Cloud Crypto Land

Edmund Schuster*

Abstract

The supposed disruptive and transformational potential of blockchain or distributed ledger technology (DLT) has received widespread attention in the media, from legislators, as well as from academics across disciplines, including law, over the past few years. While much of this attention revolved around the cryptocurrency Bitcoin (and its numerous cryptocurrency offshoots), many see the real promise of blockchain technology in its potential use for organising transactions in traditional assets, including shares and other securities, as well as for facilitating self-executing "smart contracts", which replace vague and imprecise natural language with precise and unambiguous computer code.

Focussing on non-currency applications of blockchain technology, I present a simple legal argument that seeks to demonstrate the impossibility of a meaningful blockchain-based economic system. I argue that features present in all major legal systems mean that real assets cannot be traded on blockchain-based systems, unless design choices are made which necessarily remove all advantages the technology offers over existing solutions. The same argument is shown to apply to so-called smart contracts.

The paper further argues that there is no reason to expect legislators to change current legal principles in sufficiently dramatic fashion so as to carve out a space in which applications of blockchain technology can usefully be implemented, since the potential efficiency gains ascribed to blockchain technology are based on a flawed analysis of its costs and benefits. Legal and practical obstacles therefore mean that, outside its original and circumscribed realm of cryptocurrency, blockchain technology is highly unlikely to transform economic interactions in the real world. Instead, it is argued that – depending on the specific implementation – blockchain technology is either pointless or useless for transactions in traditional assets.

Keywords: Blockchain, distributed ledge technology, smart contracts, crypto assets

---

* Associate Professor of Law, London School of Economics; Research Associate, UCL Centre for Blockchain Technologies. Email: <e.schuster@lse.ac.uk>. I am indebted to Lawrence Akka, John Armour, Daniel Awrey, Jo Braithwaite, Ross Cranston, Tatiana Cutts, Preston Byrne, Anca Bunda, Iris Chui, Jon Danielsson, Luca Enriques, Michele Finck, David Fox, David Gerard, Carsten Gerner-Beuerle, Geoffrey Goodell, Stefan Loesch, Aurelio Gurrea-Martinez, Raina Haque, Werner Haslehner, David Kershaw, Eva Micheler, Ciaran Murray, Stephen Palley, Wolf-Georg Ringe, Mathias Siems, Joseph Spooner, Tim Swanson, Angela Walch, Martin Walker, Jens Wiechers, participants at the *"Cryptoassets and the Law"* seminar at the LSE, the CryptoEconSys conference at the Massachusetts Institute of Technology, the LSE/UCL BARAC workshop, the conference on the *"Future of Money"* hosted by the Systemic Risk Centre, and the Digital Assets Project conference at Harris Manchester College, Oxford, for helpful comments, discussions, and criticism. All errors and misconceptions are, of course, my own.

I. INTRODUCTION

Blockchain or, more broadly, distributed ledger technology (DLT) has received widespread attention in the past few years. Blockchain technology was first suggested and popularised in the context of the cryptocurrency Bitcoin, but its use has since spread to many other cryptocurrencies and, importantly for this paper, it has been and continues to be suggested as a potential technical solution for many areas beyond currencies and payments. In fact, many blockchain and DLT enthusiasts see the real promise of the technology in its potential use for creating tradeable "tokens" representing real assets, such as shares, other securities, or indeed any other physical or intangible asset. Related to this, the use of blockchain technology has also been discussed in the context of so-called "smart contracts", which replace the vague and imprecise natural language typically used in recording legal agreements with precise and unambiguous computer code, running in a transparent and decentralised manner, potentially enabling automatic execution and updating of legal agreements.

So mystical and near-unlimited are the powers ascribed to blockchain technology that the former UK Chancellor of the Exchequer suggested that blockchain technology could help solve the Brexit-related problems with customs checks on the border between Northern Ireland and Ireland.[1] Equally unfounded statements about the technology by government institutions and in the media abound,[2] suggesting that enthusiasm for, and understanding of, this technology are, at best, orthogonal features.

This paper will look at non-currency applications of blockchain technology. It presents a simple legal argument for why *meaningful* implementations of blockchain-based systems for transacting in real assets are not feasible. I argue that mandatory legal principles, present across all major jurisdictions, mean that blockchain-based tokenisation – representing real assets, including fiat currencies, by digital blockchain "tokens" – cannot work, even in principle, unless design choices are made which, necessarily, remove the only real advantage blockchain technology offers, and leave us with a wasteful and slow

---

[1] See Philip Hammond, Speech at the Conservative Party conference, 1 October 2018; see BBC News, "Could Blockchain solve Irish border issue?", 2 October 2018, <https://www.bbc.co.uk/news/technology-45725572> (accessed 30 May 2019). It has also been suggested that Brexit constitutes a "golden opportunity for the City of London to […] take the lead in the new digital revolution of blockchain"; see David Blake, *Brexit and the City* [2018], available at SSRN: https://ssrn.com/abstract=3183017 (accessed 16 October 2019).

[2] See e.g. European Parliament, *Odometer manipulation in motor vehicles: revision of the EU legal framework* (2017/2064(INL)), suggesting the exploration of using a blockchain-based system for fighting odometer fraud, which would require every car in Europe to be equipped with an always-on internet connection, and once this is achieved, would then involve choosing a ludicrously inefficient system for solving the problem. See also HM Land Registry, "HM Land Registry to explore the benefits of blockchain", 1 October 2018, available at <https://www.gov.uk/government/news/hm-land-registry-to-explore-the-benefits-of-blockchain> (accessed 16 October 2019). Similarly, the Swedish land registry has also been testing the use of blockchain technology; see Shefali Anand, "A Pioneer in Real Estate Blockchain Emerges in Europe", Wall Street Journal, 6 March 2018, available at https://www.wsj.com/articles/a-pioneer-in-real-estate-blockchain-emerges-in-europe-1520337601 (accessed 16 October 2019). The Executive Director of the European Union Intellectual Property Office (EUIPO) has recently highlighted the perceived 'great potential' of blockchain technologies 'in the fight against intellectual property rights infringement'; see EUIPO, "EU Blockathon 2018 winners announced", Press Release 25 June 2018, available at <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/Blockathon/press/BLOCKATHON_PRESS_RELEASE_25jun2018_en.pdf> (accessed 4 November 2019).

database. A similar argument is shown to apply to so-called "smart contracts". Although it is possible to minimise or even eradicate the waste and computational overhead of blockchain solutions by, essentially, re-centralising the ledger, resulting systems so closely resemble traditional, widely available databases that there is little reason to expect significant benefits from their adoption compared to the status quo. Instead, it will be shown that the apparent benefits of blockchain solutions typically stem from inter- and intra-organisational standardisation of data structures and flows, and ignore or underestimate the well-known difficulties of effecting technological change and abandoning legacy solutions in the real world – and perhaps particularly so in the financial sector.

The paper further argues that there is no reason to expect legislators to change current legal principles in sufficiently dramatic fashion so as to carve out a space in which non-currency applications of blockchain technology can usefully be implemented, since the oft-promised potential efficiency gains supposedly stemming from the adoption of blockchain technology are based on a flawed analysis of costs and benefits. Legal and practical obstacles therefore mean that, at least outside its original and circumscribed realm of cryptocurrencies, blockchain technology has no future.[3]

The paper proceeds as follows. Section II provides an introduction to blockchain technology, also suggesting non-technical ways in which lawyers and other non-technologists can conceptualise its functioning. In section III, I argue that what I call *"non-naked"* blockchains[4] are necessarily either incompatible with some of the core principles of our legal system, or, alternatively, must be designed in a way that inescapably renders their use suboptimal. Section IV explores, and dismisses, possible attempts to solve the unattractive choice between uselessness and inefficiency presented in section III by changes to our current legal system. Section V briefly explores possible technical solutions to these problems. Section VI concludes that crypto assets and smart contracts have no future.

II. RE-INVENTING SECURITISATION? A LAWYER'S VIEW OF BLOCKCHAIN TECHNOLOGY

A. A Functional Description of Blockchain Technology

It is not necessary for the purposes of this paper to examine the intricate technical details of blockchain solutions. Instead, I will provide a short functional description of blockchains, focussing on the aspects relevant to the legal argument advanced in the following section.

---

[3] There are also good reasons to doubt the viability of cryptocurrencies as meaningful parts of our financial system, but these are primarily economic, not legal, in nature; see recently e.g. Jon Danielsson, "Cryptocurrencies: Policy, Economics and Fairness" [2018] Systemic Risk Centre Discussion Paper No. 86, available at <https://ssrn.com/abstract=3276606> (accessed 15 September 2020).

[4] As defined below, section II.C.

Blockchain, or distributed ledger,[5] technology of the type of interest to this paper was first described in a paper by a researcher, or group of researchers, using the pseudonym Satoshi Nakamoto.[6] In their paper, the authors describe a protocol for the creation and governance of an electronic payment system which, similar to physical cash, allows for trustless[7] peer-to-peer exchanges. While a number of implementations for electronic cash had been proposed,[8] and in some cases implemented,[9] since the early 1980s, Nakamoto's paper was arguably the first to offer a complete and precisely specified solution to the so-called double spending problem.

Conceptually, the double spending problem is a consequence of two basic features of electronic communications. First, any information transmitted electronically can always and necessarily be replicated or "replayed" by the original sender, any recipient, as well as any third party who can listen in on the communication.[10] Unlike with sending or forwarding a physical letter by mail, sending an electronic message to another person obviously does not entail the sender no longer "having" that message.

Second, there is no easy way to chronologically order a set of messages sent by one party in such a way that every third party will reliably agree with such ordering.[11] Put

---

[5] There are no universally accepted definitions of the terms "blockchain" and "DLT"; for a helpful discussion see e.g. KFK Low and E Mik, "Pause the Blockchain Legal Revolution" (2020) 69 *International and Comparative Law Quarterly* 135. For the purposes of the present paper, blockchains are the most important implementation of distributed ledger technology. Non-blockchain distributed ledgers differ from blockchains in some important technical aspects, but these differences are largely irrelevant to the argument advanced in this paper – primarily because this paper highlights problems connected to decentralisation, which are equally relevant to other DLT solutions. For an example of a non-blockchain DLT solution see e.g. the solution proposed by IOTA (www.iota.org); see Serguei Popov, "The Tangle" [2015] available at https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (accessed 15 September 2020).
Of course, many of the cryptographic concepts used in blockchains can, and frequently are, used in non-DLT projects and protocols; the scepticism expressed in this article does not relate to these underlying technologies.

[6] Satoshi Nakamoto, "Bitcoin: A peer-to-peer electronic cash system" (2008), available at <https://bitcoin.org/bitcoin.pdf> (accessed 16 October 2019).

