the global voice of the legal profession®

Blockchain technology: Is it building a brighter future?

Jane Ellis, Anurag Bana, Christian Decle

IBA Legal Policy & Research Unit

December 2016

Acknowledgements

The Legal Policy & Research Unit (LPRU) would especially like to thank Pradyumna Soni, Marina Kofman and Giselle Williams for their contributions in the preparation of this report.

Introduction

The invention of a revolutionary encoding or cryptographic technology known as 'blockchain' is already central to a significant proportion of business-to-business (B2B) and business-to-consumer (B2C) commerce, legal products and processes.

From online purchasing to medical data and prescription management, data sharing of cross-jurisdictional criminal records to possibly even management of entire countries' registers and notarisations,[1] this technology has huge potential.

But with this potential to develop in as yet undefined ways and into various unregulated areas, is the risk that ethical boundaries defining our basic rights to ownership, privacy and access to justice may be crossed.

At the core of this ethical challenge is not the technology itself, but the speed at which it is being taken up and used. We need to pause, identify the spread of blockchain's applications and regulate accordingly. This report will examine the technology underpinning blockchain, its various applications and the functional realities that are often overlooked.

Either way there is no turning back: the ship is now leaving safe waters, and we will not be able to stop its inevitable voyage into the digital unknown.

What is blockchain technology?

Blockchain is a chronological database of transactions recorded by a network of computers. Through a decentralised public ledger and a cryptographic mechanism, blockchain facilitates transactions that are sufficiently secure between two parties. Every new transaction carries an unforgettable record of the entire history of the chain and all previous transactions. Put simply, it is a ledger to which anyone can add a transaction but no one user can remove any information.

1 James Burnie and Andrew Henderson, 'Blockchain: mitigating or aggravating regulatory risk?' (2016) 5 Journal of International Banking and Financial Law 293

In a blockchain, each set of transactions is encrypted and organised into smaller datasets called blocks. Every block contains data about the relevant transaction, references to the preceding purchases, that form the block in the chain and an answer to a complex mathematical puzzle, which is used to validate the data associated with that particular block.

To ensure that only authentic transactions are recorded as a block, the network – that is all the other devices that hold the same version of the block – must confirm that any new transactions are valid, and therefore do not invalidate any former transactions.

The new block is added to the end of the existing series of blocks only after the network of computers and/or devices reach consensus (that is, 51 per cent) as to the validity of the transaction, thereby can proceed in forming a blockchain.

Once a block has been successfully added to a blockchain, it can no longer be deleted and becomes a permanent and immutable record of the transactions contained within it. This can be accessed and verified by everyone on the network.

Far-reaching applications of blockchain

Blockchain has already been used to make cryptographic tokens. These are a kind of electronic key that may be used in place of, or in addition to, a password, and can represent property or ownership, censorship-resistant communications and file sharing systems, decentralised domain name management systems (DNS) and fraud-resistant digital voting platforms.

Blockchain technology may also be used in 'smart contracts' – that is, computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts may, among other things, be used for:

- capital markets trading;
- real property and intellectual property transfers (including for digital rights management);

- energy grid management;
- insurance claims processing; and
- logistics and supply chain management.

Originators of blockchain envision other innovative uses, such as systems for the music business that packages both artists' rights management and their royalty payments together. This would be combined with a blockchain to secure the complex ownership data, and which will then automate all of the financial issues with regard to who's owed what.[2]

Blockchain is also likely to change the way lawyers approach contract drafting, administration and enforcement. And given that contract law is embedded into most commercial enterprise, there are very few areas that will escape its application. Already we see it being used in the following areas.

Bitcoin

One of the foremost applications of blockchain technology has been in digital currencies such as Bitcoin. Bitcoin is a virtual currency that relies on a decentralised blockchain. Based on a peer-to-peer creation and validation system, Bitcoin has a circulation worth over US$1.5bn. While it attracts headlines, Bitcoin and other virtual currencies present a number of risks that drive the need to regulate them closely. They are volatile: virtual currencies are not pegged to a real currency; depend entirely on technology; pose a potential threat to global money supplies, and due to their anonymity they risk being used as a cover for criminal activity.

2 Scott Rosenberg, 'How Bitcoin's Blockchain could power an alternate Internet' (Back Channel, 13 January 2015) <https://backchannel.com/how-bitcoins-blockchain-could-power-an-alternate-internet-bb501855af67#.e217pq0v2> accessed 7 December 2016

Banks

Blockchain has already found a place among the financial technology ('fintech') sector's general pattern of disruptive innovation.[3] Advocates of blockchain claim that it will reduce costs, improve service delivery and streamline digital processes. Banking group Santander's fintech investment fund calculates that use of the technology could slash settlement, regulatory and cross border payment costs by US$20bn each year.[4]

Such savings could be possible due to blockchain's decentralised distributed ledger technology. It has the potential to remove the need for any intermediaries, thus allowing parties to transfer their assets much quicker and at reduced cost. Perhaps unsurprisingly, this poses a significant threat to any financial institutions that are slow to adapt or ignore this technology completely.

