COMPUTER LAW & SECURITY REVIEW 49 (2023) 105829

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Beyond financial regulation of crypto-asset wallet software: In search of secondary liability

Tom Barbereau[a,*], *Balázs Bodó*[b]

[a] *Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, 29 Av. John F. Kennedy, Luxembourg*

[b] *Institute for Information Law (IViR), University of Amsterdam, Nieuwe Achtergracht 166, Amsterdam, the Netherlands*

ARTICLE INFO

Keywords:
Blockchain
Crypto-asset
Non-custodial wallet
Secondary liability
Decentralised finance

ABSTRACT

Since Bitcoin, the blockchain space considerably evolved. One crucial piece of software to interact with blockchains and hold private-public key pairs to distinct crypto-assets and securities are wallets. Wallet software can be offered by liable third-parties ('custodians') who hold certain rights over assets and transactions. As parties subject to financial regulation, they are to uphold Anti-money Laundering and Combating the Financing of Terrorist (AML/CFT) standards by undertaking Know-Your-Customer (KYC) checks on users of their services.

In juxtaposition, wallet software can also be issued without the involvement of a liable third-party. As no KYC is performed and users have full 'freedom to act', such 'non-custodial' wallet software is popular in criminal undertakings. They are required to interact with peer-to-peer applications and organisations running on blockchains whose benefits are not the subject of this paper. To date, financial regulation fails to adequately address such wallet software because it presumes the existence of a registered, liable entity offering said software. As illustrated in the case of Tornado Cash, financial regulation fails to trace chains of secondary liability. Alas, the considered solution is a systematic surveillance of all transactions.

Against this backdrop, this paper sets forth an alternative approach rooted in copyright law. Concepts that pertain to secondary liability prove of value to develop a flexible, principles-based approach to the regulation of non-custodial wallet software that accounts for both, infringing and non-infringing uses.

1. Introduction

On 31 October 2008, the paper *Bitcoin: A Peer-to-Peer Electronic Cash System*[1] was posted to a mailing list of cryptographers

* Corresponding author.
E-mail addresses: tom.barbereau@uni.lu (T. Barbereau), b.bodo@uva.nl (B. Bodó).

[1] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008).

https://doi.org/10.1016/j.clsr.2023.105829

and hackers. With it came the recipe for Bitcoin, a decentralised digital currency that leverages blockchain technology. After Bitcoin, developments in the space introduced other blockchains and corresponding digital currencies (aka. *altcoins*). Collectively, they are referred to as *crypto-assets*: a 'digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology'.[2]

One essential piece of software that allows users to easily hold and store crypto-assets are *wallets*. Technically speaking, wallets are not a storage of assets (like a physical wallet for fiat currencies); instead, a wallet denotes software that allows one to interact with a blockchain network through the management and storage of cryptographic identities – so-called, *keys*. There are two types of keys associated with a wallet, *public* and *private* keys. The public key serves as an address and identifier for other network participants. It is cryptographically linked to a private key, which should be treated as a confidential password, and is used to sign transactions plus grant access to the funds held in that account.[3]

The software which helps users store private keys and interact with blockchains can be issued and managed by a trusted-third party or as open-source software. The role of trusted-third parties, who act as service providers, is twofold. First, they implement and uphold security measures for the storage of private keys. Second, the actual on-chain execution of transactions is (automatically) handled by that provider on behalf of customers. Hence, wallet software plus corresponding services offered by a third-party are commonly referred to as *custodial*. This is because the private key is 'custodied' by its bearer, in this case the third-party.[4] Because these third-parties are considered by the regulators as financial service providers, they are required to follow Know-Your-Customer (KYC) standards and conduct due diligence checks on users – the cornerstone of anti-money laundering (AML) and combating the financing of terrorism (CFT) regulation.[5]

Wallet software issued without the involvement of third-parties implies that the management plus storage of private keys is delegated entirely to the user. Such wallet software is described as *non-custodial* (aka. *unhosted* and *unregistered*) wallets. As software, they are no more than a pair of private and public keys compatible with a particular blockchain, stored and used by their direct owner. The issuance of a private-public key pair is generated when the wallet is added as extension to a desktop browser (e.g., Metamask) or generated from some open-source software (e.g., MyEtherWallet). In all cases, users of non-custodial wallet software take upon themselves the burden to store the private key (or password); in turn, willingly exposing themselves to cyber-security risks.[6]

Non-custodial wallet software brings notable advantages as they are easily created and can be used at a low cost. They are the gateway to Decentralised Finance (DeFi) and other peer-to-peer applications that grew popular in use for low-cost, direct access financial services and products.[7] Since non-custodial wallets do not involve due diligence processes and are highly pseudonymous (i.e., the user identity is not attached to the key pair), they are popular for criminal undertakings. Individuals can create as many wallets as desired, easily launder money through them, and retain (relative) pseudonymity in the process and evade regulation.[8] Such wallet software was used by the North Korean hackers Lazarus Group to use crypto-asset mixers such as Tornado Cash.[9]

1.1. *Motivation and research question*

Because of their association to criminal activities, legislators began to grapple with non-custodial wallet software as early as 2018. The European Union, for instance, amended its anti-money laundering directives to account for crypto-assets and wallet service providers in the broad sense.[10] The global, coordinated efforts to regulate crypto-assets are led by the intergovernmental Financial Action Task Force (FATF). Each year, the FATF publishes a guidance document with a set of recommendations to tackle AML/CFT related crimes in the crypto-asset space. The latest 2021 FATF guidance includes a trivial footnote: the organisation claims to not be 'aware of any technically proven means of identifying the person that manages or owns an [non-custodial] wallet, precisely and accurately in all circumstances'.[11] Since there is no reliable technical way to enforce said AML/CFT regulations vis-à-vis non-custodial wallets, from a legal perspective their regulation remains controversial, irrespective of whether some or most of the non-custodial wallets are used for criminal motives.[12]

---

[2] European Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 2020 Article 3(1)(2) .

[3] Rui Zhang, Rui Xue and Ling Liu, 'Security and Privacy on Blockchain' (2020) 52 ACM Computing Surveys 1.

[4] Typical custodial wallet software providers are crypto-asset exchanges such as Binance and Coinbase.

[5] Dianna L Kyles, 'Centralised Control Over Decentralised Structures: AML and CTF Regulation of Blockchains and Distributed Ledgers' in Doron Goldbarsht and Louis de Koker (eds), *Financial Technology and the Law : Combating Financial Crime* (Springer International Publishing 2022) <https://doi.org/10.1007/978-3-030-88036-1_6>.

[6] Om Pal and others, 'Key Management for Blockchain Technology' (2021) 7 ICT Express 76.

[7] OECD, 'Why Decentralized Finance (DeFi) Matters and the Policy Implications' (OECD 2022).

[8] Kyles (n 5).

[9] U.S. Department of the Treasury, 'U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash' (8 August 2022) <https://home.treasury.gov/news/press-releases/jy0916>.

[10] See Directive (EU) 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 L 156, 1962018, p 43–74) 5.

[11] Financial Action Task Force, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (2021) para 105 <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf>.

[12] See Her Majesty's Treasury, Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022 - Response to the Consultation 2022.

The issue at hand is that financial regulation struggles with getting a grip on non-custodial wallet software offered without an intermediary which demands KYC checks and allows for AML/CFT enforcement. This observation aligns with past literature on the regulation of DeFi at large[13] and Decentralised Autonomous Organisations (DAOs) where the lack of legal footing (i.e., intermediaries) challenges the application of the law.[14] That being said, contrary to the crypto-libertarian ideologies, the difficulty to establish direct liability or problems of judicial enforcement does not automatically mean technological sovereignty, and the end of law as such. We observe that in cases of novel legal challenges posed by technologies which were engineered to evade law enforcement, public and private parties' quickly resort to alternative approaches, not least the creation of new corporate structures and legal narratives and fictions,[15] or new technological infrastructures and forensic tools.[16] Unfortunately, these efforts even extend to individual developers of open-source software being held liable. Currently, there are both civil and criminal cases in the wider blockchain space which try to establish the contours of legal obligations and liabilities of open-source software developers in relation to the uses of their software (more on that later).[17]

The inherent, *dual use* of non-custodial wallet software along with the challenge of regulating practices enabled by decentralised, open source, techno-social systems, begs the question whether the currently predominant regulatory regime – based on clear rules for intermediaries and systematically monitoring transactions – is indeed adequate. Does it have the necessary flexibility to address both, infringing and non-infringing use? What alternative approach might the law have?

1.2. *Approach and structure*

To address these questions, we begin with a socio-technical introduction of the technology and its use. It is followed by a doctrinal analysis of the present regulatory framework rooted in financial regulation. At last, we propose an alternative framework rooted in secondary liability. We analyse the possible contours of a secondary liability regime for financial regulation based on how copyrights are enforced in the digital environment. We follow this approach for three reasons. First, we expect that the similarities of the decentralised, open-source design of the technology which allows illegal uses, would lead to similar difficulties as well as solutions to how enforcement would work in the two cases. Second, the core claim of the article is that secondary liability is more suited to address and curb infringing use of non-custodial wallet software while permitting non-infringing uses. That suitability is argued on the normative basis[18] that secondary liability would achieve greater justice on the individual user's level and turn away from the prospect of systematic mass surveillance. Third, the pitfalls of secondary liability regimes in the copyright context should also serve as a warning for the possible difficulties the enforcement of financial rules, such as KYC and AML/CFT regulation could face. The scope of this work is limited on non-custodial wallets that are *software* (i.e., 'hot' wallets).

Financial regulation is not the first legal domain to encounter a decentralised technology, and the resultant emergence of illegal practices. In the past, copyright regulation dealt with secondary infringement following the emergence of Napster and its increasingly more decentralised successors, up until the fully decentralised BitTorrent and protocol-based piracy.[19] The history of copyright regulation and subsequent enforcement in the face of radically decentralised technologies offers insights that may be useful to understand possible developments in the world of blockchain.

