1 Cryptocurrencies: The Underlying Technology

Sarah Green

From: Cryptocurrencies in Public and Private Law
Edited By: David Fox, Sarah Green

Content type: Book content
Product: Financial Law [FBL]
Published in print: 14 March 2019
ISBN: 9780198826385

Subject(s):
Electronic money — Intermediated securities — Currency

(p. 1) 1 Cryptocurrencies: The Underlying Technology

I. Introduction

1.01 The cryptocurrencies discussed in this volume—of which Bitcoin was the pioneer—have a specific set of characteristics and are able to exist only because of a particular series of technological developments. These cryptocurrencies are based on decentralization and consensus: two features which also give rise to most of the legal issues analysed in this volume. A sound understanding of decentralization and consensus is therefore necessary to engage with what follows. There are now several different cryptocurrencies and distributed ledger platforms in addition to Bitcoin and its Blockchain. These are not all identical in technological terms, but they do all have common features. These common features which represent what is significant about this potentially disruptive technology are the focus of this introductory chapter.

II. Decentralization and Distributed Consensus

1.02 Decentralization and distributed consensus are the crucial components of cryptocurrencies, and they are the principal features which distinguish them from (p. 2) those forms of electronic payments that use intermediaries and electronic bank money, such as PayPal, WorldPay, and BACS. These characteristics also explain why cryptocurrencies are often described as ‘trustless’, meaning that transacting parties need not have any trust in one another in the real world, so long as they trust the payment protocol (which, for reasons that will soon become apparent, they probably should).

1.03 Decentralization in this context simply means that everyone who might want to use the currency, and so has a copy of the relevant software, also has a copy of the ledger. The ledger is a record of *every* transaction made using that currency, and each computer operating the software (known as a *node*) has a copy of the entire thing: from the beginning (the ‘Genesis Block’) to today’s latest block. This is where the term ‘Distributed Ledger Technology’ (DLT) comes from: Blockchain, which was created to underpin Bitcoin, was the first distributed ledger, but there are now distributed ledgers of several different forms. Common to all of them, however, is the idea that all participants have access to the full history of transactions made using that protocol. This is a novel way of dealing with the ages-old double-spend problem. Historically, the challenge of how to prevent double spending has been met in two ways: the first is by using physical tokens, whose corporeal form physically prevents their being spent more than once, and the second is by employing an independent third party, such as a bank, to keep a record of transactions and their effects on the subsequent spending power of the parties involved.

1.04 Cryptocurrencies achieve the same result by sharing information with every user and ensuring that the information so shared is perfectly synchronized. This way, ‘coins’ cannot be spent twice because everyone would know that this is what was being attempted, and the consensus necessary for validation and recording would not be reached. Security is thus achieved through complete transparency, and distributed ledgers have no need for any centralized record keeping, nor for any third-party intermediary to verify the integrity of transactions. In other words, ‘total validation replaces central control’.[1]

1.05 Such transparency is achieved through what is known as 'distributed consensus protocol', and this is characterized by two features:

(a) all computers on the network (referred to as 'nodes') must agree on which transaction data are ultimately recorded on the ledger, and

(b) the transaction data must have been generated by an honest node. [2]

(p. 3) **1.06** The question remains how any of this can be achieved. One method, used by Bitcoin, is known as *proof-of-work*, and this allows nodes to reach a consensus on which transactions to record and in which order to do so. (The order is of course all-important, as it is with any spending pattern, since what you have already spent determines how much you can spend in the future.) Proof-of-work is the means by which nodes persuade other nodes that the block of transactions that they wish to add to the chain is legitimate and should be trusted. The work involved here is the cryptography: the solving of a mathematical puzzle. This puzzle is of a very specific type. The optimum way of solving it is simply to work through very large numbers of trial and error iterations. In other words, lawyers might say that it is a difficult case, but not a hard one. It is clear what needs to be done, but doing it takes an immense amount of computational power[3] simply to work through the many repetitions of the same calculation, each time trying a different input. The puzzle is known as a *hash puzzle*, and success requires finding the input necessary for a function to produce a specified output. The hash function itself, which is the crux of this whole process, could be described in non-mathematical terms as a function which takes an input and produces an output that will look nothing whatsoever like the input.[4] In fact, it is practically impossible to discover the original input simply by looking at the output, unless you know the hash function. Diedrich has provided the following illustration of how hashes work.[5] There are different hash algorithms. One hash algorithm that was once popular was called MD5. For example, this text:

