Legal issues arising from the utilisation of blockchain based products in the 4th industrial revolution

ANDREW HAYNES* and PETER YEOH

Abstract
This contribution considers the nature of distributed ledger technology, or blockchain as it is otherwise known, analysing its key elements, the reasons for its emergence and development and its potential importance. The method by which it functions is analysed together with a discussion of the facilities that are being developed on it. There is also a consideration of the legal issues arising from its operation and of the facilities that utilise it. Further, there is also a consideration of the cost issues involved in using blockchain and the particular factors arising when shares and bonds are issued on a blockchain system. Criminal factors inevitably arise with the development of any new regime and key elements of this are considered. Finally, there is also an analysis of the inherent problems arising with such a system and the current situation in which the world now finds itself with blockchain, and the future issues that seem to be emerging.

*****

1 Introduction

Distributed ledger technology, or "blockchain" operates as a public ledger showing all transactions that have operated upon it, though the identities of the participants using it are obscured. Essentially, there is a ledger which is distributed on the internet on a peer-to-peer network. It runs on the users' computers, not on a central data base. Each transaction is a block that carries a cryptographic link to the previous one. Every addition of a new linked block to the chain extends it and thus makes it harder for a third party to steal another's cryptocurrency or asset because the process of rewriting the sequence of transactions becomes progressively more complicated. The essential concept is not new, its history dating back to the start of the 1990s when Haber and Stornetta created a system of documented time stamps that could not be retrospectively interfered with. Together with Bayer they then incorporated "Merkle trees" into the design to facilitate this by the successive elements being constructed into a continuing block.[1]

* Professor, University of Wolverhampton. The author worked at two major law firms and Deloitte, London before becoming an academic. He has written widely on the topics of financial regulation, financial crime and capital markets law. He has also advised governments, financial regulators, investment banks, financial services firms and legal practices in these areas. A.Haynes2@wlv.ac.uk.

1 Narayanan, Bonneau, Felten, Miller & Goldfeder *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (2016) ....; Haber & Stornetta "How to time stamp a digital document" 1991 (3(2)) *Journal of Cryptology* 99–111; Bayer, Harber & Stornetta "Improving the efficiency and reliability of

Its potential is enormous because of the very wide range of transactions that can operate on it safely and cheaply. As a result, it is emerging as one of the most important potential developments in the commercial world.[2]

This contribution will consider:

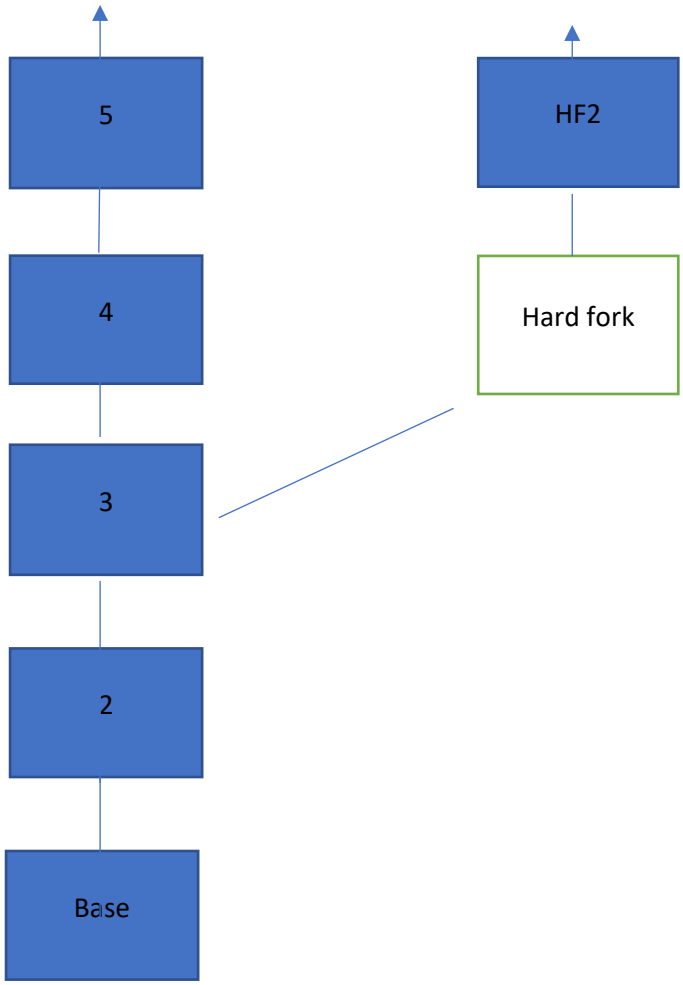
- the nature of the blockchain and the reasons for its current and future emergence;
- how it functions and the nature of the facilities that are designed to be built on it;
- legal issues relating to the operation of the blockchain itself; and
- legal issues relating to the facilities that use it, and in particular the extent to which existing laws and regulations may be applicable

