CRYPTOCURRENCIES IN THE COMMON LAW OF PROPERTY

**Abstract**

The development of cryptocurrency technology has been driven by a desire to create autonomous systems for carrying out digital transactions. The people who use them may neither seek nor want extraneous legal intervention. Property law is as much a kind of state intervention as all the more familiar rules of financial or securities regulation that have attracted so much attention from legal commentators. Property law is default law. If a certain resource can be characterised as an object of property, then the rules of property law apply to it as far as the nature of the resource allows.

The view advanced here is that many features of a common law system of property would apply to cryptocurrencies. Once the data comprising crypto-coins are understood for what they are, they should be a suitable object of property. The old binary conception of personal property consisting in choses in possession and choses in action should not be an obstacle, if indeed it ever was, to their recognition as property. With some necessary adaptation to allow for the intangibility of crypto-coins, the usual rules of derivative transfer of title and tracing could apply to them.

Granted, the common law has no ready-made rules especially designed for cryptocurrencies. But that very absence of rules may be as much an adaptive strength as a systemic failing. The common law grows by a process of principled analogy between the old and the new. The common law provides a reserve of general principle that can provide a default set of property rules for cryptocurrencies without the need for targeted statutory intervention.

# CRYPTOCURRENCIES IN THE COMMON LAW OF PROPERTY

*D M Fox*[*]

The language of property is familiar enough in discussions of cryptocurrencies. People who control a private key are commonly said to "own" the crypto-coins accessed by it. Investors are encouraged to "buy" cryptocurrencies, where buying implies some acquisition of rights in the coins and their realisable value.

But once we enter the technical realm of common law property, we find that cryptocurrencies do not make an easy fit. The difficulty goes beyond commonplace assertions about the law being slow to react to technological change.[1] To say that common law conceptions of property originally developed for a world consisting of physical objects is only to state the obvious. The reasons for the difficulty run deeper. They stem from the autonomous motivations of cryptocurrency users and the technical design of the cryptocurrency systems themselves.

The development of cryptocurrency technology has been driven by a desire to create autonomous systems for carrying out digital transactions. The people who use them may neither seek nor want extraneous legal intervention. Their motivations are part of a more general argument for cyber-space exceptionalism, which would limit the state's role in regulating virtual communities.[2] Property law is as much a kind of state intervention as all the more familiar rules of financial or securities regulation that have attracted so much attention from legal commentators.[3] Property law is default law.[4] If a certain resource can be

[*] School of Law, University of Edinburgh.

[1] Eg, S Bayern, "Dynamic Common Law and Technological Change: the Classification of Bitcoin" (2014) 71 Wash & Lee L Rev Online 22 (Bayern's paper stands as a rare consideration of the status of cryptocurrencies in private law); K Szilagyi, "A Bundle of Blockchains? Digitally Disrupting Property Law" (2017-18) 48 Cumb L Rev 9. For recognition of the general problem in common law doctrine, see S Green and J Randall, *The Tort of Conversion* (Hart, 2009), ch 5, responding to *OBG Ltd v Allan* [2007] UKHL 21; [2008] 1 AC 1; and *Your Response Ltd v Datastream Media Ltd* [2014] EWCA Civ 281, [2015] QB 41, paras [9]-[10] per Moore-Bick LJ, [38]-[39] per Davis LJ.

[2] See generally N Suzor, "The Role of the Rule of Law in Virtual Communities" (2010) 25 Berkeley Tech LJ 1817.

[3] For a small sample, see E P Pacy, "Tales from the Cryptocurrency: on Bitcoin, Square Pegs and Round Holes" (2014) 49 New Eng L Rev 121; O Marian, "A Conceptual Framework for the Regulation of Cryptocurrencies" (2015) 82 U Chi L Rev Dialogue 53; N D Swartz, "Bursting the Bubble: the Case to Regulate Digital Currency as a Security or Commodity" (2014) 17 Tul J Tech & Intell Prop 319; K V K Singh, "The New Wild West: Preventing Money Laundering in the Bitcoin Network (2015) 13 Nw J Tech & Intell Prop 37; Tu and M W Meredith, "Rethinking Virtual Currency Regulation in the Bitcoin Age" (2015) 90 Wash L Rev 271; J E Glass, "What is a Digital Currency?" (2017) 57 IDEA: J Franklin Pierce for Intell Prop 455.

characterised as an object of property, then the rules of property law apply to it as far as the nature of the resource allows. The parties are bound by property law whether they realise it or not. They need to contract out of it to exclude its operation. Experience shows that users of cryptocurrencies do not contract out (if only perhaps because the rules of private law seldom occur to them).

In their technical operation cryptocurrency systems seem designed to frustrate property law. Systems designed to obscure the claims of strangers to payment transactions, to eliminate the need for adjudication in payment transactions and to hide the real-world identity of the people behind them are not an easy object for traditional rules of property law. The systems come close to being self-regulating. Transactional outcomes are determined by cryptographic design rather than legal rules.

Despite these problems, the view advanced here is that many features of a common law system of property would apply to cryptocurrencies. They do not exist in a property void. Individual crypto-coins consist of specific units of information that, properly understood, would make suitable objects of property.[5] Ownership rights in them could be created and transferred by the usual rules of derivative acquisition of title. A former holder of crypto-coins would retain a title to them if a transaction on the blockchain was void or voidable according to the property transfer rules of common law and equity.[6] Rules of tracing would allow titles to cryptocurrencies to pass through transactions on the blockchain, and might even to allow mixtures of them to be unscrambled.[7] Property law might allow misapplied crypto-coins or their value to be recovered by a claimant even when transactions on the blockchain were, in a cryptographic sense, irreversible.

Property law matters both internally and externally to a cryptocurrency system. Internally – among the users of the system – property law is a justifiable ground for the recovery of coins or their value when they are stolen or transferred by fraud. The irreversibility of

[4] The theory of default law has been most fully developed in relation to contracts (eg, A Schwartz, "The Default Rule Paradigm and the Limits of Contract Law" (1993) 3 S Cal Interdisc L J 389), but has been extended to explain the relationship between third parties and property-holding institutions such as corporations and trusts: H Hansmann and R Kraakman, "The Essential Role of Organizational Law" (2000) 110 Yale LJ 387; and H Hansmann and U Mattei, "The Functions of Trust Law: A Comparative Legal and Economic Analysis" (1998) 73 New York University LR 434.
[5] See paras 000 below.
[6] See paras 000 below.
[7] See paras 000 below.

cryptocurrency transactions, in a purely technological sense, need not bar the reversal of their legal effect or the recognition that they are legally defective. Property law has its own systemic norms.

Externally – to third parties dealing with users of the system – the recognition of cryptocurrencies as objects of property is no less important. It is only a matter of time before cryptocurrencies are used in transactions external to the blockchain. Property is a gateway to many standard forms of transaction. A crypto-coin can never become the subject-matter of a trust or a proprietary right of security, nor will it be an asset in a deceased person's estate, unless it is first recognised as an object property.[8] The same is true of a secured creditor or trust beneficiary enforcing their claim in priority to the unsecured creditors of an insolvent coin-holder.[9] The development of a viable cryptocurrencies derivatives market requires that the primary assets from which secondary claims are constructed are capable of legal recognition as property.[10]

*Approach and terminology*

This chapter takes Bitcoin as the main example of a cryptocurrency since it is most commonly used in practice. From time to time the chapter refers to other cryptocurrencies, such Ethereum and Zerocash, when their different functionality might affect the property analysis.

The technical design of cryptocurrencies determines the kind of legal explanation applied to them. In explaining the computer science of cryptocurrencies, this chapter draws heavily on the writings of Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder at Princeton, Stanford and Maryland,[11] and on conversations with Ross

[8] Value measurable in monetary units cannot be the subject-matter of a trust unless is embodied in a specifically ascertainable item of property: *Fortex Group v. Macintosh* [1998] 3 NZLR 171. The difficultly of accommodating digital assets within inheritance rules developed for traditional forms of personal property has led to the promulgation in 2016 of the model *Revised Uniform Fiduciary Access to Digital Assets Act* by the United States Uniform Law Commission.

[9] Eg, Insolvency Act 1986, ss 283(1), 306.

[10] For regulatory recognition of developments in cryptocurrency derivatives, see US Commodity Futures Trading Commission, Release No 7731-18, (21 May 2018) "Advisory for Virtual Currency Products" https://www.cftc.gov/PressRoom/PressReleases/7731-18 (accessed 11 August 2018); and Financial Conduct Authority "Cryptocurrency derivatives" (6 April 2018) https://www.fca.org.uk/news/statements/cryptocurrency-derivatives (accessed 11 August 2018).

[11] Principally, A Narayanan, J Bonneau, E Felten, A Miller and S Goldfeder, *Bitcoin and Cryptocurrency Technologies: a Comprehensive Introduction* (Princeton and Oxford, 2016).

Anderson, Ilia Shumailov, Alessandro Rietmann and Mansoor Ahmed at the University of Cambridge Computer Laboratory.[12]

Finally, property is by nature concerned with legal rights that affect strangers to bilateral transactions.[13] Property problems usually come with at least three parties. For clarity's sake, this chapter uses the familiar alphabetical names used in the computer science literature. Alice, Bob and Carol are named as the parties in the cryptocurrency transactions, and, in complex cases, David and Erica are recruited to the transactional cast.

## A crypto-coin as an object of property

This section considers how a crypto-coin might be considered as an object of property. That task requires a closer look at what a crypto-coin actually is since its correct characterisation as a thing affects the kind of property explanation that we apply to it. The first part of the inquiry is theoretical. We ask whether a crypto-coin could make a suitable object for any regime of property rights at all.[14] This then leads to the legal doctrinal question of how, if at all, a crypto-coin would fit within the established common law rules of personal property.[15]

### Data strings recording transactions[16]

As a specific locus of monetary value, a crypto-coin is an ideational construct. Its function and value as a medium of exchange or investment commodity exist only in the shared understanding of the users who make transactions on a cryptocurrency system. The coin itself has no intrinsic value. The source of its value is extrinsic to itself, imposed by the collective belief of the people who use it.[17]

[12] The responsibility for any errors in understanding of the computer science lies with me alone.
[13] This is the "third party impact" explained by K Gray and S F Gray, *Elements of Land Law*, 5th ed (Oxford, 2008), para 1.5.28.
[14] See paras 000 below.
[15] See paras 000 below.
[16] This technical description draws on Narayanan et al, n 000 above, chs 1-3; and S Nakamoto, "Bitcoin: a Peer-to-Peer Electronic Cash System' p 2 https://Bitcoin.org/en/Bitcoin-paper (accessed 21 July 2018).
[17] The legal distinction between the intrinsic and extrinsic value of money dates from the precious metal coinages of the middle ages: see W Ernst, ch 7 "The Legists' Doctrines on Money and the Law from the Eleventh to the Fifteenth Centuries" in D Fox and W Ernst (eds), *Money in the Western Legal Tradition: Middle Ages to Bretton Woods* (Oxford, 2016). The difference with cryptocurrencies is that the extrinsic value is imposed by an informal consensus rather than by legal act of a sovereign monetary authority.

A crypto-coin takes its form from the recording of transactions on a cryptocurrency system. Stripped to its elements, the coin consists of a string of data, manifested as a readable sequence of characters, which has been generated by a transaction on the system. The transaction might have been the original one where the coin was first mined or a later one where a user transferred a coin already in existence. The data string records a transactional output of value at the public key of the person who now has the power to transact with it by using his or her private key. For this reason, the coin is often called "an unspent transaction output" ("UTXO"). Spending the coin requires the holder of the output to use it as the input for the next transaction on the system. If, for example, Alice transfers 5 BTC from her public key, $pk_A$, to Bob at $pk_B$, then the string representing the 5 BTC output at $pk_A$ becomes the input to this new transaction. The string representing 5 BTC at $pk_B$ is the new output.

