

Crypto-currencies and insolvency¹

*This lecture is dedicated to the memory of Gabriel Moss QC,
in honour of his outstanding contribution to the development
of English insolvency law*

1. There is a moment, in Douglas Adams' Hitchhikers guide to the galaxy when a spaceship carrying a motley crew of management consultants, account executives and telephone sanitizers crash lands on Earth 2 million years ago. One day they decide upon adopting the leaf as legal tender and are immensely satisfied as they become enormously rich, overnight. But pretty soon, as summer turned to autumn, they ran into a small inflation problem, due to the unexpectedly high level of leaf availability. So, to obviate the problem, and effectively revalue the leaf, they embarked on a massive defoliation campaign, and burned down all the forests.
2. This, written long before the invention, even, of the internet, neatly encapsulates one of the problems facing legal tender as it strays further from fiat currencies. Crypto-currencies create many more prompting Nouriel Roubini to describe bitcoin, to the US Senate last year, as the "mother of all scams". This evening, I am going to focus on one particular set of problems: how crypto-currencies are to be treated in the insolvency of one or other of the players involved in transactions.
3. Crypto-currencies, sometimes referred to as virtual or digital currencies, exist in many forms, employing a wide range of different technologies. No, one, definition is possible. In broad terms, however – and so as to distinguish them from other forms of crypto-asset – I intend to refer to an asset which exists in digital form and is designed to act as a medium of exchange.
4. Even within this broad definition, wide variations exist. At one extreme, there are electronic tokens issued within a closed system, such as "Linden Dollars" in the online game "second life", where the rules governing their use and exchange are laid down by the game's creator, and signed up to by those who join. These tokens may be exchanged for services and products within the game. Sometimes – as with Linden Dollars themselves – they may be exchanged outside of the game for 'real' currencies. At the other extreme, are intangible, de-centralised systems, having no terms or conditions, using distributed ledger technology and ruled by consensus rather than a central operator. The first, and the paradigm example, is bitcoin. I will use it as the basis for much of this talk.
5. At the heart of legal uncertainties around crypto-assets generally is the question whether they are a form of property recognised by English law, or something else. That is an issue which, while capable of a straightforward yes or no answer at a relatively high level of generality, raises many more subtle questions when placed into a particular context. In the context of insolvency, it raises at least the following three issues, which I will address in this talk.

¹ Lecture delivered by Mr Justice Zacaroli to the Insolvency Lawyers' Association on 17 October 2019.

6. First, if the bankrupt or insolvent company holds crypto-currencies at the point of insolvency, are they ‘property’ within the meaning of s.436(1) of the Insolvency Act 1986, so as to fall within the insolvency estate?
7. Second, is a claim to crypto-currencies within the control of an entity (such as a broker or intermediary) that becomes insolvent, a claim to recover property, or a personal claim?
8. Third, if it is a personal claim, is it to be characterised as a claim to recover money, but in a different currency, or as a claim for loss arising from the failure to deliver an asset?
9. The question whether crypto-assets qualify, generally, as items of property under the common law is the subject of important recent work by the UK Jurisdiction Taskforce, under the chairmanship of the Chancellor of the High Court. It is due, imminently, to publish a “Legal Statement” on the legal status of crypto-assets and smart contracts. It is written by senior lawyers expert in the field, with the benefit of wide consultation with and feedback from other expert practitioners, academics and technicians. Its purpose is to seek to provide clarity around their status within existing principles of the common law with a view to removing potential impediments to their development. So far as crypto-assets are concerned, the central question it sets out to answer is whether the English common law contains sufficient tools and flexibility to recognise them as a form of property. I do not propose to travel that same ground, other than to note that a number of commentators have supported the proposition that even though (as I will explain) crypto-assets do not fit within the established categories of property under English law, they should be recognised as such at common law.
10. Whether or not they fall into established categories of proprietary right, however, it might be thought, in respect of the first specific question I am concerned with (whether crypto-currencies are property within the meaning of s.436 of the Insolvency Act), that the answer is obvious. There is no doubt that they are a store of value. In the case of bitcoin they can be a store of very considerable value, given that the current exchange rate is approximately £6,600 to one bitcoin.
11. Since the purpose of bankruptcy and liquidation is to realise the value residing in all assets of the bankrupt or the company and divide it *pari passu* between all creditors, it would be an extraordinary omission if (however it might otherwise legally be classified) it did not form part of the estate.
12. The question has not, so far as I am aware, arisen for decision in England, but it arose in Russia in 2018 in the bankruptcy of Mr Tsarkov. The insolvency practitioner appointed over his estate sought an order from the Commercial Court in Moscow seeking disclosure of a crypto-currency wallet holding bitcoin, which it was claimed belonged to Mr Tsarkov. The Court declined, refusing to recognise bitcoin as an asset in the estate. Among its reasons were, first, that the legal nature of crypt-currencies was unclear, and not analogous to other forms of property and, Second, that the anonymity surrounding holding of bitcoin made it difficult, in practice, to establish ownership.
13. The case was reversed on appeal, however. The appeal court, noting that the definition of property in the Russian legislation was not exhaustive, but included “other assets”,

