Computer Code as Law: A New Frontier?

Author : Sarah Green

Date : August 5, 2019

Karen Yeung, Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law, 82 **Mod. L. Rev.** 207 (2019).

As distributed ledger or “blockchain” technology continues to offer decentralised and distributed decision-making, Yeung considers the way in which those automated processes (code as law) are likely to interact with conventional means of governance (code of law). This technology is based on peer-to-peer verification of transactions: it takes various forms, but the common theme is that the record of transactions is shared with all users of a given system, and transactions only make it on to that record after a fierce process of mathematical ratification. As a result, the intermediaries on which transactions have for so long depended, such as banks, clearing houses and property registries, are no longer required. Altruism and self-interest are aligned because all users have a vested interest in the continued integrity and success of the closed system, and third party intervention is neither required nor (for many users, at least in principle), desired.

Distribution and decentralisation are the crucial components of distributed ledger technology, and are the principle features which distinguish them from those forms of electronic payments which use intermediaries and electronic bank money, such as Paypal, WorldPay and BACS, for example. These characteristics also explain why cybercurrencies are often described as “trustless”, meaning that transacting parties need not have any trust for one another in the real world, so long as they trust the payment protocol (which, for reasons which will soon become apparent, they probably should). Decentralisation in this context simply means that everyone who might want to use the currency, and so has a copy of the relevant software, also has a copy of the ledger. The ledger is a record of *every* transaction made using that currency, and each computer operating the software (known as a node) has a copy of the entire thing: from the beginning (the “Genesis Block”) to today’s latest block. This is where the term Distributed Ledger Technology (DLT) comes from: Blockchain, which was created to underpin Bitcoin, was the first distributed ledger, but there are now distributed ledgers of several different forms. Common to every one, however, is the idea that all participants have access to the full history of transactions made using that protocol. This is a novel way of dealing with the ages-old double spend problem. Historically, the challenge of how to prevent double spending has been met in two ways: the first is by using physical tokens, whose corporeal form physically prevents their being spent more than once, and the second is by employing an independent third party, such as a bank, to keep a record of transactions and their effects on the subsequent spending power of the parties involved. Cybercurrencies achieve the same thing by sharing information with every user and by ensuring that the information so shared is perfectly synchronised. This way, “coins” cannot be spent twice because everyone would know that this is what was being attempted, and the consensus necessary for validation and recording would not be reached. Security is thus achieved through complete transparency, and distributed ledgers have no need for any centralised record-keeping, nor for any third party intermediary to verify the integrity of transactions.

Such transparency is achieved through what is known as distributed consensus protocol, and this is characterised by two features:

1. All computers on the network (referred to as nodes) must agree on which transaction data is ultimately recorded on the ledger
2. The transaction data must have been generated by an honest node

The question remains how any of this can be achieved. One method, used by Bitcoin, is known as proof-of-work, and

this allows nodes to reach a consensus on which transactions to record and in which order to do so. (The order is of course all-important, as it is with any spending pattern, since what you have already spent determines how much you can spend in the future.) Proof-of-work is the means by which nodes persuade other nodes that the block of transactions that they wish to add to the chain is legitimate and should be trusted. The work involved here is the cryptography: the solving of a mathematical puzzle, and this puzzle is of a very specific type: the optimum way of solving it is simply to work through very large numbers of trial and error iterations. In other words, lawyers might say that it is a difficult case, but not a hard one. It is clear what needs to be done, but doing it takes an immense amount of computational power simply to work through the many repetitions of the same calculation, each time trying a different input. Once this happens, the proposed block gets added to the chain and the transactions in it get confirmed. This, however, is not the only thing which happens when the block gets verified. Another of Bitcoin's revolutionary qualities is its alignment of self-interest with altruism. Verifying blocks is hard grind and very expensive in computational terms, and yet it is essential to the continuation and security of the system. So, when a node successfully adds a block to the chain, it gets rewarded with bitcoin. In the Bitcoin protocol, the verification process is known as mining, and is simultaneously the means by which new coin is minted. This is a system, therefore, in which self-interest works in favour of the collective interest, and the two are mutually reinforcing.

