Article:
Sheehan, D. (2024) Digital Assets, Blockchains and Relativity of Title. Journal of Business Law, 2024 (1). pp. 78-100. ISSN: 0021-9460

Digital Assets, Blockchains and Relativity of Title

Duncan Sheehan*

The Law Commission has recently published its final report on *Digital Assets.*[1] It is a wide-ranging look at the private law and characterisation of such assets. One fundamental question that must be asked about digital or crypto-assets is how we conceptualise ownership of them. The Law Commission make a number of recommendations and proposals, concerning the nature of property in digital assets and whether it can be seen as a tertium quid, traditionally seen as impossible because all assets are either choses in possession or choses in action.[2] It is also concerned with control as an indicium of legal title, transfers and collateral arrangements, and remedies for interference with such assets.[3] This article concentrates on those recommendations and conclusions that bear on the nature of digital assets as private property.

These questions are important; case law is reasonably clear that digital assets are potentially objects of property,[4] but doubts and questions remain. Technology alone does not provide an answer to competing claims to assets. Technology can prevent on-chain double spending, but it provides no solution to creditor claims, arising off-chain. Execution could be obtained against a defendant, but no immediate technical solution prevents the latter transferring their crypto-assets away. There is no technical solution to prevent hackers transferring crypto-assets away, appearing as the owner and passing the assets to third parties;

---

* Professor of Business Law, University of Leeds. An early version of this paper, based largely on the Commission's consultation paper, was presented at the Obligations X conference in Banff, Canada in July 2023. My thanks to the participants in the discussion, particularly to Kelvin Low. My thanks also go to members of the City of London Law Society Financial Law Committee and Mark Evans (Travers Smith LLP) in particular for discussing these issues and their own (very similar) concerns with me. Any remaining errors are mine alone.

[1] Law Commission, *Digital Assets* (HMSO, 2023) Law Com. no. 412

[2] *Colonial Bank v Whinney* (1885) 36 Ch. D. 261

[3] Law Comm (n 1) ch. 10

[4] See eg *AA v Persons Unknown* [2019] EWHC 3556; *Ruscoe v Cryptopia* [2020] NZHC 729; *B2C2 v Quoine Ltd* [2020] SGCA (I) 02; *Wang v Derby* [2021] EWHC 3054; *Janesh s/o Rajkumar v Unknown Person (Chefpierre)* [2022] SGHC 264; *CLM v CLN* [2022] SGHC 46; *Re Gatecoin Ltd* [2022] HKCFI 914

nor is there a technical solution to recovering assets invalidly transferred by an under-age and incapax owner. These are all legal questions and problems of competing claims are facilitated by the technology.[5] We can only fully understand the possible legal solutions if we understand what ownership of such assets amounts to and how it is to be identified.

This in turn requires us to understand more fully what type of assets these are. There are many different types of crypto-asset and they can be subdivided as a class in different ways. Some crypto-assets exist for the purpose of being exchanged. Bitcoin is an example of such a crypto-currency used primarily as a medium of exchange. It is also native to the Bitcoin protocol in the same way that ether is native to the Ethereum protocol. Ether was designed as a medium of payment to buy "gas" or processing power on the Ethereum blockchain. Because the Ethereum blockchain has the capacity to run smart contracts, which the basic Bitcoin protocol cannot, it has the capacity to allow a variety of applications to run on it; that needs to be paid for. A blockchain protocol might therefore also house other crypto-tokens which can serve a variety of functions. Some types of crypto-currencies known as stablecoins, such as Tether, track the value of a fiat currency and may count as a claim against an issuer. There is no issuing authority for bitcoin – which is indeed part of the point. Tether, however, is tied to the US dollar and at least claims to be fully backed by liquid dollar assets.[6] Another distinctive category is that of non-fungible token, which represent, or at least are said to represent, title to unique assets – typically associated with collectible artwork-[7] but tokens can be linked to almost any asset in a variety of different ways. What matters, however, is that all of these assets are recorded on a blockchain and exist as a string of data held at a particular public address on

[5] J Woxholth, DA Zetzsche, R Buckley & D Arner 'Competing Claims to Cryptoassets' University of Hong Kong Faculty of Law Research Paper no. 2023/27 p7

[6] https://tether.to/en/ (visited 5 May 2023); there has not in fact been a full audit of this and there is scepticism as to whether Tether is fully backed. See eg J Griffin and A Shams, 'Is Bitcoin really Untethered?' (2020) 75 Journal of Finance 1913

[7] See generally K Low, 'The Emperor's New Art: Cryptomania, Art and Property' [2022] Conv. 382

the relevant blockchain. Blockchains also come in different varieties. For our purposes in this paper, we concentrate on permissionless blockchains, such as the Bitcoin blockchain or Ethereum, as these are the major and globally most used blockchains; bitcoin and ether are also the most valuable, by market capitalisation, cryptocurrencies in the world.

This article is divided into three main sections. In the first we examine the nature of the blockchain, crypto-tokens and the technical processes by which they are held or transferred. In the second we reject the idea that such assets can be possessed. In the third we examine the Law Commission's proposals around control. The proposals for what amounts to relativity of control-based title are unnecessary and unhelpful and run counter to the Law Commission's opposition to "possession" of such assets. As the City of London Law Society Financial Law Committee (CLLS-FLC) puts it, this is a "possessory wolf in control's clothing."[8]

Digital Assets and the Blockchain

The first question we need to ask – dealt with in the first subsection of this part – is how we characterise these assets from a technical perspective. What is a digital or crypto-asset, terms I will use pretty much interchangeably? The second section deals with different ways in which they can be held and transferred and critically how the blockchain prevents double-spending.

[8] Law Commission, *Digital Assets: Responses to Consultation* (HMSO, 2022) 519 (CLLS-FLC Response)

Digital Assets as Objects of Property Rights

Digital assets exist as strings of data. However, they are more than the information they contain. Information is not property,[9] so something more is needed. Digital assets, however, exist as part of a wider technological system and operate and perform functions within the confines of that system. In a UTXO system like bitcoin there is a readable sequence of data that represents the transactional output. That data only has meaning and usefulness within the system.[10] While the information might be copyable elsewhere, it would not be useful.[11] The Law Commission initially proposed in their consultation paper that a "data object" would be an example of a new third category of property if first, it is composed of data represented in an electronic medium; secondly, it exists independently of persons[12] and the legal system and thirdly, it is rivalrous.[13] An asset is rivalrous if A's use of it restricts B's use of it. The asset should also be both identifiable and definable.[14] In the final report, responding to criticism of the concentration on data in their initial proposals, they dropped the term data object but noted that their aim was twofold. First, it was to distinguish digital assets from tangibles and secondly to indicate that the instantiation of data was a core part of the asset.[15] They also dropped this requirement to instantiate data in the report, noting that it would provide a hard edge to the category that they wish to avoid. More importantly, however, it was never clear what the importance was that the asset was information-based and why the tertium quid should be so limited. The third category

[9] *Oxford v Moss* (1979) 68 Cr. App. R. 181; Law Commission *Digital Assets* (HMSO, 2022) Law Com. C.P. no. 256, ch. 2; D Sheehan, 'Information, Tracing Remedies and the Remedial Constructive Trust' [2005] R.L.R. 82, 93

[10] D Fox, 'Cryptocurrencies in the Common Law of Property' in *Crypto-Currencies in Public and Private Law* (Oxford: OUP, 2019) para 6.43

[11] Law Com. (n 9) paras 10.32-10.33

[12] J Penner, *The Idea of Property in Law* (Oxford: OUP, 1997) p 112

[13] Law Comm (n 9) para 5.10

[14] *NPB v Ainsworth* [1965] AC 1175, but for criticism of reliance on *Ainsworth* see J Lau, 'That New Chestnut – the Proprietary Character of Bitcoin' [2020] L.M.C.L.Q. 378

[15] Law Comm (n 1) paras 4.10-4.12

on this view could never be exhaustive and there would be no reason not to have a fourth or fifth category. In the final report therefore the Law Commission concentrate on the rivalrousness of the asset, but also the asset's qualities as being independent of persons and of the legal system. These criteria are met by digital assets, which the Commission view as a notional quantity unit, manifested by the operation of software and network generated data.[16]

