Published on 31 October 2018

THE LEGAL PROBLEMS SURROUNDING BLOCKCHAINS

A Basic Overview

[2018] SAL Prac 13

Eliza **MIK**[*]
LLM (University of Warsaw), LLM (University of Sydney), PhD (University of Sydney);
Assistant Professor of Law, Singapore Management University, School of Law.

I. Introduction

1 In the overheated atmosphere surrounding blockchain technologies, predictions of what "might be" are difficult to distinguish from actual commercial applications. It is also difficult to discern the relevant characteristics of blockchains, those that require legal or regulatory attention. This paper sketches a number of important blockchain-related concepts that will facilitate the identification of legal issues that *could* arise in this area. It emphasises that it is impossible to generalise and provide advice without a thorough understanding of the underlying technologies and *the blockchain in question*. The paper commences with some definitional problems and introduces the crucial distinction between permissioned and permissionless blockchains. Next, it demystifies three terms that underlie the common belief that blockchains will revolutionise commerce: "validation", "immutability" and "smart contracts". The paper assumes that understanding the legal implications of a technology is predicated on an understanding of its characteristics. Compared to the sensationalistic descriptions of blockchains encountered in the press, its contents will appear somewhat dry.

* The author wishes to express her gratitude for the research assistance provided by Mr Dylan Mah.

II. A definitional problem

2 There is no single, accepted definition of *a* blockchain and no agreement as to which attributes are indispensable for something to be a blockchain.[1] In principle, blockchains are distributed databases, or data structures, that are maintained by a network of geographically dispersed computers, or "nodes". By definition, blockchains are made of interconnected blocks, each block containing a list of all prior transactions. The creation of each block requires a significant amount of computation ("mining"). To create a block and append it to the blockchain, each node (*ie*, participant in the network) must provide a "proof-of-work": a piece of data which is computationally difficult to produce but easy to verify. As these computations are extremely expensive in terms of electricity, it is more economical to produce valid blocks (*ie*, follow the rules) than to attempt to change previous blocks (*ie*, break the rules). Given the cost and difficulty of retrospectively changing existing blocks, the possibility of a transaction being altered or reversed is infinitesimal.[2]

3 There are 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, synchronised data stores.[3] Some blockchains have been designed for specific purposes or industries; others are generic in nature.[4] In the light of these differences, each legal analysis must be preceded with an inquiry as to the type of blockchain in question. Arguments

1 See generally Angela Walch, "The Path of the Blockchain Lexicon (and the Law)" (2017) 36 *Review of Banking and Financial Law* 713.

2 Andreas M Antonopoulos, *Mastering Bitcoin* (Sevastopol: O'Reilly, 2nd Ed, 2017) at p 196.

3 Roger Maull *et al*, "Distributed ledger technology: Applications and implications" (2017) 26(5) *Strategic Change* 481 at 483.

4 The permissioned ledger Ripple was developed to support the banking and finance industry, whereas Hyperledger Fabric supports the collaborative development of blockchain-based distributed ledgers for a wider range of industries and transaction types.

made in relation to one blockchain may lose their validity in the context of another. Generalisations are dangerous. It is also crucial to differentiate between different applications or use cases of blockchains. They range from asset registries and provenance tracking to supply chain management and transactional platforms. To date, blockchains have raised concerns regarding the legal categorisation of cryptocurrencies[5] (such as bitcoin or Ether) and fundraising-tokens (such as the ERC-20 token standard).[6] While the bitcoin blockchain serves as a useful point of reference as it embodies the original features of the technology, it must be remembered that other blockchains have grown in popularity and that their commercial deployment may lead to legal problems going beyond securities and banking regulations.

III. The main distinction: Permissioned and permissionless blockchains

4 Legal analyses must distinguish between permissioned and permissionless blockchains,[7] the main criterion being whether the nodes processing transactions are pre-defined or unrestricted.[8] "Processing" denotes the ability to view, create,

5 In the case of permissionless blockchains based on the proof-of-work, cryptocurrencies incentivise miners to maintain the ledger. Technically, they are only required in permissionless blockchains given their decentralised nature. The legal status of cryptocurrencies, which are often described as "digital assets" or a cryptographically-secured medium of exchange, is controversial: see generally Kelvin F K Low & Ernie G S Teo, "Bitcoins and other cryptocurrencies as property?" (2017) 9(2) *Law, Innovation and Technology* 235.

