PAUSE THE BLOCKCHAIN LEGAL REVOLUTION

Kelvin F.K. LOW* and Eliza MIK**

When bitcoin was released by the mysterious Satoshi Nakamoto in 2008, few could have predicted that it would attract as much attention as it has today. It has spawned a veritable host of other cryptocurrencies, including ether on the upstart Ethereum network, which boasts smart contract functionality. The underlying blockchain technology has also attracted attention, with some within the blockchain community suggesting that it can solve such diverse problems as secured digital voting to tracking food provenance. In the legal context, blockchains have been envisaged as capable of revolutionizing registries for assets ranging from land to intellectual property, modernising clearing and settlement, and even fundamentally transforming the contracting process. This paper critically evaluates the popular claims surrounding the potential of blockchain technologies to disrupt the legal system by separating hype from fact.

I. INTRODUCTION

In 2008, the world was introduced to the concept of a blockchain when Satoshi Nakamoto[1] published his white paper on bitcoin.[2] Born of the Great Recession,[3] bitcoin and its countless progeny of altcoins[4] would capture the public's imagination through the inflation of "the mother and father of all bubbles".[5] An early crash[6] in the price of this volatile[7] asset thrust the blockchain into the spotlight, prompting many to consider whether the blockchain might prove more important than bitcoin itself.[8] Interest in blockchains was drawn initially from finance and technology.[9] Hailed as a "trust machine" that "could transform how the economy works",[10] blockchains were "the future of everything".[11]

* Professor, School of Law, City University of Hong Kong
** Honorary Fellow, Melbourne Law School; Research Associate, Tilburg Institute of Law and Technology; External Research Fellow, Applied Research Centre for Intellectual Assets and the Law in Asia, School of Law, Singapore Management University
The authors wish to acknowledge the invaluable assistance of their technical colleagues Ernie Teo, Pralhad Deshpande, Anthony Lewis, Mano Thalaban, Gaurang Torvekar, Vinay Mohan, Darren Frankel, and Marco Crepaldi, without which this article could not be written.
[1] The true identity of Satoshi Nakamoto has been much speculated but remains unknown. See A. O'Hagan, "The Satoshi Affair", *London Review of Books* (30 June 2016).
[2] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (October 2008) at https://bitcoin.org/bitcoin.pdf (accessed 1 November 2018).
[3] Cf. D.B. Grusky, B. Western, and C. Wimer (eds), *The Great Recession* (New York: Russell Sage Foundation, 2011).
[4] i.e. alternatives to bitcoin.
[5] N. Roubini Testimony to the US Senate Committee on Banking, Housing, and Urban Affairs on "Exploring the Cryptocurrency and Blockchain Ecosystem" (11 October 2018).
[6] R. McMillan, "The Inside Story of Mt Gox, Bitcoin's $460 Million Disaster", *Wired* (3 March 2014).
[7] For the massive crash in 2018, see P. Vigna, "Bearish on Bitcoin: Crypto Markets Take Steep Dive", *The Wall Street Journal* (20 November 2018).
[8] "Bitcoin's Future: Hidden Flipside", *The Economist* (13 March 2014).
[9] C. Metz, "Tech and Banking Giants Ditch Bitcoin for Their Own Blockchain", *Wired* (17 December 2015). The convergence of the two fields is often dubbed "fintech" for short.
[10] "The Promise of the Blockchain: The Trust Machine", *The Economist* (31 October 2015).
[11] M. J. Casey and P. Vigna, *The Truth Machine: The Blockchain and the Future of Everything* (New York: St Martin's Press, 2018).

Three reasons are normally cited for the blockchain's revolutionary capacity. First, the "blockchain could radically alter the existing distribution of social and economic power"[12] through the disintermediation of powerful intermediaries such as banks. Secondly, for advanced industrialised economies, it could enhance operational efficiencies in commerce and beyond.[13] Thirdly, owing to the trustless trust[14] they supposedly instil, blockchains "may deliver the most significant transformational change" to developing economies absent trustworthy legal institutions.[15] Regrettably, much of the excitement over the blockchain's transformative legal prowess stems from a mutual misunderstanding. Many lawyers do not understand the core technical terms in the blockchain narrative and incorrectly assume that they map directly onto similar legal terms.[16] Concurrently, many technologists make false assumptions about how legal rules work and thus imagine legal systems ripe for disruption. As the saying goes, "a little knowledge is a dangerous thing".[17] This paper seeks to unravel the confusion on both sides of the divide by clarifying the "Technicalities" in order to disclose pitfalls in the application of blockchain in relation to "Rights & Records" and "Smart" "Contracts".

II. TECHNICALITIES

A. Definitional Conundrums

There is no single accepted definition of a blockchain and no agreement as to which attributes are indispensable for something to be a blockchain.[18] Blockchain is often defined as "[a]n open-source technology that supports trusted, immutable records of transactions stored in publicly accessible, decentralised, distributed, automated ledgers",[19] but this definition is underinclusive. Many blockchains are not open-source, publicly accessible, or decentralised. In principle, blockchains are a species of distributed databases that are maintained by a network of geographically dispersed computers, or "nodes." This means that there is no central authority in charge of the ledger and its management is instead dispersed among the nodes. In theory, this means that there is no single point of failure and no ability on the part of a single keeper of the ledger to falsify it, but it does necessarily create the challenge of ensuring that all these multiple ledgers conform to one another. As its name suggests, the ledger is made up of a chain of interconnected blocks, each block containing a list of aggregated transactions. The blocks are connected by means of cryptographic hashes,[20] so that alterations in an earlier block are

[12] K. Yeung, "Regulation by Blockchain: the Emerging Battle for Supremacy between the Code *of* Law and Code *as* Law" (2019) 82 M.L.R. 207 at 208.
[13] Above n. 11 at 208.
[14] Below text accompanying n. 24-38.
[15] Above n. 11 at 208.
[16] See, e.g., P. Paech, "The Governance of Blockchain Financial Networks" (2017) 80 M.L.R 1073.
[17] Cf. A. Pope, *An Essay on Criticism* (1709): "A little learning is a dangerous thing". The naïveté about economics among many crypto-enthusiasts have led some to christen bitcoins as "Dunning-Kruggerands": D. Gerard, *Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum and Smart Contracts* (London, Createspace, 2017) at 42. The Dunning-Kruger effect is the name given to the cognitive bias in which incompetence leads to inflated self-assessments, after the authors of the seminal paper: J. Kruger and D. Dunning, "Unskilled and Unaware of It: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments" (1999) 77 J. Pers. Soc. Pyschol. 1121.
[18] See generally: A. Walch, "The Path of the Blockchain Lexicon (and the Law)" (2016) 36 Rev. Banking & Fin. L. 713.
[19] InterPARES Trust Terminology Project: Key Blockchain Terms and Definitions (2018) https://interparestrust.org/terminology/term/blockchain
[20] A hash algorithm takes an arbitrary-length data input and produces a fixed-length deterministic result. For any specific input, the resulting hash will always be the same and can be easily calculated and verified by anyone

readily detected by checking the hash included in the block immediately following. Beyond this basic commonality, blockchains may be equipped with varying configurations of technical features.[21] Sometimes, it is more appropriate to speak of distributed ledgers,[22] as some distributed ledgers do not record data in interconnected blocks.[23]

B. Permissioned and Permissionless: A Key Distinction

We must first begin by distinguishing between permissioned and permissionless blockchains.[24] The main distinguishing criterion between them is whether the nodes processing transactions are pre-defined or unrestricted, i.e. whether anyone can operate a node or whether doing so requires permission. A "node" is a computer running the relevant software that enables the participation in a given blockchain network;[25] "processing" denotes the ability to view, create, validate, and/or add transactions to the blockchain. Permissionless blockchains, such as bitcoin or Ethereum, are constrained by ideological underpinnings. Their focus is on decentralisation and disintermediation, irrespective of whether such features are commercially necessary, simply because many enthusiasts believe that they are self-evidently desirable. In contrast, permissioned blockchains are more malleable and respond to actual, commercial needs. Free of ideological constraints, permissioned blockchains display a wider range of variations.

Permissionless blockchains are open and anonymous. They allow anyone to join the network without disclosing their identity and agreeing to any system rules or terms of use. It is only necessary to run the requisite software. The only rules that the participants must follow are those encoded in the algorithm. In principle, all participating nodes are equal and enjoy the same rights to access, use and edit the given blockchain.[26] Permissionless blockchains typically involve a native crypto-asset, such as bitcoin or ether, which serves as an economic incentive to produce blocks and hence maintain the integrity of the entire system.[27] They also rely on a consensus algorithm that leverages game theory[28] to compel strangers to cooperate in the

---

implementing the same hash algorithm. It is computationally infeasible to find two different inputs that produce the same fingerprint (a collision) or to select an input in such a way as to produce a desired fingerprint, other than trying random inputs. See: A. M. Antonopoulos, *Mastering Bitcoin*, 2nd ed (Sevastopol: O'Reilly, 2017), at p. 228

[21] Some blockchains have been designed for specific purposes or industries, others are generic in nature. For example, the permissioned ledger Ripple was developed to support the banking and finance industry, whereas Hyperledger Fabric supports the collaborative development of blockchain-based distributed ledgers for a wider range of industries and transaction types.

[22] Distributed ledgers are a broader category of dispersed, synchronised and cryptographically secured databases: R. Maull et al., "Distributed ledger technology: Applications and Implications" (2017) 26 Strategic Change 481, at p. 483.

[23] Insofar as they do not do so, they are not immutable to the same extent that blockchains are, see text accompanying nn. 56-69. Corda, a distributed ledger, developed by the R3 consortium, famously "abandoned" the concept of blocks; see generally: R. Gendal Brown, J. Carlyle, I. Grigg, M. Hearn, *Corda: An Introduction* (2016), available at docs.corda.net/_static/corda-introductory-whitepaper.pdf (accessed 6 December 2018).

[24] There are blockchains that do not fall into either categorization as they constitute a hybrid model. Sometimes, the term "permissioned" is used interchangeably with "private" and the term "permissionless" with "public" but these terms are not used consistently. See also R. Lai, D. K. C. Lee, *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2* (London: Academic Press, 2018) at p. 147.

[25] Above, n. 20, at p. 50. End users do not need to, and many do not, operate full nodes: see https://bitcoin.org/en/full-node (accessed 6 December 2018).

[26] X. Xu et al., "A Taxonomy of Blockchain-Based Systems for Architecture Design" *2017 IEEE International Conference on Software Architecture (ICSA)*, Gothenburg 2017, pp. 243-252.

[27] Miners are incentivized to add new blocks by obtaining bitcoins (when *their* block is added to the blockchain) and transaction fees (when they include a transaction in their block), indirectly, this incentive mechanism ensures the integrity and immutability of the blockchain. See above, n. 20, at p. 26.

[28] Game theory is "the study of mathematical models of conflict and cooperation between intelligent rational decision-makers.": R.B. Myerson, *Game Theory: Analysis of Conflict* (Cambridge: Harvard University Press,

absence of trust. This is necessary to ensure that all copies of the ledger conform to one another. A distributed network with non-conforming ledgers is worse than useless – confusing rather than authoritative. Today, most permissionless blockchains are based on the so-called "proof-of-work" [29] algorithm. "Proof-of-work" requires some nodes to solve a mathematical puzzle that is computationally difficult but which solution is easily verified before a new block can be added to the blockchain. This process has been christened "mining," and nodes that perform this function "miners," drawing an explicit, if inapt, metaphorical connection to gold mining.[30] As the process is extremely expensive in terms of computer equipment[31] and electricity,[32] it is more economical to produce valid blocks (i.e. follow the rules) than to attempt to change previous blocks (i.e. break the rules). Given the cost of retrospectively changing existing blocks, the possibility of altering or reversing a transaction that has been included in a block is supposedly infinitesimal.[33]

The technical attributes described above guarantee the supposed "trustlessness" of the entire system, which differs from traditional ledgers where the trustworthiness of the keeper of the ledger is indispensable. The reasoning is that one can trust the code alone, without having to trust any of the nodes running the network.[34] Trust in the code supposedly engenders trust in non-trusted counterparties or what enthusiasts call "trustless trust". Reliance on human institutions, such as banks or courts, is replaced with reliance on technology. It can be difficult for agnostics to understand how the "trustless" character of blockchains eliminates the need to trust humans since it obviously overlooks the fact that there is no immaculate conception of blockchain code.[35] It must have been coded by a human or, more likely, a group of humans. Although the process of appending individual blocks is decentralised, the process of coding the blockchain is highly centralised. For example, data from May 2015 reveals that seven individuals alone were responsible for 68% of the code for the bitcoin blockchain, earning them the epithet of "core developers".[36] Many altcoin blockchains are coded by rank amateurs, and

---

1991) at p. 1. Pioneered by John von Neumann (J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior* (Princeton: Princeton University Press, 1944) and popularised by Ron Howard (Dir.), *A Beautiful Mind* (Imagine Entertainment et al., 2001), a biographical film about John Nash, a Nobel laureate who developed the Nash equilibrium, there are well-known limitations to the sort of traditional game theory that many blockchain algorithms are built upon: see, e.g., A. M. Colman, "Cooperation, Psychological Game Theory, and Limitations of Rationality in Social Interaction" (2003) 26 B.B.S. 139.

[29] See generally: V. Buterin, "On Public and Private Blockchains", Blog Post (6 August 2015) at https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ (accessed 6 December 2018).

[30] D. Andolfatto (31 March 2014), "Bitcoin and Beyond: The Possibilities and Pitfalls of Virtual Currencies", *Dialogue with the Fed*, at pp. 16-17.

[31] K.F.K. Low and E.G.S. Teo, "Bitcoins and Other Cryptocurrencies as Property?" (2017) 9 L.I.T. 235, at p. 238.

[32] A. de Vries, "Bitcoin's Growing Energy Problem" (2018) 2 *Joule* 801. For the latest information on Bitcoin energy consumption, see https://digiconomist.net/bitcoin-energy-consumption (accessed 1 March 2019). For information on Ethereum energy consumption, see https://digiconomist.net/ethereum-energy-consumption (accessed 1 March 2019). This high monitoring cost is unsurprising since "proof-of-work" is designed assuming the absence of trust: cf. H.J. Chang, *23 Things They Don't Tell You About Capitalism* (London: Allen Lane, 2010), at pp. 41-50. If Chang's hypothesis that "[a]ssume the worst about people and you get the worst" is correct, that may also explain the widespread prevalence of fraud and scams within the crypto-community: see, e.g., S. Shifflett and C. Jones, "A Flood of Questionable Cryptocurrency Offerings", *The Wall Street Journal* (26 December 2018, updated 9 January 2019).