The rules of the system architecture define what a bitcoin (say) is and one bitcoin can be distinguished from another, as can ether or NFTs. Separability from people is vital to a thing's being potentially an object of property rights. Information is not separable. I know my secret prune juice recipe and if I impart it to you (and allow you to make prune juice) you know it. But so do I. Information is not separable from persons,[17] but digital assets are. Crypto-assets are independent of the legal system. They would exist if the legal system said nothing about them. Debts would not. They exist because the legal system says A has a claim-right that B pay. There is no debtor against whom an obligation inherent in the crypto-asset can be enforced. There is no debt. This is how the Law Commission distinguish crypto-assets from choses in action. A debt could be denominated in bitcoin or ether,[18] but this is not the same thing as saying the bitcoin or ether is a debt. A crypto-asset is rivalrous. The system architecture guarantees that if I am making use of a bitcoin, you cannot. In the context of bitcoin this simply means transferring it, but more generally a crypto-asset is rivalrous because it manifests a power to perform a given operation on a given notional quantity unit within the context of the system's architecture and that if I am carrying out that operation it necessarily limits your ability to carry it out. We cannot both transfer a bitcoin at the same time to different people even if we both have access to the private key that makes such transfer possible.[19]

---

[16] Ibid para 4.13
[17] Penner (n 12) p 112
[18] W Wilson, 'Crypto-currency and the Claim in Debt' (2023) 38 J.I.B.F.L. 25
[19] Law Comm (n 1) para 4.45; *Tulip Trading Ltd v Bitcoin Association BSV* [2023] EWCA Civ 83, [2020] 4 W.L.R. 16

It is an important corollary of this line of argument that the Law Commission believe there is a thing. This is important. Property rights are precisely that; they are rights. Choses in possession are rights in relation to things that are possessable. Choses in action refer to all other transferable legal rights.[20] Generally, the latter do not relate to things. This does not preclude digital assets from being property. To control or possess a thing, transfer it and exclude others from it – and have a legal right to do so - there must be a thing and digital assets are things; they are definable, specific and ascertainable. Initially the Commission suggested the thing was the digital asset's data structure and defined the structure as a "data string" plus "a set of transactional functionalities" such that the data string operates within the system architecture.[21] However, a digital asset is purely notional and ideational. A bitcoin is not its digital representation or any sort of data structure. We need to distinguish these for a number of reasons. A purely practical reason is that the bitcoin's digital representation changes after every transaction. It is no longer represented by the same data string.[22] Each transaction involves a payment of the unspent output to the originator. Bitcoin therefore operates what is known as a UTXO-based ledger system.[23] Outputs are coins made and inputs are coins destroyed. The recorded UTXO itself cannot therefore be the subject of property rights; it is merely the end point of the bitcoin's transactional history and indicates the person able to technically transfer the bitcoin. The UTXO, or indeed for account-based systems like Ethereum the account balance, is just the end registry entry. Registry entries are not the subject matter of property. The notional or ideational entity, represented digitally and recorded as linked to a particular public address, is. The property right is the right to exclude others from that ideational thing

[20] R Stevens, 'Crypto is not Property' (2023) 139 L.Q.R. 615, 618-619
[21] Law Comm (n 9) para 10.25
[22] A Narayanan et al *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton: Princeton UP, 2016) p 243 (https://www.lopp.net/pdf/princeton_bitcoin_book.pdf)
[23] Law Comm (n 9) para 10.19

and the benefits it brings, and to operate the system to make use of those benefits for oneself.[24] In bitcoin this benefit is simply the ability to transfer, but with different assets might include access to platform resources and so on.

Cryptography and the Blockchain

The critical feature of digital assets like bitcoin, NFTs or ether is that they run on blockchains. These are what they sound like: chains of blocks. Each block is a group of transactions which have been validated by a computer – a node of the network – and then chained together mathematically by use of hash functions.

Decentralisation and the distributed nature of consensus are key. Decentralisation in this context simply means that everyone who uses the software has a copy of the ledger housed on the blockchain. In principle therefore all computers agree on which data is recorded on the ledger.[25] One method of validating a block, used by the Bitcoin blockchain, is proof of work.[26] In essence proof-of-work is how we persuade another node to accept the transaction as genuine. There are other ways of verifying transactions. Ethereum – like most blockchain systems - uses proof of stake[27] which is much less energy intensive and works by a node putting up a stake which is lost or reduced if the node confirms an invalid block. Conversely there is a reward, proportionate to the size of the stake, for confirming valid blocks.[28] Proof-of-work therefore

[24] This is very similar, but not identical, to the view in K Low and E Teo, 'Bitcoins and other Crypto-Currencies as Property' (2017) 9 Law, Innovation and Technology 235; Low and Teo see the right itself as the subject of property. See T Chan, 'The Nature of Property in Crypto-Assets' (2023) 43 L.S. forthcoming
[25] S Green, 'Crypto-Currencies: The Underlying Technologies' in *Crypto Currencies in Public and Private Law* (Oxford: OUP, 2019) ch. 1
[26] S Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) p 3
[27] J Burnie, M Millward and M Kimber, 'What's at Stake: The Legal Treatment of Staking' (2022) 37 J.I.B.F.L. 594
[28] A Antonopoulos & G Wood *Mastering Ethereum* (Sebastopol: O'Reilly, 2019) p 321

guarantees validity by making it computationally difficult to verify a block; proof-of-stake guarantees validity by creating economic incentives to avoid misbehaviour.

Imagine that Alice wishes to transfer a bitcoin to Bob to pay for some software. Alice must have a public key. Originally the actual public key was used as the coin address, but now it is usual to hash the public key to produce a coin address.[29] She must also have a private key which allows her cryptographically to transfer that bitcoin. Alice generates a message and cryptographically signs it. The bitcoin is transferred to Bob's coin address whereupon only Bob's private key allows a transfer. Private keys are generated mathematically at the same time as the public key and the two are uniquely mathematically linked. The upshot is that private keys must be kept safe, because once lost, the public key and therefore coin address is inaccessible. Unlike a password, a new private key cannot be generated, although it can be recovered via a seed which is often a dozen or so random words. The private key is not itself property.[30] Confidential information does not count as an object of property rights.

The transaction is broadcast to the network and added to the unconfirmed transaction pool. A node will then proffer its version of the unconfirmed transaction pool to be the next block, including the Alice-Bob transfer. To confirm a block as valid, a node must find a value, a nonce,[31] as it is called on the Bitcoin network, such that taking that value, the hash for the previous block, the hash for the proposed new block and hashing the combination produces a result within a particular target range.[32] A hash function is a cryptographic tool. Its input is a string. It produces a fixed size output, and it is efficiently computed in that an output can be worked out quickly.[33] Other features are needed. First, it must be hard to find collisions where

[29] M Bartlam 'Legal and Regulatory Issues for Custodians and Administrators of Digital Assets' (2019) 33 J.I.B.F.L. 35, 36
[30] UKJT, *Legal Statement on Cryptoassets and Smart Contracts* (2018) para 85
[31] Nonce has a different meaning on Ethereum; see Antonopoulos and Wood (n 28) pp 100-102
[32] Narayanan (n 22) p 64
[33] Ibid pp 23-24

different inputs produce the same output.[34] It cannot be impossible for these to exist. The inputs can be any length and the output must be a fixed length which means there are more possible inputs than outputs. Collisions exist, but if it is in practice impossible to find them it does not matter. The second feature is that it should be unfeasible to unpick an output to work out the input.[35] Since the node cannot pick a hash in the target range and work backwards, it hashes randomly chosen nonces until by trial and error it finds one that works. Thirdly, the hash must be puzzle-friendly.[36] This implies that if someone wants to target a particular value of output and part of the input is suitably randomised it is very difficult to find another input that works. Lastly, it must be trivial to evaluate if a node has found an appropriate nonce. The nonce is published as part of the block so any other node can crunch it and see if it is right.[37] The incentive to do this is that the node validating a block gets a reward. On the Bitcoin protocol we call this mining. Every 210,000 blocks, however, the reward halves. This function limits the number of bitcoins to 21 million.[38] A second reward that can continue indefinitely even once the last bitcoin is mined is a transaction fee. The creator of the transaction sets the input to be greater than the output and the validator picks up the difference.[39]

For a crypto-currency to operate, it is crucial to prevent double-spending. Double-spending is basically impossible with notes and coins. I give you a £10 note; you have it. I cannot give it to someone else. In the crypto-context a double-spending attack occurs when Alice proceeds to generate a message to transfer the same bitcoin (transferred to Bob) to Charles. Even once Bob has accepted payment, and a block is created including that transaction, if Alice controls the creation of the next block she could spend the same bitcoin, transferring to Charles. Both

