The future of the law is crypto? 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 the upstart Ethereum boasting smart contract functionality. Furthermore, the blockchain technology underlying Bitcoin, Ethereum and other cryptocurrencies has also attracted attention, with some within the tech community suggesting that the blockchain can solve such diverse problems as secured digital voting to tracking food provenance. So far as the law is concerned, the blockchain is envisaged as capable of revolutionizing registries for assets ranging from land to intellectual property, modernizing clearing and settlement, and even fundamentally transforming the process of contracting. This paper critically evaluates these popular claims surrounding the potential of blockchain technologies to revolutionize the legal system. It suggests that much of the hype stems from a failure of blockchain evangelists to properly understand the law or the values that almost all legal systems cherish. There is also an obsession with catchphrases such as trustless, secure, immutable and self-enforcing without clearly unpacking what they truly mean in the context of the blockchain. This paper proposes to clarify these vague and cryptic concepts and explain their implications for widespread integration of the blockchain in legal processes.

INTRODUCTION

On 1 November 2008, the world was introduced to the concept of a blockchain when Satoshi Nakamoto [1] published his seminal white paper describing a cryptographic system for "electronic cash" that he named Bitcoin.[2] The timing for the introduction of Bitcoin proved fortuitous as the world's economy was mired in the worst recession since the Great Depression

[1] The true identity of Satoshi Nakamoto has been much speculated but remains unknown. See, eg, Robert McMillan (7 March 2014), "Why Bitcoin Doesn't Want a Real Satoshi Nakamoto", Wired at https://www.wired.com/2014/03/bitcoin_satoshi/ (accessed 5 April 2017), Izabella Kaminska (7 May 2016), "Bitcoin: Identity Crisis", Financial Times, Andrew O'Hagan (30 June 2016), "The Satoshi Affair", London Review of Books at https://www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair (accessed 5 April 2017).

[2] Satoshi Nakamoto (October 2008), "Bitcoin: A Peer-to-Peer Electronic Cash System" at https://bitcoin.org/bitcoin.pdf (accessed 5 April 2017).

and trust in governments were at a nadir. Many people, who disagreed with the policy responses of governments worldwide, in particular in relation to quantitative easing, found themselves drawn to the supposed inherent limit in supply of Bitcoin built into its blockchain code. Even so, adoption of the most conspicuous of cryptocurrencies took some time. The first real use of Bitcoin, to purchase two pizzas,[3] only took place more than a year and a half later on 22 May 2010. At 10,000 bitcoins for two pizzas, however, they did not capture the public imagination but two successive events shortly thereafter would dramatically affect bitcoin adoption. First, in July 2010, the first Bitcoin exchange, Mt Gox, was launched in Tokyo, Japan, allowing end users to purchase bitcoins using fiat currency rather than "mine" them personally. This allowed end users to obtain as many bitcoins as they wished, rather than limiting them to those that they could successfully mine, which in turn also drove up interest in bitcoin mining. Secondly, in February 2011, the Silk Road, an online black market for illicit goods and services, was launched as part of the dark web and Bitcoin's pseudonymous nature, which many end users mistook for anonymity, saw it being adopted as the currency of choice. The success of Bitcoin and Mt Gox saw other cryptocurrencies, called altcoins, and exchanges, being launched. The momentum it had gained, however, could not be sustained and the arrest of, Ross Ulbricht, otherwise known as the Dread Pirate Roberts, the mastermind behind the Silk Road and the bad publicity generated by the Mt Gox hack caused the price of Bitcoin to plummet in 2014. Although Bitcoin's price would recover and eventually scale even greater heights, it was around this time that interest began to build in the blockchain technology that underpinned Bitcoin.[4] Unsurprisingly, interest in the blockchain was drawn initially from the technology and finance industries.[5] In May 2015, *The Economist* mused upon the question of whether

[3] Nathaniel Popper, Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money (2015), 43-44.
[4] (13 March 2014), "Bitcoin's Future: Hidden Flipside", *The Economist*.
[5] Cade Metz (17 December 2015), "Tech and Banking Giants Ditch Bitcoin for Their Own Blockchain", *Wired* at https://www.wired.com/2015/12/big-tech-joins-big-banks-to-create-alternative-to-bitcoins-blockchain/

blockchains were "[t]he next big thing". Barely five months later in October, it hailed the blockchain as a "trust machine" and suggested that it "could transform how the economy works".[6] In the same issue, another article hailed it as "[t]he great chain of being sure about things".[7] By September 2018, after the meltdown in cryptocurrency prices from their new highs in late 2017, its enthusiasm was significantly more muted. The subtitle to an article titled "The promise of the blockchain technology" states, somewhat soberingly, "What blockchains may be able to do for your business, and what they can't". [8] As much of the hype about blockchains have revolved around revolutions in how the law may operate, it is timely to take a similarly sobering reality check.

TECHNICALITIES

Before exploring the substance of whether indeed the blockchain is ready to revolutionise law and commerce, it is necessary to introduce the blockchain and some concepts associated with it more fully. As we shall see, much of the hype over blockchains stem from unconsidered extrapolations of its qualities from pithy catchphrases that wildly exaggerate its capabilities. It must be suspected that the disproportionate enthusiasm surrounding blockchain technologies, which can be encountered in the popular press and in much of the early legal scholarship, is attributable to a general lack of understanding of the core terms commonly encountered in the blockchain narrative as well as to the incorrect assumption that technical terms directly translate into legal terms or, at least, carry the same legal effect.[9] Concurrently, many computer scientists, including Satoshi Nakamoto, who have limited expertise in law, economics or commerce, make not dissimilar assumptions about how legal rules work and imagine that the blockchain can therefore readily revolutionise the law. But there is a reason why the saying

[6] Leader (31 October 2015), "The Promise of the Blockchain: The Trust Machine", *The Economist*.
[7] Briefing (31 October 2015), "The Great Chain of Being Sure about Things", *The Economist*.
[8] (1 September 2018), "The Promise of the Blockchain technology", *The Economist*.
[9] Add MLR article.

that "a little knowledge is a dangerous thing"[10] has stood the test of time. Understanding the legal implications of a technology is predicated on an understanding of both of the technology's characteristics as well as an accurate appreciation of how the law actually works, not half-baked beliefs in one, the other, or worse, both. Accordingly, it is necessary to begin by demystifying a number of terms that underlie the common belief that blockchains will revolutionise law and commerce: "validation," "immutability," and "trustlessness." A crucial distinction between between permissioned and permissionless blockchains will be drawn, as will the practical implications of the fact that, stripped of the glorification, blockchains are, at their core, databases. In short, it is necessary to begin by distinguishing between lofty ideological claims as to what blockchains *will* do and what blockchains *can* actually do

Definational 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.[11] Blockchain technology is often defined as "[a]n open-source technology that supports trusted, immutable records of transactions stored in publicly accessible, decentralized, distributed, automated ledgers",[12] but it is obvious that this definition is underinclusive. Blockchain technologies have many configurations and variants and many of them are neither intended to be open-source nor publicly accessible. Ideological aspirations of participants in the blockchain sphere, such as those implicit in the foregoing definition, often serve as obstacles to rational discourse. In principle, blockchains are distributed databases, or data structures, that are maintained by a network of geographically dispersed computers, or "nodes." As its name suggests, blockchains

[10] The original expression, though not the idea, attributed to Alexander Pope, is, "A little learning is a dangerous thing": see Alexander Pope, *An Essay on Criticism* (1709), Part 1. This was misquoted as "A little knowledge is a dangerous thing" in *The Monthly Miscellany; or Gentleman and Lady's Complete Magazine, Vol II* (1774) at 35.
[11] See generally: Angela Walch, "The Path of the Blockchain Lexicon (and the Law)" (2016) 36 Review of Banking and Financial Law 713
[12] InterPARES Trust Terminology Project: Key Blockchain Terms and Definitions (2018) https://interparestrust.org/terminology/term/blockchain

are made of a chain of interconnected blocks, each block containing a list of all prior transactions. The connection between these blocks is by way of a cryptographic hash, so that alterations in earlier blocks will be readily detected by checking the cryptographic hash included in the block immediately following. Beyond this basic commonality, there are in truth many types of blockchains, equipped with varying configurations of technical features. In some contexts, it is more appropriate to speak of distributed ledger technologies, which denote a broader category of dispersed, synchronized and cryptographically secured data stores,[13] but to the extent that some distributed ledgers do not record data in interconnected chained blocks, the category of distributed technology is wider than that of blockchains properly so-called. Some blockchains have been designed for specific purposes or industries, others are generic in nature.[14] Consequently, each statement regarding blockchains *as such* should be qualified with references to a specific blockchain and each legal analysis should focus on the *type* of blockchain in question and on its intended use.

Permissioned and Permissionless Blockchains: A Key Distinction

Notwithstanding the foregoing, the bitcoin blockchain provides a useful point of reference for a discussion of other blockchains as its many of its characteristics are shared by other blockchains. It also exemplifies the main tenets of "blockchain ideology." However, we must first begin by distinguishing between permissioned and permissionless blockchains.[15] The main distinguishing criterion between the two is whether the nodes processing transactions are pre-defined or unrestricted, i.e. whether anyone can become a node or whether operating a node requires permission. Here, "node" refers to a computer running an instance of the relevant

[13] Roger Maull et al., "Distributed ledger technology: Applications and implications", Strategic Change (2017) 26(5) 481–489, at p 483.

[14] The permissioned ledger Ripplewas 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.

[15] There are blockchains that do not fall into either categorization as they constitute a hybrid model.

software that enables the participation in a given blockchain network;[16] "processing" denotes the ability to view, create, validate, and/or add transactions to the blockchain. The meaning of the term "transaction" may vary between different blockchains but, in principle, it denotes the transfer of crypto-currencies from one account to another or, more broadly, a change to the state of the blockchain.[17] Sometimes, permissioned ledgers are treated as synonymous with private and permissionless with public blockchains.[18] The said differentiations are not, however, made consistently and we prefer the distinction between permissioned and permissionless. Permissionless blockchains are restricted by their ideological underpinnings – they are *supposed* to display certain characteristics. They are supposed to be open, anonymous, decentralized and free of external interferences, or in the parlance of the blockchain community, be censorship resistant. In contrast, permissioned blockchains are more malleable and respond to actual, commercial needs. Given that the characteristics of permissioned blockchains are not fixed, each of them must be analyzed *in casu.* It is thus easier to make broader assumptions about permissionless blockchains.

Permissionless blockchains allow anyone to join the network without disclosing their identity, subscribing to any form of system rules or terms of use. The only prerequisite of participation is downloading the requisite software. In principle, all participating nodes enjoy the same degree of access to the network, including read and write privileges.[19] Permissionless blockchains typically involve a native cryptocurrency, which serves as an incentive mechanism

[16] Andreas Antonopoulos, *Mastering Bitcoin*, 2nd ed., (Sevastopol: O'Reilly 2017) p 50.