The blockchain works on a transaction ledger rather than on an account ledger system.[18] It records the existence and value of transactions between public keys rather than the net balance of coin value associated with each public key and available for spending from it. To return the example just given, the blockchain records the 5 BTC transaction between $pk_A$ and $pk_B$ and that, for the present, the 5 BTC output remains unspent at $pk_B$. Each transaction leading to an output has a distinct identity. What the system does not do is to record the total BTC balance of unspent transactions associated with $pk_B$.[19]

The blockchain record differs in this way from an account kept in a conventional bank money system. A bank account records every credit and debit transaction into the account but then goes on to calculate the running balance after each transaction. The account-holder spends out of the debt representing the net balance, which in legal analysis is a thing in itself and the primary object of the account-holder's legal right.[20]

With a transactional ledger, however, the recorded network of transactional links is the thing in itself. Granted, the balance generated by all those links would be ascertainable by Bob, and indeed by any other user of the system who knew the address of his public key.[21] By

[18] See Narayanan et al, supra n 000, pp 52-53.
[19] Bitcoin differs in this way from the Ethereum system which directly calculates the balance of token value available for spending.
[20] On the relationship of debtor and creditor between bank and customer, see *Foley v Hill* (1848) HLC 28; *N Joachimson v Swiss Bank Corporation* [1921] 3 KB 110.
[21] Bitcoin balances are searchable by entering the address of a public key into a number of Bitcoin user interfaces, such as http://www.homebitcoin.com/easybalance/ or https://bitcoinwhoswho.com/ (accessed 14 August 2018).

Bob's lights, as a human user of the system, he would probably think of each transaction output at $pk_B$ as combining to form a single balance of fungible value available to spend. But such an understanding of the transaction is secondary to the primary information recorded on the blockchain. It is that primary information which, if anything, has to be object of any property right that Bob may assert in relation to it.

The transaction record on the blockchain differs in one other important way from the record of debits and credits to a conventional bank account. The blockchain gives every transaction a unique identifier. It enables the most recent transactional output at $pk_B$ to be identified by reference to the input at $pk_A$ that was consumed in creating it. In turn, the input in the $pk_A$ - $pk_B$ transaction derives its identity as an output of an earlier transaction, going back to the first output on the system when the coin was mined. By this series of recorded transactional links, every coin keeps a unique identity.

It is important however to clarify what is meant by saying that every coin has a unique identity since this has a bearing on the correct form of property law analysis. The coin is only a notional entity, a convenient way of imagining the BTC value represented by the output associated with a public key. The coin representing the input to the transaction at $pk_A$ is destroyed and replaced by another coin representing the transaction output at $pk_B$. We should not imagine the data string representing the coin at $pk_A$ as being transferred to pkB. The data strings at each public key, before and after the transaction, are distinct. We can however identify the one with the other because of the recorded transactional link between them, going back to a specific mining transaction. The BTC value formerly associated with a specific data string at $pk_A$ is now associated with the data string at $pk_B$. Value flows from pkA to $pk_B$ by the consumption and creation of distinct informational entities at each public key.

To this very limited extent, there is an analogy with the way conventional bank payment systems operate. Suppose that Alice pays Bob £100 by bank transfer. The flow of monetary value between them consists in the destruction (or reduction in value) of the debt owed by Alice's bank to herself and the creation (or increase in value) of a debt owed by Bob's bank to himself.[22] Nothing which could be the subject of a property right passes directly from

[22] *R v Preddy* [1996] AC 815, applying the former Theft Act 1968, s 15. See generally D Fox, *Property Rights in Money* (Oxford, 2008), 5.23-5.24.

Alice to Bob. Any false analogy with the payment of corporeal money, such as coins or banknotes, is best avoided, both in explaining bank transfers and transfers of a cryptocurrency. If Alice pays Bob £100 in banknotes, then the transfer of monetary value tracks the movement of a continuing thing, an object of property, between them. All that happens in the bank and the cryptocurrency payments is that value flows through the consumption and creation of distinct entities, although with the difference that in the bank transaction the entities are debts while in the cryptocurrency transaction they are unique items of digital information.

**Fungibility, specificity, scarcity and exclusion**

*Fungibility as an aim of cryptocurrency design*

The fungibility of cryptocurrencies has been one of the main concerns of the designers who develop them and the users who transact with them.[23] The ideal is that a coin representing an unspent transaction output on the system should have the same exchange value in payments as any other coin on the system. This goes beyond saying that all coins on the system should carry a nominal value of 1 BTC each. The concern is that every coin nominally worth 1 BTC should be equally acceptable at 1 BTC when it is paid in a transaction for a debt of 1 BTC or when it exchanged in a "real-world" transaction for a state-issued currency, such as pounds sterling or US dollars. The concern is that the exchange value of individual coins is not fungible: it may differ from coin to coin because their traceable transactional history can identify certain of the coins as tainted. If some coins can be traced as the proceeds of criminal conduct, then some parties to payment transactions, notably coin exchanges, reject them or discount their exchange value to reflect their tainted origins. Coins that derive from clean sources – or at least sources that cannot be identified as tainted – pass in transactions at their full nominal value, which gives them a premium over those that are tainted. The solution proposed to this problem has to develop cryptographic techniques with stronger anonymity or forms of payment transaction that obscure the traceability of coins.[24] For want of any competing evidence to taint their origins and their value in exchange, all coins would be fungible with one another in payment or investment transactions.

[23] See Narayanan et al, supra n 000, at p 219; and D Vorick, 'Ensuring Bitcoin Fungibility in 2017 (and Beyond)" https://www.coindesk.com/ensuring-Bitcoin-fungibility-in-2017-and-beyond/ (accessed 21 July 2018).
[24] See further 000 below.

*Fungibility and specificity in property law*

The concern with fungibility in property law is quite different. The specificity of a resource is essential to its characterization as an object of property. Property must relate to some identifiable and discrete resource. It cannot confer a floating entitlement to all resources of the same generic type.[25] Alice's ownership of one £10 note does not entitle her to replace it with any other £10 note currently owned by Bob.

The requirement of specificity relates to another hallmark of property, which is the power in the holder of the right to exclude non-entitled third parties from access to a resource.[26] As a minimum, any resource that is made the object of property lends itself to protection against unauthorised interference or use by others. It is a kind of resource from which it is practically possible to exclude others.[27] A resource that is practically open to all takers or all users may never be a suitable – or at least an easy – candidate for exclusive appropriation to one person through a regime of property rights. Resources that are suitable for a property regime also tend to be scarce.[28] Resources which are abundantly available or which can be reproduced by anyone at will, do not naturally lend themselves to a property regime. Their existence as property depends entirely on the strength of the "trespassory" rules that control access to them and penalize unauthorized exploitation of them.[29]

In law, the fungibility or specificity of a thing is not an absolute property of the thing itself. The characterisation of the thing as fungible or specific depends instead on the perspective of the parties to a transaction and the kinds of legal right at issue between them.[30] If Alice owes Bob a debt for £100 then she can satisfy the obligation by tendering any combination of coins, notes or incorporeal bank balances with a nominal value of £100. The money here is fungible since the identity of the things tendered in payment is irrelevant to the performance

[25] A proprietary right of security, such as a mortgage charge, must attach to some specific asset or assets, even though the money raised by enforcing it may be less than the full value of the assets it attaches to.
[26] The exclusivity of property has been extensively considered in the literature. For a small sample, see J W Harris, *Property and Justice* (Oxford, 1996), 24-26 (discussing "trespassory rules"); J E Penner, 'The Bundle of Rights Picture of Property' (1995-96) 43 UCLA L Rev 711, 807-813 (discussing a duty of non-interference); J E Penner, *The Idea of Property in Law* (Oxford, 2000), ch 4; T W Merrill, 'Property and the Right to Exclude' (1998) 77 Neb L Rev 730; L Katz, 'Exclusion and Exclusivity in Property Law' (2008) 58 U of Toronto LJ 275; K Gray and S F Gray, *Elements of Land Law*, 5th ed (Oxford, 2008), para 1.5.38.
[27] K Gray, "Property in Thin Air" [1991] CLJ 252, 269-273.
[28] J W Harris, *Property and Justice* (Oxford, 1996), 23-24.
[29] Ibid, 43.
[30] The implication is that any specific asset can for some purposes be regarded as a repository of fungible wealth: B Rudden, 'Things as Things and Things as Wealth' (1994) 14 OJLS 81. For the fungibility of money, see generally D Fox, *Property Rights in Money* (Oxford, 2008), paras 1.78-1.86.

of Alice's debt for a monetary amount. As it happens, the law of property applied to traditional state-denominated currencies is structured to ensure that the exchange value of each of those means of payment corresponds, without a discount, to its nominal value. It has already come close to the end-point that developers of cryptocurrency technology are working to reach. [31]

But when money as the object of property then it as specific as any item of unique property we might imagine. The ten £10 notes owned by Alice are as uniquely and specifically hers as any specially commissioned work of art she may happen to own. If Carol takes those same notes, intending to replace them with ten others of equal value, she is as much a thief of the notes as she would be if she had appropriated one of Alice's art works.[32]

*Cryptocurrencies as either fungible or specific in law.*

From the perspective of private law, a crypto-coin would be fungible or specific like any other asset. It would be fungible when the system users treat it as a certain quantity of nominal BTC value. If Alice owed Bob a 5 BTC debt, then she would be free to use any unspent output or outputs held at her public keys, provided that they together equated to 5 BTC. As the possible object of a property regime, however, the data string constituting each coin is a specific thing. It is uniquely identifiable as the latest output of a chain of traceable transactions which connect it back to the original output on the system when the coin was first mined. It is in this sense as specific as the value traced through the bank transfer between Alice and Bob explained earlier.[33] If anything, the specific connection in the crypto-coin payment is even stronger. When Alice pays 5 BTC from $pk_A$ to Bob at $pk_B$, the transactional output at Bob's public key would carry a cryptographic record connecting it with the input at Alice's public key. Unlike the bank transfer, it would not depend on artificial legal rules of attribution, which were extraneous to the payment system, to identify the value in the input and output with each other.

*Scarcity and exclusivity*

[31] For the relationship between property transfer rules and the exchange value of money, see D Fox, *Property Rights in Money* (Oxford 2008) ch 2. The historical development of the law of property in money has generally been skewed against the assertion of adverse titles to money by a former holder of it: see D Fox, "*Banks v Whetson* (1596)", ch 1 in S Douglas, R Hickey, E Waring (eds.), *Landmark Cases in Property Law* (Oxford, Hart Publishing, pp 3-24.
[32] Eg, *R v Velumyl* [1989] Crim LR 299.
[33] See 00-000 above.

A crypto-coin also stands up well against the tests of scarcity and exclusivity. Bitcoins, for example, are scarce by systemic design. The Bitcoin protocol is designed with a cap on the number of new coins that can be mined. No more than 21 million of them can ever be created. This constraint on unlimited monetary creation is one of its characteristic features. It was intended to give Bitcoin a credibility that central-bank created state currencies were thought to have lost after the financial crisis of 2008.[34] Scarcity is also inherent in the working of individual coin transactions. The system prevents double-spending of the same coin. The cryptography that protects Alice's exclusive capacity to sign payment transactions and to pay her coin to Bob connects a finite quantity of BTC value to a unique coin. She cannot multiply the nominal BTC value in the system by first consuming 5 BTC of unspent value in a transaction with Bob then consume it again in a second transaction with Carol.[35]

Access to the data string representing the 5 BTC value is, in a practical sense, exclusive to whichever of the users –Alice or Bob – controls the public key that the data is associated with. It makes no difference that all transactions between public keys are public and discoverable by other users of the system. The publicity of the information constituting the data string does not enable the public to transact with it on the system. Mere knowledge that a certain data string is associated with a public key does not enable the public at large to use its one meaningful incident, which is its capacity to be consumed in a transaction. Like any other form of currency, the only real way to use a crypto-coin is to spend it.[36] That power lies exclusively with the person who controls its private key.