> i. MD5's designer Ron Rivest has stated "md5 and sha1 are both clearly broken (in terms of collision resistance)". So MD5 should be avoided when creating new protocols, or implementing protocols with better options. SHA256 and SHA512 are better options as they have been more resilient to attacks (as of 2009).
>
> ii. has the MD5 hash:
>
> iii. ed7f56281b8d079ff101009105f75b44
>
> iv. … The hash ed7f56281b8d079ff101009105f75b44 can be used as a unique id for the above text, for two reasons:
>
> If any punctuation or word was changed, you would get a different hash for it.
>
> You will not for your life be able to find another text that results into exactly this hash.[6]

(p. 4) **1.07** Crucially, the same hash function, applied to identical inputs, will *always* produce the same output. Applying the same hash function, however, to an input which is different from the original in only a miniscule detail will nonetheless result in a completely different output. This explains why the only way to solve such puzzles is through repeated trial and error: there are no shortcuts or clues provided by previous work, and the results of previous attempts are not in any way cumulatively helpful. Instead, nodes who wish to add a block to the chain first take a set of transactions that have been broadcast[7] across the network. They then add to this something called a '*blockhash*'. A 'blockhash' is the output generated when the hash function is applied to the whole of the previous block in the chain. This blockhash serves therefore as a unique identifier of all of the data in that previous

block, and so is what links the blocks (hence the term ‘chain’) and at the same time makes the protocol so secure: embedding this unique summary of the previous block’s data in the following block, and, therefore, in all future blocks,[8] makes the blockchain practically tamper-proof. If any node wants to alter or modify the content of any given block, it would also have to rehash all of the blocks which follow it, and compete to persuade all nodes (who would be working on the basis that the original date were correct) that the new reality was the right one. This is so difficult, particularly in terms of computational power, as to be well-nigh impossible in the current environment.

1.08 The proposing node, which has at this point taken the set of transactions it wishes to verify, and added the blockhash,[9] then starts the real work: it also adds a value as the mystery input, which is known in cryptography as a ‘nonce’. It then hashes all of this together (which means applying a specific and consistent hash function, that in the case of Bitcoin is called SHA256) and keeps doing this, using a different nonce each time, until it gets an output with the ‘correct’ number of leading zeros.[10]

> At the heart of this scheme is the fact that a nonce is hard to find but easy to verify. While it routinely takes trillions of trial-and-error calculations to find it, it requires but one calculation to verify it: to test that a nonce is in fact resulting into a hash with the required number of leading zeros when added to the block data that it was found for.[11]

(p. 5) **1.09** This is known as ‘trapdoor’ maths because of its one-way structure; it is very difficult to find the answer but, once you have the answer, it is very easy to verify that it is the right one. A simple analogy can be made with the combination to a briefcase lock. Anyone wishing to open the suitcase without knowing the combination will have to try (probably) very many attempted combinations to find the one which opens the case. Once she has found it, however, it is very easy for someone else to verify that she has found the correct combination: the verifier simply needs to put that combination into the briefcase dial and see if it opens. The result is a binary one—pass or fail. Similarly, once a node has found what it believes to be the right nonce, the other nodes verify that it is correct by simply applying it to the publicly available data. If this produces the same output (the one with the required number of leading zeros), verification is complete. Once this happens, the proposed block is added to the chain, and the transactions in it are confirmed.[12]

1.10 This, however, is not the only thing which happens when the block gets verified. Another of Bitcoin’s revolutionary qualities is its alignment of self-interest with altruism. Verifying blocks is hard grind and very expensive in computational terms, yet it is essential to the continuation and security of the system. So, when a node successfully adds a block to the chain, it is rewarded with an output of bitcoin. In the Bitcoin protocol, the verification process is known as ‘mining’, and it is simultaneously the means by which new coins are minted.[13] This is a system, therefore, in which self-interest works in favour of the collective interest, and the two are mutually reinforcing.