[17] J. Gray, (1981). The transaction concept: Virtues and limitations. In Proc. 7th Int. Conf. on Very Data Bases, pages 144–154. 337; C. H. Papadimitriou, (1986). The Theory of Concurrency Control. Computer Science Press. 401; J.D. Ullman (1988). Principles of Database and Knowledge Base Systems, volume 1. Computer Science Press. 300, 301, 337

[18] Lai, Roy & Lee Kuo Chuen, David, *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2* (Elsevier, 2018) at p 147. Where a distinction is made, the difference between permissioned and permissionless blockchains seems to relate to the *authorisation* of participating nodes to perform certain actions, and the difference between public and private blockchains seems to concern the *authentication* of the participants.

[19] 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.

to produce blocks.[20] They also often rely on a consensus algorithm, most commonly based on an idea called "proof-of-work."[21] The creation of each new block in the Bitcoin blockchain requires participants to solve a complex mathematical puzzle that is computationally difficult but which solution is easily verified. This process has been christened "mining" by the cryptocurrency community, an explicit metaphor to gold mining. The metaphor has been criticised as inapt[22] but the name has stuck. One of the difficulties with researching blockchain and cryptocurrencies is the proliferation of obfuscatory metaphors such as these. It is generally thought that as these computations are extremely expensive in terms of computer equipment[23] and electricity, 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 and difficulty of retrospectively changing existing blocks, the possibility of a transaction being altered or reversed is popularly believed to be infinitesimal.[24]

"Proof-of-work" then, together with the inclusion of hashes of earlier blocks in later blocks together guarantee the supposed "trustlessness" of the entire system. The reasoning is that one can trust the code alone, without having to trust a centralized entity or the individual nodes running the network. Reliance on humans and institutions is replaced with reliance on technology, the latter often being portrayed as virtually infallible, objective and impartial. So far as inter-bank money transfers are concerned, it would appear that banks do not play the role

[20] 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. As described in an authoritative book: "Mining achieves a fine balance between cost and reward. Mining uses electricity to solve a mathematical problem. A successful miner will collect a *reward* in the form of new bitcoin and transaction fees. However, the reward will only be collected if the miner has correctly validated all the transactions, to the satisfaction of the rules of *consensus*." ANDREAS ANTONOPOULOS, *Mastering Bitcoin*, 2nd ed., (Sevastopol: O'Reilly 2017) p 26.

[21] See generally: Vitalik Buterin, On Public and Private Blockchains, *August 6, 2015* blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[22] David Andolfatto (31 March 2014), "Bitcoin and Beyond: The Possibilities and Pitfalls of Virtual Currencies", *Dialogue with the Fed*, at 16-17 at https://www.stlouisfed.org/~/media/Files/PDFs/DWTF/Bitcoin-3-31-14.pdf.

[23] Bitcoin mining progressed from CPU to GPU to ASIC.

[24] Andreas M. Antonopoulos, Mastering Bitcoin, 2nd ed (Sevastopol: O'Reilly, 2015) 162. But see text accompanying nn ??.

of trusted third party often attributed to them within the blockchain community. Trust certainly exists but not in the form often assumed by cryptocurrency enthusiasts.[25] But perhaps more importantly, it is often overlooked that the technology is created by humans. To trust the code one must trust those who wrote the code and they are the few (i.e. centralized) rather than the many (i.e. decentralized).[26] Furthermore, although the popular blockchain narrative associates "trustlessness" with the ability to trust the code, from a technical perspective the term denotes the ability to confirm the truth of an event without recourse to a trusted third party in an adversarial environment where no-one can be trusted.[27] Moreover, there is a trend to assume that all code that is somehow related or associated with blockchains is trustless. As we shall see, many analyses fail to differentiate between different types of code in the blockchain ecosystem or, more specifically, fail to recognize that trustlessness only relates to the code of the blockchain itself.

Permissioned blockchains, such as Hyperledger Fabric or Corda, are an entirely different beast altogether. Such blockchains limit access and transaction processing to identified participants who subscribe to system rules.[28] The latter are virtually synonymous with "terms of use" or "master agreements," which govern who can join the system and how the system is to be used. As the participants are known and legally bound to adhere to certain rules (i.e. the relationship is governed not only by the rules encoded in the blockchain but by legally enforceable agreements), there is no emphasis on "trustlessness" and no need to rely on computationally intensive consensus algorithms. After all, there is no need to trust code if we can trust those who use the code. But the absence of "mining" means that abuse by trusted participants is more easily perpetrated. Permissioned blockchains restrict who can participate

[25] See text accompanying nn ???.
[26] Gili Vidan and Vili Lehdonvirta, "Mine the gap: Bitcoin and the maintenance of trustlessness" (2018) *New Media & Society* 1, especially 8-10.
[27] The problem is commonly referred to as the 'Byzantine Generals Problem,' see: Leslie Lampert et al., 'The Byzantine Generals Problem' 4 *ACM Transactions On Programming Languages And Systems,* 1982 at 382.
[28] David Yermack, "Corporate Governance and Blockchains" (2017) 21 Review of Finance 7 at 16..

in the consensus mechanism and/or transact on the blockchain. Permissioned blockchains also enable selective transparency, so that access to information can be limited to specific participants. Permissioned blockchains are typically intended for enterprise use and unconstrained by ideological underpinnings.

The Limits of "Validation": Blockchains' Achilles' Heel

The technical literature surrounding blockchains often mention that blockchains (or, to be more precise, their underlying consensus algorithms) "validate" transactions or other events. Unsurprisingly, legal literature has fixated on this term, possibly assuming that its technical meaning overlaps with the legal meaning – establishing compliance with the law or otherwise attesting to the veracity of a statement. It is often assumed that consent in the legal sense has been validated. It is necessary, however, to understand what validation means from a technical perspective, i.e. *what* is being validated, against what criteria, as well as *who* validates.

In the Bitcoin blockchain, the subject of validation are transactions and blocks. The entities involved in the validation process are nodes and miners. The process is completely automated and deterministic; and almost devoid of any room for human discretion or deviation. Although widely assumed to coincide with the legal concept of consent to a transaction, whether contract or transfer, there is in fact no relation between the two concepts. In the legal context, a transaction is associated with a bilateral or multilateral arrangement. In many legal and commercial contexts, this often takes the form of either a contract or property transfer. In the technical context, however, a "transaction" denotes the unilateral transfer of coins from one account to another as identified by their respective public addresses or "a signed data structure expressing a transfer of value."[29] As indicated above, from a purely technical perspective, a "transaction" constitutes a change to the state of the blockchain.[30] Whilst this is often bilateral,

[29] Andreas M. Antonopoulos, *Mastering Bitcoin, 2nd ed* (Sevastopol: O'Reilly, 2015) p 18, 19

[30] J. Gray, (1981). The transaction concept: Virtues and limitations. In Proc. 7th Int. Conf. on Very Data Bases, pages 144–154. 337; C. H. Papadimitriou, (1986). The Theory of Concurrency Control. Computer Science Press.

it can be unilateral in the legal sense when the holder of bitcoins transfers bitcoins from one public address to another public address, both belonging to him. Here, there is a "transaction" in the technical sense employed by the blockchain community but no legal transaction. The law does not generally permit a person to contract with himself, a rule that once prevented spouses from contracting with each other because the law regarded them as one and the same person.

Blocks contain lists of transactions. To be included in a block, all network nodes must confirm (i.e. "validate") that each transaction is correctly structured, uses previously unspent inputs and contains sufficient transaction fees.[31] Nodes must also confirm that the unlocking scripts match the corresponding locking scripts.[32] Once a transaction is aggregated into a block, the block itself must be verified by the mining process. Mining is related to the concept of decentralized consensus, i.e. finding a solution to the "proof-of-work" algorithm by hashing the block, changing one parameter at a time, until the resulting hash matches a specific target.[33]

401; J.D. Ullman (1988). Principles of Database and Knowledge Base Systems, volume 1. Computer Science Press. 300, 301, 337

[31] Andreas M. Antonopoulos, *Mastering Bitcoin, 2nd ed* (Sevastopol: O'Reilly, 2015) p 24, 25

[32] For a detailed description of validation criteria see Andreas M. Antonopoulos, *Mastering Bitcoin, 2nd ed* (Sevastopol: O'Reilly, 2015) p 218, 219. The full list of validation criteria for the bitcoin blockchain is as follows:

1. The transaction's syntax and data structure must be correct.
2. Neither lists of inputs or outputs are empty.
3. The transaction size in bytes is less than MAX_BLOCK_SIZE.
4. Each output value, as well as the total, must be within the allowed range of values.
5. None of the inputs have hash=0, N=–.
6. The transaction size in bytes is greater than or equal to 100.
7. The number of signature operations is less than the signature operation limit.
8. A matching transaction in the pool, or in a block in the main branch, must exist.
9. For each input, if the referenced output exists in any other transaction in the pool, the transaction must be rejected.
10. For each input, the referenced output must exist and cannot already be spent.
11. Using the referenced output transactions to get input values, each input value, as well as the sum, must be in the allowed range of values (less than 21m coins, more than 0).
12. The sum of input values must not be less than sum of output values.
13. The transaction fee must be sufficiently high to get into an empty block.
14. The unlocking scripts for each input must validate against the corresponding output locking scripts.

[33] 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 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. Andreas M. Antonopoulos, *Mastering Bitcoin*, *2nd ed* (Sevastopol: O'Reilly, 2015) p 228

Subsequently, each newly mined block is validated by every node in the mining network against certain *technical* criteria, which include establishing that its data structure is syntactically correct, the block header hash is less than the target (i.e. a solution to the "proof-of-work" algorithm has been found), the block size is within acceptable limits and all transactions within the block are valid.[34] The list of block validation criteria is extensive and, as in the case of transaction validation, illustrates the divergence between the technical and the legal understanding of the term.

