Cambridge Law Journal, **84(1)**, March 2025, pp. 115–142 © The Author(s), 2025. Published by Cambridge University Press on behalf of The Faculty of Law, University of Cambridge. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.
doi:10.1017/S0008197325000042

INTERFERENCE TORTS IN THE DIGITAL ASSET WORLD

HIN LIU*

ABSTRACT. *Cases across the common law world have recognised digital assets as property, but the question of how such assets should be protected against interferences remains contested. At present, the "chattel torts" (conversion, trespass and reversionary injury) do not cover digital assets, leaving a gap in protection in respect of digital assets. There have been suggestions that the tort of conversion should be extended to cover digital assets, but this article argues that this extension would be undesirable for two reasons. First, there are fundamental differences between physical and digital assets, meaning that the concepts and thresholds used in the chattel tort context generate uncertain results (and create substantial risks of incorrect results) in the digital asset context. Second, the rules governing the chattel torts are unsatisfactory and contain many negative characteristics, and so extending the chattel torts to digital assets would replicate the same negative characteristics in the digital asset context.*

KEYWORDS: *digital assets*, *property law*, *conversion*, *chattel torts*, *blockchain*, *cryptoassets*, *law and technology.*

I. INTRODUCTION

Digital assets[1] have been gaining traction in recent years and various common law jurisdictions now recognise them as objects of property rights.[2] At the moment, however, there is no legal regime that deals with

*Lecturer of Law, University of Oxford. Address for Correspondence: Faculty of Law, University of Oxford, St. Cross Building, St.Cross Rd, Oxford OX1 3UL, UK. Email: hin.liu@law.ox.ac.uk. The author would like to thank Luke Rostill and Ben McFarlane for their invaluable comments on earlier drafts of this article.

[1] The term "digital asset" can have various meanings, but for the purpose of this article it is used to refer to an exclusively controllable asset on an electronic record that is rivalrous, fully divestible and independent of the legal system and other persons: see H. Liu, "Title, Control and Possession in the Digital Asset World" [2022] L.M.C.L.Q. 597, 598–99. The focus of this article will be on blockchain assets or "crypto-tokens": see Law Commission, "Digital Assets: Consultation Paper" (Law Com. No. 256, 2022), [10.2]–[10.5].

[2] As a matter of personal property law: see e.g. *Ruscoe v Cryptopia Ltd.* [2020] NZHC 728 (New Zealand), [2020] 2 N.Z.L.R. 809; *Bybit FIntech Ltd v Ho Kai Xin* [2023] SGHC 199 (Singapore); *AA v Persons Unknown* [2019] EWHC 3556 (Comm), [2020] 4 W.L.R. 35; *Toma v Murray* [2020] EWHC 2295 (Ch); *Fetch.ai Ltd. and another v Persons Unknown Category A and others* [2021] EWHC 2254 (Comm), 24 I.T.E.L.R. 566; *Litecoin Foundation Ltd. v Inshallah Ltd. and others* [2021] EWHC 1998 (Ch); *Janesh s/o Rajkumar v Unknown Person* [2022] SGHC 264 (Singapore); *Osbourne v Persons Unknown and another* [2022] EWHC 1021 (Comm); *Re Gatecoin Ltd.* [2023] HKCFI 914 (Hong Kong).

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

interferences with digital assets: the "chattel torts" are only applicable to assets that are amenable to possession and thus only apply to tangible assets, and other causes of action only offer piecemeal protection for digital assets. Where someone causes a digital asset to be frozen[3] or burned,[4] there is very little certainty as to what remedies would be available to a claimant. Considerable uncertainty also exists in many situations where someone has been denied access to a digital asset.[5] This uncertainty is unacceptable, as it encourages people to interfere with digital assets, drives up the cost of litigation and creates the risk of defendants being able to strong-arm individuals into settling for a low sum.

On the one hand, it has been argued by various academics that the tort of conversion should be extended to cover digital assets.[6] Similarly, the Law Commission in their Consultation Paper noted that there is a "good argument for extending the tort of conversion"[7] to digital assets. This is on the basis that digital and physical assets are similar enough[8] such that it would be arbitrary not to subject them to the same interference regime. Without such an interference regime being applicable to digital assets, owners and holders of digital assets would be insufficiently protected. Also, although the arguments have focused specifically on the tort of conversion, it is not only conversion that needs to be extended to cover digital assets if the full spectrum of "equivalent"[9] interferences[10] is to be

[3] Freezing involves disabling someone from being able to enter transactions on the blockchain in respect of the digital asset or, at a minimum, disabling someone from transferring the digital asset to another address. When a digital asset is frozen, it can often be "unfrozen" with the effect that the ability to enter transactions in respect of the digital asset can be restored.

[4] A token is burned if it is destroyed or if it is transferred to a "burn address" (an address with no private key). Where an asset is transferred to a burn address, no one can have control of the digital asset anymore and no one can enter any transactions in respect of the digital asset. The digital asset is rendered obsolete, even though it technically "remains" in the burn address.

[5] Nonetheless, the remedy of a constructive trust appears to be available where a digital asset has been transferred to the transferee's address as a result of theft (see e.g. *ByBit Fintech Ltd. v Ho Kai Xin and others* [2023] SGHC 199, at [41]–[44]). In other situations that involve (e.g.) a distributed denial of service (DDoS) attack that prevents someone from being able to access their digital asset or a smart contract bug that accidentally transfers the claimant's digital asset to another address such that he is unable to access its functionalities, the remedies available are highly uncertain.

[6] See e.g. S. Green and F. Snagg, "Intermediated Securities and Distributed Ledger Technology" in L. Gullifer and J. Payne (eds.), *Intermediation and Beyond* (Oxford 2019), ch. 16, 337, 345–48. This is a logical implication of an earlier argument made by Sarah Green and John Randall that conversion should cover "digitised products" such as software (which is "excludable" and "exhaustible"): S. Green and J. Randall, *The Tort of Conversion* (Oxford 2009), 118–28 (and see text to notes 37–39 below for excludability and exhaustibility); see also T. Cutts, "Possessable Digital Assets: Response to the Electronic Trade Documents Law Commission Consultation Paper No 254 and Call for Evidence on Digital Assets 2021" (LSE Law Policy Briefing Paper No. 47, 2021), 5–6, available at https://ssrn.com/abstract=3895404 (last accessed 1 May 2023).

[7] Law Commission, "Digital Assets: Consultation Paper", [19.104]; see also [19.89]–[19.123].

[8] In the sense that they are (inter alia) independent of the legal system and can be transferred and are capable of exclusive control.

[9] E.g. less severe interferences (such as partial and more minor impairments of use that are nonetheless unauthorised). I am also using "equivalent" in a loose sense: it is difficult to find the digital equivalent of a physical interference. See Section V(A) below.

[10] And interests (i.e. including reversionary interests).

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

covered. The other "property torts" or "chattel torts" of trespass and reversionary injury would also need to be extended to cover digital assets.[11]

On the other hand, this extension has not been supported in the most recent literature. For example, the Law Commission in their Final Report has taken the view that conversion in its current form should not be applied to digital assets, revising their stance from that taken in the Consultation Paper.[12] They reached this view on the basis that physical and digital assets behave very differently and that there are potential issues with the strict liability nature of conversion.[13] Similarly, the Dubai International Financial Centre (DIFC) considered but rejected the proposal to extend the chattel torts to digital assets, opting instead in favour of a new bespoke regime that deals with digital asset interferences.[14]

This article agrees with the view in the Law Commission Final Report as well as the DIFC Consultation Paper that the chattel torts should not be extended to digital assets.[15] It is suggested that this is for two reasons. First (and most fundamentally), physical and digital assets are very different in their nature, behaviour and respective environments, meaning that the concepts and thresholds used in the chattel tort context cannot be usefully applied in the digital asset context. This, coupled with the fact that digital assets are an asset class that judges tend to be substantially less familiar with,[16] creates uncertainty and a very substantial risk of producing the wrong normative result.[17] Second, the chattel tort rules themselves are unsatisfactory, needlessly complex and create problems for innocent defendants, and so applying such rules across to digital assets will mean that these negative characteristics will be replicated in the digital asset interference context.

This conclusion would be useful to a legislature, court or law reform body deciding how best to protect against interferences with digital assets. In order to know which means of protection would be best, one needs to know the problems with the chattel torts (and with applying them to

[11] Trespass covers less severe interferences and reversionary injury covers interferences that affect the holder of a reversionary interest who does not have a right to immediate possession: see Section IV(A) below.

[12] Law Commission, "Digital Assets: Final Report" (Law Com. No. 412, 2023), [9.72], [9.73].

[13] Ibid., at [9.72], [9.73].

[14] Dubai International Financial Centre, Digital Assets Law (No. 2 of 2024) (DAL), arts. 14, 15; Dubai International Financial Centre (DIFC), "Consultation Paper No. 4 – Digital Assets Law" (September 2023), [85]–[105], available at https://edge.sitecorecloud.io/dubaiintern0078-difcexperie96c5-production-3253/media/project/difcexperiences/difc/difcwebsite/documents/difc_docs/consultation_paper_difc-digital-assets-law.pdf (last accessed 25 May 2024). Both cited an earlier version of this article in reaching their conclusions: Law Commission, "Digital Assets: Final Report", [9.72]–[9.73]; DIFC, "Consultation Paper No. 4", 25, fn. 53.

[15] The Law Commission in their Final Report focus their arguments on the tort of conversion specifically, but there is no reason why their discussion would not apply to the chattel torts generally as well: see text to notes 7–9 above.

[16] As compared with physical assets.