6 The ERC-20 token standard enables so-called Initial Coin Offerings, or "ICOs". There are different types of tokens, some of which may classify as securities.

7 There are blockchains that do not fall into either categorisation as they constitute a hybrid model.

8 Florian Glaser & Luis Bezzenberger, "Beyond cryptocurrencies – A taxonomy of decentralized consensus systems" (2015) (Paper presented at the 23rd European Conference on Information Systems (ECIS), Münster, Germany.)

validate and/or add transactions to the blockchain.[9] Sometimes, permissioned ledgers are treated as synonymous with private and permissionless with public blockchains.[10] 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. The said differentiations are not, however, made consistently. Permissionless blockchains are restricted by their ideological underpinnings – they are *supposed* to be open, anonymous, decentralised and free of external interferences. In contrast, permissioned blockchains are more malleable and respond to actual, commercial needs. Consequently, it is easier to make broader assumptions about permissionless blockchains while each permissioned blockchain must be analysed *in casu*.

A. Permissionless blockchains

5 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.[11] Permissionless blockchains typically involve a native cryptocurrency, which serves as an incentive mechanism to produce blocks.[12] They also

9 Daniel Drescher, *Blockchain Basics: A Non-Technical Introduction in 25 Steps* (Apress, 2017) at p 216.

10 Roy Lai & David Lee Kuo Chuen, "Blockchain – From Public to Private" in *Handbook of Blockchain, Digital Finance, and Inclusion* vol 2 (David Lee Kuo Chuen & Robert Deng eds) (Academic Press, 2017) at p 147.

11 Xiwei Xu *et al*, "A Taxonomy of Blockchain-Based Systems for Architecture Design" 2017 *IEEE International Conference on Software Architecture (ICSA)* 243.

12 Miners are incentivised 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

(*cont'd on the next page*)

often rely on a consensus algorithm based on the "proof-of-work".[13] The latter guarantees the "trustlessness" of the entire system. The reasoning is that one can trust the code alone, without having to trust a centralised 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. It is often overlooked, however, that the technology is created by humans. To trust the code, one must trust those who wrote the code. Claims regarding the trustlessness of permissionless blockchains must thus be approached with scepticism. Moreover, permissionless blockchains are generally transparent, with their entire contents visible to everyone. Such total transparency is, however, undesirable whenever the information recorded on the blockchain must be kept private and confidential, be it due to contractual or legal requirements.

B. Permissioned blockchains

6 In contrast, permissioned blockchains, such as Hyperledger Fabric or Quorum, limit access and transaction processing to identified participants who subscribe to system rules.[14] As the participants are known and bound by agreement, there is no emphasis on "trustlessness" and no need to rely on computationally intensive consensus algorithms. Generally, there is also no need for a native currency. This type of blockchain restricts who can participate in the consensus mechanism and/or transact on the blockchain. Permissioned blockchains also enable selective transparency, so that access to

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 M Antonopoulos, *Mastering Bitcoin* (Sevastopol: O'Reilly, 2nd ed, 2017) at p 26.

13 See generally Vitalik Buterin, "On Public and Private Blockchains" *Ethereum Blog* (6 August 2015).

14 David Yermack, "Corporate Governance and Blockchains" (2017) 21 *Review of Finance* 7 at 16.

information can be limited to specific participants. Permissioned blockchains are typically intended for enterprise use and unconstrained by ideological underpinnings.

C. The key difference: Decentralisation

7 Permissionless blockchains are by definition decentralised, with no single entity being able to control access to or the operation of the system, while their permissioned cousins assume the presence of one or more entities that "manage" the system. Despite idealistic undertones, decentralisation results in an inherent lack of accountability and governance. For example, bitcoin's consensus algorithm prescribes the rules of generating and transferring crypto tokens but does not contain any rules that determine how to change the algorithm or how to create further rules.[15] The problem has important practical implications concerning the need to upgrade the code, be it to correct errors or to adapt it to new circumstances.[16] Absent a clear governance structure, it is unclear who has the authority to make or change the rules.[17] Setting the rules in advance and making them immutable by encoding them in the blockchain does not guarantee their quality or future adaptability. No blockchain can be created perfect "on arrival". All computer programs undergo constant improvements.[18]

8 In contrast, permissioned blockchains generally assume the existence of an external governance structure and recognise

15 Mark Abramowicz, "Cryptocurrency-based Law" (2016) 58 *Arizona Law Review* 359 at 368.

16 This became visible during the recent block-size debate, which concerned the need to increase block size to enable better transaction processing capabilities. See generally Michael J Casey & Paul Vigna, *The Truth Machine* (Harper Collins, 2018) at p 72.

