BLOCKCHAIN, SMART CONTRACTS AND LAWYERS

ANDREAS SHERBORNE
DECEMBER 2017

Blockchain, Smart Contracts and Lawyers

Andreas Sherborne

Blockchain is a disruptive technology – it has the potential to radically change how we interact and transact with others. This transformative potential is no less true for the legal profession, especially with the advent of 'smart contracts' which automatically execute coded contractual terms without requiring a lawyer. Much of the work traditionally completed by lawyers may therefore be automated in the near future. What does this mean for the legal profession? This article navigates the unchartered terrain of nascent blockchain technology and its applications as well as their consequences for lawyers.

Blockchain – a distributed, immutable ledger

A great deal of hype surrounds blockchain. It receives considerable media attention, both positive and negative, and is often the subject of heated debate amongst individuals, corporations and governments alike. Bitcoin, as just one application of blockchain technology, is particularly controversial, as are other cryptocurrencies. Other blockchain applications, such as Ethereum, have also become more prominent in recent years. As this technology becomes more mainstream, it is important to understand its defining features.

Blockchain is a decentralised, immutable ledger operating on cryptographic technology between a peer-to-peer network of computers ('nodes').[1] In simpler terms, it is a book of records (a ledger) that lists transactions of value[2] between individuals. Everyone who is part of the network has an exact copy of that book of records, and can see all the transactions listed within it.[3] When a new transaction is made, the book is automatically updated for all members of the network.[4] In this sense, it is 'decentralised' – no single authority controls, maintains or monitors the record book. This decentralisation of control is the ground-breaking and game-changing aspect of blockchain technology. It challenges and disrupts the status quo because it removes the services of intermediaries and central authorities.

Historically, when it comes to transferring money or assets, we have relied on trusted third parties such as banks and governments. These intermediaries are responsible for a range of tasks related to transactional processes, including authenticating transfers and keeping records. The need for intermediaries is particularly important when making digital transactions. Digital assets, such as money, stocks, and intellectual property rights, are essentially digital files and are therefore very easy to reproduce. This creates the 'double spend problem' – where the same unit of value can be spent more than once – and has thus far prevented the direct transfer of digital assets. Requiring

[1] Satoshi Nakamoto, 'Bitcoin: A peer-to-peer electronic cash system' (Bitcoin Project Whitepaper, 2008) <https://bitcoin.org/bitcoin.pdf>.

[2] Transactions of value are not just monetary transactions or a narrow range of financial transactions. They may include transactions involving goods and property, the ownership of ideas, the casting of votes, or proving the existence of a document. Evidence of blockchain's broad application is demonstrated by Everledger, which is a distributed registry of diamond ownership and provenance (as well as other valuable assets) and helps in combatting crime and fraud.

[3] Blockchain networks can be private with restricted membership (known as 'permissioned blockchains') or they can be accessible to any person in the world ('unpermissioned blockchains'). There are also 'consortium blockchains' where the process of validating transactions is controlled by a fixed set of nodes.

[4] This means the members can always determine who owns what assets, and how much of each particular asset.

intermediaries also adds inefficiencies to the transactional process, both in terms of time and cost, and the centralised databases of records are particularly susceptible to breach.[5]

Blockchain solves the double spend problem. When a digital transaction is made, it is grouped together in a cryptographically protected block[6] with other transactions made in a particular window of time.[7] The members of the network are presented with that block and compete with each other to validate the authenticity of the transactions by using their computers to solve complex coded problems.[8] Significant computational power is necessary to complete these problems.[9] To incentivise users to expend that computational power, an economic reward is given to the user who first solves the problem (a Bitcoin blockchain network member, for example, will receive newly minted bitcoins).[10] Once authenticated by consensus, the block of transactions is timestamped and added to a chain (hence 'blockchain') in a linear, chronological order. New blocks of verified transactions are linked to older blocks,[11] creating an immutable chain that shows every transaction made in the history of that blockchain. The entire chain is continually updated and synchronised so that every ledger in the network is identical, giving each user the ability to prove who owns what assets at any given time.