[7] See on the meaning of "trustless" in the present context below text to n 35-37.

[8] See e.g. David Chaum, "Blind signatures for untraceable payments" in: Chaum et al, *Advances in cryptology* (Boston: Springer 1983) 199; see also Nick Szabo, "Bit Gold" (2005) *Unenumerated Blog* available at <http://unenumerated.blogspot.com/2005/12/bit-gold.html> (accessed 30 May 2019). See David Gerard, *Attack of the 50 Foot Blockchain* (2018) for an excellent brief summary of Bitcoin's history.

[9] David Chaum's "DigiCash" (subsequently "eCash") allowed for anonymous digital transactions by leveraging public key cryptography. Unlike the technology underlying Bitcoin, Chaum's way of achieving anonymous payments was protected by patent, and relied on a single central party to confirm transactions. For an excellent overview of the precursors of Bitcoin, see Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder, *Bitcoin and cryptocurrency technologies: a comprehensive introduction* (Princeton University Press 2016) XIII-XX. See also David Gerard, *Attack of the 50 Foot Blockchain* (2018). Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge MA: Harvard University Press 2018) 18-20.

[10] Note that even where the relevant communication is encrypted, and the underlying clear text (i.e. unencrypted) content cannot easily be extracted from the transmitted data, the transmission itself (i.e. the encrypted "ciphertext"), can always be faithfully replicated by a third party "listening" to the transmission. In case the transmission occurs over the Internet, this would typically include a number of untrusted servers forwarding (parts of) the message in question.

[11] That *some* events cannot necessarily be put into an observer-independent chronological order is of course also true on a more fundamental level (i.e. due to the laws of physics; Albert Einstein, 'Zur Elektrodynamik bewegter Körper' (1905) 17 *Annalen der Physik* 891), but this fact is of little relevance in the real world, since conflicting transactions will almost always be timelike-separated (i.e. have an objective order). For a discussion of this "problem" in the context of intergalactic payments, see Abrahim Ladha, 'Hypothetical Problems concerning the Theory of Relativity on Cryptographic Currency Implementations' [2016] *arXiv preprint*,

differently, when a user, Alice, sends two electronic messages – say, one to Bob and one to Carol – there can be no guarantee that Bob and Carol, or indeed any third party observer, will agree on which of the two messages was sent first.[12]

Each observer, including Bob and Carol, who learns about the two messages will of course *subjectively* be able to decide which of the two messages he or she received first. But where the messages were sent via a computer network resembling the internet, in which messages do not all pass through a single central network node,[13] the sequence in which any network participant receives the two (or more) messages will be affected by factors such as network congestion, the relative location within the network, relative geographic location, and others.[14]

The inability to objectively or chronologically order two messages poses a seemingly insurmountable problem for the creation of a protocol allowing for peer-to-peer transfers of digital assets.[15] Let us assume that we agree on an initial allocation of some arbitrary digital asset, for instance an electronic boarding pass entitling the "holder" (rather than the person who initially acquired it) to board a train, or perhaps a discount voucher issued by a retailer.[16] Technical solutions have long existed to reliably verify the authenticity of a message,[17] so that it would in principle be possible to allow for the peer-to-peer transfer of our digital asset. Not unlike in the case of a bill of exchange, any holder could effectively transfer the digital asset by signing and sending it to a third party, who could now be treated as the new holder, provided a complete chain of signed transactions (akin to "indorsements" in the case of bills) exists between the original allottee of the digital asset in question, and the current holder of record.[18]

Due to the abovementioned impossibility of an objective mechanism for chronologically ordering messages, however, the described system for peer-to-peer transfers of digital assets is inherently unstable. While it is easy to verify whether a message has been sent from one user to the other,[19] a valid transfer that follows the basic logic of *nemo dat*[20] will also depend on when it was sent: the original, or any intermediate, holder

---

available at <https://arxiv.org/abs/1604.04265> (last accessed 4 November 2019). The ordering problem described here is much broader in that it prevents the chronological ordering of events (messages) for which an objective order does exist.

[12] For a more detailed explanation of the double spending problem, see e.g. Narayanan et al., n 9 above, 22-24.

[13] Note that, even a centralised network would not necessarily solve this problem.

[14] See e.g. Narayanan et al., n 9 above.

[15] I use the term "digital asset" loosely in the present context. For a recent attempt of defining and classifying such digital assets, see e.g. UK Financial Conduct Authority, 'Guidance on Cryptoassets' [2019] *Policy Statement PS19/22*, available at <https://www.fca.org.uk/publication/policy/ps19-22.pdf> (last accessed: 4 November 2019). See also Garrick Hileman and Michel Rauchs, "2017 Global Blockchain Benchmarking Study" (Cambridge Centre for Alternative Finance 2017), available at <https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf> (accessed 4 November 2019).

[16] While these two examples correlate with legal rights, the same is true for digital assets which do not, such as "items" a used may acquire within a computer game.

[17] I.e. that a message was indeed authored or "signed" by a particular user.

[18] There are projects that attempt to replace traditional bills of exchange with blockchain-based tokens; see e.g. <https://billex.org/main/learnmore> (accessed 4 November 2019).

[19] From a technical perspective, it would be trivial to ensure that messages indicate the subjective or *claimed* chronological order in the chain of transactions.

[20] i.e. the principle, stemming back to Roman law, that 'no one can give a better title than he himself possesses' (*Bishopsgate Motor Finance Corporation Ltd v Transport Brakes Ltd* 1 [1949] 1 KB 322). The *nemo dat* rule is a feature

may have validly signed two separate messages, purporting to transfer the digital asset in question to two different transferees. Absent a mechanism to establish a network-wide consensus on which message was sent first, different users of the protocol would now disagree on the rightful holder of the digital asset. Unlike in the case of (order) bills of exchange, where repeated and conflicting indorsements would necessitate the creation of perfect (or near-perfect) forgeries, the two or more electronic messages sent by the dishonest transferor are by their very nature indistinguishable.[21] This feature of digital communication poses a significant problem for creating a protocol for the electronic exchange of digital assets between users, and solving it in a satisfactory way has eluded cryptographers for decades.

Before looking at the way in which blockchain technology addresses this problem, it is worth calling to mind the more common way to ensure authoritative record-keeping, especially in areas where the records kept are of economic significance. Insofar as the traditional financial system relies on network transmissions for the purposes of relaying transaction data, and also needs to decide on the chronological order of transaction messages, a simple and reliable solution to this problem exists. Transactions are simply "ordered" by a trusted party – e.g. a bank or some other intermediary. If someone tries to withdraw the last £100 in his account *twice*, for instance by near-simultaneously withdrawing cash from two different cash machines, no assurance can exist that the *real* chronological order of the two requests corresponds to that observed by the bank or other intermediary. This is, however, of little consequence, as the bank will simply accept the first *observed* instruction, and deny the second, irrespective of the actual sequence of events.[22] The bank or intermediary can thus be said to have central authority, as it keeps the authoritative records of one's account and can thus also conclusively decide the relevant order of events, rendering questions about the *actual* sequence irrelevant.

Conceptually, this is of course also the solution employed in the vast majority of other systems of record-keeping, by way of ledgers or otherwise, including the systems used to hold securities by ultimate owners, issuers, and the various layers of intermediaries in between,[23] land registries, and other databases of economic significance.

At least for the purposes of this paper, the main innovation in Nakamoto's paper was an ingenious solution to the problem of double spending discussed above.[24] The

---

of all civil and common law jurisdictions, although it is not without exceptions; see e.g. Jan H Dalhuisen, *Dalhuisen on Transnational Comparative, Commercial, Financial and Trade Law* (Oxford: Hart 2014) regarding the different approaches in relation to *bona fide* purchaser protection.

[21] Depending on the design of the protocol, the messages would likely differ in their exact content, but not in their seeming validity.

[22] The same is true in case different payees present two or more cheques drawing on an insufficient aggregate balance. The bank will generally refuse the cheques based on the order in which it processes them.

[23] For a discussion of the current system see e.g. Eva Micheler, "English and German Securities Law – a thesis in doctrinal path dependence" (2007) 123 *Law Quarterly Review* 251; for a discussion of the use of blockchain technology in the area of securities holdings, see Philipp Paech. "Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?" (2016) 21 *Uniform Law Review* 612; Eva Micheler and Luke von der Heyde, "Holding, clearing and settling securities through blockchain/distributed ledger technology: creating an efficient system by empowering investors" (2016) 31 Journal of International Banking & Financial Law 652. See also Philipp Paech, "The governance of blockchain financial networks" (2017) 80 *Modern Law Review* 1073.

[24] See also Martin Walker, *Front-to-Back: Designing and Changing Trade Processing Infrastructure*, Ch 19.

blockchain solution proposed by Nakamoto, a slightly modified version of which was then implemented as the Bitcoin protocol,[25] combines a number of known and well-understood cryptographic algorithms (or "primitives") to create a unique consensus mechanism that, in any given situation, allows for different, unrelated parties to all agree on a single sequence of transactions. The protocol does not (and could not possibly) lead to a reliable choice of the *true* sequence of events by the network, but by ensuring that one single sequence of transactions can be agreed upon by all participants in the network, it can simply treat this single choice as *authoritative* – much like a bank does in the attempted double cash-withdrawal example above. Remarkably, and counterintuitively, Nakamoto's solution achieves this consensus without relying on a single central authority to keep the "master record", or indeed anyone treated as "privileged" within the protocol.

Without going into too much detail about the technical implementation, it is worth noting that the manner in which the consensus is achieved in Bitcoin and other blockchain protocols based on the Bitcoin paper,[26] is what can perhaps be described as "wasteful by design". Rather than relying on a central authority, the authoritative history of transactions is authored, in "blocks" each summarising the last ten minutes of activity, by one of the many network participants (the so-called miners). The selection of one, out of all possible, miners to determine the next block of transaction history is based on a type of race to solve a special puzzle which involves conducting increasingly difficult, and hence costly, and entirely useless[27] calculations.[28] The first miner to solve the puzzle thus determines what counts as transaction history within the network, subject to the constraints that the history described (i) must be compatible with the previous record[29] and (ii) cannot include transactions unless they are validly signed by the transferor.

In Bitcoin, Ethereum, the second-biggest protocol,[30] as well as most other major blockchain networks, the incentive to participate in this race to solve the puzzle is created

---

[25] The exact design of the blockchain solution contained in the Bitcoin paper (Nakamoto n 6 above) is of limited importance for the argument presented here; the description in the text is highly simplified and incomplete.

