BITCOIN AS CASH IN TERMS OF THE EUROPEAN ANTI-MONEY LAUNDERING DIRECTIVE

Carolin Kaiser

Ph.D. Candidate, Rijksuniversiteit Groningen

The European Anti-Money Laundering Directive 2015/849 sets out detailed rules for the prevention of money laundering and terrorist financing. It presents a clear framework for financial institutions, covering both cash and electronic payments systems. However, the directive fails to regulate digital currencies, such as bitcoin, leaving a large lacuna in the directive. Financial institutions specializing in digital currencies are thus left to their own devices with little information about how best to address the obligations set forth in directive 2015/849. In this paper, the author will propose the application of the rules on cash to digital currencies. As digital currencies are limited to the digital sphere and operate in a closed environment, they are often mistakenly compared to e-money, but the way digital currencies operate is in fact very close to how cash is used today. Digital currencies are obtained through online exchanges, just as cash is usually obtained from an (automatic) bank teller. Cash and digital currencies are both typically exchanged between individuals without interference of a third party. Finally, there is no entity who can be obliged to track the movement of cash or digital currencies between individuals, except if a payment is exceptionally large. However, unlike anonymous cash, there exists a ledger of all transactions carried out in digital currencies, which can be used by financial intelligence units directly to track suspicious movements. Therefore, it can be argued that the application of the rules on cash could facilitate a smooth incorporation of digital currencies into the existing framework.

Table of Contents

1. Introduction

Any new technical development challenges the legal framework existing at the time it is conceived, by very simply not fitting into the existing categories to which the law applies. The internet itself is a good example of a technical development which challenged and forced many amendments into the legal framework in order to envelop the new development and its consequences. This development is still ongoing, as slowly the digital world reaches into more and more areas of the physical world, and as the two become more and more intertwined. One aspect of such an ongoing development is the inclusion of virtual currencies into the existing legal framework concerning financial transactions, and in particular the anti-money laundering rules.

In some areas of daily life, technology has almost completely replaced any older analogue way of doing things. In other areas, this development is much slower. Examples for both can be found in financial transactions. Online banking is ubiquitous, and private online banking is now the favoured way to carry out one's transactions, as it is more convenient for both businesses and consumers than going to a bank at its physical location and filling in a slip of paper. In fact, small branches of banks are being closed in response to this development, which again hurries the transition along. The increased efficiency, economy, and convenience of online banking has allowed for a nearly frictionless transition in society and swift amendments to the law, which accommodates this development. Other developments have not run as smoothly. One example for a more difficult transition is virtual currencies, and one of the legal frameworks which cause problems in this transition is the Anti-Money Laundering directive 2015/849.

The newest European Anti-Money Laundering directive was just passed in 2015, at a time when virtual currencies had already gained a large user base and significant levels of attention of the general public. Especially the blockchain technology, first introduced by virtual currencies, has entered computer sciences with much commotion. However, despite all the current interest in virtual currencies, the Anti-Money Laundering directive does not accommodate virtual currencies in the framework. In fact, the directive does not mention virtual currencies at all, and continues to cater exclusively to traditional, and for the most part analogue, financial service providers.[1]

[1] The preparatory documents do mention the importance of keeping on top of technological developments which may be used for the purposes of money laundering or

This paper thus seeks to answer the question of how to make this new phenomenon of virtual currencies fit into categories designed without so much as the proverbial nod to this particular technology. The best option, with regard to the unique characteristics of virtual currencies, appears to be to apply the rules on cash transactions to virtual currencies This not quite obvious but no less fitting analogy should create legal certainty for all businesses obliged to follow anti-money laundering rules under the directive, while at the same time creating minimal obstacles for the development of virtual currencies as an emerging technology.

The discussion of this idea is started by a short explanation of what virtual currencies are, and a summary of the existing anti-money laundering framework of directive 2015/849. Following this basic outline of the facts, the paper shall turn to the characteristics of cash and virtual currencies, in particular the anonymity of cash, and the enhanced privacy of virtual currencies, and finally outline the main advantages and disadvantages of fitting both instruments into the same category.

