The tort law applicable to the protection of crypto assets

Tobias Lutzi

Angaben zur Veröffentlichung / Publication details:

Lutzi, Tobias. 2023. "The tort law applicable to the protection of crypto assets." In *Blockchain and private international law*, edited by Andrea Bonomi, Matthias Lehmann, and Shaheeza Lalani, 399–416. Leiden: Brill. https://doi.org/10.1163/9789004514850_016.

CHAPTER 14

The Tort Law Applicable to the Protection of Crypto Assets

Tobias Lutzi

1 Introduction

As the different contributions to this book aptly demonstrate, Private International Law (PIL) often struggles to accommodate phenomena that lack a sufficiently substantial connection to the territory of a particular legal system. The protection of crypto assets against tortious interference in the form of theft, manipulation, fraud, or extortion is no exception.

This difficulty is, for at least three reasons, especially pronounced in the area of tort law.[1] First, the parties are generally not bound by any pre-existing relationship that might help to identify the law that is most closely connected. Second, PIL traditionally reacts to such a lack of meaningful connections other than the tort itself by relying on purely geographical connecting factors such as, most importantly, the "place" of the tort – which is inherently difficult to identify in the context of digital assets. Third, some of the core features of many crypto assets – such as the decentralised nature of the underlying networks and the pseudonymity of their users[2] – further complicate the application of traditional conflicts rules.[3]

This is not to say that PIL is unable to identify the applicable tort law to the protection of crypto assets.[4] While a variety of situations potentially fall into this category (2.), the traditional conflicts rules for torts accommodate them

1 This may also be the reason why the topic has so far received far less attention than the question of the applicable contract law.

2 As is regularly pointed out, the offline identity of Bitcoin inventor(s) Satoshi Nakamoto remains unknown to this day.

3 See also Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws," in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford: Oxford University Press 2019), para. 5.08; Matthias Lehmann, "Internationales Privat- und Zivilprozessrecht," in Sebastian Omlor and Mathias Link (eds), *Kryptowährungen und Token* (Frankfurt am Main: dfv 2021), paras. 22–26.

4 For a similar conclusion, see Matthias Lehmann, "Who Owns Bitcoin? Private Law Facing the Blockchain" (2019) 21 Minnesota Journal of Law, Science & Technology 93, 132–33.

with difficulty and to vastly different degrees. Thus, the *lex loci delicti* rule can be applied with somewhat surprising ease if it is understood to refer to the place of the relevant act(s) but struggles in its (now more common) understanding as the place of the damage (3.). In many cases, this difficulty can, however, be overcome by more flexible provisions that refer more broadly to the law most closely connected to the case at hand (4.). Rules for specific torts (5.) and party autonomy (6.) may also play a residual role, while proposals to simply sidestep the conflict-of-laws analysis by applying the so-called *lex cryptographica* must ultimately be rejected (7.). Perusing the rich toolbox of PIL in view of the specific challenge of protecting crypto assets in tort law thus reveals a number of strengths and weaknesses that we also observe in other cases of online torts (8.).

2 The Protection of Crypto Assets and Tort Law

Before discussing the application of specific conflicts rules to the protection of crypto assets, it might be helpful to specify which cases fall into this category (2.1). The extent to which these cases actually are subject to the conflicts rules on torts is, of course, a question of characterisation, the answer to which may differ depending on the relevant legal system (2.2).

2.1 *The Protection of Crypto Assets*

The protection of crypto assets against tortious interference and misappropriation may refer to a wide range of different situations, not all of which necessarily create novel challenges for existing conflicts rules. In order to structure the discussion of their application in the following sections, it appears useful to sort them into two separate sets of problems.

The first set involves interference with crypto assets held by another individual. Control over these assets is usually exercised through a set of keys stored in a wallet held either by the "owner" or by some intermediary (*e.g.* a centralised crypto exchange).[5] These keys may be stolen, intentionally deleted or destroyed, or simply lost.[6] Their owners may also be tricked or coerced into using them to transfer their assets to someone else.

5 Examples include *Bisq*, *Binance*, *Coinbase* and *Kraken*.

6 It is believed that about 20% of all bitcoins are lost forever because their owners have simply misplaced or permanently deleted their private keys; as of August 2021, the value of these lost coins would amount to more than 140 billion Euros.

If the assets in question involve a physical device (*e.g.* a hard disk or USB flash drive), this may simply be stolen or destroyed, which would hardly raise any new questions of PIL.[7] The fact that the stolen device contains data that gives access to assets stored on a blockchain should not distract from the fact that all relevant aspects of the tort can be localised by looking purely at its physical elements. Much like the tort law applicable to the theft of a car does not change depending on what was stored in the trunk, the law applicable to the theft of computer hardware should not depend on what was stored on it. Other types of interference with someone else's hardware, including its temporary deactivation or permanent destruction, should similarly be treated independently of whether or not the hardware was used to access crypto assets.[8]

