

9-2017

Legal risks of owning cryptocurrencies

Kelvin F. K. LOW


Singapore Management University, kelvinlow@smu.edu.sg

Ernie TEO

IBM Research

DOI: <https://doi.org/10.1016/B978-0-12-810441-5.00010-5>

Follow this and additional works at: https://ink.library.smu.edu.sg/sol_research

 Part of the [Commercial Law Commons](#), and the [Finance and Financial Management Commons](#)

Citation

LOW, Kelvin F. K. and TEO, Ernie. Legal risks of owning cryptocurrencies. (2017). *Handbook of Digital Finance and Financial Inclusion*. Vol 1: Cryptocurrency, FinTech, InsurTech, and Regulation, 225-248. Research Collection School Of Law.

Available at: https://ink.library.smu.edu.sg/sol_research/2485

This Book Chapter is brought to you for free and open access by the School of Law at Institutional Knowledge at Singapore Management University. It has been accepted for inclusion in Research Collection School Of Law by an authorized administrator of Institutional Knowledge at Singapore Management University. For more information, please email libIR@smu.edu.sg.

Legal Risks of Owning Cryptocurrencies

Kelvin FK Low* and Ernie Teo**

ABSTRACT

Cryptocurrencies like Bitcoin have matured from being associated exclusively with techies and radicals to being considered by central banks as a technology to implement digital money. Cryptocurrencies exist only in digital form and can be transferred completely between digital addresses. This is both unlike conventional electronic money as understood by laypersons which acts as a debt claim on a deposit with a trusted financial institution such as a private bank and unlike conventional corporeal money which may be physically possessed. This means that any legal rights associated with holding cryptocurrencies must be different despite it being remaining open to interpretation. In this chapter, we look at the various treatments of money in the legal sense and discuss the risks associated with each by drawing on real life examples. We conclude that fraud through hacking could potentially pose a problem to widespread adoption of cryptocurrencies as the absence of recourse against a third party such as a bank concentrates risk in holders of cryptocurrencies. Users should thus exercise caution and understand the risks before investing in cryptocurrencies. This warning requires emphasis as many parties misapprehend the cryptography within the technology as protecting them from such fraud when in fact it does no such thing.

1. INTRODUCTION

On 18 July 2016, economists at the Bank of England published a research paper studying the macroeconomic consequences of issuing central bank digital currencies.¹ The

* Associate Professor, School of Law, Singapore Management University.

** Research Fellow, Sim Kee Boon Institute for Financial Economics, Singapore Management University.

The authors would like to thank Professor Mark Findlay and Professor Yeo Tiong Min for helpful comments on an early draft of the paper. The usual caveats apply.

¹ John Barrdear and Michael Kumhof, "Staff Working Paper No. 605: The macroeconomics of Central Bank Issued Digital Currencies" (18 July 2016) (<http://www.bankofengland.co.uk/research/Pages/workingpapers/2016/swp605.aspx>). The

following day, *The Wall Street Journal* gave an account of the study under the headline ‘The Central Bankers’ Bold New Idea: Print Bitcoins’,² making a connection between the idea of a central bank digital currency to Bitcoin, the original cryptocurrency conceived by the mysterious³ Satoshi Nakamoto.⁴ One week later, in a column lauding the benefits of electronic money, a *Financial Times* columnist astutely observed that the report had mistakenly conflated two quite distinct questions:⁵ ‘One is whether individuals and companies should have access to electronic cash that is official money (in essence, claims on the central bank) rather than private money (as in today, claims on private banks, or non-bank private claims, as in bitcoin). The other question is whether official e-money should be implemented by central banks’ adopting bitcoin-style technology (so-called “distributed ledgers” where a network of computers verifies transactions and holdings) or as it is today, through centralised registers held by the money issuers.’ From an economics perspective, the distinction drawn by the *Financial Times* may perhaps be correct. However, as a matter of legal analysis (and perhaps more importantly, the risks associated with the legal analysis), the classification between official money and private money needs to be more carefully examined. This is because the different forms of money, broadly defined, expose their holders to different risks depending on their legal nature.

2. MONEY BEFORE BITCOINS

Bank of England is not alone in exploring such an initiative. See also Philip Stafford (17 June 2016), “Canada Experiments with Digital Dollar on Blockchain”, *Financial Times*; Stan Higgins (20 January 2016), “China’s Central Bank Discusses Digital Currency Launch”, *CoinDesk* <http://www.coindesk.com/peoples-bank-of-china-discusses-plans-to-issue-digital-currency/> Retrieved 1 August 2016.

² Jon Sindreu (19 July 2016), “The Central Bankers’ Bold New Idea: Print Bitcoins”, *The Wall Street Journal*.

³ The true identity of Satoshi Nakamoto has been much speculated but remains unknown. See, eg, Robert McMillan (7 March 2014), “Why Bitcoin Doesn’t Want a Real Satoshi Nakamoto”, *The Wired*; Izabella Kaminska (7 May 2016), “Bitcoin: Identity Crisis”, *Financial Times*; Andrew O’Hagan (30 June 2016), “The Satoshi Affair”, *London Review of Books*.

⁴ Satoshi Nakamoto (October 2008), “Bitcoin: A Peer-to-Peer Electronic Cash System” <https://bitcoin.org/bitcoin.pdf> Retrieved 14 March 2016.

⁵ Martin Sandbh (26 July 2016), “Free Lunch: Electronic Money is a Public Good”, *Financial Times*.

Since we are proposing to analyse the consequences (in terms of risks) of a *legal* classification, it is necessary to ground our study in a particular legal system. For our purposes, we will do so with reference to the English common law.⁶ The absolute core instances of money, of which there can be no controversy, are of course corporeal money.⁷ In England, this takes the form of metallic coins issued by the Royal Mint and banknotes issued by the Bank of England. Historically, metallic coins are the earliest form of money asset still in use today.⁸ The standard weights and composition of coinage, as well as the amount of debt for which they pass as legal tender,⁹ is today regulated by the Coinage Act 1971.¹⁰ The other indisputable form of money takes the form of banknotes issued by the Bank of England. Banknotes take the form of promissory notes that are made payable to bearer. They were part of a group of property known as documentary intangibles in which the paper form embodies a legally enforceable promise to pay. They were considered documentary intangibles because the promise to pay is regarded by the English common law as a form of intangible property, also known as a chose in action,¹¹ but the law regarded the promise as being embodied in a corporeal, documentary form. Today, the promise is primarily symbolic rather than real, the right of a holder of banknote to redeem it for payment in metallic coin having been abolished in 1914.¹² While they continue to take the form of promissory notes payable on demand by the bearer, 'a banknote presented for payment at the offices of the Bank of England would

⁶ This decision is in very large part the result of the availability of an excellent modern treatise examining money from the perspective of English private law by David Fox, *Property Rights in Money* (2008). While some or even most of our analysis may apply to other legal systems, particularly common law systems derived from English law, the jurisdictional nature of law as a discipline means that there will inevitably be variations in analysis.

⁷ Cf David Fox, *Property Rights in Money* (2008), 16.

⁸ David Fox, *Property Rights in Money* (2008), 10.

⁹ The definition of tender is irrelevant for our purposes. Readers who are interested should refer to David Fox, *Property Rights in Money* (2008), 28.

¹⁰ Coinage Act 1971, ss 2, 6 and 7.

¹¹ Chose being French for thing.

¹² David Fox, *Property Rights in Money* (2008), 47.

nowadays only entitle the bearer to be paid an equivalent amount of notes in a different denomination.¹³ They are therefore effectively pure fiat money.

Somewhat more controversial is the place of incorporeal assets as property, in large part because of the Roman classification of legal rights into rights *in rem* and rights *in personam*. 'If the argument [against treating incorporeal assets as property] were correct, it would drive a wedge through any unified treatment of money since it would require an entirely different explanation of money in its corporeal and incorporeal forms.'¹⁴ This is particularly significant because the 'de-physicalization' of money is a very real phenomenon. In 2011, corporeal money in the form of coins and banknotes amounted to only about 3.6% of the British economy.¹⁵ In Sweden, not only has the ratio of corporeal money to deposits held at banks and other financial institutions been diminishing, the amount of actual corporeal money in circulation appears to have shrunk in a phenomenon christened 'peak cash'.¹⁶ Whilst it is probably premature to write off corporeal money as outdated,¹⁷ incorporeal money¹⁸ in the form of bank deposits therefore is indisputably gaining in economic significance. The question whether such bank deposits are also properly regarded as money and whether there is property in bank money is somewhat trickier. This is because:¹⁹

[i]n legal terms, incorporeal money consists in the customer's legal right to enforce the chose in action entitling him or her to draw upon the credit balance with the bank or any overdraft facility, or to instruct the bank to make payments from the

¹³ David Fox, *Property Rights in Money* (2008), 47.

¹⁴ David Fox, *Property Rights in Money* (2008), 34.

¹⁵ Micahel Burda and Charles Wypolz, *Macroeconomics: a European Text* (6th edn, Oxford, 2013), 207.