Blockchain's decentralised, transparent and cryptographic nature allows people to trust each other and transact directly, subsequently making the need for intermediaries obsolete. There are also significant security benefits associated with this technology. A criminal would need to hack into the most recently cryptographically protected block, as well as all of the proceeding blocks,[12] and do this for every ledger in the network simultaneously – a feat that is virtually impossible.[13]

By enabling the digitisation of assets and their frictionless transfer, blockchain is driving a foundational shift from the internet of information, where users instantly receive and communicate information, to the internet of value, where users instantly exchange value in an economy where trust is

[5] These 'honeypots of data' attract hackers. Largescale information hacks of centralised databases controlled by major organisations has increased at an alarming rate in recent years. For example, DrobBox, Uber and Ebay have all been the subjects of hacks. See <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>.

[6] Blockchain uses cryptographic hash functions. The information grouped in the block is 'hashed'. Bitcoin uses SHA-256, Ethereum uses Keccak-256.

[7] For the Bitcoin blockchain, this window is 10 minutes.

[8] This consensus model is called 'proof of work'. Other consensus models are 'proof of stake' and 'closed consensus'.

[9] These members use computers that are much more powerful than the average laptop and can complete millions of computations per second ('hash rate'). This affords them an advantage when competing to solve consensus problems for reward. The specialised hardware is expensive and consumes a lot of energy to run (see Alex Hern, 'Bitcoin mining consumers more electricity a year than Ireland' 27 November 2017 *The Guardian* <https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumes-electricity-ireland> and Nicole Kobie, 'How much energy does bitcoin mining really use? It's complicated' 2 December 2017 *The Wired* <http://www.wired.co.uk/article/how-much-energy-does-bitcoin-mining-really-use>. It is also becoming more common for members ('miners') to pool their resources together and to split the economic reward between them. SlushPool, AntMiner and BTCC Pool are examples of large 'miner pools'.

[10] This process is known as 'mining', and the members of the network completing the coded problems are called 'miners'. There is cap on the amount of bitcoin at 21 million.

[11] Each block in the chain (except the very first, a 'genesis block') has a pointer to the block before it in the form of the hash of the previous block's header.

[12] At the time of writing, there are 500,421 blocks in the Bitcoin blockchain. See, https://blockexplorer.com/.

[13] If a group of hackers ('attacker nodes') controlled 51 per cent of the computational power of the network, they would, in theory, be able to control the blockchain and manipulate the transactions recorded on the blocks (known as a '51 per cent attack'). Additionally, quantum computers may be capable of performing the computational processes necessary to hack a blockchain, see Divesh Aggarwal et al., 'Quantum attacks on Bitcoin, and how to protect against them' Cornell University Quantum Physics, <arXiv:1710.10377>. However, this technology is immature and such capabilities are at least a decade away from being developed, see Masoud Mohseni, Peter Read and Hartmut Neven, 'Commercialize Early Quantum Technologies' (2017) 543 *Nature* 171.

established not by central intermediaries but through coded protocol, network consensus and cryptography.

Blockchain and legal services

Blockchain technology is likely to transform the professional legal services industry. Blockchain applications may be used for effecting the service of documents and providing a digital platform for confidential information sharing which is useful for discovery and due diligence. Blockchain also has the potential to digitise registries, such as those recording title of land and property,[14] and to facilitate the exchange of ownership without requiring intermediaries (such as lawyers to draft legal title exchange documents). Utilising the immutable storage capability of blockchain technology also means it can provide authentication services which could be of significant practical application in securing the integrity of evidence used in courts.[15] Furthermore, as the full capabilities of blockchain technology in the legal sector are not yet known, it is likely that many changes are unforeseeable as yet. However, it is clear that smart contracts integrated with blockchain technology have significant disruptive potential. This forms the focus of the remainder of this article.

Smart contracts – automatically executed contracts bound by computer protocol

Smart contracts are agreements, written in code, which automatically execute programmed functions in response to certain conditions being fulfilled. In other words, once action A occurs, it will trigger the performance of action B – similar to the way a vending machine works. If you insert money into a vending machine and choose a product it will trigger the release of that product. If you do not insert enough money, the product will not be released and the transfer aborted. This is the simplified idea underlying smart contracts.

This concept is not novel, but with the integration of blockchain technology, smart contracts have the potential to automate and guarantee the performance of a great variety of obligations without the need for a central authority, legal system, or external enforcement mechanism. Blockchain applications leveraging this technology are already being used, most notably Ethereum,[16] which is a decentralised virtual machine that executes peer-to-peer contracts. Blockchain technology also confers considerable security benefits,[17] and is both transparent and efficient.