On the other hand, where the interference is independent of where the key is stored physically, for example because it is accessed by the tortfeasor remotely or because the owner is tricked or coerced into acquiring or transferring certain assets, identifying the applicable law becomes more complicated. Considering the continuing popularity of cryptocurrencies for all kinds of cybercrimes[9] as well as the rapidly growing importance of NFTs, this scenario is arguably the most practically relevant, as a growing number of reported cases illustrates. In three cases recently decided by the Commercial Court of the High Court of Justice of England and Wales,[10] the claimants alleged that they were coerced into transferring US$ 950,000 worth of bitcoin as a ransom;[11] that they transferred £577,000 worth of bitcoin in the context of an initial coin offering fraud;[12] and that they lost US$ 2.6m as a result of crypto assets being transferred by hackers accessing their crypto wallet.[13] In the District Court for the Central District of California's recent decision in *Terpin v. AT&T Mobility*,[14] hackers had allegedly gained control over the claimant's mobile phone number

7 See also Dickinson (n 3), para. 5.11.

8 *Id.*

9 The latest Cryptocurrency Crime and Anti-Money Laundering Report by CipherTrace puts the overall volume of "crypto crime" at $1.9 bn, the vast majority of which consists of fraud and misappropriation: see CipherTrace, "Cryptocurrency Crime and Anti-Money Laundering Report" (*CiperTrace*, February 2021), 6–7 <https://ciphertrace.com/wp-content/uploads/2021/01/CipherTrace-Cryptocurrency-Crime-and-Anti-Money-Laundering-Report-012821.pdf> accessed 1 June 2022.

10 As to which see also Amy Held, Chapter 8 of this volume, subs. 2.3 and 2.4.

11 *AA v. Persons Unknown et al.*, [2019] EWHC 3556 (Comm).

12 *Ion Science Ltd v Persons Unknown & Others*, EWHC (Comm), 21 Dec 2020, reported by Amy Held, "Does situs actually matter when ownership to bitcoin is in dispute?" (2021) 36 Journal of International Banking and Financial 269, 269–272.

13 *Fetch.AI Limited et al. v. Persons Unknown et al.* [2021] EWHC 2254 (Comm).

14 *Terpin v. AT&T Mobility*, 2019 WL 3254218 (C.D. Cal. 2019).

on two occasions in order to impersonate him and gain access to his crypto wallet, ultimately stealing tens of millions of dollars' worth of cryptocurrency. While it might still be possible to localise certain elements of the tort in these cases, identifying the place of the damage can easily become very difficult.[15]

A second set of problems involves interferences with the crypto network itself. The degree of complexity and organisation of the different networks varies as widely as their vulnerability to cyber-attacks. In another Californian case, *Fabian v. LeMahieu*,[16] for instance, the plaintiff claimed he lost substantial amounts of cryptocurrency as part of a series of unauthorised transactions on the defendant's cryptocurrency exchange that resulted in a loss of assets worth US$ 170 million in total. Similarly, the DAO, arguably the most famous example of a decentralised autonomous organisation, became subject to an exploit that allowed one or several users to misappropriate about a third of its funds (which exceeded US$ 100 million at the time).[17] In reaction to the attack, the Ethereum blockchain was reset to before the attack, creating a permanent fork in the process.[18] The highly decentralised control of many blockchains also allows for subtler ways of manipulation. As many blockchains rely on consensus mechanisms, they can be manipulated (within limits) by anyone who manages to control a sufficiently high number of nodes (so-called "51 percent attacks").

As explained in the following sections, this latter group of torts – *i.e.* those directly targeting the crypto network – are the most difficult for PIL to accommodate. PIL struggles with both delocalised torts and torts involving more than two parties.[19]

2.2 *The Scope of the Applicable Tort Law*

Although each legal system is free to decide which cases it characterises as torts for the purpose of the conflict of laws, a number of general observations can be made in the present context.

First, all the situations described above necessarily involve a crypto network that operates according to certain rules, which may give rise to legal relationships that can be characterised as contractual (or even corporate).[20] Of course, this does not mean that all the claims described previously will follow this

15 See *infra* section 3.2.

16 *Fabian v. LeMahieu*, 2019 WL 4918431 (N.D. Cal. 2019).

17 See also Florence Guillaume and Sven Riva, Chapter 20 of this volume, sub. 2.1.

18 Called Ethereum Classic.

19 See also Dickinson (n 3), para. 5.12.

20 *Id.*, paras. 5.27–34.

characterisation. As explained above, if a physical device is stolen, the fact that the assets stored on it derive their value from the existence of a decentralised global network of contractual relationships will not change the characterisation of its owner's claim in tort. Yet, the more closely the facts of the case are connected to this network, the more difficult it will be to draw the line between contract and tort.

As far as EU instruments of PIL[21] are concerned, the (slightly wider) category of non-contractual obligations is traditionally defined by reference to contractual obligations,[22] *i.e.* obligations "freely assumed by one party towards the other."[23] But even where the parties are bound by a contract in this sense, not all claims between them will automatically fall under the conflicts rules for contracts. According to the latest iteration of the relevant formula stated by the Court of Justice of the European Union (CJEU), a claim will still be characterised as non-contractual "where the applicant relies, in its application, on rules of liability in tort, delict or quasi-delict, namely breach of an obligation imposed by law, and where it does not appear indispensable to examine the content of the contract concluded with the defendant in order to assess whether the conduct of which the latter is accused is lawful or unlawful."[24]

While other legal systems may have found more elegant ways to draw the line (or not to require such line drawing), it seems fair to say that except for violations of a crypto network's rules by one of its participants that directly affect other participants, the situations described above will give rise to claims that can safely be characterised as non-contractual. This is true for cases of theft or misappropriation of crypto assets, fraudulent misrepresentation and prospectus liability[25] as well as for external attacks on the functioning of the crypto

21 In particular, Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L177/6 ("Rome I Regulation") and Regulation No 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II), [2007] OJ L 199/40 ("Rome II Regulation").

