EJLT European Journal of Law and Technology

When Organised Crime Turns to Cryptocurrency: the Compatibility of Italian Patrimonial Preventive Measures with Cryptocurrency

Gaia Cavagnoli Micali[*]

Abstract

Organised crime has always adapted to different markets from which to profit. Today, one such market is that of cryptocurrency. Concurrently, EU countries have developed an interest in the Italian antimafia legal system, effective pillars of which include patrimonial preventive measures of confiscation and sequestration. But what happens if the assets to preventively confiscate are cryptocurrencies? This paper assesses whether the measures can be considered equally effective in the context of cryptocurrency. Despite the measures having existed for more than forty years, the virtual nature of cryptocurrency has been proven to not comprise an obstacle per se. However, in practice it has been argued that cryptocurrency as the object of the measures is incompatible with the existing law, the pseudo-anonymity of the blockchain, and mixing services. Some reflections and conclusions as to how these incompatibilities might be overcome are provided, aimed especially at those European legislators who are considering transposing Italian antimafia law to their jurisdictions.

Keywords: cryptocurrencies, organised crime, Italian antimafia law, patrimonial preventive measures.

[*] G Cavagnoli Micali is an LLM candidate of Information Communication Technology Law at the University of Oslo and holds an LLB in International and European Law from the University of Groningen.

1. Introduction

Judge Falcone famously stated that the way to trace the tracks of illegal activities of mafia associations is to 'follow the money'.[1] This remains true today, given that legislation targeting the associations' patrimony is an effective contrasting tool.[2] Among these instruments are patrimonial preventive measures: a legal hybrid to contain and remove illegally obtained assets from the legal economy of the state by constraining them in a preventive manner, before a crime occurs. The prominence of organised crime has recently led legislators of other European countries to look to the Italian antimafia system, including its patrimonial preventive measures, to tackle issues in their own jurisdictions. For instance, the Dutch Ministry of Justice has funded a legal study of Italian criminal laws in the fight against organised crime and with the view to taking inspiration from some of those laws.[3] It is in the interest of those European legislators to understand whether preventive measures are equally apt to contain and remove assets which organised crime has recently turned to: cryptocurrencies.

Organised crime has in fact always found diversified markets in which to invest its vast resources.[4] As assets that function on the pseudonymous blockchain, cryptocurrencies may be exploited by criminal groups looking to benefit from the privacy that this technology enables. There has been evidence of cryptocurrencies being a means of payment for large international drug trafficking schemes.[5] For instance, an investigation by the Italian police, Operation Empire, revealed a scheme

[1] Giovanni Falcone was an investigating judge in Palermo, Sicily. He formed part of the so-called antimafia pool, a team of judges instituted in 1983 as a way to centralise investigations on the Sicilian mafia named Cosa Nostra. This group conducted the investigations which led to the maxi trial of Palermo in 1986, with 475 accused; United Nations Office on Drugs and Crime, 'Fondazione Falcone' (UNODC, 2020), <https://www.unodc.org/unodc/en/untoc20/falcone.html> accessed 15 April 2023.

[2] Gaetano Insolera and Tommaso Guerini, *Diritto Penale e Criminalità Organizzata* (2nd ed, Giappichelli Editore 2019) 204.

[3] For instance, the Netherlands will be taking inspiration from Italy on laws about collaboration with justice; Dutch Ministry of Justice and Security, 'Tougher Approach to Organised Crime Under Criminal Law' (Government of the Netherlands, 3 July 2023) <https://www.government.nl/latest/news/2023/07/03/tougher-approach-to-organized-crime-under-criminal-law> accessed 19 June 2024; Laura Peters, 'The Fight Against Mafia Crime in Italy' (WODC, April 2023) <https://repository.wodc.nl/bitstream/handle/20.500.12832/3270/3370-hoofdlijnen-bestrijding-maffiacriminaliteit-italie-summary.pdf?sequence=3&isAllowed=y> accessed 20 June 2024.

[4] Federico Cafiero de Raho, Giuseppe Magliocco and Alessandro Barbera, *Il Contrasto alla Criminalità Organizzata: Attori e Strumenti* (Laurus Robuffo 2021) 127; Nicola Gratteri and Antonio Nicaso, *Fuori dai Confini: la 'Ndrangheta nel Mondo* (Mondadori 2022) 50.

[5] Luca Bianco, 'Vallone (DIA) per combattere la mafia bisogna seguire le criptovalute' (*Huffington Post,* 10 April 2022) <https://www.huffingtonpost.it/dossier/fintech/2022/04/10/news/vallone_dia_per_combattere_la_mafia_bisogna_seguire_le_criptovalute_-9147884/> accessed 12 April 2023.

of Dutch-produced synthetic drugs, destined for the American market.[6] Clients requested orders on the dark web through cryptocurrency payments in bitcoin.[7] This is merely an example of how organised crime has started to establish itself on the blockchain and make use of legislatively uncharted territory, at least from a criminal law perspective, to fruit illegal profits undisturbed.[8] These developments make the blockchain and cryptocurrency transactions on it an interesting point of possible discord with existing antimafia law.

Given the extensive subject matter, this article necessarily comes with some restrictions. First, the assessment is made with reference only to bitcoin. The currency was chosen as an example to serve the analysis, as the most used cryptocurrency to date, despite many new currencies surfacing in recent years. Though other coins exist, known as 'privacy coins' (e.g. monero), which are even more privacy-enabling, their popularity has not overtaken bitcoin use among criminals.[9] Further, because preventive measures deal with the confiscation of assets of illegal origin, their applicability may seem to overlap largely with anti-money laundering (AML) legislation. However, within this analysis, the AML landscape, which is harmonised at EU level, will not be considered.[10] For instance, there are characteristics of blockchain technology that have been argued in literature to be prone to money laundering risks.[11] Nonetheless, to preserve the necessary focus, these will not be the main point of assessment. This article instead concentrates on the effectiveness of the preventive measures when the assets to confiscate or sequester preventively are indeed cryptocurrencies. Hence, while there could be a discussion regarding the illegal origin of crypto-assets, which are then repurposed, that is not the aim here. Lastly, as section 4 will explain, the discussion regarding the benefits and disadvantages of cryptocurrencies has been popularly polarising in recent years. Whether they are good or bad for the legal economy, both privacy advocates and concerned law enforcement have fuelled the discussion. This article will briefly frame

[6] Ministro dell'Interno al Parlamento, 'Relazione del Ministro dell'Interno al Parlamento: Attività Svolta e Risultati Conseguiti dalla Direzione Investigativa Antimafia' (Gennaio-Giugno Primo Semestre 2023) 83.

[7] Ministro dell'Interno al Parlamento, 'Relazione del Ministro dell'Interno al Parlamento: Attività Svolta e Risultati Conseguiti dalla Direzione Investigativa Antimafia' (Gennaio-Giugno Primo Semestre 2023) 83; Alessandro Verelli, 'Catania: Operazione Empire, 7 arresti per traffico di sostanze stupefacenti' (Polizia di Stato, 5 April 2022) <https://www.poliziadistato.it/articolo/catania-operazione-empire-7-arresti-per-traffico-di-sostanza-stupefacenti> accessed 12 April 2023.

[8] Gratteri (n 4) 50.

[9] EU Innovation Hub, 'First Report on Encryption' (Europol, 2024) <https://www.europol.europa.eu/cms/sites/default/files/documents/EU_Innovation_Hub_First%20Report%20on%20Encryption.pdf> accessed 10 June 2024, 23.

[10] Directive of the European Parliament and of the Council of 31 May 2024 on the mechanisms to be put in place by the Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2024] OJ L/1.

[11] Mixing services, for example, are thought by many to be a means through which money laundering occurs, but they will not be discussed in that lens here, rather only with reference to patrimonial preventive measures.

this debate in the appropriate section, but its aim is not to delve deep into such discussion. Because patrimonial preventive measures will be applied only where the origin of the asset is illegal, the analysis will be made on the basis that the assets involved were illegally obtained.