said that “taking into account current economic realities and the level of development of information technologies, the broadest interpretation [of “other assets”] was justified”. S.436 of the Insolvency Act is similarly an inclusive, not exhaustive, definition of property, and includes “every description of property ... and every description of interest arising out of or incidental to property.” I have little doubt that the same conclusion would be reached here.

14. The second issue is more challenging. Let me put it into a practical perspective. Despite the fact that one of the benefits of bitcoin is that it enables financial transactions to take place without the need for banks or intermediaries, nevertheless there is a large quantity of bitcoin that is traded by intermediaries. If I am the client of a broker who trades bitcoin “on my behalf” (using that term in a legally neutral manner), and that broker goes into liquidation, what is the nature of my claim in relation to the bitcoin?
15. This might be thought to be no different from the case where a broker trading traditional assets (securities or cash) becomes insolvent: the answer depends upon the nature of the relationship made between us in the real world. Did I transact on terms that the broker held assets on trust for me? And, if not expressly, was the broker required to deal with my assets, for example by segregating them from his own, or from those of other clients, such that the law might imply a trust. But there is an important prior question in the case of bitcoin. What does it mean to say that a person either “holds” or “owns” bitcoin? That, in turn, poses a further prior question: what *is* a bitcoin?
16. I will turn to these questions in a moment, but I first need to step back, and ask (from the perspective of a property lawyer) what we mean by “money”, then see how bitcoin fits, as a practical matter, into that analysis.
17. When we talk of someone ‘having’ an item of currency, we generally mean one of two things: either they possess physical money, namely an actual coin, or they have a right against another person to have something of value transferred to them. The paradigm case being money in a bank account, which in law consists of a debt, namely a right of action against the bank. In fact – although the concept of ‘virtual’ currencies is relatively new – traditional money has long since lost its connection with actual things of value. Coins were originally items of intrinsic value, being made of precious metals. But there is no longer any intrinsic worth in a £1 coin, let alone silver or copper coins. They have value only because of what they represent. The promise by the bank of England to pay the bearer of a banknote £10 or £20 has been practically meaningless since they long ago ceased to represent deposits of gold. And what does it actually mean to say that an institution has funds on deposit with the Bank of England? If you ask: How does the Bank satisfy the obligation owed to institutions which have deposited funds? you might quickly get stuck in an existential circle.
18. But – legally – these all have a clear foundation in property law. Personal property has long recognised two categories: choses in possession and choses in action. The former is a thing of which physical possession may be taken. The latter may only be enforced by action against a third party. A coin is obviously a chose in possession. A bank account is obviously a chose in action: it can only be obtained or enforced by taking action against another. Banknotes are something of both: they are transferred by delivering possession and in the real world are dealt with in precisely the same way as coins, but in form they are a promise by the bank of England to pay – a form of action.