22 See Judgment of the Court (Fifth Chamber) of 27 September 1988, *Athanasios Kalfelis v Bankhaus Schröder, Münchmeyer, Hengst and Co. et al.*, Case 189/87 (ECLI:EU:C:1988:459), paras. 17–18.

23 See Judgment of the Court of 17 June 1992, *Jakob Handte & Co. GmbH v Traitements Mécano-chimiques des Surfaces SA*, ECR I-03967, Case C-26/91 (ECLI:EU:C:1992:268), para. 15. On the need for a consistent interpretation of the different instruments, see Recital (7) of both the Rome I (n 21) and Rome II (n 21) Regulations.

24 Judgment of the Court (Grand Chamber) of 24 November 2020, *Wikingerhof GmbH & Co. KG v Booking.com BV*, Case 59/19 (ECLI:EU:C:2020:950), para. 33.

25 Judgment of the Court (Fourth Chamber) of 28 January 2015, *Harald Kolassa v Barclays Bank plc*, Case C-375/13 (ECLI:EU:C:2015:37), paras. 36–41. See also Landgericht Berlin,

network or ledger technology. Yet, as discussed below, this characterisation does not necessarily prevent taking into account the contractual relationship.[26]

Second, not all situations involving non-contractual obligations are necessarily governed by the general conflicts rules on torts. On the one hand, some might escape these rules altogether as a consequence of being subject to more specific instruments such as the EU General Data Protection Regulation.[27] The Rome II Regulation also carves out an exception for negotiable instruments in its Article 1(2)(c), albeit with a limited scope that does not appear to extend to crypto assets.[28] On the other hand, specialised rules may apply to particular torts involving crypto assets, such as product liability,[29] unfair competition,[30] and infringement of IP rights.[31]

Third, a number of questions that appear to safely fall outside the ambit of tort law can arise as preliminary questions to a claim in tort. This might be particularly relevant for the question of ownership.[32] While many legal systems resolve these questions by applying the relevant conflicts rule of the *lex fori* independently of the law applicable to the main question, others subject both questions to the latter.[33]

Fourth, questions that fall under the applicable substantive (tort) law must also be distinguished from questions of procedure, which are traditionally

---

Case 2 O 322/18, 27 May 2005, ECLI:DE:LGBE:2020:0527.20322.18.00, para. 109, for a case of prospectus liability in the context of an Initial Coin Offering (ICO).

26 See *infra* section 4.

27 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L119/1 ("GDPR").

28 See Björn Steinrötter, "International Jurisdiction and Applicable Law," in Philipp Maume, Lena Maute, and Mathias Fromberger (eds), *The Law of Crypto Assets. A Handbook* (Munich/Oxford/Baden-Baden: Beck/Hart/Nomos 2022), para. 45; Dieter Martiny, "Virtuelle Währungen, insbesondere Bitcoins, im Internationalen Privat- und Zivilverfahrensrecht" (2018) 38 Praxis des Internationalen Privat- und Verfahrensrechts 553, 560, 564.

29 See, *e.g.*, Article 5 of the Rome II Regulation (n 21).

30 See, *e.g.*, *id.*, Article 6.

31 See, *e.g.*, *id.*, Article 8. See also the rules on *culpa in contrahedo* (*id.*, Article 12; which are particularly relevant in cases of fraud) and unjust enrichment (*id.*, Article 10).

32 See also Susanne Lilian Gössl, "IPR und Smart Contracts," in Thorsten Voß (ed), *Recht der FinTechs – Legal Aspects of Financial Technology* (Berlin: De Gruyter 2021), para. 79; Matthias Lehmann, "Internationales Finanzmarktrecht," in Jan von Hein (ed), *Münchener Kommentar zum Bürgerlichen Gesetzbuch* (8th edn, München: Beck 2021), vol. 13, part 12, para. 603.

33 See Andrea Bonomi, "Incidental (preliminary) question," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (Cheltenham/Northhampton: Edward Elgar 2017), 913–14.

governed by the *lex fori*.[34] Thus, while the applicable tort law may determine which remedies are available,[35] it will ultimately depend on the *lex fori* if a court will be able to award damages in a cryptocurrency.[36]

3 The Place of the Tort

Over the last few centuries, the *lex loci delicti commissi* rule has clearly emerged as the principal conflict-of-laws rule in the area of tort law.[37] It provides the starting point, in some form or another, in the vast majority of PIL systems.[38] Its significance is based on its generally strong connection to the tort in question (especially where the parties had no other prior contacts), its predictability for both parties, and its perceived neutrality.[39] As the number of torts "happening" in more than one "place" grew rapidly during the 20th century, though, a choice between the place of the relevant act(s) and the place where these acts produced their harmful effect(s) became necessary.[40] While many legal systems have opted for one or the other,[41] some legal systems leave the choice to the claimant.[42]

34 See Paul Torremans et al. (eds), *Cheshire, North & Fawcett. Private International Law* (Oxford: Oxford University Press 2017), 73: "One of the eternal truths of every system of private international law is that a distinction must be made between substance and procedure, between right and remedy. The substantive rights of the parties to an action may be governed by a foreign law, but all matters appertaining to procedure are governed exclusively by the law of the forum."