[17] The phrases "wrong normative result" and "wrong normative threshold" are used a number of times in this article. By these phrases, I am referring to an outcome that produces an overly narrow or overly wide scope of liability or both (as a rule may be under-inclusive in some respects and over-inclusive in other respects).

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

digital assets), in order to compare the pros and cons of extending the chattel torts to digital assets against the pros and cons of any alternative means of protection proposed (e.g. a regime that is similar to that contained in Articles 14 and 15 of the DIFC's Digital Asset Law (DAL) 2024).[18] The purpose of this article is to contribute to such an exercise by (1) showing how extending the chattel torts to digital assets gives rise to many problems and is undesirable, and thereby (2) providing a significant reference point against which other means of protection can be compared.[19]

I will first outline the limitations of the chattel torts and how these limitations give rise to a gap in protection in respect of digital assets (Section II) and then describe the argument in favour of extending the chattel torts to digital assets as well as briefly outline the two substantive arguments against doing so (Section III). I will then discuss the structure and general features of an interference with a physical asset (Section IV). Next, I will discuss in more detail the two substantive arguments against extending the chattel torts to digital assets (Sections V and VI). Finally, I will discuss why the existence of "digital trespass and conversion" cases in other jurisdictions does not negatively impact the strength of the two substantive arguments against extending the chattel torts to digital assets (Section VII).

II. Possession, Intangibles and the Gap in Protection

At present, the chattel torts (conversion, trespass and reversionary injury) only apply to assets that can be possessed, and possession at present just applies to tangibles.[20] This means that the chattel torts do not apply to digital assets.

This carries various implications. The primary implication is that various core cases of the claimant's use of his digital assets being impaired (e.g. the defendant freezing or burning the claimant's digital asset) generally do not give rise to a remedy under English law as it currently stands,[21] whereas the equivalent[22] impairment in respect of a physical asset gives rise to a claim under the chattel torts.[23] Without extending the chattel torts to digital assets, we would need to rely on the economic torts, unjust enrichment, the

[18] DAL, arts. 14–15; see also accompanying commentary in DIFC, "Consultation Paper No. 4", [85]–[105], in particular [88]–[91].

[19] However, limitations of space mean that this article will not be exploring the positive claim of what any new regime should look like.

[20] See e.g. *OBG Ltd. and another v Allan and others; Douglas and others v Hello! Ltd. and others (No. 3); Mainstream Properties Ltd. v Young* [2007] UKHL 21, [2008] 1 A.C. 1; *Your Response Ltd. v Datateam Business Media Ltd.* [2014] EWCA Civ 281, [2015] Q.B. 41.

[21] The Law Commission discusses the example of burning: see Law Commission, "Digital Assets: Final Report", [9.46]–[9.69]. The same reasoning would apply to freezing a digital asset, since freezing involves a lower degree of interference with the digital asset given that it still exists in the same address and could in many cases be unfrozen.

[22] "Equivalent" in a loose sense: see note 7 above.

[23] E.g. the physical equivalent of burning a digital asset would be to burn a physical asset or throw it away such that it can never be retrieved: both acts would constitute conversion.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

intellectual property torts and the information torts; however, these causes of action offer limited protection to claimants in such a situation.

If a defendant freezes or burns a digital asset, the economic torts may not be of assistance. First, inducing breach of contract requires a prior contract, which may not exist. Second, the "causing loss by unlawful means" tort requires a prior civil wrong committed by the defendant against a third party that affects the liberty of such a third party,[24] which may not exist especially if the defendant is interacting directly with the blockchain. Third, deceit requires the defendant to make a representation and for the claimant to rely on it,[25] which would not apply in cases where the interference does not require the cooperation of the claimant and in cases where the defendant makes no representation to the claimant. Fourth, other economic torts such as conspiracy or intimidation would clearly be inapplicable in situations where the defendant acts alone[26] or if there are no threats involved.[27]

Unjust enrichment is also of limited assistance, because neither freezing nor burning involves enrichment to the defendant. In any event, there are issues with establishing the unjust factor.[28] Likewise, the intellectual property torts (e.g. copyright infringement) and the information torts (e.g. breach of confidence or misuse of private information)[29] may not assist in cases of freezing and burning because there is usually no intellectual property right that is being infringed,[30] and there is usually no use or disclosure of confidential or private information.[31]

As such, one may wonder whether the best solution to fill this gap would be to extend the chattel torts such that they apply in the digital asset context.

[24] J. Goudkamp and D. Nolan, *Winfield and Jolowicz on Tort*, 20th ed. (London 2020), [19-023]; *OBG v Allan* [2007] UKHL 21, at [29], [51] (Lord Hoffmann); *Secretary of State for Health and another v Servier Laboratories Ltd. and others* [2019] EWCA Civ 1160, [2020] Ch. 717.

[25] See M.A. Jones, A.M. Dugdale and M. Simpson (eds.), *Clerk and Lindsell on Torts*, 23rd ed. (London 2020), [17-05], [17-35].

[26] Conspiracy requires concerted action between two or more people: Goudkamp and Nolan, *Winfield and Jolowicz on Tort*, [19-039], [19-041].

[27] The tort of intimidation requires a "threat by the defendant to do something unlawful or 'illegitimate'": *Berezovsky v Abramovich* [2011] EWCA Civ 153, [2011] 1 W.L.R. 2290, at [5] (Longmore L.J.).

[28] There is no mistake by the claimant, no failure of consideration and no duress or undue influence. The closest unjust factor is the possible unjust factor of ignorance (also formulated as lack of consent or want of authority or powerlessness), but there is "some doubt" as to "whether the law of unjust enrichment recognises any of these unjust factors": R. Gregson, "Is Subrogation a Remedy for Unjust Enrichment?" (2020) 136 L.Q.R. 481, 488; see also W. Swadling, "Ignorance and Unjust Enrichment: The Problem of Title" (2008) 28 O.J.L.S. 627; W. Swadling, "Policy Arguments for Proprietary Restitution" (2008) 28 L.S. 506; T. Cutts, "Modern Money Had and Received" (2018) 38 O.J.L.S. 1, 9.

[29] See e.g. *Coco v AN Clark (Engineers)* [1969] R.P.C 41 (breach of confidence); *Campbell v Mirror Group Newspapers Ltd.* [2004] UKHL 22, [2004] 2 A.C. 457 (misuse of private information); Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, ch. 26.

[30] And even if a token is linked to an intellectual property right (e.g. in the case of some non-fungible tokens), burning the non-fungible token (NFT) does not constitute an *infringement* of the relevant intellectual property right.

[31] E.g. the majority of situations where a token is frozen or burned do not involve knowledge (and therefore any use or disclosure) of the token holder's private key. For example, when a blockchain administrator exercises a freeze or burn permission in response to a bug or hack (see Section V(B) below), this does not require knowledge of the token holder's private key.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

III. The Argument for Extending the Chattel Torts and the Two Arguments Against

The argument that conversion should be extended to intangible assets has been commonly made.[32] In respect of digital assets specifically, this argument has chiefly taken the form of the "anomaly" argument. Specifically, since both physical and digital assets can be stolen, transferred,[33] and are objects independent of the legal system, it would be anomalous to treat them differently. If misappropriating an iPhone (in a way that the claimant can no longer access it) constitutes conversion, so should misappropriating Bitcoin (in the form of an unauthorised transfer to a different blockchain address, such that the claimant can no longer access it). The similarity between physical and digital assets has been noted by the Law Commission as well as various academic commentators[34] who make the argument that they should be treated in like manner for the purpose of conversion (and presumably also the other chattel torts).[35]

Sarah Green and Ferdisha Snagg, for example, argue that there has been an over-emphasis on tangibility, noting that tangibility is merely a proxy for the distinction between "abstract" and "concrete" things: "tangibility historically *described* those things that were concrete, but it does not follow that it had any determinative influence on that categorisation."[36] The normatively significant distinction for the law's purposes is that between abstract and concrete things. Abstract things do not have an existence independent of the legal system and relationships between individuals (e.g. debts), but concrete things do have such an existence (e.g. tables, chairs and cryptosecurities).[37] It is this distinction (as opposed to the distinction between tangibility and intangibility) that should be determinative in deciding whether the chattel tort regime applies to a particular type of asset.

[32] See e.g. Green and Randall, *Tort of Conversion*, ch. 5; S. Green, "Theft and Conversion – Tangibly Different?" (2012) 128 L.Q.R. 564; S.L.K. Shaw, "Conversion of Intangible Property: A Modest, but Principled Extension? A Historical Perspective" (2009) 40 Victoria University of Wellington Law Review 419.

[33] I.e. factually transferred from "space" to "space".

[34] See e.g. Green and Snagg, "Intermediated Securities".

[35] See e.g. ibid., at 344–48. Green and Snagg refer only to conversion, but it would seem anomalous on their reasoning to exclude trespass and reversionary injury. Excluding the latter two torts would (1) provide no protection for lesser acts of impairment that do not constitute conversion and (2) prevent reversionary owners from recovering for interferences that would constitute conversion if committed against the "immediate" owner. Indeed, Green and Snagg mention other consequences that arise from cryptosecurities being capable of possession: for example, they would "be amenable to bailment" and "hav[e] the characteristic of negotiability" (at 348), so it would seem anomalous to exclude the possession-dependent consequence of being amenable to the torts of trespass and reversionary injury; see also Law Commission, "Digital Assets: Consultation Paper", [19.101]–[19.104], though their stance is more tentative: they state that "there is a good argument for extending the tort of conversion to data objects" (at [19.104]) and that "there are good policy arguments for the extension of the tort of conversion to data objects" (at [19.103]).

[36] Green and Snagg, "Intermediated Securities", 346; see also Green and Randall, *Tort of Conversion*, ch. 5.

