. According to the head of the Attorney General's office in Rome, Bitcoin does not offer clear traceability and can be a means of laundering money, financing terrorism and the mafias, and trafficking illegal goods. In a bitcoin transaction there is in fact no guarantee of being able to verify the real identities of those involved.

Bitcoin may be used as a tool for criminals, terrorists, financiers, and tax evaders, according to the Financial Action Task Force (FATF), the independent inter-governmental agency that develops and promotes policies aimed at protecting the global financial system against money laundering, financing terrorists, and arms proliferation.

The Italian agencies of the Direzione Investigativa Antimafia (Anti-Mafia Investigation Directorate) and the Guardia di Finanza (the Italian financial police) have also issued warnings on the risks connected with using bitcoins. According to a deputy national anti-mafia prosecutor, the bitcoin is an ingenious invention, “it's just that it is a criminal invention!” The commander of the Technology Fraud Unit of the Guardia di Finanza stated that “money laundering lurks in that code”. According to the Director General of the Bank of Italy: “Bitcoin and cryptocurrencies guarantee absolute anonymity and absolute impermeability, all of which is extraordinarily attractive for those who want to launder money.”

The Crime of Money Laundering in Italian Law.

While financial authorities have warned of the risks of money laundering with bitcoin, opinions expressed in Italian legal scholarship have attempted to offer a solution to the problem by claiming that the various operations carried out using bitcoin can be included without difficulty under Italian law as part of the crimes of money laundering and self-laundering.

---

5 Quarantino (2014).
6 Mincuzzi & Galullo (2017).
7 Stefanini (2018).
8 Bonini (2014).
In Italian law, the crime of money laundering is established by Article 648-bis of the Italian criminal code, which punishes the behaviour of those who, in actions distinct from participation in the predicated offence, “substitute or transfer money, goods, or other property from an intentionally committed crime, or carry out other related operations in order to prevent identifying their criminal origin”. Regarding the purchase of bitcoins with illicitly acquired money, such conduct would come under one of the three factual models of Article 648-bis of the Italian criminal code (i.e., substitution, transfer, or carrying out other activities). Under a provision making concealment behaviour regarding money, goods, or other property unlawful, Bitcoin may come under the first or the third of such typological models.\textsuperscript{11}

Purchasing bitcoins using illicitly obtained money would also constitute another element of the crime referred to in Article 648-bis of the Italian criminal code, namely, the suitability of the behaviour to obstruct identifying the criminal origin of the goods.

From this perspective it has been stated that: “the probability that Bitcoin will become a system for laundring international illicit proceeds will be directly proportional to its ability to hinder identification of their origin. While it is undeniable that the blockchain mechanism is a valid tool for tracking online transactions carried out using Bitcoin, it has nevertheless been shown that this chain ultimately corresponds to a purely mathematical algorithm that is not only complex to resolve but frequently difficult to trace back to a clearly identifiable physical or legal person.”\textsuperscript{12}

Thus, it would be “misleading to argue that the a posteriori ability to reconstruct transactions and their digital agents is an absolute impediment to constituting it as a money laundering crime; in the case of virtual currencies, what is indeed not ensured is the link between the transaction addresses and the identity of those who actually control them, thus the possibility is highly developed that the transfer and the substitutions complicate identifying the criminal origins.”\textsuperscript{13}

In the case at hand, “it is able to ‘obstruct’ the identification of the origins, be they objective or subjective, of currency and ‘assets’, without the need for absolute impossibility, or there being a definitory constraint with regard to the physical nature of the subject matter of the conduct itself, which extends far beyond the traditional sphere of ‘money’ or currencies as they are traditionally understood.”\textsuperscript{14}

It would thus be “purely a diversionary tactic” to object that, in reality, Bitcoin is not anonymous but pseudo-anonymous, because “the ‘pseudonym’, or the Bitcoin account represented by a series of numbers and letters, once traced by law enforcement, does not allow any further tracing, and thus it continues to conceal the true physical identity of the identified account’s owner. Furthermore, as if that were not enough, a single physical person can actually own multiple

\textsuperscript{11}Pomes (2019) at 160; Di Fizio (2018) at 58.

\textsuperscript{12}Sturzo (2018) at 22.

\textsuperscript{13}Di Fizio (2018) at 58.

\textsuperscript{14}Picotti (2018) at 608.
accounts and make multiple illicit transactions, each one traceable to a different account.\textsuperscript{15}

Our Opinion on the Risk of Money Laundering.