Smart contracts have a number of potential applications. They could be used to transfer settlement funds between parties upon the performance of a defined obligation, such as a corporate acquisition or property purchase, or for automatically making payment upon delivery of goods or services. They are also particularly useful for exchanges of shares, bonds and options and for micro-financial

[14] Sweden has trialled a blockchain based title registry. See, Joon Ian Wong, 'Sweden's blockchain-powered land registry is inching towards reality' 3 April 2017 *Quartz* <https://qz.com/947064/sweden-is-turning-a-blockchain-powered-land-registry-into-a-reality/>.

[15] Blockai, Monegraph, and Verisart all utilise distributed ledger technology to allow users to create permanent records of digital content such as photographs and text, which help to protect copyright and allow for the storage of original, authentic materials digitally.

[16] Ethereum is a decentralised platform that runs smart contracts using blockchain technology. See 'Ethereum Homestead Documentation' <http://www.ethdocs.org/en/latest/>.

[17] Identical, immutable and cryptographically protected copies of the smart contract are stored across the blockchain network.

transactions. In these cases, smart contracts bring clarity, predictability, auditability, and ease of enforcement to contractual relations while mitigating the risks associated with human involvement.

Smart contracts using 'blockchain oracles' (digital agents that find and verify information in real time for use by a smart contract)[18] may allow for the encoding of more sophisticated contracts. For example, home flood insurance encoded as a smart contract may automatically release payment to the policy holder when an oracle verifies that flooding has occurred (e.g., by access to official meteorological records (a 'software oracle'), or a flood detection device installed at the home (a 'hardware oracle')).[19] Furthermore, a will written as a smart contract may automatically distribute the assets of the estate upon an oracle verifying the death of the testator or testatrix by accessing the blockchain registry of births, deaths and marriages.[20] In both of these examples, the execution of the smart contract occurs automatically upon the trigger event being verified in real-time by a blockchain oracle. This significantly improves efficiency as contracts can be performed instantly and without the services of third parties.

Although blockchain based smart contracts have significant potential to automate and guarantee a range of legal functions, their utility may be limited by a number of factors which impede their wide-scale adoption and use. Until these issues are squarely resolved, a possible near-term application of smart contracts is perhaps for legal contracts to remain drafted in natural legal language, but for certain actions to be automated using smart contracts.

Smart contracts and the law

Smart contracts do not fit neatly within the existing traditional legal frameworks of many jurisdictions. As such, their purported use in automatically performing and guaranteeing legal obligations raises a number of difficult legal questions.

Clause as code – the challenge of encoding contracts

Code is deterministic – when a particular input is given, the programmed output will always be the same. The programming language underlying smart contracts is no different. This means that smart contacts must be drafted using structured and unambiguous language readable by computers. For certain legal agreements, such as 'A shall pay £10 to B on 1 January 2018', this is unproblematic.

However, many contracts are not as straightforward because they contain legal concepts and expressions that are difficult to translate to code. A clause, for example, that triggers certain consequences in the event of 'material adverse change' is not easily inserted as code into a smart contract. The fundamental legal concepts of 'good faith', 'negligence' and 'reasonableness' are also very difficult to encode. These concepts are employed for the very reason that they give contracting parties flexibility in respect of certain obligations by not specifically determining in advance exactly what those obligations entail. Translating legal contracts into code as self-executing programs would mean losing much of the functionality of traditional legal language. As such, smart contracts perhaps have a restricted application specifically limited to those types of contracts which are easily executed, but not for those contracts which require greater nuance in their functioning.

---

[18] See, for example, Oracalize, <http://www.oraclize.it/>.

[19] For a more detailed description of how insurance policies may be effected using smart contracts, see Tim Roughton, 'Applying blockchain to insurance contracts' 4 May 2017 *Out-Law* <https://www.out-law.com/en/articles/2017/may/applying-blockchain-to-insurance-contracts/>.

[20] See, for example, My Wish, <https://mywish.io/index.html>.

A solution to this problem may be to generate a 'hybrid' or 'split' contract, whereby only certain terms of the contract are encoded, and which requests human input for those clauses which require a legal mind.[21] In the future, artificial intelligence and natural language computing may also overcome this barrier.[22]

Smart contracts – are they really contracts?

Despite their name, smart contracts are not always strictly *legal* contracts.[23] The laws of many jurisdictions take a flexible approach to formalities (such as the form of a contract), but at a minimum, a legal contract must include the elements of offer, acceptance, and intention of the parties to enter into a legal agreement.[24]

The recognition of smart contracts as legally binding is therefore crucial to ensuring that the outcome of a smart contract self-executing is legally effective and enforceable by the parties in a court of law. If, for example, it is deemed that a smart contract cannot legally pass title of an asset that it purports to transfer, then much of the potential utility of smart contracts would be lost.