2. Virtual Currencies

As has already been mentioned, virtual currencies are an entirely new phenomenon on the financial marketplace. While the idea and demand had been around for a long time, several technical difficulties remained, until in 2008, Satoshi Nakamoto proposed a decentralized virtual currency based on a peer-to-peer network.[2] After a little more tweaking on the code, Nakamoto and a handful of early enthusiasts introduced Bitcoin early in 2009. Since the successful start of Bitcoin, many other virtual currencies have been launched, some with great success.

Virtual currencies are a completely new form of financial tools. Bitcoin, the first and most successful virtual currency in existence, is both a system and the name of the unit of account used on this system. To distinguish the two, the system is spelled with a capital B, while the unit of account is not capitalized. The system is the revolutionary element. Fiat currency depends

terrorist financing. See European Commission, Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing. COM (2013)45 final, 4.

[2] See: S. NAKAMOTO (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*. To be found at https://bitcoin.org/bitcoin.pdf (last accessed 12 October 2016).

on a government establishing that currency, coining it, and establishing a central bank to implement its financial policy.

Virtual currencies are different from the fiat currency system in several ways. The virtual currency environment is not established by a government, and most virtual currencies have no ties to any official government body of any country. Instead, they are based on a peer-to-peer system, administered and run by private individuals and businesses, which may be strewn all over the world, who use their computer power to keep the system running, but who cannot be considered employees or even managers of the virtual currency. The independence of physical location and geographical ties, and the absence of staff and official representatives also protects a virtual currency environment from government interference. There is no official physical representation of any virtual currency, such as coins and banknotes. Instead, every transaction takes place purely online.

Finally, and perhaps most importantly, the peer-to-peer system does away with the importance of a central bank to administer transactions.[3] Instead, a ledger is compiled, containing all transactions ever having taken place on the system. This ledger is accessible to all users of the system. This way, when a transaction is proposed, a user can go back through the transaction history to determine whether the counterparty is in possession of the necessary amount of virtual currency for the transaction. All transactions transferring units to the user as well as all transactions of the user spending units are chronicled in the ledger, making it easy to compute the exact amount of units in the possession of any given user at any given time. Since every user is in possession of the whole ledger, a transaction attempting to spend more units than the user has in possession is rejected by the system and cannot be completed.

This final point makes the virtual currency system secure without the need for a central authority. The enduring problem prohibiting an earlier spread of virtual currencies was the so-called double spending problem. In a cash transaction, the physical coins and banknotes leave the possession of one person and pass into the possession of another person, when a transaction is completed. Electronic transactions of fiat currencies are administered by banks, who have access to a person's balance and can therefore reject a transaction when sufficient funds are lacking, or accept a transaction and grant the customer credit.

[3] S. NAKAMOTO (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*. 1.

This is different in virtual currencies. Computer systems make it possible to manufacture almost infinite numbers of copies of any computer file. A file stored on one user's computer can be copied and sent to an infinite amount of other users, while the original file remains on the first user's computer. This is an obvious problem in financial transactions, as any system in which units could be copied and transferred more than once would surely be doomed. Before Bitcoin, there was no reliable way to make a unit unique in such a way, that a user could only spend it once, rather than copying it to use the same unit again in another transaction. The only secure way to ensure the validity of transactions was the existence of a central authority keeping track of all transactions to exclude the possibility that a unit was spent twice. The virtual currency environments allow every member of a peer-to-peer network access to this ledger, thereby replacing the central authority with the sum of other users of the system.

3. The Anti-Money Laundering directive

In May 2015, the fourth European Anti-Money Laundering directive was passed and adopted. Directive 2015/849 is a powerful tool in the fight against money laundering and terrorist financing, introducing far-reaching surveillance of financial transactions and strong safeguards to be taken by all businesses offering financial transactions services.

The rules circumscribe a regime of due diligence, in which each customer must be identified before a financial transaction is carried out, and where every financial transaction itself must be scrutinized and monitored, in order to make sure that transactions which raise a suspicion of money laundering or terrorist financing are, if possible, not carried out, and in all cases communicated to the financial intelligence unit, which specializes in the investigation into terrorist financing and money laundering.