2 Distributed ledger technology

The construction looks like the diagram below. The central block at the bottom is the original arrangement and each participant adds their own block as they engage in a transaction. Each transaction includes the cryptographic hash of the prior block thus connecting them together. As shown, a separate fork can be added by someone adding a different software component, resulting in what is called a "hard fork". After that, transactions on the old software will be added to the previous structure and ones carried out on the new software will be added to the blockchain that has split off from the original construction. Either way the blockchain becomes progressively longer and safer from interference after the event with each transaction. Thus, the structure looks like this:

digital time stamping" in Capocelli, De Santis and Vaccaro (eds) *Sequences II Methods in Communication, Security and Computer Science* (1993) 329–334.

[2] This is not universally accepted. See, for example, Danielson "Cryptocurrencies: Policy, economics and fairness" *Systemic Risk Centre Discussion Paper 86* London School of Economics 14.



Hard forks are not reversible because it involves all the participants in updating. Once this is done those who do not implement the alteration to their part of the blockchain can no longer use it. Thus, there is a change in the operation of the blockchain from that point and it splits into two separate operating systems. On the other hand, soft forks introduce voluntary changes to the software and can be reversed. They occur when the majority of the miners impose their approach on any dissenting minority. Once a blockchain has developed beyond a certain stage this becomes very difficult to implement because of the numbers involved.

The blocks themselves are each made up of a header which is effectively an electronic fingerprint made up of a hash using standard cryptographic functions,[3] a time stamp and a hash

[3] De Phillipi & Wright *Blockchain and the Law: The Rule of Code* (2018) 22. Carter & Wegman "Universal classes of hash functions" 1979 (18(2)) *Journal of Computer and System Sciences* 143-154.

of the previous block. Other information may be added to it. The protocol of the relevant cryptocurrency or asset will link these together sequentially. Fink[4] defines it as

> "a database that is replicated across a network of computers updated through a consensus algorithm" [and] "a shared and synchronized digital database that is maintained by an algorithm and stored on multiple nodes (the computers that store a local version of the distributed ledger). Blockchains can be imagined as a peer-to-peer network with the nodes serving as the different peers."[5]

It is:

> "…a purely distributed peer to peer system of ledgers that utilises a software unit that consists of an algorithm, which negotiates the international content of ordered and connected blocks of data together with cryptographic and security technologies in order to achieve and maintain its integrity."[6]

Or as Vitalik Buterin, the creator of Ethereum put it, it is:

> "a….computer that anyone can upload programs to and leave the programs to self-execute, where the current and all the previous states of every program are always publicly visible, and which carries a very strong cryptoeconomically secured guarantee that the programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies."[7]

Not all blockchains operate on the same basis; the variety is extensive and they can be public and permissionless which was the original form in which they were created. Anyone can download and use the relevant software and create a new cryptocurrency or asset. Alternately, there is a private and permissioned version and there are also hybrid versions which are a mixture of the two. The private versions, as their name suggests, run on a private network or intranet. They have normally already been created to carry out a specific function and may operate inside a company or syndicate. By their nature those using the system are known and permission must be granted before someone can join in. Hybrid blockchains, as their name suggests, combine the two, and as Herian put it:

> "data from a closed network can be shielded by a registry layer and moved or released to permissionless blockchains for the purpose of allowing public scrutiny of or prescribed or specified data at a given point in time. The hybrid distinction also includes the option of

---

4 Finck *Blockchain Regulation and Governance in Europe* (2019) 1.

5 Finck (n 4) 6.

6 Drescher *Blockchain Basics* (2017) 35.

7 Buterin "Visions part 1. The Value of Blockchain Technology" (Ethereum Blog, 13 April 2015) https://blog.etherium.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology. See also Finck (n 4) 11.

> using ledgers, most likely in permissioned form as an access control medium for other, additional registries or databases in off-chain or offline servers and storage infrastructures."[8]

Almost anything can be collected and progressed on distributed ledger technology, for example a business or legal transaction can be developed from the initial contact, through the negotiations up to the final contract. If the parties later agree to amend the contract, it can be altered accordingly but any retrospective amendment is possible without the parties' agreement, so the risk of a party seeking to renege by challenging what had been previously agreed is removed. It thus has great potential for storing business and government records.