III. The Chapter Contributions to this Book

1.11 It is clear, therefore, that these technological developments have the potential to disrupt conventional payment mechanisms and change the way that parties transact and accrue assets. Largely, that disruption is already happening. The significant number of payment transactions already being carried out using cryptocurrencies means that the law governing those transactions and their results needs to develop accordingly. The various legal responses that have so far emerged have made it apparent that a consistent and

coherent set of legal principles would make the treatment of cryptocurrencies both easier and more effective.

1.12 The chapters in this book each consider a particular area of public or private law, and offer either a solution to or a workable means of approaching the problems that have either already arisen or are bound to arise soon in their application to cryptocurrencies. Although each author takes on a specific inquiry, there are (p. 6) some recurrent themes which underlie many of the legal challenges relating to cryptocurrencies, and which sometimes call for differing responses, dependent either upon the jurisdiction and background of a particular legal system or upon the specific demands of a particular context. These are the questions of whether cryptocurrencies fit the definition of property and whether they count as money for legal purposes.

1.13 In Chapter 2, the first substantive chapter of the volume, Green looks expressly at the question of whether, for the specific purposes of English private law, cryptocurrencies should be classed as money. This chapter considers the implications of cryptocurrencies being excluded from the definition of 'money' for the legitimate expectations of contracting parties: the classification of a transaction as one of sale depends on its being made for money, and not for money's worth. An exchange of goods for anything other than money would apparently fall, at least on current English authority, to be classed as one of barter or exchange, and this would exclude it from the protection provided by the Sale of Goods Act 1979 and from the remedial advantages which accrue to sellers under a contract deemed to be one of sale. Whilst the exclusion of such a transaction from the protective purview of sales law would seem to run counter to the expectations of contracting parties, Green suggests that, unless the private law definition of 'money' is relaxed, cryptocurrencies will not meet the requisite criteria. As is recognized by several of the chapters in this volume, there is little difficulty in regarding cryptocurrencies as a medium of exchange, but the other characteristics currently regarded as necessary for the recognition of such media as 'money' are less obvious. It is, as is also made clear in Proctor's Chapter 3, simply not the case that cryptocurrencies function as units of account. The present volatility in their worth against conventional state-denominated currencies renders them an unreliable store of value. Green's conclusion is that, in the narrow context of private law transactions, the function of a currency as a medium of exchange should be the criterion to which the law should pay the most attention, thereby allowing for transactions made with certain cryptocurrencies to count as contracts of sale. Whilst the conclusion of this chapter is based on an expansion of the private law definition of 'money', it would also be to reach the same result by expanding the definition of 'sale', so that payment in a conventional state-denominated form of currency should not be required. This could even take the form of an explicit statutory inclusion of cryptocurrencies, which would avoid the need to disrupt the longstanding definition of 'money', particularly when this could lead to a potential dichotomy between private law money and public law money.

1.14 Proctor's Chapter 3 picks up the analysis from this point, and examines international and public law conceptions of money. The difference in perspective of this chapter from the last is clear: whilst the use of cryptocurrencies as a medium of exchange can be liberating for private individuals, the same activity is, from the State's perspective, a threat to its monopoly over currency, and to its (p. 7) corresponding ability to regulate the cost of credit. Proctor's analysis considers the State theory of money, but also makes comparative reference to the Societary theory of money, which has received less legal recognition than the State theory, but which nonetheless provides an important empirical dimension to the acceptance of any commonly accepted medium of exchange as money.