This article aims to assess whether the Italian patrimonial preventive measures are capable of serving as an equally effective instrument when faced with cryptocurrencies. This will be achieved by first describing blockchain technology as the underlying means through which cryptocurrency operates, in order to understand what a transaction using cryptocurrency looks like. This is followed by an analysis of the patrimonial preventive measures, their criteria of application and content. Lastly, the two areas of technology and law will be discussed together to culminate in an encompassing query: to what extent are patrimonial preventive measures in the context of Italian antimafia law compatible with cryptocurrency? As the analysis will show, though the law is in theory applicable to the technology, the latter's characteristics do not allow a smooth application of the law as is.

2. Understanding Blockchain Technology and Cryptocurrency Transactions

2.1 Crypto-assets and Cryptocurrency

At EU level, crypto-assets are defined within the Regulation on Markets in Crypto-assets (hereinafter MiCA Regulation), as 'a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology'.[12] However, the term 'crypto-assets' refers to a wide range of digital assets. Its definitions are varied and there is no one settled illustration for it internationally. This paper will consider the European definition: digital assets which are recorded on some form of a distributed ledger, secured with cryptography, that are not issued by a central bank and which may be used as a means for exchange or investment.[13]

The first crypto-assets were bitcoin, introduced as an alternative payment method to traditional central bank-issued currencies. Due to the cryptographic technology they make use of, they are referred to as a type of cryptocurrency, which in turn is a type or form of crypto-assets. More specifically, cryptocurrency consists of virtual currency, a means of non-physical payment, existing strictly in its digital form.[14]

[12] Regulation 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA Regulation) [2023] OJ L150/40 art 3(1)(5).

[13] Robby Houben and Alexander Snyers, 'Crypto-assets: Key Developments, Regulatory Concerns and Responses' (Policy Department for Economic, Scientific and Quality of Life Policies 2020) <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648779/IPOL_STU(2020)648779_EN.pdf> accessed 1 April 2023.

[14] Ola M Tucker, *The Flow of Illicit Funds: A Case Study Approach to Anti-Money Laundering Compliance* (Georgetown University Press 2022) 39.

Cryptocurrencies are peculiar due to the use of cryptographic technology known as blockchain technology.[15]

2.2 Blockchain Technology

Blockchain technology is a term used to describe a computing-distributed, decentralised ledger that is shared by more than one entity and is capable of record-keeping information.[16] A simple way to grasp this concept is in reference to its terminology, which suggests it can be visualised as a stack of blocks. It starts with its foundation, which is known as the genesis block.[17] The latter consists of the block whose data was embedded first at the time the blockchain started.[18] On top of this bedrock lie any number of blocks that are interconnected and reference each other, because each block contains a 'block hash', or a block reference number, of its previous parent block.[19] Each block is a container of information, which can be unrelated or form a distinct group.[20] Since its development in 2008, blockchain technology has had two main applications: storing records in a secure manner on the one hand; and carrying out transactions on the other.[21]

2.2.1 Creation of Blocks

The process of block creation, also known as 'mining', consists of registering a new transaction on the public distributed ledger.[22] Before this can take place, however, a transaction must be propagated through the network, in order for all participants of the network to become aware of when a new block needs to be created. Let us consider the example of Bitcoin to explain this process. Whenever a system, which could be a wallet, a server or a desktop application, participates in the network, it is considered a 'node' (a Bitcoin node in this case). When a new transaction is emancipated through, for example, a wallet, it will be sent to any node of the network.[23] If this transaction is received by a node which recognises it as a new transaction, it will forward it to all other nodes to which it is connected. This is known

[15] Niels Vandezande, *Virtual Currencies: A Legal Framework* (Insertia 2018) 54.

[16] Christina Cornejo and Stacey Johnson, 'Understanding Blockchain: from Mediaeval origins to modern applications' in Sandra Hirsh and Susan Webreck Alman (eds), *Blockchain* (ALA Neal-Schuman 2020). Its origins can be traced back to the name Satoshi Nakamoto, thought to be its developer or in fact group of developers, who created this peer-to-peer method of exchanging electronic currency.

[17] Andreas Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* (O'Reilly Media Inc 2017) 196.

[18] Imran Bashir, *Mastering Blockchain: Distributed Ledger Technology, Decentralization and Smart Contracts* Explained (Packt Publishing 2018) 19.

[19] Antonopoulos (n 17) 195.

[20] Cornejo and Johnson (n 16).

[21] Sudeep Tanwar, 'Introduction to Blockchain Technology' in Sandeep Kumar Panda, Ajay Kumar Jena and Santosh Kumar Swain (eds), *Blockchain Technology: Applications and Challenges* (Springer 2021) 4.

[22] Antonopoulos (n 17) 25.

[23] ibid.

as the ‘flooding technique’.[24] Essentially, a transaction will rapidly propagate through the peer-to-peer (P2P) network, reaching many nodes. While at this stage a large percentage of nodes in the network will have become aware of the new transaction, it has not yet become part of the blockchain. For that to occur, the transaction must be verified and then mined, hence included in a new block.[25] Mining has two main purposes. First, it serves to validate the transactions and provide security by rejecting malformed ones. Second, it serves to create new bitcoin in each new block, similarly to a central bank printing new money.

The reason for the first purpose of providing security to the system is that mining is the mechanism which concretises the decentralised nature of the blockchain. In fact, mining is what enables the network consensus in lack of a central authority. This is due to the incentive scheme that ensures miner nodes supply the currency, while maintaining the security of the network. In essence, miners compete with each other to solve a complex mathematical problem, the solution of which is known as ‘proof of work’ (PoW).[26] When a miner node has solved the PoW algorithm, it has earned a reward. Rewards can come in two forms: new coins which are created with each block; and transaction fees in the form of a surplus of bitcoin. The existence of these rewards ensures that many miner nodes compete to mine a new block, hence register the new transaction on the blockchain, and that the public ledger is correctly updated with the new information.[27]

2.2.2 Main Characteristics

The blockchain has been characterised above as a ‘distributed’ and ‘decentralised’ ledger. Distributed computing can be described through the image of different independent computers existing in different locations, interacting and coordinating among themselves in order to appear as a single entity to the end-user.[28] If we consider a spider web, each node that forms at intersections of the single strings could be a computer, but could also take the form of virtual machines, containers and even physical servers.[29] In essence, a distributed ledger is a ledger that is spread across the nodes of the network and each of these has a complete copy of said ledger.[30] The number of nodes that make up the spider web becomes quite significant if we consider the concept of decentralisation: in the blockchain there is no single central authority; rather, the nodes are all capable of sending and receiving data in the interconnected network independently.[31] Such independence in the context of a distributed system may sometimes empower nodes to act faulty or even

[24] ibid.

[25] Antonopoulos (n 17) 26.

[26] Antonopoulos (n 17) 27.

[27] Antonopoulos (n 17) 28.

[28] ibid.

[29] ibid.

[30] Bashir (n 18) 17.

[31] ibid.

maliciously.[32] In any case, if a node acts unexpectedly, due to misleading data, it is denominated a 'Byzantine node'.[33]

Another inherent characteristic of blockchain is its immutable nature. This is because data can only be added in a sequential fashion.[34] This means that the further down the blockchain, the more the platform is settled and the probability of change is so low that in practice it is considered immutable.[35] This immutability is intrinsic to the previously stated decentralisation, because changes of the ledger cannot occur without agreement by the majority of the network.[36] The need for consensus in order for any update to occur makes the blockchain a self-sufficient mechanism that ensures the ledger remains immutable. Any such update is therefore facilitated by consensus algorithms, which vary based on the type of blockchain being used.[37] As the very name suggests, a consensus mechanism consists of steps that the nodes in a network take to agree on a suggested outcome.[38] Bitcoin's blockchain uses a consensus algorithm known as proof of work (PoW).