35 See Article 15(c) of the Rome II Regulation (n 21).

36 See Dickinson (n 3), paras. 5.89–92 (on English law).

37 See Thomas Kadner Graziano, "Torts," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (Cheltenham/Northhampton: Edward Elgar 2017), 1709, 1710; Stig Strömholm, "Intentional Torts," in Kurt Lipstein (ed), *International Encyclopedia of Comparative Law. Vol. III: Private International Law* (Tübingen/Leiden/Boston: Mohr Siebeck/Martinus Nijhoff 1980), ch. 33, para. 1.

38 Graziano (n 37), 1710–11.

39 *Id.*, 1711.

40 *Id.*, 1714.

41 *E.g.,* Article 4(1) of the Rome II Regulation (n 21) (place of the damage); Article 133(2) of the Swiss PILA (Federal Act on Private International Law (PILA) of 18 December 1987, SR 291) (place of the damage); Article 8(2) of the Rome II Regulation (n 21) (place of the causal event).

42 *E.g.*, Article 40(1), 2nd sentence, of the German Introductory Act to the Civil Code ("EGBGB") (Einführungsgesetz zum Bürgerlichen Gesetzbuche in der Fassung der Bekanntmachung vom 21. September 1994 (BGBL. I S. 2494; 1997 I S. 1061), das zuletzt durch Artikel 3 des Gesetzes vom 21. Dezember 2021 (BGBL. I S. 5252) geändert worden ist).

The following section will discuss how each of these two places could be identified with regard to the protection of crypto assets.

3.1 *The Place of the Relevant Act*

The connecting factor of the place of the relevant act (*locus actus*; causal event) does not raise insurmountable difficulties when applied to torts involving crypto assets.[43]

For torts involving physical acts, the involvement of crypto assets evidently raises no particular problems in this regard: as far as conflict-of-laws rules are concerned, there is no reason to treat the theft of a USB drive that contains a crypto wallet and the theft of a physical wallet that contains bank notes differently. However, even for torts that lack a physical interaction between the parties, such as the theft of crypto assets through hacking, the criterion of the place of the causal event remains helpful as even those torts will usually involve an action or decision that can be pinpointed to a specific place. It is this versatility of the criterion that has led Peter Mankowski to describe the *locas actus* as a "sleeping beauty" (in the context of international jurisdiction).[44] Besides, the criterion also has the advantage of best reflecting the defendant's expectations as to the legal system governing its behaviour, even where it takes place online.[45]

The criterion however runs into problems when applied to torts that consist of multiple acts that do not necessarily take place in a single country. Where these acts are committed by different alleged tortfeasors (*e.g.* in a Distributed Denial of Service (DDoS) attack), the law of each place of acting can easily be applied to each of them. Where these acts are committed by a single tortfeasor, on the other hand, it appears appropriate to try to identify the most significant act, the location of which should determine the applicable law. This would be in line with the jurisprudence of the CJEU, which has held that even in case of consecutive acts of infringement of a Community Design,

> the correct approach for identifying the event giving rise to the damage [under Article 8(2) of the Rome II Regulation] is not to refer to each alleged act of infringement, but to make an overall assessment of that

43 See also Martiny (n 28), 564; Tobias Lutzi, *Private International Law Online* (Oxford: Oxford University Press 2020), para. 5.79 (regarding its appropriateness in internet cases more generally).

44 Peter Mankowski, "Der Deliktsgerichtsstand am Handlungsort – die unterschätzte Option," in Rolf A. Schütze (ed), *Fairness Justice Equity. Festschrift für Reinhold Geimer zum 80. Geburtstag* (Munich: Beck 2017), 430.

45 Lutzi (n 43).

> defendant's conduct in order to determine the place where the initial act of infringement at the origin of that conduct was committed or threatened.[46]

Although identifying this place may not always be straightforward in purely practical terms,[47] if the claimant has already managed to identify an alleged tortfeasor, the claimant might also be able to pinpoint a place in which the defendant may plausibly have acted.[48]

In the context of trademark infringements committed by reserving certain key words in Google's AdWords service,[49] the CJEU has also decided that the relevant act[50] is the activation of a technical process, rather than its execution by a service provider.[51] This reasoning can helpfully be extended to the use of bots and algorithms.

Where it is impossible to identify a particularly relevant act out of numerous acts spread across different countries, a sensible fallback option might consist in applying the law of the alleged tortfeasor's country of habitual residence, at least if it is among the countries in which the alleged tortfeasor has acted.[52] This might also provide a solution for cases that would otherwise produce completely arbitrary results (*e.g.* where a tort is committed while travelling on a train that passes numerous countries) or would be open to manipulation – if

46 Judgment of the Court (Second Chamber) of 27 September 2017, *Nintendo Co. Ltd. v BigBen Interactive GmbH and BigBen Interactive SA*, Joined Cases C 24/16 and C 25/16 (ECLI:EU:C:2017:724), para. 103. See also Judgment of the Court (Fourth Chamber) of 21 May 2015, *Cartel Damage Claims (CDC) Hydrogen Peroxide SA v Akzo Nobel NV et al.*, Case C-352/13 (ECLI:EU:C:2015:335), paras. 47–49, for some similar considerations regarding international jurisdiction.