The arrangement is open to access by third parties but is also encrypted utilising both public and private keys. In the case of the commonest cryptocurrency, bitcoin, the transactions are checked, transacted and cleared and locked into the ledger on a time stamped basis in a link with the preceding transaction every ten minutes.[9] For anyone to interfere with the process would require accessing the blockchain history and retrospectively altering it, which would be almost impossible at the current level of computer capacity and software development.[10]

This can also operate just as easily on a multi-lateral basis. For example, most of the population own credit and debit cards which facilitate paying for goods and services. The arrangement operates on the basis that the data which develops in such a system is owned by the company issuing the card. They also charge an annual fee and a percentage of the outstanding amount on the card. It is normally the case that the holders of these cards have an arrangement which facilitates them spending an amount that represents a debt to the credit card issuing company. An equivalent system could be created on blockchain whereby the payment system would operate on the basis that the payor and payee deal directly with each other on the blockchain. In practice the funds could move at a speed whereby the payment would be made within ten minutes and the confirmation of transfer of title being returned at the same speed. It would still be possible for the person using the arrangement to obtain credit from third parties, but the credit provider would not need to become involved with the process and would no longer own the overall arrangement.

3 Costs

8 Herian *Regulating Blockchain Critical Perspectives in Law and Technology* (2019) 16.

9 Though in some cases, eg, Etherium, it is more frequent and can be carried out in a few seconds.

10 Tapscott & Tapscott *Blockchain Revolution* (2018) 6-7.

At present there are virtually no overheads in utilising a blockchain-based system, although this could start to change once new coins cease to be issued by the arrangement concerned, eg, bitcoin. After that point it will be necessary to find a methodology to pay miners for each transaction to be verified, or an alternative arrangement be found to validate each transaction. Even so it is a system suitably designed for carrying out financial transactions. For example, all the financial transactions carried out by banks through the SWIFT system, or cheque clearing, can be carried out directly, and at lower cost by the parties to the transaction dealing directly with each other. In this context the potential of such an arrangement is greatly increased by the proportion of the world's population in developing countries not living in the vicinity of a bank branch. The general availability iphones and similar electronic access points opens such people up to all the financial arrangements available online, and where they are so constructed on a blockchain-based system. That said, unless the user has the capacity to run the blockchain operating system on the cloud, the size of the hard drive needed to operate blockchain means that such an iphone would need to be linked to a powerful base unit, which at present may limit its use in such poorer parts of the world.

Fund managers can also operate on blockchain-based systems and thus reduce costs to the investors through reducing administration costs, the need for fewer intermediaries and partly as a result of both of these, engage in significantly less administration. In addition, the automated real-time process available on blockchain, whereby the trades both self-clear and settle, will reduce them further.[11]

Trade finance is an area where there is the potential for significant blockchain usage[12] and this was apparent from the feedback to HM Treasury's Cryptocurrency Task Force in the UK. The current arrangements involve letters of credit and/or bills of exchange being used as a vehicle for payment. In practice there are also time delays with the majority of letters of credit being initially rejected by banks for failure to be precisely accurate, often on quite trivial points of detail, because such a lapse in accuracy technically makes the claim a fraudulent one and thus the issuing bank will refuse to pay.[13] That said, the vast majority of such bills are settled

---

[11] HM Treasury "The UK Investment Management Strategy II" (Dec 2017) … https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/665668/The_Investment_Management_Strategy_II.pdf.

[12] Hong Kong Monetary Authority (HKMA) "Hong Kong and Singapore launch a joint project on cross-border trade and trade finance platform" (2017) (Press Release 15 Nov 2017) https://www.hkma.gov.hk/eng/key-information/press-releases/2017/20171115-6.shtml.

[13] *United City Merchants v Royal Bank of Canada* [1983] 1 AC 168 (HL); *Kvaerner John Brown Ltd v Lear Siegler Services Ltd* [2006] EWCA Civ 1130; and *Balfour Beatty Civil Engineering Ltd v Technical and*

within 48 hours, albeit at some inconvenience to the payee. On the other hand, if the payment system for a letter of credit and/or bill of exchange were to be constructed on a blockchain the money could be released to the vendor at the moment of the delivery of the goods, with the process being self-checking and self-recording. There is evidence of steps being taken to arrange precisely such an arrangement by the Monetary Authorities of Hong Kong and Singapore. They have provided what may be the first of many such steps in creating an international information highway to facilitate trade finance.

The initial design of the respective blockchain technologies is still at a fairly early stage and questions have been raised[14] as to whether there will be a trade-off between performance, resilience and privacy. Transactions currently take anything from ten minutes to an hour to go through, which is a big improvement on the function of bills of exchange and letters of credit.

