Internet Law Bulletin article:

Blockchain and the Law

Brydon Wang, Allens

Tips

- Blockchain technology, or shared-ledger technology, is increasingly seen as an infrastructure-level technology that can be employed in non-financial applications, such as programmable smart contracts that self-execute, digital notary services, and platforms that track and transfer digital media assets.
- Emergent non-financial applications of blockchain technology will broaden the impact of the blockchain beyond banks and other financial institutions to other forms of asset ownership transfer, such as developers who may purchase land from a blockchain land title registry; trade mark and patent holders who may exercise their intellectual property rights over the blockchain; and clients who may be a party to a smart contract.
- Knowledge-sharing opportunities need to be in place to ensure that developers and lawyers understand each other's perspectives.
- Lawyers should be aware of the potential of blockchain technology to augment their capabilities as well as disrupt their clients.
- As smart contracts are increasingly used, lawyers may need to gain a basic proficiency in coding to allow them to check that clauses and contractual mechanisms have been appropriately translated to the relevant programming language. This could be met by training as part of continuing professional development obligations or the legal industry could partner with blockchain stakeholders to produce guides and programmable standard smart contracts that could be tailored to a client's needs.

Introduction

This article begins with a brief introduction into what the blockchain is and the features of the technology that developers are looking to extend to a wider range of financial and non-financial tasks. The article then looks at regulation of the blockchain and its challenges for lawyers, before articulating the developments in scripting and sidechains that have permitted the use of the blockchain in smart contracts, title registries, and other services not contemplated under the Bitcoin protocol. The impact of smart contracts on legal practice is then explored before a conclusion as to the importance of lawyers engaging with blockchain technology is presented.

What is the Blockchain?

A blockchain is a decentralised public ledger of interactions that is duplicated and dispersed across 'nodes' connected on a network. The ledger is designed to be a 'global consensus engine'[1] that removes the need for a trusted intermediary or central authority to validate interactions. The ledger is continuously updated in 'blocks' of information that are coded and linked onto the existing blockchain. This coding process 'hardens' the blockchain by creating incremental barriers of code such that it becomes financially prohibitive to tamper with or rewrite the ledger.[2] Further, as the ledger is hosted on a network, it is resilient with 'no single point of failure'.[3]

The Bitcoin ledger of transactions is the most well-known application of blockchain technology. Bitcoin is a digital currency and payment system that employs encryption to verify transactions and record the these transactions in the blockchain. Using Bitcoin as an example, the process of coding transactions onto a blockchain can generally be broken down into the following three-step protocol:

1 A new transaction (or in more general terms, an interaction) is declared to the network.

2 Nodes on the network compile the new transaction with other new transactions in a block.

3 The transaction is verified by tracing through the blockchain ledger to ensure that the transaction is valid. Where the transaction is valid, it is coded by an algorithm to generate a 'hash' (a string of random numbers that can be de-coded to produce the actual data) and added to the blockchain. This hashing process prevents double-spending through time-stamping of the verified interaction.[4]

In Step 3 above, nodes on the network (or 'Miners') verify the interaction through a 'proof-of-work' validation system that requires Miners to compete within the network to solve a cryptographic problem to validate the transaction and code the transaction onto the blockchain. Miners are incentivised to make the validation attempt as a successful attempt would yield new Bitcoins that are effectively 'mined' through the use of the Miner's computational resources. Given there is a finite number of remaining Bitcoins that can be mined, this incentive structure will eventually be replaced by transaction fees.

While the Bitcoin protocol is open-source and can be modified, it can only be amended by majority consensus, which may be cumbersome for a developer seeking to extend the utility of the blockchain to other tasks not permitted by the current Bitcoin architecture. This majority consensus approach also makes a blockchain network susceptible to a '51% attack' — where an entity controls more than half of

[1]Wayne Vaughan, CEO of Tierion, as quoted in Aaron van Wirdum, 'The Rediscovery of Bitcoin's Blockchain: The World's Most Powerful Anchor' (3 December 2015) *Bitcoin Magazine* <https://bitcoinmagazine.com/articles/the-rediscovery-of-bitcoin-s-blockchain-the-world-s-most-powerful-anchor-1449084048>.

[2] For a more extensive introduction to the blockchain, see Antony Lewis, 'A gentle introduction to blockchain technology' (9 September 2015) *Bits on blocks* <http://bitsonblocks.net/2015/09/09/a-gentle-introduction-to-blockchain-technology/>

[3] Primavera De Filippi, 'Tomorrow's Apps will come from brilliant (and risky) Bitcoin code' (8 March 2014) *Wired* <http://www.wired.com/2014/03/decentralized-applications-built-bitcoin-great-except-whos-responsible-outcomes/>.