[33] Above, n. 20, at p. 162. But see text accompanying nn. 57-69.

[34] K. Werbach and N. Cornell, "Contracts Ex Machina" (2017) 67 Duke L. J. 313, at p. 333.

[35] The religious metaphor is frequently invoked to describe faith in the blockchain and bitcoin even has its own Bitcoin Jesus, one Roger Ver. See N. Paumgarten, "The Prophets of Cryptocurrency Survey the Bust and Boom", *The New Yorker* (22 October 2018); J. Kelly, "The Unholiest of Holy Wars: 'Satoshi' vs 'Bitcoin Jesus'", *FT Alphaville* (10 November 2018).

[36] See, e.g., in relation to the bitcoin blockchain, G. Vidan and V. Lehdonvirta, "Mine the gap: Bitcoin and the maintenance of trustlessness" (2018) New Media & Soc. 42, especially pp. 49-51.

even the core developers of more established blockchains remain frustratingly human. The recent discovery of a flaw in the bitcoin code revealed that it contained a bug[37] which would have allowed malicious miners to artificially inflate bitcoin's theoretically finite supply,[38] defeating its raison d'être.

Permissioned blockchains are a different beast altogether, limiting participation to identified participants who subscribe to system rules.[39] The latter, virtually synonymous with "terms of use" or "master agreements," govern who can join the system and how it operates. As the participants are known and legally bound to adhere to certain rules, the system itself need not be "trustless", i.e. their consensus algorithms would not need to contain code designed to curb selfish behaviour. There is no need to trust the code of the blockchain if it is possible to trust those who operate the individual nodes. A formalised governance process is usually followed – the coders are known and the code is formally vetted before inclusion. In the absence of "mining", there is no economic incentive contained within their consensus algorithms to curb selfish behavior by participants. Non-compliant participants are instead held accountable legally. In short, they rely on good old-fashioned trust.

C. The "Validation" Delusion

The technical literature often states that blockchains (or, to be more precise, their underlying consensus algorithms) "validate" transactions or other events. This has confused many into thinking that the technical meaning of the term overlaps with the legal meaning – establishing compliance with the law, declaring something legally valid, or otherwise demonstrating the truth of a statement.[40] It is necessary, however, to understand who validates what and against what criteria.

In the bitcoin blockchain, validation is inextricably linked to the concept of decentralised consensus.[41] Simply put, it is the process by which conformity of all copies of the ledger is ensured. Devotees often describe this process as involving democratisation, implying that the ability to make decisions is granted to all participants. Yet choice does not feature in decentralised decision making. The validation process is fully automated, deterministic and almost entirely controlled by the algorithm. With few qualifications, it is devoid of room for human discretion. More importantly, "validation" is premised on the fulfilment of technical conditions. In principle, a node cannot "decide" to reject a transaction meeting the validation criteria or accept one that does not. Blockchain "consensus" is thus difficult to map onto the legal and political meaning of the term, which denotes the process of reaching agreement among a group. There is some limited choice for miners, who can decide which valid transactions to include in the blocks that they mine, but miners do not represent the *demos* of a blockchain network. Given the expense involved, mining power is highly concentrated.[42] Choice in mining is thus more plutocratic than democratic. There is also an assumption that the very crude democracy inherent in blockchain consensus algorithms is

[37] See CVE-2018-17144 Full Disclosure at https://bitcoincore.org/en/2018/09/20/notice/ (accessed 6 December 2018).
[38] Fixed at 21 million bitcoins. Note that there is no cap for ether.
[39] D. Yermack, "Corporate Governance and Blockchains" (2017) 21 R.F. 7 at 16.
[40] See: Oxford English Dictionary definition of "validate"; above, n. 18, at pp. 1080-1082, referring to "[a] fail-proof system, the displacement of trust and the redefinition of truth".
[41] Antonopoulos describes decentralized consensus as an emergent artifact of the asynchronous interaction of thousands of independent nodes, all following simple rules, see: above, n. 20 at p. 217.
[42] N. Popper, "How China Took Center Stage in Bitcoin's Civil War", *The New York Times* (29 June 2016). Also see H. Murphy, "'Bitcoin whales' control third of market with $37.5bn holdings", *Financial Times* (9 June 2018).

inherently good without acknowledging that majoritarian rule can be extremely prejudicial to minorities, an acknowledgment that finds expression in most legal systems as constitutional freedoms in the political sphere and derivative actions in the economic sphere. An alternative consensus algorithm based on "proof-of-stake" is even more explicitly plutocratic.[43]

Validation relates to transactions and blocks. In law, a transaction is associated with a bilateral or multilateral arrangement. This often takes the form of a contract or associated property transfer but it is notable that even gifts are bilateral.[44] In the context of a blockchain, however, a "transaction" denotes the *unilateral* transfer of crypto-assets from one account to another as identified by their respective public addresses or "a signed data structure expressing a transfer of value."[45] Technically, a "transaction" is a change to the state of the blockchain[46] – not an exchange of bitcoins. What, then, does it mean that transactions are validated? To understand this, we must understand the process of generating blocks. Blocks contain lists of transactions. The appending of transactions in blocks rather than individually facilitates the use of cryptography to detect alterations to earlier transactions because the aggregated transactions are used to generate the aforementioned cryptographic hash linking one block to the next. If transactions are not appended in blocks, then some other method needs to be employed to detect/prevent ex-post alterations to distributed ledgers. To be included in a block, all nodes must establish that each transaction is correctly structured, uses previously unspent inputs, and contains sufficient transaction fees.[47] Nodes must also confirm that the unlocking scripts match the corresponding locking scripts.[48] Only a valid transaction can be aggregated into a block – but this does not mean that it has become part of the blockchain. Next, the block itself must be validated by the mining process. Mining consists of finding a solution to the "proof-of-work" algorithm by repeatedly hashing (i.e. applying a cryptographic algorithm to) the data comprising the block, which includes the transactions to be included as well as some random data, until the resulting hash matches the requisite specific target. Subsequently, each newly mined block is validated by every node in the network against certain technical criteria.[49] Validation thus signifies an automated, deterministic process of confirming that certain technical conditions have been met and carries no legal implications.

Obviously, the validation process cannot confirm off-chain events, i.e. events occurring in the real world. No consensus algorithm can establish or verify whether, for example, the transfer of bitcoin was actually due, whether it resulted from a legally enforceable contract, or, perhaps most significantly, whether the private key initiating the transfer of bitcoin was used by its rightful holder. As the English Law Commission recently explained, "[t]he question of whether an electronic signature is secure or reliable is a different matter from whether that signature is valid in law."[50] In technical terms, the "execution environment of a blockchain is self-contained as it can only access information in the blockchain. Information about external systems is not directly accessible."[51] Blockchains can only "see and react" to on-chain events

[43] V. Buterin, "Governance, Part 2: Plutocracy Is Still Bad", Blog Post (28 March 2018) at https://vitalik.ca/general/2018/03/28/plutocracy.html (accessed 6 December 2018).
[44] J. Hill, "The Role of the Donee's Consent in the Law of Gift" (2001) 117 L.Q.R. 127.
[45] Above, n. 20 at pp.18, 19.
[46] J. Gray, "The Transaction Concept: Virtues and Limitations," in M. Stonebraker (ed), *Readings in Database Systems* (San Francisco: Morgan Kaufman Publishing, 1988) at pp.140, 141; J. D. Ullman, *Principles of Database and Knowledge Base Systems*, vol 1; (Rockwell: Computer Science Press, 1988) at pp. 300, 301, 337.
[47] Above, n. 20 at pp. 24, 25.
[48] For a detailed description of validation criteria see: above n. 20, p. 218, 219.
[49] Above, n. 20 at p. 238.
[50] Law Commission Consultation Paper No 237, *Electronic Execution of Documents* (21 August 2018) at 20.
[51] Above, n. 26 at 6.

– an important point often overlooked by Nelsonian enthusiasts. It is, for example, reasonable to assume that most "contracts" formed on the online marketplace called Silk Road[52] were invalid or unenforceable as they were almost invariably tainted with illegality. Yet, the bitcoin payments for such goods or services were all validated by the bitcoin blockchain. The failure to understand the limitations of validation have led to such absurd projects as Legalfling,[53] an initiative to register consent to sexual relations on a blockchain.[54] As its developers acknowledge, "[i]t has limitations in case one of the parties blatantly lies."[55] Simply put, its blockchain is utterly useless precisely when it is most necessary.

D. The Highly Mutable Meaning of "Immutability"

Blockchains are often referred to as "immutable." The term can relate to three discrete situations: to the transactions or "assets" recorded in the blockchain, to other information recorded in the blockchain, or to the code of blockchain-based applications. In the first instance, it is stated that once a transaction is accepted into a block and once a block is appended to the ledger, it cannot be changed or reversed. This feature is commonly associated with guaranteed performance and transaction finality. The second situation concerns the possibility to inscribe "other information" into the blockchain, such as any arbitrary content that was not envisaged to be recorded by the bitcoin protocol. Examples of such content range from the original bitcoin white paper, political commentary, to more commercially-oriented content such as information about the ownership of real world assets, and even illicit content such as child pornography.[56] Once such content is embedded in the blockchain, it cannot be removed or changed. As a result, blockchains are often regarded a perfect record-keeping technology.[57] After all, everything that is inscribed in them stays there forever and cannot be changed. The inclusion of such information in the blockchain is the result of a "hack" of bitcoin addresses.[58] However, it is clear that the veracity of said information cannot be validated by the consensus algorithm.[59] The third situation in which the concept of immutability becomes relevant concerns the fact that (in most permissionless blockchains) it is impossible to change the code of applications running "on" it.[60]

"Immutability", it turns out, is a surprisingly mutable concept. First, not all blockchains are immutable.[61] Permissioned blockchains may give certain nodes the right to retrospectively edit the contents of a block, reverse transactions or, as part of formalised system upgrades, amend the underlying code. To the extent that such permission exists, it detracts from one of the main attractions of a distributed system: the absence of a single point of failure. It is unnecessary to hack the network if you only need to hack a single node with the permission to

[52] Illicit transactions on the Silk Road were an early use case for bitcoins that generated interest in the crypto-asset.
[53] https://legalfling.io/ (accessed 6 December 2018).
[54] Maya Salam, "Consent in the Digital Age: Can Apps Solve a Very Human Problem?", *The New York Times* (2 March 2018).
[55] https://legalfling.io/#faq in response to the question "Does this proof [sic] consent beyond any doubt?" (accessed 6 December 2018).
[56] R. Matzutt et al, "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin," in: *Financial Cryptography and Data Security* 2018. Twenty-Second International Conference , Curaçao , Netherlands (Aachen: RWTH Publications, 2018). See also Samuel Gibbs, "Child abuse imagery found within bitcoin's blockchain", *The Guardian* (20 March 2018).
[57] Above n. 18 at pp. 735, 736.
[58] The hack entails embedding additional content in bitcoin addresses or creating "fake" ASCII addresses.
[59] See text accompanying nn. 67-69.
[60] See text accompanying n. 219.
[61] See also n. 22 for distributed ledgers, which are not blockchains.

revise the network. Indeed, this is arguably less secure than a centralised register as each such node is a potential point of failure. Such permissioned blockchains trade the single point of failure of a centralised register for multiple points of failure.

Second, although "immutability" implies that something cannot be changed at all, immutability for permissionless blockchains turns out to be highly attenuated. Most infamously, a hard fork[62] (i.e. incompatible revision) of Ethereum's code was adopted by a majority of nodes in order to "undo" a hack.[63] This also "undid" all transactions appended to the blockchain, including perfectly legitimate ones, since it rolled the Ethereum blockchain back to its pre-hack state. However, not all users agreed with the decision to do so and a small but significant number of users persisted in using the older code, leading to two inconsistent Ethereum blockchains – subsequently christened Ethereum and Ethereum Classic. Apart from such hard forks in the code, random temporary forks in the blockchain records themselves recur frequently for "proof-of-work" blockchains. This is because "proof-of-work" only "acts as a randomized concurrency control mechanism, in which the block frequency is adjusted such that block collisions (i.e., concurrent appends of different blocks to the blockchain) are rare."[64] In plain English, it minimises but cannot eliminate the existence of incompatible copies of blockchains across all nodes. Such inconsistencies, or blockchain forks, arise when two or more miners successfully append different blocks onto the blockchain almost simultaneously. This results in two or more inconsistent blockchains, and although the consensus algorithm incentivises miners to mine the longest chain, it is impossible to predict which of the forked blockchains will prevail. It thus appears that blockchain immutability is not an absolute concept but rather more sixty blocks/shades of grey. Transactions get increasingly immutable as more blocks are added ahead of the block they are included in; hence the general advice to wait for six blocks of confirmation before treating a transaction as final.[65] In the parlance of the computer science community, "proof-of-work" blockchains lack "consensus finality,"[66] i.e. consensus in such blockchains can be both apparent (since nodes are unaware of forks) and fleeting (since, if a fork exists, they have no way of knowing whether their version of the blockchain will prevail). Try as it might, there are limits to how far the blockchain technology can limit the potential for multiple copies of a ledger from containing discrepancies but the scale of the challenge must also be borne in mind – today, there are more than 10,000 nodes in the bitcoin network.

