X CONVEGNO ANNUALE DELL'ASSOCIAZIONE ITALIANA DEI PROFESSORI UNIVERSITARI
DI DIRITTO COMMERCIALE "ORIZZONTI DEL DIRITTO COMMERCIALE"

"*L'EVOLUZIONE TECNOLOGICA E IL DIRITTO COMMERCIALE*"

Roma, 22-23 febbraio 2019

VINCENZO ORSINI

Fighting anonymity in blockchain technologies

TABLE OF CONTENTS: 1. Introduction. - 2. Blockchain technology. - 2.1. The concept. - 2.2. Participants. - 2.3. Consensus. - 2.4. Incentives. - 3. Anonymity in public ledgers. - 3.1. Technological barriers. - 3.2. Legal background. - 3.3. Current framework and possible future approaches. - 4. Conclusions. - 5. Bibliography.

1 Introduction.

On Tuesday 1st October 2013, the US authorities closed 'Silk Road', the most famous online black-market in the world. It sold any kind of illegal goods, such as drugs and weapons, and was famous for being completely anonymous. Silk Road was situated in the dark web and guaranteed non-traceability of the users by allowing payments only via Bitcoin[1]. This story lead many to believe, for a very long time, that the purpose of cryptocurrencies was exclusively to undertake illegal or shady activities[2]. After almost five years, it seems indeed clear[3] that

[1] *For the full story, see* - Joshuah Bearman, 'The Rise And Fall Of Silk Road, Part I' [April 2015] Wired <https://www.wired.com/2015/04/silk-road-1/> and, 'The Rise And Fall Of Silk Road, Part II' [May 2015] Wired <https://www.wired.com/2015/05/silk-road-2/> both accessed 1 July 2018.

[2] *Among others,* More Mihm, 'Are Bitcoins The Criminal's Best Friend?' (*Bloomberg*, 2013) <https://www.bloomberg.com/view/articles/2013-11-18/are-bitcoins-the-criminal-s-best-friend-> accessed 1 July 2018; Behzad Mohit, 'Bitcoin: Is It An Economic Equalizer Or A Tool For Conflict And Crime?' (*Huffington Post*, 2014) <https://www.huffingtonpost.com/dr-behzad-mohit/bitcoin-is-it-an-economic_b_6617994.html> accessed 1 July 2018; William Suberg, 'Cryptocurrency Regulation In The International Community 2015: Part 1' (*Cointelegraph*, 2015)

cryptocurrencies and -in general- blockchain technology[4] have the potential to overshadow any possible criminal use. Nonetheless, identity is an aspect that still generates several outstanding question marks.

Many blockchains do not enforce identities to be revealed. Transactions are open and transparent on the ledger, but parties remain anonymous. The distributed ledger shows only the transactions occurred, but not the parties involved (at least explicitly). Since two key features of cryptocurrencies are security and privacy[5], those blockchains can, consequently, be used for money-laundering, illegal activities or tax evasion[6]. The Silk-road case exemplifies what a dangerous application cryptocurrency can have. Anonymity poses a serious threat over society:

<https://cointelegraph.com/news/cryptocurrency-regulation-in-the-international-community-2015-part-1> accessed 1 July 2018.

[3] It will be shown later in this article that most of the financial authorities from all over the globe look with favour on the innovations that this new technology can bring. For instance, the UK Government explicitly recognized how "in distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation" in Matt Hancock and Ed Vaizey, 'Distributed Ledger Technology: Beyond Block Chain' (*UK Government Chief Scientific Adviser*, 2016) <https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review>, 4, accessed 1 July 2018. Many studies, however, still demonstrate that a big part of the transactions with cryptocurrencies are made with illegal purposes: *recently*, Sean Foley, Jonathan R. Karlsen and TTlis J. Putniii, 'Sex, Drugs, And Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?' [2018] SSRN Electronic Journal.

[4] Even though the terms "Distributed Ledger Technology" (DLT) and "Blockchain" are often used interchangeably, the latter is a specific type of a DLT that encrypts all the transactions in a chain of blocks: "every blockchain is a distributed ledger, but not every distributed ledger is a blockchain" - Shaan Ray, 'The Difference Between Blockchains & Distributed Ledger Technology' (*Towards Data Science*, 2018) <https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92> accessed 1 July 2018.

[5] Don Tapscott and Alex Tapscott, 'Blockchain Revolution' (Penguin 2016) 39-45; Zachary Zane, 'Bitcoin And Cryptocurrency: What You Need To Know' (Rolling Stone, 2018) <https://www.rollingstone.com/culture/features/bitcoin-and-cryptocurrency-what-you-need-to- know-w514552> accessed 26 December 2017.

[6] Other major risks of cryptocurrencies that have been identified are: 1) considered as fiat-alike currencies, cryptocurrencies could alter the supply of money and Central Banks could lose control over money issuance. The price stability and the precision of economic readings (e.g. GDP) would be at stake; 2) as investments, cryptocurrencies pose serious concerns in terms of transparency and investor protection; 3) as a mean of payment, cryptocurrencies could reduce the influence of the financial establishment and cause disfunctions. *See* - Raffaele Scalcione, 'Gli Interventi Delle Autorità Di Vigilanza In Materia Di Schemi Di Valute Virtuali' [2015] Analisi Giuridica dell'Economia <https://www.rivisteweb.it/doi/10.1433/80274> accessed 1 July 2018, 139-141.

"on the blockchain, nobody knows you're financing terrorism"[7]. In other words, some blockchains could be used to transfer illegally perceived money or to fund illegal activities without leaving any trace about the agents.

The shadow of anonymity in cryptocurrencies grows proportionally with their spread adoption and increase in value. Regulatory gaps are consistently endangering public interest and jeopardising the efforts of tracking illegal money flows. The 'Silk Road' is only the tip of the iceberg: many other illegal use-cases of cryptocurrencies are yet to be discovered and will likely multiply over time. Governments and regulatory bodies need to be prepared and cooperate if they want to stop a future wave of crypto-criminality.

This paper will focus on the problem of anonymity in public blockchains. The analysis will proceed by firstly analysing the intrinsic characteristic of the technology that allow anonymity and, secondly, by giving the current legal framework and some possible legal policy approaches. In fact, understanding some details about the functioning of blockchains is fundamental to determine which instruments can be adopted to cope with anonymity. Lastly, the paper will proceed to the conclusions. It will be assumed that the reader already has some rudimental understanding in the field of cryptography and blockchains[8].

2 Blockchain technology.

2.1 The concept.

Databases play a fundamental role in our society because they record information. In a very simplistic way, anything that happens in the real world such as business transactions, land registrations, or birth records are all inserted in spreadsheets and stored. Nothing that has a value is ever left unrecorded: it mainly serves the purpose of tracing pieces of information. In other words, records are needed in order to establish and verify any information.

---

[7] Based on the famous cartoon caption "on the Internet, nobody knows you're a dog" by Peter Steiner (*The New Yorker*, 5 July 1993).

[8] For a comprehensive introduction to the topic, *see* - Jean Bacon and others, 'Blockchain Demystified' (2017) 268 Queen Mary School of Law Legal Studies Research Paper <https://ssrn.com/abstract=3091218> accessed 1 July 2018.

Obviously, in order to be useful, the information needs to be reliable and uncorrupted. Traditionally, those records are kept by central institutions like banks, public authorities, organizations (and so forth) that guarantee their trustfulness and integrity. In fact, there are strict rules that declare liable those who intentionally or negligently assert incorrect information or tamper it. It is enough to consider that in many parts of the world public notaries are used to enhance trust in important transactions. **The real revolution is that blockchain technology enables to establish, verify, and keep the information in a reliable[9] manner without the supervision of a central institution[10].**

To ensure reliability, blockchains use both (I) a distributed ledger and (II) cryptographic technology:

I. Every participant of the blockchain has an identical copy of the 'spreadsheet' (ledger) and new entries need to be verified and accepted by every member. By using this simple concept of a *distributed database*, a blockchain can give a very high degree of certainty about the integrity of the information and that it has not been corrupted unilaterally by any member of the blockchain[11]: it has to be the same in every copy of the ledger. Moreover, to insert a new transaction in the ledger, every participant of the network controls the correctness of the entry.