The directive applies to all obliged parties enumerated in article 2 (1). This includes banks, insurances and investment firms, but also tax accountants, lawyers, and estate agents. All those entities have in common that they deal with large amounts of money on a professional basis. The only exception is the inclusion of traders in (luxury) goods, who must comply with the obligations of the anti-money laundering framework whenever they accept a cash payment of EUR 10 000 or more (article 11).

The obligations of these parties are twofold. In the first place, there are customer due diligence duties, which comprise the identification of all customers (article 13 (1) (a)). In the case where the customer is a legal

person, the beneficial owner must be ascertained, i.e., the corporate structure must be examined and followed, until "any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted", is found (article 13 (1) (b) jo. Article 3 (6)). Furthermore, the transaction carried out by the customer must be scrutinized, to exclude as far as possible the risk of money laundering and terrorist financing. If the customer and the obliged entity enter into a business relationship of longer duration, each transaction carried out during this business relationship must be monitored and scrutinized when it is carried out (article 13 (1) (d)).

In the second place, there are the reporting obligations. If one of the transactions of a customer raises a suspicion of money laundering or terrorist financing, the obliged entity must report this transaction to the financial intelligence unit (article 33). The financial intelligence unit must be provided with the full information record about the customer and the suspicious transaction. In addition, the financial intelligence unit has access to unspecified information collected by other government agencies (article 32 (4)). The customer is not to be informed of a report sent by the obliged entity to the financial intelligence unit (article 39).

Before continuing to virtual currencies, it should be pointed out that the anti-money laundering directive does not in fact speak of "money", but rather of "property", which term is defined in article 3 (3) as "assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form including electronic or digital, evidencing title to or an interest in such assets". This extremely broad definition of property very clearly also covers virtual currencies as possible property used for the purposes of money laundering or terrorist financing.[4]

[4] C. KAISER (2016), *The Classification of Virtual Currencies and Mobile Payments in Terms of the Old and New European Anti-Money Laundering Frameworks*, in G. GIMIGLIANO (ed.), *Bitcoin and Mobile Payments, Constructing a European Union Framework*, Palgrave Studies in Financial Services Technology, 212 f.

4. The anonymity of cash and the privacy of virtual currency systems

Cash is an anonymous means of financial transfers.[5] In a great majority of transactions, cash is exchanged between two persons who will not be known to one another. For instance, a five euro bill may be used by a customer to buy a small item from a supermarket. The cashier may routinely check the genuineness of the banknote, but if the note is genuine, there will be no reason to identify the customer. This same banknote may be handed to another customer as change in a following transaction. This customer will not know who the previous owner of that note was. When the bill is next spent, the customer will likely have forgotten where and when exactly he has received it. These details are not recorded nor remembered or attended to, because the transaction is completed when the physical banknote or coins have changed hands, and because the identity of the banknote or coin is not of the essence; it is the value of the notes or coins which is of interest to the parties.

While bank notes are marked by unique serial numbers, these numbers are highly impracticable to be tracked by any other party than an established bank. An average banknote of a small denomination will travel through many hands before it is turned back to a bank, and none of the parties by whom it is used for a transaction will typically have noted the serial number.

This is different in electronic transfers. If the customer of the supermarket in the example paid his purchases by card, this transaction is very minutely recorded. The trail left by this transaction would include the identities of both parties, i.e. their names and bank account numbers, the exact time that the transfer was made, and the amount transferred. Furthermore, this record would be accessible to both parties to the transaction as well as the intermediaries, i.e. their banks or credit card companies.