The copyright wars taught us that efforts to enforce the law may trigger technological innovation which makes such enforcement increasingly difficult. It also turned out that though the endpoint of such innovation may be a radically decentralised infrastructure, in practice, few such systems are truly untouchable by law. Somewhere in the technology stack there will be a party which acts as a chokehold on the service as a whole, and which thus may serve as an ideal locus of enforcement. In the copyright domain subsequent lawsuits both produced increasingly decentralise file-sharing systems (up until the BitTorrent protocol), but they also slowly extended the list of potentially liable parties.[20] By now, file sharing is not addressed at the level of decentralised protocols, instead Internet Service Providers (ISPs), DNS service providers, open-source code repositories are all found liable if they don't comply with rightsholders requests to stop infringing activities.[21]

[13] Dirk A Zetzsche, Douglas W Arner and Ross P Buckley, 'Decentralized Finance' (2020) 6 Journal of Financial Regulation 172.

[14] JG Allen, 'Bodies Without Organs: Law, Economics, and Decentralised Governance' [2021] Stanford Journal of Blockchain Law & Policy <https://stanford-jblp.pubpub.org/pub/law-econ-decentralised-governance/release/2>.

[15] Chris Brummer, 'Disclosure, Dapps and DeFi' [2022] Stanford Journal of Blockchain Law & Policy <https://stanford-jblp.pubpub.org/pub/disclosure-dapps-defi/release/1>.

[16] Michael Fröwis and others, 'Safeguarding the Evidential Value of Forensic Cryptocurrency Investigations' (2020) 33 Forensic Science International: Digital Investigation 200902.

[17] A civil case in the UK will move forward to establish whether developers of open-source software used to establish bitcoin networks owe 'fiduciary duties' and 'duties of care' towards users. See Parkin, Darren. 2023. "Court of Appeal Orders Tulip Bitcoin Case to Go to Full Trial." *CityAM*. Retrieved February 6, 2023 (https://www.cityam.com/court-of-appeal-orders-tulip-bitcoin-case-to-go-to-full-trial/). In the meanwhile, the developer of an open-source smart contract allowing money laundering was detained in a criminal investigation. See Fiscal Information and Investigation Service, 'Arrest of Suspected Developer of Tornado Cash' (08 2022) <https://www.fiod.nl/arrest-of-suspected-developer-of-tornado-cash/>.

[18] Dawn Watkins and Mandy Burton, *Research Methods in Law* (Routledge 2013); Michael McConville and Wing Hong Chui, *Research Methods for Law* (2nd edn, Edinburgh University Press 2017); Ian McLeod, *Legal Method* (9th edn, Palgrave Macmillan 2020).

[19] Rebecca Giblin, 'The P2P Wars: How Code Beat Law' (2012) 16 IEEE Internet Computing 92.

[20] ibid.

[21] Lital Helman, 'Pull Too Hard and the Rope May Break: On the Secondary Liability of Technology Providers for Copyright Infringement' (2010) 19 Texas Intellectual Property Law Journal 111.

Against this background, we set forth an alternative regulatory approach to non-custodial wallet software rooted in copyright regulation and its concept of secondary liability or indirect liability (under United States law), or more broadly intermediary liability (under the European Union's Digital Services Act[22]). Non-custodial wallets facilitate social, economic practices which we can hardly expect to be left to thrive in peace by regulators. Since non-custodial wallets are hard to regulate directly, the regulatory and enforcement activities will focus on various intermediaries. By using the copyright case as a template, we consider the pros and cons of such an approach in relation to the activities enabled on blockchain based systems. We foresee that approach to be fruitful as it not only provides flexibility on the individual use, but also allows for continuous assessments in terms of regulatory benefits and harms done. Note that these approaches are not mutually exclusive[23]; instead, as we argue, they are complementary.

The paper is structured as follows. From a technical perspective, Section 2 introduces the two arrangements for crypto-asset wallet software, custodial and non-custodial, as well as their respective costs and benefits. Section 3 discusses the prevalent use of non-custodial wallets for criminal purposes and reflects on the lack of liability. From a legal perspective, Section 4 presents the predominant regulatory approaches to address non-custodial wallets and discusses their drawbacks. In consideration of previous successes in targeting decentralised technologies, Section 5 argues for the adoption of principles of copyright regulation and secondary liability. Then, in Section 6 we provide an outlook on the possible implementation and discuss the (dis-)advantages of these principles. We conclude in Section 7.

2. Foundations of wallet software

Blockchain enables 'parties with no particular trust in each other to exchange any type of digital data on a peer-to-peer basis with fewer or no third parties or intermediaries'.[24] The first implementation of a blockchain is Bitcoin – a digital currency that can be transferred on a specific peer-to-peer network.[25] Bitcoin, like all subsequent implementations of blockchain, is no single technology.[26] Its three principal building blocks are (1) peer-to-peer (P2P) networks, (2) consensus mechanisms, and (3) public-private key cryptography. Smart contracts are an addition to blockchain systems that originally emerged as part of Ethereum. As we do not attempt to give a complete overview of the technology underlying crypto-assets, we direct the reader to existing literature on blockchain and smart contracts.[27] Subsequently, we introduce the central, technical notion to wallet software: public-key infrastructures.

To participate in a blockchain network, individuals require some form of digital 'identity'. In blockchain systems, the identification and authentication of peers as well as the signature of transactions relies on cryptography – notably, *public-key infrastructures* (PKIs). Each participant on the blockchain is identified by a unique public key. This public key can identify an address which can be party to a transaction as a sender or receiver. The address can represent an individual, an organisation, or a smart contract. Each address, identified by a public key can be controlled by one or more private keys. Through private keys, controllers can access the 'contents' of the address. The contents may be crypto-assets, non-fungible tokens, or messages. The private key is known to the user(s) alone and allows to initiate (sign) transfers or transactions. Together, public and private key form a unique key *pair* that is held within a piece of software colloquially called a *wallet*. The wallet is denominated as *hot* when the software is connected to the internet (typically, as downloaded application or browser extension). It is considered *cold* when the private key is stored on 'analogue' hardware (e.g., piece of paper) or digital hardware (e.g., USB).[28]

The 'custodial' status of a wallet is determined by how and whom the private keys are stored and managed. In a sense (depending on the jurisdictions), private keys may be viewed as bearer instruments. To act as custodian of that instrument grants specific rights. These rights are *de jure* in cases of contractual agreements between bearer and custodian (e.g., as is the case when opening an account with a crypto-asset exchange[29]). Bearers are *de facto* custodians in cases where the wallet is owned fully by oneself, the creator of the wallet. Hence, such wallet is denominated as non-custodial, or self-custodied wallet. Subsequently, we discuss both arrangements.[30]

2.1. *Non-custodial wallet software*

The emergence of non-custodial arrangements can be traced to the inception of Bitcoin. As virtually no services existed to interact with the Bitcoin blockchain, the need for transac-

[22] See João Pedro Quintais and Sebastian Felix Schwemer, 'The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?' (2022) 13 European Journal of Risk Regulation 191.

[23] Joseph Raz, 'Legal Principles and the Limits of Law' (1972) 81 The Yale Law Journal 33.

[24] S Nascimento and others, 'Blockchain Now and Tomorrow: Assessing Multidimensional Impacts of Distributed Ledger Technologies.' (Publications Office of the European Union 2019) EUR - Scientific and Technical Research Reports EUR 29813 EN 8 <http://publications.europa.eu/publication/manifestation_identifier/PUB_KJNA29813ENN>.

[25] Nakamoto (n 1).

[26] Arvind Narayanan and Jeremy Clark, 'Bitcoin's Academic Pedigree' (2017) 60 Communications of the ACM 36.

[27] See Michèle Finck, 'Blockchains: Regulating the Unknown' (2018) 19 German Law Journal 665; Andres Guadamuz, 'All Watched over by Machines of Loving Grace: A Critical Look at Smart Contracts' (2019) 35 Computer Law & Security Review 105338; Zhang, Xue and Liu (n 3).

[28] Pal and others (n 6).

[29] Matthias Haentjens, Tycho de Graaf and Ilya Kokorin, 'The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency, Legal Risks and How to Avoid Them' [2020] Singapore Journal of Legal Studies <https://papers.ssrn.com/abstract=3766564>.

[30] Though the term wallet, used in this paper suggests convenient analogies with cash, physical wallets, or even locks and safes, we suggest to avoid walking down that path too far. The fact that non-custodial wallets (in most cases) involve various software intermediaries, situates this discussion outside of the opened and long closed physical wallet liability domain.

tion execution and key management was delegated to and reserved for adept users.[31] One would save the details of their unique private key physically (e.g., piece of paper) or digitally (e.g., text file, hard drive, USB) – i.e., non-custodial 'cold' wallets. Those connected online, referred to as non-custodial 'hot' wallets, emerged later. They are software (either an application for download or browser extension) used to store private keys plus an interface to connect to blockchains and execute transactions. Like password managers, such wallets are encrypted and require a password to access the keys to blockchains. This paper primarily focusses on the latter.

Non-custodial wallet software can be either open-source (e.g., MyEtherWallet) or offered by third-parties (e.g., Metamask). For both non-custodial cold and hot wallets, security would depend on how the users keep their private keys: if the storage is compromised (e.g., physical theft, phishing attack, or hack), then crypto-assets could be stolen with ease.[32]

There are multiple legitimate reasons for the use of non-custodial wallets, the two most important being ideological purity, and privacy. Non-custodial wallets embody the original anarcho-libertarian / cypherpunk ideological vision of this technology. Already the Bitcoin movement saw decentralisation as a somewhat ambiguous marriage between economic, political, and organisational principles.[33] Decentralisation since enjoys a 'mythical status' in discourses around blockchain technologies.[34] Notably, the promises for the technology are to bring 'greater social justice by undermining oligopolistic and anti-democratic arrangements between big capital and governments' and radicalising 'Friedrich Hayek's and Milton Friedman's ambition to end the monopoly of nation-states'.[35] In other words, decentralisation became a 'social template' where 'distributed architectures are proposed as an alternative to authoritarian, coercive forms of political power'[36] – from state to financial intermediaries. Although we seek not to map the entire discussion on decentralisation, we note that the social template holds in the context of wallet software: more 'decentralised' (in terms of needed third-parties and the storage of keys) wallet solutions are favoured amongst more ideologically conscious users, such as Bitcoin-maximalists, cypherpunks, and HODLers[37] who generally reject the need for financial third-parties / intermediaries and are more adept with the technology.[38]

Privacy benefits are another important motive for the use of non-custodial wallets. This can be understood in two terms: data sovereignty and confidentiality.[39] Data sovereignty stresses the individuals' control over their data.[40] The latter is to be seen within a larger context of surveillance of financial transactions by third parties. Since non-custodial wallets are, by definition, pseudonymous,[41] the choice of using such a way to manage keys can be interpreted as an effort to maintain some degrees of financial privacy. As with the usage of the Tor browser, 'people's choice to use anonymity-granting technologies is a function of two structural factors [...], political need and opportunity'.[42] In states where fundamental political rights are repressed, the use of such technologies is warranted by a need to protect online identities online or risk prosecution. By contrast, in liberal democratic states, the use is driven by opportunity and general distrust that the financial system and Internet is no longer private.