There are various reasons why we are in disagreement with the considerations outlined above.

Above all, an attentive reading of the various warnings issued by the authorities in various sectors is sufficient to understand that, in many of them, either they are openly ignoring the historical and cultural context in which Bitcoin was created, or they are wildly confusing the actual characteristics of this new computer technology.

It is profoundly wrong to argue that the bitcoin was a criminal invention. Bitcoin was not created by criminals, traffickers, and/or drug dealers. It emerged from a community of computer activists called Cypherpunks who had been working on a digital money project since the 1990s. They were computer experts strongly committed to ensuring privacy; some had university experience while others were already very wealthy, thanks to the Internet. For them, anonymity was not a gimmick to escape control by police authorities but a way of countering the tyranny of surveillance.

At the same time, claiming that bitcoin does not offer clarity in tracking exchanges is to deny the way the entire system operates. All bitcoin transactions are public and are contained in a freely available distributed database. Anyone can check who sold a certain amount of bitcoins to someone else, and anyone can discover the history of every transaction. It is not particularly difficulty to check which wallet contains a certain bitcoin or the route a given amount followed to arrive at a particular destination.

The same alleged anonymity that Bitcoin guarantees to its users, which so frightens the authorities in various sectors, is more legend than fact. Bitcoin is not anonymous; it is pseudo-anonymous. This means that each user is linked to a given nickname, or pseudonym, constituted by a long string of numbers that make up the address linked to a certain wallet. It follows that it is possible to identify the originator of a given operation once the pseudonym used is known.

Numerous studies have worked out various techniques to discover the users concealed behind bitcoin addresses. Suffice it to mention BitIodine, an application created by three Italian scholars, which is capable of identifying the \textit{“addresses in clusters that could belong to the same user or group of users, classifying such users and their nicknames, and even displaying complex data extracted from the Bitcoin network”}. Work presented by a team at the University of California produced similar results.\textsuperscript{17}

Recently, a study by AgiproNews in collaboration with the Politecnic University of Milan showed that using Bitcoin for illicit purposes is even riskier

\textsuperscript{15}Sturzo (2018) at 31.
\textsuperscript{16}Spagnuolo, Maggi & Zanero (2014) at 457.
\textsuperscript{17}Meiklejohn, Pomarole, Jordan, Levchenko, McCoy, Voelker & Savage (2013).
than using electronic money or bank transfers. In particular, it emphasised that the
bitcoin is one of the more traceable currencies, and that every transaction, whether
licit or illicit, is always viewable at zero cost\(^\text{18}\).

The study cited a 2015 report published by HM Treasury and the UK Home
Office, according to which the riskiness of cryptocurrencies for money laundering
and financing terrorism was evaluated as \textit{“low.”}

The same conclusion was reached in a report issued by Elliptic, a company
that works with the risks of cryptocurrencies, and by the Centre on Sanctions and
Illicit Financing, a programme by the Foundation for Defense of Democracies
(FDD), a non-profit entity focused on foreign policies and national security. The
study, which was an in-depth analysis of a narrow sample of transactions between
2013 and 2016, analysed the trends of illicit activities carried out using Bitcoin\(^\text{19}\).
Yet, according to those same experts, the number of illicit operations committed
using Bitcoin is quite low: around 1\% of all transactions that enter the Bitcoin
network.

The report takes advantage of several computer techniques that make it
possible to identify suspicious bitcoin movements that involve Bitcoin forensics
and Bitcoin intelligence. The former refers to \textit{“the use of statistical tools for
aggregating transactions and identifying the users”}\(^\text{20}\), the second refers to
monitoring the blockchain in order to identify \textit{“addresses at risk for money
laundering”} and \textit{“to provide a probabilistic estimate of the risk of each specific
transaction”}\(^\text{21}\).

Recently, many companies have specialised in this area, including providing
consulting services to law enforcement agencies. The best known among them is
Neutrino s.r.l., an Italian company that evaluates the risk of money laundering of
each specific bitcoin transaction. The Blockchain Intelligence Group in Vancouver
is also well known, which does the same analyses as Neutrino S.r.l.\(^\text{22}\).

Thus, it does not seem like a gamble to argue that large criminal organisations
still prefer dollars to Bitcoin. This is also because the bitcoin \textit{“does not have market
liquidity”} and thus could not be easily used for money laundering purposes\(^\text{23}\).