Third, when speaking of blockchains as a perfect record-keeping technology, particularly in the field of provenance tracking and asset registries, the immutability of the recorded information is incorrectly associated with its veracity. Phrases like "the truth machine," obfuscate the fact that if the information relates to off-chain assets or events, its inscription in a block does not guarantee its accuracy.[67] The consensus algorithm is technically

[62] See text accompanying nn. 190-195. More generally, see Low and Teo, above n. 31, at pp. 259-264.
[63] See text accompanying nn. 137-139.
[64] M. Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of Work vs. BFT Replication," in: J. Camenisch and D. Kesdoğan (eds) *Open Problems in Network Security* (2016) Lecture Notes in Computer Science, vol 9591 (New York: Springer, 2016).
[65] For bitcoins. The advice is to wait for 20-25 confirmations for ethereum. However, because the average time to mine a block for ethereum is only 15 seconds compared to 10 minutes for bitcoin, the average time for the recommended number of confirmations is only six minutes for ethereum as against 60 minutes for bitcoin. Note also that the accidental fork in the bitcoin blockchain on 11 March 2013 lasted for 24 blocks and six hours: see V. Buterin, "Bitcoin Network Shaken by Blockchain Fork", *Bitcoin Magazine* (12 March 2013).
[66] Above, n. 65.
[67] See text accompanying nn. 137-139.

incapable of establishing the occurrence of off-chain events.[68] In the provenance tracking and asset registration context, it cannot verify, for example, whether it was the rightful owner who "registered" his cow or whether a particular batch of fish was actually caught in a certain location. Nor can it determine whether subsequent transfers are authorised. Any errors, either in recording or authorisation, married to immutability, simply produce enduring errors.

Fourth, even if a blockchain were technically immutable in an absolute sense, it would still be possible to substantially undo the effects of a transaction by way of a further transaction of equal value in reverse. To the extent that such transactions may be coerced by law, the "immutability" of even native crypto-assets may be suspect.[69] It is not difficult to imagine that a court may order such a reversal or at least compensation if, for example, the "transferor's" private key had been misused by a hacker. Any law reform contemplating the use of blockchain should clarify how the law relates to each of these various conceptions of immutability but none do so.

E. Blockchains as Databases

From a technical perspective, blockchains are cryptographically secured ledgers. Traditionally, ledgers are databases (i.e. collections of data) recording either transactions or assets occurring or existing outside of them. Within the law, the preferred term of art where a ledger records assets is register. For our purposes, we can treat "ledger" and "register" as synonyms and regard both as a type of database. Logically, transactions are not executed "by" or "on" the pages of ledgers. Ledgers only record information about their occurrence. Exceptionally, blockchains can be regarded as enabling transactions in the sense that transfers of native crypto-assets, such as bitcoin or ether, cannot occur otherwise than "in" the ledger.[70] But "traditional" assets, such as houses or cars and (less obviously) even copyright and carbon credits, do not exist solely on the pages of ledgers – ledgers reflect a state of the world outside of them.

This leads to the next point: the attributes of the blockchain must be differentiated from the attributes of other applications that run "on" the blockchain or form part of a "blockchain system." The differentiation requires an understanding of the technical limitations of the original blockchain. In a centralised database, modifications to its contents can only be made by a single entity, subject always to judicial oversight where asset registries are concerned. This entity controls the contents of the database and determines what other entities have read and write permissions, if any. By contrast, in a decentralised blockchain database, modifications can, in theory, be made by any node. Given that the individual nodes cannot be trusted and no single entity controls such modifications, the database itself must be trusted and incorruptible. This in turn requires the restriction of the type of permissible modifications and the manner of performing them.[71] In short, if no one is in control and anyone has the right to modify the database, such modifications must be kept simple. Broadly speaking, an increase in the complexity of transactions that can be supported by a blockchain requires that the blockchain be equipped with additional functionalities, including the ability to accept external input – protocol layers must be added on top of them.[72] Consequently, unless the usability of blockchains is to be confined to the generation and transfer of native crypto-assets,

[68] See text accompanying nn. 50-55.
[69] Low and Teo, above n. 31, at pp. 254-259.
[70] Low and Teo above n. 31, at pp. 252-254.
[71] G. Greenspan, "Why Many Smart Contract Use Cases Are Simply Impossible", *Coindesk* (April 17, 2016) at https://www.coindesk.com/three-smart-contract-misconceptions (accessed 6 December 2018).
[72] Above n. 20, at p. 218.

blockchains must be seen as only a part of a larger ecosystem of technologies built around them.[73] Even if the blockchain is "trustless" etc., this does not imply that the other components in the system share these attributes. If only the database is "trustless" but none of the other system components are, then – when evaluated as a whole – the entire system is only as good as its weakest link. Cryptomaniacs tout the opposite.

III. RIGHTS & RECORDS

One of the most oft-cited use cases for the blockchain in the law is as a form of distributed asset registry. There are now a host of initiatives, both public and private, applying the blockchain to a variety of assets ranging from land[74] to securities[75] to intellectual property.[76] Many of these initiatives are seriously misguided. This is not to say that it is impossible to have blockchain asset registries. Rather, many blockchain-enthusiasts have underestimated the complexities involved in the creation and maintenance of a registry and/or overestimated the vaunted "security" of blockchains.

A. Private Blockchain Asset Registries

First, to the extent that many of these early initiatives are entirely private, they will not be able to provide the sort of proof of ownership of the underlying assets that a public registry can provide. In this respect, we are referring not to the public or private nature[77] of the blockchain employed but the involvement or in this case, lack thereof, of government and hence, the law. Some of these private initiatives employ permissioned blockchains but many employ permissionless blockchains. Many initiatives, especially because they tout the immutability of blockchains,[78] implicitly assume that registries provide an authoritative record of ownership. This stems in part from a failure to distinguish between the thing that is the object of ownership and the record of the right to the thing. This is self-evident in bitcoin, where the object of

[73] This can be illustrated by, for example, the Hyperledger architecture, which provides the technical framework for permissioned blockchains and distinguishes between different components in this framework Hyperledger Architecture, Volume II, Smart Contracts, p. 3 https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf (accessed 6 December 2018).

[74] A project to establish a blockchain land registry in Honduras was much lauded as an instance of using the blockchain's "trustless trust" to fill the vacuum of trustworthy institutions in a developing economy: "The Great Chain of Being Sure About Things", *The Economist* (31 October 2015). For more details of the Honduras project and a more skeptical view, see V. L. Lemieux, "Trusting Records: Is Blockchain Technology the Answer?" (2016) 26 R. M. J. 110. See also N. Kshetri, "Will Blockchain Emerge as a Tool to Break the Poverty Chain in the Global South?" (2017) 38 T.W.Q. 1710. Sweden appears to be the most notable developed economy to explore a blockchain land registry: see Kairos Future, "The Land Registry in the Blockchain-Testbed" (March 2017) https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf See also J. McMurren, A. Young, and S. Verhulst, "Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers" (October 2018) https://blockchan.ge/blockchange-land-registry.pdf

[75] The Australian Stock Exchange has decided to replace its Clearing House Electronic Subregister System (CHESS) system with one using distributed ledger technology: see Australian Stock Exchange, "CHESS Replacement: New Scope and Implementation Plan Consultation Paper" (April 2018) https://www.asx.com.au/documents/public-consultations/chess-replacement-new-scope-and-implementation-plan.pdf (accessed 1 March 2019). Luxembourg passed Bill 7363, which supposedly grants transactions conducted on a blockchain the same legal status as those conducted traditionally, on 14 February 2019, an informal English translation is available at https://www.letzblock.com/blog/draft-luxembourg-law-7363 (accessed 1 March 2019).

[76] See text accompanying nn. 115-120.

[77] See text accompanying nn. 24-39.

[78] See text accompanying nn. 56-74.

ownership, "an electronic coin", is defined by its ledger entries, being "a chain of digital signatures".[79]

Although many do not perceive the difference in form between native crypto-assets and so-called electronic bank money,[80] the legal nature of these two forms of assets could hardly be more different. Native crypto-assets[81] may well be electronic assets properly so-called because their legal nature is irrevocably tied to the electronic blockchain register.[82] But that is not the case with so-called electronic bank money. Money held in bank accounts is today firmly established in most legal systems as taking the legal form of *in personam* claims against the bank.[83] This was not always the case[84] but the historical position is now irrelevant and it is its modern form that permits its "transfer" in the sense that is so misunderstood today. Such property is intangible and formless. Any register's representation of property is merely a record of the property right rather than the property right itself. The temptation to confuse the record with the right is easily dispelled when we examine registers recording tangible assets. Many jurisdictions with developed economies have well-established land registers and these registers are increasingly migrating from paper to electronic form.[85] Yet no one supposes that the transition results in land, as opposed to its record, existing in electronic form.

The confusion stems in part from a key difference between tangible and intangible property. The category of tangible property coincides with the category of *in rem* rights strictly so-called and, insofar as property is regarded as a right rather than a thing, such property entail rights that relate to things, or *res* to employ the Latin, that are separable from and distinct from the right.[86] While some would confine the category of property to such rights,[87] and it is arguable that the civilian traditions, particularly those with Germanic roots, follow such a narrow conception of property,[88] this is not true of common law systems. Common law systems have a long tradition of regarding choses in action as personal property. But it is important to observe that such property differs from that of tangible property in important respects. Unlike

[79] See Satoshi Nakamoto, (October 2008) "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf at 2.

[80] See, for example, Morten Bech and Rodney Garratt, 'Central Bank Cryptocurrencies,' BIS Quarterly Review, September 2017, at 60, "Graph 3 The Money Flower: A Taxonomy of Money."

[81] Provided they are not securities. Cf. Jay Clayton, Chairman, U.S. Securities and Exchange Commission, "Statement on Cryptocurrencies and Initial Coin Offerings" (11 December 2017). But see Financial Conduct Authority Feedback Statement FS17/4, "Distributed Ledger Technology" (December 2017).

[82] See K. F. K. Low and E. Teo, "Legal Risks of Owning Cryptocurrencies" in D. Lee and R. Deng (eds), *Handbook of Blockchain, Digital Finance, and Inclusion*, Volume 1 (London: Academic Press, 2017), 225 at pp. 241-242.

[83] For the common law, see *Foley v Hill* (1848) 2 H.L.C. 28, 9 E.R. 1002. Cf. S. Meder, "Giro Payments and the Beginnings of the Modern Cashless Payment System" in D. Fox and W. Ernst (eds), *Money in the Western Legal Tradition: Middle Ages to Bretton Woods* (Oxford: Oxford University Press, 2016) at p. 409.

[84] B. Geva, "'Bank Money': The Rise, Fall, and Metamorphosis of the 'Transferable Deposit'" in D. Fox and W. Ernst (eds), *Money in the Western Legal Tradition: Middle Ages to Bretton Woods* (Oxford: Oxford University Press, 2016) at p. 359.

[85] See, eg, R. Low, "From Paper to Electronic: Exploring the Fraud Risks Stemming From the Use of Technology to Automate the Australian Torrens System" (2009) 21 Bond L. Rev. 107.

[86] B. McFarlane and S. Douglas, "Defining Property Rights" in J. Penner and H. Smith (eds), *Philosophical Foundations of Property Law* (Oxford: Oxford University Press, 2013) at p. 219.

[87] Ibid.

[88] See K. F. K. Low and Y. C. Wu, "The Characterisation of Cryptocurrencies in East Asia" in D. Fox and S. Green (eds), *Private and Public Law Implications of Cryptocurrencies* (Oxford: Oxford University Press, 2019, forthcoming) and K. Takahashi, "Cryptocurrencies Entrusted to an Exchange Provider: Shielded from the Provider's Bankruptcy?" in C. Hugo (ed.) *Annual Banking Law Update 2018: Recent Legal Developments of Special Interest to Banks* (Johannesberg: Juta Law Publishers, 2018) at p. 1.

tangible property, where the object of the right is distinct and separable from the right itself, no such separable object exists for intangible property. This is perhaps more obvious from the supposedly archaic terminology of chose in action. Where property is in action, Blackstone explained,[89] "a man hath only a bare right." "The right *is* the *res*".[90]

The absence of a separable object renders it easier to confuse right with record, especially where the record, like the right, is itself also intangible. We see the same temptation to confuse right and record with carbon credits in *Armstrong DLW GmbH v Winnington Networks Ltd*, where carbon credits recorded in electronic registries were regarded as existing "only in electronic form".[91] A similar confusion between right and record can be found in Article 2(2) of Directive 2009/110/EC of the European Parliament and of the Council, which defines "electronic money" as "electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions … and which is accepted by a natural or legal person other than the electronic money issuer".[92] That which is stored electronically is not value per se but a record of a claim that is valuable and the muddle between record, claim, and value can lead to much unnecessary confusion.[93] This same confusion can be found in one of Wyoming's many new blockchain "enabling" laws, which defines "digital asset" as "a representation of economic, proprietary or access rights that is stored in a computer readable format".[94]

Unlike the case for native crypto-assets,[95] the use of blockchain technology as an asset registry system poses entirely different challenges. These pre-existing rights are subject to well-established rules of law, particularly in relation to their transfer. Any record keeping system that is not fully compatible with these existing legal rules will therefore require legal amendments in order to be effective. Contrary to popular belief, public registration systems are remarkably heterogeneous so far as their role as indicia of title is concerned. Some registration systems provide prima facie evidence of title such as in the case of shares,[96] patents,[97] and registered designs.[98] Some registration systems, such as that for trademarks, do not purport to provide any indication as to title at all, prima facie or otherwise.[99] Where this is the case, such as for bank ledgers, "in the absence of fraud, the customer is not precluded by the bank statement or the pass-book from disputing an error or an incorrect debit made by the bank or

[89] W. Blackstone, *Commentaries on the Laws of England, Book II: Of the Rights of Things* (Clarendon Press: Oxford, 1766) at p. 389.
[90] K. F. K. Low and J. Lin, "Carbon Credits as EU Like It: Property, Immunity, TragiCO_2medy?" (2015) 27 J.E.L. 377 at 402.
[91] [2013] Ch 156, [49].
[92] It is notable that, in its original implementation of the EU legislation, Germany took pains to describe such "electronic money" as "*Werteinheiten in Form einer Forderung gegen die ausgebende Stelle, die auf elektronischen Datenträgern gespeichert sind*" (units of account in the form of a claim against the issuing entity, which are recorded on electronic media): Section 1(14), *Kreditwesengesetz*. But *contra* Section 1(2), *Zahlungsdiensteaufsichtsgesetz*.
[93] For carbon credits, see above n. 90.
[94] Wyo. Stat. Ann. §34‑29‑101. The law envisages three categories of "digital assets": (i) digital consumer assets; (ii) digital securities; and (iii) virtual currencies. To the extent that the last category encompasses native crypto-assets, this may be accurate but the first two categories clearly envisage the digital record as reflecting off-chain enforceable legal rights.
[95] Low and Teo, above n. 31 at 252-254.
[96] Companies Act 2006, s 127.
[97] Patents Act 1977, s 32(9), although its operation in this respect is arguably somewhat indirect.
[98] Registered Designs Act 1949, s 17(8).
[99] Trade Marks Act 1994.

from insisting on its correction."[100] On the other hand, registration of a fee simple title to land in England provides far greater protection than prima facie evidence of title, going so far as to validate an otherwise void transfer.[101] Torrens systems of land registration, which also have a similar effect, vividly, if misleadingly, describe such validation as indefeasibility.[102] The entry of a notice on the register of an equitable interest in land in England behaves differently again, providing priority without validating invalid transfers,[103] an effect similar to that provided in older legislation for the registration of deeds. To the extent that a public register confers any benefits in terms of proof of ownership, this is achieved through legislation and not the mere existence of the register itself yet it is notable that practically all blockchain legal reforms to date have been completely silent as to what happens when a blockchain record departs from a traditional analysis of title. Is the record rectifiable, as is the case with most centralised registers? If so, how can rectification work in the context of a distributed and immutable register?[104] The form of such orders and the parties they are directed at would have to change, and questions of their efficacy would also have to be addressed. First, rectification can no longer operate by deleting the erroneous record. Instead, a new record would have to be added to the register to substantively though not formally undo it. Secondly, as there is no centralised authority against whom such an order can be made, and it makes no sense to make orders against thousands of operators of nodes, many of whom will be beyond the jurisdiction of a single court, such "rectification" orders would have to be directed towards individual defendants instead to use their private keys to authorise equal and opposite transactions, likely backed by the threat of contempt proceedings. However, and consequentially, if the defendant is either out of the jurisdiction or otherwise recalcitrant, the law may be powerless to rectify such errors unless the relevant blockchain permits revisions. No permissionless blockchains can allow for such revisions and not all permissioned blockchains do. Those that do introduce single or multiple points of failure within the registry depending on the number of nodes with such permission.