[37] Green and Snagg, "Intermediated Securities", 346–47. Cryptosecurities are the main focus of Green and Snagg's article.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

This is because concrete things, unlike abstract things, are "excludable and exhaustible" in the sense that they can be lost and stolen (exhaustible)[38] and capable of exclusive control (excludable) regardless of whether a legal system exists and regardless of whether anyone claims rights in relation to them.[39] If an asset is excludable and exhaustible, "it can be possessed in a legal sense".[40] This therefore allows one to group digital assets together with chattels insofar as both types of assets are concrete things,[41] thus bringing in the protections of the chattel torts.[42] As such, the chattel tort regime should apply to digital assets (which are concrete things).

This argument for applying conversion (and by extension the chattel torts)[43] to digital assets may be further bolstered by the fact that the Law Commission has proposed the extension of possession to electronic trade documents, meaning that electronic trade documents can be converted.[44] If "possession" applies to electronic trade documents, it would (on this argument) be arbitrary not to apply the concept of possession to digital assets generally.

However, even if some digital assets satisfy this *statutory* definition of possession, it does not automatically follow that the same concept or term (possession) applies (1) generally as a matter of common law and (2) to *all* digital assets. In this statutory context, "possession" is used for a particular purpose and the legislation gives effect to a specific policy: to eliminate the differential treatment between physical trade documents and digital/electronic trade documents, given that they serve the same purpose in commerce.[45] In contrast, applying the same concept (possession) to digital assets generally carries much wider implications, as many doctrines depend on the applicability of the concept (e.g. bailment, possessory security, delivery and the chattel torts) and the normative balance is different in the context of digital assets. The stakes are also much higher, since extending possession to digital assets as a matter of general common law creates the risk of distorting the law.[46]

Nonetheless, other jurisdictions apply the chattel torts to intangibles: for example, in the US, there are cases applying conversion and trespass to digital assets.[47] There is also case law in the US, Canada and

[38] Ibid., at 347.
[39] Ibid., at 346.
[40] Ibid., at 346.
[41] They discuss distributed ledger technology (DLT) cryptosecurities, but the implication of their argument is that the tort should also apply to digital assets generally.
[42] See note 34 above.
[43] The Law Commission mentions conversion: see Law Commission, "Digital Assets: Consultation Paper", [19.89]–[19.124]. But again it would be anomalous to expand conversion but not trespass and reversionary injury since the interference regime would not cover "lesser interferences" with digital assets.
[44] Law Commission, "Digital Assets: Electronic Trade Documents" (Law Com. CP No. 254, 2021), [6.110].
[45] Ibid., at [2.1].
[46] See e.g. Liu, "Title, Control and Possession", 609–16.
[47] See e.g. *Williams v Mahmood*, No. 6:21-cv-03074, 2022 WL 17812998 (W.D. Mo. Dec. 8, 2022); *Archer v Coinbase, Inc.*, 53 Cal. App. 5th 266 (2020); *Kleiman v Wright*, No. 18-cv-80176, 2019 WL 3841931 (S.D. Fla. Aug. 15, 2019); *Shin v ICON Foundation*, No. 20-cv-07363, 2021 WL 1893117 (N.D. Cal. May 11, 2021).

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

New Zealand applying conversion in the context of non-crypto "digital assets"[48] such as digital files and domain names.[49]

However, it is suggested that the arguments for extending the chattel torts to digital assets are insufficiently focused on the big picture. Specifically, they assume that physical and digital assets share enough similarities that they can be treated in the same way for the purpose of the interference torts. This assumption breaks down when one considers the fundamental differences between the two types of assets, which have been noted by the Law Commission in their Final Report, as well as the DIFC in their DAL Consultation Paper.

Both the Law Commission[50] and the DIFC believe that conversion and/or the chattel torts should not be applied to digital assets, because the two types of assets are so fundamentally different. The Law Commission notes that chattels and digital assets "behave in different ways",[51] such that applying conversion in the digital asset context would not be desirable.[52] Similarly, in the DAL Consultation Paper, the DIFC notes that physical and digital assets are "very different in nature and surrounding environments", meaning that it would be difficult to avoid "creating unacceptable uncertainty or substantially increasing the risk of incorrect decisions" if the chattel torts were to be applied to digital assets. This corresponds with the first substantive argument of this article (explored in Section V).[53]

The DIFC gives another reason why the chattel torts should not be extended to digital assets. It notes that the existing chattel tort regime is "unsatisfactory and needlessly complex",[54] such that if it were to be extended to digital assets, the same "undesirable features [would be] replicated in the [d]igital [a]sset context".[55] This corresponds with the second substantive argument of this article (explored in Section VI).[56]

In order to contextualise the two substantive arguments of this article, it will be useful to set out the general structure and elements of an interference with a physical asset.

[48] Some use the term "digital assets" in a wider sense to encompass assets that are duplicable and non-rivalrous, such as domain names and digital files.

[49] See e.g. *Kremen v Cohen*, 337 F.3d 1024 (9th Cir. 2003); *Thyroff v Nationwide*, 2007 N.Y. Slip Op. 2442 (N.Y. 2007); *Canivate Growing Systems Ltd. v Brazier*, 2020 BCSC 232, [2020] B.C.J. No. 268; *Henderson v Walker* [2019] NZHC 2184. There are also trespass to chattels cases in the digital context, for example in the case of spam: see e.g. *Compuserve Inc. v Cyber Promotions*, 962 F. Supp. 1015 (S.D. Ohio 1997).

[50] In their Final Report: Law Commission, "Digital Assets: Final Report", [9.76].

[51] Ibid., at [9.73].

[52] Ibid., at [9.76].

[53] DIFC, "Consultation Paper No. 4", [91].

[54] Ibid., at [91].

[55] Ibid.

[56] Ibid.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

IV. The Interference Regime for Physical Assets

There is a general structure to every case of interference with a physical asset. First, there is an action taken by the defendant. Second, the action impacts the claimant's asset or his use of the asset (impact). Third, the link between the action and the impact is proximate enough (proximity/causation).[57] Fourth, the defendant also has a mental state when he performs the relevant action. Finally, we need to look at what constitutes a defence to the cause of action, even if the first four elements are satisfied.

In order to ascertain whether the chattel tort regime can be transposed into the digital asset context, we need to analyse the five elements in respect of physical asset interferences and determine the consequences of applying the same threshold to digital assets.

The five elements will be explored in turn.

A. Elements 1 and 2: Action of the Defendant and Impact on the Claimant's Asset or Use of His Asset

The first two elements will be discussed together because in the context of the chattel torts element 1 (the action of the defendant) forms part of the definition of element 2 (the impact on the claimant or his asset).

The duty on the defendant consists of a duty not to (deliberately) physically interfere with the claimant's asset.[58] In the context of elements 1 and 2, the requirement that the defendant must not physically interfere with the claimant's asset can be broken down into a few subduties. First, he must not take any deliberate positive action that physically damages the claimant's chattel. Second, he must not make any deliberate physical contact with the asset (which may happen through using his own body or through other means, such as through an object). Third, he must not completely impair the claimant's use of his asset (irrespective of whether there has been any physical contact or damage).[59] Fourth, he must not enter a transaction that deprives the claimant of his title to the asset.[60]

These four duties are covered by the three torts of conversion, trespass and reversionary injury.

[57] Sometimes there is no but-for causation, e.g. in the case of subsequent converters. But-for causation is not necessary to establish liability in conversion: "the court may treat wrongful conduct as having sufficient causal connection with the loss for the purpose of attracting responsibility even though the simple 'but-for' test is not satisfied": *Kuwait Airways Corpn. v Iraqi Airways Co. (Nos. 4 and 5)* [2002] UKHL 19, [2002] A.C. 883, at [74] (Lord Nicholls); see also S. Douglas, "The Nature of Conversion" [2009] C.L.J. 198, 221–22; and note 70 below.

[58] "Deliberately" as in deliberate act of interfering with the chattel, as opposed to any knowledge that the chattel is not theirs (since the mens rea of conversion is strict liability).

[59] *Burroughes v Bayne* (1860) 157 E.R. 1196; S. Douglas, "Actionable Interferences in the Chattel Torts: A New Perspective on Economic Loss?" in S. Degeling, J. Edelman and J. Goudkamp (eds.), *Torts in Commercial Law* (Sydney 2011), ch. 5, 87, 95–96.

[60] By way of sale: see Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-22].

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

Conversion covers the most severe types of interference. Specifically, it requires a deliberate action by the defendant that either (1) physically damages the chattel (or involves physically touching the chattel) in a way that totally or severely excludes the claimant from use of the chattel[61] (even for a temporary period)[62] or (2) directly excludes the claimant from using the chattel (for any period of time) despite a lack of physical contact or damage. Examples of (1) would include taking, selling,[63] or destroying the asset, or detaining the asset with an intention to assert title,[64] or transforming the asset in a way that it loses its essential identity.[65] As for (2), this includes a sale that deprives the claimant of his title,[66] and this results in a "total exclusion of use" in the sense that the claimant's use of the asset would involve the incurring of a liability to the new owner (given that he no longer has title).[67]

Indeed, partial impairments of use do not constitute conversion in the absence of physical contact, as demonstrated by *Club Cruise Entertainment and Travelling Services Europe BV v Department for Transport; The Van Gogh*.[68] In *Club Cruise*, an official served an administrative detention notice on the claimant shipowner, mandating it to stay in port. The detention notice turned out to be invalid and the claimant sued in conversion. The court held that there was no conversion, since there was no physical contact or restraint and the claimant still had possession of the ship.