However, when compared with payment by cash or credit card this is a significant time frame and reduces the attractiveness of blockchain-based currencies as media of exchange. Transaction costs for bitcoin have been assessed at varying between US$ 0.45 to US$ 55.[15] The platform being used may also involve extra fees. This compares with no cost for using cash and a nominal, indirect one for using credit or debit cards. That said, for international transactions the picture changes. The normal banking tool is SWIFT, which in comparison with cryptocurrencies is slow and more expensive. There are other cash transfer systems but the average cost of transferring US$ 200 is 7.1%, rising to 9.4% in sub-Saharan Africa.[16]

4 Shares and bonds

Companies raise finance by either selling shares which provide a degree of equity in their business to those who will buy them, or by borrowing from banks or the open market by issuing bonds. Such share and bond offerings can now be made on blockchain and can potentially provide a far cheaper way for shares to be issued publicly. This raises the possibility of smaller companies going to market to sell shares than at present, thus hugely increasing the size of the

General Guarantee Co Ltd [2000] 68 Con LR 108. See also Haynes *The Law Relating to International Banking* (2018) 260-265.

[14] See, for example, HM Treasury, Financial Conduct Authority & Bank of England "Cryptoassets Taskforce: final report" (October 2018) 26 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf.

[15] Danielsson "Cryptocurrencies: Policy, economics and fairness" (Version 1.2 Nov 2018) Systemic Risk Centre (SRC) Discussion Paper 86 London School of Economics 20 http://www.systemicrisk.ac.uk/sites/default/files/downloads/publications/dp-86.pdf.

[16] Danielsson (n 15) 21.

share market. Legal issues still arise as share and bond sales normally have to be accompanied by a prospectus, a legal document setting out the finances of the issuing company, the details of the share issue and what the funds will be used for. These are time consuming and expensive to produce, requiring extreme care and accuracy because of the criminal and civil legal consequences that can be attracted if they are not. Many offerings currently seem to be issued on the assumption that these rules do not apply if the share issue is carried out on an initial coin offering (ICO) basis but steps are currently being taken by regulators to disabuse issuers of this fact.[17] Once those in the market place understand this the costs will rise, but it will still be potentially much cheaper than a standard share issue. Very significant cost savings will still be made though from the reduction in investment bank fees, stockbrokers and sales agents as the online sales process will hugely reduce the expense of the share issue.

Likewise, a multi-party system such as a bond issue,[18] or ICO as they are called if the bond exists in the form of an e-currency offering, can all sit on blockchain. Over US$ 3 billion was raised in this way in 2017. That said, the same legal requirements regarding prospectuses crop up here and it is clear that market participants have also been cavalier in this context. The company wishing to raise finance therefore has to list any prospectus[19] on the blockchain. The lenders can submit payment and receive their title to the debt on the system, and in due course if they wish to sell title to the debt on to another person, which frequently happens, this will also take place and sit on the blockchain record. Repayment by the borrowing company can also then take place on the same system. In addition, the automated process is much cheaper to operate than the current process and reconciliation, settlement and record keeping are all automated with all parties sharing identical data.

However, for banks there is one downside as the existing system requires clearing houses for shares and also for derivative contracts. These can take three days to clear trades even though the trades themselves will usually clear in seconds. This should not be a problem once blockchain-based systems take over as the trades will self-clear. The current system does allow participants to engage in multi-lateral netting. This consists of the parties and the clearing house

---

[17] US Securities and Exchange Commission (SEC) "Investor bulletin: Initial coin offerings" (Investor Alerts and Bulletins 25 July 2017) https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings.

[18] The issue of debt paper, normally by a corporate or government to raised finance at a stated interest rate for a set period

[19] The legal document advertising the details of the bond issue and the company issuing it. Alternately, if the bond is issued in high enough denominations to remove the risk of ordinary members of the public being able to afford them a simpler and cheaper to produce document, called an "information memorandum" will be issued.

netting all trades off against each other by each trade being constructed of a sale by the seller to the exchange or clearing house and an immediate sale by the exchange or clearing house to the buyer. As a result the exchange is a counterparty to each deal and in the event of a participant becoming insolvent all the trades that remain outstanding will be offset against each other thus hugely reducing the amount of money at risk to the other parties involved.[20] The relative ease with which LCH Clearnet was able to cope with the financial consequence of Lehman Bros collapse is a good example. There were some issues with identifying the clients to whom certain uncleared trades related, and some delays in getting margin payments back to those who required it, but essentially the multi-lateral netting approach worked well in reducing the total amount of money at risk.

What multi-lateral netting offers the banks is the opportunity to reduce greatly the amount of capital they have to hold in reserve against the trades they enter into, which is required by the Basel III banking capital requirements which are being applied in all the world's more advanced economies. In addition, reconciliation processes that can be both time consuming and slow can be avoided.[21] No doubt in due course amendments to the banking capital rules are likely to be made to move it in line with the financial risks that are left with the banks under a blockchain-based system.