2.2. *Custodial wallet software*

With an increase of different crypto-assets users can hold, the burden to manage numerous key pairs increased.[43] Such market dynamics gave 'rise to a new set of intermediaries'[44] that provide access to crypto-asset markets and blockchains by providing a user-friendly interface and key storage services (i.e., a 'hot', software-based custodial wallet) plus facilitate transaction execution. These intermediaries are typically labelled as custodians. Examples of custodians that offer said interface plus software are crypto-asset exchanges and wallet service providers. Typically, the wallet creation is free of charge as the business model of the intermediary primarily revolves around trading fees. In that capacity, they act much like banks who provide accounts to interact with the financial system.

[31] Nakamoto (n 1).

[32] Pal and others (n 6).

[33] Nathan Schneider, 'Decentralization: An Incomplete Ambition' (2019) 12 Journal of Cultural Economy 265.

[34] Balázs Bodó and Alexandra Giannopoulou, 'The Logics of Technology Decentralization – the Case of Distributed Ledger Technologies' in Massimo Ragnedda and Giuseppe Destefanis, *Blockchain and Web 3.0: Social, Economic, and Technological Challenges* (1st edn, Routledge 2019) 115 <https://www.taylorfrancis.com/books/9780429642371>.

[35] Primavera De Filippi and Benjamin Loveluck, 'The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure' (2016) 5 Internet Policy Review <https://policyreview.info/node/427>.

[36] Balázs Bodó, Jaya Klara Brekke and Jaap-Henk Hoepman, 'Decentralisation in the Blockchain Space' (2021) 10 Internet Policy Review <https://policyreview.info/open-abstracts/decentralisation-blockchain-space>.

[37] To HODL (hold on for dear life) is a colloquial term referring to users that buy-and-hold crypto-assets indefinitely.

[38] Svetlana Abramova and others, 'Bits Under the Mattress: Understanding Different Risk Perceptions and Security Behaviors of Crypto-Asset Users', *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (ACM 2021) <https://dl.acm.org/doi/10.1145/3411764.3445679>.

[39] Primavera De Filippi, 'The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies' [2016] Journal of Peer Production <https://papers.ssrn.com/abstract=2852689>.

[40] Robert Herian, 'Blockchain, GDPR, and Fantasies of Data Sovereignty' (2020) 12 Law, Innovation and Technology 156.

[41] Meaning that since no intermediary is to enforce AML/KYC compliance, addresses can be opened by individuals and organisations at will. It is important to note, that the simple choice of using a non-custodial wallet does not automatically grant full anonymity. The identification of a user is still possible through other means, such as digital forensics, that correlate other digital traces (e.g., IP address) with the wallet creation or use.

[42] Eric Jardine, 'Tor, What Is It Good for? Political Repression and the Use of Online Anonymity-Granting Technologies' (2018) 20 New Media & Society 435, 436.

[43] Recall that for each blockchain, one (1) key is needed. To interact with multiple blockchains, means holding multiple key pairs.

[44] OECD, 'Crypto-Asset Reporting Framework and Amendments to the Common Reporting Standard' (OECD 2022) Public Consultation Document.

Although the legal background of custodial arrangements is not a formal subject of this paper, note that the arrangements are laid out in the terms and conditions (and / or user agreements) stipulated by custodians. Relevant factors here are the key storage, asset segregation, and purview on transaction execution. As custodial arrangements were extensively discussed in the literature and are not the subject of this paper, we direct readers to existing literature on the subject.[45]

2.3. *The costs and benefits of custodial and non-custodial wallets*

From the perspective of crypto-asset users, the relative costs and benefits of using custodial versus non-custodial wallets can be significant. The use of non-custodial wallets put a considerable burden on the individual users in terms of private key storage and safekeeping.[46] Novices in particular, but sometimes seasoned professionals[47] find interacting with blockchains and crypto-assets challenging because of its inherently technical nature.[48] Difficulties in key management can lead to error, accidents, and monetary losses (e.g., due to forgotten passwords or deleted key pairs).

The biggest burden of non-custodial wallets is also their biggest strength: since it is the user, and the user alone who is responsible for their keys, the user can be confident in the fact that no third-party intermediary can interfere with their holdings. This has been, since their inception, the central design principle of blockchain-based systems.

Using custodial service providers relieves users from the burden of private key storage and safekeeping. Custodial service providers can also offer an extra convenience when it comes to the execution of transactions.[49] Because the key management process is embedded in the offering of crypto-asset exchanges, and as custodians of key pairs, they typically offer an end-to-end solution to interact with ledgers; from key creation and storage to transaction verification and execution. However, there are significant risks associated with third-party intermediaries, i.e., custodial service providers. These risks may be financial, or security related.

2.3.1. *Financial risks*

From a financial perspective, users as traders bear three significant types of risk when using custodial wallet software. First, custodial service providers have been witnessed to unilaterally alter user assets. Second, they can limit access to user assets at their discretion. Third, multiple custodial wallet providers have been caught using user assets as their own, in effect misappropriating their users' property. Custodial wallet providers have direct access to user assets (as they control the private keys of their users), which in settings especially absent of regulation, creates conflicts of interests and a strong potential to abuse asymmetries of information and power. Take, for example, recent events to illustrate these different forms of risks.

Binance, the largest exchange by market cap, issues the stablecoin BUSD which is the third largest stablecoin behind Tether (USDT) and USDC. On 29 September 2022, Binance announced that it would unilaterally convert users' holdings of other stablecoins, such as USD Coin (USDC), Pax Dollar (USDP), and TrueUSD (TUSD) into BUSD on a one-to-one basis.[50] Users were left without a choice.

Centralised exchanges are also found to be withholding access to the assets of their users, when markets panic.[51] In 2022, the price of Terra (LUNA) coin crashed from $120 on May 11th to $0.000001 on May 13th. Prominent crypto-asset exchanges suspended the trading of UST and LUNA tokens and prevented users to withdraw their funds. The exchanges' decision to simply halt trading led to a pejorative description as 'gatekeepers to the crypto kingdom'[52] who freely choose which tokens to list and when users may trade.

Finally, custodial service providers may even more directly interfere with their users' assets. The recent collapse of the FTX crypto-asset exchange and its closely affiliated Alameda Research has shown that those who control users' funds may, in some cases attempt to misappropriate or simply steal those funds. In 2022, FTX had lent $10 billion of its customers' assets to Alameda Research and used software to conceal doing so. Executives and senior officials were fully aware of this misappropriation of funds which were used, as it was later revealed, to pay back loans Alameda had taken to fund 'risky bets'.[53] Court documents filed by the SEC concluded that FTX's CEO Sam Bankman-Fried 'was orchestrating a massive, years-long fraud, diverting billions of dollars of the trading platform's customer funds for his own personal benefit

[45] See Haentjens, de Graaf and Kokorin (n 29); Hossein Nabilou, 'The Law and Macroeconomics of Custody and Asset Segregation Rules: Defining the Perimeters of Crypto-Banking' (Social Science Research Network 2022) SSRN Scholarly Paper 4075020 <https://papers.ssrn.com/abstract=4075020>.

[46] Abramova and others (n 38).

[47] Stephen Katte, 'Bitcoin Core Developer Claims to Have Lost 200+ BTC in Hack' (*Cointelegraph*, 2 January 2023) <https://cointelegraph.com/news/bitcoin-core-developer-claims-to-have-lost-200-btc-in-hack>.

[48] Xianyi Gao, Gradeigh D Clark and Janne Lindqvist, 'Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users', *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (Association for Computing Machinery 2016) <https://doi.org/10.1145/2858036.2858049>.

[49] Abramova and others (n 38).

[50] Binance Team, 'Binance to Auto-Convert USDC, USDP, TUSD to BUSD' *Binance Announcement* (5 September 2022) <https://www.binance.com/en/support/announcement/e62f703604a94538a1f1bc803b2d579f>.

[51] International Monetary Fund, 'Global Financial Stability Report: Covid-19, Crypto, and Climate' (International Monetary Fund 2021).

[52] Claer Barrett, 'Hard Lessons from the Crypto Crash' *Financial Times* (27 May 2022).

[53] Vicky Ge Huang, Alexander Osipovich and Patricia Kowsmann, 'FTX Tapped Into Customer Accounts to Fund Risky Bets, Setting Up Its Downfall' *Wall Street Journal* (11 November 2022) <https://www.wsj.com/articles/ftx-tapped-into-customer-accounts-to-fund-risky-bets-setting-up-its-downfall-11668093732>; Dave Michaels, Eleine Yu and Caitlin Ostroff, 'Alameda, FTX Executives Are Said to Have Known FTX Was Using Customer Funds' *Wall Street Journal* (12 November 2022) <https://www.wsj.com/articles/alameda-ftx-executives-are-said-to-have-known-ftx-was-using-customer-funds-11668264238>.