2.2.3 Public Key Cryptography

Cryptography is a branch of mathematics used in computer security.[39] Cryptographic proofs such as digital signatures are used extensively when dealing with cryptocurrencies.[40] This concept is a crucial one in order to grasp the functioning of cryptocurrency transactions. Taking the example of Bitcoin, public key cryptography is used to generate a pair of keys − one public and one private − which are necessary for a transaction to occur.[41] This type of cryptography is referred to as 'asymmetric cryptography' due to the nature of the relationship between the two keys: the public key is used to generate an address, and the private key provides a proof of ownership of said address.[42] A simple analogy is one that compares the public key to a bank account and the private key to a PIN: the former is, as the name suggests, available to all, and the latter is only known to the bank account holder and is used to enable the desired transactions.[43] The private key will be generated at random by an algorithm and will be used to create the digital signatures, while the public key will be the address to which and from which transactions develop.[44]

[32] Bashir (n 18) 12.
[33] ibid.
[34] Bashir (n 18) 17.
[35] Antonopoulos (n 17) 196.
[36] Cornejo and Johnson (n 16) 12.
[37] Bashir (n 18) 35.
[38] ibid.
[39] Antonopoulos (n 17) 56.
[40] ibid.
[41] ibid.
[42] Bashir (n 18) 80.
[43] ibid.
[44] Bashir (n 18) 36.

2.2.4 Mixing: A Legal Practice

As previously mentioned, the public and decentralised nature of blockchain allows for inherent transparency as it pertains to the history of transactions on the ledger. Such transparency will make all confirmed transactions publicly available.[45] In order to preserve some transaction-related privacy, users may turn to so-called mixing services, or tumblers. Keeping with the example of Bitcoin, any owner of the cryptocurrency can make use of the Bitcoin mixer service, which acts as an intermediary between the sending and receiving of addresses.[46] The mixer is an online service which, for a fee, acts as a pool, collecting Bitcoin deposits from all users who make use of it. Any user who has contributed to the pool, and wishes to withdraw the amount first incorporated, will receive the same amount, instead composed of pieces of bitcoin from other users of the mixer service. By combining one user's cryptocurrency with that of many others, the currency provided at origin will present a different transaction history, ultimately increasing its anonymity.[47] The service will have removed the visible link between addresses during a transaction, given that the pool size (i.e., the amount of transactions and addresses involved thereof) is large enough.[48] Due to the higher degree of protection afforded to an individual user, mixing services are often used to obscure illegal transactions.[49]

2.2.5 In Practice: an Example

The following example illustrates how a legal transaction using Bitcoin would occur in practice. Firstly, a user would open a wallet, which may be hosted (if it is through a service provider), or alternatively un-hosted (if controlled by the user themselves).[50] The wallet generates a private key, which is stored thereof. Each wallet will hold a balance of units of cryptocurrency, in this case units of bitcoin. In order for our user A to transfer X amount of bitcoin to receiving wallet B, B will present the public key, hence the address at which they desire to obtain the balance.[51] Our user will then set up the transaction in their wallet, from their own address, to that of B. User A then signs the transaction using their own private key and it will be broadcast throughout the network, using a flooding algorithm.[52] For the transaction to then become part of the blockchain and registered on it, a miner node will compete with many others to solve the mathematical problem, obtaining a PoW solution.[53] Once this has taken

[45] Tucker (n 14) 139.
[46] Tin Tironsakkul, Manuel Maarek, Andrea Eross and Mike Just, 'Tracking Mixed Bitcoins' (2020) SSRN <http://dx.doi.org/10.2139/ssrn.3701657> accessed 4 April 2023, 1.
[47] Tucker (n 14) 141.
[48] Matthias Nadler and Fabian Schär, 'Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers' [2023] *Federal Reserve Bank of St Louis Review* 1, 2.
[49] ibid.
[50] Federico Paesano, 'Following the Virtual Money: Investigating Crypto-based Money Laundering and Confiscating Virtual Assets' in Jay Liebowitz (ed), *Cryptocurrency, Concepts and Applications* (CRC Press 2023) 137.
[51] ibid.
[52] Bashir (n 18) 151.
[53] Antonopoulos (n 16) 27.

place, the transaction will be included in a new block and added to the public ledger. This transaction will be public on the blockchain, meaning that the public addresses permit some traceability: anyone on the blockchain will see that there has been a transaction from A to B. Of course, their identity may still be protected by addresses, which effectively act as pseudonyms.[54] If A and B do not want to risk their transaction being traceable, they may make use of a mixer service.

3. Patrimonial Preventive Measures in Italy

3.1 Origin and Nature

Preventive measures, as the very name suggests, are measures which may be imposed *ante* or *praeter delictum*; or: when a person has not yet been condemned of a crime, or if a crime has not even been committed.[55] They are thus also known as non-conviction-based measures, as they are imposed prior to a criminal conviction.[56] They may be personal or patrimonial. The former refers to the physical liberty of the person, and the latter to his or her economic freedom and assets. While the scope of persons against whom the measures may be applied goes beyond that of persons involved in organised crime, the measures are central to the antimafia response. Therefore, let us first frame preventive measures in the antimafia context.

Though principal to combating mafia today, they existed long before the mafia phenomenon was even known as such. At first these measures were referred to as ‘misure di polizia’ (policing measures) and mostly targeted subjects considered dangerous for the public at large: persons such as idlers, vagabonds or bandits. The measures were not criminal norms, because their application was triggered by transgressions or misdemeanours, as opposed to crimes. They were instead part of administrative law, because they aimed to protect public safety.[57] In fact, the rationale behind them is that when delinquency shifts from the preparation phase of a crime to one of execution, public safety is at risk and the state, which should safeguard its public, holds the essential responsibility of preventing a crime from occurring.[58] During post-unitary times, preventive measures can be seen in the law on ‘brigantaggio’ (against brigands) of 1863, which allowed the imposition of domicile or political exile based on suspicion.[59] Once the Fascist regime obtained power, it saw

[54] Nadler and Schär (n 48) 1.

[55] Maria Francesca Cortesi, ‘Nota Introduttiva’ in Giorgio Spangher and Antonella Marandola (eds), *Commentario breve al Codice Antimafia e alle altre procedure di prevenzione* (Wolters Kluwer 2019) 9.

[56] For insight into non-conviction-based confiscation in other EU countries, see Jon Petter Rui and Ulrich Sieber, *Non-Conviction-Based Confiscation in Europe* (Dunker & Humblot 2015).

[57] Aldo Cimmino, *Le Misure di Prevenzione Patrimoniali Antimafia: tra Norme Interne e Prospettive Sovranazionali* (Key Editore 2019) 21.

[58] Cimmino (n 57) 75.

[59] Francesco Menditto, ‘Presente e futuro delle misure di prevenzione (personali e patrimoniali): da misure di polizia a prevenzione della criminalità da profitto’ (2015) *Diritto Penale Contemporaneo*

in preventive measures a tool of police control, taking advantage of the fact that merely indications of a possible crime occurring are enough.[60] In particular, with the Testo Unico di Pubblica Sicurezza (Unified Text on Public Safety) of 1926, those who manifested a deliberate intent to commit acts against the national, social and economic order of the state could be exiled. In 1931, this was further extended to political opponents.[61] The measures eventually became a useful instrument to tackle mafia-related criminal activities.[62]

The numerous murders in Sicily during the first mafia war, which began in 1962, together with inadequate judicial prosecution, which often ended with acquittal due to lack of sufficient evidence, forced a response.[63] That same year the parliamentary commission of investigation on the mafia phenomenon in Sicily was instituted.[64] The commission's first report was a series of legislative proposals and amendments, but the only welcomed proposition at the time was to extend the scope of personal preventive measures, to also apply against mafia suspects, with Law 575/1965.[65] Patrimonial measures were instead introduced in 1982, with Law 646, commonly referred to as Law Rognoni-La Torre. It is considered a Copernican revolution of the contrast to mafia organisations because the focus shifted from the person to their assets.[66] Like most antimafia laws, this legislation is the product of an emergency normative intervention. It was in fact only approved following two attacks, which killed the very proponent of the law, Pio La Torre, and the prefect of Palermo, General Carlo Alberto Dalla Chiesa.[67] The same law also introduces article 416-bis to the Criminal Code, which identifies the mafia phenomenon as a standalone, autonomously prosecutable crime.[68] A mafia association from then on is such where its participants make use of intimidation, of the association's ties and the deriving subjugation and silence, to commit crimes, obtain control of economic activities, favours, authorisations, public procurement or making unjust profits (such as

<https://www.penalecontemporaneo.it/upload/1463736128MENDITTO_2016a.pdf> accessed 20 April 2022, 5.