The anti-money laundering directive only attempts to break into the anonymity of cash transactions when a high threshold is reached. Article 11 of directive 2015/849 sets the threshold at which persons trading in goods must apply customer due diligence measures at EUR 10 000. Such a threshold therefore only concerns sellers of luxury goods, and even for such traders, large cash transactions are no longer very common. Electronic

[5] See: Financial Action Task Force (FATF), FATF Report: Money Laundering through the Physical Transportation of Cash (October 2015). To be found at http://www.fatf-gafi.org/media/fatf/documents/reports/money-laundering-through-transportation-cash.pdf (last accessed 13 October 2016), 27 ff, 31 f. for very detailed information on the anonymity of cash and the problems created by this anonymity.

transactions, on the other hand, trigger the whole range of obligations upon the financial intermediary. Referring again to the example above, the two parties are fully identified to their respective banks, and an identity record is transferred in the transaction details. Furthermore, such a transaction will be scanned for possible red flags, pointing to possible terrorist financing or money laundering operations. While the transaction in this example is not likely to raise a red flag, reporting duties may follow if it did.

Therefore, cash and electronic transactions mark the two extremes of identification. In cash transactions, no records are retained, and the transaction is generally completely anonymous. In electronic transactions, the parties are fully identifiable by the trails left through the transactions.

Virtual currencies are unchartered territory somewhere between those two extremes. Virtual currencies are also often erroneously called "anonymous", in fact, the belief that virtual currencies are anonymous is probably the most wide-spread misconception about the system. Instead of anonymity, pseudonymity should be spoken of in this context. Each transaction made via a virtual currency system is recorded in the blockchain. As has already been shown, the blockchain is a publicly accessible record of all transactions, from which any user of the system can verify that the counterparty is in possession of sufficient funds to complete the transaction. It records the sender and recipient of each transaction, as well as an exact time-stamp, and the amount transferred. The sender and recipient are denominated by their public key, which acts as a pseudonym for the person behind the transaction. The fact that each transaction is recorded in the blockchain thus clearly eliminates the anonymity of virtual currencies as compared to cash.

5. Virtual currencies in the Anti-Money Laundering directive

When moving from the legal provisions in the anti-money laundering directive to virtual currencies, many commentators make the mistake of comparing transactions using virtual currencies to digital transactions carried out by banks or credit card companies. Surely they look similar at first glance, as in both instances, value is moved between two accounts electronically. However, the two systems are manifestly different.

The bank or credit card company is, in the first place, a legal person, falling under the categories of obliged entities in the Anti-Money Laundering directive. As such, these financial services providers certainly have an interest in following the law, and could be compelled to follow it

were they not so inclined. Any such obliged party will have physical offices and employees which could be searched or questioned by law enforcement entities, and a reputation and business interests which it will want to protect from the financial drawbacks and negative press involved in being suspected of non-compliance with the law, searched, or fined for violations. A virtual currency environment, on the other hand, is in most cases a loosely connected network of users who run the same code on their computer. There may be legal persons among them, but in a peer-to-peer network, not one of the nodes can be said to control the network. Besides the lack of a legal status, there are generally no official representatives, no offices, and what members there are to the system may be physically located in dozens of different jurisdictions, thereby effectively removed from the grasp of law enforcement agencies in any single jurisdiction. Therefore, a bank or credit card company can be obliged to comply with the anti-money laundering legislation, while a virtual currency system can not.

In the second place, electronic transactions using a bank pass or credit card always run through intermediaries. When a customer initiates a transaction using his bank pass, the transaction is in the first instance between him and his bank. The bank clears the transaction, communicates with the bank of the other party, and that bank sees to the funds being placed in the account of the counterparty. The transaction thus depends on the work of at least one, but often two or more intermediaries. This is not the case in virtual currencies. In transactions using virtual currencies, the users communicate directly with one another. Surely, transactions are still cleared by the system, and many nodes in the peer to peer system are involved in confirming the transaction, but in principle, the funds move straight from one user to another without any stopovers.

Only very few services connected to a virtual currency environment are covered by the Anti-Money Laundering directive.[6] The main entrance- and exit points of virtual currency systems are guarded and monitored for the purposes of the anti-money laundering directive. Most users of virtual currency systems enter the environment through an exchange. There are many online exchange businesses for virtual currencies, which work in the same way as analogue currency exchanges, in that the users send a certain amount of fiat currency to the exchange by credit card or other electronic means, and receive the equivalent amount of virtual currency in exchange.

