SIMONS MUIRHEAD & BURTON LLP

Blockchain – The Concept and the Law

Authors

Simon Halberstam, Head of Technology Law

Raoul Lumb, Technology Law Associate

Simons Muirhead & Burton LLP

Tel: +44 (0)20 3206 2700

Websites: www.weblaw.co.uk and www.smab.co.uk

TABLE OF CONTENTS

1. WHAT IS BLOCKCHAIN?

‘Blockchain’ software enables the distribution of the task of keeping a ledger across a network, cutting out the need for a central ledger keeper and effectively delegating the task to the users of that ledger. In other words, rather than having a single party keep a record of all of the transactions that happen within a given system, a blockchain shares the task of logging and recording those transactions amongst the people making them, with the underlying technology verifying that all users are keeping matching records.

Advocates of the technology say that it effectively solves the problem of 'trust' across networks, as it enables complete strangers to complete transactions without risk of the participating parties defaulting or failing to pay.

The most well-known (and first widespread) use of a blockchain was to power the famous/infamous bitcoins cryptocurrency, an online 'currency' that enabled its users to pay each other using units of value that existed purely online and without any kind of central bank to oversee their use. The underlying blockchain enabled users of bitcoins,, to issue and safeguard the authenticity of a currency without the need for a central bank, and to allow its users to agree to sell items of value in exchange for it without any fear that the paying party (a) did not in fact own the necessary bitcoins to pay, or (b) that the bitcoins it used were not genuine.

This was made possible by the distribution of the central ledger of blockchain transactions to key users of the system, against which all transactions which were checked for validity. The existence of this reliable decentralised ledger enabled recipients of bitcoins to confirm that they were genuine (as each coin could be verified against the ledger) and safeguarded against the possibility of an unreliable ledger-keeper modifying the ledger to their advantage (as any such attempt would have caused their copy of the ledger to desynchronise with the other copies, thus becoming invalid).

1.1 Property?

It is worth noting that, for the purposes of UK law at least, it is difficult to find any legal grounds that support the classification of crypto-assets that exist only electronically within a blockchain (including, but not limited to, bitcoins) as ‘property’.

To complicate matters further in the case of crypto-currencies, users technically have rights over specific individual units of the currency (i.e. they can point to a particular bitcoins that they personally own) rather than over generic amounts of inter-changeable currency units (e.g. a bank balance) as is the case in a traditional cash-and-banks based system.

Without government regulation specifying that particular crypto-currencies/securities are to be regarded as property (like shares and patents) they remain intangibles which are not technically property and in respect of which damages claims will be exceptionally difficult.

2. USE CASES

Blockchain has myriad potential applications, being deployable to transfer any digital rights or digitisable assets, notably currency, shares and intellectual property. However, it is particularly exciting for entrepreneurs as it enables them to dispense with layers of cost and inefficiency that are often required in order to police trust/authenticity in high value transactions.

2.1 Land Register

For example, to imagine a real life example, at present in the UK a central database of title to estates in real property (or, in plain English: ownership of bits of land) is kept by the Land Registry. Whenever land in the UK is sold, the transaction must be notified to the Land Registry and its records (the 'Land Register') changed to record the new owner. In other words, the Land Registry acts as a central ledger keeper of land transactions.

By moving the data contained in the Land Register onto a blockchain system one could, in theory, remove the need for the Land Registry itself, as its task of logging and recording transactions could be delegated to all owners of land, who would collectively keep copies of the Land Register and update and verify it each time a sale of land took place.

2.2 Financial Transactions

Similar use cases are possible in more complex scenarios, especially those which involve financial transactions and/or international trade, where the presence of ledger keepers such as central stock exchanges and trust-guaranteeing counterparties such as deposit-holding banks could all be considered to represent cost-layers ripe for disruption.

Consider, by way of example, the trading of shares in companies; currently enabled by a system of centralised stock exchanges, licensed brokers and banks. The application of blockchain technology offers the possibility of removing the need for licensed intermediaries and enabling users to buy and sell financial securities directly over a digital medium, entirely eliminating the need for third parties to effect the transaction or to verify the quality of the securities being offered. In a blockchain-enabled system, a user would simply be able to see that a particular party owned, and was offering for sale, the type of security that it was looking to buy, and a transaction could take place in real time whereby both the buyer and seller would be able to have 100% confidence that the security in question would change hands only after payment for it had cleared.

Some have even dared to suggest that the mighty legal profession could be disrupted, with so-called 'smart contracts' automating commercial deals without the need for parties to enter into paper contracts. While the author of this piece fears no machine, the possibility of using blockchains to automate and de-risk simple, standardised and/or high-volume agreements is certainly attractive and represents an obvious use case for the technology.