## Crypto-coins in the law of personal property

### *Choses in possession and choses in action*

As far as existing private law doctrine goes, cryptocurrencies do not fall into either of the conventionally-recognised categories of personal property. According to the classical statement of Fry LJ in *Colonial Bank v Whinney* in 1886, these categories refer either to choses in possession or choses in action. No intermediate category exists to cover other

[34] See R Ali et al, "Innovations in Payment Technologies and the Emergence of Digital Currencies" Bank of England Quarterly Bulletin (2014, Q3), p 6 https://www.bankofengland.co.uk/-/media/boe/files/digital-currencies/the-economics-of-digital-currencies (accessed 22 July 2018).

[35] For double-spending, see S Nakamoto, "Bitcoin: a Peer-to-Peer Electronic Cash System' p 2 https://Bitcoin.org/en/Bitcoin-paper (accessed 21 July 2018); and A Narayanan et al, *supra* n 000, pp 21-25, 34-38. See further ch 000 [Green: introduction].

[36] See para 000 above.

forms of intangible property that cannot be analysed as choses in possession.[37] The definition of property in criminal law may be wider. The Theft Act 1968 defines "property" for the purposes of theft as "including things in action and other intangible property".[38] The inclusion of "other intangible property" apart from choses in action may be a deliberate extension of the private law definition of personal property or at least mark a preference for leaving the category of intangible property open to development.

It is easy to explain why cryptocurrencies cannot be characterized as choses in possession. The data strings comprising the coins are intangible and cannot be physically possessed. The coin consisting in an unspent transactional output is just an ideational entity.

The conclusion that cyber-currencies are not choses in possession means that some standard common law methods of proprietary protection would not be available to enforce a title to them. Tortious actions, such as trespass or conversion, would not lie to protect a putative owner's title to them.[39] The prevailing view in English law, which the House of Lords confirmed in *OBG Ltd v Allan*, is that these actions depend on proof of interference with actual possession or a right to immediate possession of the subject matter of the claim.[40] Possession has been confined to its traditional sense which requires some physical control over a tangible thing. This view was strongly challenged in *OBG Ltd v Allan* but the House of Lords affirmed it.[41] An intangible thing cannot be possessed for the purposes of common law tort claims simply because one person can exercise exclusive control over access to it.[42]

Neither are cyber-currencies choses in action. This follows from the defining difference between cyber-currencies recorded on a distributed ledger and the conventional currencies

[37] *Colonial Bank v Whinney* (1885) LR 30 Ch 261, 285-86 per Fry LJ, adopted (1886) LR 11 App Cas 426 (HL).
[38] Theft Act 1968 s 4. A similar definition applies for the purpose of identifying a relevant gain or loss under the Fraud Act 2006, s 5.
[39] The common lacks an action for the direct enforcement of ownership in tangible property. Ownership is instead enforced indirectly by actions founded on a title to possession. Hence the remark commonly made that English law does not recognize an action equivalent to the *vindicatio* of classical Roman law: *OBG Ltd v Allan* [2007] UKHL 21, [2008] 1 AC 1, para [308] per Baroness Hale.
[40] *OBG Ltd v Allan* [2007] UKHL 21; [2008] 1 AC 1. For title to sue in conversion, see *Kuwait Airways Corporation v. Iraqi Airways Co (Nos 4 and 5)* [2002] 2 A.C. 883, 1083-1098 *per* Lord Nicholls.
[41] *Your Response Ltd v Datastream Media Ltd* [2014] EWCA Civ 281, [2015] QB 41. For the argument to the contrary, see S Green and J Randall, *The Tort of Conversion* (Hart, 2009).
[42] *Your Response Ltd v Datastream Media Ltd* [2014] EWCA Civ 281, [2015] QB 41; *Environment Agency v Churngold Recycling* [2014] EWCA Civ 909, [2015] Env LR 13.

that depend on the existence of centralised intermediaries.[43] In the simplest case, where Alice directly controls her own secret key for making transactions on the system, she is the putative owner of the data string representing the coin. Her ownership does not consist in the power to enforce another person's obligation for the delivery of the coin. Her situation would be different from Bob's if had £100 in his bank account. Bob's "money in the bank" is essentially his contractual right to compel the bank to pay legal tender in discharge of the debt owed to him and to authorise the bank to make payments from the account as an agent on his behalf.[44] The characterization of Bob's entitlement as the right to enforce a debt is the flipside the economists' observation that fiat money and bank money consist in circulating credit. Money consists in a notional loan enforceable by a creditor against a debtor (although in practice the creditor never calls in the loan for payment in legal tender). [45]

We need to add a refinement here to explain the rights of the users or investors in cryptocurrencies who have hold accounts with wallet service providers or cryptocurrency exchanges. At its simplest, a wallet is a place where the user stores the private and public keys that give access to the coins associated with them. Rather than hold the keys as a paper record or as a file on his or her own hardware, the user may instead hold it remotely through an online wallet service.[46] The arrangement between the service provider and the user is more akin to that of a conventional banker and its customer. The service provider holds the coins as things in themselves at public keys controlled by them. The account holder's right is to direct payments with the coins or to realize their capital value by selling them.[47] Here the depositor's rights are indeed in the nature of a chose in action. The account holder could enter into real world transactions with the chose in action, such as declaring a trust or granting an equitable security over it. But any interest of the trust beneficiary or grantee of the security would ultimately depend on enforcement of a personal claim against the service

[43] S Nakamoto, "Bitcoin: a Peer-to-Peer Electronic Cash System' p 1 at https://Bitcoin.org/en/Bitcoin-paper (accessed 21 July 2018). For the operation of the distributed consensus protocol, see A Narayanan et al, *supra* n 000, ch 2.
[44] *Foley v Hill* (1848) HLC 28; *Lipkin Gorman v Karpnale (a firm)* [1991] 2 AC 548, 573–4 per Lord Goff.
[45] A Sáinz de Vicuña, "An Institutional Theory of Money", ch 25 in M Giovanoli and D Devos, *International Monetary and Financial Law: the Global Crisis* (Oxford, 2010).
[46] See https://www.coindesk.com/information/how-to-store-your-bitcoins/ (accessed 30 July 2018).
[47] M Möser, "Anonymity of Bitcoin Transactions" (Münster Bitcoin Conference, July 2013), 2.3.

provider. If the service provider became insolvent, the beneficiary or the grantee would not have any special priority against the service provider's assets.[48]

*Intangible personal property other than choses in action*

Cryptocurrencies could only be the direct objects of property in private law if a third category of personal property were recognised apart from choses in possession or choses in action. The view of Fry LJ in *Colonial Bank v Whinney* was that there was no such third category. It is worth considering his reasons since they affect the status of the case as a general precedent.

The question in *Colonial Bank v Whinney* was a narrow point of statutory interpretation: whether shares in a public company were "choses in action" within the meaning of the reputed ownership provisions of the Bankruptcy Act 1883. Fry LJ dissented from the majority view of Cotton and Lindley LJJ in the Court of Appeal, and held that they were choses in action. The House of Lords upheld Fry LJ's analysis and adopted his reasons.[49] Fry LJ said that there could be no occupation or enjoyment of the shares themselves although there could be of the fruits (such as dividends and other benefits) arising from them. The only way to obtain the fruits was by an action at law. This should have been enough to dispose of the point. But Fry LJ went on to say that there was no third category of personal property. He disagreed with the majority's view of what a share consisted in. In their view, the registered proprietor of shares held them as things in themselves: "He has the ownership of the share, and he cannot get anything more than he has already got."[50] On the majority view, the shareholder's right to the dividends due under the shares might be a chose in action but not the shares themselves. Thus the real disagreement in the case was about the proper characterization of shares: whether they were things in themselves, over and above the entitlements associated with them, or merely an aggregation of those entitlements, all of which could be enforced by action.

The authority for Fry LJ's binary categorization of personal property was drawn from Sir William Blackstone's *Commentaries on the Laws of England* (1765-69).[51] Blackstone wrote:

[48] Compare *Space Investments Ltd v Canadian Imperial Bank Trust Co (Bahamas) Ltd* [1986] WLR 1072 where trust moneys were held by a trustee on deposit at a bank which became insolvent.
[49] (1886) 11 App Cas 426.
[50] Ibid, 284 per Lindley LJ.
[51] W Blackstone, *Commentaries on the Laws of England*, 1st ed (1766), facsimile edition, (University of Chicago Press, 1979).

> Property, in chattels personal, may be either in possession; which is where a man hath not only the right to enjoy, but hath the actual enjoyment of, the thing: or else it is in action; where a man hath only a bare right, without any occupation or enjoyment.' [52]

This explanation followed his description of the variety of 'chattels personal' which, he said, were things moveable, 'which may be annexed to or attendant on the person of the owner, and carried about with him from one part of the world to another.'[53] He proceeded in the next section to take "a short view of the nature of property in action" where a person's property was "but merely a bare right to occupy the thing in question; the possession whereof may however be recovered by a suit or action at law: from whence the thing so recoverable is called a thing or *chose, in action*'.[54] He gave examples of money recoverable on a contract or rights to damages recoverable by legal judgment and execution.

Blackstone's understanding was that all 'chattels personal' were tangible objects ultimately capable of physical possession. The purpose of his exposition was to describe 'the nature of a person's property or dominion, to which they [the chattels personal] are liable".[55] Property in a moveable object did not depend on the holder keeping it in his or her physical possession. Property in the object subsisted, albeit in 'bare' form, if a legal action was available to recover possession of it. When a thing was "in action" it was *in potentia* rather than *in esse*.[56]

Seen in this way, Blackstone's argument had more to do with the nature and enforcement of property in tangible objects than the larger categorisation of things in which property might exist. He demonstrated that property in things was not so fragile that it required continuing possession to sustain it. The legal relationship between the holder and tangible things subsisted so long as an enforceable cause of action could bring the thing back into the holder's physical possession. Blackstone did not say that no third category of personal property existed. He did not turn to the question whether property did (or could) exist in things without any tangible foundation at all. His silence on that point may have had more to do with the way he understood the proper taxonomy of public and private law than any doctrinaire position about the content of personal property. Rights such as patents, which

[52] Blackstone, *Commentaries*, vol 2, 396-97.
[53] Ibid, 387.
[54] Ibid, 396-97.
[55] Ibid, 388
[56] Ibid, 397.

would nowadays be candidates for a third category of personal property, belonged to a different part of Blackstone's scheme. In his view, patents for new inventions were statutory exemptions from the general common law prohibition on monopolies.[57] He treated them as an exemption from a larger category of public wrong instead of a species of thing that needed to be fitted into a binary scheme of common law property.