[26] Currently, the vast majority of blockchain-based activity takes place within networks based on Nakamoto's paper (n 6 above). Several proposals exist to replace this system with alternative protocols (see e.g. See e.g. Vitalik Buterin and Virgil Griffith, "Casper the friendly finality gadget" [2017] available at <https://arxiv.org/pdf/1710.09437> (accessed 30 May 2019); Vlad Zamfir, Caspar the Friendly Ghost - A "Correct-by-Construction" Blockchain Consensus Protocol, [2017], available at <https://github.com/ethereum/research/blob/master/papers/CasperTFG/CasperTFG.pdf> (accessed 30 May 2020)), but these have not yet been widely adopted. These so-called proof-of-stake (PoS) protocols (as opposed to proof-of-work (PoW) protocols) aim at achieving a randomised selection of the "historian of record" without the need for puzzle-solving. Instead a selection is made with a probability proportional to resources put at stake by network participants. For an economic analysis of PoS protocols, see Fahad Saleh, "Blockchain Without Waste: Proof-of-Stake" (2018) available at: <https://ssrn.com/abstract=3183935> (accessed 28 May 2020).

[27] By useless I mean that the calculations serve no use or purpose beyond their role in forming part of the economic incentive system that secures the integrity of the protocol itself. It is in principle possible to use the waste heat produced by the calculations, e.g. for domestic heating.

[28] The puzzle involves repeatedly evaluating a cryptographic hash function, SHA-256, by adding random characters to the proposed block. A highly accessible summary and explanation is provided by Narayanan et al (n 9 above).

[29] This is further ensured by "chaining" the blocks together by including a digest of the immediately previous block in each new block.

[30] Ethereum is the second-biggest blockchain project by "market capitalisation" (see e.g. data collected by CoinMarketCap, available at https://coinmarketcap.com/ (last accessed 8 July 2019). While market capitalisation is a highly questionable metric (it is the product of the number of outstanding crypto "tokens"

by a rule within the network protocol which rewards the winner of the race with a "special grant" of Bitcoins (or other tokens/digital assets in the case of alternative blockchains). Importantly, this race does *not* automatically result in the victory of the miner with the greatest computing power devoted to solving the puzzle,[31] but instead ensures that the probability of a victory is proportional to the computing power used. This introduces a vital element of chance to the algorithm choosing the next "historian of record" of the network.

Computations necessary for solving the puzzles of different blockchain protocols come at enormous financial and environmental cost.[32] In a way, this cost is an integral feature, rather than a bug, of the protocol. Like a peacock's tail, the function of which can be said to entirely consist of and depend on its wasteful costliness,[33] the fact that the computations necessary to win the race are very costly disincentivise the creation of both invalid blocks and entire alternative histories.

It is in this sense that blockchains are sometimes referred to as "immutable", or at least tamper-proof:[34] changing anything about the agreed history of transactions, such as reversing a transaction, necessitates the re-writing of an entire consistent history, from the point in time at which the unwanted transaction took place, until the present. Given the cost of solving the mandatory puzzles, doing this in relation to all but the most recent transactions is likely to prove prohibitively expensive for any network with significant mining activity.

B. Blockchains as "Cash Fax Machines"

From a legal perspective, the functioning of blockchains is interesting insofar as it permits universal ledger-based record-keeping while at the same time enabling trustless[35] peer-to-peer transactions. "Trustlessness", in this context, simply means that it is at least in principle possible for participants in the protocol to agree, first, that the single record (ledger) created by following the protocol's consensus rules is indeed authoritative, and second, that no party can unilaterally force the reversal of already recorded transactions. Where these two conditions are met, entries on the distributed ledger can now be treated

---

and their market price on crypto exchanges), it provides a rough approximation of the level of investment and interest in blockchains. The "market capitalisation" of Ethereum, so defined, currently (September 2020) stands at around USD 40 billion, whereas the notional value of all Bitcoin ever mined stands at around USD 200 billion.

[31] As in a classic race which invariably leads to the fastest participant winning.

[32] See Camilo Mora et al., "Bitcoin emissions alone could push global warming above 2° C" (2018) 11 *Nature Climate Change* 931; Max J. Krause and Thabet Tolaymat, "Quantification of energy and carbon costs for mining cryptocurrencies" *Nature Sustainability* (2018): 1.

[33] The so-called handicap principle; see Amotz Zahavi, "Mate selection—a selection for a handicap" (1975) 53 *Journal of Theoretical Biology* 205.

[34] See on terminology Angela Walch, "The path of the blockchain lexicon (and the law)" (2016) 36 *Review of Banking & Financial Law* 713, 735, highlighting the problems of labelling blockchains immutable.

[35] Blockchain-based transactions and relationships are often described as "trustless"; on the use of this term, see e.g. Walch, ibid, at 722.

as (digital) assets with features arguably more akin to chattels,[36] where physical possession is conceptually replaced by being the holder of record.

As long as the information recorded on the ledger relates to something approximating a currency, the closest real world analogue is, of course, cash – which was the very design goal underlying Bitcoin's creation.

This can be demonstrated by a near-accurate[37] (if unrealistic) analogy. Assuming the protocol works as intended, the functioning of a simple blockchain ledger could be replicated by a hypothetical world-wide network of fax machines, provided that each machine reliably shreds or otherwise destroys every "original" it sends, and where copying a received fax message[38] is technically infeasible. If such a network of fax machines existed, we could easily implement a system of peer-to-peer payments – people could simply fax banknotes between each other. Since receipt of a faxed banknote would guarantee the original banknote's destruction, there would be little reason not to treat the faxed banknotes as being equivalent to the original.

C. "Naked" Blockchains and Crypto Assets

The ideas presented above can be extended more directly into the realm of law, once we come to view blockchains as, simply, ways to store information in a distributed and decentralised manner. For this it may be useful to distinguish between two distinct types of blockchain records for the purposes of this paper: first, there are what I call "naked blockchains", which are generally in line with the description above.[39] Second, there are what I call "crypto assets". These concern applications of blockchain technology to represent what the legal system generally also recognises as assets, including contractual rights.

"Naked" Blockchains

The above description of blockchain technology has so far implicitly focussed on *naked*[40] blockchains. What defines a coin, token, or more generally a ledger entry, as belonging to the naked blockchain category in my terminology is that the protocol describing, creating, and governing it is self-contained in the sense that all transactions concerning it can be agreed and, crucially, executed and settled, within the protocol itself.

---

[36] The obvious parallel is the history of the negotiable instrument. Bills and notes, while technically representing a debt, have long represented a species of property in the hands of their holders; see e.g. M Lobban, "Negotiable Instruments" in W Cornish et al (eds) *The Oxford History of the Laws of England: Volume XII: 1820–1914 Private Law* (Oxford, OUP 2010) 743-748. See also section IV.A below.

[37] Even simple blockchains, such as the database behind Bitcoin, provide some additional functionality, such as multi-sig transactions, the implementation of which would be somewhat harder in the example used here.

[38] I.e. duplicating a received fax message such that it cannot be distinguished from the original when sent to another party.

[39] See also FCA, n 15 above, Low and Mik, n 5 above, and Hileman and Rauchs, n 15 above, for alternative classifications. Note that "naked" or "native" blockchain assets are not equivalent to so-called "utility tokens", as the latter are generally designed to entitle the holder to access services or content which are not (usually) offered within the protocol. Exceptions exist; see e.g. Protocol Labs, 'Filecoin: A Decentralized Storage Network' [2017] available at <https://filecoin.io/filecoin.pdf> (last accessed 4 November 2019).

[40] Assets on what I refer to as naked blockchains are also referred to as "native" blockchain assets; see also Hileman and Rauchs, n 15 above and Low and Mik, n 5 above.

For instance, the transfer of Bitcoins from one person to another does not involve an ancillary or secondary promise of something else happening (in the physical, or legal, world) the expectation of which is expressed by the transfer of Bitcoins. When two or more people agree to transfer Bitcoin, and this transfer does in fact take place according to the rules of the Bitcoin protocol, the transferor will by definition have fulfilled his part of the bargain, and the transferee will by definition have received what she has bargained for. The same is true for all other cryptocurrencies.

From this perspective, cryptocurrencies are indeed akin to cash: transferring what is analogous to a bank note does, by definition (and legal tender rules) settle a liability. No express or implied promises will typically have been made regarding the transferred asset's qualities, and the asset does not represent anything else which may for instance be defective from the transferee's perspective.

There also exists a class of native digital assets that, likewise, do not have a real world correlate, and where the protocol used for recording transactions that have taken place is self-contained in much the same way as in the case of cryptocurrencies. One example are the so-called "CryptoKitties", which are, in essence, unique digital collectibles, rendered transferable by the protocol that created them. In relation to these naked blockchains, law plays only a limited role. Just like the rules of a video game are not usually subject to scrutiny by the legal system,[41] even where certain achievements, trophies, or the like may have value both to the person holding them and in the eyes of others.

Crypto Assets

Of course, the functioning of the core technology does not depend on the nature of what is recorded in the ledger. It is then perhaps unsurprising that an old idea was reborn soon after blockchains started to attract more widespread attention: the use of the distributed ledger for what is intended to be akin to a negotiable instrument or a bearer share certificate.[42]

As explained above, blockchains allow for the peer-to-peer transfer of what are essentially unique digital assets, so there is nothing in principle that would prevent us from

---

[41] Of course, video games can still be subject to regulation, especially where in-game behaviour manifests itself outside a game; see e.g. Brett Abarbanel "Gambling vs. gaming: A commentary on the role of regulatory, industry, and community stakeholders in the loot box debate" (2018) 22 *Gaming Law Review* 231. In the same way, the use of fiat money to pay for native digital assets recorded on a blockchain can, and in part already is, subject to regulation. See e.g. BaFin, "Bitcoins: Aufsichtliche Bewertung und Risiken für Nutzer" (2013) available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html (accessed 1 May 2019). EBA, "EBA Opinion on 'virtual currencies'" (2014) available at: <http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf> (accessed 30 May 2019)

[42] See e.g. David Yermack, "Corporate Governance and Blockchains" (2017) 21 *Review of Finance*, 7; Eva Micheler. "Intermediated Securities from the Perspective of Investors: Problems, Quick Fixes and Long-term Solutions" in Louise Gullifer and Jennifer Payne (eds.) *Intermediation and Beyond* (Oxford: Hart Publishing 2019) Chapter 12; Christoph Van Der Elst and Anne Lafarre, "Blockchain and Smart Contracting for the Shareholder Community" (2018) ECGI Law Working Paper No 412/2018, available at: <http://ssrn.com/abstract_id=3219146> (accessed 30 May 2019); see also Michele Finck, *Blockchain Regulation* (Cambridge: Cambridge University Press 2019). The potential of "digital bearer certificates" has already been discussed in the 1990s by Nick Szabo; see e.g. Nick Szabo, "Formalizing and Securing Relationships on Public Networks" (1997) 2 *First Monday*, available at <https://doi.org/10.5210/fm.v2i9.548>.

treating these digital assets as electronic representations or "embodiments" of proprietary or contractual rights. This is reminiscent of the way most European legal systems have treated negotiable instruments for many centuries.[43] There are few limits to what can, in principle, be represented by a security. Some assets can directly be securitised, for others, a special purpose vehicle (SPV) holding the asset can be created, with shares or other securities issued by the SPV (economically) representing the underlying asset. It would thus seem that blockchain technology could be used for all sorts of situations in which assets are transferred.[44] The underlying or backed assets could of course also include traditional fiat currency or equivalents (now often referred to as "stablecoins"), as well as more traditional securities.