[34] Ibid pp 24-26
[35] Ibid pp 27-29
[36] Ibid p 29
[37] Ibid p 68
[38] Ibid pp 62-63
[39] Ibid pp 63-64

blocks are on the face of it valid and the next node to validate a block will not know which block to hash to.[40] The convention is that nodes will add to the longest chain, but here the chains are the same length. Commonly the node will add to the block it hears about first, but network latency and the time to disseminate new copies of the ledger means that some nodes might hear of the Alice-to-Charles block first. Bob therefore waits until the transaction is included in a sufficient number of successive blocks. Typically, we say six. Once Bob can see six consecutive blocks (which can take up to an hour) on the chain that confirm his receipt, he can safely allow Alice her software download.[41]

Could an attack on the blockchain tamper with data further down the chain, so as to recover the bitcoin from Bob *ex post*? The blockchain is essentially tamper-proof and technically immutable. Each block has a hash pointer to the previous block.[42] A hash pointer is a data structure pointing to where the information is stored along with a hash of that data. It is almost impossible to change the data such that the consequent hash function remains the same. An attacker under a proof-of-work system would have to alter the blocks and the hash pointers. That requires significant computer power – 51% of the power on the network - but is not impossible. Ethereum Classic for example has been subject to several successful attacks.[43]

---

[40] Ibid pp 58-60
[41] Ibid p 61
[42] Ibid p 32
[43] M Bridge et al (eds), *The Law of Personal Property* 3rd edn (London: Sweet and Maxwell, 2021) para 8.046; HJ Allen, '$-€-Bitcoin' (2017) 25 Maryland L Rev 877, 930; see also https://www.coindesk.com/markets/2020/08/29/ethereum-classic-hit-by-third-51-attack-in-a-month/ (visited 12 June 2023); there are variations on the 51% attack in proof-of-stake as well.

Possession of Digital Assets

The Law Commission's proposals are that the common law should develop a jurisprudence concerning a concept of control applicable to crypto-assets[44] and they explicitly state that they do not want to propose such assets be possessable. The first section sets out some of the reasons given as to why we might hold digital assets to be possessable. The second section refutes those arguments. We should not hold such assets possessable.

Arguments for Possession of Digital Assets

A judgment that digital assets are possessable, as proposed by Lai,[45] carries with it an implicit judgment that lots of other things follow – that we can bail a digital asset, or that it can be pledged, delivered, subjected to a contractual lien or converted. Lai notes a number of points of similarity between digital assets and tangible assets which leads him to conclude the former should be possessable. A thing can be possessed if a party factually possesses and intends to do so.[46] Accepting that the weight of authority is against him,[47] he argues that the true distinction is not between tangible and intangible, with the latter incapable of possession, but non-legal and legal, again with the latter incapable of possession. On this view choses in action being dependent on legal acceptance, are non-possessory, but digital assets which exist independently of the legal system can be possessed. *OBG v Allan*[48] should be confined to the latter. Lai then observes that the factual control provided by the owner's having the private key

[44] Law Comm (n 1) para 5.5
[45] J Lai, 'Possession of Crypto-Assets' [2023] J.B.L. 41
[46] Ibid 48
[47] *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281, [2015] Q.B. 41; *OBG v Allan* [2007] UKHL 21, [2008] 1 A.C. 1
[48] [2007] UKHL 21, [2008] 1 A.C. 1

that enables transactions to be done (and conversely nobody else having it) is in essence the same as the factual control provided by physical control of a table or a car or a banana.[49]

Lai observes that it is possible to intend to possess a crypto-asset. While such assets are frequently dealt with through automated processes and some suggest this causes problems for the identification of any party intention,[50] Lai makes the point that this also true of vending machines and nobody denies that the company owning the machine intends to transfer title to whoever puts in a coin.[51] Given therefore that it is possible to control digital assets in functionally the same way as we do physical ones and to intend to do so, he argues we should hold such assets to be possessable.

Arguments against Possession of Digital Assets

There are many differences between physical and digital assets. The former occupy space and move through space whereas digital assets exist at one address and then instantaneously at another.[52] I can interact directly with a physical asset but require the medium of computer code – private keys or smart contracts - to interact with a digital asset. The question is whether these differences are immaterial or whether, as Liu argues, they lead to inappropriate and unhelpful analogies which lead to wrongly decided cases.[53] Liu is right. Ownership of goods is no more than the best right to possess.[54] The same cannot – and should not – be said of digital assets.

[49] Lai (n 45) 51-52
[50] Law Comm (n 9) paras 11.66-11.67
[51] Lai (n 45) 56-57
[52] H Liu, 'Title, Control and Possession in the Digital World' [2021] L.M.C.L.Q. 597, 612
[53] Ibid 612-614
[54] D Sheehan, *The Principles of Personal Property Law* 2nd edn (Oxford: Hart, 2017) pp 14-15; see also WJ Swadling, 'Rescission, Property and the Common Law' (2005) 121 L.Q.R. 123

Law Commission's Objections

The Law Commission note four difficulties with possession of crypto-assets in the consultation paper. First, market practice does not depend on possession.[55] Secondly, they point to the complexity of possession,[56] although in the final report they suggest that a comparable degree of complexity with respect to control might be inevitable.[57] This complexity manifests itself for example in different sorts of possession, including actual possession, constructive and legal possession.[58] A person in legal possession may be in actual possession, but he need not be. A party may be in physical possession of a thing without the intention to control it, which will count as custody, but not possession. In *Burnett v Randwick City Council*[59] directors of an insolvent company claimed the right to sue in conversion for interference with the company's assets. Tobias JA held they were custodians in charge of the equipment by mere licence and unable to sue. The company was in possession.[60] Constructive possession, which overlaps with legal possession, refers to the party's right to have actual possession delivered to him immediately. The right to take immediate possession is also an indication of continued legal possession of the asset.[61] The Commission also point to the slipperiness of the term possession. Sometimes it is used to indicate the factual situation and sometimes the legal rights associated with that state of affairs.[62] This explains Crawford's insistence that possession is simply a fact. It creates, but does not define, the jural relation of property.[63] The corollary of this is that the

[55] Law Comm (n 9) para 11.58
[56] Ibid para 11.64
[57] Law Comm (n 1) para 5.17
[58] Law Comm (n 9) para 11.19
[59] *Burnett v Randwick City Council* [2006] NSWCA 196.
[60] Ibid at [96-97]; TY Lin, *Personal Property Law* (Singapore: Academy Publishing, 2014) pp 131-135
[61] *Towers & Co. Ltd v Gray* [1961] 2 Q.B. 351 at 361-362 (Lord Parker CJ).
[62] Law Comm (n 9) para 11.22
[63] MR Crawford, *An Expressive Theory of Possession* (Oxford: Hart, 2021) pp 48-51; see also S Douglas, 'Is Possession Factual or Legal?' in *The Consequences of Possession* (Edinburgh: EUP, 2014) p 56

Commission is very keen in the final report to distinguish between factual control and the legal consequences of that factual control.[64]

Thirdly, the Commission point to a couple of core elements of possession that are inapplicable or difficult to apply. The first is that factual possession is a very visible sign to the world, but the factual relation between a bitcoin and a person might be relatively less visible.[65] It is not obvious that this is right. A distributed ledger is exactly what it says – a ledger. It is therefore similar to a register, albeit one with no legal or statutory backing. If a digital asset is linked to a given public address that is publicly available information, even though the identity of the party with the corresponding private key may remain opaque. The second core element that the Commission thought inapposite is intention.[66] In respect of the intention to control two things are important. The possessor must know of the existence of the object and must intend to exclude everyone else from possession.[67] The Law Commission, however, argue that the complexity of finding intention militates against its relevance in the digital asset context where so many processes are automated. Although they accept the relevance of intention in the final report, this caution remains. They warn us that, "To search for an element of human intentionality risks introducing an unreal human element to what can often be automatic or deterministic processes."[68]

In *B2C2 v Quoine Pty Ltd,*[69] however, orders were placed for cryptocurrency at a rate of 10 BTC to 1 ETH; the buyers of the ether made a mistake that the price did not deviate markedly from the market price when in fact it was wildly out of line. Both the offer and its acceptance were done automatically in the middle of the night and only cancelled in the morning. If it is

[64] Law Comm (n 1) para 5.6
[65] Law Comm (n 9) para 11.65
[66] Ibid para 11.66
[67] Sheehan (n 54) pp 12-13; L Rostill, *Possession, Relative Title and Ownership in English Law* (Oxford: OUP, 2021) pp 19-21
[68] Law Comm (n 1) para 5.57
[69] [2020] SGHC (I) 02, [2020] 2 S.L.R. 20

too complex to identify an intention, it is presumably too complex to identify a mistaken intention. This though did not deter the Singapore Court of Appeal, which accepted that there was a mistake, not as a mistake as to the terms of the contract as the relevant algorithms functioned exactly as intended,[70] but as to how the platform would operate and the circumstances in which the contract would be formed. The test as to whether the contract was invalid was whether, in programming this default price, the programmer knew, or ought to have known, they would only be accepted by a seller acting under a mistake and sought to profit from that.[71] Mistakes, intentions and other mental phenomena can be identified – even in the crypto-asset context.