¹⁶ Editorial (24 August 2015), The Case for Retiring Another 'Barbarous Relic', *Financial Times*. See also JP Koning (26 February 2015), Sweden and Peak Cash, *Money: the Blog of JP Koning*.

¹⁷ See The Cambridge Security Initiative, *Cash is King – The Digital Revolution: The Future of Cash* (2016). According to the Chief Cashier of the Bank of England, 'Cash is now used in 52% of UK transactions.' (at 5) This is a measure of volume, not value.

¹⁸ This is the generic expression coined by David Fox comparable to the expression 'bank money' found in economic writings: see David Fox, *Property Rights in Money* (2008), 11.

¹⁹ David Fox, *Property Rights in Money* (2008), 12.

fund in his or her account as his or her agent. ... Incorporeal money is therefore a claim to be paid money in primary corporeal form, even though in all likelihood the customer will rarely seek to reduce his or her claim to payment in coins. The customer's transferable balances on the account become media of exchange in their own right.

While economists distinguish between different grades of bank money, we can gloss over these quite cursorily since we are primarily concerned with the risks arising out of the *legal* classification of money. Thus, classifications by economists according to their liquidity and yield into M1, M2 and M3 grades are not significant for our purposes.²⁰ For the purposes of this paper, it is also unnecessary to consider in detail whether such bank money is properly regarded as property as a matter of legal classification.²¹ This is because we are primarily concerned with risks arising out of *holding* particular assets, whether they are regarded as property (however defined).

However, without analysing the issue in too much detail, it suffices to observe that choses in action, whether they take the form of bank debts (money) or otherwise (non-money), have traditionally been regarded as property under English law.²² The rejection of incorporeal assets as property is largely premised upon an artificial distinction drawn between rights *in rem* (rights in relation to things) and rights *in personam* (rights against persons). The former is said to comprise the law of property whereas the latter comprises the law of obligations. Fox rightly criticises the distinction as artificial.²³ One of the chief proponents of this Roman classificatory system in English law, the late Professor Birks, conceded that 'the subdivision of rights between *in rem* and *in personam* is not exhaustive ... The category which is omitted is the category of rights which are good against all people

²⁰ David Fox, *Property Rights in Money* (2008), 17-18. See also Michael Burda and Charles Wypolz, *Macroeconomics: a European Text* (6th edn, Oxford, 2013), 206-14.

²¹ Our forthcoming paper, "Bitcoins as Property?", considers both this question as well as the question of how cryptocurrencies would conceivably fit within a broadly defined property regime.

²² William Blackstone, *Commentaries on the Laws of England Volume 2 of the Rights of Things* (Clarendon Press 1765-69), 442.

²³ David Fox, *Property Rights in Money* (2008), 34-8.

but do not follow any *res*. All of these are superstructural rights ...'²⁴ This view of property, as one of us has previously observed, requiring as it does near universal enforceability of a right, confuses exclusivity with exigibility.²⁵

This is not to say that the Roman classificatory system is wholly without value. Whilst it may be an outmoded means of identifying property in the digital age, it is ironically a very useful starting point for our identification of risks inherent in different forms of legal rights. We begin with the two different forms of money before the advent of cryptocurrencies. While we agree with Fox that they are both properly regarded as property, they happen to fall on either side of the Roman classificatory divide. Rights to corporeal money are protected by the law through *in rem* rights.²⁶ Rights to incorporeal money are debts owing by the relevant financial institution²⁷ and hence indisputably protected as *in personam* rights. In terms consistent with the Roman classification, the difference may crudely²⁸ be described as the distinction between owning something (in the case of corporeal money) and being owed something (in the case of incorporeal money). This exposes holders of corporeal money to completely different risks from

²⁴ Peter Birks, *English Private Law Vol 1* (2000), xxxviii. The late Professor attempts to salvage the Roman classificatory system by suggesting that it is perhaps exhaustive of 'rights realizable in court'. Birks opines, at xxxix: "Thus the right to bodily integrity is protected through the torts which are committed against the body, and the right to reputation is protected by the torts of defamation. Such primary rights are 'superstructural' in that they provide the superstructure over the wrong: every wrong is the infringement of a primary right." However, this cannot be correct. Superstructural rights are realizable in court through the grant of an injunction protecting the primary right.

²⁵ Kelvin F K Low and Jolene Lin, 'Carbon Credits as EU Like It: Property, Immunity, TragiCO₂medy?' (2015) 27 *Journal of Environmental Law* 377, 388-9.

²⁶ Ignoring for present purposes the token right, almost never exercised, by a holder to compel the issuing bank of a banknote by action to pay him or her an equivalent value of notes of a smaller denomination.

²⁷ *Foley v Hill* (1848) HLC 28.

²⁸ While this may be inconsistent with the wider definition of property earlier proposed, the Roman classification is better suited to our understanding of risk arising out of the differing nature of the rights.

those holding incorporeal money. The object of this paper is to demonstrate starkly the different risks that stem from holding different forms of money but before we begin in earnest, we must emphasise that risk is unavoidable. This is the case even with respect to cryptocurrencies, which came to be popularised in part because of the vaunted security of their ledgers. Some of these risks stem from fraud and it bears reminder that, in relation to a different attempt to set up a definitive register of rights (in this case land), the learned Starke J remarked that '[n]o definition of fraud can be attempted, so various are its forms and methods.'²⁹ The enactment of the Fraud Act 2006³⁰ in the UK can also be seen as an acknowledgement of the boundless creativity of the criminal mind. As the Law Commission remarked in its Report that led to the reform: 'A general offence of fraud would be aimed at encompassing fraud in all its forms. It would not focus on particular ways or means of committing frauds. Thus it should be better able to keep pace with developing technology.'³¹

Rights to corporeal money are *in rem* rights in the traditional Roman sense of the term. A right *in rem* is a right in or against a thing. It is generally enforceable against all persons, securing its holder freedom from interference by others of the thing concerned. In the case of corporeal money, the thing (or *res*) will either be banknotes or coins. The advantage of such a right is that it is enforceable against (almost) all comers. Provided the thing can be located, the law will generally permit its recovery or at least recovery of its value. The insolvency of its current holder is thus of no concern to the true owner. Rights to incorporeal money, on the other hand, are classical *in personam* rights. A right *in personam* is a right against a person (or specified persons). Bank money, being simply a particular species of debt, is in legal terms a right to repayment from the particular bank. As the right does not relate to a tangible thing, it is pointless to attempt to locate that thing. Corporeal money deposited with HSBC may be subsequently located in the vaults of Barclays Bank but the actual location of the corporeal money is irrelevant because a deposit involves a transfer of the right *in rem* of the depositor to the coins or banknotes to HSBC in return for a corresponding promise to repay (typically with

²⁹ *Stuart v Kingston* (1923) 32 CLR 309, 359.

³⁰ Chapter 35.

³¹ The Law Commission Report on Fraud 2002 (Law Comm 276), 3.

interest) on the part of HSBC. If HSBC becomes insolvent, the depositor cannot demand repayment by Barclays Bank. At first glance, it may appear that a right *in rem* is obviously superior to a right *in personam* since it is enforceable against multiple parties rather than a single (or limited) party(ies). However, careful reflection reveals that exchanging one form of right for another involves exchanging one form of risk for another. While an *in rem* right may indeed be almost universally enforceable, one needs to locate the thing itself (or at least demonstrate that a particular defendant had indeed interfered with the thing) before an action can be brought. If you cannot identify the thief of your coins or banknotes, your right to sue the thief is largely theoretical. Provided the debtor is solvent, an *in personam* right frees the holder of the right from concerns over the theft or destruction of any particular thing since the right does not relate to any particular thing.³² Therefore, risk is inevitable though its form will differ depending on the nature of the right.

3. 'DIGITAL MONEY' BEFORE BITCOINS

It may come as a shock to economists, technologists, businessmen and consumers but there is no such thing as digital money as a matter of law. At least that was almost certainly true before the invention of cryptocurrencies. References to digital money, so far as legal rights are concerned, represent sloppy thinking and a failure to distinguish the legal right held by holders of such money from the manner in which they were recorded. The distinction is crucially important to our understanding of the risks involved in holding both bank money as well as earlier iterations of digital money. It is useful to begin our analysis with bank money because the legal analysis of bank money is clearer.

³² Despite s 4(1) of the Theft Act 1968 defines property broadly as including “money and all other property, real or personal, including things in action and other intangible property”, it remains a matter of some controversy whether an *in personam* right itself should be regarded as capable of being the subject-matter of theft. See, for example, A P Simester and G R Sullivan, ‘On the Nature and Rationale of Property Offences’, in R A Duff and Stuart P Green, *Defining Crimes: Essays on the Special Part of the Criminal Law* (2005), 168. *Contra* Sarah Green, ‘Conversion and Theft – Tangibly Different?’ (2012) 128 LQR 564.