*The current authorities*

Reading Blackstone in this way, it should at least to be open to question whether the private law category of intangible property consists exclusively in choses in action, as Fry LJ said in *Colonial Bank v Whinney*. The recent authorities are divided on the point. On the one hand, Stephen Morris QC, sitting as a Deputy High Court Judge in *Armstrong DLW GmbH v Winnington Networks Ltd*, accepted that the categories of personal property were not confined to choses in action and choses in possession.[58] He returned to first principles about the defining features of property in the law, and held that an allowance under an EU carbon emissions trading scheme was a species of property. The allowance created a transferable immunity from prosecution for exceeding a carbon emissions target. On the other hand, dicta of Moore-Bick and Floyd LJJ in *Your Response Ltd v Datastream Business Media Ltd* stand against the view that there is a third category of personal property.[59] A second objection from that case was Floyd LJ's remark that information has never as such been treated as property, although the physical medium on which it is recorded may be property.[60]

It is instructive to apply the tests from *Armstrong DLW GmbH v Winnington Networks Ltd* for determining whether an intangible asset might be treated as property. The Deputy High Court judge, Stephen Morris QC, held that the intangible carbon allowance under an EU carbon trading scheme was property, and that the holder from whom it was stolen could sue on a proprietary restitutionary claim to enforce its retained legal title. The allowance was definable (to the extent of having a unique reference number), and identifiable by third parties. Its value derived partly from the possibility of trading with it in a market. It was

[57] Ibid, vol 4, 159. For the place of intellectual property rights in the modern scheme of property law, see ch 000 [Carr].
[58] *Armstrong DLW GmbH v Winnington Networks Ltd* [2012] EWHC 10 (Ch); [2013] Ch 156, considered K F K Low and J Lin, 'Carbon Credits as EU Like It" (2015) 27 *J of Environmental Law* 377-404.
[59] *Your Response Ltd v Datastream Media Ltd* [2014] EWCA Civ 281, [2015] QB 41.
[60] Ibid, at [42] per Floyd LJ.

designed to be transferable to third parties. It had permanence and stability. It subsisted over time.[61]

Cryptocurrencies satisfy all these criteria. Each crypto-coin is definable by its own unique transactional history which is discoverable from the blockchain record. The very purpose of the coins is to be transferable to third parties. Even when they are used as investment media they need to be transferable so that their holder can realise their capital value in a conventional state-denominated currency. Once the coins are associated with a new public key, the new holder has the same exclusive power to transact with them as the former holder. They are as permanent and stable in their existence as the software protocol that creates them. Admittedly, the crypto-coins are vulnerable to changes in the system design. One person's ownership of a coin does not confer any absolute veto over changes to the system that might affect the security, the transferability or, ultimately, the very existence of the coin. But that is no different from the ownership of conventional property outside the digital world. Ownership of a thing is not a guarantee against deterioration in or destruction of the thing. An account-holder with money in a bank is the owner of a chose in action but he or she takes the risk that the bank may default on its debt.

Cryptocurrencies are in one way different from the carbon trading allowance in *Armstrong DLW GmbH v Winnington Networks Ltd*. The allowances were created under a statutory scheme: they were transferable exemptions from the fine that the holder would have had to pay for emitting $CO_2$ beyond a permitted level. They were rather like the cases of the export quota, waste management licence and milk quota in earlier cases that considered the meaning of property in criminal law and insolvency law.[62] The difference is that cryptocurrencies are not created under statute so a court has not duty to recognise their existence or their method of operation. But they are at least created by scheme with defined public rules of operation. The rules bind users of the system unless the participants agree to a systemic change.[63]

The issue in *Your Response Ltd v Datastream Business Media Ltd*[64] did not turn on the existence of a third category of personal property. The main issue was whether an IT service-

[61] *Armstrong DLW GmbH v Winnington Networks Ltd* [2012] EWHC 10 (Ch), [2013] Ch 156, at [50].
[62] 000.
[63] See Narayanan et al, supra n 000, ch 7 and for Bitcoin stakeholders a currency community, see ch 000 [Geva] of this volume.
[64] [2014] EWCA Civ 281, [2015] QB 41, considered by K Low, "Perils of Misusing Property Concepts in Contractual Analysis" (2014) 130 LQR 547.

provider could exercise a possessory lien over the client's database of magazine subscribers when the client failed to pay the full fees due under the service contract. The service-provider's arguments tried to extend the traditional common law actions and remedies that depend on possession to the intangible database. The Court of Appeal did not agree. The legal notion of possession could not extend to include the service-provider's control over an intangible thing, such as the database. To have done so would have conflicted with the decision of the House of Lords in *OBG Ltd v Allan* that the tort of conversion would not lie where a person interfered with the performance of a contractual obligation to pay a debt.[65] All that made sense in the case but it was not a reason for saying that there was no intermediate category of intangible personal property. We are left nonetheless with the objections raised by Floyd LJ to treating information as property.[66] There are good reasons for distinguishing his dicta.

The law's general reluctance to treat information as property does not necessarily touch the unique data strings that constitute a crypto-coin. To be sure, information is not an easy object of property. It is hard to exclude the knowledge or use of information from the public at large and confine it to one person. The free flow of ideas is usually in the public interest. It would need some special reason to restrict the use of information by making one person the owner of it. But we have seen how the exclusivity of a crypto-coin stems from a holder's power to transact with it rather than from merely knowing of its existence and from reading the blockchain data that comprise it.[67] The digital information recording the unspent transaction output is understood as something more than the information itself. It is a medium of payment, very like a conventional currency. The whole, seen in terms of its functions, is perhaps greater than the sum of its parts.

The real objection to treating information as property should depend on the functions it is used for rather than on the plain fact that it is information. Information can be used in different ways. Society willing accepts that conventional forms of money can be the objects of property when they are used as means of payment and stores of value. Experience shows the criminal law and private law have no problem about treating coins, banknotes and incorporeal bank balances as property. If so, the reasons for treating crypto-coins differently,

[65] *OBG Ltd v Allan* [2007] UKHL 21; [2008] 1 AC 1.
[66] *Your Response Ltd v Datastream Media Ltd* [2014] EWCA Civ 281; [2015] QB 41, at [42] per Lloyd LJ.
[67] See 000 above.

simply because they consist in information, should not be compelling. If both kinds of asset serve as means of payment and stores of nominal monetary value, then the reasons for treating one as the object of property, but not the other, seem weak.

## Rules of title and transfer

### General

If crypto-coins were indeed recognised as a kind of personal property at common law, then some, but not all, settled rules of property law would apply to them. Owing to their intangibility, some rules would only apply by analogy.

It can at least be said that the lawful holder of a crypto-coin would be the legal owner of it. At common law personal property is either owned or possessed, since the common law theory of estates does not apply to it.[68] The holder's power to transact with the crypto-coins would not amount to possession in the formal legal sense. As we saw, *OBG Ltd v Allan* confirmed that the common law understanding of possession is confined to tangible things with a physical location in space.[69]

As far at the intangible nature of the crypto-coin allowed, the owner could create equitable rights in relation to it. If Alice is the lawful owner of the cryptocoins at $pk_A$, then she could declare a trust of them for Bob or grant a charge over them for Carol to secure payment of a debt. Both these transactions would happen off the blockchain, in the real world. There are well-settled rules of construction to hand that would help resolve uncertainties about the parties' intentions in identifying the specific coins that the trust or charge related to or the precise interest that Bob or Carol were intended to take.[70]

### Derivative transfers of title

*General*

The starting point is that the usual rules of derivative transfer of title would apply to crypto-coin transactions between users of the system. The rules are summed up in the maxim *nemo*

[68] See E McKendrick, *Goode on Commercial Law*, 5th ed, (London, 2016) at paras 2.25-2.27.
[69] See paras 000 above.
[70] Eg, *Hunter v. Moss* [1993] 1 WLR 934 (Colin Rimer QC); [1994] 1 WLR 452 (CA); *White v. Shortall* (2006) 206 Federal Law Reports 254 (SCNSW) (considering the declaration of trust over a fund of fungible property0.

*dat quod non habet.* If Alice pays 5 BTC at $pk_A$ to Bob at $pk_B$, then the starting point is that Bob only gets an indefeasible right of ownership in the coins if Alice was the owner of relevant transactional input and if the transaction was valid in terms of the common law and equitable rules governing derivative transfers of title. Alice can confer no better title on Bob than she has to give, and the transaction between them must be legally effective to vest her title in him.[71] These propositions are laid down as starting point for the way title transfer rules would operate to keep open the argument, considered later, that the special defence of good faith purchase for value may apply to crypto-coins, owing to their functional similarity to conventional state-denominated currencies.[72]

*Legal title and the blockchain record*

Bob's title to coins would not be legally indefeasible simply because the transaction was valid and irreversible according to the operating rules of the Bitcoin system. The general law of property defines a standard of legal validity that is external to the software protocol governing the system. The blockchain may provide a definitive record of the links between discrete transactions on the system, but it cannot be a record of their legal effect. Registration of a transaction is not legally constitutive of the system users' title to the coins associated with their public key. It does not have the same effect, for example, as registering a person as the proprietor of a legal estate in land.[73] Thus the block recording that Alice paid her 5 BTC to Bob does not necessarily make Bob the holder of the coins with an indefeasible title. His title may be defeasible for reasons external to the Bitcoin system. If Bob had wrongfully used Alice's private key to activate the transfer to himself, then his title would be void at law and in equity.[74] If he had procured the transfer to himself by a fraudulent misrepresentation, then he would be the legal owner of the 5 BTC but his title would be voidable.[75] Cyber-currency systems could only opt out of the general rules of property law if all users of the

[71] See generally J Crossley Vaines, *Personal Property*, 5th ed by E L G Tyler and N Palmer (London, 1973), ch 9; D Fox, *Property Rights in Money* (Oxford, 2008), ch 3.
[72] See 000 below.
[73] The contrast is clearly drawn in land registration systems between registration as a system of recording title and registration as a system for constituting title: see generally, K Gray and S F Gray, *Elements of Land Law*, 5th ed (Oxford, 2008), para 2.2.5.
[74] *Clarke v Shee* (1774) 1 Cowp 197 (common law); *Westdeutsche Landesbank Girozentrale v Islington LBC* [1996] AC 669, 715–16 per Lord Browne-Wilkinson (equity). For other cases making the thief a constructive trustee of stolen money, see *Black v Freeman & Co* (1910) 12 CLR 105 and generally J Tarrant, 'The Theft Principle in Private Law' (2006) 80 ALJ 531.
[75] *El Ajou v Dollar Land Holdings plc* [1993] 3 All ER 717, 734 per Millett LJ (rvsed on other grounds [1994] 2 All ER 685 (CA)); *Shalson v Russo* [2003] EWHC 1637 (Ch), [2005] Ch 281.

system agreed to dis-apply them. There would need to be a system-rule to this effect, which users accepted when they made transactions on the system. Only then could the blockchain record be constitutive of a person's title to the coins.[76]

*The blockchain record as presumptive evidence of title*

Ideas analogous to physical possession would have some relevance. When the blockchain records that a certain crypto-coin is associated with a certain public key, it raises an evidential presumption that the holder of the public key is the owner of it. Absent any other indication, it tends to show that the person holding the public key owns the coin associated with it. This is the intangible analogue to the familiar common law presumption that possession is evidence of title.[77] Its main effect is to allocate the burden of proof in a dispute over title. The person who seeks to challenge the current possessor's title to property bears the burden of proving that he or she has a better title to it. If Alice stole a car from Carol and then sold it to Bob, his possession of the car places the burden of proof on Carol in her action for conversion against him. She must prove the identity of the car and the theft of it by Alice.