[9] For practical purposes blockchain is unalterable without detection, but future advances in technology mean it is not safe forever. The PKI infrastructure that is commonly used today for blockchains will cease to be secure "within a finite number of years" - Chris Reed and others, 'Beyond Bitcoin Legal Impurities And Off-Chain Assets' [2017] Int J L & IT 2018, SSRN Electronic Journal, 9.

[10] Marco Iansiti and Karim R. Lakhani, 'The Truth About Blockchain' (Harvard Business Review, 2017) <https://hbr.org/2017/01/the-truth-about-blockchain> accessed 26 December 2017.

[11] "Storing a blockchain in a distributed manner (i.e. as a Distributed Ledger or DL) has three main advantages. First, it protects data integrity from tampering by any single centralised party. Second, a DL may be less vulnerable to attack since there is no single master copy of the ledger to target. Finally, a DL is resilient since there is no single point of failure to target with a denial of service (DoS) attack. Even if several nodes failed, the network would still continue to function" – Bacon (8) 12-13.[8]

II. Cryptographic technology is then used to: (i) achieve integrity of the data and (ii) authenticate identities:

i. *Hash functions* are used to achieve integrity of the data. This function work in such a way that, by encrypting a piece of data, it is possible to produce a unique output. It means that a single change in the input will necessarily produce a different output[12]. Transactions are, therefore, grouped in 'blocks' and encrypted using a hash function. Then, blocks are connected to each other to compose a 'chain'[13]. Every block of transactions contains a piece of the previous one. In order to fraudulently change a transaction, not only the block containing it should be tampered, but also every subsequent block. Further, all the copies of the ledger should be changed accordingly. Consequently, the longest and most distributed the chain, the safest it is[14].

ii. *Public Key Infrastructures* (*PKI)* are used to authenticate identities. The blockchain needs to make sure that the user has the right to undertake the transaction and that no one else can unduly dispose of its tokens. The system relies on a pair of linked keys (passwords) where one is private (Ks) and adopted by the user to confirm the transaction (encrypt), and the other one is public (Kp) and is needed by the network to decrypt and check the information[15]. If the Kp allows to correctly decrypt the transaction, this proves that it came from the keyholder. The asymmetry of the keys involves that the public key can only decrypt and cannot encrypt a modified transaction.

This complex system ensures *trustfulness and incorruptibility* to the data. It has the upside of attributing a very high degree of reliability to the ledger but the downside that the information stored is *permanent.* Once a

[12] The chances of having the same hash for different values are very low, in SHA256 (probably the most common hash function) is ~$1/10^{60}$ – Bacon (8) 6.
[13] Hence the term 'blockchain'.
[14] Satoshi Nakamoto, 'Bitcoin: A Peer-To-Peer Electronic Cash System' (2009) <https://bitcoin.org/bitcoin.pdf> accessed 26 December 2017, 3.
[15] Reed (9) 11; Bacon (8) 9-10; Nakamoto (14) 2.

transaction is registered, being technically impossible to rectify, it cannot be reversed without the consent of the new keyholder[16].

2.2 Participants.

Blockchains do not exist as standalone computer programs, instead they need an extended network of participants to function effectively. Looking closely, it is possible to identify different (sometimes intersecting) categories of participants, with different functions and duties. It is worth to mention that, generally[17], anyone can take any role. Early cryptocurrencies, like Bitcoin or Ethereum, involve essentially three of them[18]:

- **Users** - simply buy and sell tokens; they only indirectly contribute to the functioning of the blockchain by transacting tokens and need only to run on their computer (or using a third-party service[19]) the cryptographic program that generates the keys related to their tokens.
- **Miners** - assemble transactions into blocks and encrypt them using the hash function (so-called *mining*);
- **Nodes** - store copies of the ledger; they offer local storage capacity to keep a copy of the blockchain and they verify the validity of the transactions.

Blockchains, however, can be *public* or *permissioned*[20]. In a public blockchain, everyone can join the network and start participating in the consensus mechanism, while, in a permissioned one, the network is

[16] "The alteration would invalidate the hash of the block containing the record, and also the hashes of all subsequent blocks… Rectification can therefore only be achieved by recording a new transaction in the ledger which reverses the transaction to be modified."- Reed (9) 22.

[17] This is especially true for public blockchains. Permissioned blockchains -per definition- restrict the access and tend to select their participants and assign roles - 'Explainer | Permissioned Blockchains' (Monax). <https://monax.io/explainers/permissioned_blockchains/> accessed 26 December 2017.

[18] Bacon (8) 11-12; Nakamoto (14); Vitalik Buterin, 'A Next Generation Smart Contract & Decentralised Application Platform' (2013) <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 1 July 2018.

[19] i.e. *wallet providers*, *see* below [3.1].

[20] Helen Eenmaa-Dimitrieva and Maria José Schmidt-Kessen, 'Regulation Through Code As A Safeguard For Implementing Smart Contracts In No-Trust Environments' (2017) 13 EUI Working Papers 10-16.

restricted solely to members that have the required permission. The blockchain is private or permissioned because an authority is in charge of deciding upon admissions and roles and able to modify the "rules" of the blockchain without having to fork it[21]. This central entity functions as an **access control layer (ACL)** because it can approve separately the miners, that participate in the consensus mechanism, and the common users, that can interact with the ledger by entering data or making transactions. Conversely, public blockchains are completely open and fully decentralized.

Companies ready to embrace blockchain technology for their business purposes, but not to open their private network to everyone (e.g. for asset tracking, supply chain management or building a banking consortium), will design a permissioned blockchain and decide by themselves who can join the network and under which conditions[22]. Whereas aspects such as identity and confidentiality are of prime importance, the adoption of a "plain vanilla" public blockchain is out of question.

2.3 Consensus.

Since, as previously mentioned, every new entry in the ledger needs to be encrypted and confirmed, nodes and miners are essential. Miners will generate the encrypted blocks of transactions that will then pass under the scrutiny of the nodes. Once accepted, new blocks will become part of the blockchain. One of the key features of blockchain technology relies on its security. This means not only that the records have to be incorruptible once encrypted, but most importantly that they have to be *correct*.

Incorrect values may give *double-spend* problems. This sort of issues may arise if an individual or an organization cannot legitimately dispose of a specific asset. In plain English, if the person willing to transact does not own the good that wants to give. This would allow using the same asset more than once. The typical example is about spending the same money twice: by cash, it is impossible because the banknote is no more at

[21] For a deeper analysis, *see* - Bacon (8) 21-24.

[22] Jatinder Singh and Johan David Michels, 'Blockchain As A Service' (2017) 269 Queen Mary School of Law Legal Studies Research Paper <https://ssrn.com/abstract=3091223> accessed 1 July 2018, 7-8.

the disposal of the original holder, by digital means, it is just a matter of changing numbers on a spreadsheet.

In order to assess the correctness of the values, blockchains deploy peculiar systems of *consensus*[23]. Participants of the blockchain must control any new entry and confirm that is correct. By consensus, new transactions are grouped, encrypted and added to the chain. However, in a situation where anyone can be a miner or a node, hackers could take over the blockchain by indefinitely adding new nodes or miners. This is why consensus protocols are so sophisticated and most of them involve some sort of investment by the participants of the network (for instance, electricity and computational power). The investment ensures that the participants of the network have interest in keeping the blockchain correctly running.