This process would not be without risk though. Whilst it would significantly reduce costs in that the trading process would no longer need intermediaries, the market could end up in a decentralised financial world where trades are no longer centrally cleared and such a state of affairs "will simply be a collection of interwoven smart contracts that facilitate the buying and selling of blockchain based assets".[22] This will not offer the same facility as the present exchanges in holding capital against the risk of a participant becoming insolvent, and thus the risk of a market failure, or at least a localised one based on one collection of interwoven blockchain-based contracts, will be much higher.

5 Criminal factors

Crucially blockchain also makes it much more difficult for fraudsters to operate as they cannot go back later and hide the fraud. Any activity is recorded and clears itself removing the need

[20] Haynes (n 13) 291.

[21] European Securities and Markets Authority (ESMA) "ESMA assesses DLT's potential and interactions with EU rules" (Press Release 7 Feb 2017) https://www.esma.europa.eu/sites/default/files/library/esma71-844457584-344_2017_press_release_dlt.pdf.

[22] De Philippi & Wright (n 3) 102.

for traditional audit to verify it. Indeed, given the limited requirements placed on auditors to be "a watchdog not a bloodhound"[23] in comparison with the inability of the blockchain system to do anything other than record accurately, the future system should be much safer, automatic and not require audit fees. "If the (blockchain) ledger says something is true then it is true." [24] That said, to have a checking and regulatory capacity that works properly both auditors and regulators will need to be granted access rights to the distributed-ledger technology to check.

This makes blockchain and currencies based on it less attractive to criminals. With criminal funds, money laundering and terrorist finance there are a multiplicity of ways in which the criminals can hide their identity and the overall transaction. Blockchain records all the details of the trading and thus the capacity to hide what is going on becomes much more difficult, though there will remain the capacity for the person using the system to do so from behind a false identity. Even so police, tax authorities and intelligence services will be able to trace money flows back to their source. That said, some cryptocurrencies such as Monero and zcash are more difficult to police. Monero has an obfuscated public ledger which makes it extremely difficult to trace back. It hides the recipient of the deal and creates a new electronic address and a secret key for him or her.[25] Zcash[26] has a cryptography-based system to guarantee privacy but with a selective disclosure capacity built in. Its accounts cannot necessarily be traced and its blockchain does not store information concerning the source and destination of the "money". Thus, for money laundering and disclosure rules the owner can elect to release information or not.

The other criminal issue is that although criminals may find interfering with the blockchain process to be prohibitively complicated there is still the possibility that with cryptocurrencies or other items of value based on blockchain those parties will engage in market manipulation. The other possible way of illegally obtaining money through the new system is to hack people's computers to access their codes as was discussed earlier.

Some regulatory issues are discussed elsewhere in the book.[27] What is already apparent is that blockchain-based systems do not fit neatly into existing regulatory structures. Some

---

[23] Lopes CJ in *Re Kingston Cotton Mills (No 2)* (1896) 1 Ch 331.

[24] Interview between Austin Hill, Don Tapscott and Alex Tapscott, 22nd July 2015 (recorded in Tapscott & Tapscott (n 10) 76.

[25] Finck (n 4) 97.

[26] a joint development between Israeli and US cryptographers. See in this regard De Philippi & Wright (n 3) 67.

[27] Editor will insert a cross reference

states have categorised cryptocurrencies differently from others, and in the US money transmission is regulated at state level, whilst the impact of the new developments will have an impact both nationally and internationally. The regulators are facing a situation where the two parties to a trade or transaction will be in possession of potentially large amounts of information, whilst the regulators themselves will have access to very little. They are also operating against a background of very rapidly changing circumstances, to which, historically, they have not always adapted well.

Across all these potential activities, and the others that will be created, the new distributed systems will be more resilient that the current centralised systems.[28] This is because having separate copies of data accessible to multiple participants greatly reduces the potential risk of data loss. As the blockchain is developed with an ever-increasing number of participants, this becomes more and more the case. A web attacker would need to take control of multiple participants to attack the system, and the longer a distributed ledger has been in use the greater this number is likely to be. It could be vast. Thus, the system is capable of continuing to perform even if part of it successfully comes under attack as virtually all the participants will still be able to get direct access to their own data which will be identical. That said the Bank of England's testing of a multi node Etherium protocol-based project warranted further investigation of "scalability, security, privacy, interoperability and sustainability."[29] Even so most observers see distributed-ledger technology-based systems as stronger in these regards than the systems they are starting to replace.