[4] Note that the original paper on the BItcoin Protocol by Satoshi Nakamoto lists 6 steps that detail the behaviour of nodes on the network (an expansion of Step 3). For present purposes, this has been simplified. See Satoshi Nakamoto (24 May 2009) *Bitcoin: A Peer-to-Peer Electronic Cash System,* 3 <https://bitcoin.org/bitcoin.pdf>.

the computational resources of the network and can theoretically thwart the consensus validation system and enable double-spending of the Bitcoin. However, given that the Bitcoin validation system has a computation power that is approximately eight hundred quadrillion hash computations per second,[5] any attempt to thwart the validation process is, in theory, prohibitively expensive.

Regulation of the blockchain

Lawrence Lessig, Harvard Law School Professor, observed in the recent Sydney Blockchain Workshop (held 11 December 2015) that despite the design intent of the blockchain to provide a free-flowing transfer of digital assets without intervention of a trusted third party, the technology will still be subject to existing regulated infrastructure because the nature and 'importance of the commerce it seeks to facilitate [is such] that regulators will have no choice but to become involved in its operation'.[6]

Eyers observes that these regulators are examining how the blockchain's aim of displacing central authority or trusted third parties that 'act as shock absorbers in a time of crises' (which is not a function of decentralised ledgers) may increase systemic risk.[7] ASIC chairman, Greg Medcraft, noted in the same Sydney Blockchain Workshop that ASIC had 'embraced' the blockchain and that Treasury would review Commonwealth legislation for opportunities to improve the regulation of blockchain technology.[8]

A key area where lawyers can assist in supporting the continued evolution of blockchain technology is in engaging in further dialogue with developers to ensure that there is a deeper understanding of each other's perspectives: how the law will apply to the functionality sought by developers; and clarification of terminology—such as, the differences between how regulatory frameworks treat property, gift cards, securities or stock.[9] Lessig observes that developers must 'avoid the same mistakes that [they] made 20 years ago at the birth of the internet, with obliviousness of those in the tech community to the way in which the law would react to what they were building'.[10] Lessig proposes 'regulatory war games [to] map out ways' that blockchain technology may run into conflict with existing regulatory systems[11] and to provide mutual education of how laws can develop to encourage further innovation of the blockchain.

---

[5] Figure as at January 2016; see Blockchain Info, *Hash Rate* <https://blockchain.info/charts/hash-rate>.

[6] James Eyers, 'Why the blockchain will propel a services revolution' (14 December 2015) *AFR Weekend*<http://www.afr.com/technology/why-the-blockchain-will-propel-a-services-revolution-20151212-glm6xf>; see also Lawrence Lessig, 'Deja vu all over again: Thinking through law & code, again' (Speech delivered at the Sydney Blockchain Workshop, Sydney, 11 December 2015). <https://vimeo.com/148665401>.

[7] Eyers, above n 6.

[8] Ibid.

[9] See also: Sanchi Manchanda, Sweta Kumari, Kishroe Abhishek, and Vrijendra Singh, 'Legitimising Bitcoins in India' (2015) 21(6) *Computer and Telecommunications Law Review* 162, 167-8

[10] Lessig, above n 6.

[11] Ibid.

Future applications of the blockchain and implications for legal practice

Given the majority consensus requirement for amendments to the Bitcoin blockchain network, new platforms seeking to extend the utility of blockchain technology are now creating ledgers that are independent of the Bitcoin blockchain network or building additional data layers that utilise the Bitcoin blockchain network as base infrastructure:

- *Parallel blockchain networks through Scripting*
  Interactions on the blockchain between parties involves the transfer of a digital asset (a 'coin' in the case of a cryptocurrency like Bitcoin) that is programmable[12] and can incorporate further information that permits the blockchain to support a wide range of financial and non-financial tasks. For example, a condition precedent could be written into the code such that a transaction can be automated without third party verification to occur at a particular time or where a conditional event is met (such as when a deposit is refunded to a user after a fixed period of time, or, when transacting on the internet of things, automated unlocking of purchased cars or accommodation where payment is made).
  In order to accomplish this, some developers create parallel blockchain networks or 'altcoins' that operate on a consensus method and protocol that is scripted differently to the Bitcoin model. *Ripple* is an example of a parallel blockchain network that provides a distributed payments system that has been scripted to also provide for 'interoperability between banks and payment networks on a global scale'.[13] However, given the limited scale of altcoins, where these exist as independent public blockchains, they are more susceptible to 51% attacks as the computational resources committed under these separate networks are far less than what is committed in the Bitcoin blockchain network.
- *Sidechains and Anchoring*
  Sidechains are separate ledgers that are pegged or 'anchored' to the Bitcoin blockchain and unlike 'altcoins', do not require a user to leave the security of the Bitcoin environment.[14] These ledgers interact with the Bitcoin blockchain and benefit from the security of the very large network, but architecturally, run a separate data layer on top of the Bitcoin blockchain infrastructure, which allows for added functionality. One example of anchoring is the use of Merkle Trees and Roots. A Merkle tree is a cryptographic tool that is used to assemble data that has been compressed and scrambled into a hash. Multiple hashes (or trees) are compressed into a Merkle root that is then embedded in the Bitcoin blockchain.[15]

Together, scripting and sidechains open up the possibility of using the blockchain in a variety of ways:

---

[12] Jon Evans, 'Bitcoin 2.0: Sidechains And Ethereum And Zerocash, Oh My!' (25 October 2014) *Tech Crunch* < http://techcrunch.com/2014/10/25/bitcoin-2-0-sidechains-and-zerocash-and-ethereum-oh-my/>

[13] Gilly Wright, 'Will Blockchain Enable Better Banking?' (2015) 29(7) *Global Finance* 40, 41.