[6] See C. RÜCKERT (2016), *Virtual Currencies and Human Rights*, 16 f.. To be found at http://ssrn.com/abstract=2820634 (last accessed 13 October 2016).

Those businesses, if they are established within the European Union, are obliged parties under the European Anti-Money Laundering framework and must comply with the stipulations of the directive.[7] Another example of a service which should be covered by the anti-money laundering rules are gambling services using virtual currencies for their business.[8]

The problem with the anti-money laundering directive is thus that any transaction involving an obliged party is heavily regulated, obliging the financial services provider to identify its customers, monitor transactions, and report transactions if necessary. At the same time and parallel to this heavily regulated sector of financial transactions exist the virtual currency environments, to which, with very few exceptions, all those rules do not apply.

6. A proposal for a solution: the parallel with cash transactions

The previous section was concerned with eliminating the erroneous comparison of virtual currencies to other means of electronic transactions. Instead of comparing virtual currency transactions to electronic bank transfers, then, there is the somewhat less obvious but very fitting comparison with cash transactions.

There is one significant similarity between cash transactions and virtual currency transactions. Both transactions can be accomplished without any intermediaries. In cash transactions, the transaction is completed with the passing of the physical bank notes or coins from the hands of one party to those of another. No intermediaries are needed to clear or process the transaction, and often transactions are concluded between consumers. The simple impracticability or even impossibility of applying the rules stipulated in the directive thus created a special status for cash transactions. They are not monitored at all, unless the value of the transaction reaches the EUR 10 000 threshold.

It has already been shown that virtual currencies and cash transactions work in much the same way. The transaction is completed with the passing of virtual currency units, such as bitcoin, from the account of one user to

[7] C. KAISER (2016), *The Classification of Virtual Currencies,* 214 f.

[8] One important improvement to the fourth Anti-Money Laundering directive as compared to the previous directive 2005/60/EC is that while the previous framework only covered analogue, brick-and-mortar casinos, directive 2015/849 also covers online gambling services. See C. KAISER (2016), *The Classification of Virtual Currencies*, 218 f.

another. There is no central intermediary needed to process or complete the transaction. The transaction is included in the blockchain, which is administered via a peer to peer system by other users, but these third parties ("miners") by no means inhibit such a position as a central clearing agency would, as they exist in bank or credit card transfers.

The fact that there is no central intermediary also makes the entire framework impossible to be applied to virtual currency. There is simply no obliged party to identify parties and monitor transactions. Consequently, virtual currencies in so far fall to a large extent outside the scope of the anti-money laundering directive. Therefore, the same obstacle which prevents cash transactions to be monitored on a grand scale also prevents virtual currencies from being monitored effectively. The idea to treat two different instruments which share the same difficulty for a legislator in the same way is surely not too far-fetched.

7. Consequences of applying the rules on cash transactions to virtual currencies

Surely, proponents of a strong anti-money laundering framework will not like to see the equal treatment of virtual currencies and cash. From the point of view of advocates of a strong stand against money laundering, electronic financial transfers as offered by banks and credit card institutions create perfect conditions. Those electronic transfers contain lots of information about each transaction, such as the amount transferred, the time stamp, but also information about the sender and recipient of the funds. Full identification records about both parties to each transaction are available at the banks. And finally, and this is certainly one of the most attractive points of the anti-money laundering framework, all of the identification and monitoring duties, including the financial burden that they create, are shifted on to the financial services provider. The significant costs of such identification duties and the ongoing monitoring are thus carried by the financial services providers, and, needless to say, ultimately by their customers, who are the subjects of this monitoring.

Cash, as has been shown, is wholly anonymous. Anti-money laundering duties can only apply to transactions of an amount equal to or higher than EUR 10 000. The very large majority of cash transactions are thus not

monitored at all. Clearly, this makes cash one of the most attractive vehicles for money laundering operations.[9]

The rule, that all transactions beyond EUR 10 000 in cash do fall under the anti-money laundering framework certainly would have to be applied to virtual currencies as well. All traders in goods accepting virtual currencies as payment would be obliged to identify the customer and monitor, perhaps report the transaction depending on the circumstances, if the value of the transaction would exceed the equivalent of EUR 10 000 in the virtual currency unit of account.