However, now decentralised organisations with illegal intent have been created. Daemon for example, will enable its anonymous shareholders to manage a market on the dark web. Its aims, amongst other things, are to evade government interference.[30]

There is a further problem in that behaviour that any objective observer would regard as criminal may technically not be so because the wording of the law lags behind the technological developments. For example, the DAO hack arose when US$ 150 million was invested in Ether by around 11,000 people. The idea was to create a start-up fund which would be operated on a democratic basis by the votes of the contributors. Due to a bug in the code a hacker was able

---

[28] HM Treasury (n 14) 22.

[29] "Fintect Aggergator proof of concept." Bank of England, 2016 https://bankofengland.co.uk/research/fintech/-media/boe/files/fintech/pwc.pdf (cannot find/access)

[30] De Filippi & Wright (n 3) 145; Butnix "Daemon Wants to Become a Decentralized Etherium-Based Smart Darknet Market" The Merkle 4 April 2016 http://themerkle.com.

to remove a third of the fund without breaching the criminal law.[31] There was then a democratic vote of the contributors and 87% of the relatively small number that voted agreed to create a hard fork reversing the effect of the hack.[32] Perhaps surprisingly some opposed this on what seem to be philosophical grounds, ie, that on principle the blockchain should not be reversed.

6 Inherent problems

What then are the problems? Energy consumption needs to be considered. The process of running transactions through the secure algorithm[33] consumes a significant amount of energy. That said there seems to be a huge variation in the estimates that "experts" calculate is utilised.[34] That needs to be offset though against the quantity of electricity that would otherwise be consumed by whatever alternative method had been adopted to carry out the transaction.

The greater the resilience built into a system the more limited the capacity will tend to be and some of the systems will be designed to cater for huge numbers of users. To maintain privacy encryptions are used but there are suggestions that this can reduce performance. That said in many situations the use of encryption is a necessary factor to maintain sufficient security; so from the vantage point of the user this is not going to be a negotiable element. Finally, the resilience of a system can be strengthened by limiting the distribution of data. Unfortunately, this is often not an option as the common distributed ledger will be a key element of making the system attractive to potential users.

There may prove to be overheads related to co-ordination once the systems are in widespread use, though this should probably prove considerably less than current systems where parties other than those dealing directly with each other are concerned.[35] As years go by the complexity of some of the programs may increase in order to handle all the data, and security will become a greater concern, especially once computers that can handle mega data become operative.

---

[31] Finck (n 4) 187; Raskin "The law and legality of smart contracts" 2017 *Georgetown Law and Technology Review* 305 335; Werbach & Cornell "Contracts *ex machina*" 2017 *Duke Law Journal* 313 365.

[32] Technically there were two votes, the first on the procedure to be adopted and the second to reverse the blockchain.

[33] Algorithm 256 (SHA-256).

[34] Schneider "After the Bitcoin Gold Rush" *The New Republic* 24 Feb 2015; Kaminska "Bitcoin's wasted power" *Financial Times* 5 Sep 2014; and CIA *The World Factbook* (2012) more precise reference.

[35] Drescher (n 6) 13; Stead *What is Cryptocurrency: Your Complete Guide to Blockchain, Bitcoin and Beyond* (2018) …; Ganne *Can Blockchain Revolutionize International Trade?* (2018) 90-110.

In addition, there is as yet no standard-form platform for participants to use although IOSCO are looking into this.[36] It will be simpler to operate a system where there is an international standard, but there is no guarantee that one will emerge. Indeed, some participants may seek a competitive advantage through developing newer systems which have advantages over pre-existing ones.

7 The current situation

At the time of writing the US leads distributed-ledger technology start-ups with the UK in second place,[37] with London having the second highest number of such projects listed, closely behind San Francisco. However, the scale of the internet capacity and that of the computers most people use on the system is not capable of carrying a multiplicity of large scale blockchain transactions; the transactional capacity is not there. It will not be many years before it is and until then distributed-ledger technology is likely to develop progressively. Some aspects relevant to its development such as law and regulation, can be developed fairly quickly. Some areas such as money laundering, market manipulation and theft will always be with us but the security distributed-ledger technology provides should render them safer than other methods of financial transfer.

Strictly speaking, the World Trade Organisation (WTO) maintains that blockchain represents only one type of distributed-ledger technology, but the term now is commonly employed to refer to them in general. Many would agree that blockchain goes beyond the cryptocurrency hype. Its potential trade-related applications are numerous and could probably transform international trade significantly. Some possible deployments of cryptocurrency could include trade finance, customs and certification processes, transportation and logistics, insurance, distribution, intellectual property and government procurement.[38] Even as the technology unfolds interesting opportunities to enhance efficiencies of numerous processes trimming costs in these areas, the technology though is not a solution to everything. As such, this requires carefully weighing the costs and benefits involved. Interestingly, blockchain could

---

[36] International Standards Organisation (ISO) "ISO/TC 307 Blockchain and Distributed Ledger Technologies" (2016) https://www.iso.org/committee/6266604.html.