17 Odysseas Sclavounis, "Understanding Public Blockchain Governance" (7 May 2017) <https://blockchainreview.io/public-blockchain-governance/> (accessed 13 August 2018); this problem was brought to my attention by my colleague Marco Crepaldi.

18 An example of such process are the almost weekly Microsoft Office updates, which continually improve the codebase of the individual Office applications.

the need to amend the contents of a given blockchain and/or the underlying consensus mechanism. In permissioned blockchains, the participants are typically bound by real-world agreements that address such matters. Interestingly, even Vitalik Buterin, the creator of the permissionless Ethereum blockchain, admits that permissioned blockchains have multiple advantages, such the ability to change the rules, reverse transactions or ensure confidentiality. Buterin insists, however, that the benefits of permissioned blockchains lie in their "philosophical virtues", such as freedom and openness.[19] Leaving aside the question whether such "virtues" are commercially indispensable, it can be predicted that the use of permissionless blockchains will be accompanied by disputes concerning attempts to alter their contents or their underlying algorithms. It can also be suspected that absence of a governance structure to improve permissionless blockchains and/or to adapt them to specific purposes might hinder their mainstream adoption.

IV. Misunderstanding "validation"

9 Technical literature often mentions 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 necessary, however, to understand what validation means from a technical perspective, *ie*, what is being validated and against what criteria. In the bitcoin blockchain, transactions and blocks are the subject of validation. In the legal context, a transaction is associated with an exchange. 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

19 Vitalik Buterin, "On Public and Private Blockchains" *Ethereum Blog* (6 August 2015).

signed data structure expressing a transfer of value"[20]. Blocks contain lists of transactions. To be included in a block, all network nodes must confirm (*ie*, "validate") that each transaction is correctly structured, uses previously unspent inputs and contains sufficient transaction fees.[21] Nodes must also confirm that the unlocking scripts match the corresponding locking scripts.[22] Once a transaction is aggregated into a block, the block itself must be verified by a process called mining. Mining is related to the concept of decentralised consensus, *ie*, 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.[23] Subsequently, each newly mined block is validated by every node against certain *technical* criteria, which include establishing that its data structure is syntactically correct, the block header hash is less than the target (*ie*, 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.[24]

10 The list of validation criteria is extensive and illustrates the divergence between the technical aspects of the process and the legal understanding of the term. The foregoing description also demonstrates that "validation" denotes an automated,

20 Andreas M Antonopoulos, *Mastering Bitcoin* (Sevastopol: O'Reilly, 2nd ed, 2017) at pp 18–19.

21 Andreas M Antonopoulos, *Mastering Bitcoin* (Sevastopol: O'Reilly, 2nd ed, 2017) at pp 24–25.

22 For a detailed description of validation criteria, see Andreas M Antonopoulos, *Mastering Bitcoin* (Sevastopol: O'Reilly, 2nd ed, 2017) at pp 218–219.

23 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* (Sevastopol: O'Reilly, 2nd ed, 2017) at p 228.

24 Andreas M Antonopoulos, *Mastering Bitcoin* (Sevastopol: O'Reilly, 2nd ed, 2017) at p 238.

deterministic process of confirming that certain technical requirements have been met. It concerns the fulfilment of technical parameters that relate to on-chain events, *eg*, that the account has sufficient "funds" to spend and that the correct private key (or multiple private keys in case of multisig scripts) has been used to initiate the transaction (*ie*, spend those funds). The validation process cannot confirm real-world events, *eg*, whether the payment was actually due, whether the parties had legal capacity or whether the contract underlying the transfer of funds was legally enforceable. The background of the transaction is never the subject of validation, or the reason why certain tokens were transferred from one account to another can never be established by the underlying consensus algorithm. In sum, the technical meaning of "validating transactions" is unrelated to the legal meaning of "establishing the validity of a transaction".