There are several cryptographic means of achieving consensus[24]. Here the most famous that, currently, public blockchains adopt:

- **Proof of Work (PoW)[25]**. The blockchain assigns to the miners a mathematical problem, comparable to solving a puzzle, that has only a single correct result and requires a lot of work. The problem is difficult to solve, but easy to check. The computational power and, consequently, the electricity devoted to the cause should demonstrate the good faith of the miner and its interest in keeping the blockchain correctly functioning (because of its stake in the blockchain itself).
- **Proof of Stake (PoS)[26].** It requires nodes and miners to proof their 'stake' in the blockchain, namely their wealth (i.e. the number of tokens

[23] Traditional consensus protocols are *synchronous,* meaning that all the copies of the ledger are updated once any new block has been accepted by the already known number of nodes. In public blockchains, since everyone can join the network and the number of nodes is unknown, consensus protocols are *asynchronous,* meaning that not all the nodes have updated copies of the ledger and miners start working on the best information available to them – Bacon (8) 13.

[24] Other known protocols are (i) *Proof of Activity* - Iddo Bentov and others, 'Proof Of Activity: Extending Bitcoin'S Proof Of Work Via Proof Of Stake' (2014) 42 ACM SIGMETRICS Performance Evaluation Review, and Tapscott (2), 31-32; (ii) *Practical Byzantine Fault Tolerance (PBFT)* and (iii) *Earliest Timestamp Wins* – Bacon (8) 15, and Miguel Castro and Barbara Liskov, 'Practical Byzantine Fault Tolerance And Proactive Recovery' (2002) 20 ACM Transactions on Computer Systems.

[25] Nakamoto (14) 3; for those unfamiliar with the subject, *see* Bacon (8) 14-15.

[26] Sunny King and Scott Nadal, 'PPcoin: Peer-To-Peer Crypto-Currency With Proof-Of-Stake' (2012) <https://peercoin.net/assets/paper/peercoin-paper.pdf> accessed 1 July 2018.

held). The protocol then chooses in a deterministic way the miner that has to add the new block. The purpose is still to prove the interest in keeping the blockchain correctly functioning, but the process is different.

- **Proof of Capacity (PoC)[27].** Participants have to provide memory to the network. The protocol still requires an investment from participants, but in terms of storage. It, therefore, requires participants to give proof of their storage capacity by assigning a verification task.

New consensus protocols started to be introduced as soon as it became clear that PoW was highly demanding in terms of electricity[28]. Developers tried to combine its core functionality of guaranteeing the security of the network and correctness of the records with a technology that required less energy consumption. It is still debated[29] which is the best consensus protocol (if there is any) but what seems clear is that the appropriate consensus protocol depends on the structure of the blockchain itself and its purpose: it is not always essential to adopt PoW (or similar mechanisms) to validate blocks[30]. Ripple, for instance, is a digital payment protocol[31] that employs a verified pool of validators. Users form their *Unique Nodes Lists* (UNL) among those validators and UNLs then achieve consensus[32]. The protocol is based on the simple assumption that nodes on the lists are chosen not to let nodes to collude and defraud the system.

It is needless to say that PoW may not be necessary in permissioned blockchains, given the pre-existent trust relationships among participants[33]. Consequently, a permissioned blockchain will enable the

---

[27] Giuseppe Ateniese and others, 'Proofs Of Space: When Space Is Of The Essence', Security and Cryptography for Networks (Springer, Cham 2014) <https://doi.org/10.1007/978-3-319-10879-7_31> accessed 1 July 2018.

[28] *As later demonstrated also by* Karl J. O'Dwyer and David Malone, 'Bitcoin Mining And Its Energy Footprint' [2014] 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014).

[29] For an overview, *see* - Wenbo Wang and others, 'A Survey On Consensus Mechanisms And Mining Management In Blockchain Networks' (2018) abs/1805.02707 CoRR <https://arxiv.org/abs/1805.02707> accessed 1 July 2018.

[30] Hancock and Vaizey (3) 18.

[31] For more information, *visit* <https://ripple.com/>

[32] David Schwartz, Noah Youngs and Arthur Britto, 'The Ripple Protocol Consensus Algorithm' (2014) <https://ripple.com/files/ripple_consensus_whitepaper.pdf> accessed 1 July 2018.

[33] Singh and Michels (22) 7.

adoption of simpler consensus protocols. Further, "*the nodes may be able to process transactions more quickly, since transactions can be verified, and blocks mined, by a small number of trusted nodes*"[34]. The prerequisite is full trust in the active participants (i.e. nodes and miners) of the blockchain. Contrarily, malicious participants could manipulate the ledger to their own interest.

2.4 Incentives.

It should be clear, at this stage, that consensus comes at cost. Secure consensus protocols still require adequate hardware, time, processing power, storage and electricity. For this reason, in public blockchains, some sort of incentive mechanism for nodes and miners is needed. They handle the correct functioning of the ledger and need to be incentivized to keep on doing that. In permissioned blockchains, it may not be necessary. The organization responsible for the blockchain could provide by itself the necessary computational resources or adopt an inexpensive consensus protocol.

Let's take bitcoin as an example: as an incentive for their contribution to the blockchain, miners get rewarded with some newly generated *tokens* from the blockchain itself and a transaction fee from the users. The number of newly generated tokens for any encrypted block decreases over time. The assumption of Nakamoto was that with time, the value of bitcoin would have increased, and rewards should have proportionally reduced to reflect it[35]. The bitcoin case is peculiar because bitcoins can be generated only by mining. The total number of bitcoins is pre-set (to preserve their value) and once they finish, miners get only transaction fees[36].

Tokens are part of an incentive scheme ideated to guarantee the development and the correct functioning of the blockchain network. Generally, they are created only in two occasions: when miners group transactions in a block (as a reward) and in case of an initial coin offering (ICO). In this latter case, the developers of a blockchain offer some tokens

[34] Bacon (8) 20-21.
[35] Nakamoto (14) 4.
[36] *Ibid*.

in pre-sale to promote their network and fund their project (crowd-sale)[37]. Bitcoin, the first blockchain, is constituted solely of mined tokens, i.e. those produced validating transactions. Every token introduced in the market has been previously mined and only successively sold. More recent blockchains however, of which Ethereum is the most famous, started offering a set of tokens in pre-sale to expand their network.

An ICO serves the purpose of enlarging the blockchain network and raising funds for the underlying project[38]. Public blockchains need a large number of nodes and miners to enhance their security and increase the value of their tokens[39]. Promoters of an ICO campaign, therefore, aim to create a market for their tokens since the very beginning. Moreover, as a fund-raising tool, ICOs offer a valuable framework for project financing. 'Backers' can support a new project, such as a new technology, a product or a company, by investing their money to buy tokens of the newly opened ICO. Generally, they will be rewarded with some form of 'early-bird' incentive, like a discount on the price of the token, while the promoters will be able to use the funds received to start the project.

3 Anonymity in public ledgers.

3.1 Technological barriers.

Public blockchains, as Bitcoin, tend to be open and transparent. They are open because they allow anyone to become a node of the network, and transparent because every new block of transactions is publicly visible on the blockchain. Everyone on the internet can see the transactions happening in real time. However, **the only thing to be transparent is the transaction, not the parties**. The blockchain does not enforce identities to be revealed. Transactions are referred to addresses, and those are not related to any specific person. Public blockchain grant anonymity[40] (or pseudonymity as someone specifies[41]).

---

[37]Jin Enyi and Yen Le Ngoc Dang, 'Regulating Initial Coin Offerings ("Cryptocrowdfunding")' [2017] Butterworths Journal of International Banking and Financial Law, 495.

[38] Iris M. Barsan, 'Legal Challenges Of Initial Coin Offerings (ICO)' (2017) 3 Revue Trimestrielle de Droit Financier (RTDF) <https://ssrn.com/abstract=3064397> accessed 1 July 2018, 55.

[39] As already pointed out, more distributed ledgers seem to be safer – *see above* [2.1].

[40] Tapscott (5) 42-45.