The description of the validation process demonstrates that the term denotes an automated, deterministic process of confirming that certain technical requirements have been met. In the context of *transaction* validation, it concerns the fulfillment of technical parameters that relate to on-chain events, e.g. that the account has sufficient "funds" to spend and that the correct private key (or multiple private keys in case of multi-sig scripts) has been used to initiate the transaction (i.e. spend those funds). The validation process cannot, however, confirm real-world events, e.g. whether the payment was actually due, whether the parties had legal capacity, whether the contract underlying the transfer of funds was legally enforceable, or perhaps most significantly, was the private key properly used. The legal or commercial background of the payment is never and *can* never the subject of validation because the validation process cannot "look outside" the blockchain, or, 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."[35] Blockchains can only see and react to on-chain events – a simple but important point that is notoriously overlooked by legal blockchain enthusiasts. The conflation of blockchain "validation" with legal "consent" has led to such absurd projects as Legalfling,[36] an initiative to register consent to sexual relations on a

[34] Andreas M. Antonopoulos, *Mastering Bitcoin, 2nd ed* (Sevastopol: O'Reilly, 2015) p 238
[35] XU 6.
[36] https://legalfling.io/

blockchain.[37] But all that the "validation" process tells us, to focus on the validation of the private key, is that a particular person's private key was used. It cannot tell us that it was used by her (it could have been "stolen" from her and applied by her rapist), nor if it was signed off by her, can it tell us that she did so voluntarily (it could have been applied under duress). Even if she had freely signed her private key to the "transaction", it cannot tell us that she maintained her consent throughout the encounter. As the developers acknowledge, "It has limitations in case one of the parties blatantly lies."[38]

Similar misunderstandings seem to accompany the concept of "distributed" or "decentralized" consensus. The said terms seem to imply that the ability to make decisions is granted to all or most participants of a system. While this latter feature seems *prima facie* attractive as it implies the devolution of power to individual users, it is frequently forgotten that in permissionless blockchains, the decentralized peer-to-peer decision-making process, popularly referred to as "distributed consensus," refers to the automated and *deterministic* execution of an algorithm. There is no room for discretion, there are no individual choices beyond what is prescribed *or permitted* by the algorithm. Each node in the system follows the same protocol – the choices are binary: accept transactions or blocks that fulfill the prescribed criteria, reject those that do not. There is some limited choice for each node but they are almost always constrained by the ideological assumption that everyone participating is selfish and thus tends to encourage selfish behaviour. Miners who successfully solve the "proof-of-work" puzzle get to choose among the available "valid" transactions to include in their new block to add to the blockchain. Where two or more such transactions relate to the same bitcoins, or more precisely their unspent transaction output (UTXO), miners are free to choose the transaction offering the greater transaction fee even if it is the later transaction. Such behavior would be

[37] Maya Salam (2 March 2018), "Consent in the Digital Age: Can Apps Solve a Very Human Problem?", *The New York Times*.

[38] https://legalfling.io/#faq in response to the question "Does this proof consent beyond any doubt?"

decried as gazumping but for the community's defining transactions as only such transactions as appear on the blockchain. In other words, until some third party miner validates a transaction by adding it to the blockchain, it is assumed to have no legal effect. Nor, contrary to what is implied by the popular blockchain narrative, the decentralization of control does not translate in the ability to make actual decisions about the system, how it operates, whether it requires improvement or whether certain users or transactions should be excluded or prohibited except to the limited extent that participants are free to prefer to support a competing forked chain. Often, such choices are dictated as much by selfish reasons as ideological ones.[39]

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 contents recorded in the blockchain or to the code of the blockchain itself. 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, finality of payment or, in the context of smart contracts, with self-enforcement. It is noteworthy that this scenario pertains exclusively to transactions and assets that are native to the blockchain, they do not formally exist in the real world. The second situation concerns the fact that once any *other* data is inscribed into the blockchain, it cannot be changed. By such "other data" we mean any arbitrary content other than that envisaged to be recorded by the bitcoin protocol.[40] Such content ranges from the original bitcoin whitepaper, tributes to Nelson Mandela, prayers, political commentary on the second bank bailout and examples of cross-site scripting attacks to more commercially-oriented content such as information about authorship

[39] Cite DAO and bitcoin forks as free money.

[40] Interestingly, the embedding of such data in the bitcoin blockchain is achieved through a hack of the Bitcoin protocol, i.e. embedding additional content in Bitcoin addresses or creating "fake" ASCII addresses.

of IP rights or ownership of real-world assets to illicit content such as child pornography.[41] Unsurprisingly, although their original purpose was to disintermediate payments and create an independent payment mechanism, blockchains are often regarded a perfect record-keeping technology.[42] After all, everything that is inscribed in them stays there forever and cannot be changed. It is worth mentioning, however, that such "arbitrary" content refers to events or assets that are not native to the blockchain. The third instance concerns the fact that (in most public blockchains) it is impossible to change their underlying consensus algorithm or – the code of the blockchain itself. In this context, immutability may be regarded as a component or precursor of "trustlessness" and "censorship resistance."

More problematically, "immutability", it turns out, is a surprisingly mutable concept. First, not all blockchains are immutable. Permissioned blockchains may give certain participants the right to retrospectively edit the contents of a block, reverse transactions or even alter the underlying code. Second, although "immutability" implies that something cannot be changed *at all*, blockchain immutability is surprisingly mutable. Thus, most famously, the code of the two most prominent permissionless blockchains, Bitcoin and Ethereum,[43] have each been altered by means of forks.[44] Leaving aside the controversial issue of hard forks, random forks in permissionless blockchains occur all the time and it is impossible to predict which forked chain will prevail and which will be "orphaned", the community's chosen metaphor for abandoned chains. It appears then that blockchain immutability is not a binary black or white

[41] Roman Matzutt et al, "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin", Financial Cryptography and Data Security 2018 at https://fc18.ifca.ai/preproceedings/6.pdf. See also Samuel Gibbs (20 March 2018), "Child abuse imagery found within bitcoin's blockchain", *The Guardian* at https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content

[42] A. Walch, 'The Path of the Blockchain Lexicon (and the Law)' 36 Review of Banking and Financial Law,' 2016, p (713) p 735, 736.

[43] Moreover, at the time of writing Ethereum is transitioning from a proof-or-work to a proof-of-stake consensus algorithm.

[44] Bitcoin forked into 2 separate ledgers in March 2013, with one half of the network adding blocks to one version of the chain, and the other half adding to the other. For the next six hours, there were effectively two Bitcoin networks operating at the same time, each with its own version of the transaction history. Ethereum famously split into two as a result of the DAO hack to revert the ledger to its state before the hack.

concept but rather more akin to fifty shades of grey. Transactions get increasingly immutable as more blocks are added to the blockchain 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.[45] In truth, immutability never ever shades to black as the famous Bitcoin fork in 2013 demonstrates. This accidental fork, occasioned by software compatibility issues, is less well known than the hard forks of later years but six hours worth of transactions, roughly equal to 36 blocks, were removed from the Bitcoin blockchain in order to reverse the fork. In the parlance of the computer science community, such blockchains lack "consensus finality". There is consensus in the blockchain but it has the potential to shift and change so that the consensus is never truly final. Third, when speaking of blockchains as a perfect record-keeping technology, the immutability of the recorded data is incorrectly associated with its veracity and authenticity. Phrases like "uncensored truth" or "single source of truth," ignore the fact that inscribing data in a block does not guarantee its accuracy or authenticity.[46] Fourth, even if a blockchain were truly immutable in an absolute sense, it would still be possible to substantially reverse the effects of a transaction by way of a further transaction of equal value in reverse. To the extent that such a transaction may be coerced through judicial authority, the "immutability" of even native on-chain assets such as Bitcoin, may be suspect. It is not difficult to imagine that a court may be willing to order such a reversal if, for example, the "transferor's" private key had been misused by a hacker. Unless absolute security can be promised by the blockchain technology so that all entries are perfectly accurate, and it cannot,[47] "immutability" is a shortcoming, not a blessing.[48]

[45] Marko Vukolić
[46] See text accompanying nn ??.
[47] See text accompanying nn ???. Also see Chris Reed, et al., "Beyond BitCoin – Legal impurities and Off-chain Assets," (2018) 26 International Journal of Law and Information Technology 160 at 171.
[48] Richard Lumb (9 September 2016), "Downside of Bitcoin: A Ledger that Can't Be Corrected", *The New York Times* at https://www.nytimes.com/2016/09/10/business/dealbook/downside-of-virtual-currencies-a-ledger-that-cant-be-corrected.html

Blockchains as Databases

From a technical perspective, blockchains are *databases* or, as commonly stated, cryptographically secured ledgers. Traditionally, ledgers are 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 both are a particular type of database. Logically, transactions do not happen "on the pages" of ledgers and assets do not exist solely on the pages of ledgers. while ledgers can record transactions or contain information about transactions, they cannot enable or execute transactions. Exceptionally, they may appear to be able to do so where the blockchains record cryptocurrencies such as Bitcoin but that is the result of the peculiar nature of such assets rather than the blockchain itself.[49] To a large extent, the inability of the broader crypto-community to distinguish between a record and an asset can be traced to Satoshi Nakamoto's White Paper itself, which demonstrates an incorrect albeit commonplace grasp of interbank transfers of fiat money. But irrespective of the foregoing exception, it must be borne in mind that, in principle, blockchains are *only* databases. Apart from a limited number of native scripts, no code executes *within* the blockchain. Blockchains, by definition, have very limited computational capabilities. To state that a blockchain *in itself* could support a decentralized marketplace or serve as transactional platform is tantamount to stating that Amazon could be run "on" an excel spreadsheet or that the technology underlying the eBay is nothing but a giant google doc.

In reality, even a simple e-commerce website consists of a multi-tiered systems made of different types of servers, networking equipment and databases. [50] Consequently, if blockchains are to do more than "just store data" they require an extension of their

[49] Low and Teo, "Bitcoins and Other Cryptocurrencies as Property?"

[50] For a more detailed description of e-commerce architectures see: G P Schneider, J T Perry, *Electronic Commerce*, Cambridge 2001, p 64, 65

functionalities. This, in turn, requires the addition of protocol layers *on top* of them.[51] Unless the analysis is confined to the generation and transfer of native cryptocurrencies such as Bitcoin or Ether, blockchains cannot be analysed in isolation but must be seen as one of many components of a larger ecosystem. The need to do so can be illustrated by, for example, the Hyperledger architecture, which provides the technical framework for private ledgers and distinguishes, amongst others, between the consensus layer (which confirms the correctness of transactions that constitute a block), the smart contract layer (which processes transaction requests and determines transaction validity), the data store abstraction (which allows different data stores to be used by other components) and APIs (which enable other modules to interface to the blockchain).[52]

The fact that blockchains are "only" data structures that require additional components to support or enable a wider range of commercial applications has important practical implications. The fact that the blockchain is "trustless" and "immutable" etc. does not imply that the other components in the system share these characteristics. The features of the blockchain are not inherited by the technologies or processes that connect to or write data into the blockchain. To illustrate using a metaphor: even if a blockchain can be regarded as a perfect piece of bread – fresh, tasty and nutritious, we rarely eat bread by itself. Hence, we add butter, cheese, pickles or lettuce. If any of these additional ingredients is spoiled, the whole sandwich becomes inedible – quality of the bread notwithstanding. The point is simple: the attributes of the database must be distinguished from the attributes of the other components of the ecosystem. A database by itself cannot support or serve as a transactional platform – its technological sophistication notwithstanding. Logically, this reduces the value of blockchain-based systems. If only the database is "trustless" and "immutable" but none of the other system

[51] Antonopoulos (n 27) 218.