[37] Coindesk "Coindesk releases Q2 2018 State of Blockchain Report" https://www.coindesk.com/state-of-blockchain-q2-2018; Outlier Ventures "Blockchain Start-up Tracker" 2018 https://outlierventures.io/research/the-blockchain-startup-tracker/.

[38] Ganne *Can Blockchain Revolutionize International Trade?* (2018) ...

help implement the WTO Trade Facilitation Agreement, as well as facilitating business-to-government and government-to-government processes at the national level.

The World Economic Forum has predicted that 10% of global GDP could be stored on blockchain systems.[39] It sees it as akin to the invention of the internet, a system that functions as a general-purpose technology. Unfortunately, it remains held back by the limitations of the size of the distributed computer system.

There remain issues to be fully resolved if blockchain is to fulfil its potential; the issues of privacy, security, scalability, costs, hidden centrality, lack of flexibility and critical mass.[40] Privacy arises because the nature of the blockchain is open so that users can verify ownership and transactions. However, it is possible to limit this as has been seen with the obfuscated ledger technology used in Monero and the cryptography-based system used for zcash.

Security is a potential worry with any software system. In the case of blockchain systems the accounts are cryptographic keys that are accessed through the system. It is safe as long as only the relevant person has access to the cryptographic key. If a third parties can access its details then they can access the system as though they were the other person. The security in the system is so strong that a third party is only likely to access it if he or she are given it or accesses records the owner has kept outside the blockchain system. Related to this is the possibility that governments may require computer codes to have trapdoors built into them facilitating analysis, suspension or disabling.[41] That said, the users cannot be stopped from running the system without it, though this would presumably be illegal. Such an approach by governments would almost certainly lead to a kind of regulatory arbitrage where systems were based in jurisdictions that did not do so.

The scalability element arises as a result of the security that is built into the system. To stop later users altering earlier records the system is constructed of the history of the transactions so far with each having a hash puzzle added each time a block is added into the system. To change this retrospectively at the current level of software development would be prohibitively time consuming and expensive. The consequence of this is that processing speed and the maximum scale that the systems can currently operate on are limiting factors. This

---

[39] "Deep shift – Technology Tipping Points and Societal Impact" 7 www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.

[40] Drescher (n 6) 206.

[41] De Phillipi & Wright (n 3) 181. It could be argued that this would merely be an extension of the current arrangements whereby some governments impose obligations on those creating codes, eg, the Digital Millennium Copyright Act in the US.

overlaps with the issue of cost, though that needs to be offset against the cost of any alternative system that would have been used by the parties inst- ead. As that would often currently involve the use of third parties, those costs could be considerably higher.

The weak link may be the 51% rule discussed earlier. In a smaller system it may be possible for someone with considerable software power to achieve 51% control of relevant nodes. The larger a blockchain system becomes, the safer it is from such attacks.

The current state of legal and regulatory clarity is extremely low. Where there is any, that in one part of the world often contradicts that in another. It is an area where it is reasonable to expect rapid development. It would appear that the blockchain ecosystem is positive towards effective regulations that would deter nefarious deployment of the technology.

Despite present limitations, blockchain enthusiasts have to be mindful of the potential liability. This raises questions concerning how distributed-ledger technology should be structured, owned and ultimately regulated. In this respect, consideration should be given as to whether the system is permissioned or permissionless, whether the legal structure is specified in the pertinent agreements, the system's express or implied purpose, the system's consensus mechanism and the matter of pre-existing relationships between the parties.[42] These features could be treated in law to be one of several legal entities, from a joint venture, a multi-party contract to a partnership. For instance, the group that designs the code that governs the ledger could be deemed a joint venture, and that this could extend to nodes or even simple users of the ledger depending on the extent of their participation. Conversely, the distributed-ledger system could be treated as a multi-party contract where the group that sets up the code design and nodes under a contractual obligation to maintain the system's security and operations. These potential legal structures could also differ across disparate jurisdictions.

The challenge hinges on the ability of law makers to strike a balance between the need for governance and the avoidance of strong state intervention that could terminate the innovation.[43] There is therefore the need to analyse carefully the functional features of various concepts under evaluation and their implications and risks to enable the delivery of appropriate and sufficient response to regulatory concerns without over regulation. This is not easy as blockchain is at an early stage of development and it is not clear what forms it will evolve into.

---

[42] Zetzsche, Buckley, & Arner "Blockchain distributed ledgers and liability" 2018 (2(4)) *Journal of Digital Banking* 298-310.