"Smart Contracts"

Similarly, the fact that a blockchain can store arbitrary data has led people to realise that a blockchain can also be used as a sort of public memory for storing computer programs as well as their (intermediate) outputs. Depending on the implementation, this can then be used to run computer programs in a decentralised, transparent, and objective manner. The possibility of step-wise execution of computer programs in a decentralised fashion is relevant for the concept of "smart contracts",[45] seen by some as a potentially disruptive technological innovation for the law.[46]

The key idea behind smart contracts is that a traditional legal contract can in many ways be conceptualised as a series of contingent ("if … then") statements, which of course is also true for computer programs.[47] Smart contracts then fuse contracts and computer programs together by envisioning computer programs written in a way that mirrors what two or more parties agree to in a contract. The resulting smart contract, despite being neither "smart" nor the actual contract,[48] would then be a formalised and machine-executable record of the actual agreement reached by the parties.

---

[43] See James S Rogers, *The Early History of the Law of Bills and Notes* (Cambridge: Cambridge University Press CUP 1995) 44, 151; Eva Micheler *Property in Securities - A Comparative Study* (Cambridge: Cambridge University Press 2007); Matthias Lehmann, *Finanzinstrumente: vom Wertpapier- und Sachenrecht zum Recht der unkörperlichen Vermögensgegenstände* (Mohr Siebeck 2009).

[44] Details may differ across jurisdictions, but as long as something akin to share certificates can be so represented, most assets can at least indirectly be represented by the digital assets recorded in the blockchain.

[45] The term goes back to an article by Nick Szabo ("The Idea of Smart Contracts" (1997), available at http://szabo.best.vwh.net/smart_contracts_idea.html (accessed 30 May 2019)). For excellent explanations of smart contracts, see e.g. Kevin Werbach and Nicholas Cornell, "Contracts Ex Machina" (2017) 67 *Duke Law Journal* 313; T Cutts, Smart Contracts and Consumers (2019) 122 *West Virginia Law Review* 389.

[46] Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and The Rise of Lex Cryptographia' (2015) available at <https://papers.ssrn.com/ abstract_id=2580664> (accessed 28 May 2019).

[47] For an excellent discussion, see Shaanan Cohney and David A. Hoffman, "Transactional Scripts in Contract Stacks" 2020 *Minnesota Law Review* (forthcoming). See also Deborah R Gerhardt and David Thaw, "Bot Contracts" (2020) Arizona Law Review (forthcoming).

[48] See Edward Felten, "Smart contracts: neither smart nor contracts?" (2017) Freedom to Tinker, available at <https://freedom-to-tinker.com/2017/02/20/smart-contracts-neither-smart-not-contracts/> (accessed 30 May 2019); see also Karen Levy, "Book-smart, not street-smart: blockchain-based smart contracts and the social workings of law" (2017) 3 *Engaging Science, Technology, and Society* 1.

To the extent that the parties to the contract[49] also ascribe value to digital assets existing within the protocol used for the smart contract,[50] such an agreement can in principle be designed to be "self-executing".[51] By this I mean that a conditional statement in the computer program, such as 'once the year 2020 starts, 10 coins shall be transferred from Alice to Bob' can be an accurate description of the contractual agreement existing between Alice and Bob, and they can ensure that this program is (largely) irrevocably run by the network as a whole, and will thus trigger the actions agreed to without Alice having to take any further action (or indeed without her having a way to stop the execution). The decentralised nature in which the smart contract can be run means that the contracting parties do not need to trust a third party to give effect to or allow the execution of the smart contract. Some scholars believe that smart contracts could significantly reduce transaction and enforcement costs, and thus disrupt a number of industries, including the practice of law.[52]

D. The Market for LemonCoins

Before looking at some of the legal challenges faced by the many ambitious blockchain projects, it is worth mentioning briefly the uses to which the "crypto asset"-variety of blockchain projects has so far been put.

In his *Extraordinary Popular Delusions and the Madness of Crowds,*[53] Mackey tells the story of a 'man of genius' who defrauded the British investing public during the South Sea Bubble as follows:

> [T]he most absurd and preposterous of all, and which showed, more completely than any other, the utter madness of the people, was one, started by an unknown adventurer, entitled "A company for carrying on an undertaking of great advantage, but nobody to know what it is." […]
>
> Crowds of people beset his door, and when he shut up at three o'clock, he found that no less than one thousand shares had been subscribed for, and the deposits paid. He was thus, in five hours, the winner of 2,000 pounds. He was philosopher enough to be contented with his venture, and set off the same evening for the Continent. He was never heard of again.[54]

---

[49] That is the *actual* contract, not the "smart contract"; the latter is merely a technical implementation of the former. See also Felten, ibid; Levy, ibid. See also Michele Finck, *Blockchain Regulation* (Cambridge: Cambridge University Press 2019).

[50] Or otherwise accessible by it.

[51] On some of the technical limitations arising from the complexity of the necessary operations, see Cohney and Hoffman (n 47 above).

[52] See e.g. Wright and De Filippi, n 46 above. Wulf Kaal and Eric Vermeulen, "How to Regulate Disruptive Innovation: From Facts to Data" (2017) 57 *Jurimetrics* 169.

[53] Charles Mackay, *Extraordinary Popular Delusions and the Madness of Crowds* (London: Richard Bentley 1841).

[54] ibid at 88.

To a modern reader, the story may seem hard to believe: why would the investing public willingly hand over significant sums of money to an entirely unknown businessman in return for the vaguest of promises? When compared to some of the recent successful fundraising activities of blockchain start-ups, however, these poor investors almost appear as beacons of prudence. Though it may have been foolish to invest in an entirely unknown venture run by a stranger without any credentials, when buying shares in the company embarking on it, one would at least be entitled to any surplus it may – against all odds – create. In the case of a typical "token sale" or ICO,[55] this is typically not the case. A recent study, analysing the fifty top-grossing ICOs of 2017 which jointly raised around $ 2.6 billion USD, finds that in many cases the promoters did not even *promise* to protect the financial interests of investors.[56]

Partly in anticipation of or as reaction to the risk of enforcement action by, primarily, financial regulators across the world,[57] it has become increasingly common for sellers of "crypto tokens" to state, explicitly, that what they sell has no value, does not entitle the holder to any future cash flows, and in some cases, to state that the digital assets (or tokens) on sale lack *any* features, functionalities, uses, or any other purpose.[58] Usually, this has not proven to be a major obstacle to raising significant sums of money. In some (successful) cases, even projects explicitly marketed as Ponzi or pyramid schemes managed to attract significant funding, in some cases to the amazement of the (joking) initiators.[59] One coin, specifically and openly created as a joke, Dogecoin, at some point reached a market value of about £ 1.5 billion.[60]

Where issuers do not explicitly state that the digital assets they sell are use- and worthless, the project descriptions often still beggar belief. It was possible to buy tokens that are supposedly pegged to the price of bananas; buy coins that can then be spent at

---

[55] ICO stands for "Initial Coin Offering", in reference to IPOs of shares in companies.

[56] See Shaanan Cohney, David Hoffman, Jeremy Sklaroff and David Wishnick, 'Coin-Operated Capitalism' (2019) 119 *Columbia Law Review* 591.

[57] See recently e.g. US Securities and Exchange Commission, *Statement on Digital Asset Securities Issuance and Trading*, Public Statement dated 16 November 2018, available at <https://www.sec.gov/news/public-statement/digital-asset-securites-issuuance-and-trading> (last accessed 13 December 2018). See also Marco Dell'Erba, "Initial Coin Offerings: From Inactivity to Full Enforcement. The Implementation of the 'Do No Harm' Approach" [2018] available at <https://ssrn.com/abstract=3194863> (accessed 13 December 2018).

[58] See e.g. the EOS Token Sale, archived at https://archive.is/m3D1T (accessed 9 December 2018), stating that EOS tokens (the sale of which raised a total of almost USD 4 *billion*) *'do not have any rights, uses, purpose, attributes, functionalities or features, express or implied, including, without limitation, any uses, purpose, attributes, functionalities or features on the EOS Platform'*. See also Gerard, n 8 above, chapter 9.

The same unflattering description of the digital assets offered for sale has subsequently been adopted by, among others, TokenStars (see TokenStars Company, *Whitepaper*, available at: <https://tokenstars.com/upload/files/ace_by_tokenstars_whitepaper.pdf> (accessed 30 May 2019)), Binex, (see Binex Terms & Conditions, available at: <https://www.binex.trade/terms> (accessed 11 December 2018)), Smartchain, (see Smartchain Token Purchase Agreement, available at: <https://smartchain.io/purchase-agreement> (accessed 11 December 2018)) , Stattm, (see Stattm Ltd Disclaimer, available at: <https://stattm.com/disclaimer/> (accessed 11 December 2018)); Gemera (see Gemera Tokens Purchase Agreement, available at: <https://www.gemera.io/purchase-agreement.html> (accessed 11 December 2018)), and many others.

[59] See e.g. PonziCoin; the project's website has recently been updated to claim that the project was a *'parody art performance/joke'* and to sdvice visitors to *'[p]lease be careful when investing in shady cryptocurrencies, especially ones that look like pyramid schemes'* (see statement available at <https://ponzicoin.co/home.html> (accessed 11 December 2018)).

[60] See Gerard, n 8 above, Chapter 9.

dentists for no obvious reason; and one (now seemingly abandoned project) proposed a token sale for enrolment in a blockchain university – not to learn about blockchain, but rather to study Classics in a "digital institution" that replaces the university administration with smart contracts. Many more examples exist. Given the opacity of this part of the economy, the real source of funding is often hard to ascertain. It thus cannot be excluded that at least some of the fundraising activity is, in reality, little more than a small step in a larger money laundering scheme. To the extent this is true, the ludicrousness of the ventures may sometimes be an essential design element, protecting, rather than harming unwitting investors.[61] There can be no doubt, however, that vast sums of real money have been and continue to be invested in a still-growing number of crypto asset projects. It perhaps suffices to say that expecting blockchain to solve the Northern Irish border question would count as a relatively conservative and cautious venture in the world of blockchain.