[52] Hyperledger Architecture, Volume II, Smart Contracts,3; www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf

components is similarly "trustless" and "immutable," then – when evaluated as a whole – the entire system is only as good as its weakest part. Blockchain enthusiasts, however, seem to imply the opposite or conveniently bypass this issue, as illustrated by the following quote from a technical paper:

> "From a software architecture perspective, blockchain enables new forms of distributed software architectures, where agreement on shared state for decentralised and transactional data can be established across a large network of untrusted participants. This circumvents the need to rely on a central, trusted integration point which has the power to control and manipulate the system, and is a single point of failure. Applications built on blockchains can take advantage of properties such as data immutability, integrity, fair access, transparency, and non-repudiation of transactions. "[53]

RIGHTS & RECORDS

One of the most oft-cited use cases for the blockchain in the law is as a form of distributed asset registry. This is understandable since a register is essentially a particular type of database and blockchains are databases. There are now a host of initiatives, both public and private, applying the blockchain to a variety of assets ranging from land to securities to intellectual property. Many of these initiatives are seriously misguided. This is not to say that it is impossible to have blockchain asset registries. Rather, many of these early initiatives have underestimated the complexities involved in the setting up and the maintenance of a registry and/or overestimated the vaunted security of blockchains.

Private Initiatives to Establish Blockchain Asset Registries

[53] XU 3

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[54] of the blockchain employed but the involvement or in this case, lack thereof, of government and hence, the law. Some of these private initiatives to establish a blockchain asset registry employ permissioned blockchains whereas others will use permissionless blockchains. Many blockchain initiatives, especially because they tout the immutability of blockchains,[55] 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 ownership, "an electronic coin", is defined by its ledger entries, being "a chain of digital signatures".[56] Although many do not perceive the difference in form between Bitcoins and other cryptocurrencies modelled upon it and so-called electronic bank money,[57] the legal nature of these two forms of assets could hardly be more different. Bitcoin and other native cryptocurrencies,[58] may well be electronic money properly so-called because their legal nature is irrevocably tied to the electronic blockchain register.[59] But that is not the case with so-called electronic bank money. Bank money in the form of money held in bank accounts is today clearly established to be in the legal form of *in personam* claims against the bank.[60] This was

[54] For which, see text accompanying nn >>>
[55] For which see text accompanying nn ???.
[56] See Satoshi Nakamoto, (October 2008), "Bitcoin: A Peer-to-Peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf at 2.
[57] 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".
[58] i.e. those that are not securities.
[59] See Kelvin FK Low and Ernie Teo, "Legal Risks of Owning Cryptocurrencies" in D Lee and R Deng (eds), *Handbook of Blockchain, Digital Finance, and Inclusion*, Volume 1 (2017), 225 at 241-242, Kelvin FK Low and Ernie GS Teo, "Bitcoins and Other Cryptocurrencies as Property?" (2017) 9 Law, Innovation & Technology 235 at 252-254.
[60] *Foley v Hill* (1848) 2 HLC 28, 9 ER 1002.

not always the case[61] but the historical position is now irrelevant and it is its modern form that permits its "transfer" in the sense that we see 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. "[T]he fundamental legal nature of bank money has not changed from the early days of banking when ledger entries were made in ink on paper, whether by hand on vellum or by printing on a passbook. Just as a ledger entry on paper did not … transform bank money [and] render the incorporeal corporeal, neither does a digital entry render it digital."[62] The temptation to confuse the record with the right is easily dispelled when we turn our attention to other registers, where the asset recorded is tangible. Many jurisdictions with developed economies have well-established land registers and in many jurisdictions, these registers are migrating from paper to electronic form.[63] 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 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.[64] While some would confine the category of property to such rights,[65] and it is arguable that the civilian traditions, particularly those with Germanic roots, follow such a narrow conception of property, it is clear that this is not the case of the common law. The common law has a long tradition of regarding choses in action as personal property. But it is important to observe that such property differs from that

[61] Benjamin Geva, "'Bank Money': The Rise, Fall, and Metamorphosis of the 'Transferable Deposit'" in David Fox and Wolfgang Ernst (eds), *Money in the Western Legal Tradition: Middle Ages to Bretton Woods* (2016) 359.
[62] Kelvin FK Low and Ernie Teo, "Legal Risks of Owning Cryptocurrencies" in D Lee and R Deng (eds), *Handbook of Blockchain, Digital Finance, and Inclusion*, Volume 1 (2017), 225 at 229.
[63] See, eg, Rouhshi Low, "From Paper to Electronic: Exploring the Fraud Risks Stemming From the Use of Technology to Automate the Australian Torrens System" (2009) 21 Bond Law Review 107.
[64] Ben McFarlane and Simon Douglas, "Defining Property Rights" in James Penner and Henry Smith (eds), *Philosophical Foundations of Property Law* (2013) 219.
[65] Ibid.

of tangible property in some important respects. Unlike tangible property, where the object of the right is clearly distinct and separable from the right itself, no such object exists for intangible property. This is perhaps more obvious from the older terminology of chose in action. As Blackstone explained:[66]

> Property, in chattels personal, may be either in possession; which is where a man hath not only the right to enjoy, but hath the actual enjoyment of, the thing; or else it is in action; where a man hath only a bare right.

The absence of a separable thing renders it easier to confuse right with record, especially where the record, like the right, is itself also intangible. Thus, ledger records of bank deposits kept by banks did not cause lawyers or laymen to consider that such bank money existed in paper form, in part possibly because there would be multiple copies of such records, some offered to the customer to keep, others kept by the bank itself, which would also keep backups as a matter of prudence. But the moment the records transitioned to electronic form, the temptation to confusion became too great to resist and electronic or digital money was born. In this respect, it is notable that the use of cryptography to effect "transfers" of "digital" money predate Bitcoin by more than a decade. Hardly anyone today remembers DigiCash, openly touted as digital money. Hailed by *Wired* magazine as "the killer application for electronic networks" that is "not only going to revolutionize the Net, it will change the global economy",[67] the product nevertheless sputtered and failed[68] and Digicash Inc, the company, was declared bankrupt in 1998,[69] almost exactly a decade before Bitcoin was born. We see the same temptation to confuse right and record with carbon credits. Thus, in *Armstrong DLW GmbH v Winnington*

[66] William Blackstone, Comm II at 389.
[67] Steven Levy (1 December 1994), "E-money (that's what I want)", *The Wired* at http://www.wired.com/1994/12/emoney/
[68] Julie Pitta (1 November 1999), "Requiem for a Bright Idea", *Forbes* https://www.forbes.com/forbes/1999/1101/6411390a.html#6cbf530e715f.
[69] Wired News Report (6 November 1998), "Digicash Outta Cash", *Wired* https://www.wired.com/1998/11/digicash-outta-cash/.

Networks Ltd., EU carbon credits (technically European Union Allowances or EUAs) recorded in electronic registries were regarded by the trial judge as existing "only in electronic form".[70] We see also a similar confusion between right and record 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". 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).[71] It is unfortunate that this provision has since been repealed and replaced with a more literal translation of the 2009 Directive.[72] That which is stored electronically is not value itself but a record of a claim that is valuable and the muddle between record, claim, and value can lead to much unnecessary confusion, as was the case in *Armstrong DLW GmbH v Winnington Networks Ltd*.[73]

Unlike native cryptocurrencies such as Bitcoin, which have no existence apart from the ledger entries in the blockchain so that, if at all, the law can only accommodate legal rights to such cryptocurrencies as rights to entries on the blockchain,[74] 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

[70] [2013] Ch 156, [49], criticised by Kelvin FK Low and Jolene Lin, 'Carbon Credits as EU Like It: Property, Immunity, TragiCO2medy?' (2015) 27 Journal of Environmental Law 377.
[71] Section 1(14), *Kreditwesengesetz*.
[72] Cf Section 1(2), *Zahlungsdiensteaufsichtsgesetz*.
[73] See Kelvin FK Low and Jolene Lin, 'Carbon Credits as EU Like It: Property, Immunity, TragiCO2medy?' (2015) 27 Journal of Environmental Law 377, particularly xxx.
[74] Kelvin FK Low and Ernie GS Teo, "Bitcoins and Other Cryptocurrencies as Property?" (2017) 9 Law, Innovation & Technology 235.

keeping system that is not fully compatible with these existing legal rules will therefore require legal amendments in order to be effective. It is notable that even public registration systems are heterogeneous and function differently depending on design. Some registration systems provide some prima facie evidence of title such as in the case of shares,[75] patents,[76] and registered designs.[77] Some registration systems, such as that for trademarks, do not purport to provide any indication as to title at all, whether prima facie or otherwise.[78] Where this is the case, which is so 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 from insisting on its correction.'[79] At the other extreme, registration of a fee simple title to land provides far greater protection than prima facie evidence of title, going so far as to validate an otherwise void transfer. Section 58(1) of the English Land Registration Act 2002 provides: 'If, on the entry of a person as the proprietor of a legal estate, the legal estate would not otherwise be vested in him, it shall be deemed to be vested in him as a result of the registration.' This is similar to the indefeasibility conferred by registration in Torrens systems of land registration. The entry of a notice on the register of an equitable interest in land behaves differently again, providing priority without validating invalid transfers. Section 32(3) of the English Land Registration Act 2002 provides:

> The fact that an interest is the subject of a notice does not necessarily mean that the interest is valid, but does mean that the priority of the interest, if valid, is protected for the purposes of sections 29 and 30.

[75] Companies Act 2006, s 127.
[76] Patents Act 1977, s 32(9).
[77] Registered Designs Act 1949, s 17(8).
[78] Trade Marks Act 1994.
[79] EP Ellinger, E Lomnicka and CVM Hare, Ellinger's Modern Banking Law (OUP, 5th edn 2011) 236.

It is important to note that, 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. Private blockchain registry initiatives will not be able to confer any such benefits.

Nor would the case of bank ledgers, a private arrangement between banker and customer, be instructive for two reasons. 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. Nor do transfers of bank money operate as transfers in the normal fashion of property transfers, in part because of its contractual nature. The doctrine of privity of contract prevents transfers of contractual rights. The common law got around the doctrine of privity by employing the notion of a derivative transfer via assignment in equity. Equitable assignment permitted the law to square the circle by allocating control of the right to bring the action to the assignee whilst strictly insisting on the interposition of the assignor as claimant in any action against the obligor. This allowed an equitable assignment to achieve the economic result of a transfer without offending the rule of privity. But even so, bank "transfers" do not operate as assignments, which deal with the same asset, ie the very same debt claim (chose in action). Instead, bank "transfers" of money do not transfer the same asset. As Fox explains:[80]

> The chose in action representing the money transferred to the recipient's bank account is a distinct item of property from the chose in action representing the funds which were originally in the payer's account. The payer's title to the money is not strictly transferred. Instead, the title to the value represented in the transfer passes to the recipient because the payer's bank extinguishes (wholly

[80] David Fox, *Property Rights in Money* (2008), [5.03].

or partially) the debt which it owes the payer, and the recipient's bank creates a new debt owed by itself to the recipient.

Most other forms of property in law simply do not behave this way. Any agreement by two or more parties to the effect that some property would behave in a particular manner different to the default rules established by the law would fall foul of the *numerus clausus* principle. The *numerus clausus* (Latin for closed number) principle limits the number of types of rights which the law will recognise as property. Most transfers of property are also 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 shares and copyright.