A solution to this problem may be to draft a traditional legal contract and 'translate' it to code, so that the legal contract acts as a 'wrapper' to the automatic performance of the legal obligations executed by the smart contract.[25] This could be achieved by requiring the contracting parties to accept natural language terms that confer binding contractual effect on the transaction performed by the code (by, for example, clicking "I agree" to a set of terms). The smart-contract would then be 'launched' and self-execute with legal effect pursuant to the coded terms. Consequently, with steps taken to ensure the legal formalities and elements constituting a contract are satisfied, it is very likely that a smart contract and the outcome of its self-execution could be regarded as legally binding.[26]

Jurisdictional issues

Blockchains transcend jurisdictional boundaries as they exist as a globally distributed network of nodes and are not controlled by a specific entity. Similarly, the execution of a smart contract does not fit conveniently within the traditional basis of territorial jurisdiction. As such, it is difficult to determine which jurisdiction's laws will apply to govern contractual issues related to a particular smart contract, as well as which court will have jurisdiction to hear any resultant legal claims. Uncertainty in this respect may lead to satellite disputes as parties litigate over which jurisdiction's law ought to apply, and the appropriate forum for the claim (e.g., anti-suit injunctions, *forum non coveniens* claims etc.).

Determining the law applicable law to a contract is very important for contracting parties because they must be able to determine with some certainty their potential obligations and liabilities under the contract. As such, overcoming these complex jurisdictional issues is essential to the utility of smart contracts. It may be as simple as ensuring parties include choice of law and choice of court clauses in

---

[21] See Anurag Bana and Maxine Viertmann, 'The Not-So-Distant Future: Blockchain and the legal profession' International Bar Association (February 2017) <https://www.ibanet.org/LPRU/Disruptive-Innovation.aspx>.
[22] Agrello, 'How to Make Smart Contracts Worthy of Their Name Using Artificial Intelligence' 4 May 2017 *Agrello* <https://blog.agrello.org/how-to-make-smart-contracts-worthy-of-their-name-using-artificial-intelligence-3a90e4dd3c47>.
[23] See Josh Stark 'Making sense of blockchain smart contracts' 4 June 2016 *CoinDesk* <http://www.coindesk/com/making-sense-smart-contracts/>.
[24] For a detailed analysis of smart contracts and their place in contract law, see Max Raskin, 'The Law and Legality of Smart Contracts' (2017) 1(2) *Georgetown Law Technology Review* 305, 321.
[25] See Clifford Chance LLP, 'Are Smart Contracts Contracts?' (December 2017) <https://www.cliffordchance.com/briefings/2017/08/are_smart_contractscontracts.html>.
[26] See, in particular, Agrello, which is a blockchain based platform specialising in drafting and coding legally binding smart contracts. <http://agrello.io/>.

the contract so that these issues are pre-determined and agreed upon prior to the launch of the smart contract.

The risk of error and unintended consequences

Although smart contracts are designed to be certain and predictable, they nevertheless remain prone to software bugs and errors. As such, their self-performance may result in unintended consequences. In those cases where a smart contract self-executes in a way that the parties did not anticipate, or a vulnerability in the code is exploited (as in the DAO attack),[27] which remedies will be available, and against whom?

Such problems are compounded by the immutable and irreversible nature of the blockchain. Although the certainty that results from such permanence is a highly valuable feature of blockchain technology, it has the problematic consequence that immutable smart contracts lack traditional error correction capabilities. The program code executing the smart contract cannot be debugged after being stored on an immutable blockchain. It may, therefore, be very difficult to realise corrective justice in such situations. Due diligence of smart contracts will likely become a significant aspect of a lawyer's work to ensure there are no flaws before a smart contract is launched. Perhaps a means of ensuring code is error-free will be to run the smart contract in a simulation in order to test its performance.

Dispute resolution and arbitration

Despite certain advantages of smart contracts, they are not free from disputes arising in relation to their performance. As illustrated above, there are several potential types of disputes – a party may, for example, contest whether a smart contract is in fact legally binding, disagree as to which jurisdiction's law is the governing law, or allege misconduct and seek damages. Given the lack of a central enforcement agency and established precedent, it is difficult to predict with certainty how such issues will be dealt with and resolved. It is therefore advisable that parties include a dispute resolution or arbitration clause when contracting via a smart contract.[28]

The future for lawyers – extinction or evolution?