Table 1 – Exchange breaches exceeding 1 000 BTC in loss.[58]

Launch	Breach	Exchange	BTCs stolen	Value in USD (at date of breach)
2010–07	2011–06	Mt. Gox	2 500	40 250
2010–04	2011–08	MyBitcoin	12 500	102 500
2011–09	2012–03	Bitcoinica	43 554	213 415
2011–04	2012–05	BitMarket.eu	19 980	103 896
2012–02	2012–09	Bitfloor	24 086	298 666
2011–01	2013–03	Mercado Bitcoin	4 000	372 000
2011–10	2013–05	Vircurex	1 454	187 275
2013–03	2014–07	Cryptsy	10 000	5 895 000
2013–06	2015–01	796 Exchange	1 000	2 185 000
2013–01	2015–02	BTER	7 170	1 821 897
2012–01	2016–08	Bitfinex	120 000	68 868 000
2012–01	2016–11	Bitcurex	2 300	1 707 750
2013–01	2017–04	Yapizon	3 816	5 158 850
2014–06	2018–09	Zaif	5 966	39 585 603
2017–07	2019–05	Binance	7 000	59 908 100
2016–01	2019–07	BitPoint	1 225	12 350 450

and to help grow his crypto empire'.[54] The New York Times' Kevin Roose likened the collapse of the FTX empire to that of Lehmann Brothers in September 2008.[55]

2.3.2. *Security risks*

Custodial wallet providers do not need to be malicious to pose risks for users. Building and operating complex financial technology infrastructures is challenging. The blockchain space is full of young, sometimes inexperienced software developers. Meanwhile, the potential rewards of finding and exploiting a bug in high stakes financial applications can be enormous.[56] These factors create a space where security breaches are frequent and very damaging.

Despite measures taken to improve cyber-security (e.g., segregation of assets in terms of online/offline storage, code auditing, etc.), some attacks have led to bankruptcies and litigations, repeatedly leaving users empty-handed.[57] In Table 1, we present a selection of breaches stemming from hacking campaigns.

3. Criminal use and (lack of) liability

As discussed so far, there are benefits and drawbacks for using non-custodial and custodial wallet software. The real driver of the dynamics with regards to their public perception, recognition, and use, however, is criminality, legal compliance, and compatibility with the rest of the social, economic, institutional order. The main fault line in this regard is the following juxtaposition. On the one hand, is the ultimately unavoidable incorporation of custodial wallet service providers into the KYC/AML rules applicable to every other financial service provider. On the other hand, is the difficulty of enforcing these rules vis-à-vis non-custodial wallet users, creating on opportunity for crime and an enforcement conundrum for authorities.

Although the public-permissionless blockchain space matured considerably, criminal activities have always been part of this ecosystem – from Bitcoin's nascency and the use of crypto-assets in dark web marketplaces[59] to recent incidents in Decentralised Finance (DeFi) systems.[60] Non-custodial wallet software play multiple roles in this space. First, as acknowledged by the U.S. Department of Justice, they allow criminal actors to stay pseudonymous and 'shift large sums of money quickly and covertly across the globe to support their illegal activities'.[61] Second, non-custodial wallets are essential for using other decentralised services in the blockchain ecosystem, such as DeFi applications, or financial privacy enhancing technologies, such as mixers and tumblers. In the following, we focus on the latter.

Decentralised Finance (DeFi) is a catch-all-term for blockchain-based financial products and services that do 'not rely on centralised intermediaries and institutions but is based on public protocols and decentralised applications'.[62] This implies that DeFi services and products are provided 'by multiple participants, intermediaries, and end-users spread over multiple jurisdictions, with interactions facilitated, and

[54] SEC *v Bankman-Fried* [2022] District Court, Southern District of New York Civil Action 22, 10501, US.

[55] Kevin Roose, 'Is This Crypto's Lehman Moment?' *The New York Times* (9 November 2022) <https://www.nytimes.com/2022/11/09/technology/cryptocurrency-binance-ftx.html>.

[56] Parma Bains and others, 'Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets' (International Monetary Fund 2022) FinTech Note 2022/007.

[57] Haentjens, de Graaf and Kokorin (n 29).

[59] Stearns Broadhead, 'The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments' (2018) 34 Computer Law & Security Review 1180.

[60] Liyi Zhou and others, 'SoK: Decentralized Finance (DeFi) Incidents' (arXiv, 27 August 2022) <http://arxiv.org/abs/2208.13035>.

[61] U.S. Departement of Justice, 'The Report of the Attorney General Pursuant to Section 8(b)(Iv) of Executive Order 14067: How To Strengthen International Law Enforcement Cooperation For Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets' (US Departement of Justice 2022).

[62] Tamás Katona, 'Decentralized Finance: The Possibilities of a Blockchain "Money Lego" System' (2021) 20 Financial and Economic Review 74.

[…] enabled in the first place, by technology'.[63] On the one hand, DeFi products and services promise increases in efficiency, transparency, and accessibility of the infrastructure thanks to the lack of a centralised intermediary.[64] On the other hand, the DeFi space is home to criminal undertakings and arbitrage,[65] and provide ideal opportunities for market manipulation, such as pump-and-dump schemes, spoofing, and wash trading.[66]

Although 'existing financial regulation and policies can be applied for the same activity/risks, irrespective of the technological means through which they are provided',[67] DeFi services are often offered without registered entities or financial intermediaries. This means that the extent to which existing regulation can be enforced is limited and 'the salient, risk-reducing effect of law […] will thus be much diminished'.[68] If a user suffers losses from using a DeFi application, s/he would find it challenging to determine whom to sue on the side of that application.

The problematic is similar for the case of tumblers (aka. mixers). Tumblers are software that is used to obfuscate the transaction history of crypto-assets on the blockchain. They operate as a smart contract to which anyone can send crypto-assets, that are then mixed with other crypto-assets, and finally paid off to specified addresses. By using them it is possible to break the otherwise continuous chain of transactions as recorded on the blockchain and hide the source of the assets which arrived from the tumbler service.[69] While tumblers have plenty of legitimate uses (such as wanting to donate to a political cause in a truly anonymous way), they are particularly useful to launder money and have been used to do so repeatedly in the past.[70]

Tornado Cash is an open-source, decentralised crypto-asset tumbler for the Ethereum blockchain that was used to launder more than $7 billion in crypto-assets, of which $455 million are in connection with the North Korean Lazarus Group.[71] In response, on 8 August 2022, the Office of Foreign Assets Control of the U.S. Department of the Treasury blacklisted Tornado Cash, making it illegal to receive or send money through the mixer. Dutch authorities eventually arrested a suspected developer of the service.[72]

4. Regulation of wallet software

4.1. *Wallets under the FATF guidance*

The principal means to address non-custodial wallet software builds on financial regulation to combat anti-money laundering (AML) and countering the financing of terrorism (CFT). Provided the global impact of crypto-assets, by and in large the measures taken in national jurisdictions are guided by the intergovernmental Financial Action Task Force (FATF).[73] The organisation was created with the mandate to combat AML/CFT following the September 11, 2001 attacks on the World Trade Centre.[74] Long before the first crypto bull market of 2017, the FATF followed the developments of the crypto-asset space,[75] provided that:

> '[the crypto-asset] ecosystem has seen the rise of anonymity-enhanced cryptocurrencies (AECs), mixers and tumblers, decentralised platforms and exchanges, privacy wallets, and other types of products and services that enable or allow for reduced transparency and increased obfuscation of financial flows, as well as the emergence of other virtual asset business models or activities […] that present money-laundering/terrorist financing, fraud, and market manipulation risks'.[76]

In its latest report, the FATF observes the rise of new third-parties that mediate interactions with and within the financial infrastructure. The latest guidance informs regulators on service providers, custodial/non-custodial wallet software, and peer-to-peer (P2P) transactions. Here, the FATF introduces a key definition – that of Virtual Asset Service Providers (VASPs) – which are defined as

> 'any natural or legal person who is not covered elsewhere under the Recommendations and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
>
> i. Exchange between virtual assets and fiat currencies;

[63] Zetzsche, Arner and Buckley (n 13) 3.

[64] Fabian Schär, 'Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets' (2021) 103 Federal Reserve Bank of St. Louis Review.

[65] Alexandra Born and others, 'Decentralised Finance – a New Unregulated Non-Bank System?' (European Central Bank 2022) <https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html>; Eva Su, 'Decentralized Finance (DeFi) and Financial Services Disintermediation: Policy Challenges' (Congressional Research Service 2021).

[66] Zhou and others (n 60).

[67] OECD (n 7).

[68] Zetzsche, Arner and Buckley (n 13) 16.

[69] Christopher P Buttigieg and others, 'Anti-Money Laundering Regulation of Crypto Assets in Europe's Smallest Member State' (2019) 13 Law and Financial Markets Review 211.

[70] see Ross S Delston and Stephen C Walls, 'Terrorist Exploitation Points in the International Financial System: Major Vulnerabilities in the Anti-Money Laundering and Countering the Financing of Terrorism Framework. Avenues for Transatlantic Cooperation' in Klaus Larres and Tobias Hof (eds), *Terrorism and Transatlantic Relations: Threats and Challenges* (Springer International Publishing 2022) <https://doi.org/10.1007/978-3-030-83347-3_9>.

[71] U.S. Department of the Treasury (n 9).

[72] Fiscal Information and Investigation Service (n 17).

[73] Niels Vandezande, 'Virtual Currencies under EU Anti-Money Laundering Law' (2017) 33 Computer Law & Security Review 341; Kyles (n 5).

[74] See http://www.fatf-gafi.org/.

[75] See Financial Action Task Force, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (2014) <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>; Financial Action Task Force, 'Guidance for a Risk-Based Approach to Virtual Currencies' (2015) <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>.

[76] Financial Action Task Force, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (n 11) para 4.

ii. Exchange between one or more forms of virtual assets;
iii. Transfer of virtual assets; and,
iv. Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;
v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset'.[77]

Under this definition, a custodial wallet provider who holds private keys to crypto-assets for its users *and* performs transactions (on their behalf), ought to be classified as VASP. They are to (1) comply with the professional obligations and the conditions described in AML/CFT law and (2) register with financial authorities.

Non-custodial wallet software – though offered by some third-party – challenge this understanding. If the software provider does not execute transactions on behalf of users and, the software is merely used for the self-storage of private keys, then they are not categorised as a VASP. In peer-to-peer (P2P) '[crypto-asset] transfers conducted without the use or involvement of a VASP or other obliged entity', commonly transfers are performed 'two [non-custodial] wallets whose users are acting on their own behalf'.[78] Since in P2P transactions the real identities of both transaction participants are pseudonymous and not subject to due diligence standards, the FATF considers such transactions as a prominent way to launder money and finance terrorism.[79]

Although non-custodial wallet software, decentralised applications (see DeFi), and tumblers may fall under different FATF classifications, they all pose the following regulatory challenge: there is no clearly identifiable, registered subject of regulation, and there is none to hold directly liable for the infringement of rules.