The presumption of title from possession has been especially relevant to explaining title to money. Until the decision in *Miller v Race* (1758) a person's title to tangible coins was explained by his or her possession of them.[78] Coins were designed and struck to be physically indistinguishable from each other. Money had 'no earmark' and one piece of money was said 'not to be known' from another.[79] If Alice paid coins to Bob, then he was presumed to have the best title to them unless another person, Carol, successfully challenged him. But Carol's challenge was very unlikely to succeed even if she could prove that equivalent coins had been stolen from her by Alice. Since all the coins were physically alike

[76] The analogy here is with the rules governing conventional inter-bank payment systems. The rules are implied into the contracts between the participants in the system.
[77] *The Winkfield* [1902] P 42, 60 per Collins MR. See generally F Pollock and R Wright, *Essay on Possession in the Common Law* (Oxford 1888), 22-25 and L Rostill, "Relativity of Title and Deemed Ownership in English Personal Property Law" (2015) 35 OJLS 31. For the similar rule in Scots common law, see G Bell, *Principles of the Law of Scotland*,7th ed, (Edinburgh, 1870), paras 1313, 1314.
[78] (1758) 1 Burr 452 explained in D Fox, 'Bona fide purchase and the currency of money' [1996] CLJ 54.
[79] Eg, *Whitecomb v Jacob* (1710) 1 Salk 160; *Scott v Surman* (1742) Willes 400, 404 per Lord Willes CJ; Banks v Whetston (1596) Cro Eliz 457*; *Isaack v Clark* (1615) *Bulstrode* 307, 310 per Dodderidge J; 1 *Rolle* 126, 131.

it was practically impossible for her to prove the specific identity of the coins in Bob's possession with those that Carol had stolen from her.[80]

A similar principle would apply to crypto-coins. Although the blockchain record of transactions cannot be legally constitutive of Bob's title to the coins at his public key, it must be the best evidence of it. If Carol seeks to allege that the 5 BTC at Bob's $pk_B$ are the proceeds of a fraud or theft then, if all other things are equal, the burden is on her to prove it by challenging Bob's title. Bob can stand on his presumed title to the coins in any action that Carol may bring to recover the coins or their value from him. The principle is especially relevant, as we shall see, to the resolution of mixtures of crypto-coins and the possibility of tracing them.[81]

*Derivative transfers of title and tracing*

One small gloss needs to be added to what we would understand by a derivative transfer of title to a crypto-coin. The coin is just an ideational construct. It consists in the recorded transaction input that was consumed in the payment and the newly-recorded transaction output that was created by it. The data strings at either side of the transaction are distinct from each other. But they are related by the transactional link between them and by the flow of monetary value that they are understood to represent. Unlike a physical coin that passes as a continuing thing from payer to payee, the object of the cryptocurrency payment is not the same thing on each side of the payment transaction.

Despite this difference, the derivative transfer explanation still holds good for transactions between users of a crypto-currency system. In strict analysis, the object of the payment is traced from one public key to another rather than followed between them.[82] The output at Bob's public key is the traceable product of the input at Alice's public key because the system rules substitute Bob's output for the consumption of Alice's original input. Again we can make an analogy with the way conventional bank payment systems operate. Money transfers between bank accounts work by the simultaneous cancellation (or reduction) of a debt owed by the originator's bank and the creation (or increase) of a debt owed by the beneficiary's bank. The debt owed to the beneficiary at the end of the transaction is a

[80] See D Fox, "*Banks v Whetston* (1596)", ch 1 in S Douglas, R Hickey, E Waring (eds.), *Landmark Cases in Property Law (Oxford*, Hart Publishing, pp 3-24.
[81] 000
[82] See further paras 000-000 below.

different legal entity from the debt that was once owed to the originator.[83] The rules of the payment system define the transactional link between the two debts, which allows the one to be treated as the traceable product of the other.

The rule of derivative transfer of title applies to payments through bank payment systems. If £100 in Alice's bank account derived from a fraud that she had practised on Carol, then she would hold it subject to Carol's proprietary right of rescission. Her title would be defective to that extent.[84] If Alice then transferred the sum to Bob's account, then he would hold it subject to that defect in her title. Carol's right of rescission is enforceable against its traceable proceeds and against a transferee (provided that the transferee has not extinguished the right by receiving the payment as a good faith purchaser for value without notice).

Likewise with a cryptocurrency payment, Bob can take no better title to the transactional output at his public key than Alice had to her input to the same transaction.[85] Conventional rules of tracing would allow any defect in Alice's title to be traced to the output at Bob's public key.[86] Bob's title would not be indefeasible simply because it related to a newly-created transactional output that was distinct from Alice's input that generated it.

*Purchase for value in good faith*[87]

There is an important exception to the general rules of derivative transfer of title which may be relevant to cryptocurrencies. These are the defences of good faith purchase for value. The defences come in an equitable and a legal form.

An equitable title to any kind of personal property is extinguished against the purchaser of the legal ownership of the property if he or she purchases for value and without notice of the competing equitable title.[88] This defence would apply to cryptocurrency transactions. It would not depend whether cryptocurrencies were characterized for legal purposes as a kind

[83] *R v Preddy* [1996] AC 815, discussed at para 000 above.
[84] *Shalson v Russo* [2003] EWHC 1637 (Ch), [2005] Ch 281 (fraudulently induced payment traced through payment system).
[85] For a general comparison between fraud and theft in relation to conventional bank accounts and cryptocurrencies, see K F K Low and E Teo, 'Legal Risks of Owning Cryptocurrencies" in D Lee and R Deng (eds), *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1* (Reed Elsevier, 000, 2017), 225-248.
[86] For examples where an unexercised equity to avoid a transaction was traced through payment systems, see *El Ajou v Dollar Land Holdings plc* [1993] 3 All ER 717, 734 per Millett LJ (rvsed on other grounds [1994] 2 All ER 685 (CA)); and *Shalson v Russo* [2003] EWHC 1637 (Ch), [2005] Ch 281.
[87] See generally in relation to money, ch 000 of this volume [Green chapter].
[88] See generally John McGhee (ed) *Snell's Equity* at [4.017-4.041].

of money. The defence would mean for example that if Alice held her 5 BTC on trust for Carol but transferred them in breach of trust to Bob, then Bob would hold the output of the transaction free of Carol's equitable claim, provided that he was a purchaser for value without notice. The same reasoning would apply if the 5 BTC held by Alice were the proceeds of a fraud she had earlier perpetrated against Carol. Carol's right of proprietary rescission and restitution of the coins would be barred if Bob received them for valuable consideration and without notice of Carol's claim. The valuable consideration for the transfer would have to be found in some real-world transaction between Bob and Alice that was extraneous to the coin transaction recorded on the blockchain. As with most equitable claims enforced against third parties, Carol's recovery against Bob would come down to kind and rigour of the inquiries that Bob was expected to make if he was to assert that he had no notice of her claim. A body of case law on notice has been developed to explain the meaning of notice in conventional money payments by bank transfer. It would need to be adapted to explain how notice would work in a pseudonymous cryptocurrency system. We return to this point later.[89]

Alongside the equitable defence is the less-known common law defence of good faith purchase for value. It applies uniquely to money and, in its codified form, to negotiable instruments such as bills of exchange and promissory notes.[90] Although it is usually thought of as a defence, it is really a rule for the original acquisition of title. The rule creates a fresh, indefeasible legal title in a transferee who receives money in good faith and for value. It makes the recipient immune from the claim of any previous holder who might otherwise have retained a proprietary interest in the money. As a rule of English law, it was first formulated in 1758 to explain the currency of bank notes. It allowed a remote transferee of a stolen bank note to acquire a legal title to it. He could enforce against a bank teller who claimed to hold the note for the original owner from whom it had been stolen. Applied to cryptocurrencies, the rule would mean that if Bob was a good faith purchaser for value of 5 BTC that Alice had stolen from Carol, then he would defeat any proprietary claim by Carol to recover the coins or their traceable proceeds. He would also defeat a restitutionary claim for money had and

[89] See section 000
[90] *Miller v Race* (1758) 1 Burr 452; *Clarke v Shee* (1774) 1 Cowp 197; Bills of Exchange Act 1882, s 29.

received brought by Carol. Since Bob is an indirect recipient of Carol's money, her claim would require her to prove that she had a legal title to the money received by Bob.[91]

Unlike its equitable counterpart, the common law rule of good faith purchase for value would only apply to cryptocurrencies if the common law characterized them as money for the purposes of the rule, and if the parties to transaction chose to treat them as money rather than as an investment commodity bought with a conventional state-denominated currency. Apart from this one case, it matters actually very little to the common law of property whether or not cryptocurrencies are characterized as money. Property and money are not opposite legal categories: all the assets used as means of monetary payment are property of one kind or another. The characterization of some of them as money only affects the kind of property rules that apply to them. If they are money, then the common law rule of good faith purchase for value applies to them and they are exempted from the full force of the rule *nemo dat quod non habet*.

As the authorities now stand, it is uncertain whether cryptocurrencies would be characterized as money in the law of property. The view advanced earlier in this book is that they are not money, at least for the purposes of monetary regulation and the criminal law.[92] Historical experience shows that the application of the common law rule turns on whether a certain asset performs the usual functions of money rather than on the category of asset it belongs to. These functions are generally understood to mean that the asset is used as a medium of exchange, a unit of account, and as a store of nominal monetary value. The decision in *Miller v Race* applied to rule to banknotes because by the middle of the eighteenth century the public at large treated them as functionally equivalent to coins.[93] But Lord Mansfield's central argument that banknotes were treated 'as money, as cash, in the ordinary course and transaction of business, by the general consent of mankind'[94] might become a reason against characterizing cryptocurrencies as money for the purposes of the rule. The number of people who use cryptocurrencies is still relatively small, and the number of cryptocurrency transactions counts as only a small fraction of the payments made with conventional state-denominated currencies. The argument for characterizing crypto-currencies as money would

[91] *Lipkin Gorman v Karpnale Ltd* [1991] 2 AC 548, discussed at 000 below. For restitutionary claims founded on unjust enrichment, see generally S Watterson in ch 000 of this volume.
[92] See chs 000 {Proctor] and 000 [Green] of this volume.
[93] D Fox, "Bona fide purchase and the currency of money" [1996] CLJ 547; and D Fox, *Property Rights in Money*, (Oxford University Press, Oxford, 2008), at [8.10]-[8.13].
[94] (1758) Burr 452, 457.

become stronger if they became more commonly accepted as alternative payment media alongside traditional currencies.[95]

Even so one possible objection would remain. Unlike the bank notes considered in *Miller v Race*, cryptocurrencies are not denominated in a state-authorized unit of account. The understanding shared by users of a cryptocurrency is that each crypto-coin has a nominal value expressed in units special to its own system. Thus a transactional output representing five Bitcoins is valued in terms of Bitcoin units even though it can be exchanged for a real-world currency denominated in state-authorised units of account, such as pounds sterling or US dollars. This limitation may the one remaining stricture of the state theory of money, advanced by the early twentieth-century economist Georg Knapp and adopted by Dr Francis Mann in the early editions of his book on *The Legal Aspect of Money*.[96] In its strongest form, the state theory would have limited the legal definition of money to things issued by a state-sanctioned monetary authority and denominated in its national unit of account.[97] Money would have been confined to assets with legal tender status. The growth of other forms of money, both privately-created or created by central banks, has made the strong form of the state theory too narrow to be practically tenable.[98] But its requirement that money assets be denominated in a legally-sanctioned national unit of account probably remains essential to a common law understanding of money.

Even if a cryptocurrency were eventually characterized as money in some general legal sense, the parties to a transaction would need to treat it as money if the common law rule of good faith purchase were to apply to it. It would need to have been tendered at its nominal value in discharge of a debt or obligation denominated in the units of the currency system. The rule would not apply if the cryptocurrency were bought and sold as an investment, or where it was tendered, not for its own nominal value, but for speculation on its variable capital value against real-world currencies.