Trespass requires intentional action by the defendant that physically touches or damages the chattel (and covers lesser interferences that are not serious enough to amount to conversion).[69]

[61] Examples of where the claimant's use of the asset is severely (but not totally) excluded would include adulteration of wine (*Richardson v Atkinson* (1723) 93 E.R. 710) or arguably a "transformation of goods so that they lose their essential identity" (see M. Bridge, L. Gullifer, K. Low and G. McMeel, *The Law of Personal Property*, 3rd ed. (London 2022), [33-019]).

[62] *England v Cowley* (1873) L.R. 8 Exch. 126.

[63] Specifically, selling the asset in an unauthorised way that involves physical contact with the good (the obvious example would be delivery of the asset to the buyer).

[64] In detention cases, the defendant is entitled to "adequate time to inquire into the rights of the claimant": *Clayton v Le Roy* [1911] 2 K.B. 1031, 1051 (C.A.) (Fletcher Moulton L.J.). As such, the defendant is not liable for the detention *per se* but a detention coupled with an intention to assert title: Bridge et al., *Law of Personal Property*, [33-032], fn. 179.

[65] Bridge et al., *Law of Personal Property*, [33-019] (transformation of the good so that it loses its essential identity).

[66] Specifically, a sale that does not involve delivery or physical contact. See Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-22] (discussing *nemo dat* exceptions).

[67] For conversion, there is no but-for causation requirement. Thus, if X takes C's goods without C's permission and D takes the same good from X without C's or X's permission, D is liable in conversion, despite the fact that, but-for D's taking, C would still have been excluded from using his good – D's act itself excludes C from using the asset. In the "causation" section (Section IV(B)), I discuss the intervening acts issue as opposed to the but-for causation issue (since there is no but-for causation constraint on the defendant's liability).

[68] [2008] EWHC 2794 (Comm), [2009] 1 All E.R. (Comm) 955.

[69] See e.g. Douglas, "Actionable Interferences", 88–92. Nonetheless, the author of ch. 16 of *Clerk and Lindsell on Torts* suggest that there should be no liability in trespass where the defendant's conduct has not "gone beyond generally acceptable standards of conduct" (citing *Collins v Wilcock* [1984] 1 W.L.R. 1172, 1178 (Q.B.)), such as where a pedestrian picks up a parcel that has been dropped by

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

Nonetheless, a person can only sue in conversion if he had actual possession or a right to immediate possession of the chattel at the time of the interference and can only sue in trespass if he had possession of the chattel at the time of the interference.[70] As such, many people with a reversionary interest in a chattel (e.g. a pledgor or a term bailor) would not be able to sue in conversion or trespass.

This is where the tort of reversionary injury becomes relevant. It covers any act that would constitute conversion, trespass (or negligence), but also requires actual damage,[71] and is only available to someone who has a reversionary interest in a chattel. A person with a reversionary interest will be able to sue in reversionary injury if there has been damage to *his* interest, as opposed to damage to merely the pledgee or bailee's interest.[72]

It is worth noting that not every impairment or change in form amounts to an interference. For example, Simon Douglas gives the example of a person who buys up all the local supplies of petrol.[73] This would lead to people's use of their cars being impaired, as the cars would not have fuel anymore and so people would not be able to drive their cars. However, this impairment is not interference for the purpose of the chattel torts, because, if such an action attracted liability in the chattel torts, this would unduly limit the liberty of defendants.[74]

Overall, physical contact or physical damage is a requirement for trespass and for conversions that do not amount to a total impairment of use. It is also a requirement for the equivalent reversionary injury claim,[75] provided there is actual damage.[76] If there is no physical contact with or physical damage to the chattel, the conduct requirement is increased (i.e. there must be a total impairment of use before there can be an interference).[77] Nonetheless, in most physical asset interference cases, physical contact or damage usually exists.

another person and returns it to him: Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-133].

[70] Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-43], [16-138].

[71] Ibid., at [16-151].

[72] *HSBC Rail (UK) Ltd. v Network Rail Infrastructure Ltd. (formerly Railtrack plc)* [2005] EWCA Civ 1437, [2006] 1 W.L.R. 643; see also Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-151] (the act needs to have "the effect of depriving him either temporarily or permanently of the benefit of his reversionary interest").

[73] Douglas, "Actionable Interferences", 92.

[74] There are various restrictions on a claimant's ability to recover for pure economic losses, which are carefully policed to prevent potential defendants from being exposed to too much liability. For example, inducing breach of contract requires knowledge that the course of conduct would amount to a breach of contract, plus an intention to procure such a breach: see Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [23-28]–[23-34]. Causing loss by unlawful means requires an intention to cause loss to the claimant: at [23-78].

[75] By the "equivalent" claim, I am referring to situations where someone is suing for damage to their reversionary interest, there is no total impairment of use of the chattel and they are suing for what would otherwise amount to a trespass or a conversion.

[76] Reversionary injury requires actual damage: see Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-151].

[77] Douglas, "Actionable Interferences", 95–96.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

B. Element 3: Proximity/Causation

There is a directness requirement for trespass,[78] meaning that there is a causation constraint that limits the defendant's liability. A defendant does not commit trespass if he lays a trap for a physical object to fall into.[79] As such, situations that potentially engage the "intervening acts of causation" debate are outside the scope of the tort.

In respect of conversion, the types of actions that constitute the tort all involve a very direct causal chain (e.g. taking or destruction of an asset).[80] There is no intervening act between the defendant's action and the impact on the claimant (or his asset), because the acts that involve conversion involve one of two patterns, both of which do not involve any act in between the defendant's action and the impact on the claimant (or much time in between). First, there are cases involving direct contact with the chattel (where the defendant's action and the impact on the asset happen at the same time (or almost at the same time)).[81] Second, there are cases involving a total exclusion of the claimant's use of the chattel without any act in between the defendant's action and the claimant's exclusion from use (such as *Burroughes v Bayne*).[82] As such, the "intervening acts of causation" debate is not relevant in the conversion context.[83]

These "causation" principles also apply in respect of reversionary injury, as the tort covers the same ground as conversion and trespass[84] insofar as deliberate interferences are concerned,[85] provided that a reversionary interest is damaged.[86]

C. Element 4: Mental State

The chattel torts impose strict liability.[87] This has been criticised on the basis that it is overly harsh on defendants and does not provide "fair warning",[88]

[78] Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-132]; Bridge et al., *Law of Personal Property*, [33-004].

[79] This would be too "indirect" to count as trespass. See also Bridge et al., *Law of Personal Property*, [33-004] (there is no trespass claim against a "defendant who, instead of feeding poisoned meat directly to the claimant's dogs, lays it down for them to find it"); *Hutchins v Maughan* [1947] V.L.R. 131, 134.

[80] And sometimes there may not be but-for causation, for example in the case of a subsequent converter: the defendant's action excludes the claimant from use of his chattel but the exclusion would still have occurred without the defendant's action.

[81] E.g. where the defendant takes the claimant's chattel.

[82] *Burroughes v Bayne* (1860) 157 E.R. 1196.

[83] For the purposes of *liability* in conversion. Some "causal chain" issues (such as mitigation) are relevant at the remedies stage: see e.g. Bridge et al., *Law of Personal Property*, [33-053].

[84] Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-151].

[85] Reversionary injury also covers negligent interferences with a reversionary interest: ibid., at [16-151]; but the focus here is on deliberate interferences.

[86] Actual damage is required: ibid., at [16-151].

[87] This means that the defendant would be liable irrespective of the reasonableness of his behaviour. He just needs to intend the act constituting the interference.

[88] See Section VI(C) below.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

but one could also justify it on the basis that elements 2 and 3 are narrowly constrained. Specifically, because physical contact or physical damage is a requirement where there is no total impairment of use, this provides some degree of fair warning. The boundaries of the physical thing provide a crucial limit to the potential scope of liability,[89] which reduces (or eliminates) the need for liability to be constrained by way of a mental element.

D. Defences

There are various specific statutory defences[90] and in terms of general common law the main defence is consent.[91] If the claimant expressly or impliedly consents to the interference, the defendant has a defence.[92]

V. Argument 1: Difficulty in Applying Chattel Tort Elements and Normative Balance to Digital Assets

The most fundamental reason why the chattel torts should not be applied to digital assets is that there are many significant differences between the nature, behaviour and environment of physical and digital assets. As a result, existing concepts that are used to resolve disputes in the physical asset context are not adequate to resolve disputes in the digital asset context.

There are various differences between physical and digital assets that are worthy of note. First, physical assets have a distinct molecular boundary that defines the space that they occupy, whereas digital assets have no distinct molecular boundary. Second, the blockchain environment is an "opt-in" environment that one has the option not to join, whereas the physical environment is something that we are part of no matter what. Third, the blockchain environment is "composable" in the sense that coders can define the features of the "blockchain world" they create to a much greater degree than a person in the physical world can define the features of the assets they create.[93] Fourth, a digital asset can only be accessed through a digital device, whereas a physical asset can be accessed by making contact with the (physical) space in which it is contained. Fifth, we have a much better idea of how physical assets work and behave, given that we interact with them on a daily basis and they occupy a molecular space that our senses are attuned to, meaning that we can spot

[89] See e.g. S. Douglas and B. McFarlane, "Defining Property Rights" in J. Penner and H.E. Smith (eds.), *Philosophical Foundations of Property Law* (Oxford 2013), ch. 10, 219, 239.

[90] See e.g. Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-81]–[16-87]; Torts (Interference with Goods) Act 1977, s. 8(1); Insolvency Act 1986, ss. 234(3), 307(4), 346(7); Cheques Act 1957, s. 4.

[91] There are other common law defences based on ministerial handling, as well as based on the bailee acting on the bailor's orders: see Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [16-77], [16-78]. There is also the defence of illegality: at [16-88].