In response, the FATF guidance proposes to include a so called 'travel rule'[80] whereby VASPs are required to 'obtain, hold, and submit required originator and beneficiary information associated with [crypto-asset] transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities'.[81] The travel rule suggests that VASPs are responsible to identify transfers incoming from or outgoing to non-custodial wallet software. Effectively, upholding the travel rule would require white/blacklisting originating addresses that were previously linked with illicit activities.[82]

4.2. *National regulations of non-custodial wallets*

Numerous jurisdictions implemented regulations to tackle wallets and peer-to-peer transactions, as well as crypto-assets more broadly. Because of their intricate similarities to financial assets or securities, and the close connection between the crypto-asset and the traditional economy, jurisdictions adapt (and in some cases develop anew) financial regulation for the use of crypto-assets.[83] Subsequently, we review specific approaches taken by jurisdictions to tackle non-custodial wallet software.

4.2.1. *Ban on wallet usage*

One regulatory response to non-custodial wallet software considers a de facto or partial ban on their use. In some jurisdictions (e.g., China, Turkey, and Algeria) the purchase, sale, use, and possession of crypto-assets is illegal. This measure, by deduction, includes both, custodial and non-custodial wallet software.

Although not banning the entire crypto-asset space, some jurisdictions opted to specifically criminalise the use of non-custodial wallet software. Lithuania's Finance Ministry, as part of amendments to its *Law on the Prevention of Money Laundering and Terrorist Financing*, proposed such a specific ban on 'anonymous wallets' provided their prevalent use in the criminal underworld. At the date of writing, these amendments are yet to pass parliament before written into law.[84]

India's Ministry of Finance, together with the Reserve Bank of India, also consider criminalising the use of non-custodial wallet software. However, the Reserve Bank developed hesitation as it recognised the difficulty of doing so. As thorns in the foot of regulators, Deputy Governor Sankar cites an 'absence of technological solutions to ensuring FATF's 'Travel Rule', the problem of 'unhosted wallets', [and] the fact that P2P transactions do not involve any entity subject to AML-CFT regulations'.[85] At this stage, the government is waiting for the intergovernmental Financial Stability Board (FSB) to propose cross-border regulation for crypto-assets. It deems regulation of crypto-assets as 'effective only after significant international collaboration'. This parallels fears of early bans on Bitcoin mining activities in some jurisdictions, only to see activities resuming in the backyard of one's neighbour.[86]

4.2.2. *Implementation of the 'travel rule'*

Most jurisdictions have adopted the 'travel rule' as part of requirements to regulate money-laundering and the financing

[77] ibid 44(c).
[78] ibid 37.
[79] ibid 34.
[80] The FATF's travel rule parallels that of the United States' Bank Secrecy Act which requires financial institutions to keep records of cash transactions exceeding a certain amount.
[81] Financial Action Task Force, 'Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers' (n 11) para 38.
[82] Jason Scharfman, 'Anti-Money Laundering Compliance for Cryptocurrencies' in Jason Scharfman (ed), *Cryptocurrency Compliance and Operations : Digital Assets, Blockchain and DeFi* (Springer International Publishing 2022) <https://doi.org/10.1007/978-3-030-88000-2_5>.
[83] Apolline Blandin and others, 'Global Cryptoasset Regulatory Landscape Study' (Cambridge Center for Alternative Finance 2019).
[84] Tom Carreras, 'Lithuania to Ban Anonymous Wallets Following EU Regulation' *Crypto Briefing* (9 June 2022) <https://cryptobriefing.com/lithuania-to-ban-anonymous-wallets-following-eu-regulation/>.
[85] Shri T Rabi Sankar, 'Cryptocurrencies – An Assessment' (Reserve Bank of India 2022) Keynote address at the Indian Banks Association 17th Annual Banking Technology Conference and Awards <https://rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1196>.
[86] Wei Sun and others, 'Spatial Analysis of Global Bitcoin Mining' (2022) 12 Scientific Reports 10694.

of terrorism.[87] The FATF's guidance forms the basis of these regulations.

In the European Union, the first step taken were amendments to the 5th Anti-Money Laundering Directive (AMLD5).[88] The focus of AMLD5 is on limiting the anonymity related to crypto-assets by requiring 'providers of exchange services between virtual currencies and fiat currencies, and custodian wallet providers, [to be] registered'.[89] The second step consists of proposed changes to the Transfer of Funds Regulation.[90] On 31 March 2022, two committees of the European Parliament positively voted on provisions to the Regulation that, if adopted by the Parliament, would require VASPs to 'verify the accuracy of information with respect to the originator or beneficiary behind the [non-custodial] wallet, and ensure that the transfer of crypto-assets can be individually identified'.[91] Further, the provisions would require VASPs to systematically inform 'competent authorities' of any transfer worth 1000 euros originating from a non-custodial wallet.

The United States' Bank Secrecy Act (BSA) of 1970,[92] includes a specific passage that extended the reach of law enforcement and prosecution by targeting transactions the government deemed to be 'suspicious'.[93] Today, the BSA provides the basis for U.S. Financial Crimes Enforcement Network's (FinCEN) proposed crypto-asset rules and their implementation of the travel rule. It would require VASPs to report all transactions of more than $3 000 to the federal government.

Another, relatively less systematic implementation of the travel rule is that of the United Kingdom. The Treasury shifted course from its proposal to systematically collect all transaction data of non-custodial wallets to monitoring some, particularly suspicious addresses. In its June 2022 report, the Treasury acknowledged that 'many persons who hold crypto-assets for legitimate purposes use [non-custodial] wallets', and that no 'good evidence' shows these being used disproportionately in criminal activity. Hence, the Treasury now expects businesses to collect information for specific 'transactions identified as posing an elevated risk of illicit finance'.[94] The basis upon which a transaction is deemed to pose such a risk and how it is identified doing so remains to be defined.

4.3. *Drawbacks of the proposed regulatory regime*

Financial regulation of the crypto-asset sector – one which is inherently based on clear rules and requirements – is only able to offer limited solutions to decentralised technology such as non-custodial wallet software. Activists in the blockchain space challenged the proposed travel rule of FinCEN as it would be unconstitutional and pose threat to the Fourth Amendment. Indeed, although the

> 'financial surveillance of United States citizens by their own government is not a new phenomenon, […] FinCEN's proposed rule for monitoring and reporting cryptocurrency transactions is seemingly a natural outreach of the ever-growing U.S. surveillance state'.[95]

The prospect of mass monitoring and infringements on fundamental freedom's (n.b. privacy), are dire outlooks. Furthermore, and as acknowledged by the UK Treasury, the evidence on use of non-custodial wallet software is not present. Inherently, these are drawbacks to the current, rules-based regulatory regime.

There is one additional problem with the current financial regulation infrastructure as it stands: it lacks real enforcement powers vis-à-vis decentralised entities. Though it has well established formal and informal institutional conditions of transnational financial surveillance, investigation, and information exchange,[96] it is not, at this moment, well suited to take prompt action against entities in the decentralised technology space, even if they are caught red-handed, in clear breach of the rules. For that, one would require the cooperation of various online/internet/software intermediaries, instead of the traditional intermediaries financial regulation focuses on, such as luxury goods merchants, art dealers, financial institutions, tax intermediaries, etc.

5. On the lookout for an alternative, flexible approach to non-custodial software regulation

As noted, there are two elements to be balanced with the regulation of non-custodial wallet software. At once, and as acknowledged by the U.K. Treasury, not all use of non-custodial wallet software is per se criminal or linked to illicit activities.[97] On the other hand, the enforcement of the law is problematic vis-à-vis decentralised components of the system –

[87] Thomson Reuters, 'Cryptocurrency Regulations by Country' (2022) <https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf>.

[88] For an assessment of the European Union's 4th Anti-Money Laundering Directive and it's framework for the regulation of crypto-assets, see: Vandezande (n 73).

[89] Directive (EU) 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 para 29.

[90] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006 2015 (OJ L 141, 562015, p 1–18).

[91] General Secretariat of the Council, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on information accompanying transfers of funds and certain crypto-assets (recast) 2022 pt 39b.

[92] See An Act to amend the Federal Deposit Insurance Act to require insured banks to maintain certain records, to require that certain transactions in U.S. currency be reported to the Department of the Treasury, and for other purposes. 1970.

[93] Grant Hespeler, 'The Misguided Activism of the Cryptocurrency Industry: Reckoning with the Bank Secrecy Act of 1970' (2022) 20 Colorado Technology Law Journal 145.

[94] Her Majesty's Treasury Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 Statutory Instrument 2022 - Response to the Consultation (n 12) 28.

[95] Hespeler (n 93) 178.

[96] Pieter Lagerwaard, 'Financial Surveillance and the Role of the Financial Intelligence Unit (FIU) in the Netherlands' (2022) 26 Journal of Money Laundering Control 63.

[97] Her Majesty's Treasury Amendments to the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the

such as non-custodial wallet software, smart contracts, or decentralised applications and organisations – where liability is, if present at all, not defined clearly. Against these considerations, we conclude that the current regulatory regime does not have the necessary flexibility to account for both, infringing and non-infringing use. This begs the question whether rules-based regulations are indeed most appropriate.

Blockchain is not the first techno-social system which has substantial non-infringing uses and nevertheless, also has the capacity to shield uses and users from enforcement. Almost a quarter century earlier, peer-to-peer (P2P) file sharing software crated a similar challenge to copyright regulation.[98] P2P file sharing can be used for both infringing and non-infringing uses. Tools such as the BitTorrent protocol can also render direct enforcement against infringers ineffective, technically challenging, and sometimes outright impossible.[99] This double bind has led to the development of a complex body of law fine-tuned by both courts and legislators to protect right holder interests through the gradual involvement of various intermediaries in the technology stack, the ecosystem, and the economic value chain.