Accordingly, private registers cannot guarantee title and are at best the basis of a contractual agreement as to risk allocation among participants, with many probably even failing to amount to such. Given the origins of the blockchain in bitcoin and the comparison of its blockchain to bank ledgers, it is pertinent to explain why bank ledgers, a private arrangement between banker and customer, are a poor foundation upon which to build aspirations for private blockchain asset registries. First, the nature of bank money as an asset and the means of their "transfer" make them an inapposite case study for most other instances of property dealing. Because bank money essentially takes the form of a debt, they are fundamentally contractual in nature. As a result, it is theoretically within the rights of the parties to the contract, being the bank and its customer, to agree upon the scope of its availability within the limits of freedom of contract. But any agreement by two or more parties to the effect that other property would behave in a particular manner different to the default rules established by the law would fall foul of the *numerus clausus* (Latin for closed number) principle,[105] which limits the types of proprietary rights the law recognises.

---

[100] E. P. Ellinger, E. Lomnicka and C. V. M. Hare, *Ellinger's Modern Banking Law* 5th edn. (Oxford: Oxford University Press, 2011) at p. 236.

[101] Land Registration Act 2002, s 58(2).

[102] Cf. The Law Commission's description of the Land Registration Act 2002 as endorsing "qualified indefeasibility": Law Commission Report No 271, Land Registration for the Twenty-First Century: A Conveyancing Revolution (2001) at p. 221.

[103] Land Registration Act 2002, s. 32(3).

[104] Cf. Low and Teo, above n. 31 at 254-259. See also Yeung, above n. 12 at 214.

[105] B. Rudden, "Economic Theory v Property Law: The *Numerus Clausus* Problem" in J. Eekelaar and J. Bell (eds.), *Oxford Essays in Jurisprudence, 3rd series*, (Oxford: Oxford University Press, 1987), at p. 262. See also

Nor do "transfers" of bank money operate as transfers in the orthodox sense of the word, again because of its contractual nature. The doctrine of privity of contract prevents outright transfers of contractual rights. Common law systems circumvented the doctrine of privity by employing the notion of a derivative transfer via assignment in equity.[106] Equitable assignment permitted the law to square the circle by allocating control of the right to bring the action to the assignee whilst insisting on the interposition of the assignor as claimant in any action against the obligor. Thus, the economic result of a transfer was achieved without offending the formal rule of privity. But such assignments, which deal with the same asset, ie the very same debt claim, have nothing to do with bank "transfers" of money, which do not deal in the same asset. As Fox explained, "[t]he chose in action representing the money transferred to the recipient's bank account is a distinct item of property from the chose in action representing the funds which were originally in the payer's account."[107] To describe the process as a "transfer" is "a misnomer" as "in fact nothing tangible or intangible is transferred."[108] Rather, a debt owed by a bank to the payer is extinguished and another debt, owed by the same or another bank to the payee, is substituted for the same amount. Through this process of extinction and creation, which is not necessarily simultaneous (again unlike a true transfer),[109] value is transferred without a transfer of property.[110] But transfers of other forms of property do not behave this way. They are true transfers properly so-called. When A sells Blackacre to B, B acquires that precise plot of land. The same is also true of cars and cows and copyright in songs.

Secondly, despite the somewhat fearsome and unsettling contractual language in standard form banking contracts, such as "You agree to be liable for any transactions which, according to our records, were made using your password, whether you actually made them or not",[111] the legal efficacy of such clauses is largely untested. Although most legal systems in principle respect freedom of contract, such freedom is hardly unfettered. In the United Kingdom, all standard terms that exclude liability are subject to scrutiny for reasonableness under the Unfair Contract Terms Act 1977. Where the terms are imposed on a consumer, the terms are further subject to scrutiny under the Consumer Rights Act 2015. Significantly, such clauses contradict the standards set out in the 'Banking: Conduct of Business Sourcebook' issued by the Financial Conduct Authority.[112] In Australia, consumer protection is provided by the Australian Consumer Law.[113]

T. W. Merrill and H. E. Smith, "Optimal Standardization in the Law of Property: The *Numerus Clausus* Principle" (2000) 110 Y.L.J. 1; T. W. Merrill and H. E. Smith, "The Property/Contract Interface" (2001) 101 Colum. L. Rev. 773; B. Akkermans, "The *Numerus Clausus* of Property Rights" in M. Graziadei and L. Smith (eds.), *Comparative Property Law* (Cheltenham: Edward Elgar Publishing, 2017), at p. 100.

[106] M. Smith and N. Leslie, *The Law of Assignment*, 3rd edn (Oxford: Oxford University Press, 2018) at pp. 213-221, 230-234. See also C. H. Tham, "Joinder of equitable assignors of equitable and legal choses in action" [2017] LMCLQ 537, at 542–549.

[107] D. Fox, *Property Rights in Money* (Oxford: Oxford University Press, 2008), at para [5.05].

[108] B. Geva, "'Bank Money': The Rise, Fall, and Metamorphosis of the 'Transferable Deposit'" in D. Fox and W. Ernst (eds), *Money in the Western Legal Tradition: Middle Ages to Bretton Woods* (Oxford: Oxford University Press, 2016) 359, at p. 360. Cf. Cf. B. Geva, "The Order to Pay Money in Medieval Continental Europe" in D. Fox and W. Ernst (eds), *Money in the Western Legal Tradition: Middle Ages to Bretton Woods* (Oxford: Oxford University Press, 2016) 409.

[109] Above n. 107 at paras [5.70]-[5.73].

[110] Above n. 107 at paras [5.25]-[5.32].

[111] M. Brignall, "So You Think You're Safe Doing Internet Banking?", *The Guardian* (21 November 2015). See also I. Becker et al, "International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms", Workshop on the Economics of Information Security (WEIS), 13-14 June 2016, Berkeley, CA, USA.

[112] "Banking: Conduct of Business Sourcebook" (Release 34: December 2018), paras [5.1.11]-[5.1.12].

[113] Schedule 2 of the Competition and Consumer Act 2010 (Cth), replacing the Trade Practices Act 1974 (Cth).

As such, no private initiative to establish a blockchain asset registry will be effective in establishing title beyond proving that the correct private key was used to initiate a transaction. They can no more establish that the private key was used by its rightful holder than legally prevent the owner from effecting a transfer off-chain.[114] Even if we assume that this enhances transparency to some degree, private initiatives to establish blockchain asset registries face a further challenge. Where among the dozens of private blockchains should a purchaser look to identify the owner of any particular asset? For copyright in music alone, there are at least five blockchain initiatives that we are aware of at the time of writing: Berklee College of Music's Open Music Initiative,[115] Blòkur,[116] Mycelia,[117] Soundac,[118] and Ujo.[119] Then, there is the vexing problem of forks where the initiative utilises a permissionless blockchain, which will be examined in greater detail hereafter.[120]

B. The Byzantine Quest for Decentralisation

Before considering the suitability of permissionless or permissioned blockchains as the technological backbone of asset registries, it is necessary to consider the very different perspectives of lawyers and technologists to what can appear at first glance to be the same problem. At its heart, the law of property is concerned with the allocation of scarce resources. Although some aspects of the law deal with initial allocations of property, many of the core rules that are well-known to lawyers deal with subsequent transfers, in particular when such transfers lead to conflicting claims to the same asset. The difficult question of how such conflicting claims are to be resolved lies at the heart of the law of property. The problem is challenging because the circumstances are multifarious and competing claimants are often both innocent. The complexity of the problem is demonstrated by the range of different rules that apply in common law systems depending on the nature of the claims asserted by the competing claimants (e.g., legal or equitable) and the nature of the asset claimed (money, goods, land, or other property). Registration plays only a minor role in most disputes simply because most assets are either not registered (e.g. goods, notes and coins, copyright) or registration serves limited[121] or no[122] authoritative function in establishing title to the asset. The association of registration with authoritative evidence of ownership is most commonly developed through familiarity with land registration but even here, authoritative registers are a relatively recent phenomenon. The earliest land registries were registries of deeds,[123] for which registration conferred priority in disputes where conflicting claims had to be resolved but which was not authoritative.

---

[114] Contractual prohibitions of assignments do not actually effectively prevent the assignment of the property. For chattels, see *Taddy & Co v Sterious & Co* [1904] 1 Ch 354; *Mcgruther v Pitcher* [1904] 2 Ch 306; *London County Council v Allen* [1914] 3 KB 642; *Dunlop Pneumatic Tyre Co Ltd v Selfridge and Co Ltd* [1915] AC 847; *Barker v Stickney* [1919] 1 KB 121. For leases, see *Williams v Earle* (1868) LR 3 QB 739; *Old Grovebury Manor Farm v W Seymour Plant Sales and Hire Ltd (No 2)* [1979] 1 WLR 1397. Cf. *Linden Gardens Trust Ltd v Lenesta Sludge Disposals Ltd* [1994] 1 AC 85 in relation to purely contractual choses in action; *Tulk v Moxhay* (1848) 2 Ph 774 in relation to restrictive covenants for land.

[115] http://open-music.org/ (accessed 6 December 2018).

[116] https://www.blokur.com/ (accessed 6 December 2018).

[117] http://myceliaformusic.org/ (accessed 6 December 2018).

[118] https://soundac.io/ (accessed 6 December 2018).

[119] https://ujomusic.com/ (accessed 6 December 2018).

[120] See text accompanying nn. 190-195.

[121] For shares (Companies Act 2006, s 127), patents (Patents Act 1977, s 32(9)), and registered designs (Registered Designs Act 1949, s 17(8)), registration merely provides prima facie evidence of title.

[122] See, e.g., Trade Marks Act 1994.

[123] F. Sheppard and V. Belcher, "The deeds registries of Yorkshire and Middlesex" (1980) 6 J. Soc. Arch. 274.

Dissatisfied with the half measures of the deed registration system, Sir Robert Torrens of South Australia is credited with the birth of modern title registration, whereby registration is given authoritative effect.[124] The Torrens system spread throughout the Australian colonies, New Zealand and beyond,[125] won admiration from English lawyers,[126] and served as inspiration in part for both the Land Registration Act 1925[127] and the Land Registration Act 2002.[128] In order to understand the advantages and drawbacks wrought by these changes, it is necessary to first understand the devil's choice that the law of property often faces. Where C through fraud effects a "transfer" of property from A to B, whose claim to the asset "transferred" should prevail as between A and B? There is no universally accepted correct answer to this problem but fundamentally, any rule that favours A is said to favour what Demogue called "static" security whereas any rule that tends to favour B is said to favour what he called "dynamic" security.[129] Static security, which prefers A, favours the policy that it ought not to be possible for a property owner to be deprived of his property by the unauthorised act of another. Dynamic security, on the other hand, which prefers B, favours subsequent bona fide purchasers at the expense of the original owner. The two aspects of security, unfortunately, lie in opposition to each other. Any improvement in static security must come at the expense of dynamic security and vice versa.

For common law systems, both the common law's default rule, which is *nemo dat quod non habet*,[130] as well as equity's maxim, *qui prior est tempore potior jure*,[131] favour static security. The unfortunate consequence of this policy was that conveyancing became cumbersome, expensive and fraught with risk. Title registration along the lines of the Torrens statutes and more modern English land registers "decisively shifted the conveyancing law towards the opposing principle of dynamic security."[132] By making registration more authoritative, conveyancing was simplified but carried an often forgotten cost. A shift from static to dynamic security does not in and of itself prevent fraud, as a comparative analysis of Singapore and Malaysia, both operating Torrens systems, tellingly demonstrates.[133] All it does is shift losses when frauds occur and property owners are occasionally rudely reminded of the high cost of dynamic security. For example, in 2006 in Singapore, a 90 year old Bebe bte Mohammad, who was suffering from Alzheimer's disease, was defrauded of her property when

[124] For background as to how the Torrens system was conceived, developed and eventually born, see P. M. Fox, "The Story behind the Torrens System" (1950) 23 A. L. J. 489. Cf S. Robinson, *Transfer of Land in Victoria* (Sydney: Law Book Company, 1979), at para [1-25].

[125] For a list of jurisdictions that have adopted a Torrens system of land registration, see S. R. Simpson, *Land Law and Registration* (New York: Cambridge University Press, 1976) 81; M. Raff, *Private Property and Environmental Responsibility* (The Hague: Kluwer Law International, 2003) at p. 9.

[126] T. B. F. Ruoff, *An Englishman Looks at the Torrens System* (Sydney: Law Book Company, 1957).

[127] K. Gray and S. F. Gray, *Land Law*, 7th Ed (Oxford: Oxford University Press, 2009), at para [2-044].