Fourthly, the Law Commission suggest that the automatic import of a wide range of legal principles along with possession would cause problems;[72] the idiosyncrasies of crypto-assets are better dealt with by an analogous idea of control. The Commission argue that conversion for example cannot be simply drawn across to the digital asset space. This is correct, although the Commission, as we see later, do not follow through by rejecting the analogy with conversion completely.

Inapplicability of the Policies for Relativity of Title in Tangibles

Although some of the reasons they provided in the consultation paper for dismissing possession do not in the end stack up, such as the difficulties with intention, the Law Commission are right to reject possession. This is plain if we go back to the fundamental policy behind accepting

[70] Ibid at [115]
[71] Ibid at [124]; See for criticism K Low and E Mik, 'Lost in Transmission: Unilateral Mistakes in Automated Contracts' (2020) 136 L.Q.R. 563
[72] Law Comm (n 9) para 11.68

relativity of title to tangibles. English law has no system of registration of title of chattels. As others have pointed out, it would not be worth the candle.[73] One consequence of this is the informality of delivery as a mode of passing title. Delivery requires an intention to pass title[74] and the transfer of possession, which can be by acts and transactions which are hard to interpret and the analysis of which are extremely fact-sensitive. *Re Cole*[75] illustrates this nicely. A man showed his wife around a new house and stated, "It's all yours." This was too equivocal to allow her to claim title against the husband's trustee in bankruptcy and yet in a different context the phrase "the money is as much yours as mine" was deemed to create a trust.[76] A doctrine of relativity of title tackles this inevitable uncertainty and need for fact-sensitive judgment calls by providing a default; a person claiming a right to possess can prove it via his prior possession. This facilitates dispute resolution, but it also tracks a need for a public system of title.[77] The point of possession for Crawford is therefore not so much control *per se*, but that control signals an intention to claim a stake in the asset,[78] which must be accepted by other people.[79] Accepting that a digital ledger is simply a ledger, there is a public record of apparent, albeit pseudonymous, title to digital assets – on the ledger – and possession need not fulfil this signalling function in the digital arena.

In the context of (unregistered) land, which Rostill argues has a doctrine of relativity of title for much the same reasons as chattels,[80] there is a statutory extinguishment rule relating to

---

[73] Rostill (n 67) p 151
[74] *Re Ridgeway* (1885) 15 Q.B.D. 447; *Day v RCM* [2013] EWCA Civ 191
[75] [1964] Ch. 175
[76] *Paul v Constance* [1977] 1 W.L.R. 54
[77] L Austin, 'Possession and the Distractions of Philosophy' in *Philosophical Foundations of Property Law* (Oxford: OUP, 2013) p 182, pp 188-190; C. Rose, 'Possession as the Origin of Property' (1985) 52 U. Chi. L. Rev 73
[78] Crawford (n 63) p 63; see also Y Emerich, 'Why Protect Possession' in *The Consequences of Possession* (Edinburgh: EUP, 2014) p 30
[79] Crawford (n 63) p 79
[80] Rostill (n 67) pp 145-149; *White v Amirtharaja* [2022] EWCA Civ 11, at [56-57] (Nugee LJ); see also C Bevan, 'Adverse Possession, Relativity of Title and a Salutary Lesson for Litigants: *White v Amirtharaja* in the Court of Appeal' [2023] Conv. 92; MJ Goodman 'Adverse Possession of Land – Morality and Motive' (1970) 33 M.L.R. 284; Law Commission *Land Registration for the Twenty First Century: A Consultative Document* (HMSO, 1998) Law Com. C.P. no. 254 paras 10.4-10.10

adverse possession, which regularises the position when possession is out of kilter with "paper title". He observes the same is true of chattels.[81] The limitation period for conversion runs out after six years after which the finder obtains (best) legal title.[82] This reinforces the point that possession serves as a proxy. If you do not defend your possession, you lose it. The logic of this is inapposite to crypto-assets, where the person controlling the address to which the asset is linked can be treated as presumptively the owner. As a publicity and dispute resolution mechanism possession and control are unnecessary, because the function of indicating the (probable) owner is already taken by the blockchain record. There is no need for this type of limitation/adverse possession rule. It is impossible to "squat" on a bitcoin or to "find" it lying around in an airport lounge, as in *British Airways Board v Parker*.[83] It is impossible to "possess" or have "positive" factual control without the asset being linked in some way to your public address to which you have control via a private key. Consequently, a claim that you have it, but I ought to have it is not a claim to protect possession but to order a reconveyance.[84] There is no need in crypto-asset cases for a "mechanism by which the common law deputises someone to stand in for the owner until the owner is found."[85]

Another historically popular argument for relativity of title is that conferring rights to exclude on possessors discourages violence and prevents civil unrest.[86] This does not explain anything other than a right to exclude,[87] but for our purposes is also peculiarly inapposite to digital assets. Violence does not dispossess me of my bitcoin. If I store my private key in a paper QR code, I might be violently dispossessed of that, but my possession of the private key is protected because the paper wallet is tangible, not because it has anything much to do with

---

[81] Rostill (n 67) p 152
[82] Limitation Act 1980, s. 3(2); Sheehan (n 54) 253-254
[83] [1982] Q.B. 1004
[84] K Low, 'Confronting Cryptomania: Can Equity Tame the Blockchain' (2020) 14 Journal of Equity 240
[85] L Katz, 'The Relativity of Title and Causa Possessionis' in *The Philosophical Foundations of Property Law* (Oxford: OUP, 2013) p 202, p 205
[86] Rostill (n 67) pp 128-129
[87] Ibid p 144

my bitcoin *per se.* We need not therefore worry about "the state's monopoly on the use of force..." either.[88]

Control of Digital Assets

With possession gone, what is left? For the Law Commission this is control. The person in control is the person who can

- Exclude others from the object
- Put the object to the uses of which it is capable
- Identify themselves as having these abilities.[89]

The Commission do not recommend a statutory definition of control[90] and give three reasons for this. The first is that control will be fact and technology specific and might amount to different things in different contexts, such as multi-sig arrangements (where several parties need to agree and use their digital signatures and private keys to release assets), mining or smart contracts.[91] Secondly, they do not propose that control is part of the definition of the asset (unlike under article 12 UCC) but that the key concept is rivalrousness. While rivalrousness and control are related all it means for something to be rivalrous is that if I am using the thing you cannot also be making use of it. It is binary in character,[92] unlike control. As such it focuses attention on the quality of the asset itself rather than what is being done with it. Thirdly, the analogous idea of possession has never been reduced to statutory form.[93] Control, like

[88] Ibid p 210
[89] Law Comm (n 1) para 5.10
[90] Ibid para 5.12
[91] Ibid paras 5.13-5.15
[92] Ibid para 4.34; *Tulip Trading v Bitcoin Association of BSV* [2023] EWCA Civ 83, [2023] 4 W.L.R. 16, at [24] (Birss LJ)
[93] Law Comm (n 1) paras 5.16-5.17

possession, is basically treated as a factual matter by the Commission, a factual relationship that a person can have with a thing. Although intention is not present in the description of control with which we started, the Commission suggest that intention will help resolve issues where legal consequences flow from control. Crypto-tokens can for instance be airdropped into public addresses. A person may have factual control over the address and airdropped tokens but have no intention to accept the tokens, knowledge of them or desire to obtain them[94] and should not be treated as having title. This is no more than an application of the general rule that assets cannot be forced on us. I need to accept payment of money or it is merely tender, and I need to accept gifts made to me.[95]

The Commission argue that a change in control should always be necessary to pass title. This change of control could be on- or off-chain and would involve intention as a necessary part of the analysis.[96] Unlike with tangible assets, it seems impossible to just "intend" someone the legal owner. Digital assets are not goods under the Sale of Goods Act 1979 and title does not pass when intended to do so under section 17 Sale of Goods Act 1979. In policy terms this position seems right and we will see some of its consequences later.[97] It is undesirable to decouple title from technical ability to transfer on the blockchain more than absolutely essential. This minimises the potential for double-spending which may arise where for instance party A transfers a bitcoin to B by deed, but then transfers the same bitcoin on-chain to C.