Today, copyright regulation (potentially) extends to all kinds of parties which may play a role in the copyright infringing practices of P2P users, including, but not limited to software repositories used to collaboratively develop, host, and distribute open-source software that may be used for infringement; ISPs providing internet access for infringing users; communication platform providers disseminating (links to) copyright infringing content; cloud service providers hosting infringing services; end users; payment providers, and services facilitating money flowing to infringing actors, etc. In fact, the development of copyright law to tackle infringement in a decentralised techno-social space has led to the formulation of the following principles[100]:

(1) though there seems to be a fundamental collision between the affordances of technology (no digital scarcity, zero marginal cost of copying) and the principle of copyright (remuneration of rights holders takes place through artificial scarcity created by exclusive rights), the rules of traditional copyright would prevail;
(2) copyright enforcement may face significant hurdles in the digital space, but it is not regarded as impossible, therefore significant efforts and resources (legal, financial, political and technological) are invested in it;
(3) if establishing direct liability is not possible or feasible, indirect liability rules may be constructed to help enforcement;
(4) the actual realization of these principles hangs on the continuously reassessed balance between the benefits and the harms which emerge in a particular technological constellation.

As we'll briefly discuss in the following pages, these principles led to the development of a sophisticated legal regime which is actively and effectively used to tackle online copyright infringement. We argue that the problems surrounding non-custodial wallet software and the enforceability of financial regulation are structurally similar to the infringement taking place with the help of dual-use P2P protocols and the copyright regime. This isomorphism is not because the exchange of crypto-assets would, in any sense be similar to the digital exchange of copyrighted works, but because of the relationship of the technology (software, protocols and networks) and the enforcement capacity of the law: in both cases it is often difficult, or unfeasible to establish direct liability. First, we trace how the challenges of enforcing copyright in the digital environment led to the gradual development of a sophisticated secondary liability regime. Then, we ask the question and evaluate whether similar principles can be formulated in the case of non-custodial wallet software, and what such principles would mean in practice.

5.1. *Secondary liability and substantial (non-)infringing use*

Ever since the invention of the printing press, technological intermediaries have been at the centre of debates about their responsibilities regarding facilitating or curtailing contentious social, economic, political practices.[101] The question, throughout history, has always been the same: do the benefits of a new technology of copying and dissemination outweigh the harms caused by the illicit, or illegal uses of the same technology, and if not, should the developer/operator of such technology be liable for infringing activities conducted by others using that technology. In the context of modern technologies of reproduction, this question was first tested in the Betamax case which then served as a template for subsequent, P2P file sharing technologies.

Decided in 1984, *Sony Corp. of America v Universal City Studios, Inc.* (referred to as the 'Betamax case')[102] is a pivotal US case on the use of technology and secondary copyright liabil-

Payer) Regulations 2017 Statutory Instrument 2022 - Response to the Consultation (n 12) 28.

[98] Balázs Bodó, 'Piracy Versus Privacy: An Analysis of Values Encoded in the PirateBrowser' (2015) 9 International Journal of Communication 21.

[99] For BitTorrent, see Jason Farina, Mark Scanlon and M-Tahar Kechadi, 'BitTorrent Sync: First Impressions and Digital Forensic Implications' (2014) 11 Digital Investigation S77.

[100] See, for example, COM(2015) 626 final: COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: Towards a modern, more European copyright framework spelling out such principles as follows. "[T]he involvement of different types of intermediary service providers, seems to be a particularly promising method […] It is also important that systems that allow illegal content to be removed by hosting services, once identified, are effective and transparent and prevent legal content from being taken down erroneously. These systems, which apply horizontally to all types of illegal content, are very relevant for the enforcement of copyright, as copyrighted material accounts for a large portion of the content subject to notices."

[101] Balázs Bodó, 'Coda: A Short History of Book Piracy' in Joseph Karaganis (ed), *Media Piracy in Emerging Economies* (Social Science Research Council 2011); Adrian Johns, *Piracy: The Intellectual Property Wars from Gutenberg to Gates* (University Of Chicago Press 2010).

[102] *Sony Corp of America v Universal City Studios, Inc* (1983) 464 US 417 (Supreme Court).

ity. Universal Studios sued Sony for manufacturing video tape recorders (VTRs) that some users used to record a television program to view it later (so-called, 'time-shifting'). The Court argued that

> 'the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial non-infringing uses'.[103]

In other words, the Court held that most copyright holders who licence their works for television broadcast are not object of time-shifting by users, and hence was constituted as fair use. In conclusion, because VTRs were seen as capable of 'substantial non-infringing uses', the Court held that Sony's sale of these did not constitute secondary copyright infringement.

The question of 'substantial non-infringing uses' was raised again with the rising popularity of peer-to-peer file sharing services in the early 2000's.[104] In 1999, Napster, Inc. launched software where music files could be stored on individual computers and made available to others using the Internet. Napster operated servers to index files and transfer copies of these directly from one user to another. Napster and other P2P file sharing technologies were found to be liable under both vicarious liability (control element) and contributory liability (knowledge element). The latter is of greater interest: the Ninth Circuit Court of Appeals found that Napster had 'knowledge, both actual and constructive, of direct infringement'.[105] Because of that 'actual, specific knowledge of direct infringement',[106] the conclusions of the Betamax Case did not provide support in Napster's argumentation.

Following the Napster decision, developers of file sharing software, such as the Grokster, or BitTorrent[107] responded to the possibility of them being held directly liable for copyright infringement by increasing the levels of decentralisation. Rights holders, in response, responded by further elaborating the theory of indirect or secondary liability, and tested it on various potential intermediaries in the technological stack (e.g., internet service providers, domain name service providers), and activities of the economic value-chains (e.g., advertising, sales channels). Such liability permits someone to be held responsible for copyright infringement, even though they didn't engage in the actual infringement activities themselves.[108]

The 2004 case of *MetroGoldwyn-Mayer Studios, Inc. v Grokster, Ltd.*[109] represents the last in the row of cases on secondary liability. Grokster enabled file-sharing through peer-to-peer networks. Unlike Napster, it did not operate an indexing server and claimed it did not know whether its users used their software to distribute copyrighted files. At first, the Ninth Circuit Court of Appeals ruled in favour of Grokster because it demonstrated substantial non-infringing uses. In 2005, the Supreme Court revisited the case and eventually reversed the decision in favour of MGM Studios. The Court held that

> 'one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties'.[110]

Examples of these steps are 'advertising an infringing use or instructing how to engage in an infringing use, [which] shows an affirmative intent that the product be used to infringe'.[111] (This, as put forward by MGM as evidence, was the case for Grokster.) However, the Court claimed that 'mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability. […] The inducement rule, instead, premises liability on purposeful, culpable expression and conduct'.[112] MGM Studios was able to provide ample evidence for such conduct by Grokster, and at last, the Supreme Court unanimously concurred that Grokster could be liable for the inducement of infringement. That is, on the basis that 'advertising an infringing use or instructing how to engage in an infringing use, show an affirmative intent that the product be used to infringe'.[113]

With the development of the BitTorrent protocol, P2P file sharing software and their developers escaped law enforcement. BitTorrent is an open-source protocol to distribute whatever files via the internet.[114] Although it may and is used by many for infringing purposes, and despite both the protocol and its developers being highly visible, from a copyright infringement perspective they are largely immune. This has led enforcement efforts to try to identify and enlist other, less directly involved, and legally well protected intermediaries to curb digital copyright infringement: ISPs, communication services, search engines, etc.[115]

5.2. *Secondary liability of intermediaries*

5.2.1. *Safe harbours*

Most of the most important online intermediaries have traditionally been enjoying so called *safe-harbour* rules with regards to copyright infringement and other forms of liability for the content that flows through them. These rules, such as Section 230 of the Communications Decency Act, Section 1201 of the DMCA in the US,[116] and the European Union's E-Commerce

[103] *ibid* 442.
[104] Jack Lerner, 'Secondary Copyright Infringement Liability and User-Generated Content in the United States' in Giancarlo Frosio (ed), *Oxford Handbook of Online Intermediary Liability* (Oxford University Press 2020) <https://doi.org/10.1093/oxfordhb/9780198837138.013.18>.
[105] *A & M Records, Inc v Napster, Inc* (2000) 239 F 3d 1004 (Court of Appeals, 9th Circuit) [1020].
[106] *A & M Records, Inc. v. Napster, Inc.* (n 105).
[107] Giblin (n 19).
[108] Lerner (n 104).
[109] *Metro-Goldwyn-Mayer Studios Inc v Grokster, Ltd* (2004) 380 F 3d 1154 (Court of Appeals, 9th Circuit).
[110] *Metro-Goldwyn-Mayer Studios Inc v Grokster, Ltd* (2005) 545 US 913 (Supreme Court) [919].
[111] ibid 936.
[112] ibid 937.
[113] ibid 913.
[114] Farina, Scanlon and Kechadi (n 99).
[115] Giblin (n 19).
[116] U.S. Copyright Office, Digital Millennium Copyright Act 1998 [H.R. 2281].

Directive[117] and Copyright Directive,[118] carved out broad and important limitations to the liability of information service providers for the illegal actions of their users, under certain circumstances. (We redirect the reader to literature for a complete discussion of the liability regime imposed under the E-Commerce Directive.[119]) At the time of their emergence, these rules were aligned with a clear principle: online intermediaries (n.b., network operators) are 'mere conduits' who do not have the technical capacity and should not bear the legal responsibility to inspect communication flowing through them. Their indemnity was also an important safeguard of technological innovation, enabling the rise of services which otherwise may have never been successful, given the legal uncertainty and the possible risks and costs of being responsible for infringing uses.

In the last decade copyright enforcement was crucial in reshaping the early rules which shielded such intermediaries from liability. On the one hand, these safe harbours have fulfilled their purpose: billion-user online services, such as YouTube or Facebook blossomed thanks to these rules. Also, technology has changed, and the automated detection and filtering of infringing content is a realistic, if imperfect technological possibility now. These reasons brought the safe harbours rules under renewed scrutiny.

5.2.2. *The EU's renewed attention to secondary liability*

The rules around intermediary liability were shaped by, on the one hand, the limited liability rules spelled out in the aforementioned safe harbour rules, and, on the other hand, by precedents set by US courts. One of the most consequential re-definition of these crystallised approaches has taken place in the European Union with the Copyright Directive of 2019 and the Digital Services Act (DSA) of 2022.[120] Article 17 of the Copyright Directive, for example, defined online content-sharing service providers as those which store and give the public access to a large amount of works or other subject matter uploaded by their end-users, which they organise and promote.[121] These service providers now must obtain prior authorisation from rights holders so they can let their users share copyright protected materials.