47 See Florence Guillaume, "Aspects of private international law related to blockchain transactions," in Daniel Kraus, Thierry Obrist, and Olivier Hari (eds), *Blockchains, Smart Contracts, Decentralised Autonomous Organisations and the Law* (Cheltenham: Edward Elgar 2019), 64.

48 See also Dickinson (n 3), para. 5.12.

49 Rebranded as Google Ads in 2018.

50 For the purpose of jurisdiction under Article 7(2) of the Brussels Ia Regulation (Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, [2012] OJ 351/1) ("Brussels Ia Regulation").

51 Judgment of the Court (First Chamber), 19 April 2012, *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH*, Case C523/10 (ECLI:EU:C:2012:220), para. 34. See also Judgment of the Court (Fourth Chamber) of 22 January 2015, *Pez Hejduk v EnergieAgentur. NRW GmbH*, Case C-441/13 (ECLI:EU:C:2015:28), para. 24.

52 See Mankowski (n 44), 435.

the legal system in question does not allow for exceptions to the strict *lex loci delicti* approach anyway.[53]

3.2 *The Place of the Damage*

Although often lauded for its higher degree of predictability,[54] the place of the damage (*locus damni*) is a notoriously problematic connecting factor for online torts,[55] which often produce effects in many places at once while having virtually no connection to any particular physical place.[56] As far as crypto assets are concerned, these problems manifest themselves in both types of situations described above.

Regarding tortious interference with someone else's assets, the difficulty will usually consist in identifying the place where the damage materialised. Except for cases of theft or destruction of a physical device containing a private key, the immediate damage will usually consist in nothing more than a certain asset no longer being linked to the victim's public key. This is true for a wide range of torts, from the theft of a private key through hacking (and subsequent transfer of funds) to the extortion of crypto assets. In all of these cases, identifying the *lex loci damni* will make it necessary to localise the loss of the asset. This can arguably be done in two ways. First, the loss could be understood as being the consequence of a specific block being irreversibly added to the ledger in question, making every place in which the latter is physically stored a place of the damage. For a technology that relies on the widespread, potentially global distribution of the relevant information, this hardly seems helpful. Second, the loss could be understood to occur in the place in which the victim's wallet is stored. While this might instinctively appear as a more appropriate solution, it will rarely constitute an actual improvement over the former approach: since a wallet ultimately consists of nothing more than a set of keys, which can be stored on countless different media and in an infinite number of places, the location of the wallet is almost as unpredictable and arbitrary as the location of the ledger.[57]

Still, focusing on the wallet reveals another, potentially more helpful avenue. Given that control over a wallet is exercised through mere knowledge of a unique combination of letters and numbers, it might be considered to be

53 See *infra* section 4.

54 See Proposal for a Regulation of the European Parliament and the Council on the Law Applicable to Non-Contractual Obligations ("Rome II"), COM(2003) 427 final, 2003/0168 (COD), 11–12.

55 See Lutzi (n 43), para. 4.68.

56 Lutzi (n 43), paras. 2.35–40.

57 See also Guillaume (n 47), 63–64; Steinrötter (n 28), para. 48.

located wherever the person, who either has legitimate knowledge of the key or effectively controls the access to it, is located. Accordingly, the wallet could be considered to be localised either at the seat of the entity controlling the wallet on behalf of its "owner"[58] or at the habitual residence of said "owner."[59] The High Court of Justice of England and Wales seems to have adopted a similar approach when it considered English law to apply to alleged torts against victims domiciled in England.[60] These decisions have been criticised for equating the "owner's" domicile with the *situs* of the cryptocurrencies controlled by them[61] and for failing to take into account the case law of the CJEU,[62] which is indeed notoriously hesitant to equate the place in which the claimant's assets are concentrated with the place of damage in cases of pure financial loss.[63] Still, the particular importance of effective control in the context of crypto assets indeed provides a powerful argument in favour of considering the place from which such control is exercised as the place in which the relevant loss occurred.

If the victim does not transfer crypto assets, but is tricked into paying traditional currency in exchange for crypto assets that later turn out to be worthless, the immediate damage could plausibly be considered to already materialise in the victim's bank account, rather than in the crypto wallet. In a series of decisions on cases of prospectus liability (which is not free from ambiguity),[64] the CJEU has indicated that at least where the assets acquired have effectively

58 See Gössl (n 32), para. 73.

59 For similar lines of reasoning, see Dickinson (n 3), para. 5.12; Lehmann (n 32), para. 605; Lehmann (n 3), paras. 213–14; Martiny (n 28), 564. *Contra* Guillaume (n 47), 65.

60 *Fetch.AI Limited et al.* (n 13), para. 14; *Ion Science Ltd* (n 12), reported by Held (n 12). See also, in more detail, Held, Chapter 8 of this volume, sub 2.3 and 2.4.

61 See Held (n 12), 272.

62 See Amy Held and Matthias Lehmann, "Hacked crypto-accounts, the English tort of breach of confidence and localising financial loss under Rome II" (2021) 36 Journal of International Banking and Financial Law 708, 710–11; Amy Held and Matthias Lehmann, "Hacked Crypto-Accounts and the Continued Importance of Rome II in the English Courts: Fetch.AI v Persons Unknown" (*The EAPIL Blog*, 18 January 2022) <https://eapil.org/2022/01/18/hacked-crypto-accounts-and-the-continued-importance-of-rome-ii-in-the-english-courts-fetch-ai-v-persons-unknown/>.