III. BLOCKCHAINS AND THE LAW AS A SYNCHRONISATION PROBLEM

As discussed above, the core innovation of blockchain technology is the leveraging of cryptographic tools to solve the double spending problem. Although this is undoubtedly a significant accomplishment from an engineering perspective, it does not automatically follow that there are real world use cases for the technology. It is important to keep in mind, first, that the double spending problem only arises in situations where there is no single trusted central record keeper, who could achieve the same result at a cost several magnitudes lower than that associated with the blockchain solution.[62] Second, and crucially for the argument presented here, as far as crypto assets are concerned[63] the legal system *itself,* and courts in particular, can be understood as a mandatory central authority that is the ultimate arbiter of how assets are assigned to owners or right holders. To make this point, it may be useful to conceptualise the legal system as a whole as a ledger recording

---

[61] To the extent that financial intermediaries are willing to accept as facially legitimate and make available to the promoters funds raised through a public token sale (i.e. typically the proceeds from the sale of the raised cryptocurrencies) despite their inability to identify the "investors" or trace the origin of the funds used, token sales could obviously be used for money laundering purposes. In this scenario, actually raising *outside* funds through the token sale would be counterproductive for the scheme creators, as these outside investors may draw unwanted attention to, and have economic expectations regarding, the project. Making projects maximally unattractive to outsiders would thus be an important feature of such schemes.

[62] While the particular implementation based on the Bitcoin protocol and chosen by most blockchains today may well be superseded by somewhat more efficient solutions in the future, there is little reason to be expect the dramatic reduction in computational overhead that would be needed to approximate the trivial cost of running a centralised record-keeping system.

[63] For an excellent analysis of the common law treatment of crypto*currencies,* see D Fox, "Cryptocurrencies in the Common Law of Property" in: D Fox & S Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, Oxford, 2019) 139. See also UK Jurisdiction Taskforce, "Legal statement on cryptoassets and smart contracts" (November 2019), available at https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf (last accessed 15 September 2020).

legal rights and their owners. Based on this - admittedly somewhat simplistic and unusual - conceptualisation, the legal role of blockchains can be understood as a problem of synchronisation: How can the assignment of legal rights, as seen through the lens of the legal system, be kept in sync with the records kept within a blockchain protocol?

A. Legal Obstacles for Creating Meaningful "Crypto Assets"

To answer this question, two facts applicable to *any* system of legal norms must be acknowledged:

First, even the most party autonomy-friendly systems of private law will place a number of inviolable limits on the agreements that can lawfully be entered into and that the legal system will enforce.[64] English law, for instance, is rightly regarded as particularly committed to party autonomy and freedom of contract, especially when compared to Continental European civil law jurisdictions.[65] Under the doctrine of contractual estoppel it allows parties to enter into agreements under an assumption of circumstances that are demonstrably untrue if they so choose; parties can agree to proceed on the basis that each party understands risks associated with a complex transaction, that they have read the full documentation relating to the transaction, or indeed that they made a payment, when in reality all parties know the stated facts to be untrue.[66]

Nevertheless, even under English law, there are several categories of cases in which no amount of careful defensive drafting, and no representation made by either party, can prevent a contract from falling apart. Fraud is perhaps the clearest example – it 'unravels everything',[67] or, as Braithwaite puts it, it is *'as Kryptonite is to Superman'* when it comes to contractual estoppel.[68] Similarly, where a party lacks legal capacity, wholly or for the purposes of specific types of agreement, the doctrine of *ultra vires* means that any contract entered into will be wholly void.[69] Where the contract is illegal, or where it contravenes public policy, it will typically also be unenforceable. Most civil law jurisdictions place more

---

[64] See on this problem also Werbach and Cornell, n 45 above; Paech (n 23 above).

[65] See e.g. Gunther Teubner, "Legal irritants: good faith in British law or how unifying law ends up in new divergencies" (1998) 61 *Modern Law Review* 11; see also Hugh Collins, "Good Faith in European Contract Law" 14 Oxford Journal of Legal Studies 229, 249;

[66] See e.g. the detailed discussion in Jo Braithwaite, "Springwell-watch: new insights into the nature of contractual estoppel" (2017) *LSE Legal Studies Working Paper* No. 12/2017, available at <https://ssrn.com/abstract=2983850> (accessed 30 May 2019).

[67] Lord Denning in *Lazarus Estates Ltd v Beasley* [1956] 1 QB 702, adding that fraud 'vitiates judgments, contracts and all transactions whatsoever'.

[68] Braithwaite, ibid., 23.

[69] See *Rolled Steel Products (Holdings) Limited v British Steel Corporation* [1986] Ch 246 at 304: *'If the transaction is beyond the capacity of the company it is in any event a nullity and wholly void: whether or not the third party had notice of the invalidity, property transferred or money paid under such a transaction will be recoverable from the third party.'* The *ultra vires* doctrine is nowadays of limited importance in relation to private companies in the UK and the EU (see e.g. David Kershaw, *Company Law in Context* (2nd ed.: OUP)), but can still play a role in relation to public bodies, some charities, and non-EU companies; see e.g. *Haugesund Kommune v Depfa ACS Bank* [2010] EWCA Civ 579, [2012] QB 549. See also Werbach and Cornell, n 45 above, on the limits these concepts place on smart contracts.

significant barriers on the range of agreements that can be entered into under private law than English law.[70]

Second, and in addition to the absolute limits every legal system places on agreements that can lawfully be entered into, it is worth noting something that is entirely obvious to any lawyer: there is currently no way to encapsulate the entirety of these legal limitations in the kind of algorithmically precise language that would allow for truly objective adjudication, and this is highly unlikely to change in the near future. This is to say that no system of rules, written in computer code or otherwise, can fully encapsulate and anticipate the full range of decisions a court with human judges may reach, and do so in a manner that enables different, independently acting, agents following these rules to always reach the same outcome. This is hardly a surprising statement for (or indeed by) a lawyer, as it is effectively equivalent to stating that all lawyers as a group cannot currently be replaced by robots (at least not without altering the outcome).

For example, agreements entered into under duress may be voidable and thus rendered unenforceable under virtually all systems of private law. The definitions of duress and other relevant factors will, of course, vary significantly across jurisdictions, but what connects them is the imprecision and vagueness with which the circumstances leading to a contract's unenforceability are defined.

Taken together, these two factors result in a situation in which no amount of engineering ingenuity or trickery can reliably guarantee that a consensus reached by market participants (i.e. the users of a blockchain database, for present purposes) will invariably reach the same conclusions that the court system would.[71]

B. Choice Between a Block and a Hard Place

It then follows from the two simple and – hopefully – uncontroversial statements that (a) the legal system must be the ultimate arbiter of how contractual and property rights are ultimately allocated to legal and natural persons, and that any legal systems places limits on what parties can agree to, and that (b) the entire legal system, including its decision-making mechanisms and institutions, is far too complex to be fully encoded in machine-executable code, that any ledger purporting to keep track of legal rights – be these property rights or contractual entitlements – faces a difficult design choice:

It could, first, accept what could be characterised as a one-way synchronisation from the legal system to the blockchain ledger. This would necessitate a system by which transfers, or other transactions carried out in accordance with the code governing the blockchain protocol, but deemed unacceptable by the applicable law, can and reliably will be reversed at the direction of a court. Alternatively, the blockchain system would have to accept a – permanent and very likely growing – "synchronisation conflict": A situation where the allocation of assets, as seen through the lens of the law, deviates from what the blockchain record reflects.

---

[70] E.g. AH Angelo and EP Ellinger, "Unconscionable contracts: A comparative study of the approaches in England, France, Germany, and the United States" (1991) 14 *Loyola of Los Angeles International and Comparative Law Journal* 455.

[71] See also Low and Mik, n 5 above, who arrive at a similar conclusion .

The Obvious Solution of a "Government Backdoor"

If, as seems likely, the potential users of crypto assets and smart contracts are interested in ensuring that their enjoyment of and their rights in relation to the real world assets represented by the ledger entries are protected and enforceable by the law, a system must be implemented to achieve the synchronisation mentioned above. This is an inescapable consequence of the inevitability that, at least occasionally, transactions happening in accordance with the rules of the blockchain protocol fail to also comply with the applicable legal rules. Where, seen through the eyes of the law, such transactions or transfers are void or voidable and can thus be reversed, failure to reflect this state of affairs on the blockchain risks affecting further blockchain transactions made on the assumption of the original, but unenforceable, transaction. Even these occasional conflicts between the state of the blockchain ledger and the actual state of legal rights can quickly erode the confidence in the non-authoritative ledger.[72] Soon there would be little reason to transact inside the blockchain protocol at all, as there can be little assurance that the transaction is not affected by an unreflected legal dispute further up the chain. Accepting the synchronisation conflict is thus simply not a useful option.

The obvious solution would be to ensure that the judicial system can directly correct the entries in the ledger – which of course is exactly the solution adopted by virtually every land registry or similar public register across the globe. Due to the decentralised nature of blockchain networks, however, ensuring the implementation of judicial decisions poses significant challenges for the design of the governing protocol. Since it seems implausible that every judicial decision would *voluntarily* and reliably be adopted by the network participants as part of their consensus system, the solution to this problem would involve either an actual "government backdoor", i.e. a rule of the protocol that enables state institutions to over-ride and reverse blockchain transactions at will, or providing these special powers of reversal and at-will alteration to some other central party that credibly commits to implementing judicial decisions. These two options are largely equivalent, and they would indeed reliably solve the problem identified.

Both solutions would however undoubtedly be met with vigorous opposition on ideological grounds alone, given the origins of the blockchain movement.[73] Putting ideological considerations to one side, the *real* problem with this type solution is one of technology. As I attempted to demonstrate in section II above, *the whole point* of the intricate consensus mechanism underlying blockchain technology is one of decentralised consensus. The remarkable achievement of creating an append-only ledger that is not centrally kept by any one person or organisation, the content of which can still be agreed among strangers by just following the rules of the protocol, comes at huge efficiency costs. For instance, running the Bitcoin network currently consumes as much energy as some

---

[72] See title insurance etc.

[73] See David Golumbia, *The politics of Bitcoin: Software as right-wing extremism* (U of Minnesota Press 2016); Gerard n 8 above, Chapter 2; Alan Feuer, *The Bitcoin Ideology*, New York Times, 14 December 2013, available at <https://nyti.ms/1eceVkA> (accessed 16 October 2019).

smaller countries, while processing a miniscule fraction of the transactions processed by centralised systems, such as the Visa payment network.[74]

Giving the government direct or indirect "superuser" access to the decentralised database removes the primary design goal and achievement of blockchain technology. This, however, means that any justification for the inefficient design of the system – which was necessary for, and thus potentially justified by, the aim of decentralisation – also vanishes. We are likely left with a costly, inefficient database, which is not in fact decentralised. In the best-case scenario, using blockchain technology allows us to create an alternative, equally efficient way of running a database, without however introducing functionality not already present in existing systems.