The Directive also defines a non-exhaustive list of exclusions, where the legislator assumed that their primary purpose is not enabling users to upload and share a large amount of copyright-protected content. The exceptions include electronic communication services (e.g., Skype), providers of business-to-business cloud services and cloud services (e.g., Dropbox), online marketplaces (e.g., eBay), not-for profit online encyclopaedias (e.g., Wikipedia), not-for-profit educational and scientific repositories (e.g., ArXiv.org), and open-source software developing and sharing platforms (e.g., GitHub). This distinction is in one sense a rethinking of the substantial non-infringing uses test discussed earlier. The DSA, on the other hand, defines intermediary liability rules and content moderation obligations beyond copyright enforcement, and defines clear rules vis-à-vis other, illegal, or simply harmful content from hate-speech to terrorist propaganda.

These rules (at least in the EU) will certainly redefine and standardise intermediary liability rules with a focus mostly on very large platforms. Beyond and below these overarching, horizontal frameworks there is substantial diversity, both in terms of infringing practices (technologies, networks, techno-social constellations, business models), and enforcement efforts against them. This diversity is handled through a hodge-podge of national regulations, and a plethora of court cases where various intermediaries are brought to court to test their immunity / possible secondary liability. In various cases IPTV software developers and vendors were fined and jailed,[122] software was removed from and reinstated in software repositories such as GitHub[123]; blocking injunctions were issued against DNS providers like Cloudflare[124]; messaging services, like Telegram,[125] and cloud and mail service providers (like Amazon and Google) had to hand over data of infringing users either to rights holders or to law enforcement authorities[126]; links are routinely removed from search engine re-

[117] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market 2000 (OJL 178, 17072000 P1 - 16).

[118] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC 2019 (OJ L 130, 1752019, p 92–125).

[119] Rosa Julià-Barceló and Kamiel J Koelman, 'Intermediary Liability in the E-Commerce Directive: So Far So Good, But It's Not Enough' (2000) 16 Computer Law & Security Review 231.

[120] European Union Intellectual Property Office. and Centre for International Intellectual Property Studies (CEIPI)., *Study on Dynamic Blocking Injunctions in the European Union*. (Publications Office 2021) <https://data.europa.eu/doi/10.2814/301088>; João Pedro Quintais and others, 'Copyright Content Moderation in the EU: An Interdisciplinary Mapping Analysis' (1 August 2022) <https://papers.ssrn.com/abstract=4210278>.

[121] This definition covers services like content sharing services (e.g., YouTube), and platforms (e.g., Facebook).

[122] FACT, 'Thirty Months' Imprisonment for Pirate Software Developer' (30 November 2021) <https://www.fact-uk.org.uk/thirty-months-imprisonment-for-pirate-software-developer/>.

[123] Elliot Harmon and Mitch Stotlz, 'GitHub Reinstates Youtube-Dl After RIAA's Abuse of the DMCA' *Electronic Frontier Foundation* (17 November 2020) <https://www.eff.org/deeplinks/2020/11/github-reinstates-youtube-dl-after-riaas-abuse-dmca>.

[124] Ernesto Van Der Sar, 'Cloudflare Vows to Fight Global 1.1.1.1 DNS Blocking Orders' *TorrentFreak* (15 September 2022) <https://torrentfreak.com/cloudflare-vows-to-fight-global-1-1-1-1-dns-blocking-orders-220915/>.

[125] Sofi Ahsan, 'After Delhi High Court Ruling, Telegram Discloses Names, Phone Numbers & IP Addresses Of Users Accused Of Sharing Infringing Material' *LiveLaw* (29 November 2022) <https://www.livelaw.in/news-updates/after-court-order-telegram-discloses-phone-numbers-ip-addresses-of-users-accused-of-sharing-infringing-material-215311>.

[126] Ernesto Van Der Sar, 'Google and Amazon Helped the FBI Identify Z-Library's Operators' *TorrentFreak* (17 November 2022) <https://torrentfreak.com/how-google-and-amazon-helped-the-fbi-identify-z-librarys-operators-221117/>.

sults[127]; VPN service providers,[128] and operators of the TOR traffic anonymisation network were fined,[129] amongst others.

6. Exploring the advantages and disadvantages of intermediary liability in the blockchain space

Blockchains in general, and non-custodial software (incl. wallets, decentralised applications, and decentralised autonomous organisations) in particular, again raise the decade old question of whether certain technological architectures / configurations can shield their users from the power of law.[130] In the last two decades, it was the copyright wars, which produced important principles regarding the enforcement of laws in decentralised techno-social environments. Though there have been conflicts between code and law in other domains, (most notably around encryption, and other Privacy Enhancing Technologies[131]), only copyright had to deal with mass digital infringement enabled by decentralised technologies where direct liability is often difficult or unfeasible to establish.

It is now the turn of financial regulation to deal with mass breach of both rules and principles governing the digital system of financial services and transactions. We argued that the principles formulated in times of crisis in the copyright domain may show both the opportunities and the challenges of dealing with practices trying to evade the rule of law by relying on open-source, decentralised technologies. These principles can be reformulated to fit the blockchain space, to assess the legal fate that awaits non-custodial wallets, smart contract, and other, open-source, decentralised components of the technological infrastructure.[132]

First, some regulators, especially US financial regulators made it clear that they are willing to enforce financial regulation against the blockchain space.[133] Though the technology may have been designed to bypass and neutralise states' regulatory powers, state authorities are not willing to concede their sovereign purview anytime soon. Second, while such enforcement vis-à-vis decentralised and distributed technologies may prove – at least in theory – tricky, in practice there are enough chokeholds and bottlenecks in the technology stack, amongst stakeholders, and processes to make enforcement feasible.[134] Last but not least, the balancing exercise between benefits and harms is done from the perspective of states, and this may mean that the stakes are much higher. Courts, authorities need not just balance one private interest against another (as is the case with copyright), but the security, sovereignty, rule of law interest of a state against the abstract interest of often nebulous, libertarian communities. These principles help us spell out the possible future(s) of non-custodial wallet software.

Non-custodial wallets may be developed by clearly identifiable parties, businesses, and as such, they are the primary targets of regulation and enforcement. If the enforcement of AML/KYC regulations target such parties, the questions to be raised are (1) to what extent non-custodial wallets are used for illegal purposes, (2) do such ways to interact with (public) blockchains have uses which merit recognition and protection, and (3) how those add up against the illegal uses. Because there are many myths but few solid empirical studies on the prevalence of illegal uses of non-custodial wallets, the clarification (and ongoing monitoring) of this first question is crucial to establish direct liability rules vis-à-vis developers of non-custodial wallet software.

It is also clear that there are already good ideological, political, and legal reasons for non-custodial wallet software to 'melt into air' – that is, turn it into an open-source code or protocol without clearly liable developer or operator parties. Such a development, and the prevalent use of such software to interact with public blockchains as well as unregistered applications and organisations, will prompt a search for liable parties. The identification of end users albeit technically challenging may be possible though also costly. These costs are either borne by state authorities or intermediaries.

As was the case with P2P file sharing, pursuing end users may not be the most effective enforcement avenue, even though they are the ones clearly engaged in illegal activities.[135] Given that the very design of non-custodial wallets is to shield users from the identification of one another, such action against users may also be costly and complicated. If there is one intermediary which facilitates the illicit activities of multitudes of users, it is clearly more effective to step up against the intermediary, than against each user individually. Some intermediaries may provide a more appealing enforcement target than others. The on- and off-ramps to the blockchain ecosystem, exchanges, and other registered financial service providers (i.e., VASPs) are the most obvious chokepoints on the system, and the proposed travel rules target

[127] See: https://lumendatabase.org/.

[128] Ernesto Van Der Sar, 'Filmmakers Win $4.2 m Piracy Damages from Defunct VPN Hosting Company' *TorrentFreak* (8 November 2022) <https://torrentfreak.com/filmmakers-win-4-2m-piracy-damages-from-defunct-vpn-hosting-company-221108/>.

[129] Tim Cushing, 'Copyright Troll Sues Tor Exit Node, Gets Partial Win' *Techdirt* (2 March 2017) <https://www.techdirt.com/2017/03/02/copyright-troll-sues-tor-exit-node-gets-partial-win/>.

[130] Balázs Bodó, Jaya Klara Brekke and Jaap-Henk Hoepman, 'Decentralisation: A Multidisciplinary Perspective' (2021) 10 Internet Policy Review <https://policyreview.info/concepts/decentralisation>; Bodó, Brekke and Hoepman (n 36).

[131] Craig Jarvis, *Crypto Wars: The Fight for Privacy in the Digital Age: A Political History of Digital Encryption* (CRC Press 2020).

[132] We acknowledge that the proposition to adopt copyright regulation and principles of secondary liability are but one alternative approach. In that sense, the normative analysis undertaken here is inherently limited by our focus on one of other, possible regulatory regimes that would allow to regulate non-custodial wallet software differently.

[133] Jay Clayton and Timothy Massad, 'How to Start Regulating the Crypto Markets—Immediately' *Wall Street Journal* (4 December 2022) <https://www.wsj.com/articles/how-regulate-cryptocurrency-markets-11670110885>.

[134] It is also worth noting that unlike in the copyright case, it is not private parties, but state actors who will enforce rules, with incomparably more resources and powers than private parties.

[135] Christophe Geiger, 'Challenges for the Enforcement of Copyright in the Online World: Time for a New Approach' [2014] Max Planck Institute for Innovation and Competition Research Papers 1.

these for obvious reasons. Various blockchain infrastructure providers are also relatively accessible enforcement targets. One example are block validators which are responsible for selectively inserting new transactions to the distributed ledger. Though block validation was designed to be decentralised, various external incentives have led to considerable concentration of these activities in most major blockchain ecosystems.[136] As such, these block validators may already be legally legible, regulated entities, which may thus be obligated to filter certain transactions, such as those involving non-custodial wallet addresses.