[92] See e.g. Bridge et al., *Law of Personal Property*, [33-009].

[93] Assets in the physical world are subject to the constraints of physical laws (gravity, friction, etc.).

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

dangers arising out of them by using our senses (primarily vision and touch). This stands in contrast with digital assets where we are unable to spot similar dangers, given that the code-governed environment is unfamiliar to most people and many cases of impairment may occur outside our knowledge or foresight.

Because of these differences, concepts that are adequate to resolve disputes in the physical asset context are not adequate to resolve disputes in the digital asset context. They do not yield determinate results[94] in the digital asset context: for example, in the case of concepts such as physical interference or physical contact, the nature and environment of digital assets is such that no direct analogy with physical assets can be drawn.[95]

Yet, a judge still needs to make a decision on a given set of facts and so he or she will need to try and find the equivalent of physical interference or physical contact. However, there will not be a precise equivalent and whichever equivalent is applied will be (at best) a rough approximation. We also do not know which approximation the judge will apply, given that there are many possible options (explored below).[96]

This creates an unacceptable amount of uncertainty for parties, given that they will find it extremely difficult to predict their legal positions (since each proxy or approximation generates a substantially different scope of liability)[97] and parties will need to litigate[98] in order to find out their legal positions.[99] This creates a substantial risk of a chilling effect on users of the blockchain[100] (including centralised exchanges and operators of blockchains) as they may fear liability under the chattel torts if they take certain digital actions (and, in particular, actions on the blockchain).[101]

Apart from the problem of uncertainty, there is a significant risk that judges will produce the wrong normative threshold by picking an inaccurate equivalent. Since digital assets are technically complex and thus difficult to understand, judges may be misled into using an inaccurate proxy that produces an overly wide or narrow scope of liability. Alternatively, judges may pick a proxy that can no longer be

[94] Or at least results that are determinate enough.

[95] See Section V(A) below.

[96] See Section V(A) below. Because there is no direct equivalent, there are many possible "proxies", but each "proxy" generates a substantially different scope of liability.

[97] See Section V(A) below.

[98] Or there must be a case that is relevant enough to the parties' situation, e.g. one involving facts that are very similar to the parties' situation and that states the relevant rule in a way where it is clear enough what the outcome of the litigation would be.

[99] This puts defendants in a worse position than the "strict liability" scenario in Section VI(C) below where one can in many circumstances be able to find out their legal position by verifying whether someone owns a good.

[100] Creating chilling effects in this way carries the undesirable effect of stifling useful economic activity and innovation/experimentation on the blockchain.

[101] Such as an exchange executing an on-chain transfer of an asset (to which it only has an inferior relative title) to a third party by transferring it to him on-chain or a blockchain administrator freezing tokens in response to a suspected hack.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

seen as an equivalent to the corresponding chattel tort requirement, which effectively modifies the threshold in respect of the chattel torts while paying lip service to the requirement in question.

Judges may also produce the wrong normative threshold through directly applying the physical asset threshold to digital assets. This is because the differences in physical and digital assets (and the different policies at work) justify different requirements and applying the same requirement produces undesirable results in the digital asset context. An example that will be explored below relates to the role of digital asset "kill switches"[102] in the context of the consent defence.[103]

A. No Proxy for Physical Interference

First, in the digital asset context, there is fundamentally no equivalent of, or proxy for, the physical contact/damage requirement for trespasses and for conversions that do not lead to a total impairment of use.[104]

Physical assets have physical boundaries (i.e. molecular boundaries) and the physical contact/damage requirement provides a very important limit to the scope of liability, especially given that the chattel torts attract strict liability. It is relatively easy to identify whether there has been physical contact (touching of molecules that constitute the chattel) or physical damage (a change in the molecular structure of the chattel that renders the chattel less useful or valuable).[105] This also allows a clear distinction to be drawn between a physical interference and an impairment of use: there can be one without the other.

There is no equivalent of physical contact or physical damage to (or physical interference with) a digital asset. A digital asset is ideational and common ways in which destruction or denial or impairment of access occur include where the defendant causes (1) the freezing of the asset, (2) a "denial of service" attack, (3) a transfer of the asset to another address (whether it is a smart contract or wallet address and whether it has a private key or not)[106] or (4) destruction of the asset through burning. There is no equivalent of a physical boundary that people can walk into and interact with, because of fundamental differences in the nature of physical and digital assets. These differences

[102] A kill switch is a programmed permission to interrupt, intervene in or terminate the execution of instruction(s) on the blockchain. This can take the form of permission(s) to freeze, burn and/or transfer digital asset(s). Typically, kill-switch permissions are given to the operator or administrator of a blockchain, the issuer of a digital asset or the creator of the smart contract from which the digital asset is minted.

[103] See Section V(B) below.

[104] There is, however, no need to find a proxy in case of total impairments of use (since there is no physical interference requirement for total impairments of use: see Section IV(A) above).

[105] See Douglas, "Actionable Interferences", 89: there needs to be harm to the "actual physical structure" of the chattel and a mere impairment of use is insufficient to constitute physical damage.

[106] Burn addresses do not have private keys.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

mean that, unlike physical assets where one can cleanly distinguish impairment of use and physical interference, one cannot cleanly distinguish impairment of use of a digital asset from digital interference with the asset.

If one applies the physical damage/contact requirement[107] literally to digital assets, this will result in the claimant having no remedy in situations that involve freezing his digital asset in a way that partially impairs the use of his digital asset. This is because there is no physical damage/contact, which means there is no liability in trespass or conversion.

Nonetheless, are there any proxies that can serve as adequate substitutes for such a requirement? One possibility would be to limit actionable interferences to "on-chain" actions (as opposed to "off-chain" actions). This means that a defendant who does not take any action on the blockchain (e.g. "calling a function")[108] would not be liable for interference. This to some extent mirrors the fact that, if a defendant does not interact with or physically damage a chattel, he would not be liable in the chattel torts (unless there is a total impairment of use).

This in essence could be seen as underpinned by a "fair warning" rationale that preserves the liberty of the defendant: one should interact with the blockchain at one's own risk, but there is no liability if one does not interact with the blockchain. Similarly, with the chattel torts, the message is that one interacts with chattels at one's own risk, but there is no liability if one does not interact with chattels (unless there is a total impairment of use).

To approximate the chattel tort position further, this on-chain interference requirement could be imposed in relation to partial impairments of use, but not for total impairments of use.

However, there are two problems with using an on-chain interference requirement as a proxy. First, this requirement does not actually provide fair warning. Any on-chain function (when executed) may be a triggering condition for some other digital asset being burned or frozen.[109] To prevent this outcome, the defendant would need to search *all* of the smart contracts that exist and ensure that no digital asset would be burned or frozen as a result of executing/calling the intended function. Indeed, the analogy between "interacting with a physical asset" and "interacting with a blockchain" is a loose one. In the physical asset context, it is reasonably expected that one is supposed to "keep off" a physical asset. This is because (1) the general expectation is that

[107] Which would apply if there is no total impairment of use.
[108] Calling a smart contract function on the blockchain.
[109] Blockchain developers merely need to code this into their application as an if-then statement. They have an extremely high degree of freedom when building their applications on the blockchain: they can provide for any functionality that is compliant with the programming language used by the relevant blockchain (e.g. Solidity, in the case of Ethereum).

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

someone may (or is likely to) own it and (2) one can avoid interacting with it because it has visible boundaries, meaning that a defendant can keep off it without expending much mental energy.[110] In contrast, interacting with a blockchain (even intentionally) does not (and ought not to) give rise to the expectation of "keeping off any digital assets", because (1) a digital asset has no visible boundaries and (2) it is difficult to avoid conclusively the outcome of a digital asset being burned or frozen as a result of an on-chain interaction.

Second, the on-chain interference requirement would result in an under-inclusive rule that protects claimants insufficiently. For example, it would exclude a distributed denial of service (DDoS) attack by a defendant (which can be an off-chain activity) that prevents the claimant from being able to access his digital asset. This would happen, for example, if the claimant's private key is stored on a particular website and/or mobile application that is the subject of the DDoS attack.[111] Another example would be where there is a DDoS attack on blockchain network nodes that prevents the claimant from being able to access his asset for a substantial period of time.[112] There could also be a DDoS attack on the relevant application programming interface (API) that connects the front-end application or website (used by the claimant to access his digital assets) with the blockchain back-end architecture, meaning that the claimant would be unable to access his digital asset through the application or website.

Another possibility would to be to impose a directness requirement for digital asset interferences, by analogy with the directness requirement in trespass to goods.

However, the analogy breaks down on a very fundamental level. With physical assets, we know *what* should be directly caused in the trespass context (i.e. the physical interference: physical contact or physical damage). In contrast, with digital assets, we do not know what should be directly caused (i.e. the impairment of use, the function call, etc.). Thus, imposing a directness requirement merely begs the question of what proxy we should use as an equivalent of physical interference, because we need to know what needs to be directly caused before the analogy with trespass can stand.

Nonetheless, could we use a directness requirement to constrain the scope of interference, even though we do not know what must be directly caused?

[110] Douglas and McFarlane, "Defining Property Rights", 239–40; T.W. Merrill and H.E. Smith, "The Architecture of Property" in H. Dagan and B.C. Zipursky (eds.), *Research Handbook on Private Law Theory* (Cheltenham and Northampton, MA 2020), ch. 8, 134, 142.

[111] As the private key is stored on such an application, a denial of service attack that prevents the claimant from accessing the application means that the claimant would not be able to access the private key and thus access his digital asset(s), assuming he does not keep a copy of the private key.