Some banks and financial institutions are already investing millions of dollars in developing and testing blockchain technology, so as to incorporate it into their e-commerce and crypto-currency strategies. In January 2016 the Australian Stock Exchange (ASX), for example, announced the development of a distributed ledger solution to replace its current platform for clearing and settling trades.[5] Similarly, the Bank of America recently told reporters that it was filing a number of US patents, in relation to protecting its own blockchain-related inventions.[6]

In August 2016, it was reported[7] that four of the world's biggest banks – UBS, Deutsche, Santander and BNY Mellon – had teamed up to develop a new form of digital cash they believe would become an industry standard to clear and

3 See *'Times are a-changin': disruptive innovation and the legal profession*, International Bar Association's Legal Policy & Research Unit (2016), available at www.ibanet.org/LPRU/Disruptive_Innovation_.aspx.

4 'Blockchain Game Changer, Part 2: Adapting the technology of Blockchain', (Mason Hayes & Curran, 06 April 2016) <www.mhc.ie/latest/insights/blockchain-game-changer-part-2-adapting-the-technology-of-blockchain> accessed 07 December 2016

5 ASX Selects Digital Asset To Develop Distributed Ledger Technology For The Australian Equity Market'', (ASX Media Release, 22 January 2016) <www.asx.com.au/documents/about/ASX-Selects-Digital-Asset-to-Develop-Distributed-Ledger-Technology-Solutions.pdf.> accessed 07 December 2016

6 Arjun Kharpal and Julia Chatterley, 'Bank of America is going big on blockchain' CNBC Tech Transformers (6 November 2013) <http://www.cnbc.com/2016/01/28/bank-of-america-is-going-big-on-blockchain-plans-to-file-20-patents.html> accessed 7 December 2016

7 Martin Arnold, 'Big banks plan to coin new digital currency' Financial Times (23 August 2016) <http://www.ft.com/cms/s/0/1a962c16-6952-11e6-ae5b-a7cc5dd5a28c.html> accessed 7 December 2016

settle financial trades using blockchain technology. They are aiming for a limited and low-risk commercial launch by early 2018.

Smart contracts

The process of drafting contracts will likely change dramatically when smart contracts become common place. Smart contracts will be self-executing, meaning that once conditions A and B take place and are verified by the blockchain, the cryptocurrency will be automatically unlocked, becoming immediately controlled by the other party. These transactions are virtually irreversible for all their demonstrable verifiability and this will be compounded when we consider the pseudo anonymous nature of the participants in these types of transactions.[8]

Initially, there may be workarounds,[9] in the form of built-in arbitration mechanisms. These may at least permit the transaction to be reviewed under traditional legal systems. Such mechanisms, however, will need to be engineered into the code of individual smart contracts at their drafting stage.

Similarly, there will be a need to incorporate mechanisms to address issues such as intellectual property, confidentiality, governing law and choice of law.

The entire coding process will be very different to drafting extensive and lengthy contracts using traditional templates and editing with a word processor; smart contracts are likely to be drafted with a handful of lines of code such as:

```
#include credit library

#include blockchain library

Var Debtor = ABC Corp.

Var Creditor = ABC Lender
```

8 Joe Dewey and Shawn Amuial, 'Blockchain technology will transform the practice of law' (Bloomberg, 25 June 2015) <https://bol.bna.com/blockchain-technology-will-transform-the-practice-of-law> accessed 7 December 2016

9 Workaround refers to a method or a technique in place to circumvent a problem without eliminating it.

New Document = new Credit Agreement.create {debtor:Debtor, creditor:Creditor, type:working capital}

New Document.interest = Libor(30 day)

Very quickly, we will see code 'libraries'[10] being established, which will develop uniformity and overall user and client confidence in the use of smart contracts. We might presume that there would then be an 'app' for the coding and use of smart contracts.[11] This could mean significant transactional savings and an expedited pace at which parties can close deals and move their money.