There are cases where ownership of a digital asset is separated from control over it. One example might be a void transfer of a digital asset, maybe due to mistake or incapacity.[98] To analyse such cases the Law Commission posit a type of control-based relativity of title, implicit

[94] Ibid para 5.60
[95] J Hill 'The Role of the Donee's Consent in the Law of Gifts' (2001) 117 L.Q.R. 127; Sheehan (n 53) p 53
[96] Ibid para 5.54
[97] H Liu, 'Transferring Legal Title to a Digital Asset' (2023) 38 J.I.B.F.L. 317
[98] Law Comm (n 1) paras 5.45-5.46

in the consultation paper, and explicit in the final report.[99] Relativity of title is also possible under analyses that see the factual transactional ability as the subject of property. The mistaken payee has such a factual transactional ability, which proponents of this view (like Chan, who in fairness does not discuss this question)[100] may wish to protect. This section identifies in turn three major problems with the Commission's analysis which should lead to its rejection. First, the Commission are reinventing the wheel. If at the end of the day, they propose a system of control-based relative title very similar to the possession-based relative title of tangibles they would be better off simply accepting that digital assets should all be possessable, not just electronic trade documents,[101] although such a recommendation would on the view advanced here be mistaken as the policy drivers for possessory title do not apply to the digital context. Secondly, it is unnecessary and unsupported by authority. Equity can and does deal with the different problems that arise much better than the common law will. Thirdly, it is unhelpful. Digital assets share some features with tangibles in that they are rivalrous and exist independently of the legal system. They also share features in common with choses in action. They are intangible. As such we have the opportunity to stand back and decide as a policy matter how we should deal with them, but the Commission's proposals for control also lead to "quasi-pledges" and in one area a type of "quasi-conversion" without addressing the policy questions that arise alongside that – for example whether a collateral taker should be subject to a duty of care to the collateral provider to look after the crypto-collateral in question.

[99] Ibid paras 5.81-82

[100] Chan (n 24); see also J Sarra and L Gullifer, 'Crypto-Claimants and Bitcoin Bankruptcy: Challenges for Recognition and Realisation' (2019) 28 International Insolvency Review 233, 243; D Fox, 'Digital Assets as Transactional Power' (2022) 37 J.I.B.F.L. 3

[101] Law Commission, *Electronic Trade Documents* (HMSO, 2022) Law Com. no. 405; see now Electronic Trade Documents Act 2023, ss. 2-3

Superior and inferior legal titles to chattels are, as we have seen, an aspect of possession. Legal title to a tangible asset is the same thing as entitlement to possess. Even a thief, or a transferee from a thief, has title, albeit of limited value.[102] Indeed ownership means no more than the best right to possess.[103] It is this entitlement to possess that counts as the interest at stake. The interest is absolute, but the titles are relative.[104] That the Commission are suggesting such a control-based analogue to possessory title is explicit in the final report, but was also clear from their consultation paper argument that the transferee in a mistaken transfer context would "obtain a control-based interest in the crypto-token good against the world except for the transferor…the transferor would retain the (superior) legal title… even though it did not retain control over the crypto-token."[105] The transferee's factual control is then protectable; this is presumably by way of the discrete tort to be developed by analogy with conversion. He has actual control, but the transferor's superior title presumably amounts to a right to demand reconveyance or to demand immediate control – ie it is the same as the superior title party's right to demand immediate possession. It seems not inappropriate to call this constructive control of the asset. Further superior legal title is presumably protectable against third parties. The Law Commission said in their consultation paper that they did not wish to introduce such "grades" of control,[106] but the effect is that they have done so.

---

[102] [2001] 1 W.L.R. 1437, at 1450 and subject to Torts (Interference with Goods) Act 1977 s. 8(1); *Webb v Chief Constable of Merseyside Police* [2000] Q.B. 427; *Gough v Chief Constable of West Midlands Police* [2004] EWCA Civ 206; G Battersby, 'Acquiring Title by Theft' (2002) 65 M.L.R. 603; Rostill (n 67) pp 106-107
[103] Sheehan (n 54) p 15
[104] E McKendrick (ed), *Goode and McKendrick on Commercial Law* 6th edn (London: Penguin, 2020) para 2.21
[105] Law Comm (n 9) para 13.35; see also M Kimber and D Stoean, 'Bind to Law: Soul-Bound Tokens and Property Law' (2022) 37 J.I.B.F.L. 7
[106] Law Comm (n 9) para 11.58

Not only is relativity of control-title nothing more than relativity of possessory title, but control is very similar to possession and this is essentially, as we saw, Lai's argument in favour of possession of digital assets. First, factual possession is often described in terms of the ability to control the asset. The degree of factual control required depends on the nature of the asset. The degree of control required for smaller items will be greater than for larger ones and the larger the thing under consideration the clearer the need to talk of control as opposed to possession in its more colloquial sense. In *The Tubantia*[107] for example the claimants had already done work at great cost and extracted a small amount of cargo from the vessel when the defendants also attempted to salvage the wreck. The claimants were said to be in possession even though their divers and equipment were not permanently on site, but only when weather and tides permitted. There was sufficient physical control for the claimants to be in possession. Secondly, both factual possession and intention to control are important. With regard to tangible assets, the alleged possessor must know of the existence of the object and must intend to exclude everyone else from possession.[108] In *Lockyer v Gibb*[109] for example it was held that I may be mistaken as to what the asset is and not therefore know that I have it. In that case I am not in possession if my mistake is as to the identity of the asset, but I am in possession if it is a mistake purely about attributes. This also applies to control. I am, as we have seen, not in control of the thing, and have presumably no title to it, if I do not know it has been airdropped into my public address.

We can illustrate these difficulties further by noting how difficult it is to get a piece of rice paper between control in digital assets and possession of electronic trade documents. The Law Commission have a discussion of the elements of possession in the *Electronic Trade Documents* report in which they discuss the need for factual control coupled with an intention

[107] [1924] P. 78
[108] Sheehan (n 54) pp 12-13; Rostill (n 67) pp 19-21
[109] [1967] 2 Q.B. 243

to possess the thing.[110] One of their requirements for a document to be a possessable electronic trade document therefore is that it be amenable to exclusive control. This is a question of fact, and the Commission specifically refused to be drawn on whether it needs to be positive or negative control or both.[111] Nor is this defined in section 2(2) Electronic Trade Documents Act 2023, but it is notable that in outlining their concept of factual control of digital assets both negative control (excluding others) and positive control (ability to use) are referenced. The Law Commission suggest a useful rule of thumb with regard to electronic trade documents that if a party has sufficient control that, were it tangible it would be reduced to possession, they have control.[112] Rivalrous digital assets – other than electronic trade documents – like bitcoin are equally amenable to such exclusive control. That being the case, there will likely be pressure to make the former possessable by analogy with the statutorily possessable trade documents.

Relativity of Title is Unnecessary

The Law Commission suggest that disputes are likely to arise as to the consequences of a person's having control and provide examples of when difficult problems will arise – where the person in control is not the person recorded on the blockchain as the owner/controller, where he is not the person with "superior legal title" or where he exercises some level of joint control.[113] They argue first that these disputes will require some view of relativity of title to solve and secondly that in the context of "third category" things, ie those objects of property not choses in possession or choses in action there is already authority in favour of relative title.