Better Alternatives to Government Back-doored Blockchains

Adopting the direct or indirect government backdoor solution described above means that the users of the system need to trust the state to not interfere unduly with the operation of the protocol. While history teaches us that no permanent assurance for this can ever exist, people generally accept this state of affairs in relation to the various record keeping systems already run by the state.

Importantly, however, once a blockchain is designed to be and stay legally compliant, i.e. synchronise its records with the state of affairs as seen by the law, we should now compare it with alternative available designs with the same features. Two competing designs are immediately obvious. First, the system could be replaced by a government-run database. There is no question that such a database can always be designed at a technical level to be at least as efficient as a blockchain solution. This is because a government-run system simply has no need for a consensus mechanism, but can instead run as a traditional database. Experience shows that, when governments do this, results tend to be highly efficient.[75] Given that, in our scenario, the government already is a trusted central authority for the blockchain in question, there are no obvious disadvantages resulting from a switch to a government-run registry. It is worth noting here that no amount of improvement in the efficiency of blockchain technology could completely remove the efficiency advantages of a centralised system; no blockchain-based system can be *more* efficient than an equivalent centralised database.

It may not always be possible to convince the (or a) government to create a registry for every class of assets or rights that one may want to put on a blockchain. Moreover, actors in the technology, finance, and legal industries may well have good reasons beyond distrust in the government for wanting to design and create their own systems, as indeed

---

[74] Recent estimates suggest that the total energy consumption of the Bitcoin network is comparable with that of Austria; see e.g. Bitcoin Energy Consumption Index, available at <https://digiconomist.net/bitcoin-energy-consumption> (accessed 16 October 2019)

[75] See for example the UK Land Registry, which runs an insured ledger of around £ 6 trillion worth of assets at a total cost of about 0.006%, with about half of this cost going to the Treasury as profit. Own calculations based on UK Land Registry annual financial statements (available at <https://www.gov.uk/government/publications/hm-land-registry-annual-report-and-accounts-2017-to-2018/financial-statements>, accessed 11 December 2018) and ONS estimates of land value in England and Wales (see ONS, *UK National Accounts, The Blue Book: 2018* [2018], available at <https://www.ons.gov.uk/economy/grossdomesticproductgdp/compendium/unitedkingdomnationalaccountsthebluebook/2018>, accessed 11 December 2018).

they have been doing for centuries. In this case, rather than creating a blockchain based protocol with the mentioned built-in mechanisms for synchronising it with the legal system, one could always just incorporate an SPV and task it with running the ledger. While it is, admittedly, true that this solution introduces a certain risk of the SPV's managers acting dishonestly, the managers themselves will of course be under the jurisdiction of the courts. This means that, as long as dishonest behaviour on the part of the record-keepers is easily and quickly identifiable,[76] any undesirable behaviour could be corrected – including where necessary by the courts.

As mentioned before, a truly decentralised database will necessarily introduce a certain level of inefficiency compared to a more conventional centralised database design. It is undoubtedly possible that future advances in database technology and cryptography, as well as further advances in the efficiency and cost of computing will render the inherent advantages of centralised database systems trivial. While the proof-of-work design of Bitcoin is extremely wasteful, some other, less inefficient, solutions exist[77] and could be further developed, resulting in blockchain or DLT-based databases to operate at virtually no additional cost compared to alternative centralised solutions. Even if that were the case, however, it would not justify particular enthusiasm, at least outside the database technology sector. As argued above, the way all modern legal systems operate necessarily removes the core advantage of decentralisation – put simply, under the rule of law, true non-hierarchical decentralisation is impossible because *ruling* always necessitates a hierarchy. Thus, a blockchain solution that performs (almost) exactly as well as a centralised system could in principle be widely adopted, but its defining feature – true decentralisation – could not be put to use.

It follows that reliably synchronising a blockchain with the legal system renders its use pointless. Distributed ledgers simply cannot be designed to be *more* efficient than centralised alternatives; no matter what system is proposed, reducing the number of network nodes to one will increase its efficiency, and even in principle it cannot *reduce* it. It has previously been shown that *failing* to achieve synchronisation renders all crypto assets, including stable coins and blockchain-based payment solutions, as well as smart contracts useless in practice. None of this means that using blockchain technology does not work, of course. The argument is, simply, that the design choices necessary to *make* it work mean that it offers no functionality in addition to what traditional databases have offered for decades. One should thus not expect any meaningful change to follow from the – conceivable – wide adoption of the technology.

Enterprise Blockchains and other Blockchains in Name Only

Another way to address the technical as well as legal problems posed by permissionless blockchains are so-called "enterprise blockchains", which are often discussed as a potentially promising way for leveraging DLT technology, with several large projects

[76] There are several ways to ensure that they objectively are, leveraging some of the same technology that is used in blockchains.

[77] These include Proof-of-Stake consensus protocols; see n 26 above.

currently in various stages of development and early implementation.[78] These are perhaps best described as a semi-centralised DLT-based systems. What such enterprise blockchain systems typically have in common is that they replace the inherently open architecture of permissionless blockchains, in which anyone can, in principle, participate in the consensus protocol,[79] with some form of *permissioned* access. For instance, a number of industry players could decide to set up a DLT system for, say, trading securities but design it in a way that limits participation in the consensus mechanism to a set of pre-approved trusted node operators. The system could then be made accessible to either only these trusted participants, or to the public.[80]

Such a design clearly addressed the technical drawbacks of a truly decentralised, permissionless blockchain system. A Bitcoin-inspired proof-of-work design is resource-intensive and inefficient, but permissioned DLT-based databases can avoid the associated costs. Since only trusted parties participate in establishing consensus, there is no inherent need for costly and wasteful-by-design mining as in proof-of-work systems. Similarly, the challenges posed by alternative consensus protocols[81] can also largely be avoided. Such permissioned systems can thus likely operate at no, or virtually no, additional cost compared to traditional databases.

Enterprise blockchains typically also solve the legal synchronisation problem discussed above. Since the state of the ledger is ultimately determined jointly by a group of actors who (a) trust each other, (b) presumably have an interest in maintaining the system they created or run in a useful state, and (c) will typically be subject to the jurisdiction of some court, transactions that violate mandatory legal rules, or that are declared void by a competent court, are likely to not be included in the ledger, or else can be reversed where necessary.

However, such systems are blockchains in name only. It is hardly surprising that the challenges posed by blockchain technology can be avoided by adopting a design which removes the very feature of blockchain technology which distinguishes it from other, existing and widely available systems, i.e. the reliable establishment of consensus between parties who do not necessarily know or trust each other. These systems can work efficiently; they do not however offer anything that had not been previously available to businesses who had an interest in such systems.

---

[78] See e.g. HM Land Registry, 'Could blockchain be the future of the property market?' [2019], available at <https://hmlandregistry.blog.gov.uk/2019/05/24/could-blockchain-be-the-future-of-the-property-market/> (last accessed 16 October 2019); Hyperledger, 'Case Study: How Walmart brought unprecedented transparency to the food supply chain with Hyperledger Fabric' [2018], available at: <https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf> (last accessed 16 October 2019); R3, *Case Study: How R3 is working with CryptoBLK, HSBC and other banks and corporates to revolutionize and revitalize trade finance letters of credit, using the power of the Corda blockchain platform* [2018], available at: <https://www.r3.com/wp-content/uploads/2019/04/CryptoBLK_CS_Jan2019.pdf> (last accessed 16 October 2019).

[79] Be that by "contributing" computational resources or for instance by acquiring the relevant crypto tokens that enable participation in the system's consensus protocol and/or governance.

[80] In the latter case, the public could access, view, and interact with the system, but updating the ledger would always require some or all of the pre-authorised, trusted parties to agree.

[81] These include Proof-of-Stake consensus protocols; see n 26 above.

Similarly to what was discussed above in relation to unpermissioned blockchains,[82] a group of mutually trusting parties could simply incorporate a joint subsidiary and task that company with administrating the database. Any such database can easily be designed so as to require the explicit agreement of a number of actors in order to update its internal state, should this be required. In fact, all features offered by an enterprise blockchain solution can easily be replicated by long-existing technology. It follows that even if enterprise blockchain systems are exactly as efficient as traditional databases, they would not offer anything new. Consequently, there does not seem to be a *rational* basis for expecting that enterprise blockchains will revolutionise the way our economy works.

IV. CHANGING THE LAW TO UNLEASH THE BLOCKCHAIN

A. The Lex Mercatoria as an Early Version of "Code is Law"

One possible and important objection to the simple argument presented above is that the law could potentially be changed so as to accommodate the operation of blockchain systems. Arguably, this is partly what happened in relation to negotiable instruments when the *lex mercatoria* (or law merchant) was adopted by legal systems across Europe.[83] On first glance, the current situation of blockchain solutions may appear strikingly similar to that faced by merchants in the 16th and 17th centuries in England, as well as in most other European jurisdictions. Merchants had in mediaeval times[84] developed a practice, which can loosely be described as starting to treat intrinsically worthless pieces of paper as valuable representations of proprietary and contractual rights. At least according to some of the accounts of the legal history that followed, courts and later legislators came to accept and ultimately endorse this practice.[85]

In doing so, the legal system could be regarded as adopting an early version of "code is law": to a certain extent, it accepted, notwithstanding its general and long-standing rules of contract and property law, that the rules merchants had internally agreed upon should be allowed to govern their interactions. This entailed giving legal effect to and enforcing some claims and transfers which would *not* have been considered valid under general law,

---

[82] See text to n 76 above.

[83] See Lobban, n 36 above; see also Eva Micheler, *Wertpapierrecht zwischen Schuld- und Sachenrecht, zu einer kapitalmarktrechtlichen Theorie des Wertpapierrechts* (Vienna, Springer 2004); Matthias Lehmann, *Finanzinstrumente: Vom Wertpapier- und Sachenrecht zum Recht der unkörperlichen Vermögensgegenstände* (Mohr Siebeck Tübingen 2009) 17; Holden, *History of Negotiable Instruments in English Law;* McLoughlin, *Negotiable Instruments*. See also James S Rogers, *The Early History of the Law of Bills and Notes* (Cambridge: Cambridge University Press CUP 1995), arguing that this account overstates the importance of negotiability in the development in England. See also Gilles Cuniberti, "Three Theories of Lex Mercatoria" (2014) 52 *Columbia Journal of Transnational Law* 369.