[128] Ibid. See also Law Commission Consultation Paper No. 254, "Land Registration for the Twenty-First Century: A Consultative Document" (1998); Law Commission Consultation Paper No. 227, "Updating the Land Registration Act 2002: A Consultation Paper" (2016).

[129] R. Demogue, "Security" in A. Fouilleé, J. Charmont, L. Duguit and R. Demogue (eds), F. W. Scott and J. P. Chamberlain (trans), *Modern French Legal Philosophy* (New York: The Macmillan Company, 1968) at p. 418.

[130] No one may give what he does not have.

[131] He who is earlier in time is stronger in law.

[132] P. O'Connor, "Registration of Title in England and Australia: A Theoretical and Comparative Analysis" in E Cooke (ed), *Modern Studies in Property Law Vol 2* (Oxford: Hart Publishing, 2003) at pp. 85-86.

[133] H. W. Tang and K. C. Loh, "A Law Which Favours Forgers: Land Fraud in Two Torrens Jurisdictions" (2011) 19 Australian Property Law Journal 130, highlighting the different incidences of fraud in the two Torrens jurisdictions. As Singapore used to be part of Malaysia from 1963-1965, the comparison of the two jurisdictions is particularly instructive. In Singapore, land fraud is remarkably uncommon. In Malaysia, it is significantly more widespread.

one of her adopted daughters forged a mortgage, which was registered, in favour of a bank.[134] Another Torrens jurisdiction, New Zealand, has recently shifted slightly away from dynamic security through a controversial amendment to its legislation.[135] It has also been suggested that Torrens registration facilitated the dispossession and exclusion of indigenous people in British colonies.[136] It is not difficult to imagine the process of transitioning to blockchain asset registration being used as a similar opportunity to dispossess the underprivileged since the initial recording process will be dependent on the trustworthiness of third parties who tag, map, and register the off-chain assets,[137] a problem vividly described as, "garbage in, garbage out".[138] It is thus unsurprising that by some accounts, the Honduras Title Project stalled owing to "political issues".[139]

The "insurance principle" underlying most Torrens registration systems is also telling. Although often heralded as the third[140] key principle of Torrens registration, it was most likely established to overcome the hostilities of vested interests opposed to the shift from static to dynamic security.[141] However, insurance needs to be funded and unless taxes are raised, this can only be achieved through higher transaction fees but this partly recreates one of the problems title registration was supposed to solve. That title registration legislation is not some magic wand that will cure all ills can be seen in the Hong Kong experience, where differences over the adequacy of insurance have prevented the Land Titles Ordinance,[142] enacted in 2004, from being brought into force.[143]

There is a further cost to the shift to title registration – all such systems operate in a "bijural" fashion.[144] They are bijural in the sense that they straddle two conflicting bodies of law. Many title registration systems confer title to the interest recorded regardless of the validity of the registered instrument. Whilst in theory no void instrument should ever be registered, in practice some defects will pass undetected by the registry and appear on the register. This necessitates a system of rules to determine when such registrations may be set aside or overridden. Bijuralism demonstrates that whilst modern title registration systems are more authoritative,[145] they are not absolutely authoritative. An absolute monojural title

[134] *United Overseas Bank Ltd v Bebe bte Mohammad* [2006] 4 SLR(R) 884; [2006] SGCA 30. Fortunately for Bebe, she could avail herself of the state insurance despite the relatively parsimonious regime operating in Singapore: see B. Crown, "Whither Torrens Title in Singapore?" (2010) 22 S.Ac.L.J. 9. Cf. H.W. Tang, and K.F.K. Low, *Tan Sook Yee's Principles of Singapore Land Law*, 4th edition (Singapore: LexisNexis, 2019) at pp. 268-269.

[135] New Zealand Land Transfer Act 2017, ss. 54-57, introducing the controversial concept of manifest injustice.

[136] S. Keenan, "From historical chains to derivative futures: Title registries as time machines" (2019) 20 Soc. & Cult. Geogr. 283.

[137] Cf Lemieux, above n. 74.

[138] A. Mizrahi. "Factom CEO: Blockchain-based Transparent Mortgages Can Restore Trust in Markets." *Finance Magnates* (3 March 2016) at www.financemagnates.com/cryptocurrency/interview- 2/factom-ceo-blockchain-based-transparent-mortgages-can-restore-trust-in-markets/ (accessed 6 December 2018).

[139] P. Rizzo, "Blockchain Land Title Project 'Stalls' in Honduras", *Coindesk* (26 December 2015) at https://www.coindesk.com/debate-factom-land-title-honduras (accessed 1 March 2019).

[140] Alongside the "mirror principle" and the "curtain principle".

[141] R. T. J. Stein and M. A. Stone, *Torrens Title* (Sydney: Butterworths, 1991) at p 349-350; R A Woodman and P J Grimes, *Baalman on The Torrens System in New South Wales* 2nd edition (Sydney: Law Book Company, 1974) at p. 389.

[142] Cap 585.

[143] N. Ng, "Overdue law on land titles could have simplified flat-buying in Hong Kong, Audit Commission says", *South China Morning Post* (23 November 2017).

[144] P. O'Connor, "Deferred and Immediate Indefeasibility: Bijural Ambiguity in Registered Land Title Systems" (2009) 13 Edinburgh Law Review 194 at 195-196.

[145] Cf Land Registration Act 2002, s 58(1).

registration system is theoretically possible but it will operate extremely harshly – as "indefeasibility on steroids" [146] – unless all possibility of error can be precluded. History reminds us that hard-edged rules emphasising certainty tend to invite pushback in the form of ambiguous rules whenever the former dictate harsh outcomes that are undesirable.[147] For example, the "muddy" doctrine of part performance was judicially engineered to undermine the "crystalline" formalities demanded by the Statute of Frauds 1677. Given the many vulnerabilities of blockchains, particularly its dependence on the end user's ability to safeguard their private keys, the adoption of an absolute rule of "code as law" for blockchain asset registries is simply untenable. All well-drafted asset registration systems contain provisions for the rectification and/or alteration of errors that can creep into the register.[148] But the "immutability" of blockchains is an obstacle to rectification.

The perspective of computer scientists is very different. The key advantage of a distributed system is its built-in redundancy. However, the price of distribution is the potential for inconsistency. Where the distributed system is a database, this entails the possibility that dispersed copies of the database might contain different information. This is, of course, a nonexistent problem in centralised databases. The challenge for computer scientists is to ensure consensus throughout the distributed system (i.e. all end users see the same content) in addition to reliability. There are two main causes of failure of consensus in a distributed system. First, there could be a network failure in which, although the nodes forming the network work perfectly, the network that connects them fails, usually partially, leaving some nodes unconnected to others. Whilst such failures can be minimised, they cannot be wholly avoided. Secondly, the network could be fully functional but one or more nodes could fail. Node failures can be divided into "fail stop" and Byzantine failures. When a node encounters a fail stop, the other nodes would at least be aware that it has failed because it stops working altogether. A Byzantine failure, on the other hand, is any failure in which a node operates in a flawed manner. The reasons for such failure are infinitely varied, ranging from data corruption, a bit flip in memory, to the node having been compromised by malicious software. The name originates in a seminal computer science paper that used the metaphor of several divisions of a Byzantine army camped outside an enemy city to describe the problems of achieving consensus in distributed systems when parts of it malfunction in a way that other parts are unaware of.[149] Consequently, the task of building distributed systems tolerant to such malfunctions came to be known as developing Byzantine fault-tolerance. Traditional Byzantine fault-tolerant systems were designed with so-called state machine replication, in which a service is deployed in a set of servers rather than a single central server. State machine replication is also known as active replication and can be contrasted with the primary-backup, or passive, replication that most computer users are familiar with. State machine replication generally tolerates under a third of "malicious" nodes[150] but is limited in scalability in terms of numbers of nodes.[151]

The bitcoin blockchain employs a different technique to ensure distributed consensus. Although not explicit in his white paper, an archived email connects the bitcoin "proof-of-

[146] Low and Teo, above n. 31 at p. 240.
[147] C. M. Rose, "Crystals and Mud in Property Law" (1988) 40 Stan L Rev 577. See also H. E. Smith, "Rose's Human Nature of Property" (2011) 19 Wm. & Mary Bill. Rts. J. 1047.
[148] Land Registration Act 2002, Sch 4, paras 1 and 2.
[149] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem" (1982) 4 ACM Transactions on Programming Languages and Systems 382.
[150] Above n. 149, at 384-387.
[151] M. Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of Work vs. BFT Replication," in: J. Camenisch and D. Kesdoğan (eds) *Open Problems in Network Security* (2016) Lecture Notes in Computer Science, vol 9591 (New York: Springer, 2016).

work" algorithm to the problem of Byzantine failure.[152] The "proof-of-work" consensus greatly enhances scalability in terms of the number of nodes that a network can accommodate but it is notoriously energy intensive and arguably environmentally unsustainable.[153] It also does not offer the same consensus finality afforded by state machine replication.[154] Conventional wisdom suggests that the "proof-of-work" protocol is resistant to up to 50% malicious nodes, hence the popular references to what is called the 51% attack. This is because the bitcoin blockchain code favours the longest blockchain. Since mining is resource intensive, short of controlling a majority of the computing power, it is extremely difficult if not impossible for malicious parties to corrupt the ledger by "undoing" earlier transactions. However, it has been demonstrated that, under certain circumstances, only 25% of nodes needs to be compromised in order to undermine "proof-of-work" blockchains.[155] Furthermore, actual instances of 51% attacks are already happening.[156] Although such attacks have primarily targeted altcoins with smaller networks, they nevertheless serve as an important cautionary tale. Permissioned blockchains where multiple nodes enjoy editing privileges are an even worse cybersecurity nightmare as each node with editing privileges is a separate and additional point of failure.[157]

Although these security flaws are concerning, the main difficulty with transposing computer science approaches to security onto those of property law is one of incompatible perspectives. In designing distributed computer systems, computer scientists generally focus on network security. However, the weakest link in any computer network is invariably the end user rather than the network hardware or software. Whilst securing the machines rather than their human users may be the best that computer scientists can do, such an approach is wholly inadequate as a matter of property law to support a transition to unqualified dynamic security. Transfers on a blockchain are initiated by the use of private keys, which act like passwords when accessing the blockchain-based accounts identified by public keys. Whilst asymmetric key cryptography, which underlies the private-public key pair, is extremely secure when it comes to ensuring the integrity and secrecy of communications, it cannot determine that the private key was used by its rightful holder – a point recently emphasised by the Law Commission.[158] There is an undisputable, mathematical link between the private and public key, but there is no similar link between a private key and its user.[159] End users must maintain a delicate balance between maintaining absolute secrecy of one's private key and simultaneously ensuring that it has sufficient backups in case a copy of the key is inadvertently

---

[152] https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html (accessed 6 December 2018).
[153] de Vries, above n. 32. Cf. J. Becker et al, "Can We Afford Integrity by Proof-of-Work? Scenarios Inspired by the Bitcoin Currency" in R. Böhme (ed), *The Economics of Information Security and Privacy* (New York: Springer, 2013) at p. 135.
[154] See text accompanying nn. 64-66.
[155] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable" in N. Christin and R. Safavi-Naini (eds), *Financial Cryptography and Data Security – 18th International Conference, FC 2014* (2014) at p. 436.
[156] A. Hertig, "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular", *Coindesk* (8 June 2018) at https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/; J. I. Wong, "Every cryptocurrency's nightmare scenario is happening to Bitcoin Gold", *Quartz* (24 May 2018) at https://qz.com/1287701/bitcoin-golds-51-attack-is-every-cryptocurrencys-nightmare-scenario/. (both accessed 6 December 2018).
[157] See text accompanying n. 61.
[158] Above n. 50 at p. 16.
[159] C. Ellison and B. Schneier, "Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure" (2000) 16 *Computer Security Journal* 1 at p. 2. See also S. Mason and T. S. Reiniger, "'Trust' Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?" (2015) 21(5) C.T.L.R. 135, deliberately referencing the famous *New Yorker* cartoon by Peter Steiner with the caption, "On the Internet, nobody knows you're a dog" (5 July 1993).

lost.[160] If the private key is stored on a device connected to the Internet, it can be hacked like any computing device. Blockchain trustlessness provides "*zero* protection from … hacking, which is not only possible but commonplace."[161] "Online lists curated by bitcoin community members suggest bitcoin exchanges have been involved in up to 60 high-profile hacking incidents since the digital asset class was created in 2009. The true scale of the hacking problem, however, is hard to estimate".[162] Although most high profile hacks have been directed at exchanges, individuals have also been targeted.[163] What is the point of securing the network if the end users are left exposed? "Only amateurs attack machines; professionals target people".[164] The risks of hacking have resulted in the practice of keeping private keys in so-called cold wallets, which are media, including paper, unconnected to the Internet. However, this trades off convenience for security. Such keys can also be "stolen" if they are gleaned by dishonest strangers.[165] Good old-fashioned violence will also do the trick.[166] To the extent that any blockchain anticipates the use of smart contracts, the coding vulnerabilities of such "contracts" could expose asset holders to the sort of hack that gripped the crypto-community when the DAO was hacked.[167] Given that the vast majority of land title frauds today target the end user rather than the registry,[168] the implementation of blockchain technology for traditional asset registries is unlikely to reduce incidences of fraud, especially considering the poor cybersecurity practices of the average computer user.[169] Moreover, the elderly are likely to be disproportionately exposed to such frauds.[170] It is notable that a leading security technologist has recently declared that "[t]here's no good reason to trust blockchain technology".[171]

C. Essential "Centralisation"?

One common refrain among enthusiasts advocating blockchain asset registries is that decentralisation will speed up certain transactions by eliminating intermediaries and

---

[160] Cf. R. Armstrong, "Cryptocurrency exchange boss's death locks away $150m in digital assets", *Financial Times* (6 February 2019), detailing the loss of US$150m worth of crypto-assets following the alleged death of QuadrigaCX founder, Gerald Cotten, supposedly the only person who could access the private keys to several cold wallets. But see C. Stokel-Walker, "The QuadrigaCX Crypto Mystery Deepens as Wallets Turn up Empty", *Wired UK* (4 March 2019).

[161] Low and Teo, above n. 82, at p. 236.

[162] I. Kaminska "Bitcoin Bitfinex exchange hacked: the unanswered questions", *Financial Times* (4 August 2016).