3. LEGAL RISKS INHERENT TO BLOCKCHAIN SOFTWARE

While the distributed, indelible, tamper-proof ledgers that blockchains enable solve a number of practical problems, they also raise a number of legal issues.

We are not positing that there are fundamental flaws in blockchain technology that render it unfit for purpose, but rather that, as with all new technologies, new methods of working raise new risks and challenges for all parties.

3.1 Irrecoverability and Irreversibility

The most obvious risk inherent in blockchain technology is the fact that the ledgers it creates are indelible and irreversible. No change to the collective ledger can be made without the agreement of all ledger keepers, which prevents a lone actor from reversing or correcting a transaction without unanimous agreement. While on a practical level that key feature of blockchains enables them to 'solve' the issue of untrustworthy users of a network and is one of their major selling points, it also gives rise to the system's most obvious Achilles heel, the ability of untrustworthy users to hide behind the technology and evade remedial enforcement after deceiving or defrauding others.

By way of example, consider a situation whereby A has masqueraded as a trustworthy individual (say, a member of an overseas royal family) and persuaded B to transfer an electronic asset (a bitcoins or any other intangible) to him via a blockchain system, perhaps by offering a payment in cash (outside the blockchain) which then never arrives. In usual circumstances B would, on discovering the fraud, have the option of seeking a court order to compel A to return his property to him. Should A refuse to comply, then either (a) bailiffs could be dispatched to seize and return the property in question, or (b) where the goods were intangible and their transfer tracked on a centralised ledger, the ledger keeper could be ordered to simply reverse the record of the transaction and restore the relevant goods to B.

However, in a blockchain scenario, neither of the above courses of action is workable; there is nothing physical for bailiffs to seize and no central ledger-keeper to reverse the transaction. Without the cooperation of A, the inbuilt security features of the blockchain prevent the return of B's property.

Similarly, consider a situation whereby A compromises and unlawfully gains access to B's account on a blockchain-enabled system and, having done so, arranges a series of transactions with C. On discovering those transactions, B must either persuade C to reverse them, or seek a court order to have them reversed. At that point B runs into the same issues of irreversibility noted above. Further, while from a legal perspective C's title to stolen property would be dubious, in a blockchain-enabled system his title to the relevant assets cannot be reversed or labelled invalid by a central ledger keeper, nor can the assets be removed from his possession by an enforcer of the court's will such as a bailiff.

In both situations there remains the possibility of B suing A (or possibly C) for the cash value of the relevant assets, assuming that B and/or C are not insolvent, or of having A or C imprisoned for contempt of court (should they refuse to obey an order to reverse the relevant transactions) but neither of those remedies solves the problem that B will have lost the original asset and probably cannot get it back without counterparty co-operation. As noted above, seeking a cash equivalent of the asset may be impossible, or simply an unsatisfactory remedy; and while having A or C imprisoned may make B feel better, it won't restitute the original asset.

3.2 Pseudonymity and Trust

Identity deception is another trust issue which may undermine blockchains. 'Pseudonymity' connotes that whereas a party's online identity can be verified, its offline identity is unverifiable.

While it is fair to note that pseudonymity is a problem for all online networks (be they commercial in nature or otherwise) and not unique to blockchains, the issue is one of particular significance for ‘open’ networks (those that do not have a gatekeeper to regulate access and to verify the identities of the parties entering them) and for networks that seek to facilitate valuable transactions.

A fundamental appeal of blockchain-based systems is that they enable network ‘trust’, allowing users of open networks to rely on other members of that network doing what they have promised to do e.g. making payments or releasing assets. This reliance often entails disintermediation, with the parties not engaging or involving third parties (escrow agents, deposit holding banks or lawyers). Such third parties would, in usual circumstances, be expected to perform their own due diligence and verify the identities of the parties taking part. This approach exposes the parties to identity-fraud.

Pseudonymity has obvious risk implications when coupled with the issues of irreversibility noted above.

Advocates of blockchain technology will of course argue that security safeguards can be put in place to verify identities in real time and to prevent unauthorised access to accounts, but the world is yet to see a failsafe system for achieving either aim.

3.3 Illegal and Anti-Social Activities

Pseudonymity, as well illustrated by the “Silk Road”, facilitates money laundering and trade in illicit articles such as narcotics and offensive weapons.

Clearly, bitcoins represents an extremely early and unsophisticated example of a blockchain-enabled network, and one would anticipate better gate-keeping solutions in the future.

3.4 Smart Contracts – the beginning of the end for lawyers?

A very interesting corollary of blockchain technology are self-executing contracts or, at least, self-executing contractual provisions. In this context, there is much discussion about Ethereum which is a decentralized blockchain platform capable of running smart contracts.