[110] Law Comm (n 101) paras 5.34-5.49
[111] Ibid para 6.82
[112] Ibid para 11.86
[113] Law Comm (n 1) para 5.76; *Tulip Trading Ltd v Bitcoin Association* [2022] EWHC 667 (Ch), at [3] (Falk J)

The examples that the Law Commission give do not support their conclusion, however. The Commission say in the final report, "There seems little sense in a legal system which does not permit a holding intermediary who holds digital assets on behalf of a large number of users to pursue a hacker…"[114] This must be right but says nothing about a need for relativity of title as a trustee intermediary would have such a right. There are two points to make. First, the conclusion that the intermediary has a lesser common law title[115] to the assets contradicts the assumption, recognised in law in the USA by *Archer v Coinbase,*[116] that legal title passes with the private key. This is also implicit in the Law Commission's proposals that an off-chain change of control can transfer a digital asset and is often pithily expressed as, "Not your keys, not your coins." The only discriminating factor then on the Law Commission's view between Coinbase receiving full and lesser legal title is intention, despite their caution about fictional intentions. In *Archer* the plaintiff sued Coinbase in conversion for failing to allow him access to "his" Bitcoin Gold after a fork created the new currency. The California Court of Appeals rejected the claim. Coinbase had no duty, contractual or otherwise, to provide access to or support the new currency, which implies they were not Archer's coins. The point is that Coinbase held the private keys (not Archer) and owned the coins – this should be so despite Coinbase's August 2023 terms and conditions stating the title remains with the user (clause 5.19A). Secondly, there may be a trust.[117] The trust option is perfectly workable and is not one the Law Commission reject. There are real problems both conceptual and practical, however, if one tries to combine trusts and lesser legal title as two options in a flexible "toolkit"[118].

[114] Law Comm (n 1) para 5.90
[115] Ibid para 7.101
[116] 53 Cal App (5th) 266 (2020)
[117] Ibid para 7.95 *B2C2 v Quoine Pty Ltd* [2020] SGHC (I) 02, [2020] 2 S.L.R. 20; *Ruscoe v Cryptopia Ltd* [2020] NZHC 758
[118] See on the advantage of a "toolkit" Law Comm (n 1) para 5.34

English law does not allow parties to have anything they want. It is perfectly open to the courts to say that title to digital assets can be "split" but it must be done by equitable means.

Turning now to the Commission's claim that there is (albeit contested) authority in their favour, in *Armstrong v Winnington Networks Ltd*[119] fraudsters hacked into the database recording entitlements to carbon credits, reallocated Armstrong's credits to themselves and selling them onto Winnington. The allowances were intangible property[120] and have been described as neither chose in possession not choses in action,[121] although comments to that effect in *Armstrong* are half-hearted. The allowances are Hohfeldian liberties, permitting the emission of a given amount of carbon dioxide. Morris QC decided that the fraudster acquired the allowances subject to a constructive trust,[122] with the fraudsters holding "de facto legal title" on trust for the victim.[123] Winnington was liable to Armstrong in knowing receipt, since they had made inquiries as to the fraudsters' authority to sell the allowances,[124] but decided to go ahead without waiting for the answers and despite their suspicions about the vendor's title.

Far from giving succour to the Law Commission,[125] the decision demonstrates the need to closely analyse the type of asset in play. There is Australian authority that a thief holds the stolen chattel on constructive trust for the victim;[126] more accurately he holds his possessory title on trust.[127] This is referred to by Lord Goff in *Westdeutsche Landesbank Girozentrale v Islington LBC*[128] in respect to a stolen bag of coins. This does not work with carbon credits. If

[119] [2012] EWHC 10, [2012] 3 W.L.R. 835; D Sheehan, 'Bona Fide Purchase, Knowing Receipt and Proprietary Claims to Land and Carbon Credits' (2013) 24 K.L.J. 424; K Low and J Lin, 'Carbon Credits as EU Like It: Property, Immunity, TragiCO2medy' (2015) 27 J. Environmental Law 377
[120] [2012] EWHC 10, [2012] 3 W.L.R. 835, at [52]
[121] Ibid at [32]; *Shulev v Global Trading Ltd* [2022] EWHC 1685, at [113] (Butcher J)
[122] [2012] EWHC 10, [2012] 3 WLR 835, at [127]
[123] Ibid at [276]
[124] Ibid at [265-266]
[125] As they claim; Law Comm (n 1) para 5.83; see also *LMN v Bitflyer Holdings* [2022] EWHC (Comm) 2954
[126] *Black v S Freedman & Co* (1910) 12 C.L.R. 105
[127] J Tarrant, 'In Defence of the Theft Principle' (2009) 3 Journal of Equity 175; such a trust is likely superfluous. See R Chambers, 'Trust and Theft' in *Exploring Private Law* (Cambridge: CUP, 2010) p 225
[128] [1996] A.C. 669

the asset were a debt, the debtor either discharges the debt or he does not.[129] If the debt is discharged the payee had "title" prior to its discharge. If not, he did not. Likewise in *Armstrong* either the fraudsters (and so Winnington) had permission to emit the carbon or Armstrong did. Since Morris QC concluded that legal title remained in Armstrong, Armstrong had permission to emit the carbon.[130] In other words, the registry entry is not conclusive. There is no room for "de facto" title. In *Jones v Persons Unknown*[131] Jones was duped into purchasing approximately 90 bitcoin, which the fraudsters dissipated. By chance Jones located the bitcoin at an address controlled by Huobi and claimed them back. Huobi was said to be a constructive trustee of the bitcoin as it had control of the wallet to which the bitcoin had been paid,[132] but there is no detail as to why this was appropriate. We might see *Jones* as following *Armstrong* and involving Huobi holding "de facto" legal title on trust, but the proper analysis is instead that Jones was duped and therefore the fraudsters' title was voidable for fraud. The only question is whether Jones was barred as against Huobi from rescinding.

The discussion also illustrates how recognition of a third type of asset other than choses in possession or choses in action can drive an assumption that they must be treated the same. They are not the same. A carbon credit is different from a digital asset, which in turn is different from a patent, which is not a chose in action by statute.[133] Whether we call them choses in action or "third category" things there is no escape from analysing the characteristics of the

[129] Something made more complex by the rules on assignment and priority between competing assignments of choses under the rule in *Dearle v Hall*, but this does not seem to affect the point as for carbon credits. D Fox, 'Relativity of Title at Law and in Equity' [2006] C.L.J. 330
[130] [2012] EWHC 10, [2012] 3 W.L.R. 835, [287]; Low & Lin (n 119) 390-391
[131] [2022] EWHC 2543
[132] Ibid [21]; K Low and T Chan, 'Post-Scam Crypto Recovery: Final Clarity or Deceptive Simplicity' (2023) 139 L.Q.R. 379
[133] Patents Act 1974, s. 30(1)

asset to hand. The "third category" distinction obscures rather than illuminates[134] and notably many decisions accepting that digital assets are objects of property do not decide the matter.[135]

Relativity of Title is Unhelpful

The primary reason the introduction of relativity of title is unhelpful is that it pushes us to inappropriate and unworkable policy conclusions. This section lays out three: the implications for custodial arrangements via a crypto-exchange, conversion and possessory security rights.

Operation of Custodial Arrangements by Intermediaries

There are different approaches to holding crypto-assets. Crypto-assets may be held directly. Colloquially we talk of bitcoin being stored in wallets, although strictly this is untrue. A wallet is software for storing the private keys used to access the coin address associated with the crypto-currency.[136] Indeed it does not even have to be software; the least sophisticated type of wallet is, as we have seen, a paper wallet where the private key is encoded as a QR code.

Crypto-assets can also, and more commonly, be held indirectly via an intermediary. This is our focus in this section. To deposit, withdraw or exchange crypto-currency will require an account. By opening the account and sending a bitcoin to a public address associated with that account you give up control to the exchange. There is a payoff, however. Opening a wallet

[134] K Low, 'Crypto-assets and the Renaissance of the Tertium Quid' in *Research Handbook on Property Law and Theory* (Cheltenham: Edward Elgar, 2023) forthcoming. L van Setten, 'Cryptographic Tokens: Three Categories of Personal Property' (2023) 38 J.I.B.F.L. 102; UKJT (n 30) para 86(a)
[135] *Ruscoe v Cryptopia* [2020] NZHC 729, at [102-121]; *B2C2 v Quoine Pte Ltd* [2020] SGCA (I) 02, [2020] 2 S.L.R. 20, at [139-144]
[136] Antonopoulos and Wood (n 28) 79-80

with a crypto-custodian outsources the private key risk and the customer can still access the account even if his password is lost.[137] Custodians either maintain an omnibus blockchain address to which all the cryptocurrency they hold on behalf of clients is sent or separate addresses. Gemini for example characterise their custody arrangements as a bailment and maintain separate addresses.[138] The commonest position though is for the custodian to operate a single pooled address, with segregated addresses as a premium service. Having segregated accounts as standard would be too cumbersome with many more transactions, those between clients, requiring to be confirmed on the blockchain rather than by an internal ledger entry.[139] With an omnibus account the custodian does not generally commit to retain specific UTXO, but to maintain the appropriate value of coins.[140] The repayment claim may be contractual,[141] or the custodian may – as *Ruscoe v Cryptopia*[142] makes plain - hold on trust for the clients if the three certainties are met and the intermediary cannot trade with the assets in its own right. This was not the case in *Re Gatecoin*[143] and the claimants were there relegated to personal claims in insolvency against the exchange.