[84] The practice was already widespread in parts of Europe since at least the 14th century. See e.g. Edward Jenks, "On the Early History of Negotiable Instruments" (1893) 9 *Law Quarterly Review* 70. See also A. H. Pruessner, "The Earliest Traces of Negotiable Instruments." (1928) 44 *American Journal of Semitic Languages and Literatures* 88, arguing that the principle idea behind the creation of negotiable instruments was already known and used as early as 2000 B.C. in Babylonia.

[85] See Holden, n 83 above; Jenks, ibid; McLoughlin, n 83 above. See also the account by Rogers, n 83 above.

based solely on compliance with the merchants' rules. Could not legal history repeat itself and create what some enthusiasts term '*lex cryptographica*'?[86]

To explore this prospect, it is important to briefly highlight both the main reason for the legal system's incorporation and adoption of the law merchant in relation to negotiable instruments, as well as the extent to which it required a significant departure from then-existing legal principles.

First, early merchants lacked reliable long-distance communication, and the risks associated with transporting large amounts of physical gold money across vast distances were considerable. In this context, the development of bills of exchange and other negotiable instruments was an extremely efficient and sophisticated way to solve a problem for which no easy alternative solutions were available. Negotiable instruments enabled a type of international commerce the conduct of which would otherwise not have been possible, and this clearly was in the interest of the state and hence the legal system.[87]

Second, the acceptance and endorsement by the legal system of the law merchant was never absolute. The various legal rules adopted across Europe have always maintained a significant backstop, i.e. there have always been types of transactions where, for instance, the possession of a negotiable instrument would *not* be equated by the legal system as giving its holder the rights associated with it.[88] For instance, where the signature on a bill[89] or cheque had been forged, this rendered the instrument void, as is still the case. Similarly, if the person signing a bill has no authority to do so, no right is created for the holder, unless the act is later ratified. It should be clear from these examples that even in the case of negotiable instruments, the law – although coming fairly close to it in normal circumstances – has never fully accepted a "code is law" approach in which mere possession of a bill automatically and without exception creates rights for its holder. This is further evidenced by the large body of jurisprudence regarding bills of exchange, cheques, and notes.

B. Why the Law Will not Endorse Crypto Assets

It is submitted that neither of the two factors which facilitated the legal endorsement of the law merchant – i.e. its unrivalled usefulness given the technology at the time and the possibility for the legal system to only *partly* endorse the system – is present in relation to crypto assets, and that it is thus unlikely that the law will endorse them in the same way it endorsed negotiable instruments.[90]

---

[86] De Filippi and Wright, n 9 above, 72-80.

[87] See Jenks, n 85 above, writing in 1893 *"Bills of Exchange, with their kindred documents, have rendered international commerce possible."* See also Pruessner, n 84 above, writing about the principles underlying negotiable instruments: *'After this principle was once discovered, its advantages and benefits were found to be so manifold that nothing could stay its victorious advance.'*

[88] This is, admittedly, a somewhat imprecise way of putting it. It is perhaps more accurate to say that the law merchant *itself* did not see these transactions as creating valid obligations.

[89] See e.g. s24 Bills of Exchange Act 1882; see also Geneva Convention Providing a Uniform Law for Bills of Exchange and Promissory Notes [1930].

[90] But see the discussion in Paech (n 23 above) at 1099-1100.

It may be somewhat surprising to an observer of the blockchain space that the advantages of blockchain technology are so casually dismissed, given that it seems to have been proposed a solution to virtually every human problem.[91]

It is submitted, after a broad, if admittedly incomplete and unsystematic analysis of proposed blockchain use cases and advantages,[92] that virtually all claims of real-world applications of this technology are based on a misunderstanding of (i) the reasons for the status quo and (ii) the right comparator when benchmarking a proposed solution to a perceived problem.

In relation to the first point, the majority of blockchain application proposals suffer from the same flawed analysis of the status quo, something which could be called the "junior business consultant fallacy". By that I mean that rather than understanding the path dependence of the way in which solutions to particular problems have evolved over time, and rather than appreciating and estimating the often enormous switching costs involved in changing legacy systems, the starting point is often the true, but uninspired finding that systems that have evolved over several centuries tend to be less efficiently designed than what a moderately talented designer could achieve if given the opportunity to start from scratch today. By adopting this approach one will, of course, find problems waiting to be solved behind every corner.

Second, and perhaps more importantly, even in cases where the current system of doing things – be it transferring money, sending bills of lading, or anything else – is indeed so inefficient that it should be changed, any proposed solution should self-evidently be benchmarked against all other solutions that *also* require a wholesale change of the status quo. There is, for instance, little doubt that the global payment infrastructure and technology is inefficient and less resilient than one would want. Given its evolution and history, this is hardly surprising. Proposing an alternative system that performs better than the *current system* if adopted by everyone is of course a trivial task – almost any system would meet this requirement. Candidate systems should instead be compared to each other, rather than to the status quo. This point should be entirely obvious; it would hardly be worth making if not for the fact that, it is submitted, observing it would rule out blockchains as good solutions for all, or at the very least virtually all, problems humans face.

Finally, the incomplete endorsement that the early merchants' negotiable instruments received, i.e. one that still contains carve-outs for forged signatures, lack of authority, and the like, would not suffice to render cryptoassets viable. Since there is no way for the protocol to distinguish between minor and grave violations of the underlying legal principles, only a full "code is law"-like change of our private law system could create a reliable basis for meaningful blockchain systems.

The Empty Promise of Smart Contracts

---

[91] Some examples are referred to in section II.D above. See also Cohney et al., n 56 above.

[92] For a recent systematic analysis of blockchain-based projects that involved raising funds from the "investing" public, see Cohney et al., n 56 above.

It has already been argued above that, first, it is hard to see how the adoption of smart contracts would bring about significant efficiency gains, and second, that even if it did, such advantage would not depend on adopting *blockchain*-based smart contracts.

Proponents of a blockchain future often seem to assume that the limitations of natural legal language and its inherent ambiguity are a problem in need of a solution, and that smart contracts may offer it. From this perspective, the most obvious potential advantages of smart contracts would then be to equip lawyers (or, perhaps ultimately, the parties themselves) with a "better language" in which to express contractual promises, to enable computers to read and "execute" these contracts without human interaction, and to do so in a decentralised and "trustless" way.

Natural language vs. Computer Code

To lawyers, the first advantage may sound somewhat peculiar, as it refers to a problem few, if any, lawyers have ever experienced. To the extent that lawyers struggle to express promises in precise terms, this will rarely be the consequence of inherent limitations of the language they use. Even where it is, legal practitioners have long made use of more formal languages (or "code"), where mathematical precision is required or useful. There are many circumstances in which lawyers (or their clients) already decide that a particular promise within a contract can best be expressed in unambiguous mathematical form. Bond documentation, for example, frequently expresses the amounts of certain future payments in the form of a mathematical equation, because doing so is more efficient and more precise than describing the same promise in natural legal language. Nothing *in the law* prevents parties from agreeing to have their relationship governed more extensively by promises written in mathematical language or computer code.

The reason why entire contracts are not usually written in a more formal and precise language is exactly *because* it is impracticable for any (non-trivial) contract to specify all possible contingencies.[93] This problem is not the consequence of linguistic imprecision, but rather follows from the complexity of the world surrounding us, our inability to predict future events with certainty, and the costs associated with processing and communicating information.

The open-ended, context-sensitive, and ambiguous nature of legal language, then, is a technique used to alleviate the need to draft fully contingent agreements.[94] Much more rigid than casual language, legal drafting language has developed, and continues to develop, to exactly inhabit the useful middle ground between the unnecessarily vague and the unhelpfully rigid and inflexible, presumably with the aim of minimising transaction costs. It would therefore be wrong to expect efficiency gains to derive from smart contracts replacing the precise and rigid language of code for the more traditional legal language.

---

[93] See e.g. Oliver Hart and John Moore, "Incomplete contracts and renegotiation" (1988) 56 *Econometrica* 755.

[94] See also Jeremy M. Sklaroff, "Smart Contracts and the Cost of Inflexibility" (2017) 166 University of Pennsylvania Law Review 263.

Calls for a dramatic change in legal education to prepare us for a smart contract and blockchain future[95] thus look somewhat premature.

Part-automation of Contracts

It is also important to emphasise that the ability to agree to contractual terms expressed entirely in algorithmic form – whether that be computer code or an Excel spreadsheet – does not depend on smart contracts running on a blockchain network. Unsurprisingly, however, and arguably in line with the aforementioned advantages of using traditional legal language, very few, if any, contracts attempt to express the entire agreement in the language of computer code.

It may be worth noting in this context that, while entire agreements will rarely ever be expressible (at least expressible *efficiently*) in computer language, many contracts can be said to create a framework for very simple and repeated interactions between the parties, which in essence constitute the execution of that contract.

A commuter in London, for instance, may have a contractual relationship, expressed in natural language, with Transport for London (TfL), the main public transport operator. The central part of this relationship involves TfL giving access to the public transport system to the commuter, in exchange for payment. Over the past decades, several technical solutions have been developed which allowed TfL to essentially encode this central part of its contractual relationship with its customers into machine instructions. A system for reliably storing electronic credits on an access card has long been available, thus enabling the automation of the "payment" process. More recently, technical solutions have become widely available which perform much the same function without the need to first deposit such electronic credits with TfL, thereby allowing the interlinking of a system directly with the wider payments architecture. It has also long been technically possible to link such a payment system with gates that physically control access to people. The, by far, most frequent execution of the agreement between TfL and a customer –access against payment – can, and has long been, therefore be encoded in a machine-readable form.

The technical feasibility of this part-automation of the contract will hardly surprise the reader, and similar systems exist around the world and across industries; every cash machine, airport luggage locker, payphone, etc. follows this logic. Why, then, should we not expect that we will soon reach the point at which encoding entire agreements, rather than just execution frameworks for sub-parts of it, will become both possible and popular? The reason to be sceptical is that technical solutions tend to show quickly diminishing returns in terms of the real-world problems they solve. First, the mere fact that moving from partial to full automation necessarily means designing technological solutions for less and less frequently occurring scenarios; even if the costs of such solutions were constant, this would already imply diminishing returns to automation. Second, while it is often trivial (and very useful) to automate formal, repetitive, and easy parts of interactions, the less predictable and formalised parts of an agreement would typically require

---

[95] See e.g. Mark Fenwick, Wulf A Kaal, Erik PM Vermeulen, "Legal Education in the Blockchain Revolution" (2017) *University of St. Thomas (Minnesota) Legal Studies Research Paper* No. 17-05, available at <https://ssrn.com/abstract=2939127> (accessed 14 October 2019).

disproportionately *more* complex technical solutions to render them reliably self-executing. As Minsky remarked, what we 'vaguely call common sense is actually more intricate than most of the technical expertise we admire'.[96] For instance, an automated system that reliably reimburses commuters who, say, exit a station due to a cancelled train – which, ideally, happens far less frequently than the normal "pay for access" scenario – is likely to be far more complex and difficult to design than the system dealing with the standard scenario.[97]

One does not need to reject the idea that all contracts can, *in principle*, be reduced to a complex collection of contingent if -then statements in order to doubt that *expressing* contracts in this way is, and will remain, infeasible.[98] One can accept that, on the deepest level, disciplines like child psychology or even poetry reduce to quantum physics *in principle*, but regard the language and tools of quantum physics as entirely useless for the purposes of these subjects. It is primarily the complexity and richness of the world surrounding us that makes us use more manageable higher-level abstractions and simplifications to describe and solve the problems we face. The exact level of abstraction depends on the complexity of the task at hand, and will be lower for, say, calculating a satellite's orbit, and much higher for most areas of human biology; every discipline will seek, and generally arrive at, its own "sweet-spot", trading-off precision and practicality. The world of legal relationships is no different, and imprecision in legal language in large parts represents the level of abstraction which lawyers and others regard, benefitting from centuries of experimentation, as most useful in the legal domain.