A problem which presents itself is that the level of protection against money laundering and terrorist financing in virtual currencies will not be very high if the rules on cash are applied to it. However, if this lower level of protection is deemed acceptable in cash transactions, it should also be accepted for transactions in virtual currencies. The level of risk of abuse of cash is very likely higher than that of virtual currencies. In the first place, cash is the preferred option for money laundering and terrorist financing operations. This has not changed significantly since virtual currencies have established themselves in the market place.

The conversion of virtual currencies into fiat currency can be a complicated calculation. Virtual currencies are notoriously unstable, the exchange rate can sore and plummet over great margins within a short time. This difficulty can only be overcome by exact time stamps, and the threshold for consumer due diligence obligations should therefore also only apply to transactions exceeding the equivalent of EUR 10 000 at the exact time at which the transaction was completed, disregarding the development of the exchange rate before and after the transaction. This is a problem which any trader or service provider whose transactions cross the border of the Eurozone is already familiar with, as the exchange rate of other fiat currencies will certainly also vary over time, though perhaps not as drastically as that of virtual currencies.

Furthermore, while virtual currency systems thus elude the reach of the anti-money laundering framework, the users of the virtual currency environment are not wholly beyond the reach of the anti-money laundering rules.[10] The widespread use of exchanges in order to enter and exit the virtual currency environment has already been mentioned. Certainly those exchanges can be classified as financial institutions and therefore as obliged

[9] FATF Report, *Money Laundering through the Physical Transportation of Cash*, 27 ff, 31 f. for detailed figures.

[10] C. RÜCKERT (2016), *Virtual Currencies and Human Rights*, 12.

parties.[11] All online exchanges operating under the law of any member state of the European Union therefore are bound by the national law implementing the European anti-money laundering framework. Many already do.[12]

Similarly, gambling services, which make up a large part of the traffic in virtual currencies, are obliged under the anti-money laundering framework and thus must comply with the obligations set out therein.

Finally, despite the similarities between how cash and virtual currencies work, there is one great difference between the two. While cash is wholly anonymous, all transactions carried out in virtual currency environments are listed in the publicly accessible blockchain. Therefore, although there is no entity which can be obliged to monitor all transactions carried out in virtual currencies, law enforcement can well monitor the blockchain itself. Virtual currencies are therefore by no means anonymous, nor do they allow as ample opportunities for criminal transactions as does cash.

8. Conclusion

To go back to what was said in the start, almost all new technologies put significant problems before the legislator when the existing legal framework must be amended to accommodate the new development. Also, many emerging technologies have been demonized as vehicles for crime. The world wide web is a good example for both, and has not yet left either of those problems behind itself.

Virtual currencies are still in an early stage of development and public acceptance. The European legislator now carries a significant burden of responsibility to regulate virtual currencies sensibly, in order to both address the risk which virtual currencies undoubtedly bring with them, but at the same time, legal regulation of the technology must not stifle its development. This paper was intended to start a discussion on how such a sensible regulation may be begun.

To sum up, it could be argued that some sensible regulation within the framework of the existing laws would be better than legal uncertainty and fragmentation of regulation if member states themselves fill in the lacuna left by the directive. As virtual currencies are necessarily rooted in an online

[11] C. RÜCKERT (2016), *Virtual Currencies and Human Rights*, 10 f.

[12] See, for instance, the policies of Bitfinex at https://www.bitfinex.com/terms and https://www.bitfinex.com/privacy (last accessed Oct. 12th, 2016). Similar terms of service and policies are applied by all the major exchange services.

context, the services provided utilizing virtual currencies also take place on the internet, which means that there is a high level of cross-border transactions. Different regulation of virtual currencies therefore would work to the detriment of the development of this technology. Therefore, the European level should be the preferred arena for the development of a framework regulating virtual currencies in the context of money laundering and terrorist financing, and in all other areas as well.