[43] Borg & Schembri "The regulation of blockchain technology" in Dewey (ed) *Blockchain & Cryptocurrency Regulation* (2019) 187; Yeoh "Regulatory issues in blockchain technology", 2017 (25(2)) *Journal of Financial Regulation and Compliance* 196-208.

Technologically blockchains are also rather limited in that every full node must process each transaction and keep a full copy. This inevitably slows down its utilisation, a problem that will increase as the size of a blockchain grows. Security for users will potentially be at the price of growing inefficiency. That said, there are developments such as off-chain payment channels, arranging for different nodes to store and process only part of the process, carrying out calculations outside the chain and directed acrylic graphs which do not use a linear blockchain approach.[44] Other approaches will also no doubt emerge.

Accordingly, regulatory intervention should be functional, technology-neutral and premised against regulatory goals and principles.[45] Indeed, like the Internet before it, distributed-ledger technology should be subject to regulation from governments around the world.[46]

Finally, while blockchain provides potential benefits in terms of improved transparency and reduced transaction costs by the more effective managing of data and streamlining of processes, improving supply chains, enabling tracking and management of intellectual property, improving the reliability and traceability of records, reducing the speed and cost of settlement, facilitating copyright and patent protection, as well as improving efficiency through automated reporting and smart contracts, its broader applications are facing various significant challenges. These include, amongst others, the following:[47]

i. Transaction capacity and scalability issues relative to conventional banking payments system.

ii. Rising concerns over privacy and security matters. In particular, blockchain-design choices frequently lead to inevitable trade-offs needed between performance, privacy and the degree of decentralisation. Future technical progress, hopefully, could potentially resolve these.

iii. Interoperability challenges between different blockchains, between applications built on the same blockchain, and between blockchain and legacy systems.

iv. Rising fears over the theft or loss of private keys. This is best exemplified by the bitcoin theft of almost US$500 million from Mt. Gox in 2014.[48]

---

44 Finck (n 4) 31.

45 Supra note [186], Borg & Schembri (n 43) …

46 Rodrigues "Law and the blockchain" 2019 (104(2)) *Iowa Law Review* 679-730.

47 Madir "Introduction- what is FinTech" in Madir (ed) *Fintech Law and Regulation* (2019) 1 …

48 Editor's footnote: See in this regard Takahashi "Cryptocurrencies entrusted to an exchange provider: Shielded from the provider's bankruptcy?" in Hugo (ed) *Annual Banking Update* (2018) 1 et seq.

v. Trade-offs in relation to the governance of blockchains.

vi. To achieve wider deployment, the technology needs to be fully accommodated within public policy and legal frameworks, and this suggests the need for clear rules.

vii. Competition issues may need attention. This is because as permissioned blockchain networks advanced to become essential infrastructure, say in clearing and settlement, competition issues may surface around access.

Though still in early days, in 2016, France installed rules allowing the holding and transfer of non-listed securities via blockchain, with Japan enacting rules requiring the registration of virtual currency exchange business operators; and with the 26 member states in the EU in 2018 signing a Declaration to create the European Blockchain Partnership, as well as cooperating in the setting up of a European Blockchain Services Infrastructure to support the delivery of cross-border digital public services marked by the highest standards of security and privacy.[49]
The advent of blockchain is viewed by some as a revolutionary event moving through the five stages of denial, anger, negotiation, depression, and eventually acceptance.[50] At its commencement, bitcoin was largely ignored as an internet-based money without mainstream interest or a future. Then concerns arose as a result of it being used for criminal purposes by money launderers, terrorists and drug dealers. However, the range and use of blockchain-based products has become increasingly apparent and the extent of the usage of such arrangements has grown rapidly. Along with other exponential technologies[51] such as the Internet of Things (IoT), 3D, edge computing, robotics and artificial intelligence (AI) it has become one of the symbols of the Fourth Industrial Revolution,[52] as their business and public processes may prove to be many times faster, better, and cheaper.

---

[49] Digibyte "European countries join blockchain partnership" (10 April 2018) https://ec.europa.eu/digital-single-market/en/news/european-countries-join-blockchain-partnership (accessed 12/11/19).

[50] Mignon "Blockchain-perspectives and challenges" in Kraus, Obrist & Hari (eds) *Blockchains, Smart Contracts, Decentralized Autonomous Organizations and the Law* (2019) ... .

[51] Ismail, Malone, & Van Geest *Exponential Organizations* (2019) …

[52] World Economic Forum (WEF) "Globalization 4.0: Shaping a global architecture in the Age of the Fourth Industrial Revolution" WEF Annual Meeting 22-25 January 2019 Overview, http://www3.weforum.org/docs/WEF_AM19_Meeting_Overview.pdf (accessed 12/11/19).