Since Bitcoin was the first blockchain to be implemented, and assuming that cryptocurrencies are the most dangerous form of blockchain in terms of money-laundering, illegal activities or tax evasion, it seems correct to analyse the problem of anonymity by using it as a case-study. Nonetheless, *any blockchain involves tokens of some kind*[42], and the reasoning that will be made for Bitcoin could easily be transplanted to any token. Tokens operate as a reward for the miner, and consequently, are the basis of the *consensus* mechanism. Without them, there is no incentive to spend computational power on a public blockchain. Only private blockchains could afford to operate without tokens[43].

In order to start transacting, the first thing that a user must do is to create a Bitcoin address[44]. The address is like a bank account number. It is only a recording number that enables to send and receive bitcoins. However, differently from a bank account number, it is not related by any mean to the user or to a specific location. It is just a unique number, and comes with a set of encryption keys that allow to receive or transfer the bitcoins. Any address has its own keys.

Bitcoin addresses are created via specific software or using the online website of Bitcoin. The operation does not require any identity information, and can be done as many times as wanted. One person can

---

[41] Some clarify that the term "pseudonymous" is better suited because every transaction is recorded transparently in the distributed ledger - European Central Bank, 'Virtual Currency Schemes – a further analysis' (ECB 2015) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 1 July 2018. Moreover, for some authors pseudonymity would plausibly allow the traceability of the parties - Massimo Amato and Luca Fantacci, 'Per Un Pugno Di Bitcoin' (Università Bocconi editore 2016); Hancock and Vaizey (3) 51. Even though it is surely possible to somehow trace parties, it does not reduce the danger of illegal activities because: 1) tracing parties does not seem so easy and straightforward as described: transactions should be grouped and linked to a unique address, but one person can have multiple addresses; 2) many techniques exist that can ensure not to leave any trace (e.g. TOR); 3) some cryptocurrencies can be completely non-transparent; 4) criminals could even create their own cryptocurrency – *of the same idea*, Stefano Capaccioli, 'Criptovalute E Bitcoin. Un'analisi Giuridica' (Giuffrè 2018) 253; Stefano Capaccioli, 'Riciclaggio, Antiriciclaggio E Bitcoin' (2014) 46 Il Fisco, 4562; Ludovica Sturzo, 'Bitcoin E Riciclaggio 2.0' (2018) 5 Diritto Penale Contemporaneo <https://www.penalecontemporaneo.it/d/6006-bitcoin-e-riciclaggio-20> accessed 1 July 2018, 21.

[42] Pavel Kravchenko, 'Does A Blockchain Really Need A Native Coin?' (Medium, 2016) <https://medium.com/@pavelkravchenko/does-a-blockchain-really-need-a-native-coin-f6a5ff2a13a3> accessed 26 December 2017.

[43] For the reasoning, *see* [2.4].

[44] The whole procedure can be undertaken on <www.bitcoin.org>.

(and should) have multiple addresses. In this way, the risk of losing all the bitcoins is mitigated: if someone stoles an address, the user does not lose all the bitcoins but just part of them.

Addresses can be stored offline or online. A user may even decide to keep them on a piece of paper, and it will never be possible for any hacker to steal it (so-called *cold-storage*). Notwithstanding, they are commonly stored into 'wallets'. A wallet is only a database of a third party that contains all the addresses of the user, and is generally protected by encrypting passwords[45].

Since the transactions are anonymous, it should be clear that the only way to proceed with identifications is to intercept the connecting points between offline-value and cryptocurrencies (i.e. when *fiat* money is converted into cryptocurrency). The easiest way to trace identities back is, obviously, to start from bitcoins exchanges. Nonetheless, thinking that the problem would be solved that easily, is quite naïve.

Hence, it seems useful to repeat the four ways to obtain a bitcoin:

1. *Mining*. The only way to receive a bitcoin directly from the blockchain is to mine it. As it has been already mentioned, bitcoins are only issued for miners. Anyone can mine, it is just a matter of electricity and computational power.
2. *From a miner* in exchange for any asset, as in a common sale.
3. *From a third party* that has already bought it from a miner.
4. *Through a facilitator.* A facilitator is a virtual currency exchange platform. As traditional currency exchanges, they buy and sell cryptocurrencies. Moreover, they often offer users the possibility to set up wallets on their infrastructures.

Other blockchains give the possibility to acquire some tokens also through an ICO[46]. A pre-set number of tokens is allotted for a pre-sale.

[45] Financial Action Task Force, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (FATF 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 1 July 2018, 7-8.
[46] *See* above [2.4].

Users can purchase them directly from the promoters of the blockchain before it starts to operate[47].

Any of those mediums could be adopted to transfer illegally perceived money or to fund illegal activities. It is, therefore, of vital importance to consider every one of them when trying to cope with the problem of anonymity in the context of AML/CTF. Consequently, the following part of the paper will highlight the position of some EU authorities, analyse the measures ultimately adopted at EU level, and evaluate their effectiveness (given the peculiar technological framework and the available mediums to obtain a token).

3.2 Legal background.

Let's take one step back. On one hand, the legal tools to combat and repress money-laundering, illegal activities or tax evasion are mainly of criminal law. On the other hand, prevention is based on the collaboration between national bodies, international organizations and private counterparties and is aimed to intercept in advance illegal money flows[48]. This anti-money laundering regime was born in the 80s as a response to narco-trafficking with the establishment of the Financial Action Task Force (FATF)[49] and its most notorious prevention tools in the financial system are Know-Your-Customer (KYC) and Customer-Due-Diligence (CDD) obligations posed over certain entities[50].

---

[47] The transaction is undertaken via smart contract - for more information, *see* 'Smart Contracts, Legal Agreements For The Digital Age' (Clifford Chance 2017) 2 <https://www.cliffordchance.com/briefings/2017/06/smart_contracts_-legalagreementsforth.html> accessed 1 July 2018; Antony Lewis, 'Three Common Misconceptions About Smart Contracts' (Bits on blocks, 2018) <https://bitsonblocks.net/2017/03/07/three-common-misconceptions-about-smart-contracts/> accessed 1 July 2018.

[48] Laura La Rocca, 'La Prevenzione Del Riciclaggio E Del Finanziamento Del Terrorismo Nelle Nuove Forme Di Pagamento Focus Sulle Valute Virtuali' (2015) 1 Analisi Giuridica dell'Economia, 202.

[49] The FATF "was established by the G-7 Summit that was held in Paris in 1989" and its main responsibilities are "examining money laundering techniques and trends, reviewing the action which had already been taken at a national or international level, and setting out the measures that still needed to be taken to combat money laundering" - 'History Of The FATF - Financial Action Task Force (FATF)' (Fatf-gafi.org, 2018) <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 1 July 2018.

[50] For an outline of the history and applicability of the European anti-money laundering legislation, *see* - Niels Vandezande, 'Virtual Currencies Under EU Anti-Money Laundering Law' (2017) 33 Computer Law & Security Review, 343-350.

In EU, under the fourth anti money-laundering (AML) Directive[51], KYC obligations required[52] certain entities (such as banks, accountants or law firms)[53] to identify customers and monitor their business relationships[54]. The extent of such a CDD is on a risk-sensitive basis[55] and can result in simplified[56] or enhanced[57] measures. Those entities will then have to report[58] suspicious transactions[59] to designated state bodies[60] that can operate together with EU Financial Institutions Units (FIU) to analyse and suspend the transaction[61]. Failing to comply may result in effective, proportionate and dissuasive sanctions[62]. In other words, organizations have to keep track of their customers and their transactions and report/suspend those that seem suspicious. Starting from this information, law enforcement bodies will eventually investigate and take action.

AML/CTF measures assume that there is an intermediary that can forward information about to suspicious transactions and that can be sanctioned in case of non-compliance. Unfortunately, blockchain technology is -by definition- decentralized and does not require intermediaries. However, some intermediaries like exchanges, wallet providers, and trading platforms started to operate in the crypto-world. As a consequence, many authorities proposed to appoint them responsible for KYC and CDD obligations.