[60] ibid.

[61] Cimmino (n 57) 23.

[62] Cimmino (n 57) 48; this occurred mostly after the report of the Parliamentary Antimafia Commission of 1963.

[63] Francesco Menditto, 'Misure di prevenzione personali e patrimoniali e compatibilità con la Cedu, con particolare riferimento all'ampliamento dei destinatari delle misure e all'introduzione del principio di applicazione disgiunta' (anno) European Rights <http://www.europeanrights.eu/public/commenti/menditto_su_misure_prevenzione_e_cedu.pdf> accessed 2 June 2024, 4.

[64] Giuliano Turone, *Il delitto di associazione mafiosa* (Giuffrè Editore 2015) 17.

[65] ibid, 18.

[66] Cimmino (n 57) 48.

[67] The attack of 1982 killed Pio La Torre, Sicilian regional secretary of the political party PCI and member of the Parliamentary Antimafia Commission, and PCI politician Rosario Di Salvo. General Dalla Chiesa was killed in the massacre of Via Carini in Palermo, which saw two other victims, including his wife Emanuela Setti Carraro, and the protection officer Domenico Russo.

[68] Art 416bis Italian Criminal Code.

procuring others votes in elections).[69] This definition, together with the creation of patrimonial preventive measures, commenced a new season of contrast.[70]

Because all legislative initiatives to combat mafia associations came to be in the context of grave killings, the antimafia laws were enacted quickly and constituted a scattered landscape. That is why in 2011 the Antimafia Code (hereinafter AMC)[71] was developed to collect and organise the many laws targeting mafia-organised crime, dating back to 1965.

Italian antimafia law today is a framework composed of various instruments, inter alia a strict detention regime known as '41-bis', and the reliance on collaborators of justice. Preventive measures are merely one aspect of this *acquis*. Over time personal measures have lost their bite, especially given ECtHR scrutiny.[72] Patrimonial measures, however, remain central to the antimafia response, because attacking an association at the root of its purpose − the economic advantage − threatens its solid structure and can weaken it, or even demolish it. Despite their long history, preventive measures have always remained a topic of debate among legal scholars, particularly with regards to their legal nature. They cannot be considered punishments, as no crime has been committed or established; but, on the other hand, nor are they entirely administrative either. Therefore, a general understanding in literature is that preventive measures are hybrids: a mixture of substantive criminal law, administrative sanctions, and decriminalised offences.[73]

3.2 Criteria of Application

Though patrimonial measures were incorporated into the preventive system at a later stage than the personal measures, the two categories still share some overlap in their applicability. At their origin, in fact, patrimonial measures were implemented in accordance with the accessory principle: a patrimonial measure was only applied if associated with an already existing personal measure.[74] However, over time jurisprudence saw a shift from a method centred around the dangerousness of the person, towards one centred around the illegal acquisition of assets by a dangerous person.[75] Eventually a new principle was established: that of disjointed applicability of the personal and patrimonial measures, whereby the two categories are applied

[69] ibid.

[70] Cimmino (n 57) 48.

[71] Decreto legislativo 6 settembre 2011, no 159, 'Codice delle leggi antimafia e delle misure di prevenzione, nonché nuove disposizioni in materia di documentazione antimafia, a norma degli articolo 1 e 2 della legge 13 agosto 2010, n. 136' (D Lgs 159/2011).

[72] In *DeTommaso v Italy*, a violation of article 2 Additional Protocol was found due to the personal measure of imposing compulsory residence leaving too much discretion to the courts, and thus lacking foreseeability, see *DeTommaso v Italy* App no 43395/09 (ECHR, 23 February 2017).

[73] Antonio Balsamo, 'Soggetti Destinatari' in Giorgio Spangher and Antonella Marandola (eds), *Commentario breve al Codice Antimafia e alle altre procedure di prevenzione* (Wolters Kluwer 2019) 16.

[74] Menditto (n 59) 31.

[75] Menditto (n 59) 32.

independently of each other.[76] Nonetheless, due to their initial connection, the two share general criteria of application. Essentially the conditions of applicability of personal measures are also followed for a patrimonial assessment.[77]

Three general criteria pertain to the application of personal measures, of which only two are relevant in the case of patrimonial implementation. The first is that the subject must fall under one of the two categories of 'dangerousness' provided for by the legislator: generic and qualified. These two categories essentially delineate the subjects upon whom a measure can be imposed; this will be analysed further below.

The second criterion to be fulfilled is that the dangerousness must be concretely 'social' in nature. This is an element peculiar to the preventive system. Here, social dangerousness is the predisposition of a subject to commit a future crime. It is to be evaluated through a global consideration of the individual, including the persistence over time of illicit behaviour.[78] Where this assessment provides evidence that a particular vigilance on part of the authorities is needed in order to avoid the actual enactment of a crime, a preventive measure may be imposed.[79]

The third criterion to implement a personal measure is the concurrency of the dangerousness and the application of the preventive measure. This requirement exists to ensure that a personal measure is applied only at the time when the subject is actually dangerous. However, it does not translate to patrimonial measures, where in fact a measure may be imposed even after the death of the subject in question. Patrimonial measures do not require concurrency, because the past social dangerousness of the subject reverberates on the asset; and because the limitation of economic liberty under the Italian Constitution allows more restrictions than a measure restricting an individual's physical freedom.

3.2.1 Subjects of the Measures

Because the measures are intended to be imposed *praeter* or *ante delictum* and may have a punitive effect, it is essential to determine the precise categories of persons who can be affected. The category of generic dangerousness, often referred to as 'simple dangerousness', is articulated in article 1 AMC. Within this type of dangerousness, there are two behaviours that launch a preventive measure. Firstly, subjects who habitually live off of, at least partly, the proceeds of crime. 'Proceeds' refers to any economic advantage that the subject has obtained after committing a crime.[80] This behaviour is economic in nature, and allows for a relatively broad category of persons to be included: potentially those with conduct elusive to taxation

[76] ibid.

[77] ibid.

[78] Menditto (n 59) 23; Adriano Pirozzi, 'Il Procedimento Applicativo, Art 4 I Soggetti Destinatari' in Ranieri Razzante (ed), *Commentario al Codice Antimafia*, *D.Igs*. *6 settembre 2011*, *no 159*, *e successivi aggiornamenti* (Pacini Editore 2020) 7.

[79] Cass. Pen. sez. VI n. 12511 del 6 febbraio 2001.

[80] Balsamo (n 73) 17.

responsibilities.[81] Secondly, 'generic dangerousness' refers to a less economically centred behaviour, which includes individuals dedicated to the commission of crimes against the physical or moral integrity of minors, public health, security or tranquillity. This category covers several criminal conducts to be potentially considered, for example the repeated inobservance of a personal preventive measure. Because of the relatively wide articulation of this provision, many legal scholars have criticised generic dangerousness as being too vague. However, a recent judgment of the Constitutional Court limited this vagueness by eliminating a previously existing third type of behaviour: individuals who are habitually dedicated to illegal activities.[82] This is used to encompass those who are regularly involved with economically relevant criminal matters.[83] In either case, with all the instances described, factual evidence of these behaviours is required.

Qualified dangerousness, laid down in article 4 AMC, presents a much more detailed list of relevant behaviours. It explicitly refers to specific criminal offences, of which there must be suspicion. In contrast with regular criminal proceedings, the type and degree of proof required in the preventive system is not in need of elements of certainty, but factual circumstances that can be objectively evaluated and lead to the reasonable probability of the subject having committed those crimes.[84] The cited crimes include, among others, suspicion of being part of a mafia association as defined in article 416-bis Criminal Code.