Today, electronic banking allows us to view our bank balances digitally over the Internet. Yet the fundamental legal nature of bank money has not changed from the early days of banking when ledger entries were made in ink on paper, whether by hand on vellum or by printing on a passbook. Just as a ledger entry on paper did not, except in the case of banknotes,³³ transform bank money render the incorporeal corporeal, neither does a digital entry render it digital. This is an easy mistake to make, for both lawyers and non-lawyers. In *Armstrong DLW GmbH v Winnington Networks Ltd*,³⁴ for example, EU carbon credits (technically European Union Allowances or EUAs) recorded in electronic registries were regarded by the trial judge as existing ‘only in electronic form.’ This, one of us has observed, is ‘not strictly accurate’ and reflects ‘a failure to distinguish between a right and its record’.³⁵ ‘Registration systems serve as *records* of rights. They do *not* represent the rights themselves.’³⁶ Thus, in the context of carbon credits, it is not the carbon credits but their ‘inconclusive *record* that exists in electronic form.’³⁷ The carbon credits themselves were, like bank money, entirely without form. From the perspective of risk, this distinction is crucial. Where there has been an unauthorised transfer out of a customer’s account, and the account is adjusted to reflect the unauthorised transfer, ‘[t]he basic answer in English law is that, in the absence of fraud, the customer is not precluded by the bank statement or the pass-book from disputing an error or an incorrect debit made by the bank or from insisting upon its correction.’³⁸ If such errors stem from fraud, provided they are detected quickly, before money is withdrawn, reversing such transfers is often simply an exercise in reversing a data entry.

³³ The nature of banknotes in their original form is complicated and would be distracting for our purposes. They fall within a category of property called ‘documentary intangibles’, a name that reveals the tensions and contradictions within this concept.

³⁴ [2013] Ch 156, [49].

³⁵ Kelvin F K Low and Jolene Lin, ‘Carbon Credits as EU Like It: Property, Immunity, TragiCO₂medy?’ (2015) 27 *Journal of Environmental Law* 377, 391.

³⁶ Kelvin F K Low and Jolene Lin, ‘Carbon Credits as EU Like It: Property, Immunity, TragiCO₂medy?’ (2015) 27 *Journal of Environmental Law* 377, 391.

³⁷ Kelvin F K Low and Jolene Lin, ‘Carbon Credits as EU Like It: Property, Immunity, TragiCO₂medy?’ (2015) 27 *Journal of Environmental Law* 377, 391.

³⁸ EP Ellinger, E Lomnicka and CVM Hare, *Ellinger’s Modern Banking Law* (5th edn, OUP 2011) 236.

Consider the recent Bangladesh Central Bank cyber-heist. On 4 February 2016, unknown hackers used the SWIFT credentials of employees of the Bangladesh Central Bank to send transfer requests to the Federal Reserve Bank of New York requiring the latter to transfer millions of the Bangladesh Bank's money to bank accounts in, *inter alia*, the Philippines and Sri Lanka. In this way, \$81m was transferred to Rizal Commercial Banking Corporation in the Philippines and \$20m was transferred to Pan Asia Banking Corporation in Sri Lanka. It is necessary to explain how such money 'transfers' work in legal terms before delving further into the facts of the cyber-heist. As Fox explains, '[t]he explanation of how property in incorporeal money is transferred has very little to do with the law governing the transfer of chattels by delivery. Far more relevant are the principles of the law of contract and agency, and the enforcement of title to choses in action.'³⁹ There is in truth no 'transfer' of property, only a transfer of value:⁴⁰

The chose in action representing the money transferred to the recipient's bank account is a distinct item of property from the chose in action representing the funds which were originally in the payer's account. The payer's title to the money is not strictly transferred. Instead, the title to the value represented in the transfer passes to the recipient because the payer's bank extinguishes (wholly or partially) the debt which it owes the payer, and the recipient's bank creates a new debt owed by itself to the recipient.

Unlike a transfer of corporeal money, which involves the simultaneous extinction of the transferor's rights to the banknotes or coins and the vesting of the transferee's rights to the same, 'transfers' of incorporeal bank money involves no such simultaneous vesting and extinction.⁴¹ The time when the transferee acquires irrevocable rights to the

³⁹ David Fox, *Property Rights in Money* (2008), 165.

⁴⁰ David Fox, *Property Rights in Money* (2008), 165.

⁴¹ 'A payment instruction may become irrevocable before the point is reached where a payment to the beneficiary becomes complete. There may be a hiatus during which neither the originator nor the beneficiary has a complete title to the money which is being transferred between them. This marks a significant difference from payments made by the physical delivery of corporeal money where the transfer of title from the payer and to the recipient happens simultaneously. It is a consequence of the fact that a payment of incorporeal money is always made through a bank

transferred sum, in the form of a debt owing by its bank, is dependent on the terms of its contract with its bank and the rules of banking practice governing the particular transfer.⁴² It is clear, however, that this is neither the time its bank receives the payment instruction, the time its bank receives the funds transferred (typically in the form of incorporeal money it holds with a correspondent bank), nor the time a credit entry is made in the bank's ledger for the transferee's account.⁴³ The only way to be absolutely sure of a secure receipt is for the transferee to withdraw the funds transferred. The timing of the Bangladesh heist appears to have been chosen carefully to take advantage of the weekend when no one at the New York Fed was available to respond to attempts by the Bangladesh Bank to halt the transfer orders,⁴⁴ probably in the hopes that this will permit the hackers sufficient time to withdraw the funds from the accounts to which they had been transferred. This was true of the transfers to Rizal Commercial Banking Corporation.⁴⁵ However, the transfer to Pan Asia Banking Corporation, though receiving far less media attention, is more instructive for our purposes. Although the transfer had already been cleared by the Fed, the recipient bank had not released the funds to the

acting as intermediary between the parties to the payment transaction, and of the distinct identity of the choses in action by which the money is represented.' : David Fox, *Property Rights in Money* (2008), 185.

⁴² David Fox, *Property Rights in Money* (2008), 180.

⁴³ David Fox, *Property Rights in Money* (2008), 181-183.

⁴⁴ Kim Zetter (17 May 2016), That Insane, \$81m Bangladesh Bank Heist? Here's What We Know, *The Wired* (<https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/>)

⁴⁵ 'It turns out that the four-day lapse before the fraud was uncovered was plenty of time for \$81 million to be transferred from the Bangladesh Bank account at the New York Fed to Wells Fargo Mellon Bank, Citibank, and Bank of New York, to Rizal Commercial Banking Corporation's Settlement Division, to bank accounts for a Chinese businessman at a local branch at RCBC, and then on to casinos in the Philippines': Chelsea Allison (2 June 2016), Anatomy of a Bank Heist, *Fin* (<https://fin.plaid.com/articles/anatomy-of-a-bank-heist>). It should be noted that even so, of the \$81m, some \$68,305 funds that had not been withdrawn were eventually put on hold: Arun Devnath (16 March 2016), Printer Error Triggered Bangladesh Race to Halt Cyber Heist, *Bloomberg News* (<http://www.bloomberg.com/news/articles/2016-03-16/printer-error-set-off-bangladesh-race-to-halt-illicit-transfers>)

account holder and so the transfer could simply be, and was indeed, reversed once the fraud was clearly established. In this case, it appears that Pan Asia Banking Corporation had contacted its routing counterpart, Deutsche Bank, because, according to an official,⁴⁶ '[t]he transaction was too large for a country like [ours]'. Upon checking, Deutsche Bank 'came back and said it was a suspect transaction.' This was because the request had misspelt the recipient's name as *Shalika Fandation* instead of *Shalika Foundation*. Thus, 'the typo was caught in time to freeze the funds, which were returned to Bangladesh Bank's account in New York via Deutsche Bank on Feb 17.'⁴⁷ In legal terms, the Bangladesh Central Bank's statement of accounts with the Federal Reserve Bank of New York was corrected to reflect the wrongly debited \$20m.