[163] N. Popper, "Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency", *The New York Times* (21 August 2017).

[164] B. Schneier, "Semantic Attacks: The Third Wave of Network Attacks", *Crypto-Gram* (15 October 2000) at https://www.schneier.com/crypto-gram/archives/2000/1015.html#1. See also M. Evans, et al, "Human behaviour as an aspect of cybersecurity assurance" (2016) 9 *Security and Communications Networks* 4667; C. Ellison and B. Schneier, above n. 159, at p. 4.

[165] L. Coleman, "Researcher has bitcoin stolen off his back in a public experiment", *Crypto Coins News* (11 November 2015) at https://www.ccn.com/researcher-bitcoin-stolen-off-back-public-experiment/ (accessed 6 December 2018).

[166] N. Popper, "Bitcoin Thieves Threaten Real Violence for Virtual Currencies", *The New York Times* (18 February 2018).

[167] See text accompanying nn. 229-233.

[168] Joint Law Society and HM Land Registry Note, *Property and Title Fraud* (September 2017).

[169] See, e.g., A. Das et al, "The Tangled Web of Password Reuse" in *NDSS 2014* at http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2017/09/06_1_1.pdf; J. Hong, "The State of Phishing Attacks" (2012) 55 *Communications of the ACM* 74.

[170] Low and Teo, above n. 82, at p. 242, drawing on the broader Internet experience for the elderly, for which see E. L. Carlson, "Phishing for Elderly Victims: As the Elderly Migrate to the Internet Fraudulent Schemes Targeting them Follow" (2007) 14 *The Elder Law Journal* 423, at pp. 424, 428-9.

[171] B. Schneier, "There's No Good Reason to Trust Blockchain Technology", *Wired* (6 February 2019).

simplifying clearing and settlement.[172] It is not obvious, however, that speed is necessarily desirable for certain transactions. Conveyancing is, in many jurisdictions, a multi-stage transaction mired in formality. This can make it appear outmoded and unnecessarily complicated. Yet, on closer examination, such formalities, to the extent that they are slowing down the transaction, may be serving their intended function. Many jurisdictions require contracts relating to transfers or other dealings in land to take on written form because the formal documentation serves a cautionary function.[173] This in turn is justified because transactions relating to land are likely to be by far the most financially significant transactions that most people will undertake in their lifetime. The time taken between contract and conveyance also facilitates fraud detection.[174]

It may be that improving the speed of transactions is more desirable in financial markets but does the use of a blockchain per se permit the elimination of intermediaries and the simplification of the processes of clearing and settlement? Although this is widely assumed to be the case among blockchain enthusiasts,[175] it is only partially true. According to Geva, "[i]n its narrow sense, 'clearing system' is a mechanism for the calculation of mutual positions within a group of participants ('counterparties') with a view to facilitate the settlement of their mutual obligations on a net basis. In its broad sense, the term further encompasses the settlement of the obligations, that is the completion of payment discharging them."[176] Where the subject of intermediation is securities, disintermediation through the use of blockchain technology should not be too difficult,[177] particularly in jurisdictions like the UK, where intermediation is not mandatory to begin with.[178] Since one of the main advantages of intermediation was "the ease of trading and settlement",[179] provided relevant legislation is passed, the use of a blockchain could in theory provide similar ease of trading and settlement without the need for intermediation. However, intermediation in securities ownership became widespread not merely because they enabled faster transacting, but also because intermediaries offered other services "such as record keeping, investment management services and the provision of finance."[180] Considering that crypto-assets are native to decentralised blockchains, the proliferation of crypto-asset exchanges suggests that there is a commercial demand for intermediation that blockchains will not eliminate and a proposal for scaling bitcoin, the Lightning Network,[181] bears an eerie resemblance to clearing and settlement.[182]

---

[172] See, eg, Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry" (2016) 2 *Financial Innovation* 24.

[173] P. Critchley, "Taking Formalities Seriously" in S. Bright and J. Dewar (eds), *Land Law: Themes and Perspectives* (Oxford: Oxford University Press, 1998) 507. For a more general discussion of the functions of formalities, see Lon L Fuller, "Consideration and Form" [1941] 41 Columbia L Rev 799. Also see T. G. Youdan, "Formalities for Trusts of Land, and the Doctrine of *Rochefoucauld v Boustead*" [1984] C.L.J. 306;

[174] Joint Law Society and HM Land Registry Note, *Property and Title Fraud* (September 2017).

[175] Cf. Australian Stock Exchange, "CHESS Replacement: New Scope and Implementation Plan Consultation Paper", above n 75, at p. 6.

[176] B. Geva, "The Clearing House Arrangement" (1991) 19 Can. Bus. L. J. 138.

[177] Cf. House of Commons Treasury Committee, 22nd Report of Session 2017-19, Crypto-Assets (12 September 2018) at p. 13.

[178] L. Gullifer, "Ownership of Securities: The Problem Caused by Intermediation" in L. Gullifer and J. Payne (eds), *Intermediated Securities: Legal Problems and Practical Issues* (Oxford: Hart Publishing, 2010) 1 at p. 2.

[179] Above n. 178 at p. 3.

[180] Above n. 178 at pp. 3-4.

[181] J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments" (Draft Version 0.5.9.2, 14 January 2016) at https://lightning.network/lightning-network-paper.pdf (accessed 1 March 2019).

[182] R. Auer, "BIS Working Papers No 765: Beyond the Doomsday Economics of "Proof-of-Work" in Cryptocurrencies" (January 2019) at pp. 20-21, available at https://www.bis.org/publ/work765.pdf (accessed 1 March 2019). Also see S. Coppola, "The Fat Controller of the Lightning Network", Blog Post (17 January 2018)

Securities are, moreover, the easy case for a blockchain asset registry because a single issue of securities is essentially fungible.[183] This is not the case where derivatives trading or inter-bank money "transfers" are concerned. It is convenient to use the example of inter-bank money "transfers" since it is the very example used by Nakamoto to illustrate the means by which blockchain technology can facilitate money transfers through disintermediation. Nakamoto misunderstands the role of financial institutions in inter-bank payment systems. The central problem, according to him, is double-spending and the role of these financial institutions is to serve as a trusted third party to ensure that no double spending occurs. Accordingly, if the same function can be performed by an algorithm, these trusted third parties can be disintermediated. He predicted that this would lower transaction costs because the presence of these intermediaries makes it impossible for "[c]ompletely non-reversible transactions … since financial institutions cannot avoid mediating disputes."[184] If this is correct, then we could simply apply the blockchain technology to the banking industry and achieve Nakamoto's objectives without the need to create a crypto-asset such as bitcoin. In short, continue dealing in the same fundamental asset – fiat money – but keep records using the blockchain. The problem with this view, apart from its misprediction as to fees,[185] is that it misunderstands how an inter-bank money "transfer" works and the nature of the trust a depositor invests in his bank when he deposits money with it. By depositing his money, a depositor is effectively lending it to the bank,[186] who is free to deal with it as it wishes. The trust inherent in the process lies in the depositor's belief in the bank's creditworthiness and predates inter-bank transfers. What we call an inter-bank money "transfer" is far more complicated than most technologists appreciate. If bank money is simply a debt owing by a bank, then it must be obvious that an *inter*-bank money transfer cannot possibly involve the transfer of a fundamentally fungible asset since a debt is only as valuable as the creditworthiness of its debtor. In fact, there is no "transfer" of any property, only a transfer of value.[187]

Bank "intermediaries" are essential to the process of such transfers. This is demonstrated by examining what happens with an "in-house" money transfer where both payer and payee have accounts at the same bank.[188] Here, the bank simultaneously reduces its liability to one customer (the payer) and increases its liability to another (the payee). It can do so not because it helps solve a double-spending problem but because it is a common obligor to both payer and payee. Where there is an *inter*-bank money transfer, the absence of a single common obligor complicates matters. For inter-bank money transfers within a single jurisdiction of the fiat currency of that jurisdiction, this complication is typically resolved by the banks' relationship to the central bank. The central bank serves as the common obligor to the payer's bank and the payee's bank, thus allowing the adjustment of accounts across all four relationships: (i) between the payer and the payee; (ii) between the payer's bank and the central bank; (iii) between the payee's bank and the central bank; and (iv) between the payee and the

---

at http://www.coppolacomment.com/2018/01/lightning-and-fat-controller.html (accessed 1 March 2019); I. Kaminska, "BIS trolls bitcoin", *FT Alphaville* (23 January 2019).

[183] R. Goode, "Are Intangible Assets Fungible?" [2003] LMCLQ 379.

[184] Above n. 2 at p. 1.

[185] I. Kaminska, "But, but… I thought Bitcoin was supposed to be cheap?", *FT Alphaville* (17 March 2017).

[186] Above n. 83.

[187] See text accompanying nn. 106-110.

[188] R. Cranston et al, *Principles of Banking Law*, 3rd ed (Oxford: Oxford University Press, 2017) at p. 339. For the civilian position, see Cf. B. Geva, "The Order to Pay Money in Medieval Continental Europe" in D. Fox and W. Ernst (eds), *Money in the Western Legal Tradition: Middle Ages to Bretton Woods* (Oxford: Oxford University Press, 2016), 409.

payee's bank. The role played by the central bank may sometimes be taken by a correspondent bank where the transfer crosses borders and/or is made in a foreign currency. There may also be multiple correspondent banks involved if the payer's bank and the payee's bank do not share a banking relationship with a single bank so multiple banks must be used to bridge their accounts. Such payments are the source of the most chagrin among bank customers, but they are slow and expensive because multiple banks are involved and thus many more accounts need to be settled before a transfer can be finalised. To apply blockchain technology without fundamentally changing the nature of banking and inter-bank money transfer would therefore entail the creation of not one blockchain ledger but hundreds of thousands of inter-linked sub-ledgers,[189] which, if they utilise different blockchains, create problems of interoperability.

D. Forks in Chains: Stumbling Blocks?

All distributed ledgers, whether they employ blockchains or not, have the potential to fork (i.e. develop inconsistencies). Network failures can leave some nodes unconnected to other nodes. This is a problem for any distributed asset registry as one of the functions of a register is to allow the public to determine who they should be dealing with in relation to a particular asset. Such network failures cannot be wholly precluded and inconsistent records will be exacerbated by the use of "proof-of-work" blockchains, which occasionally fork randomly even in the absence of network failure.[190] Such temporary random forks are arguably inconsequential where the particular asset is not constantly traded, such as land, where the time between transactions tends to be measured in years rather than milliseconds. In that time, any prior transaction to a particular plot of land would have been buried under hundreds of blocks and any temporary aberrant fork long abandoned. However, it is less difficult to ignore for asset classes which are actively traded on a consistent basis such as securities. To the extent that some blockchain enthusiasts see the blockchain as accelerating even land transactions, such random forks necessarily take on a more problematic manifestation.

However, even worse than these random temporary inconsistencies are the more lasting hard forks[191] (i.e. incompatible revisions) of the blockchain code, which though less common, have occurred with disturbing frequency. The Ethereum blockchain famously forked permanently into Ethereum (ETH) and Ethereum classic (ETC) in 2016 when a hard fork of its code was adopted by a majority of nodes to reverse a hack[192] but a minority persisted in running the "classic" code. Bitcoin forked into bitcoin (BTC) and bitcoin cash (BCH) in 2017 over ideological differences, before forking again into bitcoin gold (BTG) in the same year, and forking and merging with ZClassic, itself a fork of an altcoin, ZCash, to form bitcoin private (BTCP) in 2018. Most recently, in November 2018, bitcoin cash further forked into bitcoin ABC (BCH ABC) and bitcoin SV (BSV). Such forks can have dramatic negative economic consequences, as the recent fork of bitcoin cash demonstrated.[193] Compared to forks of asset registries of real world off-chain assets, however, such consequences are trivial as there is no need to match forked registers to real world assets – a fork in a blockchain land registry does not create a duplicate Blackacre Classic. The solution to the problem of forks is not obvious. Taking the Ethereum hard fork as an example, it is not obvious that the choice of a majority of users to adopt the revised code should prevail over that of the minority. The majority users' decision to do so was obviously self-serving in that they wished to regain control over assets

[189] Cf. M. Arnold, "Swift says blockchain not ready for mainstream use", *Financial Times* (8 March 2018).
[190] See text accompanying nn 65-67.
[191] On forks more generally, see Low and Teo, above n. 31, at pp. 259-264.
[192] See text accompanying nn. 213-217.
[193] J. Kelly, "Bitcoin's repeated splits undermine its long-term value", *Financial Times* (19 November 2018).

which they lost. Yet in doing so, some perfectly legitimate transactions were simultaneously undone, with the consequence that some innocent parties may have suffered losses which was not compensated. But if the solution is not to be found in majoritarian decision-making, then on what basis should the law resolve such forks? As was the case with resolving the question of the finality of a blockchain register in the face of an unauthorised transfer,[194] no legislation supposedly facilitating blockchain asset registries have provided any clues as to how this problem may be resolved. Instead, lawmakers who clearly do not understand the technology present such legislation on the basis that the blockchain is merely an iterative rather than revolutionary form of registry. However, it is simply not true that the use of blockchain registers, "is from a technological point of view a new type of dematerialized security, but one that legally has attached to it the same rights as conventional dematerialized securities",[195] as Luxembourg's lawmakers suggest. The use of the blockchain technology creates fundamentally different problems which the existing law has no solutions for.

IV. "SMART" "CONTRACTS"

"The first thing we do, let's kill all the lawyers."[196] While crypto-enthusiasts have yet to incite murder, there have been many claims of the impending disruption of the legal profession[197] – a "disruption" premised on the idea that "smart contracts" eliminate the need to trust the other transacting party or to rely on traditional legal institutions, such as lawyers and courts. Purportedly, "smart contracts" guarantee performance of the contractual obligations embedded therein, eliminating disputes and dispensing with lawyers and courts. While "smart contracts" may be an interesting tool that some lawyers may wish to familiarise themselves with, the prophecies of widespread unemployment of lawyers stem from a poor understanding of both "smart contracts" as a technical concept as well as how legal contracts support commerce.