63 See Judgment of the Court (Second Chamber) of 16 June 2016, *Universal Music International Holding BV v Michael Tétreault Schilling and Others*, Case C-12/15 (ECLI:EU:C:2016:449), paras. 31–32, 35; Judgment of the Court (Second Chamber) of 10 June 2004, *Rudolf Kronhofer v Marianne Maier and Others*, Case C-168/02 (ECLI:EU:C:2004:364), para. 20. See also Matthias Lehmann, "Where Does Economic Loss Occur?" (2011) 7 Journal of Private International Law 527, 537–540.

64 See Tobias Lutzi, "Ein wenig Wind um nichts: Das Bankkonto als Schadensort?" (2019) 39 Praxis des Internationalen Privat- und Verfahrensrechts 290, 290 et seq.

been worthless at the time of purchase, the place of the immediate damage is the place of the victim's bank account (*i.e.* the seat of the bank).[65]

Finally, if a tort is directed at the crypto network itself, for example because it is committed through manipulation of the consensus mechanism, there seems to be no way around trying to localise the ledger itself. Since it is a feature of most DLT applications that the ledger is simultaneously stored in a high number of virtually unpredictable places, this exercise will often result in a vast mosaic of applicable laws.[66] In closed and relatively small networks, which can be administered by even a single entity, it might indeed be possible to pinpoint the 'location' of the network. In all other cases, though, the *locus damni* should ideally provide nothing more than a starting point for the search of the law most closely connected to the case.

4 The Closest Connection

One of the reasons that the *lex loci delicti commissi* rule has stood the test of time despite the inappropriate results it occasionally produces is the fact that many legal systems allow their courts to deviate from its mechanical application in appropriate cases. While this deviation originally concerned cases in which both parties had a common domicile or residence in a country other than the one of the tort,[67] some systems, including the Rome II Regulation[68] (the provisions of which will continue to apply in the UK),[69] have meanwhile adopted a more open-textured exception that allows for the application of the law of the country to which the case is "manifestly more closely connected."[70]

Such escape clauses are particularly useful in the growing number of situations that only have a tenuous connection to the *locus delicti* (if at all), but may still be connected to a particular legal system. This is the case for many torts

65 Judgment of the Court (First Chamber) of 12 September 2018, *Helga Löber v Barclays Bank PLC*, Case C-304/17 (ECLI:EU:C:2018:701), para. 36; *Harald Kolassa* (n 25).

66 See Lehmann (n 3), paras. 207–08. Applying these laws distributively (following the so-called "mosaic approach") is only possible where the resulting damage can be split between the different countries concerned.

67 Graziano (n 37), 1711. See also Article 4(2) of the Rome II Regulation (n 21); Article 133(1) of the Swiss PILA (n 41).

68 Article 4(3) of the Rome II Regulation (n 21).

69 By virtue of Section 3 of the UK European Union (Withdrawal) Act 2018 and the Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc) (EU Exit) Regulations 2019, SI 2019/834, as amended by SI 2020/1574, Regulation 11.

70 On the underlying rationale, see COM(2003) 427 final, 2003/0168 (COD) (n 54), 12–13.

that are committed online, which increasingly take place within the normative environments of online platforms and similar ecosystems.[71] Similarly, while a tort the measurable effects of which are limited to a distributed ledger can prove difficult or even impossible to localise, it may still be closely connected to a particular legal system.[72]

Applying the escape clause to such a tort makes it possible, first, to take a pre-existing relationship between the parties into account.[73] Where the parties are personally bound to each other by a contract, the escape clause enables the courts to apply the *lex contractus* to all related claims between these parties. In the present context, this is especially relevant for active participants (nodes) in the same network, whose relationship may be characterised as contractual (depending on the nature and rules of the network in question).[74] While identifying the *lex contractus* will still be difficult even in this type of situation, the aim of legal certainty strongly militates in favour of extending the result of this exercise to any parallel claim in tort.

Even where the parties are not bound by a contract *inter se*, they may still be connected through a network of contracts that establishes a close link to a particular legal system. Especially in closed, centrally administered blockchains, participants will regularly be in a relationship with the host or administrator that can fairly be characterised as contractual. If these individual contracts contain a choice-of-law clause,[75] it should very much be in the interest of legal certainty to extend this choice also to the relationships between participants.[76] The same might be true for open networks that require all participants to agree to certain terms and conditions pointing expressly or implicitly to a certain legal system,[77] or if tokens are acquired under a law chosen by the parties to the transactions and the alleged tortfeasor (who may even by one of these parties)[78] is aware of this choice. If no choice has been made, it might still be possible to identify a close connection to a legal system, which would be

71 See Lutzi (n 43), paras. 5.122–24.

72 See also Michael Ng, "Choice of law for property issues regarding Bitcoin under English law" (2019) 15 Journal of Private International Law 315, 336–38 (regarding questions of property); Steinrötter (n 28), para. 49; Gössl (n 32), para. 74.

73 See Article 4(3), 2nd sentence, of the Rome II Regulation (n 21): "A manifestly closer connection with another country might be based in particular on a pre-existing relationship between the parties, such as a contract, that is closely connected with the tort/delict in question." See also Article 133(3) of the Swiss PILA (n 41). See also Martiny (n 28), 564.