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",[81] the legal efficacy of such clauses are largely untested. Although most legal systems in principle respect freedom of contract, such freedom is hardly unfettered. 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 Unfair Terms in Consumer Contracts Regulations 1999. Significantly, such clauses contradict the standards set out in the 'Banking: Conduct of Business Sourcebook' issued by the Financial Conduct Authority.[82]

For the foregoing reasons, no private initiative to establish a blockchain asset registry will be effective in establishing title beyond providing evidence that a private key was used to

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

[82] 'Banking: Conduct of Business Sourcebook' (Release 9: August 2016), paras 5.1.11-5.1.12. The 'Banking: Conduct of Business Sourcebook' replaces 'The Banking Code: Setting Standards for Banks, Building Societies and Other Banking Service Providers' (March 2005), paras. 12.5, 12.9, 12.11-12.12, 12.14-12.16.

sign off on a particular transaction. Owing to the limitations of blockchain technology, this cannot be assumed to constitute the sort of consent to a transfer that the law traditionally requires. Moreover, even assuming they enhance transparency to some degree to those who know where to look, private initiatives to establish blockchain asset registries still face a challenge. Where among the dozens of private blockchains, which can easily proliferate to hundreds if not thousands, should a purchaser look to identify the owner of any particular asset? For copyright in music alone, there are at least the following blockchain initiatives that the authors are aware of: Berklee College of Music's Open Music Initiative,[83] Blòkur,[84] Mycelia,[85] Soundac,[86] and Ujo.[87] Then, there is the question of forked blockchains where the particular initiative utilises a permissionless blockchain.[88] In truth, many of these blockchains do not serve as registers of ownership regardless of what their marketing materials say but rather are simply systems of rights management with a particular focus on licensing. But even if they simply serve as a system of rights management, there is a necessity to address the elephant in the room. What happens when the system's record of rights no longer accurately reflects the position at law? If licence fees are paid to the wrong persons, then the operators of these systems, if they can be identified, and perhaps even the payees, may potentially be guilty of authorising infringement and end users may be liable for, in the case of music, copyright infringement.

Asset Registries and 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 computer scientists to what can appear to be the same problem. At

[83] http://open-music.org/
[84] https://www.blokur.com/ (accessed 21 August 2018).
[85] http://myceliaformusic.org/ (accessed 21 August 2018).
[86] https://soundac.io/
[87] https://ujomusic.com/ (accessed 21 August 2018).
[88] See text accompanying nn ??.

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 the competing claimants are often both innocent. The complexity of the problem is demonstrated by the range of different rules that apply 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, money in the form of notes and coins, copyright) or registration serves limited[89] or no[90] 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,[91] for which registration conferred priority in disputes where conflicting claims had to be resolved but which was not authoritative. Although this form of land registration can be traced back to the 17th century, this supposedly antiquated form of registration system survives today in the former colony of Hong Kong. The Hong Kong Land Registration Ordinance,[92] enacted on 28 February 1944, was the third Ordinance to be enacted by the colonial Legislative Council and is the oldest Ordinance in operation in the Special Administrative Region today. As Hunter J in *Financial and Investment Services for Asia Ltd v Baik Wha International Trading Co Ltd* succinctly explained, "Validity and priority

[89] 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.
[90] See, eg, Trade Marks Act 1994.
[91] Francis Sheppard and Victor Belcher, "The deeds registries of Yorkshire and Middlesex" (1980) 6 Journal of the Society of Archivists 274.
[92] Cap 128.

are different concepts. The second [i.e. priority] only arises between valid effective documents."[93]

Dissatisfaction 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.[94] The Torrens system spread throughout the Australian colonies, New Zealand and beyond,[95] won admiration from English lawyers,[96] and served as inspiration in part for both the English Land Registration Act 1925[97] and the English Land Registration Act 2002.[98] In order to understand the advantages and drawbacks (and it must be stressed that there are drawbacks) wrought by these changes, it is necessary to first understand the devil's choice that the law of property faces on a regular basis. 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.[99] 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 act of another. Dynamic security, on the other hand, which prefers B, favours subsequent bona fide purchasers at the expense of the

[93] [1985] HKLR 103, at 112-113. Hunter J's decision has been cited with approval in *Shih Ching Yang v Tsoi On Pong* [2011] 3 HKC 432, [2011] 3 HKLRD 271, at [41] (To J); *King Glare Ltd v Secretary for Justice* [2008] 6 HKC 450, at [36] (Lam J); and *HKSAR v Lau Kam Ying* (2013) 16 HKCFAR 595, at [19] (Tang PJ).

[94] For background as to how the Torrens system was conceived, developed and eventually born, see P Moerlin Fox, "The Story behind the Torrens System" (1950) 23 Australian Law Journal 489. Cf S Robinson, *Transfer of Land in Victoria* (1979) ch 1.

[95] For a list of jurisdictions that have adopted a Torrens system of land registration, see SR Simpson, *Land Law and Registration* (1976) 81; M Raff, *Private Property and Environmental Responsibility* (2003) 9.

[96] Theodore BF Ruoff, *An Englishman Looks at the Torrens System* (1957)

[97] Kevin Gray and Susan Francis Gray, *Land Law*, 7th Ed (2009), at [2-044].

[98] Ibid. See also Law Commission Consultation Paper No. 254, "Land Registration for the Twenty-First Century: A Consultative Document" (1998) at http://www.lawcom.gov.uk/wp-content/uploads/2015/04/lc254.pdf; Law Commission Consultation Paper No. 227, "Updating the Land Registration Act 2002: A Consultation Paper" (2016) at http://www.lawcom.gov.uk/app/uploads/2016/03/cp227_land_registration_web.pdf.

[99] R Demogue, "Security" in A Fouilleé, J Charmont, L Duguit and R Demogue (eds), FW Scott and JP Chamberlain (trans), *Modern French Legal Philosophy* (1968), 418.

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. Neither form of security is obviously better. Consider the position of B in the aforementioned example. It may seem obvious that B would favour dynamic security but the problem with dynamic security is that, inasmuch as it favours B in his acquisition of property, it operates against him the moment he acquires it so that if another fraudulent party D came along and transferred the same asset to E, dynamic security would favour E over B. For common law systems, it is notable that both the common law's default rule, which is *nemo dat quod non habet*,[100] as well as equity's maxim, *qui prior est tempore potior jure*,[101] favour static security. The unfortunate consequence of this policy, even as mitigated by the older deeds registration system, 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."[102] By making registration more authoritative, conveyancing was simplified and costs were in theory reduced. But the shift carried a cost, which many, including some lawyers today, often fail to appreciate. We see this ignorance in some economists advocating title registration in developing economies as if it were some sort of silver bullet that can dispel poverty.[103] A shift from static to dynamic security does not somehow in and of itself prevent fraud and therefore engender economic growth, as a comparative analysis of Singapore and Malaysia, both operating Torrens systems, reveals.[104] All it does is shift losses when frauds occur and property owners within Torrens jurisdictions are occasionally rudely reminded of the high cost

[100] No one may give what he does not have.
[101] He who is earlier in time is stronger in law.
[102] Pamela 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* (2003) 81, at 85-86.
[103] See, eg, World Bank Development Report, 2002: *Building Institutions for Markets*. Hernan De Soto …
[104] Tang Hang Wu and Loh Khian Chung, "A Law Which Favours Forgers: Land Fraud in Two Torrens Jurisdictions" (2011) 19 Australian Property Law Journal 130.

of dynamic security. In 2006 in Singapore, a 90 year old Bebe bte Mohammad, who was suffering from Alzheimer's disease, was defrauded of her property when one of her adopted daughter's forged a mortgage, which was registered, in favour of a bank.[105] In 2010 in Perth, Roger Mildenhall, who lived in South Africa, was defrauded of his property when a forged transfer of his property was registered in favour of an innocent purchaser.[106] At a more macro level, Torrens title registration has also been regarded as facilitating the dispossession and exclusion of indigenous people and minorities by the colonists.[107] It is not difficult to imagine the process of transitioning to blockchain asset registration similarly being used as an 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.[108] This problem is simply and vividly captured by the expression, "garbage in, garbage out"[109] – if the recorded data is incorrect, the record is incorrect.

The complexity of registration can also be detected in the "insurance principle" underlying most Torrens registration systems. Although often heralded as the third[110] key principle of Torrens registration, it was more likely than not established to overcome the hostilities of lawyers opposed to the shift from static to dynamic security.[111] Insurance needs to be funded and short of doing so through increased taxation, it can only be achieved through

---

[105] *United Overseas Bank Ltd v Bebe bte Mohammad* [2006] 4 SLR(R) 884; [2006] SGCA 30. See also Khushwant Singh (26 September 2006), "70-year-old retiree loses bungalow to bank on appeal", *Straits Times*. The 70 year old retiree referred to in the newspaper headline is the other adopted daughter of 90 year old Bebe bte Mohammad.

[106] Courtney Trenwith, 25 May 2012, *WA Today* at https://www.watoday.com.au/national/western-australia/agency-investigated-after-home-sold-without-owners-knowledge-20120525-1z8vm.html.

[107] Sarah Keenan, "From historical chains to derivative futures: Title registries as time machines" (2018) Social & Cultural Geography (forthcoming).

[108] Cf Victoria Louise Lemieux, "Trusting Records: Is Blockchain Technology the Answer?" (2016) 26 Records Management Journal No. 2.

[109] Mizrahi, Avi. (3 March 2016). "Factom CEO: Blockchain-based Transparent Mortgages Can Restore Trust in Markets." *Finance Magnates.* Retrieved from www.financemagnates.com/cryptocurrency/interview- 2/factom-ceo-blockchain-based-transparent-mortgages-can-restore-trust-in-markets/

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

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

higher transaction fees. But that was part of the problem title registration was designed to solve. It is notable in this respect that some Torrens jurisdictions with low registration fees have extremely anemic insurance provisions.[112] That title registration legislation is not some magic wand that will cure all ills can be seen in the Hong Kong experience. In 2004, the Hong Kong government passed its Land Titles Ordinance,[113] intending to drag Hong Kong conveyancing practice from the 17th century of registration of deeds to title registration modernity. To date, it has not been brought into force.[114]

There is a further cost to the shift from static to dynamic security. All title registration systems operate in what has been described as a "bijural" fashion:[115]

> Systems of registered title are "bijural", in the sense that they straddle two bodies of law – the positive system and the ordinary rules of property law. The legal rule of the positive system is that registration confers title to the interest shown, irrespective of whether the registered instrument is valid. While title registration statutes provide for registers to be set aside on specified grounds, they remain authoritative so long as they stand.
>
> Bijuralism is unavoidable in a positive system because no registration statute operates as an exhaustive code for the transfer of property rights in land. All are founded upon the ordinary rules, except to the extent that they are modified or excluded by the title registration statute. In theory, no instrument should ever be registered unless it is valid under the ordinary rules. In practice, many

[112] Singapore.
[113] Cap 585.
[114] Naomi Ng (23 November 2017), "Overdue law on land titles could have simplified flat-buying in Hong Kong, Audit Commission says", *South China Morning Post* at https://www.scmp.com/news/hong-kong/community/article/2121147/overdue-law-land-titles-could-have-simplified-flat-buying.
[115] Pamela O'Connor, "Deferred and Immediate Indefeasibility: Bijural Ambiguity in Registered Land Title Systems" (2009) 13 Edinburgh Law Review 194 at 195-196.