A. Maybe Contracts?

At a technical level, smart contracts are self-executing ledger-modification instructions, e.g. "if X occurs, send Y amount of tokens from account A to account B." Attempts at analysing the term from a legal (or technical) perspective are, however, rendered difficult by the existence of a multitude of inconsistent definitions.[198] Although the original definition of "smart contracts" associates them with the embedding of legal terms in hardware and software to prevent breach or to control assets by digital means,[199] the term has evolved to include many unrelated concepts,[200] ranging from ERC20 tokens, Hyperledger Fabric's ChainCode[201] to "stateful

[194] See text accompanying 121-171.
[195] Above, n. 75.
[196] William Shakespeare, *Henry VI, Part 2* (1591), Act IV, Scene 2.
[197] S. Ozelli, "Smart Contracts Are Taking Over Functions of Lawyers: Expert Blog", *Cointelegraph* (12 January 2018) at https://cointelegraph.com/news/smart-contracts-are-taking-over-functions-of-lawyers-expert-blog (accessed 6 December 2018).
[198] V. Buterin, 'Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform' (2015) (https://github.com/ethereum/wiki/wiki/White-Paper); F. Zhang, et al., 'Town Crier: An Authenticated Data Feed for Smart Contracts' (2016) Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security 270.
[199] N. Szabo, "Smart Contracts: Formalizing and Securing Relationships on Public Networks" (1997) 2 (9) *First Monday*; for a broader review of smart contracts see: E. Mik, "Smart Contracts: Terminology, Technical Limitations and Real-World Complexity" (2017) 9 L.I.T. 269.
[200] See text accompanying nn 18-23.
[201] Hyperledger Architecture, Volume II, Smart Contracts (April 2018) p. 8 https://www.hyperledger.org/wp/content/uploads/2018/04/Hyperledger_Arch_WG_Paper_2_SmartContracts.pdf (last accessed 6 December 2018)

executable objects" hosted on a blockchain[202] or "programs that can be deployed and run on a blockchain."[203] While the original definition positions "smart contracts" firmly within the legal arena and assumes that they will affect legal relations, many of the newer definitions regard "smart contracts" as purely technological phenomena, virtually synonymous with Distributed Applications on the Ethereum blockchain.[204] Consequently, it is illogical to inquire whether smart contracts are enforceable in general because each "smart contract" is different and some "smart contracts" have no legal implications whatsoever. Absent a common understanding what "smart contracts" are, legal scholarship struggles to form a cohesive argument, particularly when attempting to distinguish them from other "digital," "electronic", or "online" agreements. In principle, "smart contracts" are not contracts in the legal sense although nothing stands in the way of them having legal effects. In law, a "contract" is a concept that refers to an agreement between two or more parties or to the embodiment of such agreement, usually taking the form of a document containing writing. In contrast, technical writings refer to "smart contracts" as entities or a particular type of technology. It is common, for example, to encounter sentences where "smart contracts" *do, receive* or *communicate with* something.

Setting aside those instances where the term is used in a strictly technical sense, the common misconception that "smart contracts" have the potential to disrupt the legal system derives from both the confusion in terminology and the assumption that the technical characteristics of blockchains, decentralisation and trustlessness in particular, somehow render traditional legal institutions redundant. The key term in the "smart contract" narrative is "self-enforcement". Purportedly, instead of being enforced by tradition legal institutions, "smart contracts" can self-enforce "on" or be enforced "by" a blockchain, thus "strengthening promissory obligations without state involvement."[205] Unfortunately, the meaning of self-enforcement remains unclear as it seems to conflate two distinct stages in the life of a contract: performance and adjudication – a conflation built on top of the confusion between "rights" and "records".[206] The blockchain supposedly executes the "smart contract" in an unbiased and unstoppable manner. Its performance is guaranteed as neither of the parties can change their mind and refuse to perform. The execution of the code is thus synonymous with the performance of the obligation embodied therein. If performance is guaranteed, however, enforcement should not be required – assuming that "enforcement" refers to the ability to seek judicial assistance in the event of breach. Performance and enforcement are mutually exclusive. The assistance of the courts is only required if "things go wrong" – and "smart contracts" purportedly prevent things from going wrong. Upon closer analysis, most "smart contracts" are simply technological tools for automating the performance of certain obligations rather than a source of obligations.[207] To complicate matters, it has also sometimes been claimed that while "smart contracts" eliminate the need for judicial enforcement, the parties retain the option to do so.[208] The underlying reasoning is that although legal enforcement is unnecessary, it should remain possible. This approach seeks to reconcile the indiscriminate trust in technology with the practical recognition that, for "smart contracts" to gain commercial acceptance, it helps that they are legally enforceable.

---

[202] I. Nikolic et al., "Finding the Greedy, Prodigal, and Suicidal Contracts at Scale" (2018) https://arxiv.org/pdf/1802.06038.pdf (accessed 6 December 2018).
[203] Above, n. 28 at 1.
[204] For an overview of Distributed Applications , see: https://www.stateofthedapps.com (accessed 6 December 2018).
[205] Above n. 34 at p. 357.
[206] See text accompanying nn. 74-195.
[207] J. Cieplak, S. Leefatt, "Smart Contracts: A Smart Way To Automate Performance" (2017) 1 Geo. L. Tech. Rev. 417.
[208] Above n. 34 at pp. 355, 356

As a matter of contract law, there are no legal obstacles to representing contractual obligations in code or to automating certain aspects of formation or performance. The prerequisites of enforceability for common law systems can be reduced to the idea of an agreement intended to be legally binding in which promises are supported by consideration.[209] It is trite law that agreement can be expressed in any manner.[210] A contract can be formed orally or by conduct, it can be expressed in words (either spoken or written) or in computer instructions. At least theoretically, there are no obstacles to an agreement being manifested in code in its entirety. Moreover, it is also possible to express intention by means of automated processes. This has been expressly recognised by the common law since at least 1970[211] and is also true of civilian systems.[212] Nor, as vending machines and algorithmic trading demonstrate, is automated performance legally problematic, except where automation fails due to technical problems. [213] Indeed, the automation of aspects of formation and/or performance of standardised, mass-market contracts has been gaining in popularity since the mainstream adoption of computers and the development of the Internet - well before blockchains existed.

There are also no legal obstacles with regards to consideration so far as common law systems are concerned.[214] Consideration need not be adequate, it only needs to be sufficient in the eyes of the law.[215] The focus is on reciprocity, not on equivalence of value. [216] The parties can exchange money in return for goods or services, or bitcoins[217] in return for a music download. One must be careful, however, not to equate "smart contracts" with transactions in the technical sense within the blockchain environment. The latter are unilateral acts,[218] though in a "smart contract", consideration will often take the form of such transactions, i.e. transfers of crypto-assets from one account to another. The law in most legal systems is thus no obstacle to "smart contracts" and no legal reform is necessary in order to "encourage" their adoption. It is simple naiveté and wishful thinking that has seen the inflated promise of "smart contracts" outstrip commercial adoption. If anything, the most pressing legal reform lies in identifying

[209] H. Beale (gen. ed.) *Chitty on Contracts*, 32nd edn (Oxford: Sweet & Maxwell, 2015) at paras. 1-016, 2-001.
[210] Above n. 196 at para. 4-001, J. Beatson, A. Burrows, J. Cartwright, *Anson's Law of Contract*, 29th ed. (Oxford: Oxford University Press, 2010) at p. 75.
[211] *Thornton v Shoe Lane Parking Ltd* [1971] 2 QB 163.
[212] M. Gimmy, *Vertragsschluss im Internet*, in D. Kroeger and M. Gimmy (eds), *Handbuch zum Internetrecht* (Berlin: Springer, 2000) at p. 86.
[213] Consider the 2010 flash crash that is widely considered to have been exacerbated by high frequency algorithmic trading: see the Joint Report of the Commodity Futures Trading Commission and Securities Exchange Commission, "Findings Regarding the Market Events of May 6, 2010" (30 September 2010) at https://www.sec.gov/news/studies/2010/marketevents-report.pdf (accessed 1 March 2019). For a popular account, see M. Lewis, *Flash Boys: A Wall Street Revolt* (New York: W. W. Norton & Company, 2014). See also C. Clearfield and J.O. Weatherall, "Why the Flash Crash Really Matters", *Nautilus* (23 April 2015). Consider also the spectacular failure of algorithmic automation that contributed to the fatal crashes of Lion Air Flight 610 and Ethiopian Airlines Flight 302 and the grounding of Boeing 737 Max jets worldwide: J. Nicas, N. Kitroeff, D. Gelles and J. Glanz, "Boeing Built Deadly Assumptions Into 737 Max, Blind to a Late Design Change", *The New York Times* (1 June 2019). See also M. Minasi, *The Software Conspiracy* (New York: McGraw-Hill, 2000), at pp. 43-44, describing the bug that led to the crash of Korean Airlines Flight 801 on 6 August 1997, again involving Boeing, and at pp. 23-24, describing the infamous GM litigation involving a bug that affected the fuel injector of the Chevrolet 2500 pickup truck. For the judgment in the latter case, see *General Motors v Johnston*, 592 So 2d 1054, 1992 (Supreme Court of Alabama).
[214] For the civil law equivalent, see M. Chen-Wishart, "Consideration and Serious Intention" [2009] Sing JLS 434 at 453-455.
[215] *Chappell & Co. Ltd. v. Nestle Co. Ltd.* [1960] A.C. 87 (H.L.); *Bainbridge v Firmstone* [1960] AC 87.
[216] *Currie v Misa* (1875) LR 10 Ex 153.
[217] Bearing in mind its controversial status as a currency: see above n. 31.
[218] See text accompanying nn. 45-46.

the appropriate legal solution to algorithmic failures when "smart contracts," whether embedded on blockchains or not, are deployed.

B. Guaranteeing Performance?

The main selling point of "smart contracts" is their purported ability to reduce transaction costs by eliminating the need to trust the other transacting party by technologically precluding the possibility of breach. Code is final, deterministic and impartial, and hence superior to humans, who are indecisive, unpredictable, and biased. Once a "smart contract" is set in motion upon a blockchain – its code cannot be changed[219] and its execution cannot be stopped. Performance is guaranteed because any subsequent human interference is impossible. Alas, this both overestimates the technical capabilities of "smart contracts" and underestimates the difficulties of the contracting process.

First, the blockchain narrative often fails to distinguish between the code of the blockchain and the code of "smart contracts." As indicated, applications running "on top of" or connecting to the blockchain do not share its characteristics. Thus, "smart contracts" running on blockchains are not even trustless to the limited extent that the blockchains may be.[220] As "smart contracts" may control the transfer of crypto-assets and tokens, a coder tasked with writing a "smart contract" has an economic incentive to intentionally include "errors," such as "backdoors," designed to steal such assets. To the extent that consensus algorithms, such as "proof of work," may curb incentives to behave selfishly,[221] they are irrelevant to the coding of "smart contracts" since the latter are created off-chain before being deployed on the blockchain. The open source character of "smart contracts" is generally irrelevant as it is impossible to establish how they will operate without subjecting them to extensive testing. The ability to inspect the code cannot guarantee its quality. Moreover, as most parties will likely lack the expertise to evaluate the viability of a particular "smart contract," they will have to rely on external security audits.[222] In effect, in order to trust the code of a "smart contract", the parties will have to trust its coder(s) and/or its auditor(s). It is also notable that "smart contracts," as a technological innovation, predate the blockchain.[223] What the blockchain adds to "smart contracts" is that it ensures the integrity of their code and guarantees their decentralised and hence secure execution. Once activated on the blockchain, the "smart contract" becomes immutable to the same extent as their host blockchain.[224] While blockchain-based "smart contracts" can achieve the same limited immutability as blockchains, it should not be assumed that immutability is necessarily desirable.[225] The inability to alter the code of the "smart contract" will prevent the correction of errors or the introduction of new functionality that reflect changed commercial circumstances.

---

[219] See text accompanying nn. 56-69; but see B. Marino, A. Juels, "Setting standards for altering and undoing smart contracts" in A. J. Bertossi et al (eds) *Rule Technologies. Research, Tools, and Applications,* Lecture Notes in Computer Science, vol 9718 (New York: Springer, 2016).

[220] See text accompanying nn. 34-38.

[221] See text accompanying nn. 28-33.

[222] N. Atzei, M. Bartoletti, and T. Cimoli, "A Survey of Attacks on Ethereum Smart Contracts (SoK)," in M. Maffei and M. Ryan (eds), *Proceedings of the 6th International Conference on Principles of Security and Trust - Volume 10204* (New York: Springer, 2017) at pp.6, 10, 11; K. Bhargavan,et al., "Formal Verification of Smart Contracts: Short Paper," in T. Murray and D. Stefan (eds), *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis* (New York: NY ACM, 2016) at p. 91.

[223] Szabo, above n. 186.

[224] See text accompanying nn. 67-69.

[225] See text accompanying nn. 245-254. Cf. *Arnold v Britton* [2015] UKSC 36; [2015] 2 W.L.R. 1593. See also S. Blandy, S. Bright, and S. Nield, "The Dynamics of Enduring Property Relationships in Land" (2018) 81 M.L.R. 85.

Secondly, apart from the transfer of native, on-chain crypto-assets, common sense dictates that few contractual obligations can be automated or enforced "by" a smart contract. Logically, the "smart contract" will not move trucks or build houses. In practice, mainly payment obligations can be automated.[226] "Smart contracts" are often seen as perfect vehicles for the automation of interest rate swaps or other derivatives as the latter can be expressed in numbers and formulae.[227] In this context, legal scholars and practitioners often debate the relationship between the code of the "smart contract" and its accompanying legal agreement, if any.[228] The assumption is that in most circumstances "smart contracts" cannot exist "on their own" but require an underlying, traditional legal agreement that constitutes the source of obligations. In such an event, however, there is always a risk that the code of the "smart contract" diverges from the original obligation, usually due to a failure to correctly convert natural language into code, be it due to the incompetence of the coder or due to the inherent difficulty of translating legal obligations into a series of if-then statements. In the event of such divergence, it becomes necessary to agree on which "version" prevails. In most circumstances, the contracting parties would have negotiated an agreement in a natural language before translating it into code – not vice versa.