1.15 Despite the reference in the title of the chapter to public international law conceptions of money, it is clear that there is in fact no such thing. Money is regarded by public international law as whatever domestic systems determine it to be. That said, there are other international definitions which could be seen to circumscribe a State's ability to exclude cryptocurrencies from its definition of money for all purposes. Here, Proctor's discussion returns to the theme of property recurrent throughout this volume, and, in this chapter, specifically to Article 1, Protocol 1, of the European Convention on Human Rights. Proctor makes it clear that cryptocurrencies form a new asset class and, as such, a species of property or possession, thereby requiring States to consider the protection of holders' property interests when regulating their use and holding. In Proctor's view, this would seem to be the most pressing international and public law concern for the time being, since the level at which cryptocurrencies are currently used is, he suggests, not yet high enough to disrupt financial markets or to require a consequent shift in the public international law approach to them.

1.16 Zellweger-Gutknecht's contribution in Chapter 4 segues into Proctor's analysis in dealing specifically with the regulatory regime for cryptocurrencies and other value data. 'Value data'—the existence of which has been made possible by the advent of distributed ledger technology—is defined by Zellweger-Gutknecht as assets which are both 'excludable and rivalrous'. Both are essential characteristics in a commercial and legal environment in which tangibility (which is intrinsically excludable and rivalrous) has ceased to be the touchstone of value. Here, Zellweger-Gutknecht uses 'excludable' to refer to data from which the holder can completely exclude others, thereby giving her effective possession of it and the value which derives from it. Her definition of 'rivalrous' is that which can be consumed only once, or once at a time, and so is not subject to the double-spend problem. Zellweger-Gutknecht argues that these characteristics, and the consequent ways in which value data perform as assets, mean that the legal regime to be applied to them need not differ greatly from that currently applied to assets that are more conventional. Whilst conventional currencies are lodged with trusted intermediaries, the trusted element of a cryptocurrency holding is the technology itself.

1.17 At this point, we see another recurrent theme of the book: the existence of a functional analogy between cryptocurrencies and conventional currencies, despite the obvious physical and technical differences between the two. The legal regime to which Zellweger-Gutknecht refers here is the rules relating to segregation rights (p. 8) and the bearing of insolvency risk. If, she argues, parties are willing to trust the technology in the same way in which they trust an intermediary institution such as a bank, then applying established rules to the transaction makes sense. Such parties do after all have the freedom to contract using the mechanism of their choice. The pertinence of this analogous approach is fortified by Zellweger-Gutknecht's observation that the nature of transactions in value data is very similar in function to that of conventional transactions. Both consist of an extinction of value in one location and a corresponding increase elsewhere.

1.18 Dickinson's Chapter 5 on the conflict of laws implications of cryptocurrencies marks the transition to the next chapters of the volume. It deals with the cross-jurisdictional underpinnings to many of the private law questions that follow. Given the inherently global nature of cryptocurrencies, the reach of Chapter 5 is especially significant. The optimistic tenor of Dickinson's analysis is that, despite their novel form, cryptocurrencies do not require the formulation of wholly new solutions to the issues they present. Rather, what is needed is the careful selection of devices from the existing private international law toolbox.