[112] This kind of attack does not need to involve any on-chain action: a regular botnet DDoS attack can achieve the same effect.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

It is suggested that a directness requirement is too vague. Directness usually means sufficient proximity in relation to the (1) time taken between the defendant's action and the relevant consequence and (2) number of events between the action and the consequence, and also means that (3) the original action carries a high degree of influence in generating the relevant consequence.[113] However, these three elements are very open-ended and are difficult to apply to digital assets since it is difficult to generate a determinate result purely from applying these criteria. For example, it is difficult to know the boundaries of each of the criteria[114] and the weighting of each factor, and this creates room for judges to be able to manipulate instrumentally the criteria to reach a desired result, at the expense of the law's predictability and consistency.

Another proxy may be one based on the direct linguistic equivalent of "(intentional) physical contact": namely, "(intentional) digital contact". However, if "digital contact" (i.e. interacting with a digital device or system) were to be the equivalent threshold, there would simply be no fair warning to potential defendants (especially since conversion is a strict liability tort).

This contrasts with the position as regards physical assets, because physical assets have a boundary (and so avoiding intentional physical contact or damage is relatively easy). It is (relatively) not a big ask to require a person not to make contact intentionally with physical objects in his proximity, not to perform intentional acts that lead to damage to physical objects and not to perform intentional acts that lead to someone being totally excluded from using a physical object. Given these constraints, it may be argued that imposing strict liability provides a substantial degree of fair warning to defendants.[115]

By contrast, in the digital asset context, people intentionally interact with functions on-chain and update data off-chain, in a way that may cause damage, destruction, or exclusion of access to digital assets without them knowing. It is difficult to know when one's conduct will cause such consequences.

For example, in the context of the prediction markets, someone might deploy a smart contract for the purpose of a sports bet and designate a website as the source of authority for the final score. Funds (in the form of digital assets) would be locked up in that smart contract (and could, for example, be jointly owned by all parties to the bet) and subsequently distributed to the person who wins the bet. The smart contract can designate any website as the "ultimate source of information" for the

[113] As opposed to e.g. a significant cause of the consequence being the voluntary action of C.
[114] E.g. what is the "allowable time period" between the action and the damage/consequence?
[115] Nonetheless, the strict liability nature of conversion has been criticised for its harshness on innocent defendants: see Section VI(C) below.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

final score and the problem arises where such a website misreports the relevant score, causing the tokens to be distributed to the wrong person.

In this case, there is potential liability for causing the "diversion" or "misappropriation" of a digital asset. This liability could attach to the operator of *any* website that shows sports scores. It is difficult for the operator of any such website to know whether the information displayed on their website is being used for the purposes of a smart contract oracle. Extrapolating further, the same issues would apply to prediction markets more generally and, importantly, in the context of financial derivatives.

When coupled with strict liability, the requirement of digital contact would make people hypervigilant, would lead to a waste of people's mental energy in thinking about whether they might be liable and might cause them to take preventive or defensive action. As such, their liberty (and economically useful activity) would be stifled. This position is similar to that in respect of pure economic loss, where a high mental requirement is imposed.[116] The law does not impose strict liability for causing pure economic loss, because doing so would stifle ordinary activity and make people hypervigilant.[117] Indeed, the ethos of the blockchain as an open-source environment where people are encouraged to experiment with code[118] should be respected: imposing strict liability in the blockchain environment would run directly counter to such an ethos.

B. Blockchain Environment/Policy (v Physical Environment/Policy)

The blockchain environment is very different from the physical environment and this means that the policies that are relevant in the blockchain world produce a different normative balance as compared to those in the physical world. This means that the scope of defences available (as well as the scope of prohibited actions) in respect of digital asset interferences are likely to be very different to that in respect of physical assets.

For example, there can be kill switches and other coded permissions that are given to people so that they can (e.g.) burn or freeze an asset. If such people burn or freeze an asset with the intention of doing so, this would be an intentional action that directly leads to C's use being impaired or destroyed (as he would not be able to transfer the asset and (in the case of burning) not be able to access the asset as well). Such situations may arise, for example, if there has been a bug or hack (or a suspected bug or hack) and the developer/administrator exercises the kill switch to

[116] For example, inducing breach of contract requires knowledge that the course of conduct would amount to a breach of contract, plus an intention to procure such a breach: see Jones, Dugdale and Simpson (eds.), *Clerk and Lindsell on Torts*, [23-28]–[23-34]. Causing loss by unlawful means requires an intention to cause loss to the claimant: at [23-78].

[117] There would be potentially indeterminate liability.

[118] For example, composability is a crucial feature of the blockchain: people can use and combine existing code to create new applications.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

investigate what has been happening with the code, with the effect that the claimant is no longer able to use or access his asset at all.[119] This would constitute the equivalent of a physical conversion,[120] and there is no defence to conversion that applies here. The consent defence would not apply in many (or most) instances since claimants in many (or most) instances would not even be aware of such a kill switch or permission,[121] and so there is no express or implied consent.[122] Also, even though the defendant may argue that the claimant opted into the blockchain world (and his particular protocol) and thus consented to its rules (or "logic"), this would not succeed. This is because such "logic consent" does not involve actual consent (whether express or implied) or perhaps even hypothetical consent (i.e. where the claimant would have consented if he was made aware of the effect of the protocol rules).

However, there is a strong argument that this is the wrong normative result[123] and that a defence ought to be available in (at least some) such circumstances. This is because the kill switch/permission was constructed as part of the blockchain environment. It was deliberately created (i.e. the effect was intended), as opposed to being an accidental consequence of bad programming.

A particular blockchain environment can be constructed in a multitude of ways and one can create the rules that govern such a blockchain environment/application. This stands in contrast with the physical environment where the physical laws are relatively fixed/immutable. As such, if a blockchain developer decides to design a blockchain that includes a kill switch that is intended to be used in circumstances where the assets are in danger of imminent misappropriation or destruction by a hacker or in danger of being destroyed by an unintended bug, affording no defence to the developer where those precise circumstances exist (despite the lack of consent from the claimant) may be thought to be unfair. This is because it frustrates the very purpose of the developer's deliberate design choice to add in a kill switch to protect the integrity of the blockchain.[124]

[119] Under this specific example, the claimant cannot access or use the asset at all. In other circumstances, a freeze permission may be exercised but the claimant can still access certain functionalities in respect of the asset (e.g. the ability to sign a signature from the address in which the asset is contained and/or exercise a voting right in respect of it).

[120] Here there would be a total impairment of use.

[121] In case there is any ambiguity, "permission" here refers to the coded permission (the factual power to freeze or burn the asset that is given to the developer/administrator under the relevant code), as opposed to permission (consent) given by C in relation to the impairment of use.

[122] In general, people are not aware of kill switches or burn/freeze permissions in respect of a particular digital asset, because they do not read (or understand) the underlying code that contains such permissions or any associated documents that may alert them to the possibility of such permissions. In this general scenario, there would be no actual (express or implied) consent to the exercise of such permission(s).

[123] Specifically, that there is too much liability on the defendant.

[124] When the integrity of the blockchain is under threat, this creates the potential for a lot of harm and the harm that would otherwise be caused by the bug or hack would often be much greater than the harm caused to the claimant's asset whose use is (non-consensually) impaired as a result of using the kill

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

Also, a blockchain environment is an opt-in environment (in the sense that a person can choose whether to engage with it or not), unlike the physical environment (which every person has no choice but to engage with). If one chooses to enter a blockchain environment, it would seem fair to suggest that, in certain circumstances within people's reasonable expectations,[125] those with kill-switch/burn permissions should be allowed to exercise their power to transfer/freeze assets as intended by the design of the blockchain.

However, a claimant is not reasonably expected to look out for his blockchain environment in the same way that he is expected to look out for his physical environment. Looking out for one's physical environment merely requires one to be (visually and kinaesthetically) attentive to one's surroundings, which is already habitual for most people and thus does not take much effort. In contrast, looking out for one's blockchain environment carries vastly higher information costs, as it requires a detailed understanding of code (which the vast majority of people do not have) as well as the ways in which it could malfunction. Indeed, even programmers cannot anticipate all bugs/loopholes in the code, so it would be extreme to suggest that an average user of the blockchain should be expected to do so. Thus, if the particular use of a kill switch is outside a claimant's reasonable expectations, a defendant in general ought not to be afforded a defence.

Overall, it is clear that the threshold of fair warning and the relevant contextual considerations are very different across physical and digital assets, which means one would expect a substantially different scope of liability in respect of interferences with the latter.

VI. Argument 2: Chattel Tort Rules Themselves Are Unsatisfactory and Arguably Too Harsh

The law surrounding chattel torts is unsatisfactory. The rules themselves are messy and needlessly complex, in that they are weighed down by unnecessary conceptual baggage and shrouded in vague language. Also, the strict liability of the chattel torts is arguably too harsh as it gives rise to problems for innocent defendants. Therefore, applying the same rules to digital assets would lead to the same undesirable features being replicated in the digital asset context.

switch. This is because many people can be affected at once by such hacks and bugs, a large amount of high value assets can be quickly misappropriated or drained, further damage could be done to the blockchain and internal company operations, and limiting the (potential or actual) damage from these hacks and bugs is a time-sensitive task.

[125] Such as where there is an imminent danger of a hack that significantly threatens the security of the assets on the relevant blockchain.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

Three features will be explored: (1) the "right to immediate possession" concept, (2) the lack of a universal definition of conversion and vague formulations of the tort and (3) the strict liability nature of the chattel torts.