To demonstrate the simplification of process and financial benefits that could be made to both lawyer and client, consider the example of the management of an estate by an elderly father, who wishes to divide his estate equally to his children upon his death. A lawyer might code a trust in accordance with the father's intentions and upload it onto the blockchain. The contents of this blockchain would be algorithmically encrypted into an alphanumeric string to uniquely identify the trust. A program coded onto the trust would scan an online death registry, which, upon the father's death, would immediately trigger a search of financial registries for each of the children, thereafter dividing the equity of the estate to each child accordingly. The estate would be disbursed, almost immediately, in accordance with the father's wishes with no need for the estate to be revisited by a lawyer or to pass through any probate office.[12]

Insurance

A recent Deloitte paper on the use of blockchain suggests it may have use beyond simply facilitating payments.[13] In the context of insurance, it can be used to review claim history, thereby preventing multiple claims arising from the same incident. Additionally, using the internet of things (IoT)[14] to incorporate

10 Ibid.
11 Application software designed to run on smartphones and other mobile devices.
12 See note 5.
13 Alexander Shelkovnikov, 'Blockchain applications in insurance' (Deloitte, 2016) <https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/innovation/ch-en-innovation-deloitte-blockchain-app-in-insurance.pdf> accessed 07 December 2016
14 Nicole Kobie, 'What is the internet of things?' The Guardian (6 May 2015) <http://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google> accessed 7 December 2016

insured items into the blockchain, it could provide an automatic transfer of cash from an insurer for repairs when the item is broken. Decentralisation could see huge reductions in fraudulent claims, which already cost the sector £1.32bn (US$1.74bn) across all insurance products.[15] It could also help to identify instances of fraud, through the establishment of a public, tamper-proof database to track ownership and transfer of assets – including property and valuables.

In creating a digital history of assets, insurers and insurance companies alike could see significant savings in the streamlining of payments of premiums and claims. For example, the company Everledger[16] uses blockchain technology to provide a permanent ledger for the certification and transaction history of individual diamonds. The users of Everledger are able to know who owns which diamond, and where it is at any given point in time. It can trace the movement of diamonds across platforms such as eBay or Amazon, working together with insurers when diamonds are reported as stolen locally, and with organisations such as Interpol and Europol when diamonds have crossed borders or entered onto the black market.

Decentralisation of corporate and political governance systems

The role of blockchain in decentralisation

Many functions of our daily lives are managed through centralised systems of government, be it local, sovereign state or federal. Within these systems are further centralised structures operating in business or in the public sector – central banks, utilities, service and food supply chains, legislation and the judiciary, taxation or centres of learning.

15 George Swan, Claire Harrop, and Priti Lancaster, 'Blockchain technology for insurers' (Lexology, 2006) <http://www.lexology.com/library/detail.aspx?g=e094d7bc-4a6f-4f66-b6ba-03e0488c31b5> accessed 7 December 2016

16 Grace Caffyn and others, 'Everledger brings Blockchain to fight against diamond theft' (Companies, 1 August 2015) <http://www.coindesk.com/everledger-blockchain-tech-fight-diamond-theft> accessed 7 December 2016

Each organisation maintains a series of ledgers that manage both 'in' and 'out' flows of information on law, wealth and/or property – everything from the tallying of votes to collecting taxes and maintaining property registries. It is the democratic exercise of distributing and redistributing wealth and maintaining law and order.

We are familiar with the operation of these centralised systems to provide laws and resolve potential disputes, and to produce and distribute resources and services. However, the drawback of such a centralised approach is that, to improve efficiency, organisations are only able to vertically and horizontally integrate with each other. This further consolidates markets and generates even larger concentrations of power, most often at the expense of the individual.[17]

Blockchain technology offers decentralisation of some of these institutions and organisations. Its impact would be far reaching in scaling down governance and institutional designs. Take for example a system in which a corporation is comprised of sets of passive shareholders,[18] sharing limited roles within its core business management. Blockchain-based governance applications could offer real-time accounting and almost instantaneous voting mechanisms to those shareholders, potentially making markets more effective overall. Similarly, electing boards of directors could be as simple as making real-time nominations and subsequent employment packages, rather than using paper mailings or insecure e-proxy services. It may also be applicable to the submission of corporate proposals or calls for reform within the organisation. Corporations would be more dynamic, shareholder voices could be heard and legitimate concerns addressed.[19]

Expanding the concept into the public sector, blockchain-based governance could make it easier for small and large communities to reach consensus, in overcoming the coordination problems inherent in large-scale democratic voting. Improved encryption techniques could enable digital public voting to be viable at a national level, or could equally be scaled down to deal with

17 Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain technology and the rise of lex Cryptographia by Aaron Wright, Primavera de Filippi: SSRN' (SSRN, 20 March 2015) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> accessed 7 December 2016

18 See note 2.

19 Ibid.

local issues – for instance, voting on council budgets via mobile devices or wearable technology. Local participants could make their position known or provide feedback directly. In the case of the budget example, once the budget was approved, the allocated funds could be immediately released to relevant departments using smart contracts.[20]

The dark side of decentralisation

As a powerful decentralised database, blockchain has the capacity to be used to support machine-to-machine communications and capitalise from the IoT in its ability to provide reliable records on the history of asset ownership. Our cars already are connected to the IoT, with telematics now commonplace. While this may help in the enforcement of security rights, it might also be used for digital repossession, giving rise to a darker side of blockchain application. For example, if a payment for a car was missed a creditor could shut the car down electronically until the payment was made.