This is the effect of *Moss v Hancock*.[99] Hancock owned a five-pound gold coin that had been presented to him as a gift. Like many specially-issued commemorative coins nowadays, five-

[95] See further B Geva and D Geva in ch 000 of this volume.
[96] F A Mann, *The Legal Aspect of Money*, (1st ed, Oxford University Press, Oxford, 1938).
[97] Ibid, at p 7.
[98] A Sáinz de Vicuña, "An Institutional Theory of Money", ch 25 in M Giovanoli and D Devos, *International Monetary and Financial Law: the Global Crisis* (Oxford, 2010).
[99] [1899] 2 QB 111.

pound gold pieces were legal tender although the coin in the case had never been put into circulation. A thief stole the coin and exchanged it at the appellant's shop second-hand jewellery shop for five sovereign coins of £1 each.

The question was whether the shopkeeper was liable to make restitution of the five-pound gold piece to Hancock under criminal legislation for the restoration of stolen property then in force.[100] The shopkeeper's contention was that he was not liable since he had received the coin as a purchaser for value in good faith, so that he had an indefeasible title to it. Darling and Channell JJ in the Divisional Court disagreed with him: the gold piece was the subject of a sale (as a medal might have been) to a dealer in curios, and the fact that it had been exchanged for an equivalent face value in sovereigns did not weigh against this conclusion. The appellant could only have availed himself of the bona fide purchase rule if he had received the coin in payment for goods purchased or in discharge of a debt. The case shows how an asset can switch between monetary and non-monetary status, depending on how the parties to a transaction choose to treat it.

For the time being, therefore, cryptocurrencies denominated in their own currency unit are unlikely to count as money for the purposes of the common law good faith purchase rule, particularly if the parties to a transaction treat them as investment commodities. It may be, however, that that limitation will make little difference to the recovery prospects of person whose crypto-coins have been stolen or taken by fraud. The victim of a theft or fraud usually has concurrent rights of recovery in equity, and they would in any event be barred by the operation of the separate equitable defence of purchase for value without notice.

## Mixture, following and tracing

### Mixtures of cryptocurrencies

A consequence of treating cryptocurrencies as an object of property is that the standard rules of following and tracing would apply to them. They may allow cryptocurrencies to be identified in and traced through mixtures. An example of a mixture would be where a 5 BTC input from a legitimate transaction between Alice and Bob and another 5 BTC input from a fraudulent transaction between Alice and Carol were each identifiable with two outputs

[100] Larceny Act 1861, s 100.

associated with the same public key controlled by Bob. The combined balance of 10 BTC value associated with his pubic key would derive from two distinct transactions. If Bob then paid 5 BTC to David, the question would be whether the output at David's public key derived from the legitimate Alice-Bob transaction or the fraudulent Carol-Alice transaction or in some proportion between the two.

Some modifications to the standard tracing rules may be needed to allow analytical differences between cryptocurrencies and conventional state-denominated currencies issued in the form of bank notes, coins and incorporeal bank balances. But if tracing is successful, it may provide the evidential foundation for an equitable proprietary claim against the real-world holder of a public key. Bob (or David) may find himself liable to restore 5 BTC to Carol as the proceeds of the fraud perpetrated on her by Alice. Significantly, if Bob (or David) were insolvent the specific traceability of Carol's coins might exempt them from the definition of the defendant's bankrupt estate so that Carol could recover them in priority to his general creditors. Tracing may also support a personal claim for restitution through an equitable action for knowing receipt.[101]

*Mixing in practice*

Obviously, the actual mixing of crypto-coins is more complex than the simple example just given. [102] Users of cryptocurrencies may deliberately mix their coins to frustrate the proof of transactional links between payments or to obscure their real-world identity. Dishonest users resort to some distinctive payment techniques. They split large amounts of stolen coins between multiple public keys. A sophisticated version of splitting involves setting up "peeling chains" where small amounts are peeled off large holdings held at a single public key. The peeled chains are then re-combined, and the peeling process repeated.

Mix services and shared wallet services obscure the connection between input and outputs in payment transactions. The aim is not necessarily dishonest. Suppose that Alice wishes to

[101] See 000 below.

[102] For surveys, see S Meiklejohn et al, "A Fistful of Bitcoins: Characterizing Payments among Men with No Names" (December 2013) University of California <http://cseweb.ucsd.edu/~smeiklejohn/>; M Möser, "Anonymity of Bitcoin Transactions" (Münster Bitcoin Conference, July 2013), 2.1-2.3; J Bonneau et al, "Mixcoin: Anonymity for Bitcoin with Accountable Mixes" in N Christin and R Safavi-Naini, *Financial Cryptography and Data Security FC 2014* (Heidelberg, Springer, 2014); Narayan et al, n 000 above, at pp 151-59.

pay 5 BTC to Bob without disclosing her public key.[103] Alice transfers her coins to one of many designated public keys controlled by a mixer service. If the service provider has enough clients, it will receive payments from many different users, with each payment going to one of its many keys. It then pays 5 BTC to Bob, using coins from another public key and paid in by a different client. This breaks the specific transactional connection between the initial input at Alice's public key and the output at B's.[104]

Wallet service providers may routinely make payments in this way on their clients' behalf. The system requires the service provider to keep records to match inputs with outputs. Alice's anonymity in the process is only secure so long as the provider destroys the records after each transaction, which it usually undertakes to do. If the inputs and outputs were in the same amount, then it would generally be possible to identify one as the proceeds of the other. Users of shared wallets are therefore encouraged to divide their inputs into a number of smaller output units.

Some mixer services deliberately operate to obscure the transactional history of stolen coins. Despite their name so-called "coin laundries" do nothing to clear the taint of illegality carried on the coins and their proceeds. They merely make proof of the coins' unlawful origins very difficult indeed for law enforcement agencies or honest users of the system. They exploit to an extreme the legal rule the burden of proving a competing title to money lies on the person who wants to challenge the title of the person currently in control of it.[105]

Blockchain transactions are not entirely anonymous. Blockchain cluster analysis can ascertain the probability that a certain public key is associated with an identified person in the real world.[106] When inputs at distinct public keys are consumed to make a single output or when the change from a transaction is paid to a new public key, it can be shown that the public keys are controlled by the same person. Combined with test purchases made to known public keys, it is possible to identify the real-world organisation that controls them. The clustering of coins known to be stolen at certain public keys might taint all coins associated with the same key with doubts about the lawfulness of how key-holder obtained them. This

[103] See Möser, n 000 above.
[104] In principle, the private law rules of tracing would allow the output at Bob's public key to be identified as the proceeds of the input at Alice's public key. The terms of the mix service contract would allow the one to be attributed to the other. See further para 000 below.
[105] See paras 000 above [title from possession].
[106] See Sarah Meiklejohn et al, "A Fistful of Bitcoins: Characterizing Payments among Men with No Names" (December 2013) University of California <http://cseweb.ucsd.edu/~smeiklejohn/>.

has a direct bearing on taint analysis of the blockchain and the meaning of constructive notice applied to cryptocurrency transactions.[107]

**Tracing and cryptocurrencies**

Three general points run through this whole account of tracing and cryptocurrencies.

*Cryptocurrencies are traced not followed*

The identification of cryptocurrencies in payments and mixtures would strictly be an exercise in tracing rather than following. The distinction was explained by Lord Millett in *Foskett v McKeown*: 'Following is the process of following the same asset as it moves from hand to hand. Tracing is a process of identifying a new asset as the substitute for the old.'[108] Crypto-coins are data strings recording the inputs and outputs of identifiable transactions on the blockchain. As we saw, the input data string does not pass from one public key to another.[109] It is instead consumed in the transaction and replaced by a new output at the payee's public key. The output data string is the substitute for the original data string that was used as the input to the transaction. Strictly, the two data strings are distinct assets. It is only the BTC value associated with the input that is traced into the output. To this extent, the process is the same as tracing value through a payment of incorporeal bank balances.

*The blockchain and traceability*

The unique transactional history recorded in some crypto-coins, such as Bitcoins, may mean that it can never be mixed in an absolute sense. So long as the transactional history of the data representing the coin (or a fractional part of it) is verifiable on the system, then it may never completely lose its distinguishing identity. It is different from an ordinary coin or banknote which carries none of its transactional history with it as it passes from hand to hand. Following a coin or a banknote requires the claimant to prove its transactional history by extrinsic evidence or by relying on the artificial rules of identification developed by the courts.

[107] See para 000 below.
[108] *Foskett v McKeown* [2001] 1 AC 102, 127 per Lord Millett.
[109] See paras 000-000 above.

But the theoretical traceability of crypto-coins should not make the victims of cyber-theft or cyber-fraud unduly optimistic about the prospects of recovering their property. The unscrambling of a mixture always depends on the sophistication of the identification processes at hand and a choice about the artificial identification rules that the courts apply to the mixture. As we have seen, the splitting, peeling and mix services that have been developed to make Bitcoins fully fungible in their exchange value are designed to make the specific traceabilty of Bitcoin value very difficult indeed.[110]

*Pseudonymity and tracing*

The final point relates to pseudonymity. Even if the transactional history of a crypto-coin is traceable, evidence extrinsic to the blockchain would be needed to identify the people in the real world who control the public keys recorded on it. Unlike the tracing of traditional currencies, the challenge may be less in plotting the passage of the money from its source to its destination than in identifying the people behind each stage of the process. This goes beyond saying that the victim of a cyber-theft or cyber-fraud needs to find a real person to sue, rather than just their public key. The artificial rules of identification developed by the courts depend on the fault or innocence of the person handling the money.[111] The identity of the person behind the public key may therefore be relevant to deciding which tracing rule a court should apply.

**Attribution in cryptocurrency transactions**

*Attribution by the blockchain record or by an external transaction*

We begin with the simple case outlined earlier:[112] Alice defrauds Carol of 5 BTC at her public key, $pk_C$, and pays it to a newly-created public key, $pk_A$, that has no other transaction outputs associated with it. She then transfers the sum from $pk_A$ to Bob at $pk_B$. Provided that the usual pre-conditions to tracing are satisfied,[113] Carol could trace the value of her original 5 BTC into the transactional output now at $pk_B$. They are linked by two transactions on the

[110] See paras 000-000 above.
[111] Eg, *Re Hallett's Estate* (1880) 13 Ch D 696, 727-28 per Jessel MR; *Re Diplock* [1948] Ch 465, 525-26 per curiam; See generally L D Smith, *Law of Tracing* (Oxford, 1997) 85-88; 177-81.
[112] See paras 000 above.
[113] The original asset must have been held on a fiduciary relationship or the transaction between the claimant and the first transferee must have generated a distinct equitable title to the asset. The logic of requirements has been widely criticized but they have not yet been overruled: *Foskett v McKeown* [2001] 1 AC 102, 128-29 per Lord Millett.

system ($pk_C$ - $pk_A$ and $pk_A$ - $pk_B$), each of which is consists in the corresponding consumption and creation of inputs and outputs. There is no need to look to any evidence extraneous to the blockchain to prove that the parties would have intended the outputs to be attributable to the inputs. The attribution link is inherent in the operation of the system, and the parties must be taken to have understood this.

It may be, however, the parties were using the payments recorded on the blockchain to carry out some external transaction between themselves in the real world. For example, Alice might have been buying goods from Bob and the 5 BTC represented the purchase price due to him. If so, Carol would have to elect between two possibilities for tracing. She could either trace into the 5 BTC payment received by Bob or into the goods received by Alice in return. Tracing into the goods might seem the better option since very likely Bob would have received the 5 BTC as purchaser for value without notice. Any equitable title that Carol might otherwise have asserted against him or the 5 BTC output at $pk_B$ would have been extinguished. But tracing into the goods now in Alice's hands would require Carol to rely evidence external to the blockchain. She would need to know that there was a sale between Alice and Bob which identified the goods as the consideration given in return for her money. Alice and Bob's intentions expressed in the real-world transaction between them would define the goods as the traceable product attributable to the coins.