A. Right to Immediate Possession

The right to immediate possession concept is highly problematic and should not be applied in the digital asset context.[126] It is used to determine the outer limits of whether a person has title to sue in conversion,[127] but the language of right to immediate possession is fundamentally vague and does not provide much guidance. It is unhelpful insofar as "right to immediate possession" is synonymous with "right to sue for interference with possession" and it is also unhelpful insofar as a person with title to the good already has a right to possess the good.[128] In this sense, the notion of a right to immediate possession does not provide much further guidance on what is required to have title to sue for conversion. It does not easily map onto the threshold of "you must have title[129] but not have granted a chattel lease or pledge" and many judges have made mistakes (e.g. in holding that a mere contractual right to possession confers title to sue).[130]

This vague language of right to immediate possession is problematic because it obscures the issue of whether the chattel lease is a derivative interest, as well as the *numerus clausus* debate that informs it.[131] These issues are fundamental and need to be clarified, because the general principle across property law is that a person with title can sue for interference unless he has granted a derivative interest. Yet, these considerations are not confronted in the conversion context and are hidden under the concept of the right to immediate possession. At the same time, the technical language gives it the appearance of legitimacy despite it merely being a conclusory label: "a right to immediate possession" describes the default rights of a person who has title (insofar as he has a right to exclude), but is vague and unhelpful as a *test* for who has the right to sue for interference. This gives judges room to reach a desired conclusion without transparent reasoning to justify it.

If the right to immediate possession concept were to be applied in the digital asset context, this conceptual confusion (as well as room for opaque reasoning) will be replicated, and the fundamental *numerus*

[126] For more discussion of this point, see e.g. Liu, "Title, Control and Possession", 611–12.
[127] A person can sue in conversion if they have actual possession or the right to immediate possession.
[128] See Liu, "Title, Control and Possession", 611.
[129] This includes relative titles.
[130] As noted by Nicholas Curwen: see N. Curwen, "Title to Sue in Conversion" [2004] Conv. 308, 312–16.
[131] The *numerus clausus* debate is engaged because the issue arises as to whether the chattel lease is on the permitted list of property rights under English law and, if not, whether the reasons in favour of recognising it on the list of property rights outweigh the reasons against: see e.g. Liu, "Title, Control and Possession", 611; see also B. McFarlane, "Identifying Property Rights: A Reply to Mr Watt" [2003] Conv. 473, 486–87.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

clausus and fragmentation of title[132] issues will not be clarified let alone confronted.

B. Definitions and Formulations of Conversion

Furthermore, there is no universal definition of conversion and the current formulations of conversion are vague. Indeed, Lord Nicholls in *Kuwait Airways Corpn. v Iraqi Airways Co. (Nos. 4 and 5)*[133] stated that it is "well nigh impossible" to define the tort,[134] and Selvam J. also noted that conversion is "too elusive to be expressed in words".[135]

The lack of a clear formulation of the tort makes it difficult for people to know the normative threshold for interference, insofar as it requires them to slice through a layer of conceptual baggage to discern what the general normative threshold is.

For example, conversion has been referred to as a denial of the claimant's title to the chattel[136] by a defendant's assertion of title over the claimant's chattel.[137] This formulation does not provide much practical guidance, as it does not answer the very questions of (1) what acts constitute a *denial* of title and (2) what acts constitute an *assertion* of title by the defendant. Similarly, conversion has been described as an "intentional act or dealing with goods" that is "inconsistent with or repugnant to the rights of the owner".[138] This again does not provide much practical guidance, because it fails to answer the very question of when the act becomes "inconsistent with" or "repugnant to" the rights of the owner.[139] It is far from clear that formulations like "denial and assertion of title" or "inconsistency" or "repugnancy" map onto the substantive threshold for conversion set out in Section IV.[140]

Such formulations, if interpreted at face value, can produce many different results. It is difficult to infer the general threshold for interference from such formulations/definitions and it is necessary

[132] This issue arises because the chattel lessor is not allowed to sue, yet the chattel lease does not contain the features of a proprietary interest. See e.g. S. Douglas, *Liability for Wrongful Interferences with Chattels* (Oxford 2011), 33–36 (chattel lease does not contain the features of a proprietary interest).

[133] [2002] UKHL 19.

[134] Ibid., at [39] (Lord Nicholls states that "framing a precise definition of universal application is well nigh impossible").

[135] *The Endurance I ex Tokai Maru* [2000] SGHC 99, at [30]. Likewise, William L. Prosser has noted that some of the definitions of conversion have been "so general and so vague in their terms as to be meaningless": W.L. Prosser, "The Nature of Conversion" (1957) 42 Cornell Law Review 168, 168.

[136] Bridge et al., *Law of Personal Property*, [33-014], fn. 115.

[137] Ibid., at [33-014]; *Francis Hollins and Others v George Fowler and Others* (1874–75) L.R. 7 H.L. 757, 785 (Brett J.) ("acts done with the intention of transferring or interfering with the title to or ownership of [goods], or which are done as acts of ownership of them"); *Lancashire and Yorkshire Railway Co. and others v MacNicoll* [1918–19] All E.R. Rep. 537, 540–41 (Atkin J.) ("an intention on the part of the defendant . . . to deny the owner's right or to assert a right which is inconsistent with the owner's right").

[138] *Bunnings Group Ltd. v CHEP Australia Ltd.* [2011] NSWCA 342, 82 N.S.W.L.R. 420, at [124] (Allsop P.).

[139] Indeed, Allsop P. also quoted Lord Nicholls's statement in *Kuwait Airways v Iraqi Airways* [2002] UKHL 19, [2002] A.C. 883 that the tort is "well nigh impossible" to define precisely: ibid.

[140] See Section IV above, in particular Section IV(A).

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

therefore to slice through a layer of conceptual baggage in order to discern what the general threshold is. This causes confusion and uncertainty: indeed, the authors of *The Law of Personal Property* note that "much of the difficulty in conversion lies in estimating the required seriousness of the defendant's interference",[141] and similarly Douglas notes that it is an "almost impossible task for a lawyer to advise a client on the merits of a possible claim"[142] outside certain well-established categories of conversion. These problems will be replicated in the digital asset context, as judges will not be able to discern with ease what the threshold requirement for interference is and may reach arbitrary decisions because of the lack of guidance provided by the existing formulations of conversion.

Also, the fundamental purpose of vagueness is to provide the necessary flexibility to respond to context, to avoid running the risk of making the formulation overly precise (which causes over-inclusiveness and under-inclusiveness).[143] However, the vagueness that exists in the chattel torts goes beyond what is necessary to respond to context. One can be a lot more precise than this, for example, by adopting a formulation of conversion that makes it reasonably clear what is required: Douglas, for example, suggests that conversion should be defined as an "intentional exercise of exclusive control" over another's chattel.[144] As with the right to immediate possession, the existence of vague rules also creates room for judges to bend[145] doctrine to reach the right normative result, which compromises the transparency of the judge's reasoning. This ought not to carry forward into the digital asset context.

C. Strict Liability

Furthermore, the strict liability nature of the chattel torts is arguably too harsh on innocent defendants, as it holds them liable for honest but

[141] Bridge et al., *Law of Personal Property*, [33-014].

[142] Douglas, "Nature of Conversion", 198.

[143] See e.g. T. Endicott, "Law Is Necessarily Vague" (2001) 7 Legal Theory 379; T.A.O. Endicott, *Vagueness in Law* (Oxford 2000).

[144] See Douglas, "Nature of Conversion", 199. This yields significantly more determinate results than formulations such as "denial" and "assertion" of title or intentional acts that are "inconsistent" with or "repugnant" to the rights of the owner, which are either circular or insufficiently helpful. Such formulations are vague and do not act as a sufficient constraint on the outcomes that can be reached by a judge in a particular case. For example, the notion of whether the defendant's action is "repugnant" to the rights of the owner is a matter of subjective judgement and gives rise to a very wide possible range of interpretations and thus outcomes that can be reached in a particular case. This stands in contrast with Douglas's proposed formulation, because the idea of an intentional exercise of "exclusive [physical] control" is relatively clear in English law (such as in the adverse possession context: see e.g. *Powell v McFarlane and Another* (1979) 38 P. & C.R. 452, 470–71 (Slade J.); *J A Pye (Oxford) Ltd. and Another v Graham and Another* [2002] UKHL 30, [2003] 1 A.C. 419, at [40]–[41] (Lord Browne-Wilkinson)) and is much less subjective, thus significantly constraining the possible outcomes that can be reached by a judge.

[145] By "bend(ing)", I am referring to changing the shape of a doctrine or concept such that it is incompatible with its underlying rationale.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

reasonable mistakes.[146] For example, if an asset is sent to the defendant and he sends it to someone else under the (honest and reasonable) mistaken belief that the asset is his, he commits conversion and is liable to pay the full value of the goods to the defendant.[147] This can be seen as an unfair result, because it often defeats reasonable expectations of the defendant, given that there are many situations where such a defendant may very reasonably believe that he owns the relevant good.[148] Also, it becomes very hard for people to plan their activities in such a way that they can predict the legal consequences of those activities and they would either (1) need to expend time and cost to verify whether the asset is owned by someone else (in order to avoid the risk of liability) and often never find out the answer or (2) simply refrain from acting (or attempt to avoid getting themselves into situations where goods may be owned by a third party). Insofar as this result is thought to be unfair,[149] it should not be replicated in the digital asset context.[150]

For example, a centralised digital asset exchange could receive a cryptocurrency from a client (especially if it has done the relevant AML/KYC[151] checks) into its own address where the client did not have the best title.[152] In this case, the exchange would receive the client's (inferior) title[153] and either hold it on trust or hold it outright subject to a contractual obligation to return an equivalent quantity of cryptocurrency.[154] If the exchange later uses the cryptocurrency for proprietary trading and executes an on-chain transfer of the

[146] N. Curwen, "The Remedy in Conversion: Confusing Property and Obligation" (2006) 26 L.S. 570, 582–83; S.F.C. Milsom, *Historical Foundations of the Common Law*, 2nd ed. (London 1981), 379; A. Tettenborn, "Conversion, Tort and Restitution" in N. Palmer and E. McKendrick (eds.), *Interests in Goods*, 2nd ed. (London 1998), ch. 32.