19. But Bitcoin is different. With apologies to those in the room with more awareness of the technology than I have, I will attempt to offer an explanation of what we mean when we talk of a bitcoin.
20. It depends upon three essential concepts: the blockchain; distributed ledger technology (“DLT”); and the public and private keys of users.
21. Blockchain is, at its simplest level, a record of transactions in which each transaction comprises a “block” which is added to the “chain” of all prior transactions.
22. Divorced from DLT, we could create a blockchain on a whiteboard in this room with an invented currency: the Insolvency Lawyers Association Dinarius, or the “ILAD”. I have one ILAD which I record on the whiteboard. I then transfer half to A and half to B. The whiteboard contains the identification details of me, each of A and B, the amount I transfer to each of them, and the date and time. And so on: each onward transaction is recorded by adding another block to the whiteboard containing similar details. The ledger will show a series of chains of transfers so that you can see precisely how each ILAD ended up where it is currently shown to be.
23. This example, however, is still close to traditional money, because I hold the pen, so I decide which transfers of ILAD it is appropriate to record on the whiteboard ledger. I am playing the part of the banking system, which we currently rely on to verify and authorise transactions.
24. The next step is to add in the distributed ledger technology. Instead of one whiteboard ledger, the ledger exists in digital form, and there are as many copies as there are participants in the system and any change to the ledger happens simultaneously in all copies. The really important feature, which distinguishes it from traditional money, however, is the absence of a central operator who determines which transfers are valid, and which are not. Instead, the task of verifying transactions is undertaken by users, who can choose to lend their computing power to solve complex mathematical problems which (in a way which I confess I have consistently failed to understand) has the result of determining whether a block is to be added to the chain.
25. Finally, rather than identifying any person in the real world as a party to transactions, the only information known by the system, and published in a block to be added to the chain, is something called the public key of a user. That is – in essence – its digital address; a number containing 256 bits. So each block will record a transfer from one public key to another, the amount of bitcoin being transferred and a time stamp.
26. Each user also has a private key; a long string of 64 numbers and letters, connected to but impossible to reverse engineer from the public key. Bitcoin are transferred by a user combining his or her private key with their public key. The private key is thus an essential component. If someone else has it – they can control “your” bitcoin. If it is lost, you have lost the ability to control (and so realise any value in) your bitcoin. There are plenty of stories of people having lost a hard drive on which a private key was stored and in the process have lost forever bitcoin worth tens of millions of pounds.