This does not, however, prevent blockchain enthusiasts from agreeing that the code comprises the entire agreement in a manner not unlike an "entire contracts clause", as happened in the most infamous of "smart contracts", the DAO (or Decentralised Autonomous Organisation). The DAO was set up as an investment fund on the ethereum blockchain in which investment decisions would be voted upon by investors rather than left to fund managers.[229] After attracting more than US$168m worth of crypto-asset, a bug[230] in its code allowed a "hacker" to siphon off some US$50m worth of invested funds.[231] But if the "entire contracts clause" found on the DAO website[232] is to be taken seriously, then it is arguable that the "hack" was perfectly legal since it was permitted by its code and the code constituted the complete contract.[233] There are frequent references to the concept that "code is law" – a concept that has lost its original meaning (i.e. code regulates behaviour more effectively than legal rules)[234] and became a "suitcase expression" carrying different connotations depending on the context. Exceptional circumstances apart, it is generally unreasonable to expect that parties would agree to be bound by code alone – especially if they cannot "read" code and hence understand or predict how it will execute.

Thirdly, in order for a "smart contract" to perform the contract, it must have access to the means of performance, i.e. the asset to be transferred, when the contractual conditions are met. However, the only way to *guarantee* such performance at the time of contracting is to ensure that the "smart contract" has access to such assets as are necessary for performance *at the outset*. Furthermore, "smart contracts" can ensure performance only if such performance

[226] But see also text accompanying nn. 172-189.
[227] Above n. 207 at p. 420.
[228] J. Sklaroff, "Smart Contracts and the Cost of Inflexibility" (2017) 166 Univ. Penn. L. Rev. 263.
[229] C. Metz, "The Biggest Crowdfunding Project Ever – the DAO – is Kind of a Mess", *Wired* (6 June 2016).
[230] For an etymology of the word "bug", see Minasi, above n. 213 at pp. 24-26.
[231] K. Finley, "A $50 Million Hack Just Showed that the DAO was all too Human" *Wired* (18 June 2016).
[232] Although the terms have now been deleted from the DAO website, they can be found on Reddit: www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/d4cy4v0/ (accessed 6 December 2018).
[233] J. Dietz, "DAOs, Hacks and the Law" *Medium* (18 July 2016) at https://medium.com/@Swarm/daoshacks-and-the-law-eb6a33808e3e (accessed 6 December 2018).
[234] L. Lessig, *Code, Version 2.0* (New York: Basic Books, 2016).

entails the transfer of on-chain assets. No blockchain can control assets or events existing off-chain and we have seen how the concept of a perfectly authoritative blockchain ledger is arguably more dystopian than utopian.[235] Even if we buy into the rhetoric of the absolute authority of a blockchain ledger, ownership without enjoyment is futile. If I purchase a cup of coffee, I wish to drink it, not simply be recognised on some blockchain as its owner. Besides, even if we assume that off-chain assets can be tokenized, for this utopian ideal to work, we must effectively rid the world of credit. After all, to ensure perfect performance – all tokens must be "locked" by the "smart contract" upon formation and remain locked until payment. Logically, such a "solution" seems unproductive as it excludes value from the system until the "smart contract" executes.[236] Credit is neither good nor evil.[237] Properly deployed, credit can help an economy to grow,[238] but many within the crypto-community are obsessed with perfect performance at all costs, an unsurprising attitude given the origins of the blockchain.[239] In macroeconomic terms, the price of guaranteed performance may be a radically contracted economy.

Fourthly, "smart contracts" must have access to off-chain information to determine when to "self-enforce" because blockchains cannot "see", and hence validate, anything that happens off-chain. Whenever a payment is conditional upon off-chain events/performance, so-called "oracles" are required to enable "smart contracts" to function. Oracles are service providers who confirm – on the basis of external data sources – the occurrence of off-chain events.[240] Upon their verification of such event, an oracle provides its digital signature on the relevant unlocking script that controls the tokens to be transferred. While oracles solve the technical problems stemming from the "insulated" character of blockchains, they annihilate their "trustless" and "decentralised" character by delegating trust to external entities and information sources.[241] In effect, the contracting parties must not only trust the code of the "smart contract" but also the code of the oracle and the authenticity of the data it uses to confirm performance.

Finally, blockchain enthusiasts underestimate the difficulties of contract drafting, especially if it is to be undertaken exclusively or extensively in code. Most contractual disputes arise out of either unforeseen events or disagreement over the meaning of open-ended terms. Both problems are, however, difficult to avoid. Coders share the same human fallibility as contracting parties and their legal advisers – they cannot predict the future. Even when risks can be foreseen, it is not easy to agree on how to allocate them without resorting to open-ended terms.[242] However, computer code does not accommodate such messy solutions. Such commonplace legal standards as "reasonable care," "best efforts" or "good faith" are impossible to express in code and difficult to replace.[243] To the extent that they are replaceable, any loss in ambiguity would mean that greater precision is required. Greater precision,

[235] See text accompanying nn. 121-171.
[236] I. Nikolic et al., "Finding the Greedy, Prodigal, and Suicidal Contracts at Scale" (2018) https://arxiv.org/pdf/1802.06038.pdf (last accessed 1 August 2018) p 5
[237] For an anthropological account of credit as well as both the good and evil it has wrought, see D. Graeber, *Debt: The First 5,000 Years* (New York: Melville House, 2011). Cf. Sir K. Cork et al, *Report of the Review Committee on Insolvency Law and Practice* (1982) Cmnd 8558, Chapter 1, pp. 9-13.
[238] Cf. Y.N. Harari, *Sapiens: A Brief History of Humankind* (New York: HarperCollins, 2015), at pp. 305-333.
[239] See text accompanying nn. 1-11.
[240] Above n. 198, at 270.
[241] Mik, above n. 199, at p. 296.
[242] See M. P. Gergen, "The Use of Open Terms in Contract" (1992) 92 Col L Rev 997.
[243] Mik, above n. 199, at p. 294; K. E.C. Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law' (2017) 3 Engaging Science, Technology, and Society 10 at 11.

however, often comes at the price of greater complexity. In effect, the transaction costs may increase as more time will be spent negotiating every detail, drafting in precise terms, and converting the contract into computer code, which complexity also substantially increases the incidences of bugs.[244]

The difficulties of coding are also severely underrated, especially given the number of novice coders with rudimentary technical skills[245] that have been attracted by the blockchain's libertarian promises. The process of coding is highly exacting[246] as it entails formulating precise instructions that describe how to complete a particular task while anticipating all possible variations in conditions that might affect its operation.[247] In coding, there is no officious bystander to add lines of code that go without saying[248] or reinterpret code that must have gone awry.[249] Coding has been likened to "writing *War and Peace* – but with no typos."[250] Unfortunately, "[i]ndustry average experience is about 1-25 errors per 1000 lines of code for delivered software."[251] The industry average for "smart contracts" on the ethereum network, the most popular blockchain hosting "smart contracts", is dramatically worse at more than 100 bugs per 1000 lines of code.[252] Nor do bugs simply increase in number proportionally to the length of the code. Although it might be thought that code that is twice as large would contain twice as many bugs, in fact, "the density of defects – the number of defects per 1000 lines of codes – increases."[253] Simply put, doubling the number of lines of code will likely more than double the number of bugs in the code.[254]

Once the difficulties of expressing obligations in code and creating error-free code are properly understood, and the realities of commercial negotiation fully appreciated, the true impact of "smart contracts" on the legal profession can be more firmly grasped. "Smart contracts" will not solve many of the problems arising out of commercial contracts. They can only "solve" some problems by creating others. Instead of promisees having to enforce promises against promisors, promisors will have to take action to try to reverse "self-executing" performance triggered by bugs in the code or inaccurate information supplied by oracles. In most cases, "smart contracts", if at all useful, are better utilised to automate certain aspects only (i.e. specific clauses or obligations) of a contract drafted properly in natural language. The sparing use of code will limit the number of bugs and the underlying legal contract can provide a safety net for the inevitable residual bugs. The expense involved in creating such "smart clauses" also suggest that they will only be cost-effective where a standard form will eventually be used in scale, such as the automation of compensation for flight delays in order to save costs

---

[244] C. Jones, *Estimating Software Costs* (2nd Ed, New York: McGraw-Hill, 2012), at p. 450.
[245] See generally: F. Al Khalil et al., "Trust in Smart Contracts is a Process, As Well" In: Brenner M. et al. (eds) *Financial Cryptography and Data Security*, Lecture Notes in Computer Science, vol 10323 (New York: Springer, 2017).
[246] Above n. 244 at p. 444.
[247] A rudimentary exercise anyone with no coding experience can try which demonstrates the difficulties with coding can be found above, n. 230, at pp. 26-27.
[248] *Shirlaw v Southern Foundries (1926) Ltd.* [1939] 2 K.B. 206 at p. 227 (MacKinnon LJ).
[249] *Investors Compensation Scheme Ltd. v West Bromwich Building Society* [1998] 1 WLR 896 at p. 913 (Lord Hoffmann) Cf. Above n. 227 at p. 444.
[250] Above, n. 230, at p. 27.
[251] S. McConnell, *Code Complete*, 2nd Edition (Washington: Microsoft Press, 2004) at p. 521. See also Minasi, above n. 213, for a scathing critique on the software industry's attitude towards bugs.
[252] P. Vessenes. "Ethereum Contracts Are Going To Be Candy For Hackers", *Blockchain, Bitcoin and Business* (18 May 2016) at https://vessenes.com/ethereum-contracts-are-going-to-be-candy-for-hackers/ (accessed 6 December 2018).
[253] Above n. 251 at p. 652.
[254] Above n. 251, Table 27-1, at p. 652.

and grow the market for flight delay insurance,[255] rather than for bespoke contracts. Their repeated usage would test the code and the legal contract can then serve as the basis for coders to debug the "smart clause" so that performance improves over time.[256] Errors in the meantime can be dealt with outside the "smart clause" on the basis of the underlying legal agreement.

V. CONCLUSION

Crypto-enthusiasts promised us an explosive blockchain revolution in the law. Tantalised by a technology most of them failed to understand, a tremendous amount of effort has been exerted by lawmakers throughout the world towards accommodating blockchain in the law. Some of these appear to have borne fruit, as demonstrated by reforms in Wyoming and Luxembourg, but it remains to be seen whether these fruits prove more sour than sweet as they demonstrate zero acknowledgement of the technology's limitations and provide no answers to obvious challenges to the its use.[257] Others, such as those in Honduras, appear to have permanently stalled. Yet others, such as those in Sweden and Australia, either have no concrete timelines for actual operational use[258] or else face delays owing to uncertainties.[259] Despite the lack of tangible achievements,[260] more efforts continue to pour into this exercise, with the English Law Commission soon to grapple with the utterly hypothetical notion that smart contracts and blockchains will increase efficiency, trust and certainty.[261] In the face of Brexit, such a waste of legal resources seems downright barmy.[262] Comparisons to the Internet are woefully off the mark,[263] and regrettably, a detailed examination of the technology exposes both its limitations

[255] See, e.g., Axa's Fizzy https://www.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy. But note that the claims by the vendor that the platform is 100% secure should not be taken seriously and must be taken as pure puff and read in light of all the limitations enumerated in this paper. It is notable that all of this automation could have been achieved without the blockchain, just without the attendant fanfare and hyperbole and it is probably the case that there has simply been insufficient demand for such an industry to grow.

[256] Cf. above n. 244 at p. at 446.

[257] Consider Japan's experience in regulating cryptocurrency exchanges following the disastrous Mt Gox hack of 2014. On 26 January 2018, yet another Japanese cryptocurrency exchange, Coincheck, one licensed under the new regime, suffered an even worse hack, leaving Japan with the dubious honour of having suffered the two worst crypto-asset hacks in the history of the asset class. See L. Lewis and R. Harding, "'Crypto crazy' Japanese mystified by virtual heist", *Financial Times* (3 February 2018). For a legal analysis of the Tokyo District Court's decision in the Mt Gox insolvency, see Low and Wu, above n. 88, and Takahashi, above n. 88.

[258] C. Kim, "Sweden's Land Registry Demos Live Transaction on a Blockchain", *Coindesk* (15 Jun 2018) at https://www.coindesk.com/sweden-demos-live-land-registry-transaction-on-a-blockchain (accessed 1 March 2019).

[259] Reuters, "ASX delays blockchain transition by six months", *The Sydney Morning Herald* (4 September 2018).

[260] Many blockchain projects are quickly abandoned and never proceed past the pilot stage. See, e.g., in the context of international development, the devastating report by J. Burg, C. Murphy, and J.P. Pétraud, "Blockchain for International Development: Using a Learning Agenda to Address Knowledge Gaps", *MERLTech* (29 November 2018) at http://merltech.org/blockchain-for-international-development-using-a-learning-agenda-to-address-knowledge-gaps/ (accessed 6 December 2018). Cf. L. Mearian, "Blockchain: What's it good for? Absolutely nothing, report finds", *Computerworld* (5 December 2018). In 2017, Deloitte reported that only 8 percent of blockchain projects of 86,034 blockchain projects on GitHub were active, despite a relatively lenient definition of active to mean being updated at least once in the last 6 months: see J. L. Trujillo, S. Fromhart and V. Srinivas, "Evolution of Blockchain Technology: Insights from the GitHub Platform", *Deloitte Insights* at https://www2.deloitte.com/insights/us/en/industry/financial-services/evolution-of-blockchain-github-platform.html (accessed 1 March 2019).

[261] The Law Commission Annual Report 2017-18 (Law Com No 379) (19 July 2018) at 10.

[262] But it is notable that the Chancellor of the Exchequer believes that the blockchain can resolve problems with the Irish border post-Brexit: see D. McCum and J. Kelly, "Chancellor's blockchain idea is a desperate scrape of the Brexit barrel", *FT Alphaville* (2 October 2018).

[263] E-mail was widely used within a year or two of Arpanet's (a precursor of the Internet) deployment: see K. Hafner and M. Lyon, *Where Wizards Stay Up Late: The Origins of the Internet* (New York: Simon & Schuster, 1996) at pp. 160-218. Soon after the various localised networks such as Arpanet were connected to one another

and the many misunderstandings rampant among both legal and technological cryptomaniacs. Properly decrypted, the promised blockchain legal revolution appears to be a damp, and regrettably widely distributed, squib.

in the mid to late 1980s, the world wide web was soon born and proliferated rapidly: see T. Berners-Lee, *Weaving the Web: The Past, Present and Future of the World Wide Web by its Inventor* (London: Orion Business Books, 1999); J. Gillies and R. Cailliau, *How the Web was Born: The Story of the World Wide Web* (Oxford: OUP, 2000).