As automation and digitisation spreads across all industries and sectors of the economy, the question must be asked, how will this affect the legal profession? The creation of self-executing contracts represents a new frontier for lawyers who may find themselves in a rapidly changing legal landscape.

It is very likely that the nature of legal work will change significantly. In the long term, certain practices may be reduced to automation, namely conveyancing and wills and estates, while transactional lawyers will perhaps find a large part of their work can be executed automatically by smart contracts. This, however, does not mean extinction for lawyers. Automation lends itself primarily to those operational tasks which are repetitive and time-consuming, and so it may be that lawyers find themselves with more time to focus on legal issues. Moreover, lawyers will likely be able to take on larger portfolios of work as algorithms efficiently complete high-volume, low-risk tasks. Similarly, previously cost-prohibitive work may become profitable. For example, high-volume, low-value tasks

[27] David Siegel, 'Understanding the DAO Attack for Journalists' 19 June 2016 *Medium* <https://medium.com/@pullnews/understanding-the-dao-hack-for-journalists-2312dd43e993>.
[28] James Rogers, Harriet Jones-Fenleigh and Adam Sanitt, 'Arbitrating Smart Contract Disputes' *International Arbitration Report* (October 2017, Norton Rose Fulbright) 21 <http://www.nortonrosefulbright.com/files/20170925-international-arbitration-report-issue-9-157156.pdf>.

such as micro-transactional work and contract review may become cost-effective. This does, however, mean that perhaps fewer law graduates who traditionally have completed this work as junior lawyers will enter the legal profession.

Lawyers will also need to learn new skills in order to serve the interests and demands of their clients. Indeed, lawyers with programming and coding skills are already in demand,[29] and so it may become more common for legal graduates to have combined their studies in law with STEM subjects or computer science.[30] Given the diverse range of legal relationships, it is likely that lawyers with coding skills will be integral to the drafting of bespoke smart contracts and ensuring due diligence of those contracts. Additionally, as the clients of law firms begin to interact with blockchain applications they will require lawyers who have the requisite knowledge and expertise to navigate the relevant legal and regulatory issues that arise.[31]

Consequently, it is foreseeable that lawyers will still play an important role in the future despite a shift away from the traditional paradigm. As this shift occurs, law firms will need to embrace technology and innovation in order to secure their competitiveness in a dynamic marketplace and to meet the evolving interests and demands of their clients.[32]

Conclusion

Blockchain is certainly a disruptive technology. The many applications of distributed ledger networks will transform the way in which we interact and transact with others in the future. As intermediaries begin to play a diminished role in an increasingly decentralised economy, lawyers will need to adapt to the changing landscape. This is especially true given the advent of smart contracts which have the potential to automate a great variety tasks traditionally carried out by lawyers. Despite this, however, several challenges to the wide-spread adoption of smart contracts mean that the services of lawyers will still be required. These emerging fields and novel questions of law will require the application of human legal minds. Algorithms automating repetitive legal tasks will allow lawyers to focus on pertinent legal issues while expanding their work portfolios. Lastly, law firms will be required to place greater importance on technology and innovation in order to retain a competitive edge in the market.

[29] Yasmin Lambert, 'Company Legal Teams Combine Digital Skills with Law' 2 June 2017 *Financial Times* <https://www.ft.com/content/617ab842-3bcd-11e7-ac89-b01cc67cfeec>. Hoss Layne, 'Understanding the Future of the Law on the Blockchain' 25 October 2016 *Medium* <https://medium.com/the-exofiles/understanding-the-future-of-the-law-on-the-blockchain-a5a661d1cacc>.

[30] For example, Harvard Law School offers the course 'Programming for Lawyers'. See <http://hls.harvard.edu/academics/curriculum/catalog/default.aspx?o=71516>.

[31] See Gabrielle Patricks and Anurag Bana, 'Rule of Law Versus Rule of Code: A blockchain-driven legal world' International Bar Association (November 2017) <https://www.ibanet.org/Document/Default.aspx?DocumentUid=73B6073F-520D-45FA-A29B-EF019A7D7FC9>.

[32] See Romain Keppenne, 'Legal Tech and Other Smart Contracts: What future for legal automation?' 23 May 2016 *Paris Innovation Review* <http://parisinnovationreview.com/articles-en/what-future-for-legal-automation>.