Even in respect of money that has been withdrawn by the transferee, the loss does not necessarily fall on the account holder because the statement of accounts is not authoritative and normally, barring contractual terms to the contrary, losses stemming from any unauthorised 'transfers' fall on the bank rather than its customers. The contract between the bank and the customer may attempt to shift these losses onto customers. In some jurisdictions, such as Canada, this has taken the form of the practice of inserting verification clauses into their contracts with customers. Such clauses would 'impose on the customer a duty to peruse his account statements promptly and to notify the bank of any errors or irregularities within a specified time. Failure so to notify the bank should be deemed to constitute a verification by the customer of the balance struck'⁴⁸ However, as Ross Anderson, Professor of Security Engineering at the Computer Laboratory at the University of Cambridge observed, 'Since the late 1990s the move to phone banking and then the internet has led to contract terms and conditions along the lines of "You agree to be liable for any transactions which, according to our records, were made using your

⁴⁶ Serajul Quadir (10 March 2016), How a Hacker's Typo Helped Stop a Billion Dollar Bank Heist, *Reuters* (<http://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight-idUSKCN0WC0TC>)

⁴⁷ Chelsea Allison (2 June 2016), Anatomy of a Bank Heist, *Fin* (<https://fin.plaid.com/articles/anatomy-of-a-bank-heist>)

⁴⁸ EP Ellinger, E Lomnicka and CVM Hare, *Ellinger's Modern Banking Law* (5th edn, OUP 2011) 240-1.

password, whether you actually made them or not”.⁴⁹ Drafted in extremely broad and all-encompassing terms, it should be observed that such clauses are subject to statutory control. Although directed towards verification clauses, the following statement applies equally to clauses that purport to transfer liability for unauthorised online transactions onto customers:⁵⁰

Where the bank’s customer is a consumer, or a non-consumer dealing on the bank’s written standard terms of business, [such clauses] run the risk of being held unreasonable and, therefore, ineffective under the [Unfair Contract Terms Act] 1977. Under section 13(1)(c) of UCTA 1977, clauses that exclude or restrict rules of evidence or procedure are treated in the same way as those that exclude or restrict liability. Where the customer is a consumer, the clauses is also at risk of being held to be unfair and, therefore, unenforceable under the [Unfair Terms in Consumer Contracts Regulations] 1999. Schedule 2, paragraph 1(q) of the Regulations indicates that a term may be unfair where it has the object and effect of unduly restricting the evidence available to a customer against his bank or imposes a burden of proof on the customer that should, by law, be on the bank.

Clauses that are as widely drafted as those referred to by Professor Anderson are unlikely to survive judicial scrutiny and it is likely that banks will shoulder the losses rather than pass them onto customers if litigation is simply threatened unless the sums involved are large and/or it is able to demonstrate gross negligence on the part of their customers. First, banks make substantial savings through internet banking and if customers stopped using these services because they feel that the system cannot be trusted, these savings

⁴⁹ Miles Brignall (21 November 2015), So You Think You’re Safe Doing Internet Banking?, *The Guardian* (<https://www.theguardian.com/money/2015/nov/21/safe-internet-banking-cyber-security-online>). See also Ingolf Becker et al, ‘International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms’, *Workshop on the Economics of Information Security (WEIS)*, 13-14 June 2016, Berkeley, CA, USA.

⁵⁰ EP Ellinger, E Lomnicka and CVM Hare, *Ellinger’s Modern Banking Law* (5th edn, OUP 2011) 243. See also Nicholas Bohm et al, ‘Electronic Commerce: Who Carries the Risk of Fraud?’ (2000) 3 *Journal of Information, Law and Technology* (https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/)

would be lost.⁵¹ Secondly, litigation, as already observed, is likely to lead to such clauses being pronounced ineffectual, especially since they seem to contradict the standards set out in the 'Banking: Conduct of Business Sourcebook' issued by the Financial Conduct Authority.⁵²

Consider then the precursors of Bitcoin that are *not* bank money. In the early nineties, a product called DigiCash was launched which openly touted itself as digital money.⁵³ There were two problems with the product, one of which proved fatal. As its inventor, David Chaum, observed, 'It was hard to get enough merchants to accept it, so that you could get enough consumers to use it, or vice versa'.⁵⁴ This practical problem resulted in DigiCash Inc, the company, being declared bankrupt in 1998. However, it is the lesser of the two problems that interest us. Digital money, it turns out, is not money in digital form after all. Rather, similarly to bank money recorded digitally, digital money (sometimes also called electronic money) is an *in personam* claim on the issuer (chase in action) that is stored digitally (or electronically, including magnetically).⁵⁵ While the accounts may be recorded digitally and may perhaps be more secure (one of the vaunted attributes of DigiCash was its use of cryptography to secure the records) than banks' statements of

⁵¹ Cf 'Banks choose not to advertise the number of electronic attacks taking place on their systems but instead prefer to pay back the lost amount and then raise the general service charges.': The Cambridge Security Initiative, *Cash is King – The Digital Revolution: The Future of Cash* (2016), 4.

⁵² 'Banking: Conduct of Business Sourcebook' (Release 9: August 2016), paras 5.1.11-5.1.12. The 'Banking: Conduct of Business Sourcebook' replaces 'The Banking Code: Setting Standards for Banks, Building Societies and Other Banking Service Providers' (March 2005), paras. 12.5, 12.9, 12.11-12.12, 12.14-12.16. See also Ingolf Becker et al, 'International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms', *Workshop on the Economics of Information Security (WEIS)*, 13-14 June 2016, Berkeley, CA, USA

⁵³ Steven Levy (1 December 1994), E-Money (That's What I Want), *The Wired* (<http://www.wired.com/1994/12/emoney/>)

⁵⁴ Julie Pitta (1 November 1999), Requiem for a Bright Idea, *Forbes* (<http://www.forbes.com/forbes/1999/1101/6411390a.html>)

⁵⁵ Reg. 2(1) of The Electronic Money Regulations 2011 (SI 2011/99) defines 'electronic money' as 'electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer ...'

accounts, such digital money, if it is even legally money at all, is completely incorporeal as a matter of law. The records may take on a digital form. The right itself has no form whatsoever. It therefore exposes holders to the same sort of risks as bank money – primarily the insolvency of the issuer. Where the issuer is regulated under the Electronic Money Regulations 2011,⁵⁶ this risk is diminished (though not eliminated) through regulations such as the imposition of capital requirements.⁵⁷ Regulated electronic money is always ‘redeemable’ and is thus best construed as debts against the issuer (much like bank money). The rights conferred by issuers to holders of non-regulated electronic money will vary depending on the terms of the contract but they likely remain *in personam* claims against their issuers, though the claim may not take the form of a debt (ie a claim for a sum of money). It may instead be a claim for services of a certain monetary value but the claim is always an *in personam* against the issuer. As such, it will always expose holders to the insolvency risk of the issuer. We posit therefore that the risk of ‘theft’ through hacking is likely to be treated similarly to hacks of bank accounts.

While there are some suggestions in the literature which attempt to assign proprietary or quasi-proprietary status to the electronic token that represents the value of the electronic money,⁵⁸ all such accounts nonetheless resort to a personal obligation against the issuer as the means by which such electronic money attains its commercial value. Furthermore, all accounts that seek to reify (ie reduce to the nature of a thing) the electronic token, as opposed to treating it merely as a record of a right (as we have suggested), have failed to properly account for how such electronic tokens are transferred nor have they explained the nature of their legal protection in any detail. Such accounts are analogous to the original form which banknotes (sometimes privately issued) took where the value in the banknotes lies in the obligation of their issuers to pay an equivalent value in fiat currency (or coins in the case of banknotes issued by Central

⁵⁶ Reg 3 of The Electronic Money Regulations 2011 (SI 2011/99) sets out exclusions.

⁵⁷ See reg 19 of The Electronic Money Regulations 2011 (SI 2011/99).

⁵⁸ Cf Richard Hooley, ‘Payment in a Cashless Society’ in Barry AK Rider (ed), *The Realm of Company Law: A Collection of Papers in Honour of Professor Leonard Sealy* (1998), 233; Alan L Tyree, ‘The Legal Nature of Electronic Money’ (1999) 10 JBFLP 273; David Kreltzheim, ‘The Legal Nature of “Electronic Money”’ (2003) 14 JBFLP 161, 261.

Banks). However, the analogy breaks down because for banknotes, as promissory notes, the *in personam* obligation was reduced to corporeal form and the banknotes were essentially protected and transferred similarly to other corporeal property. Electronic tokens, on the other hand, are fundamentally distinct and incorporeal. In the first place, it is not clear if they are capable of transfer in the property law sense of the word. When we speak of transferring digital files, for example, the process is distinct from that of delivery of a corporeal thing by one person to another. Rather, the 'transfer' process involves the creation of a copy in a new medium before the 'original' copy is deleted in the original medium. This process simulates, but is not identical to, a transfer properly so-called.⁵⁹ Likewise, there is no account of what forms of interferences 'holders' of electronic tokens will be protected from as a matter of law since a basic understanding of property law reveals that the owner of any property is not always entitled to protection from all forms of unwelcome activity. A landowner, for example, cannot complain of neighbours looking over into their land because there is no such thing as visual trespass.⁶⁰ Finally, even if correct, treating such electronic tokens as electronic embodiments of incorporeal *in personam* rights simply exposes 'holders' of such tokens to *both* the risk of loss/destruction *and* the risk of their issuer's insolvency since all issuers to date have been private issuers rather than State issuers.

4. BITCOINS: A PRIMER

In his/her/their white paper, Nakamoto describes a cryptographic system for 'electronic cash' in which payment transactions are verified on the basis of group consensus rather than through financial institutions serving as trusted third parties. According to Nakamoto, the inherent weakness of a trust based model was that transactions are not completely non-reversible. As such, financial institutions cannot avoid mediating disputes which 'increases transaction costs, limiting the minimum practical transaction

⁵⁹ Kelvin F K Low and David Llewelyn, 'Digital Files as Property in the New Zealand Supreme Court: Innovation or Confusion?' (2016) 132 *Law Quarterly Review* 394, 396.