27. Returning to the first of my prior questions (what *is* a bitcoin? what is the *asset* which we say we hold or own when we say we hold or own bitcoin?), some might suggest that it is the private key, because (as I said) the private key is essential to controlling the bitcoin. As a famous bitcoin podcaster (Andreas Antonopoulos) put it: “your keys, your bitcoin; not your keys, not your bitcoin”. But the fact that the private key is necessary in order to transact bitcoin does not make it the thing that is the bitcoin. Indeed it presupposes the opposite, since it gives control, but over something else. Therefore it is to the something else we must look to identify that which is the “bitcoin”.
28. In any event, the private key is merely information: a string of numbers with no intrinsic value. It is just that knowledge of them is required in order to transact bitcoin. It may be recorded on a piece of property, for example on a computer, or even written down on a piece of paper. But there are significant hurdles in the way of regarding it as property itself. For example, although knowledge can be acquired by it being passed from one person to another, it cannot be the subject of a transfer as property can, in the sense of a subtraction from the transferor and addition to the transferee, because the person who passes on the information does not thereby cease to have the information.
29. The second candidate is the computer code recording the blockchain itself. While the code is a record of every prior transaction in that bitcoin, however, it is difficult to equate this with “the bitcoin”. If A transfers bitcoin to B, this is not effected by a transfer of the code. Instead, it is effected by addition of new code. That is, a new block is added to the chain.
30. So, what are we left with? As Louise Gullifer and Janis Sarra put it in an article entitled “Crypto-claimants and Bitcoin Bankruptcy: Challenges for Recognition and Realisation” in March 2019: the most likely candidate for being considered property is the “thing that is the subject matter of the transfer, which does not even exist as a piece of code”. In other words, a bitcoin is an entirely imaginary thing: it is the concept which users in the system treat as being transferred from one public address to another when a block is successfully added to the chain recording that the transfer has taken place. It is of less intrinsic value - even - than the leaf that the imagined ancient earth-dwellers used for currency. As Adam and Eve discovered, a leaf has its uses. But a block added to a chain on a digital system is of no actual use to anybody. It has value only because sufficient users of the system believe that it does. But that (as I have explained) is not so different from many fiat currencies: as demonstrated at moments of financial crises by runs on banks and runaway inflation.
31. So far, I have considered the first prior question – what *is* a bitcoin. I turn, then, to the second prior question: how do you identify the owner of the bitcoin? With traditional forms of money, since they exist either as things in possession or things in action, the identity of the owner (subject only to real world relationships of trust, bailment and the like) is in the first instance straightforward: it is the person in possession of the thing in possession, or the person in whom the right of action against another is vested. Going back to my broker/client analysis, it is conceptually possible (but practically unlikely) that the broker will be in physical possession of coins or notes. More likely, the broker will be the person in whom the relevant right of action is vested. Generally speaking that is because the broker is the named holder of a bank account, or of a securities account with another intermediary. In either case, therefore, it is the broker who can be said, in law, to hold or be the owner of the money. The extent to which the client has

a proprietary interest in the money is to be defined by the terms of the relationship - express or implied – between the client and the broker.

32. From my analysis of what a bitcoin actually is, however, it can be seen that it fits into neither category of property – at least as those categories are currently understood. They cannot be things in action, since they do not constitute a right against any third person. Of course, a right can be generated by a contract with a third person to require the transfer of a bitcoin, in the same way that a contract can be made with someone to transfer pound coins, but the bitcoin itself is no more a right against a third person than a pound coin. While the computer code records all prior transactions between public keys (behind which we might assume sit real people), it does not itself represent a right of action against any counterparty. The participants in the system do not undertake any legal obligations towards each other.
33. Nor – under traditional legal analysis – can a bitcoin constitute a chose in possession. As recently re-affirmed by the Court of Appeal in *Your Response v Datateam Business Media* in 2015², “Possession is concerned with the physical control of tangible objects.” In that case, although entering information onto a digital database altered the physical properties of the equipment, it did not render the information itself capable of being possessed. Whatever a bitcoin (or probably any other crypto-asset) may be, it is intangible, and not something capable of physical control.
34. There is a good argument, and strong academic support, for the proposition that it is not beyond the wit of the common law to recognise a new category of property: virtual choses in possession. See, for example an article by Joanna Perkins and Jennifer Enwezor in the journal of international banking and finance law entitled “The Legal Aspects of Virtual Currencies”³, where they point out that bitcoin share many of the characteristics of physical property: they can be transferred and stored in a way that they can be lost; and they can be transferred by – at least notionally – placing them in a digital wallet on the user’s computer.
35. Even if we conclude that there is a new category of virtual things in possession, however, that does not in itself solve the problem of how to identify its owner. Going back to the broker/client again, in contrast to the case with bank accounts or securities, there is no physical thing which the broker possesses and no account (representing a claim against any third party vested in the broker). The most that might be said is that the broker is the person who in practice operates the private key so as to exercise control over the transfer of bitcoin in the system.
36. So, even though the private key is not to be equated with the bitcoin, should we equate ownership of the bitcoin with the person “in possession” of the private key? This is the obvious starting point, because it is the private key which connects a person in the real world to the virtual system. It is problematic, however, given the difficulties I have already mentioned: because of the difficulties surrounding possession and in particular the transfer of possession of something which exists only as information. If knowledge of the private key is shared, for example among friends to avoid it being lost, is there joint ownership among all with knowledge? What about someone who stumbles across

² [2015] QB 41, at [23]

³ JIFBL (2016) vol 31

a copy of the private key, or forces it from the broker at gunpoint: surely, that would not make that person the owner of the bitcoin any more than someone who obtains at gunpoint the secret code of the entry system to a building owns the building.