Other issues could also arise due to the unchangeable nature of a transaction encapsulated within an inflexible code. Regulators are examining blockchains to understand how they might actually increase systemic risk as they threaten to replace centralised systems that can act as shock-absorbers in a time of crisis, something that blockchains, as decentralised ledgers, cannot.[21]

There will be other challenges, not least of which is the 'discovery problem': that is, how will users of anonymous, crypto-secured networks find one another in order to transact business; and how will we know if those parties are legitimate and not simply powerful and illegal enterprises undertaking antisocial online activities?[22]

On an individual level, in commodity-based transactions, the fact that the parties may not even know each other's identity means that if one party feels aggrieved about some aspect of the execution of the contract (eg, misrepresentation or

20 See note 5.

21 James Eyres, 'Why the blockchain will propel a services revolution?' (Financial Review, 14 December 2015) <http://www.afr.com/technology/why-the-blockchain-will-propel-a-services-revolution-20151212-glm6xf> accessed 7 December 2016

22 See note 2.

fraud), they may not necessarily have any redress in the courts This will clearly will raise serious issues for policy makers. Consumer protection, the applicability of domestic laws versus international transactional laws, jurisdictional issues and conflict of laws are some of these issues that would need to be resolved.

Attempts to regulate against these shortfalls may be found to be ineffective. This is because in most cases there would not be an individual upon whom the coercive power of the state could be exercised. The decentralised nature and global reach of blockchain's structure creates that unchecked anonymity: who do we fine? Who should be indicted? Which regulatory authority has jurisdiction? This is further exacerbated when we consider the anonymous nature of the many peer-to-peer economic 'goings-on' that take place on the 'darknet' through proxy networks such as The Onion Relay (TOR), a network that makes IP addresses virtually untraceable.[23]

Algorithmic governance[24]

If we were to speculate, widespread deployment and adoption of smart contracts could even see the creation of custom-built legal systems, in which people are free to choose and to implement their own rules within their own techno-legal frameworks. Blockchain could thereby support and facilitate the deployment of a decentralised alternative to our current legal systems and provide a version of a new 'digital' common law. This could consist of an interconnected system of rules interacting with one another in a reliable and predictable way, without the need of any third party institution to enforce these rules.

As opposed to existing legal systems, which apply regardless of whether they have been consented to, people would be free to choose from a particular set of provisions that better reflect their underlying preferences or needs. In fact, people could choose to participate in two or more regulatory frameworks, perhaps even arbitrarily switching between them depending on the circumstance.

23 See note 17.
24 See note 5.

Such algorithmic governance could also be employed voluntarily by individuals who might wish to ensure they achieve certain self-selected goals, such as losing weight. Once an individual had set a goal, they could then use algorithms to help withstand the temptations of the contemporary world.

This is particularly significant given how many of us already rely on specific sensors and devices to collect data about ourselves and our environment, which we use to improve both ourselves and our communities (especially popular are those in the field of personal health, where big data analysis is helping to identify and provide potential solutions to specific diseases). Everything from monitoring our sleep to analysing our eating habits; from counting steps to calculating daily intake of calories – it seems we are already very willing to rely on algorithms to govern our everyday behaviour.

Consider, then, what might happen if these algorithms were linked with self-enforcing smart-contracts: people trying to lose weight might be informed of their progress, with the algorithms suggesting they walk to work or do more exercise or even suggest a daily menu that would be best for their diet. But, more than this, the smart contract algorithmic governance system might prevent those individuals from purchasing highly caloric products, or shut off access to the internet, mobile phones and other distractions in order to ensure that they comply with their predefined goals.

There are drawbacks to algorithmic governance. For example, when proprietary companies such as Google and Facebook continually frame and reframe our experiences of the digital world to their own ends, store our personal usage data in truly massive Internet silos, for unspecified and ambiguous purposes. It is the opaqueness of these algorithmic rules which leave us with little, to no, insight into how these companies truly decide how they sort, display and use our information.

The digital impetus: blockchain technology across the globe

The Commonwealth: secure messaging

Many reputable organisations have taken blockchain technology to heart and are using it in their search for solutions to long-standing problems, mostly due to security risks and shared technologies. In May 2016, the Commonwealth Secretariat announced[25] its intention to develop a blockchain app to combat cross-border crime. Effectively this will be a secure communication tool for governments and law enforcement, which could be used as a means to connect disparate entities and clarify identity in a digital environment. It will:

- help distribute the burden of electronic evidence sharing between jurisdictions within the Commonwealth; and

- be made available primarily to the Commonwealth Network of Contact Persons (CNCP) – Commonwealth justice officials who provide advice on criminal investigations and obtaining evidence abroad.