The FATF in 2014 published a report[63] where it warned of the risk posed by virtual currencies[64] and then published in 2015 its guidance for a

---

[51] Directive 2015/849 Of The European Parliament And Of The Council Of 20 May 2015 *on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing* OJ L141/73.

[52] The 4th AML Directive has been recently amended by the 5th AML Directive - further considerations will be made below [3.3].

[53] 4th AML Directive, art. 2.1.

[54] *Ibid,* art. 13.1.

[55] *Ibid,* art. 13.2.

[56] *Ibid,* art. 15-17.

[57] *Ibid,* art. 18-24.

[58] *Ibid,* art. 33.

[59] *Ibid,* art. 11.

[60] *Ibid,* art. 34.

[61] *Ibid,* art. 32.7.

[62] *Ibid,* art. 58.1.

[63] Financial Action Task Force (45).

[64] The term "virtual currency" was firstly used by the ECB and included: 1) *closed virtual currency schemes* that have no connection with real-world money (e.g. World of Warcraft

risk-based approach to virtual currencies[65] where it clarified the applicability of its previous recommendations. In particular, the FATF focuses on *convertible* virtual currencies (i.e. those that can be converted in fiat currency and vice versa) and recommends the regulation of exchange platforms by requiring forms of registration or licensing that could ensure compliance with AML/CTF measures[66]. Hence, the risk-based approach proposed by the FATF consist in extending the KYC/CDD obligations over cryptocurrency exchanges.

It has already been highlighted that is quite naïve to think that the anonymity problem could be solved so easily, and that any medium usable to purchase token should be taken into consideration. This kind of approach appears ineffective because it only intercepts cashflows passing through a secondary market -i.e. the facilitator- and completely forgets that a token can be purchased or created in many other ways.

In the meanwhile, the European Central Bank (ECB) in a report of 2012[67], later updated in 2015[68] observed that cryptocurrencies are still not

---

Gold); 2) *virtual currency schemes with unidirectional flow*, where virtual currency can be bought with *fiat* money but not converted back (e.g. Nintendo Points); 3) *virtual currency schemes with bidirectional flow,* that allow both conversions (e.g. Bitcoin). It does not narrow the definition only to cryptocurrencies issued via blockchain but also more centralised schemes - European Central Bank, 'Virtual Currency Schemes' (ECB 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 1 July 2018.

[65] Financial Action Task Force, 'Guidance For A Risk-Based Approach to Virtual Currencies' (FATF 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 1 July 2018.

[66] (A) Applicable Recommendations for countries: Risk-Based Approach (RBA)(Recommendation 1); national cooperation and coordination (Recommendation 2); registration or licensing requirements for MVTS (Recommendation 14); identification and mitigation of risks associated with new technologies (Recommendation 15); *de minimis* threshold for cross-border wire transfers of 1000 eur/usd (Recommendation 16); adequate regulation and supervision (Recommendation 26); effective, proportionate, dissuasive sanctions (Recommendation 35); international cooperation (Recommendations 37-40).

(B) Applicable Recommendations for covered entities (i.e. intersection nodes between crypto-activities and *fiat* currency): RBA (Recommendation 1), customer due diligence (CDD) (Recommendation 10); record-keeping (Recommendation 11); registration or licensing requirements for MVTS (Recommendation 14) identification and mitigation of risks associated with new technologies (Recommendation 15); AML/CFT program requirements (Recommendation 18) and suspicious transaction reporting (Recommendation 20).

[67] European Central Bank (64).

[68] European Central Bank (41).

widely adopted and that are not yet capable of putting in danger the safety and stability of the financial and monetary systems. However, despite the numbers, it recognized its potential risk for ML/TF, and, together with exchanges it pointed the attention towards wallet providers, trading platforms, ATM manufacturers and exchange-traded funds[69].

Unsurprisingly, the ECB did not propose any course of action. Its main concern was not to recognize cryptocurrencies to have legal tender capacity[70] in order not to grant them some sort of legitimacy[71] and encourage their use[72]. Thus, it defined cryptocurrencies as a 'special' type of e-money, substantially denying them any legal consequence[73]. As a result, it declared that cryptocurrencies could not have been regarded as being subject to the 2nd Payment Service Directive[74] (PSD2) or the E-Money Directive[75] (EMD). In the opposite case, the 3rd AML Directive[76] would have found immediate applicability[77].

[69] *Ibid,* 8.
[70] *Ibid,* 23.
[71] The definition given by the ECB is "*a digital representation of value, not issued by a central bank, credit institution or e-money institution, which, in some circumstances, can be used as an alternative to money*" – *ibid*, 25.
[72] The reason being that cryptocurrencies "could also undermine users' confidence in electronic payment instruments, in e-money and/or in specific payment solutions, such as those in place for e-commerce" – *ibid,* 5.
[73] The difference stands in the fact that e-money issuers must have an authorization and, most importantly, e-money accounts and funds received are expressed in the same currency (e.g. Euro, dollars, etc). Conversely, cryptocurrencies are fully decentralized and have their own denomination (and the exchange rate tends to fluctuate) - ECB (64) 16-17; ECB (41) 24-25.
[74] Directive 2015/2366 Of The European Parliament And Of The Council of 25 November 2015 *on payment services in the internal market* (2015) OJ L337/35.
[75] Directive 2009/110/Ec Of The European Parliament And Of The Council of 16 September 2009 *on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC* (OJ L 267/7).
[76] Directive 2005/60/Ec Of The European Parliament And Of The Council of 26 October 2005 *on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing* (OJ L 309/15).
[77] For a complete analysis about the inapplicability of the PSD2 and of the EMD, *see* - Vandezande (50).

The European Banking Authority (EBA) also intervened *in subjecta materia*[78]. In fact, it released its opinion in 2014 and proposed a more interesting (and quite complex) approach to cryptocurrencies:

- In the **long term** it proposed the creation of a 'scheme governance authority' as a mandatory requirement for a virtual currency scheme to be regulated as a financial service. In other words, a legal person responsible for the ledger and accountable for any misuse would be the condition to interact with existing regulated schemes. This entity would also be obliged of: i) complying (together with all the third-party service providers) with KYC/CDD requirements; ii) having strict corporate governance rules such as fitness and probity standards, transparency rules, etc; iii) fulfilling capital requirements and guaranteeing payments and refunds. Despite the doubts of someone[79], this structure is perfectly compatible with a decentralised system and would be feasible with the adoption of a permissioned blockchain. It reflects, however, the willingness to ban public blockchains in the long-run in favour of more controllable ones.
- In the **short term** it recommended national supervisory authorities (i) to discourage institutions from buying, holding or selling virtual currencies, thereby 'shielding' regulated financial services from them and (ii) to declare virtual currency exchanges as 'obliged entities' under the AML Directive.

The position of the EBA is interesting because it considers posing KYC/CDD obligations on exchanges as a transitory solution before a more widespread adoption of cryptocurrencies. In the long-run, the EBA imagines to restrict the permissible blockchains only to those that have an ACL[80] and that can be *technically* compliant with KYC/CDD requirements. Even though it appears to be drastic because it assumes that in the future most public blockchains should be banned, this solution is at least coherent and seem aware of the fact that a light-approach (like the one

[78] European Banking Authority, 'Opinion 2014/08 of the 4th of July 2014 on 'virtual currencies'' (EBA 2014) <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 1 July 2018.
[79] Scalcione (6) 155-158.
[80] *See* [2.2].

proposed by the FATF) could be ineffective and leave consistent loopholes.

Notwithstanding the recommendations of the FATF and the fact that the opinion of the EBA was released during the legislative procedure, the EU Council did not include virtual currencies exchanges under the scope of the 4th AML Directive and left it as an option of Member States[81]. Surely, MS could have decided to include also cryptocurrency exchanges in the scope of their internal AML/CTF measures, but some authors started to question whether virtual currency service providers could have been considered obliged entities even without explicit mention by the Directive[82].