37. And in relation to the broker/client relationship, what if that knowledge has from the outset been shared between the broker and client – such that they both have a copy for safekeeping? Which of them is then the “owner”? And what if the client, fearing the insolvency of the broker, ensured it obtained a copy of the string of numbers shortly before the broker went bust? Would the client have thereby become the owner and, if so, how could that be described as a transfer of property in the bitcoin from the broker to client?
38. The practical consequences in the insolvency of the broker could be very significant, particularly where the broker has wrongly transferred bitcoin away. With money in a bank account, ownership rights of the client will depend upon a trust being declared over the broker’s legal interest in the account. The client’s rights are always equitable. But if the true analysis is that the client – not the broker – is the direct owner of the bitcoin, and not merely an equitable interest carved out of the broker’s legal interest – then the analysis of the client’s rights against third party transferees might be very different (dependent on the *nemo dat* principle as opposed to being at the mercy of equity’s darling) and that much stronger.
39. I do not purport to have the answers to these conundrums, but if there is one piece of practical advice arising from this, it is that - given the uncertainty surrounding legal ownership as between the intermediary and client, it is essential that this be expressly addressed in the terms of the contract between them. For example by way a term that states, at least as between the two of them, that one or other is intended to be the owner of the bitcoin. If the client is the intended owner, then the contract will spell out that the broker is simply employed to effect transactions in the client’s bitcoin. If the broker is the owner, then the contract will define the nature of the client’s interest by reference to that ownership right of the broker: probably by declaration of trust in the client’s favour.
40. I have deliberately focused on a simple, bi-partite arrangement. The uncertainties multiply once you are dealing with an intermediary acting for numerous clients, and have to consider concepts such as co-ownership and pooling.
41. As the Russian court in Mr Tsarkov’s case noted, the difficulties in identifying the owner of crypto-assets have important practical consequences in insolvency as well. First, the informality and lack of transparency surrounding bitcoin may make it difficult to identify that the bankrupt had an involvement with bitcoin at all. There are no bank statements, and no transaction records other than the blockchain itself, which is wholly anonymised: it records all public keys, but does not identify any real person behind those keys.
42. On the other hand – while existing in the ether – bitcoin have value in the real world only when exchanged for something of use such as fiat currency, products or services. So it is likely that there will have been interactions with other people in the real world, which have left a trace – in bank accounts or emails or other communications, from which conclusions can be drawn about the bankrupt’s likely involvement with bitcoin.