3.3 Content of Patrimonial Preventive Measures

Patrimonial preventive measures are described under articles 20 and 24 AMC as two separate measures: 'sequestro' (sequestration) and 'confisca' (confiscation) respectively.[85] However, the two measures are interconnected; sequestration is often simply a first step towards imposing a confiscation measure.[86]

3.3.1 Sequestration

The preventive sequestration of a subject's assets may take place where the individual disposes directly or indirectly of those assets, and where the assets' value appears to be disproportionate in relation to the declared income or economic activity carried out by the individual.[87] In other words: if on the basis of sufficient indications there is reason to believe that those assets are either the result of illicit activities, or constitute their reuse. The 'result of' alludes to the economic advantages

[81] The mere occasional tax evasion is not enough on its own to prove dangerousness, if all the other elements of dangerousness are not fulfilled.

[82] D Lgs 159/2011 art 1(a); Corte Costituzionale Sentenza no 24 del 2019.

[83] Balsamo (n 73) 17.

[84] Cass. Pen. sez. II no 1023 del 16 dicembre 2005; Canino, in CED Cass., no 233169.

[85] D Lgs 159/2011 art 20; D Lgs 159/2011 art 24.

[86] Alessandro Parrotta, 'Le misure di prevenzione patrimoniali' in Ranieri Razzante (ed) *Commentario al Codice Antimafia D.Lgs. 6 settembre 2011, n. 159 e successivi aggiornamenti* (Pacini Editore 2020) 37.

[87] D Lgs 159/2011 art 20.

obtained directly from an illegal activity;[88] and the term ‘reuse’ refers to a more indirect correlation with illegal conduct, such as the reuse of assets to establish businesses.[89] The elements that indicate the disproportion are at this stage provided by the authorities who request the implementation of the patrimonial measure.[90] This is the reason why sequestration is said to be carried out *inaudita altera parte*, without the chance for the subject or any third parties to contrast them.[91]

The disproportion is to be assessed by looking at each asset of the subject’s patrimony at the time of the single obtainment of it.[92] It is not necessary for the application of the measure to prove a causal link between the dangerousness of the subject and the illegal origin of the assets. The rationale behind sequestration is merely to act preventively to momentarily freeze the illegally obtained assets and neutralise the dangerousness of their presence in the legal economy.[93]

The measure is carried out by the judicial police, irrespective of whether there are legal or personal rights of enjoyment of the asset.[94] If the assets in question are to be confiscated and there is a concrete risk that they will be dispersed, subtracted or alienated, their emergency sequestration may be requested.[95] This is when the sequestration takes place before the hearing. However, there is a temporal limitation to this requirement: if the emergency measure is not validated within 30 days from the request, it becomes null and void.[96] In non-emergency situations, in fact, a hearing is held where the subject can provide evidence of the legitimate origin of the asset. Within fifteen days of the hearing a decree is issued by the tribunal, which also determines the length of application of the measure: between one and five years.[97] Third parties who seem to be owners or partial owners of sequestrated assets are to appear before the tribunal within the thirty days following the sequestration, with motivated decree.[98]

3.3.2 Confiscation

No later than one year and six months after the assets that were sequestered have been registered with the judicial administration, the tribunal must deposit a decree of preventive confiscation.[99] Otherwise, the sequestration becomes null. However, there is the possibility to extend this period for another six months if the patrimonial

[88] Stefano Finocchiaro, ‘La confisca e il sequestro di prevenzione' in Enrico Mezzetti and Luca Luparia Donati (eds), *La Legislazione Antimafia* (Zanichelli Editore 2020) 9.

[89] ibid.

[90] Menditto (n 59) 37.

[91] Menditto (n 59) 36.

[92] Cass. sez. IV no 37166 del 17 settembre 2008.

[93] Parrotta (n 86) 29.

[94] D Lgs 159/2011 art 21(1).

[95] D Lgs 159/2011 art 22(1).

[96] D Lgs 159/2011 art 22(2).

[97] Parrotta (n 86) 33.

[98] D Lgs 159/2011 art 23(2).

[99] D Lgs 159/2011 art 24(2).

investigations are particularly complex.[100] Following the sequestration, the subject and any third parties involved may and must provide appropriate proof that the assets are legitimately obtained and owned.[101] This can be done, for example, by showing the availability of legitimate amounts of money in a bank account, which were used to purchase the asset in question.[102] In the event that the legitimate origin of the assets cannot be produced, the confiscation decree will be issued by the tribunal and the assets in question will be confiscated indefinitely.[103] It was established first by jurisprudence and later codification in the AMC that assets which can be explained by occurrence of tax evasion are not properly justified assets.[104] It is most common to first apply sequestration and then confiscation, though the AMC does not prohibit a different order of application.[105] This means that assets could be confiscated without having been previously sequestered.[106]

A debate exists in doctrine with regards to the real nature of preventive confiscation: on the one side it is a preventive measure; on the other it is regarded by many as a sanction disguised as a preventive measure.[107] While the details are outside the scope of this paper, it should be noted that, according to the law, confiscation is considered preventive in nature because the measure removes from the subject a part of their patrimony which is illegally generated in the first place. Differently, a penal confiscation goes beyond this limit and exceedingly subtracts assets from the patrimony as a form of punishment.[108]

3.3.3 Confiscation and Sequestration ‘by Equivalent’

If it is impossible to proceed with the sequestration because the subject does not dispose of the illegally obtained assets, directly or indirectly, authorities may request a sequestration by equivalent.[109] This measure consists of sequestering assets of corresponding value to that of the assets no longer available to the subject.[110] This means that the illegitimacy of the equivalent asset is not a necessary presumption for application of the measure. It simply must have an equal value. The purpose of these measures is to still deprive the subject of the profits of criminal activity, by engraving the assets available to the subject, even where the actual result, or reuse of illegal profits is not obtainable.[111] In 2017 a reform changed the assumptions necessary for application. Until then, the subject must have had the aim of dispersing and

[100] ibid.

[101] Parrotta (n 86) 35.

[102] Menditto (n 59) 37.

[103] D Lgs 159/2011 art 24(1).

[104] ibid.

[105] Parrotta (n 86) 37.

[106] Cass. Pen. Sez. Unite no 20215 del 23 febbraio 2017.

[107] Finocchiaro (n 88) 25.

[108] Finocchiaro (n 88) 30.

[109] Valerio De Gioia and Gian Ettore Gassani, *Codice Antimafia e delle Misure di Prevenzione* (La Tribuna 2020) 24.

[110] D Lgs 159/2011 art 25.

[111] Cass. Pen. sez. Ter. no 182 del 27 gennaio 2011, 2.

concealing the assets from authorities. Instead, currently the only requirement is that it is no longer possible to proceed with the direct sequestration of the assets due to the lack of their availability to the subject.[112] The introduction of this measure has been proven useful in cases of money laundering or reuse of those illegal assets that interrupt the correlation between the asset and the crime.[113]

4. The Compatibility of the Technology with the Law

Crypto-assets are a double-edged sword. The pseudo-anonymity of the underlying technology can be useful for those law-abiding citizens seeking further privacy protection, but it can also enable those trying to evade the law. For this reason, they are often at the centre of a polarising debate. On one side of the discussion are those who believe crime on the blockchain is the exception, not the rule, and that the technology has been unjustly tarnished.[114] In a way, because all transactions are immutably recorded on the publicly available ledger, it could even be deemed less anonymous than traditional currency, especially cash.[115] On the other side are those who think of cryptocurrencies as the 'Wild West of the internet'.[116] As reported by Europol, illicit activity on the blockchain is decreasing, which is of course a positive datum.[117] At the same time, most cybercrime ransomware is carried out with cryptocurrency payments.[118] The decentralised nature of blockchain renders it more resistant to traditional forms of crime prevention, where a single authority could monitor and enforce rules.[119] Adopting a negative view on technology appears both unrealistic in light of the new legal steps taken by the European Commission, and also unnecessary in light of desired innovations and ongoing law improvements, also in other disciplines.[120] In the midst of these developments, the question whether or not preventive measures also cover cryptocurrency requires an analysis focused on its

[112] Legge 17 ottobre 2017 no 161 Modifiche al codice delle leggi antimafia e delle misure di prevenzione, di cui al decreto legislativo 6 settembre 2011, no 159, al codice penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale e altre disposizioni. Delega al Governo per la tutela del lavoro nelle aziende sequestrate e confiscate, art 5.