The new app will be useful, not only in providing secure access to encrypted communication methods, but will also validate and store the identities of contacts on the blockchain thereby removing the need for a central Commonwealth database.

NASDAQ: in the provision of accurate record-keeping

In May 2015, NASDAQ announced[26] that it would employ blockchain technology to enhance the equity management capabilities offered by its private market platform as part of an enterprise-wide initiative. They said they would initially: introduce a coloured coin innovation whereby the value of real world assets can be represented and managed in a blockchain, leverage the Open Assets Protocol

25 'Commonwealth announces new app to fight cross-border crime', (The Commonwealth, Press Release, 02 May 2016) <http://thecommonwealth.org/media/press-release/commonwealth-announces-new-app-fight-cross-border-crime.> accessed 07 December 2016

26 'Nasdaq Launches Enterprise-Wide Blockchain Technology Initiative' (NASDAQ, Press Release, 11 May 2015) <http://ir.nasdaq.com/releasedetail.cfm?releaseid=912196.> accessed 07 December 2016

in order to enable the issuance and transfer of assets and launch a blockchain-enabled digital ledger technology, which would provide extensive integrity, audit ability, governance and transfer of ownership capabilities.

NASDAQ was one of the first multinational financial services companies to explore ways to leverage the blockchain in a non-currency manner. In its first application it hopes to provide a fully-electronic, distributed ledger-style solution for accurate record-keeping, to complement ExactEquity™ – the 'Nasdaq Private Market's' cloud-based equity management solution. This enables private companies to manage their capitalisation tables and stock plans more efficiently.

US State of Delaware's blockchain initiative[27]

On 2 May 2016, almost a year after the NASDAQ announcement, Delaware Governor Jack Markell announced his support for the creation of a new method of representation of corporate share ownership. Already being the home for many start-up and venture capital-backed businesses (as well as 66 per cent of Fortune 500 companies), the state of Delaware would have the capability – as well as traditional certificated and uncertificated shares – to issue shares using the same technology that underlies the virtual currency Bitcoin.

As an integral part of the 'Delaware Blockchain Initiative' this would involve the creation of a new type of share registration for Delaware corporations: distributed ledger shares. This was described as a significant development in the course of corporate affairs, and even 'the beginning of an inexorable transition to blockchain-based share registration'.

Other elements to Delaware's initiative include:

- assurances that virtual currency and blockchain businesses will not face new proscriptive regulation in Delaware;
- the Governor's support for the amendment of Delaware law to accommodate distributed ledger shares; and

27 Marco A Santori, 'Delaware Announces Support for Blockchain-based Corporate Shares' (Pillsbury Winthrop Shaw Pittman LLP, 2 May 2016) <available at /www.lexology.com/library/detail.aspx?g=cd0bfd98-b53a-43bf-822f-96f9a6e6c333> accessed 07 December 2016

- the creation of the office of the Blockchain Ombudsman, who will be a point of contact for those seeking to do business using blockchain technology in Delaware.

Expanding on the benefits of the technology, the state of Delaware has included voting and other governance processes in its considered application of blockchain technology. It claims that the adoption of blockchain will be rapid and suggests that entities incorporated in Delaware should consider developing a blockchain strategy through Pillsbury, the state's Legal Ambassador to the industry.

Medical records

IBM launched its Autonomous Decentralised Peer-to-Peer Telemetry (ADEPT) project, in partnership with Samsung, in January 2016. The project featured the Ethereum protocol to connect household devices and allow them to transact over the IoT[28]. It will only be a matter of time before our 'fitbots', or 'Sweatcoins' (awarded using an iPhone app after tracking a user's physical steps) and other connected technology will be tied into decentralised medical ledgers, to manage and keep in check our physical and mental well-being.

In August 2016, an Australian start-up[29] made use of blockchain technology to facilitate data sharing in healthcare. The focus is on the identity module, which aims to develop digital identities by using a horizontal platform to securely share data across the entire healthcare network.

28 See note 17.

29 Richard Kastelein, 'Australian Startup Cyph MD uses Blockchain Technology For Data Sharing in Healthcare' (Blockchain News, 9 August 2016) < www.the-blockchain.com/2016/08/09/australian-startup-cyph-md-uses-blockchain-technology-data-sharing-healthcare> accessed 07 December 2016

Honduras and Estonia: blockchain *in situ*

Smaller countries seem abler to resolve their technological shortfalls by leap-frogging over existing out-dated infrastructure and directly embracing new technology, building it from the ground-up. Accordingly, countries such as Honduras[30] have already committed to replacing their existing real-estate records with blockchain technology.