**Tracing through mixtures**

*Balances and transactional outputs*

Suppose next that Bob already has 5 BTC associated with his public key, $pk_B$, before the 5 BTC from Alice is paid to it. There would then be a net balance of 10 BTC units of value. But each transactional output generating the balance would be separately recorded on the blockchain since, as we saw earlier, the blockchain maintains a transaction ledger rather than an account ledger. While the value derived from the two sources may be mixed, the data strings that embody them remain distinct. Each keeps its unique transactional history just as it would if it had been the only transaction output associated with the public key.

The distinction between transactional outputs at the same public key is important to our analysis of the next transaction from the same public key. We suppose now that Bob pays 5 BTC from $pk_B$ to David at $pk_D$. The question is whether he uses the 5 BTC derived from Carol or the 5 BTC derived from Alice as the input. The answer may not be provided by the

system itself. Provided that there was an unspent balance of 5 BTC at $pk_B$, the system would validate the transaction to David. The consumption of one coin or the other would arbitrarily determined by the system. Unlike the simpler transaction where Alice drew on an "unmixed" balance at $pk_A$ to pay Bob, the system rules could not resolve the legal problem of how to attribute the output at $pk_D$ to a specific previous input. An evidential impasse would have been reached which could only resolved by resorting to artificial presumptions.

**Cryptographic and legal rules for tracing through mixtures**

Cryptographers have proposed three possible ways out of the impasse: 'poison', 'haircut' and 'first in first out'.[114] The cryptographers' concern is slightly different from the one here, which is to prove a specific tracing link with a view to asserting a property right over a certain transactional output. Their concern is to find a formula for determining which coins in the system are clean and which are 'tainted' because they derive in some way from criminal activity. Coin exchanges try to maintain the integrity of the system by only selling clean coins to their customers. They use blockchain analysis techniques to test the origins of the coins they sell.[115]

*The poison approach: a punitive causation rule*

The poison approach takes the most extreme approach to tainting. Any output that derives from a criminal transaction is treated as 100% tainted by it. On that approach, the 5 BTC remaining at Bob's $pk_B$ would be completely tainted, as would the 5 BTC at David's $pk_D$. The result of the poison approach is that the taint spreads ever-wider, infecting more and more coins as transactions with them extend and spread.

The poison approach to taint analysis would not be the right starting point for rules of attribution in private law tracing. It works by a punitive theory of causation rather than a theory of exchange attribution, which was the rationale of tracing explained in *Foskett v McKeown*.[116] In the end the private law rules are concerned with identifying a specific asset which is the object of a property right. They are not concerned with penalizing people because their money derives in a loose causal sense from criminal wrongdoing.

[114] The explanation in this section draws heavily on R Anderson et al, 'Bitcoin Redux' (2018) at http://www.cl.cam.ac.uk/~rja14/ (accessed 23 July 2018).
[115] See further paras 000-000 below.
[116] [2001] 1 AC 102, 137 per Lord Millett.

*The haircut approach: proportionate division*

The haircut approach works by determining proportionate shares. Outputs are tainted in proportion that the coins at the payer's public key were tainted. In our example of the Bob-David transaction, the remaining 5 BTC at Bob's $pk_B$ would be deemed 50% tainted, as would the 50% at David's $pk_D$. The approach has an intuitive appeal: the unspent transaction outputs at each public key are treated as a mixture of fungible value, which passes to each new output of a transaction. The haircut approach is the default method of taint analysis used by blockchain analysts. The taint spreads with every new transaction but, unlike the poison analysis, it divides the BTC value of the taint into ever-smaller amounts. The proportion of the taint diminishes as outputs are mixed again. Eventually, the proportion of a taint associated with outputs at a public key becomes too small to be easily discovered.

The haircut approach has a strong analogy in the private law rules of tracing. Proportionate sharing is the default approach taken at common law and in equity when fungible property is mixed or where an asset is bought with mixed money. In *Indian Oil Corporation Ltd v Greenstone Shipping SA (Panama)*[117] oil belonging to different parties was mixed. They held it as owners in common in proportion to their actual ascertained contributions. In *Foskett v McKeown* a trustee wrongfully paid £40,000 trust money to himself and used it to pay two of the five annual premiums on a life insurance policy. The trust beneficiaries were awarded a 40% proportionate share in policy proceeds when the trustee died. The trend of recent cases on tracing payments through current bank accounts has also been to allocate any remaining balance in the account in proportion to the credits of individual trust claimants' money. If, for example, Carol wrongfully mixed £100 money from the Alice trust with £100 belonging to the Carol trust, and then withdrew £100 from the account, the remaining balance and the withdrawal would be attributed in half shares between Alice and Bob.[118] When applied to a current bank account, the proportionate allocation approach has the virtues of relative simplicity and analytical accuracy. When there are many transactions in the account, it is easier to take a proportionate approach to division than to match specific debits and credits. It is also consistent with the modern analysis of a current bank account. The account consists

[117] [1987] QB 345.
[118] Eg, *Barlow Clowes International Ltd (in liq) v Vaughan* [1992] 4 All ER 22; *Re French Caledonia Travel* (2004) 22 ACLC 498. See also *Russell-Cooke Trust Co.* v *Prentis* [2002] EWHC 2227 (Ch), [2003] All ER 478.

in a debt for a single net balance rather than a series of individuated debts, each of which is created by a specific deposit.[119]

*The first in first out approach:* Clayton's Case

Applying the first in first out approach to a blockchain transaction means that the earliest unspent transactional outputs associated with a key (in this sense, 'first in') are deemed to be the first consumed as inputs to the next transaction (in this sense, 'first out'). The rule is relatively easy to apply because every transaction is time-stamped. In our example of the Bob-David transaction, the 5 BTC transferred to David would be deemed to consume the earlier 5 BTC unspent transactional output attributable to Bob. The 5 BTC remaining at Bob's $pk_B$ would represent the proceeds of Carol's original money. The advantage of the first in first out approach is that it tends to concentrate the taint in fewer but larger transactional outputs. Unlike the haircut approach, the taint is not spread ever more widely and thinly across transactions.

The cryptographers' first in first out approach also an analogy in private law: the rule in *Clayton's Case*.[120] Traditionally, *Clayton's Case* was used as the default method of allocating mixed funds in a current bank account which were attributable to two or more contributors (unless the fault of one of them justified favouring the other contributor with a more advantageous identification rule that tended to preserve his or her contribution to the mixture).[121] Withdrawals from the account are treated as consuming credits to the account in the order that they were made in. The rule in *Clayton's Case* has fallen out of favour in recent tracing cases. It is difficult and expensive to apply to complex mixtures with many contributors.[122]

More significantly, its use in bank money tracing cases rests on an illogical foundation.[123] The rule was originally devised to allow the appropriation of debits to credits between the holder of a bank account and the bank. It rested on the theory that a bank account was a

[119] *N Joachimson v Swiss Bank Corporation* [1921] 3 KB 110. For the historical evolution of the notion of a bank account as a debt, see *Re French Caledonia Travel Ltd* [2003] NSWSC 1008, (2003) 48 ACSR 97, at [48]–[55] per Campbell J.
[120] *Devaynes v Noble, Clayton's Case* (1816) 1 Mer 767, 572.
[121] See further paras 000-000 below.
[122] *Barlow Clowes International Ltd (in liq) v Vaughan* [1992] 4 All ER 22; *Commerzbank AG v IMB Morgan Plc* [2004] EWHC 2771 (Ch); [2005] 2 All ER (Comm) 564.
[123] DA McConville, "Tracing and the Rule in Clayton's Case*"* (1963) 79 LQR 388; L D Smith, *Law of Tracing* (Oxford, 1997), 183-94.

series of debts, each created by a single deposit and then reduced or cancelled as withdrawals were made against it. That is no longer the modern analysis: the current balance on the account stands as single and undivided debt without regard to the several items which as a matter of history contribute to that balance.[124] The rule was never intended to be used for apportioning the balance due to the holder of a bank account between two or more third party claimants whose money had been paid into the account.[125]

Nonetheless the first in first out rule in *Clayton's Case* may still be appropriate starting point for tracing cryptocurrency payments through a mixture at a public key. The transactional record on the blockchain corresponds more closely to the series of individuated debts that the rule in *Clayton's Case* was originally developed for. Each unspent transactional output at the public key retains its distinct transactional history. Outputs are not combined to generate a new entity equal to the total unspent balance at the key. The first in first out approach may work more naturally on a transactional ledger than it would on the account-based ledger-system used for conventional bank money. It has been described as "deterministic and, at least in principle, straightforward."[126]

First in first out would therefore be the appropriate tracing rule to apply where the money of two or more innocent claimants was mixed at a single public key. In our example of the Bob-David transaction,[127] the 5 BTC transferred to David would be treated as a payment of Bob's own money. The 5 BTC remaining at Bob's $pk_B$ would represent the proceeds of Carol's original money. If Bob then made a second payment of 5 BTC to Erica at $pk_E$, Carol would trace to the unspent output at $pk_E$.

*Variations from* Clayton's Case

The first in first out rule of appropriate would only be a starting point for tracing flows of BTC value through transactions. The legal tracing rules are artificial presumptions designed

[124] RM Goode, *Payment Obligations in Commercial and Financial Transactions* (London, 1983), 12–13; S McCracken, *Banker's Remedy of Set-Off* (2nd edn, London, 1998), 24; and *Re Footman Bower & Co Ltd* [1961] 1 Ch 443, 450 per Buckley J. The pivotal decision was *N Joachimson v Swiss Bank Corporation* [1921] 3 KB 110.
[125] See *Re French Caledonia Travel Ltd* [2003] NSWSC 1008, (2003) 48 ACSR 97, at [48]–[55] per Campbell J, and D Fox, *Property Rights in Money* (Oxford, 2008), paras 1.46-1.51.
[126] R Anderson et al, 'Bitcoin Redux' (2018) at http://www.cl.cam.ac.uk/~rja14/ (accessed 23 July 2018).
[127] See para 000 above.

to resolve evidential uncertainty. They could be displaced if the parties to the transaction had a different intention or if one of the parties who created the mixture was at fault.[128]

Even if the two contributors to the mixture were innocent of any wrongdoing to the other, the rule in *Claytons' Case* could sometimes be displaced, as it would in mixture of conventional bank money. The mixed fund of value remaining at the public key and the outputs of any further transactions from it would be divided proportionately between the contributors regardless of the sequence of transactions associated with the public key. The examples given in the cases are where the claimants were victims of a common fraud in a shared investment scheme. The understanding that they would share the risks and returns investment proportionately between them would extend to the risks of fraudulent appropriation of their funds.[129] In the end, the proceeds of their value would be traced and recovered on the on the haircut or proportionate share approach.

More commonly, however, the rule would be displaced where the holder of the public key was guilty of some wrong against the claimant.[130] Wrongdoing usually consists in some fraud or breach of fiduciary duty committed against the claimant, or in receiving funds with notice of their tainted origins. The holder could not rely on his or her own wrong to take advantage of the evidential uncertainty created by the mixture. Let us return to the example where Alice defrauds Carol of 5 BTC and procures a transfer of them to herself at $pk_A$. Alice then transfers 5 BTC to Bob at $pk_B$ who then transfers an additional 5 BTC to the same public key. Suppose also that Bob receives the 5 BTC from Alice with notice of her fraud. Even if he then pays 5 BTC to David, Carol could treat the remaining 5 BTC unspent output at $pk_B$ as the traceable proceeds of her money. Since Bob is a wrongdoer, the actual order of transactional outputs would be displaced when Carol traced against him. It would be irrelevant that the system rules would demonstrate a prima facie transactional link between Carol's money and the first output at Bob's public key. Bob's fault would displace the operation of the first in first out rule. The legal rules of tracing would supplant the system rules recording transactional links on the blockchain.