> invalidating defects are not patent on the face of the instrument and can easily pass undetected through the registry's examination. …
>
> The issue for all systems of registered title is how to deal with bijural inaccuracies.

Although the outcome, being a more authoritative register, appears to end users as a simplification of the entire process of conveyancing, the bijuralism involved in reaching this result means that there is actually greater complexity for the operators of the system, being the conveyancers and registry personnel. In addition to learning the underlying rules of property (which are already in themselves quite complicated), they also have to master the new rules imposed by the relevant registration statute as well as the rules relating to how they interact with one another.[116]

Perhaps even more significantly, it remains notable that whilst under such modern registration systems, registration is more authoritative,[117] they are not absolutely authoritative. "There is no known property law regime that operates in [an absolutely authoritative] fashion – to a property lawyer, this is indefeasibility on steroids."[118] An absolute code is not theoretically impossible but will operate extremely harshly unless all possibility of fraud and mistake can be precluded.[119] This is one of the reasons why all title registration systems to date have been bijural systems. Monojural title registration regimes exact a price no society has hitherto been willing to pay. It is in this context that the aforementioned Achilles' heels in the blockchain's vaunted security needs to be borne in mind. Without absolute security, which the blockchain does not offer, the adoption of an absolute rule of code as law is simply untenable

[116] This raises the question of the suitability of the timing for introducing title registration for developing economies. If the institutions are not ready to deal with the additional complexity, would title registration achieve its objectives?

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

[118] At 240.

[119] Experience suggests that judges are unlikely to accept such harsh outcomes without pushback: see the seminal article by Carol M Rose, "Crystals and Mud in Property Law" (1988) 40 Stan L Rev 577. See also Henry E Smith, "Rose's Human Nature of Property" (2011) 19 Wm & Mary Bill Rts J 1047.

unless one is prepared to bear the harsh consequences. All well-drafted asset registration systems contain provisions for the rectification of errors that can creep into the register, though the scope for rectification may be narrower or wider depending on policy objectives. It is here that the other characteristic of the blockchain, being its "immutability", can prove problematic for an asset registry. If a fraud occurs and the transferee either cannot be found or is simply recalcitrant, then the blockchain registry cannot be corrected, which would make further trade in the underlying asset difficult if not impossible.

The perspective of computer scientists is very different. The blockchain "proof-of-work" is a recent solution to a problem that dates to the advent of distributed computing. The key advantage of a distributed system is its built-in redundancy. However, the price of distribution is the potential for inconsistency within the system. Where the distributed system is a database, this entails the possibility that different copies of the database might contain different information. This is, of course, a nonexistent problem in centralised databases, though this is not to say that all the information it contains is accurate. The challenge for computer scientists was to ensure consensus throughout the distributed system in addition to reliability. There are two main causes of failure in a distributed system. First, there could be a network failure in which, although the individual computers that form the network are working perfectly, the network that connects them fails, usually partially, leaving some nodes unconnected to other nodes. Secondly, the network could be fully functional but one or more nodes could fail. Node failures in turn are divided into fail stop and Byzantine failures. The latter are significantly more troubling than the former. When a node encounters a fail stop, the other nodes in the network would at least be aware that it has failed because by definition, it stops working altogether. It stops transmitting and receiving any data and no user can obtain any service from such a node. A Byzantine failure, on the other hand, is any failure in which a node operates in a flawed manner. The reasons for such error are infinitely varied, ranging from

data corruption from a bit flip in memory, the node running older outdated software and hence sending invalid messages, to the node having been compromised by malicious software. The reason such failures are called Byzantine failures stems from a seminal 1982 computer science paper entitled "The Byzantine Generals Problem"[120] in which the metaphor of several divisions of a Byzantine army camped outside an enemy city was used to vividly describe the problems of achieving consensus in distributed systems when parts of it malfunction in a way that other parts are unaware of. The image of traitorous Byzantine generals has forever since represented malfunctioning[121] nodes in distributed computing to generations of computer scientists and the task of building distributed systems tolerant to such malfunctions came to be known as developing Byzantine fault-tolerance. Traditional Byzantine fault-tolerant designs were designed with what computer scientists called state machine replication, in which a service is deployed in a set of servers rather than a single central server. This ensured fault tolerance through redundancy and also improved system performance and capacity. State machine replication is also known as active replication and can be contrasted with what most people would be more familiar with, which is primary-backup, or passive, replication. Such state machine replication generally tolerates under a third of malicious nodes[122] but is limited in scalability in terms of numbers of nodes.[123] The Bitcoin blockchain employs a different technique to ensure distributed consensus. Although Satoshi Nakamoto's famous white paper does not name the Byzantine Generals Problem, an archived email from the inventor of Bitcoin connects the dot between his proof of work blockchain solution to the problem.[124] The use of proof of work consensus greatly enhances scalability in terms of the number of nodes that a

[120] Leslie Lamport, Robert Shostak and Marshall Pease, "The Byzantine Generals Problem" (1982) 4 ACM Transactions on Programming Languages and Systems 382.
[121] Excepting fail stop malfunctions.
[122] See Lamport, Shostak and Pease.
[123] Marko Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of Work vs. BFT Replication"
[124] https://www.mail-archive.com/cryptography@metzdowd.com/msg09997.html.

network can accommodate but it is notoriously energy intensive[125] and does not offer the same consensus finality afforded by Byzantine fault-tolerant state machine replication.[126] Even when all nodes are functioning entirely properly, temporary forks in the blockchain do occur, and whilst such forks will usually resolve themselves eventually,[127] this results in the absence of consensus finality in proof of work blockchains.

Conventional wisdom suggests that the Bitcoin blockchain protocol is resistant to up to 50% malicious nodes, hence the popular references to what is called the 51% attack. Whilst this is thought to demonstrate the protocol's tremendous resilience, both theory and reality have demonstrated otherwise. Theoretically, it has been demonstrated that, under certain circumstances, only 25% of nodes needs to be compromised in order to compromise proof of work blockchains.[128] Furthermore, instead of accumulating the necessary computing power by building it, which is extremely costly, it is possible to design an attack on proof of work blockchains by renting computing power or simply paying operators of nodes off-chain,[129] both strategies which make such attacks more accessible than conventionally thought. We are also seeing more actual instances of such 51% attacks in the press.[130] Although such attacks have

[125] Alex de Vries, "Bitcoin's Growing Energy Problem"(2018) 2 *Joule* 801. Also see Emily Atkin (6 December 2017), "The Environmental Case Against Bitcoin", *The New Republic* at https://newrepublic.com/article/146099/environmental-case-bitcoin; Izabella Kaminska (7 November 2017), "The environmental costs of bitcoin are not worth the candle", *Financial Times*; Eric Holthaus (6 December 2017), "Bitcoin Mining Guzzles Energy—And Its Carbon Footprint Just Keeps Growing", *Wired* at https://www.wired.com/story/bitcoin-mining-guzzles-energyand-its-carbon-footprint-just-keeps-growing/. For the latest information on Bitcoin energy consumption, see https://digiconomist.net/bitcoin-energy-consumption.

[126] Marko Vukolić, "The Quest for Scalable Blockchain Fabric: Proof-of Work vs. BFT Replication"

[127] But see text to nn ???.

[128] Ittay Eyal and Emin Gün Sirer, "Majority is not enough: Bitcoin mining is vulnerable" in Nicolas Christin and Reihaneh Safavi-Naini (eds), *Financial Cryptography and Data Security – 18th International Conference, FC 2014* (2014), 436.

[129] Joseph Bonneau, "Hostile blockchain takeovers (short paper)". Also see https://www.crypto51.app/, a website which lists the estimated costs of a 1 hour 51% attack cost for a host of cryptocurrencies that utilise the proof of work protocol.

[130] Alyssa Hertig (8 June 2018), "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular", *Coindesk* at https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/; Joon Ian Wong (24 May 2018), "Every cryptocurrency's nightmare scenario is happening to Bitcoin Gold", *Quartz* at https://qz.com/1287701/bitcoin-golds-51-attack-is-every-cryptocurrencys-nightmare-scenario/; Dan Robitzki (31 May 2018), "Hackers Commandeered 3 Cryptocurrency Networks, Stole Millions", *Futurism* at https://futurism.com/cryptocurrency-51-percent-attack/.

primarily targeted so called altcoins, i.e. alternatives to Bitcoin, with much smaller networks than the Bitcoin network, these attacks should serve as an important cautionary tale for plans for permissioned blockchain asset registries, which will likely have similar small networks although their permissioned nature will provide some measure of additional security over the permissionless blockchains of these altcoins. Nevertheless, the main difficulty with transposing computer science perspectives of security to that of property law is one of incompatible perspectives. In designing for distributed computer systems, whether through Byzantine fault tolerant state machine replication or proof of work blockchains, computer scientists are focused almost entirely on network security. So far as the end user is concerned, other than the use of asymmetric cryptography, there is "*zero* protection from other forms of fraud, such as hacking, which is not only possible but commonplace."[131] Asymmetric cryptography, more commonly known as public key cryptography, is extremely secure but for the human factor. Human actors must maintain a delicate balance between maintaining absolute secrecy to one's private key and simultaneously ensure that there are sufficient backups of the same in case a copy is inadvertently lost. Private keys stored on computers connected to the Internet are susceptible to hacking but in order to use them on a distributed network built upon the Internet, devices must connect to it at some point. According to the *Financial Times* in 2016, "[o]nline lists curated by bitcoin community members suggest bitcoin exchanges have been involved in up to 60 high-profile hacking incidents since the digital asset class was created in 2009. The true scale of the hacking problem, however, is hard to estimate".[132] Although most high profile hacks have been directed at exchanges, individuals have also been targeted.[133] This will be unsurprising to computer security experts. "Only amateurs attack machines; professionals

[131] Low and Teo, at 236.
[132] Kaminska.
[133] Nathaniel Popper (21 August 2017), "Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency", *The New York Times*.

target people".[134] 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 and even so, private keys can also be "stolen" if they are gleaned by dishonest strangers, as happened to the CEO of a financial services company who left his account information in his car while having it valet parked.[135] Good old-fashioned violence will also often do the trick.[136] To the extent that any relevant blockchain asset registry anticipates the use of so-called "smart contracts", coding vulnerabilities could expose asset holders to the sort of hack that gripped the cryptocurrency community when the DAO was "hacked". [137] Considering the atrocious cybersecurity practices of the vast majority of people,[138] this is a gaping hole that must be plugged, if it indeed can be plugged, before blockchain asset registries are deployed for widespread usage by the general public.