Estonia has taken the technology to the core of its government and financial institutions, using it in the provision, distribution, storage and management of a Public Key Infrastructure[31] or ID cards. These cards allow citizens to order prescriptions,[32] vote, bank online, review their children's school records, apply for state benefits, file their tax return, submit planning applications, upload their wills, apply to serve in the armed forces and around 3000 other functions. Entrepreneurs are also able to use the ID card to file their annual reports, issue shareholder documents and apply for licences. Government officials even use the ID card to encrypt documents for secure communication, review and approve permits, contracts and applications, and submit information requests to law enforcement.

The realities

Blockchain technology has the potential to both help and harm. Numerous reports demonstrate, for example, how virtual currencies such as bitcoin have become the currency of choice for internet-enabled traditional crime on the darknet, facilitating trade in illegal drugs and weapons. One study puts a value on trade from just one such market place trading in illegal drugs as being US$1.2m and Interpol has also identified the dangers of malware and

30 See note 5.

31 Mark Walpot, 'Distributed Ledger Technology: beyond block chain' (Government Office of Science, 2016) <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf> accessed 7 December 2016

32 Oscar Williams-Grut, 'Estonia is using the technology behind the bitcoin to secure 1 million health records' (Business Insider, 3 March 2016)<http://uk.businessinsider.com/guardtime-estonian-health-records-industrial-blockchain-bitcoin-2016-3.> accessed 07 December 2016

other illegal data being imbedded within the blockchain used by some virtual currencies.[33]

Lack of regulation

Because the technology is so new, regulators at EU-level are taking a cautious approach to blockchain. While they recognise the positive impact that developments could have for consumer welfare and economic development, there are many calls for regulation to deal with the risks this new technology could bring. There are particular concerns that blockchain technology may be used for money laundering, terrorist financing and fraud. This, in turn, can result in governance gaps, systemic risk, regulator resources and legal uncertainty.

At the beginning of March 2016,[34] in less than 24 hours, the UK's Financial Conduct Authority (FCA), the European Parliament and the Financial Stability Board (FSB), published three documents, demonstrating the extent of their interest in (i) using; and (ii) beginning to regulate, cryptocurrencies and the blockchain.

The problem for regulators is that decentralised applications and blockchain-based organisations are difficult to control and regulate. Digital currencies, if they gain widespread adoption, may be impossible to shut down precisely because they are not centralised and not controlled by governments or subject to the authority of any regulators. The pseudo-anonymous nature of the blockchain technology combined with encryption could potentially hamper law enforcement's ability to uncover and clamp down on illegal activity, such as tax avoidance or communications between terrorist cells.

In an effort to address the early financial issues associated with the widespread use of virtual currencies, the Her Majesty's Revenue & Customs in the UK (HMRC) set out its views on the tax treatment of Bitcoin and other

33 Working Group report available at http://thecommonwealth.org/sites/default/files/press-release/documents/P14195_ROL_Virtual_Currencies_D_Tait_V5_LoRes.pdf.

34 Chris Finney, 'International regulators take an interest in crypto-currencies & the blockchain: regulation is on its way' (Cooley LLP, 1 March 2016) <available at https://fsregulation-risk.com/2016/03/01/international-regulators-take-an-interest-in-crypto-currencies-the-blockchain-regulation-is-on-its-way> accessed 07 December 2016

cryptocurrencies.[35] It confirms that transactions involving cryptocurrencies will subject to the usual corporation tax, income tax and capital gains tax rules – unless or until HMRC announces any changes – reflecting the potential uncertainty as to how cryptocurrencies will be taxed in the future. Following suit, the European Court of Justice on 26 October 2015 ruled that the exchange of traditional currency for Bitcoin virtual currency and vice versa constituted a valued-added-tax (VAT)-exempt supply of services. Both the European Court of Justice and HMRC have stated categorically that they do not comprise tangible property and are not legal tender. If bitcoins are not legal tender, this means that existing tax rules cannot be directly applied (as these rules generally assume payment with legal tender).[36]

Access to justice

Perhaps the biggest impact of blockchain will be on those with the least to gain and the most to lose. The issues become clearer when viewed from the perspective of those who are challenged financially and/or do not have the same level of access to justice as many corporate entities[37] or wealthy individuals. The biggest challenge to those without means is the lack of access to the actual technology itself; the digital age may be upon us and relatively advanced, but in no way does it provide free and balanced access to either the tools or the devices that allow us to be a part of that digital world. Whether it is Bitcoin, access to banking or insurance and especially smart contracts, any advantages that might result from use of such systems and processes would be excluded from those who have no digital access.