Accepting a type of bailment, the client would have superior legal title and the custodian a lesser title according to the Law Commission.[144] The assets would be pooled and therefore the clients would hold under a legal tenancy in common. Tenancies in common, unlike joint tenancies, require only the unity of possession; no co-owner can therefore exclude another from

---

[137] M Haentjens, T de Graaf & I Kokorin, 'The Failed Hopes of Disintermediation: Crypto-Custodian Insolvency' [2020] S.J.L.S. 526, 533-534

[138] Ibid 537; A Held, 'Intermediated Cryptos: What your Exchange-hosted Wallet really holds' (2020) 35 J.I.B.F.L. 540, 543

[139] K Low, 'Trusts of Crypto-Assets' (2020) 34 T.L.I. 191; K Low, 'Quoines in Cryptopia: when (if ever) are Crypto-Asset Exchanges Trustees?' [2020] Conv. 70; see also *Re Gatecoin* [2022] HKCFI 914

[140] Haentjens et al (n 137) 558

[141] Ibid 561

[142] [2020] NZHC 728; see generally N Yeo, 'Crypto-Exchanges: The Basics' (2023) 38 J.I.B.F.L. 459

[143] *Re Gatecoin Ltd* [2022] HKCFI 914, at [43, 60-65]; J Liu, 'An Analysis of the Gatecoin Case in Hong Kong: Trusts and Crypto-Assets' (2023) 34 I.C.C.L.R. 544; *Wang v Darby* [2021] EWHC 3054; J Lam, 'Establishing Proprietary Claims over Crypto-assets' (2022) 36 T.L.I. 94

[144] Law Comm (n 1) para 7.103

possession.[145] In terms of tangible assets, the type of commingling to which we refer can take the form of either confusion or commixtion.[146] The former refers to the mixture of granular things (sugar, barley) and the latter the mixture of liquids (oil). In both cases the goods are said to be fungible; it physically does not matter if a party has one unit rather than another unit of the asset. Likewise, it does not matter if a party withdraws one ether rather than another. They are indistinguishable. Indeed, despite their technical distinguishability, it hardly matters in most cases which bitcoin is withdrawn.

The primary issue is how such a tenancy in common would be created. In *Re Stapylton Fletcher*[147] cases of wine which had not been segregated by customer were sold to them as tenants in common until individual cases were appropriated to their individual contracts. The judge accepted that a tenancy in common could be used to remedy an unforeseen mixing, damage or loss[148] and observed that if a tenancy in common can be brought about by operation of law it can be equally brought about by agreement. Where A purchases wine and then delivers it to B, knowing that B already has cases of similar wine and he might not get the exact same case back, A therefore agrees to hold by way of tenancy in common with the other bailors.[149] There are two scenarios. In the first the client transfers digital assets acquired from a third party to the custodian's omnibus account, who purports to hold the assets in that omnibus account such that the clients are tenants in common of full legal title. As we have seen, the Law Commission suggest that intention alone cannot transfer title to a digital asset. The logic is that the custodian cannot take control of a pool of ether and hold then for a group of clients as tenants in common because if the custodian is being put in control of client A's ether how can

[145] Sheehan (n 54) pp 8-9
[146] Ibid pp 28-29
[147] [1994] 1 W.L.R. 1181; *Hill v Reglon* [2007] NSWCA 295; *Re London Wines* [1986] P.C.C. 121; Bridge et al (n 43) paras 19.005-19.006
[148] [1994] 1 W.L.R. 1181, at 1199
[149] Ibid at 1198; Goode and McKendrick (n 104) paras 8.41-844

control also be transferred to the other clients? It is not. One could respond that A transfers his ether to the custodian to hold on his (and others') behalf. Delivery to the custodian is constructive delivery to the other clients, but such an argument is largely fictional. The second scenario is that the custodian sells assets to the client and purports to hold on their behalf, but if factual control remains in the custodian how has legal title transferred to the clients? On the Commission's proposals it has not. The Law Commission is guilty of rejecting the very analysis it requires to rely on. On the view that a change of control should be needed to pass any form of legal title, it is impossible for a custodian receiving assets from another to hold them as bailee for legal tenants in common.

Even assuming that this contradiction can be avoided, another issue arises if the custodian places all custodial assets in the same omnibus account but accepts some on a trust basis so that the clients are equitable tenants in common and some on a bailment basis such that the clients hold superior title as legal tenants in common and the custodian has a lesser control-based interest. The issue is whether the trust could validly co-exist with the bailment. It cannot. There is no problem with the trust *per se*. In *North v Wilkinson*[150] the judge accepted that a trust over constantly changing business assets was conceptually possible. A beneficial interest would to 5% of "such fluctuating credit balance as might exist from time to time."[151] This implies that where there is a trust over a fund of ether the fact that the quantity of ether in the trust might change as new beneficiaries come in is irrelevant as is that the trustee-custodian might mix client funds with his own. All of this was accepted through the orthodox application of trust principles in *Ruscoe v Cryptopia*.

However, if the trustee-custodian mixes the assets with others to which he holds lesser control-based title and clients hold superior legal title the analysis is impossible. Do some of

[150] [2018] EWCA Civ 161, [2018] 4 W.L.R. 41
[151] Ibid at [16-24]

the clients (the A group who retain superior legal title) hold on trust for other clients (the B group who have equitable title)? If so, how are they invested with factual control of B group assets? They are not invested with any such control and do not hold on trust. The custodian is holding the B group assets on trust; if he has superior title to the commingled assets, however, vis-à-vis the A group assets he has both superior title and lesser title. If the analogy with possession holds, this is conceptually impossible. There is only one interest (in control); the only question is how (relatively) strong it is. The lesser title held from the A group is subsumed in the custodian's superior title over the whole commingled fund. Yet this defeats the object of the A group who lose their proprietary interest. If this is to avoided, there must be two funds held at the same address, but this raises the question of what happens in the case of a shortfall. Legal interests take priority over equitable interests so presumably the A group of clients recover their assets first and the B group are left to seek recovery of any losses from the trustee custodian. This, however, proves there is only one fund. Only then could a priority dispute arise. Not only is this an analytical mess, but an open invitation to fraud. The problem arises as a result of the Commission's desire to provide a smorgasbord or "palette"[152] of options from which parties can choose, options which are not analytically compatible. Courts and litigants have also been guilty of similar confusion, as is clear from *Janesh s/o Rajkumar v Persons Unknown (Chefpierre),*[153] where the claimant sought both conversion – entailing he had legal title – and an equitable proprietary claim – suggesting he did not.

[152] Law Comm (n 1) para 7.107
[153] [2022] SGHC 254; T Chan and K Low, 'DeFi Common Sense: Crypto-Backed Lending in Janesh s/o Rajkumar v Persons Unknown (Chefpierre)' (2023) 86 M.L.R. 1278

A burn address is one from which the asset cannot be retrieved; it is permanently out of circulation. As such the Law Commission identify a possible remedial lacuna in cases where the claimant has lost control of his digital asset. In cases where one party is enriched at the expense of another and has a valid unjust factor, the owner might be able to launch a successful unjust enrichment action.[154] This is not true in the case of burn addresses, where the defendant is not enriched by the asset. Green and Randall have, however, proposed that tangibility not be a prerequisite of the availability of conversion. Control of intangibles can be equated to factual possession, provided that the claimant has sufficient manual or cognitive indicia of possession,[155] a view that surfaced in the consultation paper[156] and is similar to Lai's argument outlined earlier. The Law Commission, however, pulled back in the final report from its prior more extensive acceptance of a type of conversion to propose the limited development of discrete principles of tortious liability to protect parties in such cases, developed by analogy with conversion.[157]

While it is not completely clear what this would amount to, the analogy with conversion suggests that the party whom we are protecting is the party with control. The controlling party, the custodial intermediary, will therefore be able to make good their legal title with some form of "quasi-conversion". Is the implication that the owner may have a tort of "quasi-reversionary injury" if he is unable to immediately demand redelivery from a custodian? Reversionary injury is an unfamiliar tort, but a pledgor (say) without an immediate right to possession cannot avail