V. Problems surrounding "immutability"

11 Blockchains are often described as immutable. As anything that is inscribed into a block cannot be erased or reversed, blockchains are portrayed as a perfect record-keeping technology, creating certainty and permanence as well as "keeping track of things in a reliable and trusted way".[25] There are, however, numerous problems with the term. First, the word "immutable" must not be used to describe all blockchains because not all blockchains share this attribute. In permissioned ledgers certain participants may have the right to alter the contents of a block as well as the underlying consensus mechanism. Second, "immutability" implies that something is not capable of change. In practice, however, the two most prominent permissionless blockchains, Ethereum and Bitcoin, have been changed by means of forks and remain at risk of 51%

25 Angela Walch, "The Path of the Blockchain Lexicon (and the Law)" (2017) 36 *Review of Banking and Financial Law* 713 at 737.

attacks.[26] Third, immutability is often mistaken for veracity or authenticity. The fact that something is recorded in a blockchain does not, with few exceptions, guarantee its truth or correctness. Statements that the blockchain provides a "single source of truth" are misleading. The data recorded in a blockchain may be false because it might have been entered erroneously or as a result of fraud. Blockchains, like other records, may not correctly reflect reality.

12 More importantly, a permissionless blockchain can only correctly reflect on-chain events, *ie*, the generation and/or transfer of native tokens or cryptocurrencies.[27] After all, only transactions (in the technical sense) are validated by the underlying consensus algorithm. As indicated, the correctness, occurrence and/or authenticity of events occurring outside of the blockchain, *ie*, off-chain, *cannot* be confirmed.[28] In such instance, the quality of the information recorded in the blockchain depends on the trustworthiness of the entity providing such information. Moreover, when a blockchain records the transfer or creation of assets existing in the real world, such as land or shares, it becomes necessary to devise a technology of tagging and subsequently mapping such assets onto blockchains *and* to contractually agree that such mapping will be regarded as authoritative. Even then, however, the blockchain can only record who *should* own the off-chain asset but cannot control or guarantee its actual physical location or lawful possession. In sum, given that the immutability of the

26 Bitcoin forked into two separate ledgers in March 2013; due to a bug in the code Ethereum famously split into two as a result of the Decentralized Autonomous Organization hack.

27 The security of the blockchain is largely attributable to the fact that it is, technically, insulated from outside interferences. As a side effect, the blockchain cannot see anything that happens outside of it.

28 One must differentiate between the recording of transactions in blocks and recording other information in a block. In the former instance, the transaction depends on the blockchain to determine its validity; it occurs "within it", such as when some bitcoins are transferred between accounts. In the latter, the "empty space" within a block is used to record other information, ranging from text to graphics and video files. This "operation" is made possible by encoding hex values into "fake" bitcoin addresses.

record does not guarantee its correctness, this particular feature of *some* blockchains may not be their main selling point.

VI. Problems surrounding smart contracts

13 Another problematic concept is that of a "smart contract". At a *technical* level, smart contracts can be described as self-executing ledger-modification instructions, *eg*, "if X occurs, send Y amount of tokens from account A to account B". There are dozens of inconsistent definitions and descriptions,[29] with completely unrelated concepts being subsumed under this term. Depending on the context, smart contracts may be synonymous with ERC20 tokens,[30] Distributed Applications on Ethereum,[31] Hyperledger Fabric's chaincode[32] or "stateful executable objects" hosted on a blockchain.[33] The original definition, which associated the term with the embedding of legal terms in hardware and software to prevent breach or to control assets by digital means,[34] seems to have gradually lost its relevance. As is the case of blockchains, each smart contract must be analysed *in casu*. Consequently, it seems illogical to inquire *"are smart contracts enforceable?"* because each smart contract is different and may have no legal implications

29 Vitalik Buterin, "Ethereum White Paper: A Next Generation Smart Contract and Decentralized Application Platform" (2015) <https://github.com/ethereum/wiki/wiki/White-Paper> (accessed 13 August 2018); 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.

30 The point is mentioned at para 3 above.

31 For an overview of Distributed Applications, see <https://www.stateofthedapps.com> (accessed 1 August 2018)

32 Hyperledger Architecture, Volume II, "*Smart Contracts*" (April 2018) at p 8.

33 Ivica Nikolic *et al*, "Finding the Greedy, Prodigal, and Suicidal Contracts at Scale" (2018) <https://arxiv.org/pdf/1802.06038.pdf> (accessed 1 August 2018).

34 Nick Szabo, "Smart Contracts: Formalizing and Securing Relationships on Public Networks" (1997) 2(9) *First Monday*; 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.

whatsoever. Despite these conflicting approaches, it is often generalised 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 a narrow, legal sense, one could posit that smart contracts automate payment obligations.