It is notable that the vast majority of registry frauds today target the end user rather than the registry so that the implementation of blockchain technology for traditional asset registries is unlikely to reduce incidences of fraud. Indeed, to the extent that it exposes end users to miscreants around the world rather than to those who are close to them,[139] it is seriously arguable that the risks are amplified. "[I]t is [also] likely that the elderly are likely to be disproportionately exposed to such [frauds] since they are likely to have the most wealth whilst at the same time being among the least tech savvy of all users".[140] Advocates of blockchain

[134] Bruce Schneier. Cf. Mark Evans, Leandros A Maglaras, Ying He and Helge Janicke, "Human behaviour as an aspect of cybersecurity assurance" (2016) 9 *Security and Communications Networks* 4667.
[135] Maras 2015
[136] Nathaniel Popper (18 February 2018), "Bitcoin Thieves Threaten Real Violence for Virtual Currencies", *The New York Times*; Nupur Anand (11 April 2018), "In India, criminals are now extorting bitcoin from their victims", *Quartz India* at https://qz.com/india/1249603/bitcoin-crime-kidnapped-indian-businessman-paid-200-bitcoin-ransom/.
[137] Add footnote.
[138] Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov and XiaoFeng Wang, "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; Jason Hong, "The State of Phishing Attacks" (2012) 55 *Communications of the ACM* 74.
[139] Many registry frauds today are perpetrated by family and loved ones.
[140] Low and Teo, at 242.

asset registries, particularly the computer scientists among them, need to overcome what psychologists call the false consensus effect,[141] in which individuals tend to overestimate the degree to which others share their characteristics or beliefs – chief in this respect, their cybersecurity practices and willingness to impose losses on those who do not behave similarly responsibly.

Clearing the Air on the Necessity of "Centralization"

One common refrain among advocates of decentralization and blockchain asset registries is that decentralization will enable us to speed up certain transactions by eliminating the need for intermediaries and simplifying clearing and settlement.[142] In the first place, it is not obvious that speed is necessarily desirable for certain transactions. Take the process of conveyancing, for example. It is, in many jurisdictions, a multi-process transaction mired in formality. Viewed from one perspective, it can appear outmoded and unnecessarily complicated. Yet, on closer examination, such formalities, to the extent that they are slowing down the transaction, are precisely serving the function they were intended to perform. Many jurisdictions require contracts relating to transfers or other dealings in land to take on written form precisely because the formal documentation serves a cautionary function.[143] This in turn is justified because, save perhaps for the 1%, transactions relating to land are likely to be by far the most financially significant transaction that the average person will undertake in their lifetime.[144] It may be that improving the speed of transactions is more obviously desirable in financial markets but does

[141] Lee Ross, David Greene, and Pamela House, "The 'false consensus effect': An egocentric bias in social perception and attribution processes" (1977) 13 *Journal of Experimental Social Psychology* 279.

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

[143] Patricia Critchley, "Taking Formalities Seriously" in Susan Bright and John Dewar (eds), Land Law: Themes and Perspectives (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. For a history of the formality rules in England, see T G Youdan, "Formalities for Trusts of Land, and the Doctrine of *Rochefoucauld v Boustead*" [1984] CLJ 306;

[144] Kelvin FK Low, "Informal Dealings with Land: Retaining the Knotty Apron Strings" (2010) 22 SAcLJ 704.

the use of a blockchain per se permit the elimination of intermediaries and simplifying the processes of clearing and settlement?

Although this is widely assumed to be the case among blockchain enthusiasts, we will see that this is only partially true. According to Geva:

> In 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.

Where the subject of intermediation is securities, disintermediation through the use of blockchain technology should not be too difficult, particularly in jurisdictions like the UK, where intermediation is not compulsory to begin with.[145] Since one of the main advantages of intermediation was "the ease of trading and settlement",[146] 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 simply because they greased the wheels of finance, but also because intermediaries offered other services to clients, "such as record keeping, investment management services and the provision of finance."[147] Securities are, however, the easy case for a blockchain asset registry because a single issue of securities is fundamentally fungible.[148] This is not the case where derivatives trading or inter-bank money transfers are concerned. It is most convenient to use the example of inter-bank money transfers since it is precisely the

[145] Louise Gullifer, "Ownership of Securities: The Problem Caused by Intermediation" in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities: Legal Problems and Practical Issues* (2010) 1 at 2.
[146] Louise Gullifer, "Ownership of Securities: The Problem Caused by Intermediation" in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities: Legal Problems and Practical Issues* (2010) 1 at 3.
[147] Louise Gullifer, "Ownership of Securities: The Problem Caused by Intermediation" in Louise Gullifer and Jennifer Payne (eds), *Intermediated Securities: Legal Problems and Practical Issues* (2010) 1 at 3-4.
[148] Roy Goode, "Are Intangible Assets Fungible?" [2003] LMCLQ 379.

example used by Satoshi Nakamoto to illustrate the means by which blockchain technology can facilitate money transfers through disintermediation.

Satoshi Nakamoto's white paper fundamentally misunderstands the role of financial institutions in inter-bank payment systems. The central problem, 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. This would, according to him, 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."[149] If this is correct, then we could simply apply the blockchain technology to the banking industry and achieve the objectives Satoshi Nakamoto set out without the need for the invention of a cryptocurrency such as Bitcoin. In short, continue dealing in the same fundamental asset, being fiat money, but keep records using the blockchain.

The problem with this view is that it involves an erroneous analysis of how an inter-bank money transfer works and the nature of the trust a depositor invests in his bank when he deposits money with the bank. When money is deposited by a customer with his bank, his account is credited with the sum of the deposit because the relationship between bank and customer is one of debtor and creditor.[150] By depositing the money, the customer is lending it to the bank, who is free to deal with it as it wishes, including lending it out to another customer. The trust inherent in the process lies in the customer's belief that the bank is credit worthy and will be able to repay the sum together with any interest when called upon to do so. What we call an inter-bank money transfer turns out to be far more complicated than most people, including surprisingly many bankers, appreciate. If bank money is simply a debt owing by a

[149] Satoshi Nakamoto at 1.
[150] *Foley v Hill*.

bank, then it must be obvious that an inter-bank money transfer cannot possible involve the transfer of a fundamentally fungible asset. A debt owing by Citibank is hardly the same as a debt owing by Barings Bank since a debt is only as valuable as the creditworthiness of its debtor. In fact, there is no transfer of any asset at all. As Geva explains:

> At common law, a debt was looked upon as a strictly personal obligation, and its assignment was prohibited. For its part, equity did not play any role in the early development of payment mechanisms in English law. Thus, a credit transfer has been explained as a process under which the debt owed to the payer by his bank is ultimately replaced by a new debt owed to the payee by his bank. To that end, the characterization of the process as a 'transfer' is certainly a misnomer, as in fact nothing tangible or intangible is transferred. Rather, one debt, owed by a bank to the payer, extinguishes (or decreases), and allows for another debt, that of a bank to the payee, to arise (or increase) and substitute it substantially for the same amount.[151]

As Fox elegantly clarifies, there is not a transfer of property but only of value.[152] Bank intermediaries are fundamental to the ability to effect such a transfer of value. This is perhaps most easily demonstrated by first examining what happens with what has been categorized as an 'in-house' money transfer, which is what occurs when both payer and payee have accounts at the same bank.[153] This is the simplest case because the bank is simultaneously reducing its liability to one customer (the payer) and increasing its liability to another (the payee). It can do so not because of some trust that the latter has in it to prevent the former from double-spending its money but because it is, in this transaction, the common obligor to both. Where there is an inter-bank money transfer, the absence of a single common obligor complicates matters. For

[151] Benjamin Geva 360.
[152] Fox [5.03].
[153] Ross Cranston et al, 339.

inter-bank money transfers within a single jurisdiction of the fiat currency of that jurisdiction, the absence of a common obligor between payer and payee is typically solved by their 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 payee's bank. The role played by the central bank may sometimes be taken instead by a correspondent bank, typically where the inter-bank money transfer crosses borders and/or is made in a foreign currency within the same jurisdiction. There may also be multiple correspondent banks involved because 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 have been described as complex payments and are the source of the most chagrin among bank customers. 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 not the creation of a single blockchain ledger but hundreds of thousands of inter-linked sub-ledgers.[154]

Forks in the Chain: Stumbling Blocks?

All distributed ledgers, whether they employ blockchains or not, have the potential to fork. As we have seen, 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. Leaving aside network failure, however, the "proof-of-work" protocol to establish consensus also produces random forks. This is because "proof-of-work" only "acts as a randomized

[154] Martin Arnold (8 March 2018), "Swift says blockchain not ready for mainstream use", *Financial Times*.

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. However, as concurrency control is only probabilistic and as block propagation over a network can take some time, collisions do happen, resulting in temporary forks on the blockchain that PoW-based blockchains are prone to even if all nodes are honest."[155] Even worse than these random temporary forks are the permanent forks that, though rare, have occurred with both Bitcoin and Ethereum. Ideological differences result in end users supporting one or another (or sometimes both) fork of a blockchain. This may not pose too much of a problem for native on-chain assets such as Bitcoin and Ether since, although forks were initially dreaded as disastrous, they have increasingly come to be seen as "free money". However, forked asset registries of off-chain assets are a different matter altogether. After all, a fork in a blockchain land registry does not create a duplicate Blackacre.

"SMART" "CONTRACTS"

"The first thing we do, let's kill all the lawyers."[156] While crypto-enthusiasts have yet to incite murder, there have been many wild claims of the impending disruption of the legal profession.[157] 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 work.

Definitely Maybe Contracts?

At a *technical* level, smart contracts can be described as self-executing ledger-modification instructions, e.g. "if X occurs, send Y amount of tokens from account A to account

[155] Marko Vukolić.
[156] William Shakespeare, Henry VI, Part 2, Act IV, Scene 2.
[157] Selva Ozelli (12 January 2018), "Smart Contracts Are Taking Over Functions of Lawyers: Expert Blog", *Cointelegraph* at https://cointelegraph.com/news/smart-contracts-are-taking-over-functions-of-lawyers-expert-blog.

B." There are, however, dozens of inconsistent definitions and descriptions,[158] with completely unrelated concepts being subsumed under this term. Depending on the context, smart contracts may be synonymous with ERC20 tokens, [159] Distributed Applications on Ethereum, [160] Hyperledger Fabric's ChainCode,[161] "stateful executable objects" hosted on a blockchain[162] or simply "programs that can be deployed and run on a blockchain."[163] The original definition associated the term with the embedding of legal terms in hardware and software to prevent breach or to control assets by digital means.[164] Interestingly, despite the fact that this definition is still being referred to, it seems to be gradually losing its relevance – to the point of being ignored. Although the original definition (and the paper it derives from) can be accused of multiple simplifications and an undisciplined use of legal terms, at least it attempts to "position" smart contracts within the legal arena, i.e. it does not treat them as purely technological phenomena. In contrast, many newer definitions regard smart contracts as virtually synonymous with distributed applications. As a result, each instance of a smart contract must be analyzed *in casu* and, as in the case of blockchains, legal analyses must refrain from making generalizations about smart contracts. For example, it seems illogical to inquire *"are smart contracts enforceable?"* because each smart contract is different and may have no legal implications whatsoever. Each discussion of the term must commence with a

[158] Vitalik Buterin, 'Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform' (2015) (https://github.com/ethereum/wiki/wiki/White-Paper); Fan 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

[159] The point is mentioned at para 3 above.