⁶⁰ *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479.

size and cutting off the possibility for small casual transactions.’⁶¹ If payment transactions are reversible, it also entails merchants undertaking the risk of non-performance on the part of their counterparties since apparent payments can be subsequently rescinded. Bitcoin was envisaged as ‘an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.’⁶² As a result of the central role played by cryptography in the system, bitcoin and its derivatives are known as cryptocurrencies. Once properly validated, bitcoin transactions are irreversible.⁶³

Unlike DigiCash, the absence of an issuer or trusted third party means that bitcoin and other cryptocurrencies cannot be regarded as an *in personam* claim on an issuer and so must be analysed differently from bank money and earlier forms of digital money. It also obviously differs in nature from corporeal money in the form of banknotes and coins since there is no corporeal thing (*res*) for any legal right to relate to. If legal protection in the form of property rights attach to bitcoins, it is likely to be in the form of universal abstract rights akin to intellectual property, which do not neatly fall into either Roman classification.⁶⁴ It is not entirely clear what, if any legal rights, attach to bitcoins and other private cryptocurrencies like bitcoin. It has thus been argued that ‘[t]here is ... a good policy reason for the conclusion that one cannot, in a private law sense, “own” bitcoin.’⁶⁵

⁶¹ Satoshi Nakamoto (October 2008), “Bitcoin: A Peer-to-Peer Electronic Cash System”, at 1 <https://bitcoin.org/bitcoin.pdf> Retrieved 14 March 2016.

⁶² Nakamoto, *ibid* at 1.

⁶³ This is not strictly speaking true. They are not unilaterally irreversible but a payee can always repay a payor. This is not technically a reversal in the sense of erasing the initial transfer but it is in substance a reversal through the addition of a further transaction in reverse.

⁶⁴ It is possible to classify intellectual property as *in rem* rights if one does not insist on a strict requirement of a *res* (thing) that is separable from the legal right. Compare William Swadling, ‘Property: General Principles’ in Andrew Burrows (ed), *English Private Law* (3rd edn, OUP 2013) [4.03] with William Swadling, ‘Property: General Principles’ in Peter Birks (ed), *English Private Law Volume I* (OUP 2000) [4.52]. Cf Simon Douglas and Ben McFarlane, ‘Defining Property Rights’ in James Penner and Henry E Smith (eds), *Philosophical Foundations of Property Law* (2013), 219.

⁶⁵ Tatiana Cutts and David Goldstone QC (14 June 2015), Bitcoin Ownership and its Impact on Fungibility, *Coindesk* (<http://www.coindesk.com/bitcoin-ownership-impact-fungibility/>)

Among cryptocurrency enthusiasts, a not insignificant segment subscribe to the idea of immutability, even in the face of demonstrable fraud, as if it were some sort of code of law. This can be seen in the aftermath of a hack of a curious ‘fund’ called the DAO (or Decentralized Autonomous Organization). Set up as an investment fund which would allow all the investors to have a say in the investments made (as opposed to fund managers),⁶⁶ the DAO attracted more than US\$168m worth of a cryptocurrency called Ether.⁶⁷ Unfortunately, on 17 June 2016, a hacker managed to siphon off some US\$50m worth of the invested Ether.⁶⁸ The hack tested the immutability of the Ethereum ledger. The core developers of Ethereum eventually decided on a hard fork of the ledger, in effect a sort of reset that rolled back the entire Ethereum network to its state before the hack.⁶⁹ The hard fork was approved by 97% of the Ethereum network.⁷⁰ This in effect created two versions of the ledger. The original intent of the developers (and those voting for the hard fork) was for the compromised ledger to wither away, the original compromised ledger refused to go away.⁷¹ The survival of this zombie chain that refuses to die, now styled as Ethereum Classic to distinguish it from the hard forked Ethereum which is now

⁶⁶ Cade Metz (6 June 2016), The Biggest Crowdfunding Project Ever – the DAO – is Kind of a Mess, *The Wired* (<http://www.wired.com/2016/06/biggest-crowdfunding-project-ever-dao-mess/>)

⁶⁷ Nathaniel Popper (27 March 2016), Ethereum, a Virtual Currency, Enables Transactions that Rival Bitcoin's, *The New York Times* (<http://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables-transactions-that-rival-bitcoins.html>)

⁶⁸ Klint Finley (18 June 2016), A \$50 Million Hack Just Showed that the DAO was all too Human, *The Wired* (<http://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/>)

⁶⁹ Joon Ian Wong and Ian Kar (18 July 2016), Everything You Need to Know about the Ethereum ‘Hard Fork’, *Quartz* (<http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/>)

⁷⁰ Andrew Quentson (8 July 2016), Ethereum Reaches Unanimous Agreement to Hardfork, *Crypto Coins News* (<https://www.cryptocoinsnews.com/ethereum-reaches-unanimous-agreement-hardfork/>)

⁷¹ Aaron van Wirdum (20 July 2016), Rejecting Today’s Hard Fork, the Ethereum Classic Project Continues on the Original Chain: Here’s Why, *Bitcoin Magazine* (<https://bitcoinmagazine.com/articles/rejecting-today-s-hard-fork-the-ethereum-classic-project-continues-on-the-original-chain-here-s-why-1469038808>)

called Ethereum One, demonstrates that there is a significant segment of the cryptocurrency community who 'would like to see a strict adherence to the original concept of code as law.'⁷²

5. CRYPTOCURRENCY RISKS

Professor Eugene Howard Spafford, a leading computer security expert, was once quoted as saying, 'The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards – and even then I have my doubts.'⁷³ A cryptocurrency network is vulnerable at several levels. Some of these vulnerabilities are theoretical but many have in fact been exploited in practice. At the personal level, a person's private cryptographic key can be 'stolen'. If it is stored electronically on his personal computer or mobile device, this 'theft' or hack can be achieved using malicious e-mail attachments or applications or by using keystroke logging devices or software to trace the private cryptographic key as it is typed in. Even if the private cryptographic key is not stored electronically but offline, for example using a so-called paper wallet, access to the private cryptographic key will still allow a 'thief' to make off with one's bitcoins, as happened to the CEO of a financial services company who left his account information in his car while having it valet parked.⁷⁴ At the exchange level, security loopholes may allow hackers to gain access to an exchange's hot wallet. The most famous case of such a hack is that of Mt Gox, one of the earliest and biggest bitcoin exchanges where US\$460 million worth of bitcoins were apparently 'stolen' by hackers.⁷⁵ More recently, roughly US\$72 million worth of bitcoins were 'stolen' by hackers from

⁷² Kyle Torpey (5 August 2016), Ethereum Experts Debate Merits of Two Ethereum Chains, *Bitcoin Magazine* (<https://bitcoinmagazine.com/articles/ethereum-experts-debate-merits-of-two-ethereum-chains-1470432064>)

⁷³ Quote by Eugene H Spafford in AK Dewdney (March 1989), "Computer Recreations: Of Worms, Viruses and Core War", *Scientific American*, 110.

⁷⁴ Elliot Maras (11 November 2015), "Researcher Has Bitcoin Stolen off His Back in a Public Experiment", *Crypto Coins News* <https://www.cryptocoinsnews.com/researcher-bitcoin-stolen-off-back-public-experiment/> Retrieved 17 March 2016.

⁷⁵ Robert McMillan (3 March 2014), "The Inside Story of Mt Gox, Bitcoin's \$460 Million Disaster", *Wired*.

Bitfinex, an exchange based in Hong Kong. At least, they were worth US\$72 million before the hack. The price of bitcoins plunged on news of the hack.⁷⁶ There are also security flaws at the network level though the threat here has mostly remained theoretical. Technically, if a person or more likely group of persons gains control of more than 50% of the total network hash power of the bitcoin network, they can invalidate transactions and/or double spend bitcoins from their own bitcoin addresses. Such an attack is unlikely to occur for a number of reasons. First, it is extremely expensive to amass sufficient computing power to launch such an attack. Secondly, such an attack will lead to widespread reluctance to accept bitcoins as payment, causing its value to plummet; a counterproductive effect for persons controlling sufficient nodes to launch such an attack as they are likely to hold a lot of bitcoins.⁷⁷ However, coding vulnerabilities in 'smart' contracts⁷⁸ that employ cryptocurrencies could also expose holders of cryptocurrencies to hacks such as that carried out against the DAO. It appears that the vaunted security of cryptocurrencies, through the use of cryptography, is limited to 'preventing double spending attacks or the forging of coins.'⁷⁹ This is confirmed on a careful reading of Satoshi Nakamoto's White Paper, the object of which was to 'propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate

⁷⁶ Amie Tsang (3 August 2016), Bitcoin Plunges After Hacking of Exchange in Hong Kong, *The New York Times*.

⁷⁷ See Joshua A Kroll, Ian C Davey and Edward W Felten, "The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries" *The Twelfth Workshop on the Economics of Information Security* (2013), 11-12.