[147] He is also liable if he mistakenly believes he is authorised to do so. Professor Milsom provides the example of an "innocent auctioneer [who] sells another's property": see Milsom, *Historical Foundations*, 379. See also *Willis v British Car Auctions* [1978] 1 WLR 438, 442 (auctioneer liability for sale and subsequent delivery to purchaser).

[148] Or that there is no one with a superior title, or that his action(s) are authorised. A defendant is liable no matter how bona fide his belief that there is no adverse interest: see e.g. *OBG v Allan* [2007] UKHL 21, at [311] (Baroness Hale).

[149] For general arguments that strict liability is unfair or has the potential to be unfair, see e.g. E.J. Weinrib, *The Idea of Private Law*, revised ed. (Oxford 2012), ch. 7; T. Nagel, *Mortal Questions* (Cambridge 1979), 31; H.L.A. Hart, *The Concept of Law*, 2nd ed. (Oxford 1994), 173, 178–79. Also, the Law Commission notes that the strict liability nature of conversion means that there may be "unjustified . . . liability in tort [in the digital asset context]" should conversion be extended to digital assets, for example in situations where "participants will interact with digital objects – largely by taking control of them – without knowing any information about their counterparty": see Law Commission, "Digital Assets: Final Report", [9.73].

[150] Also, where the relevant action from the defendant does not involve a *purchase* (e.g. where a defendant freezes or burns (or executes an on-chain transfer of) a digital asset he believes he owns), a bona fide purchase defence would not operate to avail him even if such a defence were to exist. Thus, even with a bona fide purchase defence, having strict liability would not offer sufficient protection to defendants insofar as such a regime would still hold them liable for honest but reasonable mistakes.

[151] Anti-money laundering (AML) and know your customer (KYC).

[152] I.e. where he had an inferior relative legal title.

[153] There is currently no bona fide purchase defence for digital assets.

[154] H. Liu, L. Gullifer and H. Chong, "Client-Intermediary Relations in the Crypto-Asset World" in P.S. Davies and C-H Tan (eds.), *Intermediaries in Commercial Law* (Oxford 2022), ch. 11, 213.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

cryptocurrency to its counterparty (without knowing of the defect in title),[155] this would prima facie constitute a conversion in the absence of a bona fide purchase defence[156] and the true owner[157] could bring an action against the exchange. This can be seen as an undesirable result as it causes problems for innocent exchanges: they may end up being liable in conversion and thus take defensive measures to avoid this risk, even if such measures cause a wasteful depletion (or otherwise inefficient use) of their assets.[158]

VII. "Digital Trespass and Conversion" Cases in Other Jurisdictions

At this point, one may nonetheless argue that the existence of "intangible trespass and conversion" cases in other jurisdictions means that extending the chattel torts to digital assets does not pose a problem. It is argued that this conclusion is mistaken, for two reasons.

First, most of the cases involving conversion and trespass to intangible assets do not involve an interference with digital assets: they mainly involve impairments of use of digital files or domain names.[159] It does not follow that digital assets should be covered by conversion and trespass.[160] There are policies specific to the digital asset environment that are not relevant in the context of digital files or domain names, such as the composability of the underlying blockchain environment. This leads to the wrong normative threshold being applied to digital assets, for example where (as mentioned earlier)[161] the consent defence in conversion and trespass does not take into account the fact that a defendant blockchain administrator ought to be able to impair use of a claimant's digital assets in some situations where he needs to engage a kill switch and freeze the state of the blockchain in order to prevent a suspected bug or hack.

In any event, some of the conversion cases involving intangible assets can be recharacterised. For example, where the claim involves impairment of use of a domain name (e.g. where the defendant fraudulently persuades the domain name registrar to register a domain name in his favour), this is in essence a claim for pure economic loss. A domain name involves a contractual right against the service provider and a domain name by

[155] I.e. where the exchange does not know that it does not have the best title.

[156] Nonetheless, although there is currently no bona fide purchase defence for digital assets, the Law Commission is suggesting that there should be a bona fide purchaser rule that applies to all cryptoassets: see Law Commission, "Digital Assets: Consultation Paper", [13.84], [13.50]–[13.90]. It remains uncertain whether this change would be implemented.

[157] I.e. the person with the best title.

[158] See also City of London Law Society, "Law Commission Consultation Paper on Digital Assets: Response of the City of London Law Society" (4 November 2022), 17, available at https://archive.clls.org/storage/2022/11/Law-Commission-Consultation-FINAL-4-November-2022.pdf (last accessed 1 May 2023).

[159] As well as spam cases: see e.g. *Compuserve v Cyber Promotions*, 962 F. Supp. 1015 (S.D. Ohio 1997).

[160] And reversionary injury.

[161] See Section V(B) above.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

itself confers no title to any separate object of property (such as the underlying computer servers that perform the relevant operations in respect of the domain name). Here, there would be a remedy under the unlawful means tort.[162] It is suggested that, since there is no interference with any concrete object of property to which the claimant has title or a possessory interest,[163] domain name interferences should not by themselves[164] fall within the scope of the property torts.

Second, although there are US cases that have applied the chattel torts to digital assets,[165] this does not change the fact that the two substantive arguments in this article still apply as far as English law is concerned. The fact that the chattel torts apply to digital assets in the US[166] does not remove the fact that the cases often involve complex factual scenarios that require nuanced balancing acts (where the English chattel torts are unsuited to dealing with). An example would be *Shin v ICON Foundation*,[167] where an unintended loophole in the code caused the claimant to mint extra tokens for free. The defendant administrators of the blockchain system froze the claimant's tokens without his consent.[168] The system rules enabled such freezing to occur and the act of freezing was intended to reverse the effects of the loophole/bug in the code.

The conversion issue was not fully dealt with in the judgment given the nature of the application,[169] but a judge who is tasked with tackling the issue in full would need to deal with a complex and nuanced balancing act. One needs to balance (1) the fact that the defendant impaired the use of the claimant's digital asset and (2) the fact that the claimant minted extra tokens in accordance with the rules of the system/program, against (3) the defendant's desire to reverse the unintended effects of the program.

If we were to apply the English law chattel torts to the facts of *Shin*, we would again run into the risk of the physical asset threshold producing the wrong normative result in the digital asset context. Assuming there is a relevant interference (based on the fact that there was a complete

[162] There would be deceit against X (the domain name registrar): there has been a fraudulent representation to the domain name registrar, which the registrar has acted upon. Even if the registrar suffers no loss as a result of the deceit, the "wrong to third party" element is satisfied: *OBG v Allan* [2007] UKHL 21, at [49] (Lord Hoffmann).

[163] The terminology of a "possessory" interest is ambiguous, but I am referring to an inferior relative title or a derivative interest such as a pledge. Also, the Law Commission has noted that domain names are not data objects because they are not independent of the legal system: see Law Commission, "Digital Assets: Consultation Paper", [8.19], [8.24].

[164] I.e. in the absence of damage to any physical object.

[165] See e.g. *Williams v Mahmood*, No. 6:21-cv-03074 (W.D. Mo. Dec. 8, 2022); *Archer v Coinbase, Inc.*, 53 Cal. App. 5th 266 (2020); *Kleiman v Wright*, No. 18-cv-80176 (S.D. Fla. Aug. 15, 2019); *Shin v ICON*, No. 20-cv-07363 (N.D. Cal. May 11, 2021).

[166] More precisely, in some US jurisdictions.

[167] *Shin v ICON*, No. 20-cv-07363 (N.D. Cal. May 11, 2021).

[168] And compelled Binance and Kraken to freeze the tokens that were transferred to them. Given limitations of space (and for the purposes of simplicity), I will focus on the tokens frozen directly by ICON.

[169] See e.g. *Shin v ICON*, No. 20-cv-07363, at 15–18 (N.D. Cal. May 11, 2021) (conversion issue dealt with briefly). The case involved a motion to strike.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press

impairment of use of the claimant's digital assets), the consent defence would not be available to the defendant since the claimant did not consent to the freezing of the tokens. However, the consent defence does not take into account the fact that it may be justified for the defendant to exercise a kill switch especially in situations where there was an unintended loophole/bug in the code that was exploited by the claimant. Ultimately, after balancing the relevant considerations, a judge may reach the conclusion that, from a normative perspective, there should not be a defence, but the problem is that there is simply no doctrinal tool capable of accommodating these competing considerations. Having no defence *to consider* apart from consent[170] means that this crucial issue does not even end up being discussed.

VIII. Conclusion

This article has argued that, although there is a gap in protection in respect of digital assets, it should not be filled by extending the chattel torts. Physical and digital assets are too different in terms of their nature, behaviour, environment and underlying policies, and judges are substantially less familiar with digital assets as compared to physical assets. This means that the concepts that are used to resolve disputes in the physical asset space are either unhelpful or produce the wrong normative result in the digital asset space. This is compounded by the fact that chattel tort rules are unsatisfactory in that they are vague, needlessly complex and create problems for innocent defendants, and so applying the chattel torts to digital assets will lead to a replication of these mistakes in the digital asset context.

As such, the task of ascertaining the appropriate scope and method of protection in respect of digital asset interferences should be approached without the baggage of the chattel torts. Ideally, it should be approached afresh, so that the normative issues can be tackled from the ground up.

[170] Statutory defences are not relevant in this situation.

https://doi.org/10.1017/S0008197325000042 Published online by Cambridge University Press