74 See Dickinson (n 3), paras. 5.27–34.

75 Which is not unusual: see Lehmann (n 3), para. 150.

76 See Gössl (n 32), para. 75. See also Lutzi (n 43), para. 5.144, by analogy.

77 See Ng (n 72), 338 (regarding Bitcoin).

78 See Landgericht Berlin (n 25), para. 116, for a case of prospectus liability.

justified not only by considerations of party expectations and legal certainty but also by policy considerations: as more and more states are starting to claim prescriptive jurisdiction over (certain) crypto networks, it appears sensible to align the applicable tort law with the legal system to which a particular network is particularly closely connected.

A number of factual elements can be considered in order to establish such a relevant connection:[79] the nature of the right for tokens that transfer a right;[80] the seat of the administrator for centrally administered ("permissioned") ledgers;[81] the expectations of the initial programmers of the algorithm as to the governing law, as far as it is identifiable (sometimes referred to as the *lex creationis*);[82] the seat of the supervisory authority, as far as it can be identified with reasonable certainty.[83] Formulating general rules as to which of these connecting factors should take precedence would not only far exceed the scope of this paper but also hardly be possible given the wide range of torts and crypto networks, and their rapidly evolving structure. Still, if several of the aforementioned factors point towards the same legal system, the case for displacing the traditional *lex loci delicti* approach becomes increasingly convincing.[84]

5 Rules for Specific Torts

In reaction to the growing importance of tort law and the increasingly wide range of torts governed by the same set of general connecting factors, many systems have adopted specialised rules to cover specific types of torts for which the *lex loci delicti* rule has proven particularly inadequate.[85] In the present context, these rules should only play a residual role. Where they apply, though, the fact that they often focus on particular elements of the tort that are usually both more appropriate and easier to identify than the *locus delicti* significantly facilitates the conflicts analysis in cases of torts against virtual assets.

79 See also Gössl (n 32), para. 74.

80 See Landgericht Berlin (n 25), para. 115; see also Lehmann (n 3), paras. 172–174.

81 See Lehmann (n 3), paras. 157–158; Lehmann (n 32), para. 605.

82 See also Lehmann (n 3), paras. 151–154.

83 See *id.*, paras. 155–156; Gössl (n 32), para. 74; Steinrötter (n 28), para. 49–50.

84 See Landgericht Berlin (n 25), paras. 114–18, referring to numerous factors creating a close connection to German law (which the court deemed sufficient for the purpose of Article 4(3) of the Rome II Regulation (n 21), without having even tried to establish the necessary point of reference under its Article 4(1)).

85 See Graziano (n 37), 1715–16.

In EU PIL,[86] for instance, this is particularly true for the special rules on acts of unfair competition, which shift the focus towards the affected market.[87] The rules on product liability could similarly be seen as facilitating the search for the applicable law by offering a cascade of relevant connecting factors, although the CJEU has recently reiterated that only physical objects (and electricity) can constitute a defective product (in the context of the EU Product Liability Directive),[88] independently of the harmful information it may contain.[89] For claims based on data protection law, the General Data Protection Regulation (GDPR)[90] helpfully defines its own scope of application by reference to the place of establishment of the data processor/controller.[91]

The same cannot be said for the area of IP law, though. It seems to be almost globally agreed that claims arising from infringements of IP rights must be subject to the *lex loci protectionis*.[92] Applied to infringements committed on the internet, which make content available in countless places at once, this approach quickly runs into problems. Claimants need to seek protection under countless different national laws, while defendants are exposed to liability under just as many legal systems. For infringements committed in the context of a blockchain that is automatically and unalterably stored on a decentralised network of computers, potentially requiring global enforcement of a

86 In addition to the rules for specific torts discussed in this paragraph, this is also true for other non-contractual obligations, for which Articles 10–12 of the Rome II Regulation (n 21) shift the focus towards the putative or pre-existing relationship between the parties (if there is any).

87 See *id.*, Articles 6(1), (3).

88 Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, [1985] OJ L210/29. According to the Explanatory Memorandum of the Rome II Regulation (COM(2003) 427 final, 2003/0168 (COD), 13), the definition of the Directive also applies to the Rome II Regulation (*contra* Piotr Machnikowski, "Article 5 Rome II Regulation," in Ulrich Magnus and Peter Mankowski (eds), *ECPIL: Rome II Regulation* (Cologne: Otto Schmidt 2019), paras. 26–27).

89 Judgment of the Court (First Chamber) of 10 June 2021, *VI v KRONE – Verlag Gesellschaft mbH & Co KG*, Case C-65/20 (ECLI:EU:C:2021:471).

90 GDPR (n 27).

91 See *id.*, Article 3. On the question of whether Article 3 also governs the applicable law in areas in which the Regulation defers to the individual member states, see Merlin Gömann, *Das öffentlich-rechtliche Binnenkollisionsrecht der DS-GVO* (Tübingen: Mohr Siebeck 2021), 529–738.