These “smart” contracts are encoded programs and applications which enable automated performance of contract provisions. Because we are dealing with blockchain, this self-execution should run without any third party intervention whatsoever. For example, if the blockchain registers that A has transferred a particular digital asset to B, the associated smart contract may trigger a notification to B’s bank that it should transfer the agreed monetary consideration from B’s bank account to A’s.

However this pans out, there is a range of legal issues that arises from the deployment of smart contracts. For example, what happens with the “cooling off” period in consumer contracts? We have already considered the irreversibility issue above.

Similarly, if the offline event triggered by the smart contract goes wrong or does not happen for whatever reason, what are the remedies of the “wronged” party? In a traditional contract, rescission would be the likely solution, putting both parties back into their original pre-contractual positions. However, with blockchain, this will not be viable.

As technology lawyers, we do not feel threatened by the advent of smart contracts. Someone still needs to draw up the terms of the contract which is then encoded and someone needs to check that the encoding is an accurate representation of those terms. Thus, it would seem that rather than usurp the legal function, it will mean more co-operation between lawyers and programmers. Heaven forfend, lawyers may even have to contemplate becoming competent programmers themselves so that they can cover both aspects and increase their practice domain.

4. PRIVACY

Flowing directly from concerns about situations that can arise where the users of a blockchain network are anonymous/pseudonymous, come the concerns about the legal implications for blockchain networks in which users are not, i.e. systems in which users' offline identities can be easily deduced from their online handles (or where offline identities and online handle are one and, the same). How can such a system, which relies upon a full and frank record of all transactions made across it being made available to all users, ever adequately ensure user privacy?

That question goes to the heart of the user privacy standards with which companies operating in Europe are obliged to comply as a result of the Data Protection Act 1998 (and EU equivalents) and, in time, the General Data Protection Regulation.

In the UK, companies are obliged by the Data Protection Act to ensure that any 'Personal Data' (data from which users can be personally identified) which they collect is kept securely, is not subject to 'further processing' by unauthorised third parties, and is stored for no longer than is reasonably necessary.

How any of these aims could be achieved in a system that relies upon granting full access to all users' transaction records to all other members of the network (or, at least, all ledger keepers in the network) and making sure that those records are held permanently and indelibly is unclear. For example, consider the possibility of a blockchain-enabled system that enabled transactions between businesses and consumers, and in which all parties were personally identifiable; how would the blockchain's operator meaningfully bar users of the network from mining the ledger's record of transactions for data on similar transactions made by third parties? Such mining would represent 'unauthorised processing' of the data, but the fact that it could then be sold on, or used for undesirable activity such as direct telemarketing by the processor could represent a further breach.

Contractual undertakings extracted from users of the system might alleviate the problems. For example, commitments by network members to use secure, encrypted environments, to use the data solely for operation of the chain and for no longer than strictly necessary for the purposes of the transaction.

However, the duration of retention issue is particularly complex as blockchain ledgers should be permanent and indelible which flies in the face of the data protection stance.

The only way to cut the Gordian Knot would appear to be to make users pseudonymous and not personally identifiable on the blockchain. However, as noted above, this raises its own issues.

Obviously, the privacy concerns are lesser where a system is designed solely for business-to-business use but there could still be major confidentiality considerations.

5. REGULATION

For entrepreneurs considering launching blockchain ventures, the simple newness of the format renders it inherently vulnerable to changes in the regulatory environment. It is worth noting that jurisdictions such as Bolivia have banned the use of crypto-currencies within their territories and that many others have heavily regulated the use cases for blockchain systems.

Such regulations will proliferate if the use of blockchain technology becomes more widespread. This is especially so if such technology disrupts the gate-keeping function of regulated entities such as banks and law firms which serve, amongst other things, to protect consumer interests and transactional integrity.

Furthermore, those intending to apply blockchain technology to financial services, healthcare and the processing of personal data can expect their current regulatory burden to increase exponentially.

6. CONCLUSION

We are not suggesting that blockchains cannot and/or will not be used heavily in the future for a wide range of commercial purposes. The technology is compelling and has the ability to streamline and disrupt a wide range of industries. However, as with all new technologies, it does not solve all existing problems and creates many of its own.

Finally, machines and smart-contracts have not yet managed to eradicate lawyers (or cockroaches) entirely, so entrepreneurs considering launching innovative blockchain / distributed ledger businesses would be well advised to consult reputable legal advisers before launching their ventures, especially if their malevolent intention is to disrupt harmless, incumbent professionals.

Further Information

For further information, please contact the authors

Simon Halberstam

Tel: +44 (0) 20 3206 2781

Email: Simon.Halberstam@smab.co.uk

or

Raoul Lumb

Tel: +44 (0) 20 3206 2791

Email: Raoul.Lumb@smab.co.uk