43. Second, assuming that the bankrupt did have such an involvement, the informality makes it much easier for the bankrupt to hide assets, either by effecting transfers to friends or family, or purporting to hide behind such people, e.g. by not holding any record himself of the public or private key, but leaving it to others to do that, so that he can claim that it is they, and not he, who “own” the bitcoin.
44. Third – and conversely – if the trustee discovers the record of a private key in the possession of the bankrupt, he may claim the reverse position, that he is merely the keeper of the record of the key for X or Y, who actually “owns” the bitcoin.
45. Ultimately – these are similar problems to those that already exist with bankrupts intent on hiding assets from their trustee (perhaps with an added layer of complexity) and are to be addressed using the existing tools: s.366 in particular.
46. Turning to the third and final issue on my list: if the claim to recover bitcoin is personal, then what is the nature of that claim? This might arise in the claim against my insolvent broker. If the broker fails to return to me bitcoin, but my claim is a purely personal one, is it characterised as a secondary claim for damages based on the broker’s failure to comply with his primary obligation to account to me for bitcoin? Or is it a claim for payment in the currency of bitcoin?
47. The same question could arise in other circumstances: for example, what if I conclude a transaction of sale with someone on terms that they will pay me in bitcoin, but they become insolvent while the contract is still executory. Do I have an action for the price (in bitcoin)? Or merely a claim for unliquidated damages based on breach of contract to deliver a commodity?
48. If the claim is analysed as one in debt, i.e. for payment of bitcoin as money, then in order for a pari passu distribution to be made it is essential for it to be converted into the currency in which the insolvency estate is to be administered before any distribution can be calculated and made. This is enshrined in statute: Insolvency Rule 14.21 requires any debt payable in a foreign currency to be converted to sterling at the date of commencement of the insolvency.
49. Although as a matter of language, it may be a strain to say that bitcoin is a “foreign” currency, the rule is an embodiment of the pari passu principle I have just mentioned, combined with the principle of a notional realisation and distribution of assets on day one. Accordingly, there is a good argument for saying that “foreign” should – on a purposive construction – include any non-sterling currency.
50. Given the volatility of bitcoin -and other crypto-currencies – and the fact that the valuation of the claim may well depend on a different date in either case, the difference between treating it as a foreign currency claim, or as a damages claim for failing to deliver a commodity could be enormous.
51. The question whether crypto-currencies can be considered money has been the subject of much debate. As with all questions relating to crypt-assets, there is no one-size fits all answer. In 2016, the FMLC produced a paper which concluded “that virtual currencies which have achieved status as a medium of exchange within a significant

user community have a good claim to be regarded as money”. They pointed out that there is no single wholly satisfactory theory of what money is, as a matter of law. Some commentators focus on its function as a sovereign currency, i.e. that it must be backed by a state. But this arguably fails to account for something which is widely accepted to be money – namely a credit in a current bank account – which consists solely of a private law relationship of debtor-creditor. Some commentators focus on the concept of legal tender. But this fails to account for the fact that under English law we undoubtedly regard US dollars and Japanese Yen as money, but neither is legal tender in this jurisdiction. Of greater use is the “societary” theory of money, in the words of Charles Proctor in *Mann on the Legal Aspects of Money*, negotiability of coins and notes stems from their ability to “pass in currency” –that is that they are commonly and continuously accepted as payment in exchange for articles of commerce.

52. This involves a question of fact – the answer to which will change over time. So, the more that bitcoin is in fact commonly and continuously accepted as payment in exchange for articles of commerce, then the more it is likely to acquire the status of money.
53. Economists point to a three-fold test for money: (1) it is a store of value; (2) it is a medium of exchange; and (3) it is a unit of account. The UK Cryptoasset Taskforce (comprising representative from the Bank of England, the FCA and the Treasury) concluded in a paper in 2018 that crypto-assets are not to be considered as a currency or money, precisely because they are too volatile to be a good store of value, they are not widely-accepted as a means of exchange and they are not used as a medium of account. The taskforce’s principal focus was, however, on regulatory issues, rather than on the narrow, legal questions I have posed in this insolvency context. While there may be good reasons for not regulating crypto-currencies as “currency”, and their volatility cannot be denied, as I have pointed out, the question of consistent use as a medium of exchange and the question of use as a unit of account are fact based, and can change over time. If volatility alone was a ground for excluding something from the definition of money, then did that disqualify the Italian Lire in times past? Or the Mexican Peso more recently?
54. If a crypto-currency is inherently unstable, then that may be a reason why it is not widely used as a medium of exchange, but it would seem doubtful that volatility alone precludes it from qualifying as “money”.
55. In conclusion, these are just three questions that might arise in the insolvency of parties involved in crypto-currency transactions. There are many more I could have considered. For example: is a claim to be paid in crypto-currency a “debt”, so as to found a statutory demand in bankruptcy? And, given that transactions in Bitcoin are intended to be immutable, and wholly anonymised, there may well be practical difficulties in relation to transactions rendered void, or voidable, by the Insolvency Act: how do you approach the setting aside of a transaction where (a) the transaction cannot be reversed and (b) the identity of the counterparty is unknown? But these, and other, questions I leave to another day.