1.19 The conflict of laws is principally concerned with rules of jurisdiction and applicable law: the former to decide whether an English court has the competence to decide a particular case, and whether it will do so, and the latter to determine which national law or laws to apply to the dispute. The most obvious issue which arises in relation to cryptocurrencies is that such questions have historically been resolved by reference to physical location: either of the parties or of their actions. Such an inquiry seems inauthentic in relation to transactions made in cryptocurrencies, both because the transaction itself has no obviously relevant tangible presence and because the identity of the parties, given the potentially pseudonymous nature of cryptocurrency exchange, will make the location of the actors very difficult. Nonetheless, Dickinson cautions against overstating the problems this causes, and makes the crucial point that there is in any event no 'one-size-fits-all' solution to the treatment of transactions in cryptocurrencies. It is important, both for the purpose of private international law and for other legal inquiries, to pay attention to the specific functional features of the transaction concerned, in the same way that the law currently differentiates between different types of transaction made in the conventional way. Where, for instance, a transaction is made between two individuals on a contractual basis, the settled means of resolving contractual disputes can apply. Equally, where an actor has behaved wrongfully in relation to another by, for instance, appropriating property, the location of that action can be of as much assistance as it has been in the past. Notwithstanding the virtual nature of the currencies themselves, the fact that the parties maintain a physical presence in the world means that rules relating to physical location and territorial connection remain as valuable in relation to cryptocurrencies as they are in any other private international law problem. Dickinson gives a picture of how courts can approach cryptocurrency transactions, as well as their creation or 'mining', without causing (p. 9) undue disruption to existing private international law reasoning. In so doing, he describes what parties to cryptocurrency transactions actually hold as a result of their participation, something which is by no means obvious. He argues that the participants have a legitimate expectation, founded on the technology of the system, that the consensus rules will not be changed so as to deprive them of their association with particular units of that currency. This provides a very useful concept to carry forward into the analysis which follows it.

1.20 Fox's contribution in Chapter 6 deals with the characterization and treatment of cryptocurrencies in the common law of property. He makes it clear why this matters, even though users of cryptocurrencies rarely show much interest in legal regimes that may apply to their transactions. Property law is default law, and so it should apply to their transactions unless the parties exclude its operation. This analysis links with the ideas in the chapters of both Green and Dickinson. Fox takes the view that cryptocurrencies are best dealt with through the application and analogical development of existing legal doctrine rather than through the wholesale creation of new concepts. For the common law of property, this would involve abandoning the long-standing, but increasingly untenable, rule that the only objects of property are choses in action and choses in possession. Just as Zellweger-Gutknecht argued that cryptocurrencies have excludable and rivalrous characteristics, Fox explains how the substance and function of cryptocurrencies tell us more about their amenability to a property analysis than does their virtual form. As he points out, even the rules of tracing and derivative transfer of title could be adapted to apply to cryptocurrencies. In common with both Green and Proctor, Fox contends that cryptocurrencies do not meet the criteria necessary to amount to 'money' in the law. They are not denominated in a State-authorized unit of account. This is, however, a separate question from their status as objects of property. It is clear from the chapter that the two questions are distinct.

1.21 Carr's Chapter 7 builds upon the common law concepts set out by Fox. It considers how the forms of property analyses in civil law and mixed legal systems would need to be adapted to accommodate cryptocurrencies. The principle focus of the proprietary analysis, as far as civilian systems go, is whether cryptocurrencies would count as a *res*, capable of forming the object of a property right. As with the common law analysis, this question is independent of whether the currency could count as 'money'. The challenge then is to explain how cryptocurrencies could be accommodated in a legal regime that analyses *res* as either tangible things or intangible rights. Carr's argument develops a common motif of the book, which is that in deciding which legal principles to apply to cryptocurrencies, their incorporeal form should be subordinated to their function and purpose. This is also brought to bear on the civil law requirement of specificity, which could be satisfied, Carr suggests, by the cryptographic uniqueness of such currencies, and the control over them which is made possible by the exclusivity of their private keys. Ultimately, he concludes, the extent to which civilian and mixed systems (p. 10) accommodate cryptocurrencies will depend, in much the same way as any other legal system, on the breadth and force of commercial demand.