\textbf{Our Opinion on Money Laundering in Italian Law}

The observations stated in Italian legal doctrine regarding the possibility of
establishing the crime of money laundering do not seem convincing either.
While agreeing with the choice to classify the bitcoin as a form of \textit{“other
asset”}\(^\text{24}\), we do not agree with the stated reasoning with regard to the other

\(^{18}\)Tripoldi (2017).
\(^{19}\)Fanusie & Robinson (2018).
\(^{20}\)Perugini (2018).
\(^{21}\)Danielli, Di Maio, Gendusa & Rinaldi (2018) at 40.
\(^{22}\)Dal Checco (2017).
\(^{23}\)Frediani (2014).
\(^{24}\)The term \textit{“other asset”} seems to come closest to the concept of \textit{“altra utilità”} used in Italian law,
which uses \textit{utilità} to refer to anything that can be used to replace what has been obtained through
criminal activity.
behavioural requirement of Article 648-bis of the Italian Criminal Code, namely that behaviour must be carried out in such a way that it obstructs identifying the criminal origin of the laundered goods.

On this point, while noting that bitcoin transactions are perfectly traceable, it can be inferred that an obstacle exists from the fact that virtual money transactions would ensure the anonymity of the various users.

We do not agree with this point of view.

Even setting aside the fact that Bitcoin does not ensure any anonymity, as previously stated, we should recall that in the case of money laundering the obstacle should not generically be the concern of investigations, but rather identifying the criminal origin of the goods\(^{25}\). This means that not all obstructive activities are punishable, but only those that “affect, either materially or legally, the ‘other asset’ itself in some way.”\(^{26}\)

Legal scholars have argued that any operation that deceives or disguises reality, and which affects other aspects of the actual event, may be punished on other grounds, but such activity cannot constitute money laundering\(^{27}\). Someone who buys something of criminal origin, reports it to the authorities, and then assists with reconstructing its criminal origin while obstructing the search for the perpetrator, is not responsible for money laundering\(^{28}\).

Consequently, if concealing the origin of an asset is done by obstructing the identification of the perpetrator of a crime (the so-called “concealment of the perpetrator” of the predicated offence), this cannot be constituted as money laundering\(^{29}\).

Take the example of transferring a vehicle obtained fraudulently by several individuals who use a false document to take title of the vehicle, which they then sell. In this case the actions do not constitute money laundering because the actions taken to conceal reality do not regard the asset itself, but rather the perpetrators of the legal manoeuvres used to sell it\(^{30}\).

This principle is confirmed regarding payments using stolen bank cheques after replacing the beneficiary’s information. According to the Corte Suprema di Cassazione (the Supreme Court at the top tier of the Italian ordinary jurisdiction) “when the accused only cashes cheques of illegal origin into their own bank account, after replacing the beneficiary’s information with their own and endorsing the cheque, without tampering with the information identifying the issuing bank or the serial number of the cheques, such behaviour shall not be qualified as money laundering.”\(^{31}\)

And yet, if the problem with Bitcoin is that it ensures its users anonymity, in the light of Italian legal scholarship and the ruling just cited, it seems clear that the obstruction referred to in Article 648 of the Italian criminal code does not apply in such cases. With Bitcoin, only the concealment concerns the possible owner of the

\(^{25}\)Maugeri (2016) at 140.

\(^{26}\)Maugeri (2016) at 141.

\(^{27}\)Razzante (2011) at 34; Faiella (2009) at 163; Magri (2007) at 442.

\(^{28}\)Zanchetti, (1997) at 368.

\(^{29}\)Faiella (2009) at 260.

\(^{30}\)Razzante (2011) at 34; Magri (2007) at 455.

virtual money, which could be concealed by pseudo-anonymity. From a physical point of view, the asset undergoes no concealment, resulting in perfectly traceable and visible transactions.

That said, however, a clarification is required: acquiring virtual money through online transactions does not seem to constitute the crime of money laundering; however, it may do so in the case of purely cash payments.

Cyberlaundering is traditionally broken down into two types: “instrumental cyberlaundering” and “online cyberlaundering”. The former is when at least one of the three phases of laundering (placement, layering, and integration) is carried out digitally. A typical example of instrumental cyberlaundering carried out via Bitcoin is purchasing virtual money with the cash proceeds of a crime.

In online cyberlaundering, all phases in the process of laundering dirty money take place digitally. The money to be laundered is already available in digital form, and the laundering procedures tend to be quick and easy. Online cyberlaundering takes place when purchasing virtual money with money that is already virtual.