[113] Cafiero de Raho (n 3) 114.

[114] William Magnuson, *Blockchain Democracy Technology*, *Law and the Rule of the Crowd* (Cambridge University Press 2020) 98.

[115] ibid.

[116] Magnuson (n 114) 97.

[117] Joint Working Group on Criminal Finances and Cryptocurrencies, 'Seizing the opportunity: 5 recommendations for crypto asset-related crime and money laundering' (2022) Europol <https://www.europol.europa.eu/cms/sites/default/files/documents/2022_Recommendations_Joint_Working_Group_on_Criminal_Finances_and_Cryptocurrencies_.pdf> accessed 10 June 2024.

[118] See reports such as those provided by ChainAbuse, <https://www.chainabuse.com/chain/BTC?page=0&filter=RANSOMWARE>.

[119] Magnuson (n 114) 98.

[120] The European Commission has published a proposal for a Digital Euro, see Commission, 'Proposal for a Regulation on the establishment of the digital euro' COM(2023) 369 final.

illicit use. Evidently, this does not mean that all use of cryptocurrency is illegal and negative for the legal economy.

This section aims to explore whether, from a legal perspective, patrimonial preventive measures, as they are, are sufficiently effective to sequester and confiscate cryptocurrency assets. In particular, the theoretical compatibility is first contemplated, to determine if the virtual nature of cryptocurrency presents an obstacle to application in principle. To determine this preliminary theoretical question, the definition of 'cryptocurrency' under Italian law must be considered. This national delineation is inevitably influenced by EU legislation. Then, three critical points will be identified as arguable impediments to the adoption of patrimonial preventive measures: the object of the measures; the blockchain's pseudo-anonymity; and mixing services.

4.1 Theoretical Compatibility

4.1.1 European and National Definition

When in 2017 Italy transposed the IV Anti-Money Laundering Directive, it expanded the scope to include 'virtual currencies', anticipating the European legislator who then incorporated them into Directive V.[121] The implementation occurred with Legislative Decree no 90 of 25 May 2017. This law defined virtual currencies as a digital representation of value, which is neither emitted nor connected to a central bank or public authority, and which is used as a means of exchange for the purchase of assets and services, transferred, archived and negotiated electronically.[122] This definition largely coincides with the later EU definition, which did not limit the purpose of virtual currency to purchase of services or assets; rather, it remained broader.

However, with the entry into force of the MiCA Regulation, the definition that becomes relevant for our assessment is that of crypto-assets. MiCA describes them as digital representations of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology.[123] Hence, the scope was expanded even further in order to ensure as far as possible that future technological changes will remain compatible with the law. As a regulation, MiCA is directly applicable in the Italian legal order and, though a definition in a criminal law sense is lacking, this definition is the one relied upon. However, responses from Italian

[121] Council Directive (EU) 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, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC [2015] OJ L141.

[122] D Lgs 25 May 2017 no 90, art 1.

[123] MiCA Regulation, art 2(1)(5).

legal doctrine with regard specifically to preventive measures are yet to come at the time of writing.[124]

4.1.2 Compatibility and Case Law

The above-described broadness of scope in defining cryptocurrency is advantageous for the application of patrimonial preventive measures as it conforms well to the equally broad scope of application of sequestration and confiscation. In fact, the law itself does not refer to any limitations as to what can be considered a 'bene' (asset) that can be sequestered. It only requires that the assets in question are the result of illegal activities.[125] The Court of Cassation has established that sequestrable assets are also ones which have been purchased with sums of currency that were illegally obtained.[126] There must be a causal link between the crime and the reuse of the illicit profits, and the crime must be subjectively attributable, through reasoned indications, to the author of said crime.[127] This means that the subject's cryptocurrency may be sequestered or confiscated not only if the cryptocurrency was a means of payment for the commission of a crime or if the assets were exchanged from illegally obtained fiat currency, but also if a physical asset is purchased through illegally retrieved cryptocurrency.

The law is formulated in such a way that the illegal origin of the asset is a necessary requirement, but that the central aspect of the preventive measures is rather the dangerousness of the subject and therefore presents requirements strictly related to the subject. Testament to this statement is the existence of the above-described sequestration 'by equivalent', where the sequestration of a different, legally existing asset is possible in the absence of the illegally obtained one. The only limitation to sequestration by equivalent is that the legal asset must be of equal and corresponding value to the illegal one, to avoid the risk of over confiscation.[128] Often the asset that is sequestered will be property such as real estate. However, it need not necessarily be physical in nature and cases of sequestered bank accounts are possible and used regularly.[129] While the blockchain differs from a legal bank account with a central authority involved, it is similar in that both could be considered virtual in nature.

Although case law which directly addresses the applicability of patrimonial measures to cryptocurrency has yet to appear, there have been some judgments in the lower courts which indirectly accept the compatibility. An example is a case from 2021 where the preventive sequestration of profits of crime in the form of bitcoin was ordered.[130] The person concerned had self-laundered proceeds from prostitution, by

[124] The response of the Italian legislator is not needed due to the direct applicability of European Regulations, which do not require a national implementation to have an effect.

[125] D Lgs 159/2011 art 20.

[126] Cass. Pen. sez. Unite no 10280 del 6 marzo 2008.

[127] ibid.

[128] Cass. Pen. sez. Unite no 26654 del 27 marzo 2008.

[129] Parrotta (n 86) 29.

[130] Cass. Pen. sez. II, no 2868 del 7 ottobre 2021.

transferring them to foreign cryptocurrency exchangers.[131] The public prosecutor had requested the preventive sequestration, or alternatively sequestration by equivalent, of the proceeds of self-laundering. The Court of Cassation did not find the requested application of a preventive measure inadmissible merely due to the assets being virtual in nature.

Therefore, cryptocurrency is not to be excluded as a sequestrable asset simply because of the virtual nature of the currency. As long as the illicit origin of the asset or proof as to the illicit asset's use as a payment for a legal asset is established, the patrimonial measures may be invoked against the subject. This confirms the theoretical compatibility of cryptocurrency and patrimonial preventive measures.

4.2 Critical Points of Incompatibility

Despite compatibility in principle, there are arguably characteristics of the technology that become an impediment to smooth applicability of the law, or that require more nuances to be made. Three such elements are examined below.

4.2.1 The Object of the Measures

Until now, there have been few cases involving the sequestration of bitcoin (i.e., of the cryptocurrency itself). Cryptocurrency as the object of sequestration, however, raises two concerns. The following hypothetical case illustrates these complications. Suppose the Italian police have reasoned suspicions to believe subject A is part of a mafia association. Therefore, A falls into the category of qualified dangerousness under article 4(a) AMC. Investigators hold factual elements of proof of a transaction having taken place on the blockchain. This is a payment in bitcoin for carrying out a drug trafficking exchange. The public prosecutor wants to issue a request for the preventive sequestration of the illegally obtained bitcoin.

The first issue is that sequestering bitcoin itself fails to fulfil the very aim of sequestration. The cryptocurrency is simply data, and its sequestration alone would not constrain subject A's access to it. Where with another asset such as fiat currency, locating the asset and linking them to the originating criminal activity is enough, with cryptocurrency a transaction can be initiated by anyone possessing the address's private key, and locating it is not sufficient.[132] In fact, if subject A holds possession of the private key, he or she can always move the currency elsewhere, sell it or exchange it for fiat currency.[133] Essentially, the police cannot consider the cryptocurrency under their control, unless they possess the private key.[134] Hence, sequestration should involve the attainment of the private key to the relevant address.

[131] ibid; the exchangers would receive large sums of fiat currency in euros through wire transfers, and would convert the money into bitcoin.

[132] Paesano (n 50) 137.