[154] See eg *Fetch.ai v Persons Unknown* [2021] EWHC 2254; *Robert Ong Thien Chen v Luno Pty Ltd* [2021] 3 All Malaysia L Rev 143; A See and M Yip, 'Restitution for Mistakenly Transferred Bitcoin' [2022] L.M.C.L.Q. 46
[155] S Green and J Randall, *The Tort of Conversion* (Oxford: Hart, 2009) 132; S Green, 'The Subject Matter of Conversion' [2010] J.B.L. 218, 224-225
[156] Law Comm (n 9) paras 19.103-19.104
[157] Law Comm (n 1) para 9.76

himself of conversion. Instead, he sues in reversionary injury,[158] which is aimed at mopping up where there would otherwise be no liability despite the claimant's loss.[159] The Commission do not discuss the tort of reversionary injury, but the borrower's superior legal title must still be protected. Conversion and reversionary injury provide the wrong analogy, however. Conversion protects possession, but since the policy drivers for protecting possession are not present it is inappropriate to base protection of digital assets on an analogy to conversion and by extension reversionary injury or trespass. It is not enough to say that the owner of a bitcoin's property rights are a bit like those of the owner of a chair. This is a false invocation of the "property syllogism"[160] and ignores relevant disanalogies, such as we have seen, concerning the nature of the assets. What is needed is a careful analysis of the nature of the asset and the duties to be imposed. The Law Commission's – albeit now more limited – analogies with conversion are as apt to mislead as help.

Common Law Security Interests: Pledges

The Commission observe that under the 2022 revision of articles 9 and 12 of the Uniform Commercial Code a secured creditor may perfect a security interest by control and obtain priority over collateral takers who have registered their security. "It would be odd for the law to recognise this factual state of affairs and to acknowledge that some legal consequences…. can flow… but not to describe it as giving rise to some form of legal interest…"[161] In fact, the Commission's would be the odd position. To illustrate, I might seek to create an equitable fixed

[158] On which see Sheehan (n 54) pp 205-207; A Tettenborn (ed), *Clerk and Lindsell on Torts* 23rd edn (London: Sweet and Maxwell, 2022) paras 17.148-17.149
[159] *HSBC Rail (UK) Ltd v Network Rail Infrastructure Ltd* [2006] 1 All E.R. (Comm) 345 (CA); *Halliday v Holgate* (1868) L.R. 3 Ex. 299
[160] B McFarlane and S Douglas, 'Property, Analogy and Variety' (2022) 42 O.J.L.S. 161, 163
[161] Law Comm (n 1) para 5.84

charge over my bitcoin. It is typical for crypto-lenders such as Youhodler[162] or Bitcoin Suisse[163] to require that the collateral be deposited in their digital vault. The effect of this, assuming that full title is not transferred and a mortgage created, is that the lender with factual control now also has a lesser legal proprietary interest – defeasible on discharge. It is a common law pledge, not an equitable charge and the Commission have accepted that there is scope for a control-based security interest.[164] This would be a further development of their position that the common law might usefully develop an analogous concept to bailment.[165] This creates some real problems.

The bailee generally has a duty of care to the bailor -with the burden of proof reversed. This means that typically in cases concerned with tangible assets the bailee of a tangible asset must show he has not been careless if the asset is destroyed.[166] Imagine now that the vault is hacked, and my bitcoin provided as collateral stolen. Does the lender (who after all thought they were taking an equitable fixed charge) have a duty of care to me? The logic of the Commission's position is yes; although they do not explicitly argue for a duty of care in digital bailments in any detail, they do say that obligations imposed on a controller "especially if made subject to a duty of care" would have a social and protective function.[167] However, this result may impose on a collateral taker unexpected liabilities, which he does not have as a chargee or mortgagee[168] and against which he has not insured. We can go further. The Law Commission, as we have noted before, suggest that intention alone cannot transfer title to a digital asset. Intention is important in determining the legal consequences of control,[169] and change in

[162] See https://www.youhodler.com/crypto-loan (visted 31 Aug 2023)
[163] See https://www.bitcoinsuisse.com/collateralized-loans (visited 31 Aug 2023)
[164] Law Comm (n 1) paras 8.36-8.39
[165] Ibid paras 7.101-7.109
[166] Sheehan (n 54) p 243; *Port Swettenham Authority v Wu* [1979] A.C. 580
[167] Law Comm (n 1) para 7.108
[168] *AIB Finance Ltd v Debtors* [1998] 2 All E.R. 928
[169] Law Comm (n 1) para 5.56

control is needed for the transfer of title.[170] The result largely erases the distinction between a pledge and an equitable fixed charge (how else can we "fix" the charge without providing the chargee with some degree of control), but also largely erases the distinction between a pledge and a legal mortgage and more generally between "possessory" or "control-based" security interests and "non-possessory". Factual control is needed for the transfer of title, so a legal mortgage over digital assets requires a change of control just as a pledge does. The same answer might be given to the question whether the security needs registration under the Commission's yet to be fully fleshed-out proposals for "provision" of collateral as a perfection mechanism.[171] Intention is the only possible discriminant. The Law Commission again relies on intention whilst claiming scepticism as to whether finding intention is always possible.

Further difficulties mount if a lender tries to take a control-based pledge over an unallocated commingled fund. It is impossible to transfer constructive possession of part of a tangible bulk since we cannot be sure which specific part (barrels of oil or bushels of wheat) are to be attorned.[172] By analogy this is presumably true of passing constructive control of part of a fund of bitcoin. Equitable principles would allow for a charge to be taken over such an unallocated bulk. However, it would be difficult to see the practical distinction between a charge and a pledge – or indeed a mortgage - if courts deviated from the principle that transfer of a portion of a bulk was impossible with regard to digital assets.[173] Neither the pledgee (with "constructive control") nor the chargee would be in factual control, both would have the same remedies against the debtor in default and the same question would arise whether they are exempt from registration. There would be a priority distinction in that a pledge being a common law security would take priority, but how is a court to identify one from the other? Although

[170] Ibid paras 6.44-6.47
[171] Ibid para 8.135
[172] Bridge et al (n 43) paras 16.024-16.026
[173] Law Comm (n 1) para 8.37 and n 884

this is beyond our scope in this paper this may be what the Commission allude to in saying, "…There might also (or instead) be value in considering the parallel introduction of a novel type of security, capable of broad application as a meaningful alternative to mortgages and charges."[174]

Conclusion

The argument of this essay is simple. The Law Commission's proposals with regard to control and relativity of title to digital assets are misguided. While digital or crypto-assets can be seen as objects of property rights, and while they do have common features with tangible assets, such as their independence from the legal system, the policy drivers that lie behind possessory title do not apply. Digital assets should not, despite superficial similarities, be possessable. Nor should control be given a similar role. First, control seems largely indistinguishable from possession and the control-based title that it generates is largely indistinguishable from possessory title. Reinvention of the wheel is pointless. If the Law Commission wishes to apply a concept pretty much the same as possession to digital assets it should argue they are possessable. Secondly, control-based title is unnecessary. Equitable interests under a trust can solve all of the problems the Law Commission is concerned with. Thirdly, control-based title creates analytical headaches. It assumes for example that the problem of taking lesser control-based title over unallocated portions of a bulk is easier than the like issue of taking a lesser possession-based title, but more importantly at least two logical contradictions emerge. The Law Commission refuse to accept intention or agreement alone as a root of a transferee's title but must accept it to allow a tenancy in common in custodial intermediary cases. This has

[174] Ibid para 8.133

overtones of “cake-ism”. Their enthusiasm for a “palette” of legal options also leaves the possibility open for the incoherency of a custodian intermediary apparently having both a superior and inferior legal title over the same assets in the same mixed pool at the same time.

The article has been mainly critical. It has been intended to show why the Law Commission are wrong about control, but a more positive conclusion is possible. If relative control-based title is undesirable in policy terms and gives rise to apparently legally impossible outcomes, the contrary option must be adopted at least in the absence of the (vanishingly unlikely)[175] decision that crypto-assets should not, as a legal policy matter, be ownable. Title to digital assets, like title to all other intangibles, must be unitary. Having recognised the right to these things, only then can we decide how to protect it.

[175] But see Stevens (n 20) who argues for exactly this decision