⁷⁸ 'Smart' contracts are not really smart in the sense that artificial intelligence is smart. They are really simply the digital world's equivalent of vending machines and are perhaps more accurately labelled called 'automated' contracts. The manner of their automation is entirely dependent on human coding and therefore a smart contract is as dumb as its code: see Matt Levine (17 June 2016), Blockchain Company's Smart Contracts were Dumb, *Bloomberg* (<http://www.bloomberg.com/view/articles/2016-06-17/blockchain-company-s-smart-contracts-were-dumb>)

⁷⁹ Izabella Kaminska (4 August 2016), Bitcoin Bitfinex Exchange Hacked: the Unanswered Questions, *Financial Times* (<https://next.ft.com/content/1ea8baf8-5a11-11e6-8d05-4eaa66292c32>)

computational proof of the chronological order of transactions.’⁸⁰ The cryptographic protocols of the blockchain only promise to prevent double-spending. They provide *zero* protection from other forms of fraud, such as hacking, which is not only possible but commonplace. As the *Financial Times* reported, ‘[o]nline lists curated by bitcoin community members suggest bitcoin exchanges have been involved in up to 60 high-profile hacking incidents since the digital asset class was created in 2009. The true scale of the hacking problem, however, is hard to estimate.’⁸¹ This is despite bitcoin’s (and other cryptocurrencies) current miniscule scale in terms of transaction volume as compared to other payment services.⁸² More generally, it has been observed that, ‘[o]n an almost daily basis it seems major companies with whom citizens share their precious financial data and identities have been hit by external and internal attackers. Many have simply not had adequate basic protection measures in place; others have been caught short by the ever-changing inventiveness of hackers with which they cannot keep pace.’⁸³ Thus, ‘while antivirus software preciously detected most malware, it now detects only a minority of it.’⁸⁴ Online crime, leading computer security experts say, ‘has taken off as a serious industry since about 2004.’⁸⁵ According to these experts:⁸⁶

⁸⁰ Satoshi Nakamoto (October 2008), “Bitcoin: A Peer-to-Peer Electronic Cash System”, 1 <https://bitcoin.org/bitcoin.pdf> Retrieved 14 March 2016.

⁸¹ Izabella Kaminska (4 August 2016), Bitcoin Bitfinex Exchange Hacked: the Unanswered Questions, *Financial Times* (<https://next.ft.com/content/1ea8baf8-5a11-11e6-8d05-4eaa66292c32>)

⁸² Robert Grossman, Atanasios Mitropoulos and Jonathan Boise (2 April 2014), Sizing Up Bitcoin, *The Why? Forum* (<http://thewhyforum.com/articles/sizing-up-bitcoin>)

⁸³ The Cambridge Security Initiative, *Cash is King – The Digital Revolution: The Future of Cash* (2016), 23.

⁸⁴ Tyler Moore, Richard Clayton and Ross Anderson, ‘The Economics of Online Crime’ (2009) 23 *Journal of Economic Perspectives* 3, 5.

⁸⁵ Tyler Moore, Richard Clayton and Ross Anderson, ‘The Economics of Online Crime’ (2009) 23 *Journal of Economic Perspectives* 3.

⁸⁶ Tyler Moore, Richard Clayton and Ross Anderson, ‘The Economics of Online Crime’ (2009) 23 *Journal of Economic Perspectives* 3, 3-4. See also David S Wall, ‘Cybercrime, media and insecurity: The Shaping of public perceptions of cybercrime’ (2008) 22 *International Review of Law Computers & Technology* 45, 50-51.

In the old days, electronic fraud was largely a cottage industry, local and inefficient: a typical card fraudster ran a vertically-integrated small business. For example, he might buy a card-encoding machine, get a job in a shop where he could copy customers' cards, and then go out at night to steal cash from automatic teller machines (ATMs). ...

But now criminal networks have emerged – online black markets in which the bad guys trade with each other, with criminals taking on specialized roles (Thomas and Martin, 2006). Just as in Adam Smith's pin factory, specialization has led to impressive productivity gains, even though the subject is now bank card PINs rather than metal ones. [S]omeone who can collect bank card and PIN data or electronic banking passwords can sell them online to anonymous brokers at advertised rates of \$0.40-\$20.00 per card and \$10-\$100 per bank account (Symantec, 2008). The information needed to apply for credit in someone else's name, such as name, social security number, and birthday, fetches \$1 to \$15 per set. The brokers in turn sell the credentials to specialist cashiers who steal and then launder the money.

The Anti-Phishing Working Group, in its latest quarterly report, notes that the number of unique phishing websites detected per month rose from 48,114 in October 2015 to 123,555 in March 2016, a 250% increase over 6 months; the number of unique phishing e-mail reports increased from 99,384 in January 2016 to 229,265 in March 2016; and that there is an average of 227,000 new malware samples per day in the 4th Quarter of 2015, rising from an average of 225,000 per day a year ago.⁸⁷ While these statistics should be taken with a pinch of salt, as some members of the group have a vested interest in exaggerating the scale of the problem,⁸⁸ there is a distinct upward trend in cases of online fraud and even experts alive to the difficulties with statistics from the security industry acknowledge that the frauds are increasing in sophistication.⁸⁹ Fraudsters, it appears, are endlessly inventive. No system is immune from fraud. Often, they will target the weakest link in a system. As computer security expert, Bruce Schneier once remarked, 'Only

⁸⁷ APWG Phishing Activity Trends Report, 1st Quarter 2016 (published 23 May 2016).

⁸⁸ David S Wall, 'Cybercrime, media and insecurity: The Shaping of public perceptions of cybercrime' (2008) 22 *International Review of Law Computers & Technology* 45, 53.

⁸⁹ See also Tyler Moore, Richard Clayton and Ross Anderson, 'The Economics of Online Crime' (2009) 23 *Journal of Economic Perspectives* 3.

amateurs attack machines; professionals target people.⁹⁰ In the case of bitcoins and other cryptocurrencies, running off blockchain technology, the weakest link will often be the end users (including cryptocurrency exchanges) rather than the integrity of their ledgers, which appear to remain largely secure. In 2014, Ciaran Martin, the Director General for Cyber Security at GCHQ observed that, apart from the threat from cybercrime, cyber risk in the financial sector can also arise from terrorism, a major conflict between states that draws in the UK, and a major accident or natural event.⁹¹ Presumably, such attacks are aimed not so much at financial gain but at destabilising the economy of the victim state. If holders of cryptocurrencies (fiat or otherwise) are not protected from hacking, then any economy that is dependent on such cryptocurrencies (presumably greater in the case of fiat cryptocurrencies) will be vulnerable to such exceptional attacks.

The increasing concern over cybercrime stands in marked contrast to the '[m]arked reductions [that] have been seen in property crime since peak levels in the 1990s'.⁹² Some of the theories on why property crime has fallen include 'significant improvements in forensic and other crime scene investigation techniques and record keeping, such as fingerprinting and DNA testing' as well as 'changes (real or perceived) in technology such as CCTV', both of which may have a deterrent effect as they are perceived to increase the likelihood of conviction.⁹³ By contrast, cyber criminals are, at least presently, at an advantage compared to the law enforcement agencies. '[O]nline crime usually crosses

⁹⁰ Bruce Schneier (15 October 2000), *Semantic Attacks: The Third Wave of Network Attacks*, *Crypto-Gram* (<https://www.schneier.com/crypto-gram/archives/2000/1015.html#1>)

⁹¹ Ciaran Martin (15 July 2014), *Speech at the Financial Services Summit 2014* (<https://www.gchq.gov.uk/speech/director-general-cyber-security-gchq-speaks-financial-services-summit-2014>)

⁹² Office for National Statistics, *Statistical Bulletin, Focus on Property Crime: 2014-2015* (26 November 2015) (<http://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/focusonpropertycrime/2014to2015>)

⁹³ Office for National Statistics, *Statistical Bulletin, Focus on Property Crime: 2014-2015* (26 November 2015), '5. Existing Theories on Why Property Crime has Fallen' (<http://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/focusonpropertycrime/2014to2015>)

national boundaries. Existing mechanisms for international police cooperation are expensive and slow – designed to catch the occasional fugitive murderer, but not for dealing with millions of frauds at a cost of a few hundred dollars each.⁹⁴ Furthermore, whereas ‘conventional crime is generally committed by marginal members of society’, cyber criminals ‘tend to be educated and capable, but they live in societies with poor job prospects and ineffective policing.’⁹⁵ Cybercrime, as with so much activity related to the Internet, is perceived by the criminals as being relatively anonymous.⁹⁶ It has even been suggested that another barrier to deterrence lies in ‘the inability of key stakeholders in criminal justice systems to grasp fundamental aspects of technology aided crime.’⁹⁷ Thus, although reports of serious cybercrime are escalating, there has not been a corresponding increase in conviction rates, ‘with many investigations and prosecutions failing to get off the ground’.⁹⁸

It is against this factual backdrop that we must examine the legal risk that follows from holding cryptocurrency. The Bitfinex hack is instructive in terms of our study. As a lawyer

⁹⁴ Tyler Moore, Richard Clayton and Ross Anderson, ‘The Economics of Online Crime’ (2009) 23 *Journal of Economic Perspectives* 3, 16.