3.3 Current framework and possible future approaches.

Subsequently, prompted by the terrorist attacks in France in 2015, the Commission expressed its intention to "*bring anonymous currency exchanges under the control of competent authorities by extending the scope of the AMLD*" and "*applying the licensing and supervision rules of the Payment Services Directive (PSD)*"[83]. The lack of regulation at EU level was almost immediately filled. It did not take much time before the EU proposed to bring virtual currencies exchanges and (also) wallet providers within the scope of the AML Directive[84]. A process that concluded with the publication of the 5th AML Directive[85].

Slight changes were made from the content of the communication of 2015. On one side, the final text of the Directive included not only cryptocurrency exchanges but also wallet providers in the list of obliged entities under the AML Directive. On the other side, it did not find a place the application of either the PSD2 or the EMD. The reasoning provided

[81] Vandezande (50) 347-349.
[82] *Ibid.*
[83] EU Commission, 'Communication COM (2016) 50 to the Council and the Parliament *on an Action Plan to further step up the fight against the financing of terrorism*' (2 February 2016) 1.2.
[84] EU Commission, 'Proposal 450/2016 of the 5th of July 2016 for a Directive of the European Parliament and of the Council *amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC*' (COM(2016) 450 final).
[85] Directive 2018/843 Of The European Parliament And Of The Council of 30 May 2018 *amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU* (2018) OJ L156/43.

here is quite straightforward. Even though the PSD2 imposes automatically AML/CTF requirements, its content goes well beyond the scope of the AML Directive. It provides also a licensing obligation for regulated entities, minimum capital requirements, safeguarding requirements, and consumer protection rules: all measures that are inapplicable to public and decentralized blockchains. Moreover, it could have given more legitimacy on the virtual currency market[86] (as also supposed by the ECB[87]). The EBA welcomed the proposal and most of its structure[88].

Despite the general approval upon the measure, it may only be seen as transitory (in accordance with the original opinion of the EBA[89]). There are several reasons why the sole imposition of KYC/CDD obligations on exchanges and wallet providers seems ineffective:

- First, as some authors argued, that "*to be effective, such rules should be implemented globally. If the review procedure is implemented only in a few countries, the users will simply switch to the bitcoin exchange service providers in other countries where there is no review procedure in place.*"[90] Alone, this measure results only in a burden that could have a negative impact on existing service providers and new market entrants[91]. It is very unlikely that malicious people, knowing about the AML/CTF rules, will still turn to European facilitators. They rather engage with foreign ones.

---

[86] EU Commission, 'Impact assessment accompanying the document Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 *on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC*' SWD(2016) 223 final, 30–31.

[87] European Central Bank, 'Opinion of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/ 849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC' (ECB 2016) <https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2016_49_f_sign.pdf> accessed 1 July 2018, 2-3.

[88] It probably considered the proposal as a good solution to mitigate the risks in the short-term - European Banking Authority, 'Opinion 7/2016 of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)' (EBA 2016) 5. <https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD> accessed 1 July 2018, 4–5.

[89] EBA (78).

[90] Eenmaa-Dimitrieva and Schmidt-Kessen (20), 7.

[91] Vandezande (50) 351-352.

- Secondly, as mentioned before[92], cryptocurrencies can be bought not only via exchanges, but also privately from third parties (miners or subsequent token-holders). Exchanges constitute only a secondary market for individuals willing to buy/sell their tokens. It seems natural that anyone needing to avoid regulatory burdens and costs will opt for a private sale. In this case, the transaction would escape the newly introduced measures and, probably, would be left unrecorded. It could be argued that those transfers of funds involve traditional financial institutions; that people engaging in cryptocurrency transactions still uses *fiat* money to purchase tokens; and that it would be possible to strengthen the existing KYC obligations of traditional financial institutions. The problem here stands in the fact that money transfers towards private counterparties are difficult to label as suspicious because the underlying cryptocurrency transaction still remain anonymous; and that cash transactions remain untraceable.
- Thirdly, cryptocurrency can be produced by mining, and miners do not need any licence or duty to register. It means that ML/TF could simply be pursued through mining. On one hand, illegally perceived money could be used to produce cryptocurrency (i.e. paying the electricity bills) and then converted again in "clean" *fiat* money. On the other hand, anonymously generated cryptocurrency allows to fund illegal activities without any risk to be traced.
- Lastly, it is worth to remind that wallets are not strictly necessary to store tokens. A wallet provider is only a third party that offers its own database to store the Ks of its customers. Users can store their passwords in their own portfolio, even offline (*cold-storage*)[93]. For this reason, it is very unlikely that malicious users will leave their tokens in custody of an organization that is obliged to perform KYC/CDD on their customers. Cold-storage, personal wallets, or foreign wallet providers will surely be preferred.

Furthermore, the imposition of AML/CTF rules -by itself- is not an assurance about the reliability of the provider[94]. Investors may think that

[92] *See* [3.1][3.2].
[93] Enrico Messina, 'Bitcoin E Riciclaggio', Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale (Giappichelli 2017), 381.
[94] As noted by the EBA (88) 5.

the market is regulated and that there are some safeguards for their transactions. This circumstance is dangerous because it could potentially boost the confidence in a market that remains unsafe and that offers few guarantees to its participants.

In order to make more effective and coherent the rules adopted by the EU, the Directive should necessarily be integrated with other measures that consider the decentralized nature of blockchain technology: (i) Financial authorities should impose a mandatory disclosure about the detention of virtual currencies. Dissuasive sanctions should then be applied to whoever fails to comply or gives false statements[95]. (ii) Miners should be forced to register in national/European lists and to disclose their level of production[96]. (iii) Transactions performed outside exchanges that are AML/CTF compliant should be necessarily reported to the competent national authority by the parties themselves[97].

Adopting these complementary measures makes more complicated to legally dispose of a token without leaving traces: anonymous transactions would become unlawful. Identification would be performed either by third party services subject to the 5th AML or by the users themselves. Both miners and mere token-holders would have to disclose the amount and addresses of cryptocurrency produced/owned and report their transactions (if not made via an AML-compliant exchanges). Every European user, transacting in a non-transparent way, would then infringe the law. As a result, this measure will drastically increment the number of known cryptocurrency addresses and, consequently, the ability to exploit data to derive information about unknown users and perform their identification[98].

---

[95] Financial authorities could make sure that the statements are true by requiring the addresses of the tokens, monitoring their movements, and later checking the if the required annual reports are correct.

[96] Since there are only some hints about miners on the blockchain, it would be possible to find (a) those who do not register themselves via electricity consumption; and (b) value of production by analysing the current hash rates (if they are in the territory of the State). A process that appears specular from the one adopted by - O'Dwyer (28).

[97] For instance, it could be imagined a procedure that enables the parties to simply identify themselves and fill an online form on the website of the competent EU body.

[98] It is outside the scope of this paper to review the techniques that could be adopted to perform user identification on a blockchain. What seems clear is the fact that with more known addresses traceability becomes easier. For a comprehensive literature review on the topic, *see* - Jordi Herrera-Joancomartí, 'Research And Challenges On Bitcoin

A more drastic approach to solve the problem of anonymity consists in completely ban cryptocurrencies as they are known today. The ban can be either absolute or implicit. In the first case, detention and disposal of cryptocurrencies is prohibited. It is the case of countries like Algeria, Bolivia, Egypt, Iraq, Morocco, Nepal, Pakistan and United Arab Emirates[99]. In the second case, the ban is implicit because financial institutions within their borders shall not facilitate transactions involving cryptocurrencies. In this way, *fiat* money must necessarily cross the national borders in order to be converted in cryptocurrency, and public authorities can more easily trace cross-border money flows. Bahrain, Bangladesh, China, Colombia, Dominican Republic, Indonesia, Iran, Kuwait, Lesotho, Lithuania, Macau, Oman, Qatar, Saudi Arabia and Taiwan have already implemented a similar approach[100].