14 Apart from the payment of money or the transfer of a digitised asset, few contractual obligations can be automated or executed "by" a smart contract. Unsurprisingly, 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",[35] 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.[36] In the event of conflict, which one prevails? What if the code failed to capture contractual intent? Abstracting from the broader question whether the encoding of contractual terms into deterministic code is possible and desirable,[37] three technical problems must be pointed out.

A. Access to means of performance

15 *First*, if a smart contract is to automate and *guarantee* performance, it must have access to the means of performance, *ie*, the asset or token to be transferred when payment conditions are met. Blockchains, such as the original bitcoin blockchains or

35 Jenny Cieplak & Simon Leefatt, "Smart Contracts: A Smart Way To Automate Performance" (2017) 1 Geo L Tech Rev 417 at 420.

36 Jeremy Sklaroff, "Smart Contracts and the Cost of Inflexibility" (2017) 166 U Pa L Rev 263.

37 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* 1 at 11.

Ethereum, can ensure performance only if such performance consists in the transfer of their native tokens. Neither permissionless nor permissioned blockchains can control assets or events existing or occurring outside them. This means, however, that all such 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.[38] In other words, performance can only be *guaranteed* if it takes the form of tokens which are native to a particular blockchain and if such tokens are taken out of circulation until they are due.

B. Access to information about performance

16 *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 them. This is why so-called "oracles" are required, *ie*, service providers who confirm – on the basis of external data sources – the occurrence of off-chain events, including performance.[39] 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 decentralised character of permissionless blockchains by creating dependencies on external entities and information sources.[40] Again, the use of oracles assumes the existence of legal agreements regulating their use.

38 Ivica Nikolic *et al*, "Finding the Greedy, Prodigal, and Suicidal Contracts at Scale" (2018) <https://arxiv.org/pdf/1802.06038.pdf> (accessed 1 August 2018) at 5.

39 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.

40 Eliza Mik, "Smart Contracts: Terminology, Technical Limitations and Real World Complexity" (2017) 9 *Law, Innovation & Technology* 269 at 296.

C. Bugs in the code

17 *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 cryptocurrencies 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 decentralised character of permissionless blockchains does not change the fact that 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 on the blockchain. The resulting security challenges are frequently highlighted in technical literature.[41]

VII. Concluding observations

18 Aside from the aforementioned technical "deficiencies" of many permissionless blockchains, another general point must be made. It is generally underappreciated that, from a technical perspective, blockchains are databases. They record certain events, such as the generation or transfer of cryptocurrencies or other "digital assets". Otherwise, they have limited computational capabilities. For blockchains to become commercially useful, their functionalities must be extended. This in turn requires adding protocol layers *on top* of them.[42] It is thus necessary to see blockchains as one element in a larger ecosystem, which includes components that may not necessarily

41 See generally Loi Luu *et al*, "Making smart contracts smarter" (2016) *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* 254.

42 This design reflects the concept of "separation of concerns", which dictates that the individual functions of a program (*eg*, presentation, business logic, data) be independent from each other to optimise their performance.

share their characteristics, such as trustlessness, security or immutability, *etc*. Legal analyses must not focus exclusively on the blockchain but examine the entire system and acknowledge its complexity. Lawyers and regulators alike must not assume that the technical meaning of a word seamlessly maps onto its legal meaning or indiscriminately trust in the promises made in technical literature.

19 Once the actual meaning of certain blockchain-related terms becomes apparent, the actual use cases of permissionless blockchains seem limited. In particular, immutability, coupled with the absence of clear governance structures, seems detrimental for many commercial applications. No organisation or commercial relationship can be governed exclusively by algorithms. Blockchains require an external governance process enabling the network participants to make decisions about the network. Deploying blockchains as rights registries or tools for provenance tracking requires the ability to change the record and, more importantly, to identify the rights holders.[43] These features are, however, notably absent in permissionless systems. It can be anticipated that permissioned blockchains will be more useful from a commercial perspective. They will also create fewer legal problems than their permissionless equivalents as their use will be limited to sophisticated, identifiable parties who will use the blockchain on the basis of prior agreement. For the time being, lawyers and regulators must resign themselves to examining different blockchains and fine-tuning their analyses to specific technological features. They must also be ready to include computer scientists and programmers in their discussions.

43 Chris Reed *et al*, "Beyond BitCoin – Legal impurities and Off-chain Assets" (2018) 26(2) *International Journal of Law and Information Technology* 160 at 171.