To a certain extent this has already happened on the Ethereum blockchain with regards to transactions involving Tornado Cash. As noted earlier, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) barred all stateside individuals and entities from using the service. The sanction was issued for Tornado Cash's role in laundering $7 billion.[137] This was the first time an open-source software protocol was listed on the Specially Designated Nationals and Blocked Persons List. Given that the Ethereum blockchain has a complex block proposal / validation structure to promote decentralisation, it is all the more noteworthy, that at the time of writing more than 70% of all blocks were compliant with the OFAC sanctions.[138] This means that the entity which inserted the transactions in the block decided to respect the OFAC regulation. In this process, crypto-economic incentives coupled with the dominance of regulated entities, resulted in a voluntary compliance mechanism in an otherwise censorship resistant technology stack. This is, again, something we have witnessed in other, informal, infringing P2P communities.[139]

Other, more centralised stakeholders are also easy enforcement targets. Blockchain infrastructure providers, such as Infura and Alchemy provide APIs to interact with the blockchain. Many non-custodial wallets software (n.b., Metamask) rely on these to interact with the blockchain rather than the user running their own node. These providers already blocked Ethereum API access for Tornado Cash, meaning that users can no longer connect to the Tornado Cash front-end using those non-custodial wallets.[140] The same API providers have previously blocked users in countries under financial sanctions. This was the case for users in Russia and Venezuela.[141]

Absent of such voluntary compliance at the primary, blockchain infrastructure layer, there are still multiple possible enforcement targets. These may include cloud service providers (which run Virtual Machines on which blockchain software is running), ISPs, and code repositories which host software. The sanctioning of Tornado Cash, again, provided a litmus test for the potential legal compliance risks different online intermediaries may think they face. GitHub first banned then unbanned the code repository for the mixer software.[142] Websites which enable users to interact with the service became inaccessible. Domain names of the service became inaccessible.[143] Similar measures can also be taken against non-custodial wallet software developers and providers.

Finally, there is a long standing theoretical[144] as well as legal debate about the duties of care obligations, and fiduciary status of open-source software developers in the blockchain space. A UK court will be considering whether there is a fiduciary relationship between users and developers.[145] Though a civil case may not be fully relevant from a criminal perspective, a decision which would establish the responsibility of open-source software developers vis-à-vis how their systems are used may have far reaching implications for criminal cases as well – both in terms of the availability and accessibility of fully open-source, non-custodial software. We have already witnessed the first steps in this direction, when Dutch authorities arrested a man suspected of being a Tornado Cash developer on money laundering charges.[146]

In sum, the current developments speak not just about the principles at play, but also spell out the elements missing from the current legal / policy landscape:

- there is no reliable data on the extent of illegal activities conducted through such decentralised services;
- there are no clear tests for policymakers and courts to balance the benefits and the potential harms which come with such services; and,
- there are no clear safe harbour rules applicable to non-custodial wallet software, decentralised applications/organisations, their developers and operators.

[136] See Sarada Prasad Gochhayat and others, 'Measuring Decentrality in Blockchain Based Systems' (2020) 8 IEEE Access 178372.
[137] U.S. Department of the Treasury (n 9).
[138] See: https://www.mevwatch.info/.
[139] Balázs Bodó, 'Set the Fox to Watch the Geese: Voluntary IP Regimes in Piratical File-Sharing Communities' in Martin Fredriksson and James Arvanitakis (eds), *Piracy: Leakages from Modernity* (Litwin Books 2014).
[140] Chainalysis Team, 'Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions' (*Chainalysis Blog*, 30 August 2022) <https://blog.chainalysis.com/reports/tornado-cash-sanctions-challenges/>.
[141] Danny Nelson, 'Crypto Industry's Sanctions Woes on Full Display in MetaMask's Venezuela Hiccup' *CoinDesk* (4 March 2022) <https://www.coindesk.com/business/2022/03/04/crypto-industrys-sanctions-woes-on-full-display-in-metamasks-venezuela-hiccup/>.
[142] Margaux Nijkerk, 'Crypto-Mixing Service Tornado Cash Code Is Back on GitHub' *CoinDesk* (22 September 2022) <https://www.coindesk.com/business/2022/09/22/crypto-mixing-service-tornado-cash-is-back-on-github/>.
[143] Immanual Milton, 'Crypto Mixer Tornado Cash's Accounts Are Disabled After US Sanctions' *Bloomberg* (8 August 2022) <https://www.bloomberg.com/news/articles/2022-08-08/crypto-mixer-tornado-s-accounts-are-disabled-after-us-sanctions>.
[144] Angela Walch, 'In Code(Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains' in Philipp Hacker and others (eds), *Regulating Blockchain. Techno-Social and Legal Challenges* (Oxford University Press 2019) <https://papers.ssrn.com/abstract=3203198>; Rodrigo Seira Silva-Herzog, Brent A. Plummer and Nelson M. Rosario, 'Blockchain Development and Fiduciary Duty' [2019] Stanford Journal of Blockchain Law & Policy <https://stanford-jblp.pubpub.org/pub/blockchain-dev-fiduciary-duty/release/1>.
[145] Darren Parkin, 'Court of Appeal Orders Tulip Bitcoin Case to Go to Full Trial' (*CityAM*, 3 February 2023) <https://www.cityam.com/court-of-appeal-orders-tulip-bitcoin-case-to-go-to-full-trial/>.
[146] Fiscal Information and Investigation Service (n 17).

The secondary liability regime in the context of copyright enforcement has long and rightly been criticised for its potential to over-blocking and its chilling effects.[147] There are many uses of copyrighted works, such as parody and pastiche which tend to be blocked by various intermediaries, because the adjudication of such uses is often complicated, and intermediaries tend to err on the side of their own legal safety, and the rights of the copyright holders at the expense of the rights of their users.[148] Such misplaced incentives at the level of intermediaries may lead to users rather not coming forward with expressions which would otherwise be legal, in anticipation of a negative outcome.[149]

The aforementioned, missing elements in the financial enforcement space may lead to similar suboptimal outcomes in the interaction with crypto-assets. Intermediaries may be incentivised to err on the side of over-blocking, censoring software with substantial legitimate uses, or censoring transactions which may look suspicious, though under proper scrutiny would be perfectly legal. The lack of clear rules limiting intermediary liability may turn parties which have neither the expertise nor the resources to police the vast and complicated financial system.

The digitisation of financial transactions, and the emergence of multiple value exchange infrastructures – including the sovereign, blockchain-based ones – have highlighted some of the competing interests that need to be balanced under these new infrastructural conditions[150]: the individual's right to financial privacy and anonymity, the businesses' right to freely conduct trade, and the public interest in fighting money laundering, tax-avoidance, the financing of terrorist organisations, or business fraud. Financial enforcement is also a continuous balancing exercise between these interests, and the more various non-financial intermediaries are brought into the process, absent of clear guidance in the dimensions above, the more contentious this exercise could be.

7. Conclusion

Our analysis contributes to fragmented literature on regulation of non-custodial wallet software for crypto-assets. Because the use of said software for non-infringing relative to infringing uses remains empirically unsubstantiated, we highlighted that countering their use for criminal ventures and illicit activities in the space provides ample need to revisit the efficiency of financial regulation. Since its inception, regulators were challenged by the space provided that non-custodial software, by definition, lack a legal footing. Hence, the application of financial regulation – which assumes the existence of some registered firm, person, or entity – remains limited. Beyond re-evaluating the efficiency of financial regulation, we questioned the proposals which consider an extension of the travel rule to account for all transactions involving non-custodial wallet software.

In response to these shortcomings, we proposed a turn towards more flexible regulatory means. The issue at stake is the liability of software providers when users commit illicit activities. Motivated by this endeavour, we investigate one of other possible regulatory regimes: under secondary copyright liability, jurisdictions dealt with decentralised software and its concepts may provide the needed flexibility to the law. Courts may, on the basis of an evaluation of a wallet's (non-) infringing use or provider's affirmative intent, allow to monitor specific non-custodial wallets instead of systematically tracking all transactions. It also provides means for courts to hold intermediaries in the technology stack and the economic value chain liable.

We foresee the contribution made in this work to be of value to a broader debate on the regulation of the non-custodial crypto-asset space. The proposed approach of secondary liability may indeed prove valid to develop regulatory frameworks applicable to the field of Decentralised Finance, and the emerging applications and organisations that characteristically lack the described legal footing.

Declaration of Competing Interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

PayPal's financial support is administered via the FNR, and by contractual agreement, PayPal has no involvement in Barbereau's research. Barbereau declares that he holds crypto-assets.

Data availability

No data was used for the research described in the article.

Acknowledgements

This research was funded in whole by the Luxembourg National Research Fund (FNR) and PayPal, PEARL grant reference 13342933/Gilbert Fridgen. For the purpose of open access, the author has applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

The Blockchain and Society Policy Research Lab has received funding from the European Research Council under the

[147] Robert Gorwa, Reuben Binns and Christian Katzenbach, 'Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance' (2020) 7 Big Data & Society 205395171989794; João Pedro Quintais and others, 'Safeguarding User Freedoms in Implementing Article 17 of the Copyright in the Digital Single Market Directive: Recommendations from European Academics' [2019] Available at SSRN 3484968; Jennifer M Urban and Laura Quilter, 'Efficient Process or Chilling Effects-Takedown Notices under Section 512 of the Digital Millennium Copyright Act' (2005) 22 Santa Clara Computer & High Tech. LJ 621.

[148] Joao Quintais, 'The New Copyright in the Digital Single Market Directive: A Critical Look' [2020] European Intellectual Property Review.

[149] Wendy Seltzer, 'Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment' (2010) 24 Harvard Journal of Law & Technology 171.

[150] V Ferrari, 'Money after Money: Disassembling Value/Information Infrastructures' (PhD Thesis, University of Amsterdam 2023) <https://dare.uva.nl/search?identifier=30904422-2233-4400-bc5f-e7971b33f758>.

European Union's Horizon 2020 research and innovation program (grant agreement no. 759681).

Author Information

Tom Barbereau is a doctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg and a visiting researcher at the Institute for Information Law, University of Amsterdam. His-academic research focuses on socio-technical controversies in and of decentralized technologies; not least, in the development of 'self-sovereign' identity regimes, Decentralized Finance, and Decentralized Autonomous Organizations.

Dr. **Balázs Bodó** is an associate professor, senior research scientist at the Institute for Information Law, University of Amsterdam, and the Principal Investigator of the European Research Council funded Blockchain and Society Policy Research Lab. He is a two-time Fulbright Scholar (2006–7, Stanford University; 2012 Harvard University), and a former Marie Skłodowska-Curie fellow (2013–15). His academic research focuses on domains and processes of knowledge production and exchange: their histories; social, economic and technological organization; and regulation.