1.22 The magnitude of commercial demand is certainly relevant to the analysis of Low and Wu in Chapter 8. They consider the characterization of cryptocurrencies in East Asia, a region in which the growth of cryptocurrencies has been faster than elsewhere in the world. The region makes for an interesting comparative analysis, not least because Japan, at one end of the spectrum, has explicitly included cryptocurrencies in its Payment Services Act, whilst China, at the other end, banned cryptocurrency exchanges in 2017. In South Korea, the other jurisdiction considered in this chapter, the technology has been neither especially embraced nor outlawed. Cryptocurrencies are not classified as 'money' in any of the jurisdictions, but the question arises again whether property rights arise in relation to them. It is perhaps not surprising that, in seeking to answer this question, this chapter also analyses the concepts of 'tangibility', 'excludability', and 'control', the latter two seeming to capture the realities of the contemporary commercial environment better than the first. Low and Wu lament that paucity of attention, both judicial and academic, which has to date been paid to the private law conception of cryptocurrencies, and they point to several cases from Japan and South Korea which demonstrate how this neglect has led to a failing in the protection of investors and of their assets. The class of assets to which they refer does encompass cryptocurrencies, since it seems that in East Asia, as in the other jurisdictions analysed in this volume, there are strong arguments to be made in favour of recognizing such currencies as capable of being the objects of property rights. Once more, however, there is in East Asia, no consensus about exactly how to categorize such assets, since they do not appear to fit comfortably into any existing taxonomy. In relation to Japan and South Korea, and even more so in relation to China, Low and Wu do not conclude on an optimistic note about the legal security of cryptocurrency transactions in the absence of any specific legislation to recognize their status as property.

1.23 In his Chapter 9, Hare asks whether there is any possibility of reconciling the principles and practices employed by traditional banking with the trading and holding of cryptocurrencies. Like other analogical approaches in this volume, he takes three basic functions of traditional banking, storing value, making payments, and lending, and investigates the extent to which the same functions can be performed through the medium of cryptocurrencies. Whilst alluding to the question whether cryptocurrencies can be classed as money, Hare focusses the analysis in his chapter on the related but nonetheless distinct question of how the holder of any unit of cryptocurrency stores its economic value, and the legal implications of these arrangements.

1.24 One of the principal analogies employed by Hare is that of the traditional banker-customer relationship and the functionally similar relationship between a holder (p. 11) of cryptocurrency and the provider of an online storage wallet. Such a relationship, he suggests, is better regarded as contractual than proprietary in nature. Although the contents of the contract will be different from that between a banker and customer, sufficient similarities exist to make the effort of transposing the relevant principles worthwhile. The relationship between a cryptocurrency holder and a digital wallet provider is, for instance, unlikely to be treated as creating a fiduciary relationship in the absence of any specific undertaking on the part of the latter or vulnerability on the part of the former. This must be correct: it would be quite remarkable for the provider of an online wallet to be subjected to more onerous responsibilities than a retail bank providing fiat currency services for its customers. Some of the difficulty inherent in this may well derive from the nature of the language used by those creating and dealing in cryptocurrencies: the notions of ‘wallets’ and ‘storage’ do not make for easy transposition on to the legal realities of the situation.

1.25 The principal legal reality of relevance for Fairpo in Chapter 10 is that, for tax purposes, governments are rarely concerned with the form in which individuals accumulate wealth, as long as they pay in an acceptable fiat currency. In general, therefore, cryptocurrencies are regarded for the purposes of tax as forms of property rather than currency (there appearing to be no problem with such a classification in this context). Fairpo argues that this conceptual distinction is less important than the practical need for tax laws to be as equal, certain, and administratively efficient as possible, something which is currently not always the case. One of the reasons for this is that tax authorities are still inclined to view cryptocurrencies as predominantly a payment mechanism as opposed to an investment vehicle, even though the last two years have seen a marked increase in such currencies being held with a view to realizing a later sale at a profit. As with so many of the other contexts in which the increased use of cryptocurrencies gives rise to problems, the difficulties surrounding their taxation often arise, according to Fairpo, because of a failure of the relevant authorities to grasp the nettle and to set out clearly the way in which such assets will be taxed and the reasons for so doing. This may well be, with a glance back to Proctor’s chapter on international regulation, partly because those authorities do not yet regard the level of use of cryptocurrencies to be sufficient to necessitate such changes, but, if so, the failure of the law to provide prospective guidance is particularly problematic for taxation. Fairpo identifies Australia, however, as a jurisdiction which has already managed to reduce unfairness in the way that cryptocurrency assets are taxed, and goes on to point out that, in 2018, the United Kingdom announced the setting up of a taskforce, with the specific aim of providing such guidance. It would seem, therefore, that there is at least some indication of a shift in thinking where the taxation of cryptocurrencies assets is concerned.