[133] Antonio Rosato, 'Profili Penali delle Criptovalute' (2021) Diritto Penale Globalizzazione <https://www.dirittopenaleglobalizzazione.it/wp-content/uploads/2021/01/Profili-penali-delle-criptovalute-Rosato-Antonio.pdf> accessed 20 April 2023, 141.

[134] Paesano (n 50) 137.

Obtaining the private key may give rise to a further complication, not explored in detail in this paper, which is the possibility that the subject has encrypted the private key to further secure it. It may take a considerable amount of time and resources to decrypt the private key. It is possible that a complicated encryption will take too long, giving the subject a chance to move the assets before investigators can decrypt it. It should be considered that even if this should happen, subject A may not be the only person who has knowledge of the private key. This is not far-fetched if the case at hand considers a criminal organisation, where different individuals act at different levels. If A has shared the private key among other participants of the association, even if law enforcement authorities have obtained the key from A through preventive sequestration, any of the collaborators may move the cryptocurrency and retain possession before the execution of the preventive measure. This makes the knowledge of the private key on its own not sufficient to properly execute the preventive measure. Therefore, it would be most appropriate to enact the unavailability of the asset to subject A through sequestration of the private key, and the subsequent transfer of the cryptocurrency to a police-controlled and secure address.

It is good practice for the police to then set up the new wallet using an encryption mechanism. This works as a second password to access the real private key, which in itself cannot be changed from the original. This encryption can be done at any point in time, meaning investigators could ensure the protection of the cryptocurrency after they have transferred it to the new wallet, adding a further layer of security. This is a necessary and crucial step in the process of ensuring protection of the assets, because the original private key will not be rendered useless. This will work, so long as the process is carried out before any other accomplice can remove the funds themselves from the original address.

It should be noted that an additional complication arises at the stage of locating the address and obtaining the private key. There is a factual difference between a hosted and an unhosted wallet.[135] In the former situation, a crypto-asset service provider will be involved. This means that a third party is holding the private and public key for its user. If the user loses the private key, the provider may help them retrieve access to their wallet. Similarly, authorities could request the private key from the provider and easily obtain access to the wallet, even preventing access, as with a regular bank account.

Recently, this has been further substantiated by the Transfer of Funds Regulation, which requires the obtaining of identification information by crypto-asset service providers of their wallet holders, with the aim of tracing the transfers of crypto-assets. For this to occur, at least one of the addresses must be hosted.[136] This Regulation in fact excludes from its scope transactions between unhosted wallets.

[135] Paesano (n 50) 134.

[136] Regulation (EU) 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 [2023] OJ L150/1.

With unhosted wallets, only the account holder has access and is aware of the private key, and no one is capable of retrieving the cryptocurrency of that address, unless they somehow gain possession of the private key. Even if this does happen, it could be that the subject has encrypted their private key to add a further layer of security, which authorities would need to decrypt before they can make use of. If there is no service provider to facilitate this, the process clearly becomes more strenuous. In most cases, a record of the private key may be dispersed, in whole or in part, across the individual's devices, which may need to be searched to obtain it.[137]

The second problematic aspect of sequestering the cryptocurrency is that the extreme volatility of the cryptocurrency markets needs to be taken into account.[138] A way around this would be to convert the bitcoin into fiat currency, in order to preserve its initial value at the moment of sequestration.[139] However, this raises questions of arbitrariness of power by the judicial police, who are only in charge of retrieving the illegal profit, without changing its value or form.[140] Although this issue has attracted discussion in the literature, this precaution is not necessary as the situation is arguably no different from any other asset which is depreciating while in the custody of law enforcement.

4.2.2 Pseudo-anonymity

Blockchain's characteristic of granting its users pseudo-anonymity presents an incompatibility with the criteria of application of patrimonial preventive measures. As described above, the application of a measure is strictly intrinsic to the establishment of a subject's dangerousness and social dangerousness, as well as to the need for this subject to dispose directly or indirectly of the asset in question.[141] When dealing with bitcoin, however, it cannot be established with absolute certainty that a person is the one who controls a bitcoin address. This does not necessarily pose issues with the dangerousness requirement, because similarly to the hypothetical scenario described above, there may be other physical world-related factual circumstances that allow its establishment. However, obtaining proof of the direct or indirect disposability of the asset may be difficult in such a scenario. If the identity of a dangerous subject cannot be matched with the identity behind a bitcoin address, the criteria of application of preventive measures risk losing their legal certainty and effectiveness.

At the stage of sequestration, the burden to demonstrate the disposability is on the authorities.[142] With a physical world example, if subject A's asset of sequestration is a house suspected of being purchased with illegal profits, authorities may prove A's disposability of the house, possibly through its purchase agreement. Or even more likely, the valid identification required to open a bank account may be used to link the

[137] Paesano (n 50) 137.
[138] Rosato (n 133) 28.
[139] Rosato (n 133) 142.
[140] ibid.
[141] D Lgs 159/2011 art 20.
[142] Menditto (n 59) 36.

financial transactions using the account to the real identity of its holder. Such instances would be considered proof of disposing of the asset *directly*. The legislator included indirect disposability to allow the measures to be imposed even in situations where aliases, or figureheads, are being used to disguise the real identity of the asset owner. Nonetheless, there is still the need for proof of disposability, even if indirect. Furthermore, if the assets are formally registered as owned by third parties (not the subject deemed dangerous), the judge holds the obligation to explain the reasons for the presumed fictional registration in the name of the third party.[143] The proof requires thus even more rigour than with direct disposability.[144]

When determining how this same process of obtaining proof of disposability works with bitcoin, the distinction between hosted and unhosted wallets becomes relevant once again. With a hosted wallet, in a best-case scenario, a crypto-asset service provider will have registered the person as the owner of a wallet, their identification will have been checked as required by the Transfer of Funds Regulation, and it is that person who will be deemed dangerous. In this case, direct disposability would be proven quite easily, and the preventive measures may be applied. In the worst-case scenario with a hosted wallet, the person registered to formally have control of the wallet is not the person who has been deemed dangerous. That could mean that the person is being used as a third-party alias, similarly to the physical world example. In this case, indirect disposability would apply and it is then up to the prosecutor, through more traditional investigation techniques, to link the third person to the dangerous subject, and the judge must explain why there is reason to believe this is a formality and they are acting as a figurehead.

When a bitcoin address is created, an alphanumeric address is generated, which allows the sending or receiving of bitcoin. Any transaction involving this address is then recorded and visible on the public blockchain. It is such record-keeping that leads to the blockchain being described as 'pseudonymous'.[145] Bitcoin forensics may retrieve the IP addresses that carry out the activities.

For these reasons, some believe the blockchain to be inherently transparent, and its record-keeping nature to be a positive aspect, able even to help detect crime.[146] It has been argued that in some ways the blockchain is less anonymous than traditional currency.[147] This is true especially with cash. Where cash can be physically hidden, the public ledger will immutably and publicly display the transactions that have been made, not allowing the same haven that cash would. Where the owner of an address is known, as is the case with hosted wallets, all the transactions that said address has

[143] Menditto (n 59) 34.
[144] ibid.
[145] Bashir (n 18) 132.
[146] Tom Lyons and Ludovic Courcelas, 'Blockchain and Cybersecurity: a Thematic Report' (European Union Blockchain Observatory and Forum 20220) <https://www.blockchain4europe.eu/wp-content/uploads/2021/05/report_security_v1.0.pdf> accessed 18 May 2023, 18.
[147] ibid.

concluded can be traced. Even Europol has deemed the blockchain as an opportunity to investigate crime and gather intelligence, even confiscate illicit assets. A point to stress, though, is that it is only with the right tools, techniques and data that law enforcement can follow these assets. One of Europol's recommendations is to strengthen public–private cooperation when it comes to increasing capacity of investigative tools. This is in line with the overall tendency of what has been termed 'privatised surveillance', where companies are called upon to cooperate with the state for the purpose of fighting crime.[148] Whether this is a correct approach is outside the scope of this analysis, though it is indicative of where law enforcement action is possibly headed.[149]

With unhosted wallets, however, things are much more complicated. Disposability – direct or indirect – is harder to prove. That is because there is no link between the subject and the unhosted wallet. The owner, or the person who has access to that wallet, is the one who knows the private key. That could be the subject, or anyone else in the criminal group. Therefore, the fact that the public ledger records transactions does not necessarily link a specific person or identity to a wallet.[150] Unhosted wallets and the blockchain then provide anonymity which means criminals do not even have to resort to using third-party identities to disguise themselves. Disposability is then arduous to prove.