⁹⁵ Tyler Moore, Richard Clayton and Ross Anderson, ‘The Economics of Online Crime’ (2009) 23 *Journal of Economic Perspectives* 3, 6.

⁹⁶ Monty Raphael QC, Celia Marr and Kate Parker, ‘Online, Invisible and Criminal’, *Fraud Intelligence* (August/September 2015), 1. (<http://www.petersandpeters.com/wp-content/uploads/2015/10/Online-invisible-and-criminal-Fraud-Intelligence.pdf>) See also Mohamed Chawki et al, *Cybercrime, Digital Forensics and Jurisdiction* (2015), Chap 7 ‘Anonymity, Privacy and Security Issues in Cyberworld’. Strictly speaking, this is not so much anonymity but the lack of resources available to follow the digital trail: see David S Wall, ‘Cybercrime, media and insecurity: The Shaping of public perceptions of cybercrime’ (2008) 22 *International Review of Law Computers & Technology* 45, 51. In relation to bitcoin, see Andy Greenberg (29 January 2015), ‘Prosecutors Trace \$13.4m in Bitcoins from the Silk Road to Ulbricht’s Laptop’, *Wired*.

⁹⁷ Cameron S D Brown, ‘Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice’ (2015) 9 *International Journal of Cyber Criminology* 55, 56.

⁹⁸ Cameron S D Brown, ‘Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice’ (2015) 9 *International Journal of Cyber Criminology* 55, 56.

explained to the *Financial Times*, ‘With Bitfinex, user wallets were segregated. As a result, the relationship was seemingly more custodial in nature. In other words, the hack resulted in the theft of users’ property’.⁹⁹ This particular *Financial Times* report is equal parts tantalising and frustrating. It drew an analogy to a thief stealing contents from users’ safety deposit boxes rather than the contents of their bank accounts. Quoting the same unnamed lawyer, the report added, ‘[t]his matters because in the bank account situation, losses are necessarily socialised whereas socialising deposit box losses would be theft’. Whilst the result is mostly correct (losses are not always socialised)¹⁰⁰ if indeed the ‘stolen’ bitcoins were held on trust,¹⁰¹ it fails to explain why the legal analysis would lead to a different result than the ‘theft’ of bank money from an ordinary bank account. A custodial relationship, in common law jurisdictions, would either take the form of a bailment or a trust. In the case of cryptocurrencies, which are incorporeal property if they are property at all, it would seem that this relationship cannot be explained as a bailment,¹⁰² which leaves the trust analysis. If trust property is ‘stolen’, then it is its beneficial owner that bears the loss, subject to possible claims against the trustee for breach of duty (in this case, a duty of care). The reason why money ‘stolen’ from a bank

⁹⁹ Izabella Kaminska (5 August 2016), Legal Tussle Looms for Bitcoin Holders in Hacked Bitfinex, *Financial Times* (<https://next.ft.com/content/c3b9f89c-5b18-11e6-9f70-badea1b336d4>) Contra Clare Baldwin (6 August 2016), Bitfinex Exchange Customers to Get 36 Percent Haircut, Debt Token, *Reuters* (<http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10I06H>)

¹⁰⁰ Cases involving gross negligence on the part of the customer are not socialised. Consider the scenarios derived from decisions of the UK Financial Ombudsman chosen by the authors of this international comparative report on bank fraud reimbursement: Ingolf Becker et al, ‘International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms’, *Workshop on the Economics of Information Security (WEIS)*, 13-14 June 2016, Berkeley, CA, USA, at 12-13.

¹⁰¹ Segregation and non-segregation are merely indicators of the legal relationship (in this case, trust or personal obligation) between the exchange and its customers. The correct classification will always turn on a careful examination of the contract between the parties. Cf Clare Baldwin (6 August 2016), Bitfinex Exchange Customers to Get 36 Percent Haircut, Debt Token, *Reuters* (<http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10I06H>)

¹⁰² Norman Palmer et al, *Palmer on Bailment* (3rd ed, 2009), 1-006. But see Chap 30.

account is not treated this way is because, as we have seen, the statement of accounts does not represent the legal rights of the bank customers (or any rights at all). It is merely an imperfect record of the customers' rights. It is only upon withdrawal of the 'stolen' money that a cyber-theft is effective and the money so withdrawn belongs not to the customer but the bank. When a customer deposits money (in whatever form) with a bank, any legal rights to *that* money is transferred to the bank in exchange for an *in personam* claim against the bank. Account holders thus do not hold any property rights to any particular assets belonging to the bank. Rather, they all have *in personam* claims (debt claims) against the bank (reflected as its liabilities, not assets). As they do not hold any particular assets in the bank, nothing can be stolen from them in the conventional sense of the word.

Consider a bank with four customers: Alan, Beatrice, Charles and Diana. Just as Alan's account with the bank is merely a debt claim against it, the same is true of Beatrice, Charles and Diana. These accounts represent liabilities owing by the bank; they do not represent claims on any particular assets belonging to the bank. Hence, the bank is free to use the £50 deposited by Diana to repay Alan if his account has been hacked. This is because, upon deposit, the £50 belongs to the bank, not Diana. It is for this reason that banks *may* (not must or will) socialise losses among account holders. It may not do so in two circumstances. First, depending on the terms of its banking contract and the circumstances surrounding a particular hack, a bank may try to transfer the loss to the particular customer, perhaps on the grounds of the customer's gross negligence. Secondly, provided its assets still exceed its liabilities, there is simply no cause to 'socialise' the loss. It is only in the event that the bank is insolvent and unable/unwilling to transfer the loss to the particular affected customer that the loss is 'socialised' or 'shared' with unaffected customers. This 'socialisation' of loss is in effect the flipside of not having any legal interest *in* an asset belonging to the bank which can be stolen. While no particular asset held by the bank belongs to the customer, the customer runs the risk that the bank may become insolvent. While the risk of insolvency is minimised through banking regulation, including inter alia, reserve ratios or capital requirements and

deposit insurance,¹⁰³ it is not and cannot be eliminated.¹⁰⁴ Where an exchange ‘holds’ bitcoins for its customers in the way that a bank holds money for its account holders, the bitcoin holders are exposing themselves to the insolvency risks of the exchange. Interestingly, by preferring to socialise the losses, Bitfinex appears to have taken the view that this is the legal arrangement they had with their customers, contrary to the assessment of the lawyer quoted in the *Financial Times*.¹⁰⁵ Where, however, an exchange holds bitcoins in a custodial capacity, the bitcoin holders exchange the insolvency risk of the exchange for risk of loss/destruction of *their* bitcoins. If the exchange were to become insolvent, they can simply ‘withdraw’ *their* bitcoins without suffering any loss. Nevertheless, as we have already observed, it is not true that a customer of Bitfinex is entirely without remedy against Bitfinex even if their bitcoins were held on trust rather than simply owed to them. If it can be demonstrated that Bitfinex was negligent in its custody of the relevant bitcoins, it will be liable to its customers who suffered a loss through the hack. Whether it will have sufficient assets to reimburse these customers is, of course, an entirely different matter. This is because it must be recalled that if a trust analysis is correct, most if not all of the other bitcoins it holds will also likely belong beneficially to its other customers (whose wallets were not hacked). A direct holder of cryptocurrencies would be in a similar position to an account holder at Bitfinex whose account has been hacked. Indeed, this holder would be even more vulnerable (legally as a matter of risk) because there would simply be no entity at all to pursue a negligence claim against. If the loss was the result of carelessness, it was the holder’s own carelessness.

¹⁰³ Section 213 of the Financial Services and Markets Act 2000 (c 8) requires the Financial Services Authority to set up a Financial Services Compensation Scheme.

¹⁰⁴ See, eg, Charles W Calomiris, ‘Bank Failures, the Great Depression, and Other “Contagious” Events’ in Allen N Berger, Philip Molyneux and John OS Wilson (eds), *The Oxford Handbook of Banking* (2nd ed, 2014), 721.

¹⁰⁵ Clare Baldwin (6 August 2016), Bitfinex Exchange Customers to Get 36 Percent Haircut, Debt Token, *Reuters* (<http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10I06H>). If its assessment of the legal effect of its arrangement with its customers is wrong, then Bitfinex is exposing itself to lawsuits from customers whose wallets were *not* hacked.