Banning cryptocurrencies (as they are known today) does not mean closing the doors to blockchain technology, but simply requiring more control over it. Private blockchains enable to adopt an *access control layer* (ACL) that, as already noted by Professor Reed[101], could enable trusted institutions to apply Know Your Customers (KYC) and Customer Due Diligence (CDD) requirements to the users. In other words, a central institution could allow authorized organizations to fulfil anti-laundering obligations and, consequently, this would enable to perform financial transactions on a blockchain in an effectively regulated way. As mentioned in the previous subparagraph, this is probably also the long-term perspective of the EBA[102].

Anonymity' [2015] Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, par. 3.

[99] Regulation Of Cryptocurrency Around The World' (The Law Library of Congress, Global Legal Research Center 2018) <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> accessed 1 July 2018.

[100] *Ibid*; Kenneth Rapoza, 'Cryptocurrency Exchanges Officially Dead In China' (Forbes.com, 2017) <https://www.forbes.com/sites/kenrapoza/2017/11/02/cryptocurrency-exchanges-officially-dead-in-china/#3cb1559c2a83> accessed 26 December 2017.

[101] Reed (9), 13-14, *citing* WEF, The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services (August 2016, https://www.weforum.org/reports/the-future-of-financial-infrastructure-an-ambitious-look-at-how-blockchain-can-reshape-financial-services).

[102] European Banking Authority (78) 39-43.

Even though this measure appears as the most effective it comes with some obvious caveats. First of all, it is unnecessarily drastic, because the risks do not seem to be so extensive to justify the ban. Secondly, such a top-down regulation is incapable of harnessing the blockchain technology towards a more transparent form. The technological structure is decentralized by nature, and a central authority could only distort it. Hence, banning cryptocurrencies that are not AML- compliant means simply to derail the development of blockchain technology. The development of the internet offers an interesting perspective: the internet was able to develop and to became what we use and appreciate today because it was never directly posed under the governance of a central authority[103].

4 Conclusions.

Blockchain technology is undoubtedly disruptive. It records information in a totally new and reliable way. By using the simple concept of a distributed database, and an advanced cryptographic system, a blockchain can give a very high degree of certainty that the information stored is integer and has not been tampered. However, all that glitters is not gold. Many blockchains do not enforce identities to be revealed: transactions are open and transparent on the ledger, but parties remain anonymous. It means that those blockchains can be used to transfer illegally perceived money or to fund illegal activities.

While permissioned ledgers could be governed by creating an ACL that performs KYC/CDD duties, public blockchains pose a serious threat for the society. Public blockchains are anonymous by nature and there is a high risk that could be used to escape the boundaries of the law. Identification is not a simple procedure and governments from all over the world are trying to tackle the problem.

The FAFT published its first report back in 2014 recommending bringing virtual currency exchanges into the scope of AML/CTF regulations. In response, most of the EU bodies expressed their position. Worth to mention are, respectively, the reports[104] of the ECB and the

[103] For an interesting overview of the topic, *see* - Jack L Goldsmith and Tim Wu, Who Controls The Internet? (Oxford Univ Press 2006).
[104] European Central Bank (41)(64).

opinion[105] of the EBA. The main concern of the first one was to distinguish so-called cryptocurrencies from *fiat* money and operate moral suasion not to encourage the adoption of them. In fact, if widely used, they could alter the supply of money and Central Banks could lose control over money issuance. The latter proposed a more complex approach: in the short-term it asked to list virtual currency exchanges as obliged entities under the AML Directive, while in the long-term it recommended the presence of a 'scheme governance authority' as a requirement for blockchains to interact with existing regulated institutions (presumably adopting a permissioned ledger scheme).

The EU did not implement any measure under the 4th AML Directive, but waited until 5th of July 2016 to propose the necessary amendments. Main elements of the recently adopted 5th AML Directive are the extension of KYC/CDD obligations over virtual currency exchanges and wallet providers, and the absence of any reference to the PSD2 or the EMD.

This light-touch approach of the EU, albeit the result of a precise political choice, has been criticised in this paper for its ineffectiveness. It has been highlighted that cryptocurrencies can be bought not only via European exchanges, but also abroad and privately from third parties (like individuals or miners) or even produced; and that wallet providers are not absolutely necessary to store tokens. Further measures have then been proposed to make unidentified transactions outlaw. It has been proposed a mandatory disclosure of both token detention and production, and the imposition of transaction reports whether the parties decide not to adopt an AML-compliant exchange.

Few words have been spent also on cryptocurrency bans. Despite their effectiveness, they seem to be too drastic. Even though permissioned ledgers could offer a viable solution to apply KYC/CDD requirements and identify blockchain users, this top-down regulation risks to block the technological development and distort the nature of blockchains.

[105] European Banking Authority (78).

5 Bibliography.

1. 'Explainer | Permissioned Blockchains' (Monax) <https://monax.io/explainers/permissioned_blockchains/> accessed 26 December 2017.
2. 'Top Seven Ways Your Identity Can Be Linked To Your Bitcoin Address' (99 Bitcoins) <https://99bitcoins.com/know-more-top-seven-ways-your-identity-can-be-linked-to-your-bitcoin-address/> accessed 26 December 2017
3. Allen C, 'The Path To Self-Sovereign Identity' (Lifewithalacrity.com, 2016) <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html> accessed 26 December 2017
4. Amato M Fantacci L, Per Un Pugno Di Bitcoin (Università Bocconi editore 2016)
5. Ateniese G and others, 'Proofs Of Space: When Space Is Of The Essence', Security and Cryptography for Networks (Springer, Cham 2014) <https://doi.org/10.1007/978-3-319-10879-7_31> accessed 1 July 2018
6. Bacon J and others, 'Blockchain Demystified' (2017) 268 Queen Mary School of Law Legal Studies Research Paper <https://ssrn.com/abstract=3091218> accessed 1 July 2018
7. Barsan I. M., 'Legal Challenges Of Initial Coin Offerings (ICO)' (2017) 3 Revue Trimestrielle de Droit Financier (RTDF) <https://ssrn.com/abstract=3064397> accessed 1 July 2018.
8. Bearman J, 'The Rise And Fall Of Silk Road, Part I' [2015] Wired<https://www.wired.com/2015/04/silk-road-1/> accessed 1 July 2018
9. Bearman J, 'The Rise And Fall Of Silk Road, Part II' [2015] Wired<https://www.wired.com/2015/05/silk-road-2/> accessed 1 July 2018
10. Bentov I and others, 'Proof Of Activity: Extending Bitcoin'S Proof Of Work Via Proof Of Stake' (2014) 42 ACM SIGMETRICS Performance Evaluation Review
11. Buterin V, 'A Next Generation Smart Contract & Decentralised Application Platform' (2013) <https://github.com/ethereum/wiki/wiki/White-Paper> accessed 1 July 2018

12. Capaccioli S, 'Riciclaggio, Antiriciclaggio E Bitcoin' (2014) 46 Il Fisco
13. Capaccioli S, Criptovalute E Bitcoin. Un'analisi Giuridica (Giuffrè 2018)
14. Castro M Liskov B, 'Practical Byzantine Fault Tolerance And Proactive Recovery' (2002) 20 ACM Transactions on Computer Systems
15. Eenmaa-Dimitrieva H, Schmidt-Kessen MJ, 'Regulation Through Code As A Safeguard For Implementing Smart Contracts In No-Trust Environments' (2017) 13 EUI Working Papers
16. Enyi J Ngoc Dang YL, 'Regulating Initial Coin Offerings ("Cryptocrowdfunding")' [2017] Butterworths Journal of International Banking and Financial Law
17. EU Commission, 'Communication COM (2016) 50 to the Council and the Parliament on an Action Plan to further step up the fight against the financing of terrorism' (2 February 2016)
18. EU Commission, 'Impact assessment accompanying the document Proposal for a Directive of the European Parliament and the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC' SWD(2016) 223 final, 30–31.
19. EU Commission, 'Proposal 450/2016 of the 5th of July 2016 for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC' (COM(2016) 450 final)
20. European Banking Authority, 'Opinion 2014/08 of the 4th of July 2014 on 'virtual currencies'' (EBA 2014) <https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> accessed 1 July 2018.
21. European Banking Authority, 'Opinion 7/2016 of the European Banking Authority on the EU Commission's proposal to bring Virtual Currencies into the scope of Directive (EU) 2015/849 (4AMLD)' (EBA 2016) <https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD> accessed 1 July