One way to do so would be to trace the IP address to find where that transaction occurred from. However, it is fairly easy to conceal an IP address, especially in the case of a structured criminal group, who can outsource technical expertise to their advantage, and likely conceal their steps to a considerable degree. It is in this particular case that identifying the subject or matching an identity is very difficult. Hence, the pseudo-anonymity of the blockchain is only useful from an investigative point of view, in the sense that the police could see that the assets went from point A to point B. These movements are not necessarily linked with an identity. If they occur through hosted wallets, where identification by a service provider is required, then the criteria of disposability can be fulfilled, either directly or indirectly.

However, if one wallet is unhosted, and even more so, where both wallets within a transaction are unhosted, connecting the transaction to a person and thereby proving disposability is quite difficult. That is where the built-in anonymity can be exploited by criminals wanting to act undisturbed. The disposability criteria are important for legal certainty, especially because this is preventive confiscation, not a punishment after a crime has been committed. Therefore, loosening that requirement might help overcome the technological obstacle, but it would undoubtedly damage the measures' legality and foreseeability.

[148] Christian Thönnes and Niovi Vavoula, 'Automated predictive threat detection after Ligue des Droits Humains' (Verfassungsblog, 12 May 2023) <https://verfassungsblog.de/pnr-threat-detection-ii/> accessed 20 June 2024.
[149] A similar instance is content moderation under the Digital Services Act.
[150] Magnuson (n 114) 104.

4.2.3 Mixing

If the pseudo-anonymity is problematic when faced with the disposability criteria, once mixer services are involved, the risks of total anonymity become increasingly prevalent. Imagine that subject A, after having obtained illegal profits, wants to protect the secrecy of the transaction even further by making use of a mixer service, thereby reducing the traceability of the transaction even further.[151] This will obscure the transactional history, cancelling the origin of the transaction and essentially laundering the illicit payment. Anonymity is then reinforced, given that the mixer service will allow the user to schedule their own withdrawals at randomised times and in randomised amounts. Additionally, the fact that the amount is withdrawn from a different address than the inputting one provides an extra layer of privacy to subject A. Together, all these elements restrict further the certainty that subject A will have been the one to carry out this transaction.

A second issue is that the practice of mixing frustrates the application of patrimonial preventive measures, as one of the requirements for its execution is not fulfilled. That is the requirement that the asset to be sequestered must be the result of illicit activities or the reuse of their profits thereof.[152] As per this requirement, in the hypothetical scenario, subject A's bitcoin would initially fall under the first category of assets derived directly from an illegal activity. However, where subject A makes use of a mixer service, the asset is laundered and its origin is arguably no longer a directly illegal one, as required by the 'as a result of' threshold. The asset will be consist of other users' bitcoin, eliminating the traceability which would reconnect the illegality of the initial drug trafficking. This leaves the second requirement of 'reuse' as the only possible one applicable to the mixed bitcoin. The cryptocurrency would have to be considered as an asset indirectly obtained from illegal activity. However, this threshold has until now referred to investments made into establishing other businesses or the purchase of other assets through those illegal profits.[153] A mixer service is neither a means of investment nor a purchase of other assets. Hence, the change in form and nature of the mixed cryptocurrency does not entirely align with the establishment of illegal origin of a sequestrable asset.

A final and further issue involves the disproportionality between the critical asset and the subject's patrimony. In fact, while the burden of proof to determine the legal origin of the asset lies on the subject, the public prosecutor must still, upon request of implementation, establish the disproportion.[154] This assessment requires looking at the subject's patrimony at the time of the single acquisition of the asset. However, if a mixer service is used and the subject obtains the asset's value at randomised intervals, for randomised, possibly smaller amounts, the disproportion will be more

[151] As described in Section 2.2.4, in return for a fee, the mixer service will provide them with the same amount of Bitcoin that they had inserted but emit it as smaller coins collected from a pool of clients of the mixer service.

[152] D Lgs 159/2011 art 20.

[153] Parrotta (n 86) 38.

[154] Menditto (n 59) 36.

difficult to prove. As opposed to one large sum of cryptocurrency reaching the subject's address, there will be multiple smaller amounts of currency that reach more than one address to which the subject holds the private key, making the transactional history much more difficult to reconstruct.

4.3 Recommendations and Conclusions

It has been argued that the sequestration and confiscation of cryptocurrency is in principle possible. However, in practice, three main technical features of cryptocurrency have been identified as incompatible with preventive patrimonial measures. Firstly, cryptocurrency as the sole object of sequestration is problematic to carry out. Secondly, the blockchain's pseudo-anonymity presents an obstacle to the fulfilment of the disposability criteria for applying the measures. Lastly, the use of mixer services presents a further impediment to the identification of the subjects, as well as a practice detrimental to pinpointing the illegal origin of the asset to be sequestered, and the determination of its disproportionality.

For European legislators who are looking at the Italian patrimonial preventive system to tackle organised crime, it is recommended that the three points of incompatibility found above are considered, and that other options within the preventive system are observed, to aid those inadequacies. One possible solution to the first incompatibility is that emergency sequestration under article 22 AMC is instead required for any sequestration with cryptocurrency as its object. In fact, for the solution described above, i.e., sequestering the private key, followed by the transfer of the assets to a separate wallet, to be successful, the process must occur before the subject or anyone else can remove the assets themselves. The requirement of emergency is that there is concrete risk of the assets being dispersed, subtracted or alienated.[155] Such circumstances would be entirely fulfilled due to how quickly this transfer can take place when cryptocurrency is involved. While this arguably undermines the whole purpose of having a separate provision for dire situations, the nature of the asset would warrant this intervention. Therefore, when the sequestration of cryptocurrency is ordered, the private key would be taken and used to transfer the assets before any hearing is held, not giving the opportunity to the subject to remove it.

Another possible solution to the hindrance of mixer services could be to apply the sequestration (and confiscation) by equivalent to all cryptocurrency-related measures. As described in section 2 above, this measure does not need the establishment of a link between the asset and the crime behind it. This renders such measures useful where the mixing services have obscured the transactional history of the cryptocurrency and no longer allow a clear link. This way the mixed cryptocurrency may still be sequestered as the 'equivalent asset' rather than the

[155] D Lgs 159/2011 art 25.

direct asset. A limitation to this solution is that the condition for applicability requires the actual illegal assets to be unavailable to the subject.[156]

Although the issue here arises because the assets are no longer available for the judicial police, this does not necessarily hold true for the subject themselves, who may still know the private key to the relevant addresses. Of course, the asset that is the equivalent object of sequestration may simply be a legal asset that is in no way related to the cryptocurrency or the blockchain and could be, for example, property of the subject that holds the same value. Therefore, it could be considered appropriate to apply sequestration (and confiscation) by equivalent, whenever cryptocurrency is concerned. Nonetheless, this would not necessarily solve the issue of having to prove disproportionality, which remains a requirement for the application of a patrimonial measure.

Neither of these possible solutions address all the points of incompatibility that have been raised in this article. European legislators are therefore encouraged to consider these options as a starting point from which to develop legislation more tailored to the technology.

From the above presented analysis, this paper draws three overarching conclusions. First, the object of sequestration (and confiscation) of cryptocurrency should entail more nuanced considerations: after obtaining the private key, the assets should be transferred to a secured wallet. Second, those European Member States that plan to create patrimonial preventive measures in their legal systems should consider, as a starting point, applying the conditions for emergency sequestration to any preventive measure involving cryptocurrency. Lastly, to overcome the complexities of mixing services, European legislators who want to implement patrimonial preventive measures should contemplate sequestration (and confiscation) by equivalent, through an AML-lens.

[156] ibid.