And yet, as previously mentioned, acquiring bitcoins with money of illicit origin, according to the definition of online cyberlaundering, does not seem to obstruct identifying the criminal origin of the asset. In this particular example, the entire operation is tracked. When purchasing bitcoins, there is no obvious concealment. Normally, a purchase is paid for by wire transfer or credit card, and law enforcement agencies can very easily trace it back to the alleged crime. If one chooses to use a virtual currency, one must provide the identity of the user, as required by recent anti-money laundering regulations (Decreto Legislativo n. 90 of 25 May 2017).

Bitcoins are registered on the blockchain, and all transactions regarding every single unit are always visible at zero cost. The system is so transparent that, once a given suspicious bitcoin has been identified, it is possible to find out who has used it: all the way back to the origin of the blockchain. A case in point is the Silk Road issue; after the arrest of the site operator, investigators followed the bitcoins to track down everyone who had any role in the online platform operating in the deep web.

Instrumental cyberlaundering operations are a different matter. In such cases, users purchase virtual money using cash. This is not a widespread practice in the crypto-world, as cash exchanges presuppose physical encounters between the parties, and Bitcoin platform users typically interact virtually from their various corners of the world.

And yet, acquiring bitcoins using money of criminal origin from someone other than the perpetrator of the alleged crime does seem to constitute the specific case referred to in Article 648-bis of the Italian criminal code. In this case, with the transition from the physical to the virtual world, bitcoin is potentially capable of severing all links between the illicit proceeds and the alleged crime. This transition irremediably cuts off all ties between the substituted good and the predicated

33Capaccioli (2015) at 254.
34Frediani (2018).
offence, constituting an example of actual concealment of the physical object of the crime.

In the case of a person who purchases a quantity of bitcoins using cash obtained as the result of a crime, if he or she makes the transaction by working with a private individual, without resorting to an official currency, it is not subject to any sort of control or reporting obligation.

The person could easily exchange money for bitcoins, with no tracking at all. Once the transaction has been completed, no one would be able to connect the bitcoins with the alleged crime. There would be no possible traceability of the bitcoin transactions, because the operation was anonymous at its source when the cash was converted into virtual currency.

Furthermore, since Bitcoin is based on a decentralised system incompatible with any intervention by any central authority, it ensures the impossibility of any physical goods being confiscated. Indeed, if the investigating agencies do not have individuals’ passwords – or better yet, the encryption keys – of a given wallet, they cannot actually seize anything.

Lastly, the decentralised structure of Bitcoin makes oversight extremely difficult. There is no authority to which the State can turn to order that all suspicious transactions be reported. The system is based on a peer-to-peer network automatically managed by an algorithm.

Conclusions

This paper has attempted to analyse the relationship between Bitcoin and money laundering in Italian law. We have sought to show that using virtual currency does not pose serious laundering risks. Indeed, in this case virtual money, rather than being a tool for criminals and launderers, would truly be a Trojan horse. If money launderers were to invest significant capital in Bitcoin, in a single blow they would risk attracting the attention of all law enforcement agencies.

This is similar to what happened with the Internet in the early 2000s. At that time many commentators decried the risk of money laundering that lurked behind using the web.

Indeed, in an interview on 11 December 2000, Edward P. Rindler, a special adviser to Bill Clinton, then President of the United States of America, argued that the Internet was the new frontier of globalised crime and explained that it was possible to launder dirty money via the web. Alessandro Scartezzini, of the Transcrime research centre at the University of Trento, was of the same view. According to Alessandro Pansa, the Director of the Central Operational Service of the Central Anti-Crime Directorate of the State Police, and Donato Masciandaro, a

---

35Morone (2018); Frediani (2018).
36Tamburini (2014).
37Calabrò (2000) at 17.
38Montefiori (1998) at 23.
professor at the Bocconi University of Milan, the Internet would be favourable to an increase in laundering dirty money. Today, however, there is unanimous belief that only the transition from cash to digital money is capable of defeating money laundering; thus the Internet has gone from being a dangerous tool to a valuable ally in the fight against money laundering. Who knows? Might something similar happen with Bitcoin?

References


---


Pomes, F. (2019). ‘Le valute virtuali e gli ontologici rischi di riciclaggio: tecniche di repressione’ in Diritto penale contemporaneo, rivista trimestrale 2:159-176