2018, 4–5.
22. European Central Bank, 'Opinion of 12 October 2016 on a proposal for a directive of the European Parliament and of the Council amending Directive (EU) 2015/ 849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC' (ECB 2016) <https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2016_49_f_sign.pdf> accessed 1 July 2018, 2-3.
23. European Central Bank, 'Virtual Currency Schemes – a further analysis' (ECB 2015) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf> accessed 1 July 2018
24. European Central Bank, 'Virtual Currency Schemes' (ECB 2012) <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> accessed 1 July 2018.
25. Financial Action Task Force (FATF), 'History Of The FATF' (Fatf-gafi.org, 2018) <http://www.fatf-gafi.org/about/historyofthefatf/> accessed 1 July 2018
26. Financial Action Task Force, 'Guidance For A Risk-Based Approach to Virtual Currencies' (FATF 2015) <http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf> accessed 1 July 2018.
27. Financial Action Task Force, 'Virtual Currencies: Key Defini- tions and Potential AML/CFT Risks' (FATF 2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 1 July 2018
28. Foley S, J KarlsenT Putniii, 'Sex, Drugs, And Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?' [2018] SSRN Electronic Journal
29. Goldsmith LJ Wu T, 'Who Controls The Internet?' (Oxford Univ Press 2006)
30. Hancock M Vaizey E, 'Distributed Ledger Technology: Beyond Block Chain' (UK Government Chief Scientific Adviser 2016) <https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review> accessed 1 July 2018
31. Herrera-Joancomartí J, 'Research And Challenges On Bitcoin Anonymity' [2015] Data Privacy Management, Autonomous

Spontaneous Security, and Security Assurance
32. Iansiti M, Lakhani KR, 'The Truth About Blockchain' (Harvard Business Review, 2017) <https://hbr.org/2017/01/the-truth-about-blockchain> accessed 26 December 2017
33. Kravchenko P, 'Does A Blockchain Really Need A Native Coin?' (Medium, 2016) <https://medium.com/@pavelkravchenko/does-a-blockchain-really-need-a-native-coin-f6a5ff2a13a3> accessed 26 December 2017
34. La Rocca L, 'La Prevenzione Del Riciclaggio E Del Finanziamento Del Terrorismo Nelle Nuove Forme Di Pagamento Focus Sulle Valute Virtuali' (2015) 1 Analisi Giuridica dell'Economia
35. Lewis A, 'Three Common Misconceptions About Smart Contracts' (Bits on blocks, 2018) <https://bitsonblocks.net/2017/03/07/three-common-misconceptions-about-smart-contracts/> accessed 1 July 2018.
36. Messina E, 'Bitcoin E Riciclaggio', Norme, regole e prassi nell'economia dell'antiriciclaggio internazionale (Giappichelli 2017)
37. Mihm M, 'Are Bitcoins The Criminal's Best Friend?' (Bloomberg, 2013) <https://www.bloomberg.com/view/articles/2013-11-18/are-bitcoins-the-criminal-s-best-friend-> accessed 1 July 2018
38. Mohit B, 'Bitcoin: Is It An Economic Equalizer Or A Tool For Conflict And Crime?' (Huffington Post, 2014) <https://www.huffingtonpost.com/dr-behzad-mohit/bitcoin-is-it-an-economic_b_6617994.html> accessed 1 July 2018
39. Nakamoto S, Bitcoin: A Peer-To-Peer Electronic Cash System (2009) <https://bitcoin.org/bitcoin.pdf> accessed 26 December 2017
40. O'Dwyer KJ Malone D, 'Bitcoin Mining And Its Energy Footprint' [2014] 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014)
41. Rapoza K, 'Cryptocurrency Exchanges Officially Dead In China' (Forbes.com, 2017) <https://www.forbes.com/sites/kenrapoza/2017/11/02/cryptocurrency-exchanges-officially-dead-in-china/#3cb1559c2a83> accessed 26 December 2017
42. Ray S, 'The Difference Between Blockchains & Distributed Ledger Technology' (Towards Data Science, 2018)

<https://towardsdatascience.com/the-difference-between-blockchains-distributed-ledger-technology-42715a0fa92> accessed 1 July 2018
43. Reed C and others, 'Beyond Bitcoin Legal Impurities And Off-Chain Assets' [2017] SSRN Electronic Journal
44. Reed C, Internet Law (2nd, Cambridge University Press 2004)
45. Reed C, What is a signature, 2000(3) JILT
46. Regulation Of Cryptocurrency Around The World' (The Law Library of Congress, Global Legal Research Center 2018) <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf> accessed 1 July 2018
47. Rivest RL, Shamir A and Adleman L, 'A method of obtaining digital signatures and public key cryptosystems' (1978) 21 Communications of the ACM 120
48. Ruppert P, 'Privacy, Tax Evasion, And The Development Of Cryptocurrencies' (2017) 1 Georgetown Law Technology Review
49. Scalcione R, 'Gli Interventi Delle Autorità Di Vigilanza In Materia Di Schemi Di Valute Virtuali' [2015] Analisi Giuridica dell'Economia <https://www.rivisteweb.it/doi/10.1433/80274> accessed 1 July 2018
50. Schwartz D Youngs N Britto A, The Ripple Protocol Consensus Algorithm (2014) <https://ripple.com/files/ripple_consensus_whitepaper.pdf> accessed 1 July 2018
51. Singh J Michels D, 'Blockchain As A Service' (2017) 269 Queen Mary School of Law Legal Studies Research Paper <https://ssrn.com/abstract=3091223> accessed 1 July 2018
52. Smart Contracts, Legal Agreements For The Digital Age' (Clifford Chance 2017) 2 <https://www.cliffordchance.com/briefings/2017/06/smart_contracts_-legalagreementsforth.html> accessed 1 July 2018.
53. Sturzo L, 'Bitcoin E Riciclaggio 2.0' (2018) 5 Diritto Penale Contemporaneo <https://www.penalecontemporaneo.it/d/6006-bitcoin-e-riciclaggio-20> accessed 1 July 2018
54. Suberg W, 'Cryptocurrency Regulation In The International Community 2015: Part 1' (Cointelegraph, 2015) <https://cointelegraph.com/news/cryptocurrency-regulation-in-

the-international-community-2015-part-1> accessed 1 July 2018
55. Tapscott D, Tapscott A, Blockchain Revolution (Penguin 2016)
56. Vandezande N, 'Virtual Currencies Under EU Anti-Money Laundering Law' (2017) 33 Computer Law & Security Review
57. Wang W and others, 'A Survey On Consensus Mechanisms And Mining Management In Blockchain Networks' (2018) abs/1805.02707 CoRR <https://arxiv.org/abs/1805.02707> accessed 1 July 2018
58. World Economic Forum, 'The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services' (August 2016, https://www.weforum.org/reports/the-future-of-financial-infrastructure-an- ambitious-look-at-how-blockchain-can-reshape-financial-services)
59. Zane Z, 'Bitcoin And Cryptocurrency: What You Need To Know' (Rolling Stone, 2018) <https://www.rollingstone.com/culture/features/bitcoin-and-cryptocurrency-what-you-need-to-know-w514552> accessed 26 December 2017