[160] For an overview of Distributed Applications , see: https://www.stateofthedapps.com (last accessed 1 August 2018)

[161] 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 1 August 2018)

[162] Ivica 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)

[163] XU 1

[164] Nick Szabo, "Smart Contracts: Formalizing and Securing Relationships on Public Networks" (1997) 2 (9) *First Monday* no page numbers; for a broader review of smart contracts see: Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real-World Complexity' (2017) 9 Law, Innovation & Technology 269

determination whether - in a particular context - the smart contract in question has or purports to have legal effects.

The common misconception that "smart contracts" displace or exist independently of the law derives in part from the confusion in terminology and in part from the assumption that the technical characteristics of blockchains, decentralization and trustlessness in particular, somehow place them outside of the purview of traditional legal instutions. It is increasingly recognized, however, that for "smart contracts" to gain commercial relevance, they must be legally enforceable. It is, of course, illogical to inquire about the legal status of "blockchain-based code" or "stateful objects on the blockchain." Whether a particular "smart contract" gives rise to a legally binding contractual arrangement depends the type of "smart contract." Their legal status can only be contemplated if such "contracts" purport to embody or execute legal rights and obligations. In such instance, it must be assumed that the usual rules relating to contract formation apply.

It becomes immediately apparent that, from the perspective of contract law, there are no legal obstacles to "smart contracts." Its trite law that intention can be expressed in any manner.[165] A contract can be formed orally or by conduct, it can be expressed in words (either spoken or written), Morse code or in computer instructions. There are also no legal obstacles with regards to the second prerequisite of enforceability, consideration.[166] Consideration need not be adequate, it only needs to be sufficient in the eyes of the law.[167] The focus is on reciprocity, not on equivalence of value. The parties can exchange money in return for goods or services, or bitcoins in return for music download.[168] More importantly, there are also no

[165] Andrew Phang, ed. *The Law of Contract in Singapore* (Singapore: Academy Publishing, 2012) 418: 'Unless otherwise provided-for, generally by way of statute, the common law does not impose any requirements as to formalities or the manner of execution of a contract for such agreement to be legally binding.'
[166] *Currie v Misa* (1875) LR 10 Ex 153.
[167] *Chappell & Co. Ltd. v. Nestle Co. Ltd.* [1960] A.C. 87 (H.L.).
[168] I bypass the question whether bitcoin is legal tender, sale or barter.

legal obstacles to automating the performance of contractual obligations.[169] The possibility of automating transactions or expressing contractual intention by means of automated processes has been expressly recognized by e-commerce regulations, such as the United Nation Convention on the Use of Electronic Communications in International Contracts [170] or the U.S. Uniform Electronic Transactions Act.[171] Similarly, the Australian Electronic Transactions Act 1999 (Cth) ("ETA"), confirms the ability to form contracts by electronic means. Section 8 states a transaction is not invalid merely because it took place by means of electronic communication. Section 15C provides that a contract formed by the interaction of an automated message system and a natural person, or the interaction of automated message systems, is not unenforceable purely for the absence of direct human involvement. An "automated message system" includes a computer program, without review or intervention by a natural person each time an action is initiated or a response generated by the system.

The main obstacle would be one of intent. Why would the parties draft a legal contract exclusively or even primarily in code? Machine language is not the native language of most contracting parties and it is more likely that they negotiated an agreement in a natural language before translating it into code than vice versa. It is possible that some parties in some circumstances might prefer the code to be authoritative but it seems unlikely that most parties in most circumstances would be similarly inclined, much less all parties all of the time.

Executing Performance?

[169] R Nimmer, 'Electronic Contracting: Legal Issues' (1996) 14 *J Marshall Journal of Computer & Information Law* 211.

[170] See: Convention on the Use of Electronic Communications in International Contracting, Nov. 23, 2005, U.N. Doc. A/60/21, Article 12: A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability solely on the ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

[171] See UETA comment 1 to Section 14, which confirms that contracts can be formed by machines functioning as electronic agents for parties to a transaction. It negates any claim that lack of human intent, at the time of contract formation, prevents contract formation. When machines are involved, the requisite intention flows from the programing and use of the machine.

It is often stated that smart contracts reduce transaction costs by eliminating intermediaries, reducing the need to trust third parties and shielding from counterparty risk by technologically guaranteeing performance. In doing so, the legal profession would be disrupted. The ability to guarantee performance is often referred to as "self-enforcement." Purportedly, as the code of the smart contract is executed by the blockchain, it is no longer necessary to rely on traditional, legal institutions of enforcement, such as courts. Code is deterministic and impartial, and hence superior to human judges, who are unpredictable, expensive and biased. There is a tendency to conflate the "execution" of code with "enforcement" of contract and its "performance", a conflation built on top of the confusion between "rights" and "records".

Apart from the transfer of native, on-chain assets, few contractual obligations can be automated or executed "by" a smart contract. Although it is often thought that fiat money can be transferred on a blockchain, this is doubtful without the introduction of a central bank issued cryptocurrency.[172] Smart contracts are often seen as perfect vehicles for the automation of interest rate swaps or other derivatives. They could, for example, be used "to encode the terms of the swap, import information from a rates provider, and automate payments from the parties' accounts,"[173] providing all parties with "transactional transparency." 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.[174] The underlying assumption is that in most circumstances smart contracts cannot exist "on their own" but require an underlying, traditional legal agreement. In this sense, they serve to automate *some* of its obligations. In such event, however, there is a risk that the code of the smart contract does not match the underlying

[172] See text accompanying nn xxx.
[173] Jenny Cieplak & Simon Leefatt, "Smart Contracts: A Smart Way To Automate Performance" (2017) 1 Geo L Tech Rev 417 at 420
[174] Jeremy Sklaroff, "Smart Contracts and the Cost of Inflexibility" (2017) 166 Univ Pennsylvania L Rev 263

obligation, be it due to a failure to correctly translate natural language into code or due to a failure to capture the original contractual intent. The question arises: in the event of such discrepancy, which one prevails? The underlying agreement or the self-executing code? Abstracting from the broader question whether the encoding of contractual terms into deterministic code is possible and desirable,[175] three technical and one practical problems must be highlighted.

First, if a smart contract is to automate and *guarantee* performance, it must have access to the means of performance, i.e. the asset to be transferred when the contractual conditions are met. Blockchains, such as the original bitcoin blockchains or Ethereum, can ensure performance only if such performance consists in the transfer of their native tokens. As indicated, neither permissionless nor permissioned blockchains can control assets or events existing or occurring outside of them. 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 be able to proclaim to the world that I own that cup of coffee. 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 invocation and remain locked until payment. Logically, such "solution" seems impracticable as it excludes value from the system until the smart contract executes.[176] Given the origins of the blockchain in the post-Lehman Brothers financial crisis, this attitude is unsurprising. But credit is neither good nor evil. Properly deployed, credit can help an economy to grow but many within the crypto-community are obsessed with perfect performance at all costs.

[175] Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real-World Complexity' (2017) 9 *Law, Innovation & Technology* 269 at 294; Karen 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

[176] Ivica 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

Second, smart contracts must also have access to off-chain information to determine whether payment is due. It must be remembered that blockchains cannot "see" or validate anything that happens outside of them. As indicated above, 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."[177] This is why external verifiers, so-called "oracles," are required. In principle, oracles are service providers who confirm – on the basis of external data sources – the occurrence of off-chain events, including contractual performance.[178] Upon such event, an oracle provides its digital signature on the relevant unlocking script that controls the tokens to be transferred. While oracles seem like a simple solution to a complex technical problem, they annihilate the "trustless" and "decentralized" character of permissionless blockchains by creating dependencies on external entities and information sources.[179] Again, the use of oracles assumes the existence of legal agreements regulating their use.

Third, as smart contracts are computer programs, they are susceptible to programming errors, both accidental (which are statistically inevitable) and intentional. As smart contracts control value in the form of crypto-currencies or tokens, there are financial incentives to create and exploit such errors. The open source character of many smart contracts is irrelevant as it is extremely difficult to establish how a smart contract will operate without actually running it. The ability to inspect the code does not guarantee its quality. Moreover, the decentralized character of permissionless blockchains does not change the fact in order to trust the code of the smart contract we must trust its coder. The problem is particularly prominent in the case of Ethereum, where everybody can (theoretically) create a smart contract and make it available

[177] XU 6.
[178] Fan 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
[179] Eliza Mik, 'Smart Contracts: Terminology, Technical Limitations and Real-World Complexity' (2017) 9 Law, Innovation & Technology 1 at 296

on the blockchain. The resulting security challenges are frequently highlighted in technical literature.[180]

Finally, non-lawyers often underestimate the difficulties of contract drafting. Many contractual disputes arise out of unforeseen events. This is because neither the parties nor their legal advisers can predict the future. Unless coders have this special ability, unforeseen events will plague "smart contracts" as they have regular legal ones. Even when various possibilities can be foreseen, it is not necessarily easy to get parties to agree on how risk is to be allocated between them. Open ended terms can help parties to overcome these difficulties in order to reach an agreement.[181] However, machine language does not accommodate such a messy "solution". How can you code for "reasonable care" or "best efforts" or "good faith"? If such often-used legal terms cannot be coded, what can they be replaced with? If the choice is always between strict liability and no liability, the outcome will very often be no contract. Even if parties somehow manage to reach agreement, the loss of ambiguity means also that greater precision is required but that greater precision comes at a price. The more complex the code, the more statistically likely it is to contain programming errors (bugs). Bugs are not a problem if debugging is an option but many members of the crypto-community worship at the altar of "immutability". "Immutable" bugs are a pestilence.

CONCLUSION

Despite the general tenor of this paper, it should not be assumed that we are either technophobic or somehow anti-blockchain. In the right circumstances, and with the appropriate awareness of the technology's strengths *and* limitations, both blockchain databases and "smart contracts" may be valuable tools to both law and commerce. In some instances, this will require the adjustment of established rules of law in order to leverage the benefits that these technologies

[180] See generally: Loi Luu, et al., "Making smart contracts smarter," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp 254–269

[181] See Mark P Gergen, "The Use of Open Terms in Contract" (1992) 92 Col L Rev 997.

may offer. However, half-blind prophecies of an "immutable" blockchain utopia will not do and it is essential that both lawyers and technologists learn from each other before jumping to conclusions about an impending blockchain revolution. If indeed there is a potential impending revolution, half-baked attempts to hurry it along may precisely doom it to failure. Pausing the blockchain legal revolution may thus best ensure that we leverage the most of these exciting new technologies.