[128] See generally L D Smith, *Law of Tracing* (Oxford, 1997), 77-89, 195-206.
[129] *Barlow Clowes International Ltd (in liq) v Vaughan* [1992] 4 All ER 22, 31 per Dillon LJ, 41 per Woolf LJ; *Russell-Cooke Trust Co v Prentis* [2002] EWHC 2227 (Ch); [2003] All ER 478; *Ontario Securities Commission and Greymac Credit Corp* (1985) 55 OR (2d) 673. For a similar approach to distributing the unspent residue of a public appeal, see *Re British Red Cross Balkan Fund* [1914] 2 Ch 419.
[130] The leading examples involving conventional bank money are *Re Hallett's Estate* (1880) 13 Ch D 696; *Re Oatway* [1903] 2 Ch 356.

Attributing fault to one of the parties requires the claimant to rely on evidence extraneous to the blockchain record. It requires at the very least that the claimant can identify the real-world identity of a person who controls the public key. It would therefore be vulnerable to the special evidential difficulties of tracing in a pseudonymous and decentralised system.

**Notice in cryptocurrency payments**

The equitable doctrine of notice would be relevant to cryptocurrency payments in two main ways. It would determine whether transferee of crypto-coins took them as a purchaser for value without notice of any equitable claim affecting them.[131] It would determine also whether the transferee took them as a wrongdoer for the purposes of the special rules of tracing.[132]

The meaning of notice in payments of conventional bank money is now reasonably settled. Notice can be either actual or constructive.[133] Since most cryptocurrency payments happen pseudonymously, it would be rare that a recipient would directly know enough about the origins of a coin or the real-world identity of a payer to have actual notice that derived from a fraud. A recipient might have actual notice if the fraud had been well publicised the public key from the payment came was notorious for unlawful activity. In practice, if notice was to figure at all, it would be constructive notice that mattered. The test supposes that the recipient is fixed with notice of facts that it would have discovered if it had made reasonable inquiries. The due level of inquiry is defined by the norms commonly accepted as usual and proper in the kind of transaction in question. Notice resolves itself into a mixed question of 'industry practice' and the commercial propriety of taking risks in relation to unknown third party interests.[134] The recipient can start with the assumption that it is dealing with honest people.[135] But it must make inquiries if there is a 'serious possibility' a third party has a proprietary right to the money received or if the facts known to it would give a reasonable person serious cause to question the propriety of the transaction.[136] If this much is known to

[131] See paras 000.
[132] See paras 000.
[133] *Barclays Bank plc v O'Brien* [1994] 1 AC 180, 195-196, per Lord Browne-Wilkinson.
[134] *Sinclair Investments (UK) Ltd v Versailles Trade Finance Ltd (In Administration)* [2011] EWCA Civ 347; [2012] Ch. 453; *Papadimitriou v Crédit Agricole Corpn and Investment Bank* [2015] UKPC 13, [2015] 1 WLR 4265.
[135] *Macmillan Inc v Bishopsgate Investment Trust Plc (No.3)* [1995] 1 W.L.R. 978, 1014 per Millett J.
[136] *Papadimitriou v Crédit Agricole Corpn and Investment Bank* [2015] UKPC 13, [2015] 1 WLR 4265 at [20] per Lord Clark JSC.

the recipient, it is fixed with constructive notice of an interest if it made a considered choice to look no further.

The test used in bank payment transactions supposes that the recipient has some knowledge of the real-world identity of transferor and the kind of transactions from which the money derives. Bank transactions operate between account holders whose identity can at least be verified against standard KYC checks. In a cryptocurrency transaction, however, none of that information is likely to be known, or at least known with any great probability. The recipient's knowledge of the provenance of coins would have to be gathered from its analysis of the blockchain record or from published analyses of tainted coin transactions.[137] As we saw, there is no consensus yet among about the proper approach to identifying tainted coins,[138] and taint-tracking services may differ in the identified probabilities of risk associated with suspected coins.[139] The poison and haircut approaches to taint analysis may report a greater degree of tainting than is consistent with the rules of tracing applied in private law.

We might imagine that an industry practice would develop that a certain published record of blockchain tainting was regarded as a standard for testing coin transactions. A failure to consult the record might amount to constructive notice of any adverse risk disclosed by it. Eventually, industry norms may emerge among coin exchanges that hold themselves out as the leading or responsible players in the market. Even so, a tension is unavoidable between traditional court-enforced standards of notice and the aims of cryptocurrency designers and users. The courts' approach to risk-taking in conventional payment transactions has been informed by standards of commercial ethics, which requires a recipient to have some regard to the risk that he or she is handling money that may belong to another.[140] The designers of cryptocurrency technology, however, are aiming to develop complete anonymity and fungibility in payments, so as to reduce transaction costs.[141] The price of that development is the elimination of adverse legal titles that might otherwise have been recognised in the

[137] Eg, the http://www.cl.cam.ac.uk/~is410/taintchain/ (accessed 24 July 2018).
[138] See para 000 above.
[139] See R Anderson et al, n 000 above, section 3.4.
[140] Compare the approach to dishonest risk-taking in claims for dishonest assistance in breach of trust: *Royal Brunei Airlines Sdn Bhd v Tan* [1995] AC 378, 389-90 per Lord Nicholls; and *Cowan de Groot Properties v Eagle Trust* [1992] 4 All E.R. 700, 707 per Knox J.
[141] One of the systemic aims of Bitcoin protocol was to eliminate the cost of mediating disputes between users: see S Nakamoto, "Bitcoin: a Peer-to-Peer Electronic Cash System' p 1, https://Bitcoin.org/en/Bitcoin-paper (accessed 21 July 2018). For the attempts to develop powerful forms of anonymity by the Zerocash and Zerocoin system, see A Narayanan et al, supra n 000, 159-67.

victims of fraud. The development favours an extreme form of security of transaction over security of interest, achieved by technical design rather than by legal rules.[142] In the end, general law tests of constructive notice can only be as good at protecting security of a defrauded owner's interest as the kinds of technology they are applied to.

## Remedies

The recognition of property in cryptocurrencies is pointless unless private law also supplies effective remedies to enforce the claimant's interest. Titles to cryptocurrencies would in fact lend themselves well to enforcement by some kinds of non-possessory remedies at common law and in equity.

*Tort actions*

Since crypto-coins are intangible, a legal title to them could not be directly enforced by a tort action for wrongful interference with goods. Actions in conversion or trespass, which are usual means of enforcing legal titles to personal property, would not be available. This follows, as we saw, from the decision in *OBG Ltd v Allen*[143] which confined the possessory torts to their traditional domain in protecting titles to corporeal property capable of physical possession.[144] That limitation would not apply to a restitutionary action for money had and received aimed at the direct enforcement of the claimant's legal title in the crypto-coins. It would not rest on any theory of tortious interference with possession.[145] A different stumbling block might be instead that the restitutionary action would require recognition that the coins were money. The view proposed earlier in this chapter is that they are not.[146]

Some indirect protection through the possessory torts action would be possible. The actions would be available to protect wrongful conversion of computer hardware or a written document that recorded a user's private key. Where the defendant's interference was directed at using the crypto-coins accessed by the private key, the claimant's damages should include

[142] The distinction is a classic theme in the literature on commercial law: eg, M Franklin, 'Security of Acquisition and Transaction' (1931) 6 Tul LR 589; L Ellis, 'The Transfer of Moveables by a Non-Owner' (1980) 55 Tul LR 145.
[143] *OBG Ltd v Allan* [2007] UKHL 21; [2008] 1 AC 1.
[144] See paras 000 above.
[145] *Lipkin Gorman v Karpnale Ltd.* [1991] 2 AC 548.
[146] See para 000 above. For the place of cryptocurrencies in the law unjust enrichment, see ch 000 [Watterson].

the market value of the crypto-coins, at least in cases where the conversion was permanent.[147] The same would be true if defendant detained the hardware or record only temporarily but in the meanwhile used the private key to spend the crypto-coins.[148]

*Equitable remedies*

A claimant's best prospects for proprietary protection of title would be in equity. An equitable title enforced through a constructive or resulting trust or through an equitable lien does not require the object of the claimant's interest to be corporeal. Indeed, in many of the leading cases, the claimant has enforced a title against a fund of incorporeal bank money.[149] A personal remedy to recover the value of cryptocurrency would also lie through an action for knowing receipt.[150] It would not matter whether the cryptocurrency was characterised money or as a commodity. In *Re Montague's ST* Megarry V-C assumed that the action would in principle lie even when the defendant received personal chattels.[151] The claimant would need to prove that the defendant received the crypto-coins with some unconscionable knowledge of the claimant's interest, which would bring into play some of the factual inquiries needed to prove constructive notice of it.[152]

A cryptocurrency user who was the victim of a theft or fraud might not in fact be limited in his or her prospects of recovery by the need to found on an equitable, rather than a legal, title. The trend of recent authorities has been to recognise concurrent equitable titles to trace and recover misapplied money.[153] The claimant is not left to rely on a retained or re-vested legal title, which would have been vulnerable to the old rule that the common law cannot follow or trace money through a mixture.

---

[147] *BBMB Finance Ltd v Eda Holdings Ltd* [1990] 1 WLR 409. On the distinction between permanent and temporary conversions, see generally A Hudson, "Money claims for misuse of chattels", ch 33 in N Palmer and E McKendrick (eds), *Interests in Goods*, 2nd ed., (London, 1998).
[148] cf *Sollaway v McLoughlin* [1938] AC 247; *IBL v Ltd v Coussens* [1991] 2 All ER 133.
[149] *Re Hallett's Estate* (1880) 13 Ch D 696; *Foskett v McKeown* [2001] 1 AC 102.
[150] *BCCI (Overseas) Ltd v Akindele* [2001] Ch 437.
[151] *Re Montague's ST* [1987] Ch 264.
[152] See para 000 above.
[153] A thief is said to hold stolen property on a constructive trust: *Westdeutsche Landesbank Girozentrale v Islington LBC* [1996] AC 669, 715–16 per Lord Browne-Wilkinson. The victim of a fraudulent misrepresentation can rely on an equitable title to proprietary rescission which leads to the recognition of a resulting trust: eg, *El Ajou v Dollar Land Holdings plc* [1993] 3 All ER 717, 734 per Millett LJ (rvsed on other grounds [1994] 2 All ER 685 (CA)); *Shalson v Russo* [2003] EWHC 1637 (Ch), [2005] Ch 281, 000 per Rimer J.

## Conclusion

Fitting cryptocurrencies into the common law of property may not be an easy task but it is not impossible. Once the data comprising crypto-coins are understood for what they are, they should be a suitable object of property at common law and in equity. The old binary conception of personal property consisting in choses in possession and choses in action should not be an obstacle, if indeed it ever was. With some necessary adaptation to allow for the intangibility of crypto-coins, the usual rules of derivative transfer of title and tracing could apply to them.

Granted, the common law has no ready-made rules especially designed for cryptocurrencies. But that very absence of rules may be as much an adaptive strength as a systemic failing. The common law grows by a process of principled analogy between the old and the new. Incremental responses to practical innovation have been the driver of all common law development. It has rarely been left with no answer at all. The common law can therefore provide a default set of property principles to govern cryptocurrency transactions. Statutory intervention is not essential.