For such direct holders of cryptocurrencies, there are nevertheless a number of parties that it may wish to pursue, provided they can be identified. First, it is likely that any hack would involve acquiring the holder's private key. This would expose the hacker, provided he/she/they can be identified, to a claim for breach of confidence. Secondly, they may wish to trace their stolen bitcoins or other cryptocurrency in the hopes of recovering them or at least their value. With the passage of time, this party is unlikely to be the hacker. Whether this can be done will depend in part on the cryptocurrency concerned and in part on how the law chooses to respond to cryptocurrency as property. The traceability of subsequent holders of cryptocurrency will depend on the anonymity protocols of the particular cryptocurrency. Bitcoin, it should be remembered, is not completely anonymous but only pseudo-anonymous. While the identity of the address holder is not known, all transactions related to the address are in fact transparent and tracked in the blockchain. With the appropriate information, including publicly available information, it is possible to track some bitcoin transactions.¹⁰⁶ It has been estimated that 'almost 40% of users can be, to a large extent, recovered even when users adopt privacy measures recommended by Bitcoin.'¹⁰⁷ Some cryptocurrencies, such as darkcoin,¹⁰⁸ are designed to offer far greater anonymity than bitcoin. This will make tracking 'stolen' darkcoins far more difficult than tracking 'stolen' bitcoins. Even assuming they are successfully tracked, holders face great uncertainty in terms of the protection that the law will afford them. At one extreme, though we consider this unlikely, especially if cryptocurrencies achieve mainstream adoption, the law may adopt the attitude of the adherents to Ethereum Classic. In other words, the code is law and immutability means immutability. There is no known property law regime that operates in this fashion – to a property lawyer, this is indefeasibility on steroids. At the other extreme, the common law courts could apply the principle of *nemo dat quod non habet*¹⁰⁹ strictly so that subsequent

¹⁰⁶ Andy Greenberg (29 January 2015), "Prosecutors Trace \$13.4m in Bitcoins from the Silk Road to Ulbricht's Laptop", *Wired*.

¹⁰⁷ Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun, "Evaluating User Privacy in Bitcoin" in Ahmad-Reza Sadeghi (ed), *Financial Cryptography and Data Security* (2013), 34.

¹⁰⁸ Andy Greenberg (21 May 2014), "Darkcoin, the Shadowy Cousin of Bitcoin, is Booming", *Wired*.

¹⁰⁹ No one gives what he does not have.

holders of the 'stolen' cryptocurrencies are liable to their 'true owners' for their value in an action emulating the tort of conversion that exists for corporeal money, regardless of whether they are bona fide purchasers of the same. This is possible because the key attribute of money in the legal system is its attribute of currency. This involves 'the creation of a fresh indefeasible title in a person who receives money as a bona fide purchaser for value.'¹¹⁰ By tempering the harsh *nemo dat* rule with such a robust defence, the law indirectly supports the economic function of money as a medium of exchange.¹¹¹ Its applicability to cryptocurrencies may be doubted, and thus the harsh *nemo dat* rule may be applied in full (at least in some instances), for two reasons. First, 'the question whether the law should treat a certain kind of asset as money ... can only be answered by observing whether the community where it circulates treats it as such.'¹¹² It is far from clear that bitcoin, to say nothing of all its competing cryptocurrencies, has come to be generally acceptable as a medium of exchange. Secondly, even where a particular class of asset has acquired the attribute of currency, the bona fide purchase rule 'would not apply when money was transferred as a specific good or as a commodity'.¹¹³ Thus, in *Moss v Hancock*, a second-hand jewellery shop bought a stolen five-pound gold piece for five sovereigns. In determining whether the shop was liable to restore the coin, the court rejected the shop's invocation of the bona fide purchase defence because the gold piece had been sold to the shop as a dealer in curios rather than paid as money for goods or services. A significant segment of the cryptocurrency community treats bitcoins and similar cryptocurrencies as investments rather than as a medium of exchange. This explains in part the Chinese dominance of bitcoin computing power. As Bobby Lee, chief executive of BTCC, explained to *The New York Times*, 'For one thing, the Chinese government had strictly limited other potential investment avenues, giving citizens a hunger for new assets. Also, ... the Chinese loved the volatile price of Bitcoin, which gave the fledgling currency network the feeling of online gambling, a very popular activity in

¹¹⁰ David Fox *Property Rights in Money* (2008), 19.

¹¹¹ David Fox *Property Rights in Money* (2008), Chap 2.

¹¹² David Fox *Property Rights in Money* (2008), 8.

¹¹³ David Fox *Property Rights in Money* (2008), 20.

China.’¹¹⁴ Such cryptocurrency investors may find that, even if some cryptocurrencies achieve the legal status of currency, they may not take advantage of the bona fide purchase rule that comes with that status. This means that, for pure investors in bitcoin, their investment carries the risk that they become liable to the ‘true owners’ of any ‘stolen’ bitcoin that they may acquire, even if they did so bona fide at full market price.

6. CONCLUSION

It is early days yet in the development and adoption of cryptocurrencies. While a number of central banks have expressed interest in cryptocurrencies, including fiat varieties of the same, their suitability for wide adoption and/or eventual replacement of either corporeal money or bank money is a matter that deserves closer reflection. Particularly disconcerting are the frequency of hacks of cryptocurrency exchanges and the lack of information of hacks at the level of individual holders. This is despite the fact that cryptocurrencies remain very much a niche product. It is thus difficult to estimate the scale of the problem should fiat cryptocurrencies be adopted, or worse mandated, as replacement for corporeal money. Presumably, the property status of fiat cryptocurrency will not then be in issue since Parliament can simply enact laws to confirm its status. However, differing in nature as it does from bank money, which many laypersons also regard as digital money, losses stemming from cybercrime in the form of hacking will hit individual holders particularly hard whereas hacks of bank accounts are typically borne by banks and spread to its other depositors in the form of fees and bank charges. Mandatory fiat cryptocurrencies will provide an opportunity for large scale lucrative fraud. The risk of loss through ‘ownership’ of what may be the first true form of digital money would also be difficult to guard against because unlike theft of corporeal money, cyber theft is an unbounded crime and there is no requirement of physical proximity between perpetrator and victim. Cybercrime not only removes the need for proximity between perpetrator and victim, the nature of the Internet gives perpetrators a far wider reach. Whilst there are only so many burglaries a skilled burglar can commit in any given

¹¹⁴ Nathaniel Popper (29 June 2016), How China Took Centre Stage in Bitcoin’s Civil War, *The New York Times*

(<http://www.nytimes.com/2016/07/03/business/dealbook/bitcoin-china.html>)

time, automation allows the perpetrator of a cybercrime to reach a significantly greater number of victims so that relatively few offenders can reach a very large number of victims in a very short amount of time.¹¹⁵ Not only is there likely to be an explosion of cyber-theft, considering current trends in cyber-crime,¹¹⁶ it is likely that the elderly are likely to be disproportionately exposed to such losses from a switch to cryptocurrency. This is unsurprising since they are likely to have the most wealth whilst at the same time being among the least tech savvy of all users.¹¹⁷ This means that any central bank which is serious about issuing fiat cryptocurrency must consider seriously the problem of cybersecurity at the individual user level (a problem that may well prove intractable) or instituting some form of insurance for loss through hacking, or both. It must also seriously consider phasing in any cryptocurrency whilst maintaining the continued use of coins and banknotes, though this will somewhat diminish the appeal of cryptocurrencies as a tool for the easy application of negative interest rates as compared to corporeal money.¹¹⁸ Perhaps even more importantly, the relevant officials looking into developing fiat cryptocurrencies should beware the hype surrounding the blockchain technology that underpins bitcoins and other cryptocurrencies. While promoters vigorously proclaim the security of ledgers operated using the blockchain, they often fail to mention that the

¹¹⁵ David S Wall, 'Cybercrime, media and insecurity: The Shaping of public perceptions of cybercrime' (2008) 22 *International Review of Law Computers & Technology* 45, 55.

¹¹⁶ Eric L Carlson, 'Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting them Follow' (2007) 14 *The Elder Law Journal* 423, 432-433. See also National Fraud Intelligence Bureau and City of London Police, *Cyber Crime – Victimology Analysis* (February 2016) (<https://www.cityoflondon.police.uk/news-and-appeals/Documents/Victimology%20Analysis-latest.pdf>).

¹¹⁷ Eric L Carlson, 'Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting them Follow' (2007) 14 *The Elder Law Journal* 423, 424, 428-9.

¹¹⁸ It is notable that one of the earliest mention of cryptocurrencies, specifically bitcoins, by a Bank of England official was that by Andrew Haldane, the Chief Economist, as a speech given at the Portadown Chamber of Commerce, Northern Ireland: Andrew Haldane (18 September 2015), *How Low Can You Go?* (<http://www.bankofengland.co.uk/publications/Documents/speeches/2015/speech840.pdf>)

blockchain's system of cryptographic proof is directed *exclusively* towards the problem of double spending. The blockchain technology provides *zero* protection against any other kinds of fraud. In other words, the blockchain protects the network from user fraud but does not protect users from other frauds. However, unless such other frauds are suitably addressed, presumably through the use of other technological innovations, the issue of fiat cryptocurrency must be regarded as extremely foolhardy. In the meantime, the only proper advice for persons looking to invest in/use private cryptocurrencies must surely be *caveat emptor*.