The homeless, infirm, vulnerable and interned: all of these groups will be disadvantaged by either their naivety as to what is involved, or their inability to object and/or correct things when they go wrong. When the use of anonymous, crypto-secured blockchain networks are enlarged exponentially, the same issues that may befall all of us will prove particularly difficult for unprotected and

35 HM Revenue & Customs, *Revenue & Customs Brief 09/14.*

36 Machiel Lambooij, 'Retailers Directly Accepting Bitcoins: Tricky Tax Issues?' (Derivatives & Financial Instruments May/June 2014) <www.freshfields.com/uploadedFiles/Locations/Global/Digital/content/dfi_2014_03_int_4.pdf.> accessed 07 December 2016

37 Joe Dewey and Shawn Amuial, 'Where are we going? Exploring the Blockchain's Utility' (Bloomberg Law, 2 October 2015) < https://bol.bna.com/where-are-we-going > accessed 07 December 2016

vulnerable individuals. If there were some aspect of contract execution (eg, misrepresentation or fraud), they may not have any redress in the courts, a fact that will again raise serious issues for policy-makers.

Such a future presents us with the frightening image of 'Judge Dredd' style court-actions whereby smart contracts' self-enforcement protocols are innocuously triggered by those who may not be aware or may not even be party to those systems.

In the roll-out of blockchain technology for electronic payments, voting, IoT, medical records government registries etc., there are a number of positives for those who are less well-off. Blockchain can be used to capture information such as individuals' birth certificates, National Insurance numbers, passport details, driver's licence and any other information pertinent to creating a Legal Entity Identifier (LEI), which – as in Estonia – allows people to readily prove their identity. This will strengthen the enforceability of electronic signatures and will make signing-up for financial products much more straightforward. This is being presented as a benefit of blockchain technology – good for business, good for the consumer, good for government.

There are also potential socio-economic benefits, such as getting the 'unbanked banked'. This could deliver solutions to the ever-growing problem of immigration, by getting immigrants housed, into work and integrated into society, providing bank accounts and addition to government registers. It can also give individuals a means to securing their own personal blockchain to prove their individual identity. BlockCrushr Labs[38] unveiled a solution using blockchain technologies to ensure funds could be given to buy meals and other necessities to service this precise group of the 'unbanked'.

It is important to understand that this is not an altruistic act; these funds can only be spent for their intended purpose. It does not allow the carrying of 'cash'. This solution only permits the anonymous loading of smart 'digital food wallets' through common payment methods such as smartphones, credit cards and PayPal, and the 'smart wallets' may then only be spent securely at

38 Craig Armstrong, FinTech Update: Who can stop the blockchain train? (Shoosmiths LLP, 9 June 2016), available at < www.shoosmiths.co.uk/client-resources/legal-updates/fintech-update-who-can-stop-the-blockchain-train-11413.aspx.> accessed 07 December 2016

participating food retailers. One obvious question is whether a homeless person, for example, even owns a smartphone, credit card or a Paypal account. In these circumstances, authorities could provide a smartphone for this specific purpose with all the necessary apps uploaded; however, the financial cost associated with such a scheme would arguably be problematic.

Blockchain – mere 'puffery'?

When we look past the publicity and fanfare, the biggest concerns surrounding the application of blockchain have arisen from within the digital technology industry itself. To evaluate these concerns, we need to breakdown the various issues at play:

- first, untangling the technical knots;
- second, understanding what sets blockchain apart;
- third, looking at the product we are actually being sold.

1. Untangling the technical knots

Blockchain is an assemblage[39] of three interlocking components: (i) consensus; (ii) authentication; and (iii) immutability, and the technology behind each of these three components actually predate both Bitcoin and blockchain by decades. The consensus mechanism is built into the underlying application logic, while the authentication technology is provided by public key cryptography – both of which are already common in existing distributed systems. But it was the addition of the third component, immutability, provided by what is termed 'proof-of-work'[40] and used in concert with the first two technologies, that created something truly original. It was this 'proof-of-work' element that tied the other two technologies together, and it is this that became known as 'blockchain'.

39 Jonathan Wolinsky, 'With Blockchain, Where There's Smoke, There's Usually More Smoke' (CoinDesk, 19 June 2016) < www.coindesk.com/blockchain-technology-smoke-more-smoke.> accessed 07 December 2016

40 Robert Wolinsky, 'Can Trust-Based Private Blockchains Be Trusted?' (CoinDesk, 5 March 2016)< www.coindesk.com/can-trust-based-private-blockchains-be-trusted> accessed 07 December 2016

2. Understanding what makes blockchain so different

Data sharing and storage systems traditionally depended on 'trust' between all parties not to breach each other's security or confidentiality by respecting natural and legal persons' boundaries, be they digital or hard-copy. All of these trust systems are regulated by governments and corporates alike, but still largely depend on entities respecting the need to maintain them to protect personal, confidential or enterprise-based data.