1.26 The Gevas’s Chapter 11 rounds off the volume by considering the use of cryptocurrencies as a kind of ‘community currency’, and projecting this on to (p. 12) likely future developments, as well as the legal responses to them. In doing so, Geva and Geva take lessons from the history of community currencies and transpose them to the current legal landscape to identify what is both valuable and valued about non-State currencies. Their conclusions about this enable them to suggest what might be the most future-proof characteristics of non-State currencies. In keeping with the conclusions reached by several other contributors (albeit for different reasons), Geva and Geva point to the volatility of most non-State currencies, which results from the absence of central bank or State backing. At the same time, the potential attraction of a decentralized and largely unregulated currency is clear. It may also be that the security provided by distributed ledger technology means that cryptocurrencies suffer from fewer security and trust issues than did previous incarnations of non-State currencies. It is certainly the case that they already enjoy a wider

user base than any community currency that has gone before. As with much of the analysis in this volume, some speculation has to be made: whilst cryptocurrencies are closer to their teenage years than their infancy, the law's ability and inclination to deal with them appears still to be nascent.

1.27 The phenomenon of cryptocurrencies marks a revolution in the theory and practice of payment mechanisms. Contemporary accounts in the mainstream news display a kaleidoscope of views on their value and significance: fears of criminality and anarchy, hope in democratized currencies that are delinked from State control, puzzlement at the basic technical mechanics of their operation, fascination, and awe at the power and rapidity of technological advancements. One thing is for sure. Cryptocurrencies are here to stay, and we predict that their use will grow rather than diminish in significance. Like the Internet itself, cryptocurrencies will acquire their own unstoppable momentum as their value and utility become more widely appreciated.

Footnotes:

* Sarah Green, Professor of Private Law, School of Law, University of Bristol, UK.

1 H Diedrich, *Ethereum* (Wildfire Publishing, 2016) 113.

2 For a more detailed and technical description of this, see A Narayanan, J Bonneau, E Felten, A Miller, and S Goldfeder, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton University Press, Princeton, 2016) 28–50.

3 Around $300 million dollars a year on Bitcoin alone, which is comparable to the annual electricity bill for the whole of Ireland. See Diedrich (n 1) 150.

4 In the Bitcoin protocol, the hash function takes an input of any length and always produces an output of a fixed length.

5 For present purposes, the substantive content of the text being hashed is irrelevant.

6 Diedrich (n 1) 106–07. Although, as Diedrich makes clear, it is theoretically, if not practically, possible to find another text which results into exactly this hash. This practical impossibility is considered to provide sufficient security.

7 This means, for example, that Alice has purported to transfer a certain amount of bitcoin to Bob by entering the details of his public key (which functions rather like an e-mail address) and issuing instructions for the network to transfer that amount from her stock of bitcoin to his. It would be foolhardy, however, for any payee to trust the integrity of any transaction at this stage because it has not yet been validated or added to the block chain.

8 And, by definition, the previous block will be similarly linked to all the blocks preceding it.

9 'Adding' here takes the form of concatenation of data strings.

10 The 'correct' number is dictated by the protocol, and it does not matter what it is—it is just a test for the nodes to prove the work they have done.

11 Diedrich (n 1) 149.

12 To a certain extent anyway. There is a possibility of 'forking', which will be discussed below.

13 There is, however, only a finite number of bitcoin available: 21 million.