For increasingly complex tasks, it thus seems unlikely that the benefits of removing manual overrides and other non-automated parts of a system dealing with rare and exceptional occurrences becomes technically feasible and economically viable, unless we see dramatic changes in the available technology. In fact, it seems likely that full automation of most real-life contractual relationships would depend on the development of systems with human-like general intelligence. However, if and when reliable, artificially intelligent systems become available, this is likely to trigger fundamental changes to the economy, and there is little reason to believe that blockchain-based solutions to current problems will remain relevant in this scenario.

Decentralisation and self-execution

In addition to the inherent disadvantage of using the hyper-precise and rigid language of computer code, another reason may explain the unpopularity of this option, and it is a reason that will in my view continue to haunt any smart contract implementation.

Let us assume that, exceptionally, two parties want to enter into a contract where the *promise itself* can efficiently be expressed in the language of code. The contract would almost certainly have to be of the most primitive nature, as argued above, but the situation

---

[96] Marvin Minsky, *The Society of Mind* (Simon & Schuster 1988) 72.

[97] This is also true in other areas of technological development; see e.g. self-driving cars.

[98] See on a similar point Noam Chomsky, "Language and Nature" (1995) 104 *Mind* 1, 10; Noam Chomsky, Lawrence Krauss, and Sean Carroll, 'Science in the Dock' [2006] Science And Technology News, 1 March 2006, available at https://chomsky.info/20060301/ (last accessed 4 November 2019). 14B See also e.g. Paul Krugman, "White Collars Turn Blue" [1996] The New York Times, 29 September 1996, Section 6, Page 106.

may still arise. Of course, the whole point of having smart contracts is that they are dynamic, rather than static, i.e. that they react to inputs, as any non-trivial computer program does. But what are these inputs? The only input that objectively exists in both the real world and within the protocol is the passage of time.[99] All other inputs, or circumstances, that may give rise to a change in the mutual obligations under a contract must ultimately be *mediated into* the computer protocol by interactions with the real world.

Where this is not the case, even indirectly, the participants are best described as playing a video game. Where this process *does* occur, the rigidity, objectivity, and precision achieved by the smart contract implementation is a mirage, since subjective judgements and decisions indirectly enter the contract by virtue of the smart contract's reliance on external inputs, interpreted and mediated into the protocol by a third party who the parties must trust. Trustless and algorithmic contracting is thus only truly possible in cases where the only input is the passage of time, and, importantly, where execution of the contract can also be achieved purely within the protocol – that is, where a naked blockchain asset is to be transferred between parties at a future predetermined time. This describes a class of agreements unlikely to be widely used in the foreseeable future.

V. SOLUTIONS THAT DO NOT INOLVE A CHANGE OF THE CURRENT LEGAL SYSTEM

It is, finally, worth briefly addressing whether alternative solutions or workarounds exist that could address the problems discussed above, but which do not require a change of the current legal system, i.e. an explicit endorsement of blockchain solutions by the legislator.

A. THE USE OF "ORACLES"

It has been suggested[100] that, in order to ensure compliance with the law, so-called "oracles" could be used to signal the information contained in court judgements to the blockchain protocol, which could then use it in the same way it may be able to use any other input. The flaw in this solution is that it really does not address the actual problem described above. Oracles may or may not be useful in transporting information about a court decision into the realm of the blockchain protocol. They do not, however, change

---

[99] Even the passage of time cannot necessarily be determined objectively by the protocol, but in most circumstances it approximately will be.

[100] Both in relation to crypto assets and in relation to naked blockchains; see De Filippi and Wright, n 9 above, 50; Kevin Werbach, "Trust, But Verify: Why the Blockchain Needs the Law" (2018) 33 *Berkeley Technology Law Journal* 489, 547-548; ; Werbach and Cornell, n 45 above, 336; Dominick Battistini, "Using Blockchain Technology to Facilitate Anti-Money Laundering Efforts" (2016) *Economic Crime Forensics Capstones* 15; see also Vitalik Buterin, *Decentralized Court* (2016), available at <https://www.reddit.com/r/ethereum/comments/4gigyd/decentralized_court/> (accessed 22 May 2020).

the fact that either the oracles simply convey the information contained in court decisions reliably and automatically, in which case the situation is indistinguishable from having a government backdoor, which it was shown renders using a blockchain suboptimal; or, alternatively, oracles decide themselves which judgements to mediate into the blockchain, in which case they become a central authority themselves, in addition to introducing the drawbacks discussed in section III.B above.

The same is true for blockchain governance structures.[101] These will have to either reliably implement the decisions of the competent courts of law, in which case they do not add decentralisation and thus cannot justify using a blockchain system in the first place, or they will do so with less than perfect reliability, in which case the blockchain system will be unable to create the legal effects it is designed to effect.

B. A Crypto-Friendly Anchor Jurisdiction

Another approach would be to rely on choice-of-law clauses. As long as *some* jurisdictions adopt "crypto-friendly" laws,[102] one may argue, parties could always include choice-of-law clauses in the relevant contracts to ensure their transactions are subject to the law of a jurisdiction that will tend to give effect to whatever happens on the blockchain. This proposed solution overlooks the fact that choice of law rules are subject to explicit and implicit *ordre public* limitations. Since a "code is law" approach will at least occasionally require that a crypto-friendly legal system gives effect to transfers even where they were initiated under duress or as the result of fraud, choice of law rules are unlikely to offer a permanent solution to the problem identified above.

C. Other Proposed Solutions

It has also been proposed[103] to solve the conflict between the law and the blockchain representation of assets by having parties agree to a blockchain-based arbitration procedure. Apart from the technical legal problems of this approach, it is hard to see why parties should feel more comfortable about being subject to what is in essence central authority by the adjudicators, than they would about publicly accountable judges. Even if

---

[101] See e.g. Paech (n 23 above).

[102] Suggestions typically include Malta, Cyprus, and Switzerland. See also the recently adopted Liechtensteiner 'Blockchain Act' (Token- und VT-Dienstleister-Gesetz, adopted on 3 October ; TVTG). The approach of Liechtenstein provides a good example of the problems discussed here, as it explicitly requires any invalid transfer that happened on the blockchain to be reversed in accordance with general private law rules; see Art 6 (3) TVTG.

[103] See e.g. the Mattereum, "Smart Contracts. Real Property.", working paper available at <https://www.mattereum.com/upload/iblock/af8/mattereum_workingpaper.pdf> (accessed 11 December 2018); see also OpenLaw, "OpenCourt: Legally Enforceable Blockchain-Based Arbitration" available at <https://media.consensys.net/opencourt-legally-enforceable-blockchain-based-arbitration-3d7147dbb56f> (accessed 31 May 2019). See also Jake Goldenfein and Andrea Leiter, "Legal Engineering on the Blockchain: 'Smart Contracts' as Legal Conduct" (2018) 29 *Law and Critique* 141.

they were, the solution again introduces privileged[104] participants into the protocol; as argued above, it would be preferable in this case to simply have the blockchain adjudicators centrally run the network to start with, which would avoid the computational costs of running the consensus algorithm and dramatically simplify the network, without altering the level of centralisation.

Other governance-based solutions,[105] which attempt to address the inability of any algorithmic protocol to capture the complexity of real-world human interactions by introducing a collective decision-making mechanism that can override the normal operation of the protocol, face a similar problem. Irrespective of the exact governance mechanism used (e.g. voting by network participants), using the legal synchronisation problem described above, any such solution can be placed on a spectrum. On one end of the spectrum, a governance mechanism would operate in complete obeyance of the law, implementing court decisions, reversing transfers, and the like; on the other, it would reach its own entirely autonomous decisions, having no regard to legal rules that are not part of the protocol. The latter design, quite obviously, does not solve the problem at all. The former design is merely a more complicated implementation of the "government back-door" discussed above, as *ex hypothesis* it would always produce the same result, and implement the decisions of, the competent courts. Any governance solution occupying a point in between these two extremes would face both these limitations (and thus a trade-off between uselessness and pointlessness).

Finally, artificial intelligence is often mentioned as a potential solution for virtually all problems encountered by blockchains. Of course, an artificially intelligent system that is capable of replacing the legal system does not seem to be an immediate prospect; and when it is, one would hope that making such a system the world's judge will not be the humans' first move.

VI. CONCLUSIONS

This paper has made an attempt to demonstrate that the current hype surrounding blockchain technology is largely unjustified, at least as far as crypto assets and smart contracts are concerned. Whereas the law arguably does not have much to say about purely digital assets, as soon as they try to interface with what lawyers would recognise as the real world, crypto assets and smart contracts face a difficult choice: They must either accepting the legal system as the ultimate arbiter of legal rights, or risk falling into oblivion. I have tried to show that either option renders the use of blockchain technology largely pointless, and that its adoption does not offer any advantages over well-known, existing, and widely used technology. This is not to say, of course, that blockchain technology will not be adopted; it may well be. However, the technology itself is unlikely to change the way our economy works.

---

[104] In the sense of having some authority not possessed by other participants.
[105] For a discussion in the context of financial transactions, see e.g. Paech (n 23 above).

I have also attempted to show that, typically, the promised advantages of blockchain technology do not, in fact, stem from the technology itself, but rather from the implicit prerequisite for its adoption: the large-scale and coordinated redesign of existing market and IT infrastructure, and the ensuing improvements in inter-operability. One potential positive effect of blockchain technology could be that the (in my view unwarranted) excitement surrounding it will encourage businesses to rebuild and update legacy systems sooner, and in a more coordinated way. There is little doubt that doing so could prove beneficial for the economy.