However, there are many unscrupulous individuals (and corporates) who can and do violate any or all imposed security regulations, mostly for profit, but sometimes to expose indiscretion or cross-border injustices. Last year in July 2015 in the US alone, we saw banks amongst 22 financial companies accused of colluding to manipulate auctions of US Treasury securities to the sum of US$6bn. And later that year, Wall Street's top banks were forced to agree to a settlement of US$1.87bn over allegations that they conspired to rig the market for credit derivatives. Clearly, it seems our current systems of trust do not always work.

Immutability is therefore a necessary ingredient. The vaunted resiliency of blockchain technology – self-enforcement – would not be transferable without the historical record immutability provided by the proof-of-work protocol. The proof-of-work protocol generates a 'trustless' environment, put in place (by design) as a non-traditional countermeasure to the collusion and/or falsification of individuals or organisations (such as banks) in their efforts to breach the requirement of a 51 per cent consensus. A trustless environment is created by a cost equation, which determines whether the rules have been followed. This bypasses the need for traditional countermeasures imposed on participants to 'follow the rules' (rules which have demonstrably failed).

3. Finally, we shine a light on what is hidden in the shadows

What makes the trustless environment so attractive is that the 51 per cent consensus describes a risk-assessment mechanism: the energy required, or 'hashing power cost', to overturn the historical record is quantifiable and this quantifiable risk makes proof-of-work very appealing from a transaction, tax and audit perspective. This is what drives the interparty efficiency of blockchain technology.

Therein lies the crux of the issue: the deterministic and external validation capabilities provided by the proof-of-work protocol to retain self-enforcement and historic immutability comes at a price – a big price. Bitcoin pays approximately US$400m to US$500m each year to provide the immutability for its historical record, and no other blockchain technology currently employed – anywhere – has matched that expenditure.

So what is everyone excited about?

It appears that what we are seeing in general is not a re-creation of the Bitcoin-style efficiency. Rather this is 'second generation' blockchain technology, where practitioners have attempted to circumvent the high costs with various software workarounds. In doing so, they either do not realise or do not care that both the externality and resource consumption associated with proof-of-work are essential to providing the immutability of the record. Without that the blockchain becomes just a common protocol information-sharing environment.

There are still, it must be said, many benefits to these common protocols for sharing information. But with such a desire to commercialise blockchain technology, one must consider whether to secure the provenance of the historical record of a distributed-ledger blockchain system under proof-of-work rules, or return to previous trust-based or 'permissioning' rules. We have seen that trust-based blockchain systems are insecure and use non-empirical software 'workarounds', so building a distributed ledger without proof-of-work, while economical, will ultimately fall prey to the same security breaches, collusions and market rigging that we are fast becoming used to.

There are no traditional deterrents, regulations or countermeasures that have protected us from those in the past, so it really does seem that there are no viable alternatives. What is more important is that we must now be alert to the fact that the Bitcoin-style, trustless, blockchain 'efficiency' is being already sold under the term 'blockchain' without actually being delivered. Companies like R3CEV are then forced to admit that they are not building blockchains, but actually 'distributed ledgers'. Others including Ripple, Blythe Masters' Digital Asset Holdings' Hyperledger, Chain and IBM also appear to be developing and building common protocol (permissioned) information sharing systems, with workarounds, but calling them 'new and revolutionary'.

Conclusion

Once the fog has lifted and we can see the road ahead, the technology that everyone has been talking about may end up not being all it promised to be. But there are distinct benefits to using blockchain, even in its less-secure permissioned form:

- it does offer the functionality of carrying value, so allows instant transfers of funds, which can be applied to almost every area of our lives;
- the technology can be combined with IoT to protect and track the operation of our hand-held or wearable devices, and by default ourselves;
- it can become the engenderment of new levels of trust between disparate jurisdictions, and;
- it may even improve access to justice by reducing the costs of deploying restricted legal aid funding, thereby extending the number of people that can be given assistance.

Blockchain could also bring financial services to millions of people with internet access but no bank accounts[41] and provide a semi-secure method of transferring money directly between individuals. This could be of particular benefit to opening up the insurance market to individuals who have limited access to banking services but are still in need of asset insurance.

Provided we all understand that the technology we are signing up to will not provide the equivalent efficiency and absolute immutability afforded by Bitcoin-style blockchain technology and that any security will be susceptible to some of the same breaches in security and corporate collusion that we have become used to, then this offers a great opportunity for those firms who can innovate in time.

Ultimately, those firms that are willing to adapt and embrace this technology will be able to provide more effective and efficient services, which may lead to a competitive advantage over those firms who do not evolve. Among all the uncertainties, there can be little doubt that the technology is with us now and there is no turning back.

41 See note 9.

the global voice of
the legal profession®

International Bar Association
4th Floor, 10 St Bride Street
London EC4A 4AD, United Kingdom
Tel: +44 (0)20 7842 0090
Fax: +44 (0)20 7842 0091
Email: LPRU@int-bar.org
www.ibanet.org