92 See Paul Goldstein and Bernt Hugenholtz, *International Copyright. Principles, Law, and Practice* (Oxford: Oxford University Press 2010), 138. See also Article 8 of the Rome II Regulation (n 21), which according to Recital (26) of the Regulation preservers the "universally acknowledged principle of the *lex loci protectionis*."

given IP right, these problems are emphasised even more. With distributed ledger technology now also being actively discussed as a potential solution for the administration of copyright-protected works and their protection against online piracy,[93] it remains highly unfortunate that the proposed alternatives to the *lex loci protectionis* rule[94] have so far failed to gain traction outside of academia.[95]

6 Party Autonomy

In the interest of painting a complete picture, it should be mentioned that to the extent that PIL systems carve out a role for party autonomy in tort law,[96] a party choice of law might – in theory – also be possible in certain situations involving crypto assets.[97] Except for torts committed within a system of consensus rules that already include at least an implicit choice of law (which, as shown above, might also be taken into account in other ways),[98] it is highly unlikely that the participants in a decentralised and usually pseudonymous network select the applicable tort law.[99]

7 *Lex Cryptographia*

As with many other innovations in the context of the internet,[100] the proposal has been made to abandon the conflict-of-laws analysis altogether and instead

93 See, *e.g.*, Sebastian Pech, "Copyright Unchained: How Blockchain Technology Can Change the Administration and Distribution of Copyright Protected Works" (2020) 14 Northwestern Journal of Technology and Intellectual Property 1, 1 et seq.

94 See, *e.g.*, European Max-Planck Group on Conflict of Laws in Intellectual Property (CLIP), *Principles on Conflict of Laws in Intellectual Property* (CLIP 2011), Article 3:603; American Law Institute, *Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes* (American Law Institute 2008), § 321. See also Lutzi (n 43), paras. 5.163–172.

95 See, *e.g.*, *Pez Hejduk* (n 51), confirming a similar approach with regard to international jurisdiction.

96 See, *e.g.*, Article 14 of the Rome II Regulation (n 21).

97 See Guillaume (n 47), 70.

98 See *supra* section 4. See also Peter Mankowski, "Article 14 Rome II Regulation," in Ulrich Magnus and Peter Mankowski (eds), *ECPIL: Rome II Regulation* (Cologne: Otto Schmidt 2019), paras. 17–19.

99 See also Lehmann (n 3), paras. 148–49.

100 For a short overview of this line of thought, see Lutzi (n 43), paras. 2.14–15.

directly apply the consensus rules and similar norms that govern the crypto network in question as the *lex cryptographia*.[101]

While there certainly are some conceptual arguments that seem to support this proposal,[102] especially where it focuses more on overcoming flaws of traditional legal systems than on replacing them altogether, subjecting torts against crypto assets exclusively to a perceived *lex cryptographia* would not only clash with the discipline's traditionally strong focus on state law[103] but would also be subject to the same pertinent criticism that has prevented the *lex informatica* and similar constructs from ever gaining recognition as a serious alternative to state law.[104] The fragmented and opaque nature of such systems is especially pronounced in the case of crypto networks.[105] In addition, it would certainly be very difficult to find a legal basis for a direct application of the *lex cryptographia* in tort cases – on which it would rarely provide much guidance anyway.

Once again, this does not mean that PIL requires courts to completely ignore the normative context of a tort. *Au contraire*, it has long been acknowledged that identifying the applicable law does not prevent courts from considering rules that are part of a different legal system as "local data," which are part of the relevant matrix of facts.[106] For torts that are committed within the normative environment of a crypto network, for example through intentional violation or manipulation of the consensus rules, these rules must evidently be part of the analysis, regardless of whether or not these rules can be considered a legal system on their own.

---

101 See Guillaume (n 47), 71–75; Carla L Reyes, "Conceptualizing Cryptolaw" (2017) 96 Nebraska Law Review 384, 384 et seq; Aaron Wright and Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (*SSRN*, 10 March 2015) <http://dx.doi.org/10.2139/ssrn.2580664>.

102 See Lutzi (n 43), paras. 5.131–33.

103 As to which see Ralf Michaels, "The Re-state-ment of Non-State-Law: The State, Choice of Law, and the Challenge from Global Legal Pluralism" (2005) 51 Wayne Law Review 1209, 1228–31; Pierre Mayer, "Le phénomène de la coordination des ordres juridiques étatiques en droit privé" (2007) 327 Recueil des cours, para. 39.

104 See Lutzi (n 43), paras. 5.134–38.

105 See also Lehmann (n 3), paras. 50–51.

106 See Tim W Dornis, "Local Data," in Jürgen Basedow et al. (eds), *Encyclopedia of Private International Law* (Cheltenham/Northhampton: Edward Elgar 2017), 1166; see also Lutzi (n 43), paras. 5.147–49. This approach is reflected in Article 17 of the Rome II Regulation (n 21).

8 Conclusion

The protection of crypto assets provides an interesting test case for the traditional PIL rules in tort. It highlights the difficulty of localising pure economic loss, especially where it takes place within a decentralised, virtual environment, simultaneously stored on countless computers all around the globe.

At the same time, the problem emphasises the potential of two connecting factors, which will only become more relevant as our lives are spent increasingly online: first, the place of acting, which not only avoids many of the uncertainties involved in finding the place of the damage and often points to an applicable law that is both predictable and closely connected to the case at hand; and, second, an open-textured escape clause, which reflects the fact that a growing number of torts happen within environments that can be linked to a particular legal system. As in other online cases, trying to find the legal system that best reflects the parties' expectations as to the legal norms governing their behaviour in a seemingly virtual world arguably remains a more promising enterprise than trying to localise assets that are inherently delocalised.