The ethos underlying these technological developments (particularly that of Bitcoin) is that peer-to-peer transactions should be able to avoid the intervention of intermediaries or external regulators. In Yeung's view, the belief that blockchain systems are capable of operating outside of conventional law rests on two assumptions: first, that conventional state legal systems are rendered redundant by the alternative governance frameworks offered by distributed ledger technology and, second, that the state will not intervene in these alternative modes of governance because it has no interest in doing so. Yeung makes it clear from the outset that the notion of a self-contained cybertopia in which national laws hold no sway is not likely to be realised: whilst the genius of blockchain technology allows for exceptionally high transactional security, it can do nothing to guarantee the wraparound rights that conventional law protects and upholds, such as security of personal integrity, property and dignity.

Yeung sets out three models of potential interaction between conventional law and blockchain systems, which she labels "cat and mouse", "the joys of marriage" and "uneasy coexistence and mutual suspicion". The first of these arises in a context in which blockchain systems are used deliberately to try and evade the reach of conventional law; a form of cyber-anarchy which provokes the state into asserting its sovereignty in some substantive way. Yeung's prediction is that this will not take the form of wide-ranging, high-level regulation, but will instead occur on a more localised, ad hoc basis as individual "mice" are identified and reined in. So, for instance, a state is unlikely to allow the formation and enforcement of private contracts which exploit inequalities of bargaining power between commercial entities and consumers. Once attention is brought to any such arrangements, national law is very likely to step in and subject such transactions to some form of regulation, as it commonly does with conventional contracts.

The "joys of (patriarchal) marriage" model describes a situation in which the supremacy of conventional law is ultimately recognised, and in which there is a mutual commitment to co-operation between the two available modes of governance and decision-making. This refers to a situation in which parties transacting by means of distributed ledger technology do so in order to take advantage of the efficiencies of that medium, rather than with any desire to evade regulation and accountability. In such circumstances, their agreements will recognise and accommodate the restrictions imposed by national laws. For example, parties making a contract on a blockchain platform for software development services might code into their agreement a means of granting one party a compensatory amount of cryptocurrency in the event of a breach by the other party. This recognises the authority of national law, but does not require the intervention of a judge or court.

Finally, Yeung's "uneasy coexistence" refers to a situation in which there is mutual suspicion from both sides, but in which intervention from national law enforcement will only occur where there is a threatened or perceived harm to third parties. This account reads like something of a hybrid of the previous two models: there is no express avoidance of national law by contracting parties, but neither is there an open or willing accommodation of its authority. Instead, both parties and national authorities warily keep tabs on each other, interacting only when is necessary for the prevention of

unacceptable risk or loss.

Underlying the uncertainty of regulation and dispute resolution in this context is the constantly-evolving technological foundation on which it all sits, and the challenges this presents to established “bright line” boundaries between the private and public legal spheres. Should blockchains be regulated? Or should individual private disputes be resolved on an ad hoc basis? Yeung predicts that, ultimately, both code of law and code as law will have to provide some form of combined solution by finding an equilibrium which, like any other legal construct, balances the creation of value with the prevention of harm. Brave new technology invites brave new ideas.

There is a certain inevitability in this combined outcome: the impetus behind the development of autonomous code was the desire to achieve pure peer-to-peer interaction, but it is naïve to think that anyone, however technologically literate, can unilaterally contract out of states’ legal jurisdiction. The ability of parties to design their own dispute resolution processes could be a very welcome means of reducing transaction costs, judicial time and what can sometimes be a long wait for an appropriate remedy. It must, however, be a process within a process; reflecting the objectives, constraints and policies of the wider legal landscape of which it forms part. The efficiencies and advantages of coded agreements should, in other words, enhance individuals’ rights but not to bypass them.

Cite as: Sarah Green, *Computer Code as Law: A New Frontier?*, JOTWELL (August 5, 2019) (reviewing Karen Yeung, *Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law*, 82 **Mod. L. Rev.** 207 (2019)), https://torts.jotwell.com/computer-code-as-law-a-new-frontier/.