[14] Adam Back, Matt Corallo, Luke Dashjr, Mark Friendenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timon, and Pieter Wuille (22 October 2014) *Enabling Blockchain Innovations Through Pegged Sidechains* <http://www.blockstream.com/sidechains.pdf>.

[15] van Wirdum, above n 1.

- *Financial applications*

  The key advantages offered by the blockchain in the Bitcoin environment is its ability to capture 'several key components of a transaction — recordkeeping, auditing, monitoring, enforcement, or asset custody'.[16] The diminution of a trusted third party to undertake these components of a transaction (also known as 'disintermediation'[17]) provides increased efficiencies[18] that can lead to quicker settlement periods and reduced reliance on existing 'trust-obviating' technology (such as accounting systems and banking services — particularly around the verification of account holders).

  Kharif observes that this could allow Bitcoin 2.0 platforms to deliver savings in '[verification] fees shouldered by buyers and sellers in the $1.22 trillion global electronic commerce market, as well as in financial services, cloud computing and other areas'.[19] Kiviat similarly observes that this '[integration of] several components of the trading-clearing-settlement value chain' will allow Bitcoin 2.0 platforms to participate in the $600 billion global remittance market.[20]

  Consequently, the blockchain will increasingly be looked at to determine if it can be brought within existing payment-and-transfer processes to provide greater efficiency, lower fees and to make the adopting entity more competitive. An example of this is the 'interledger protocol' that will allow the various altcoin ledgers to interact to 'create a global standard of payments'.[21] It is envisaged that the protocol will create ad hoc consensus groups for each transaction through a third-party 'connector' or 'validator', and in this way permit banks to 'interface with... distributed ledgers without actually joining them'.[22]

- *Non-Financial Applications*

  Scripting and sidechains can extend the utility of blockchain technology to a host of non-financial tasks, such as: smart contracts[23] (discussed in detail in the next part of this article), digital title

---

[16] Trevor Kiviat, 'Beyond Bitcoin: Issues in regulating blockchain transactions' (2015) 65 *Duke Law Journal* 569, 585.

[17] Noah Thorp describes 'disintermediation' as 'the transference of trust, data, and ownership infrastructure from banks and businesses into distributed peer to peer network protocols'; see Noah Thorp (18 May 2015) *How Society will be transformed by CryptoEconomics* <https://medium.com/@noahthorp/how-society-will-be-transformed-by-crypto-economics-b02b6765ca8c#.v86v691y3>.

[18] Chris DeRose, 'Get Ready for the Rise of the Blockchain (21 April 2015) *American Banker* <http://www.americanbanker.com/bankthink/get-ready-for-the-rise-of-the-blockchain-1073843-1.html>.

[19] Olga Kharif, 'Bitcoin 2.0 Shows Technology Evolving Beyond Use as Money' (28 March 2014) *Bloomberg Business* <http://www.bloomberg.com/news/2014-03-28/bitcoin-2-0-shows-technology-evolving-beyond-use-as-money.html/>

[20] Kiviat, above n 16, 586-7. Medcraft suggests that there is a fourth advantage — market access — given the blockchain's global nature, but it is unclear how significant this advantage is compared with other internet-based solutions; see Greg Medcraft, 'Bitcoin's Blockchain technology has great potential — and risks' (26 October 2015) *The Australian* <http://www.theaustralian.com.au/business/bitcoins-blockchain-technology-has-great-potential--and-risks/news-story/c9b8c3ef435f0b5cc5aa2bd0ed65d3c8>.

[21] Cade Metz, 'The Plan to Unite Bitcoin with all other Online Currencies' (6 January 2016) *Wired* <http://www.wired.com/2016/01/project-aims-to-unite-bitcoin-with-other-online-currencies/>.

[22] Ibid.

[23] Nick Szabo coined the term 'smart contracts' in 1997 to describe contracts that 'reference [valuable and digitally-controlled property] in a dynamic, often proactively enforced form'; see Nick Szabo (1997) *The Idea of Smart Contracts*. Note that Szabo also

tracking, transfer and recording of digital media assets, buying and selling of digital stocks, digital crowdfunding, digital insurance, identity verification services, voting systems and professional certificates[24].

Where the blockchain is utilised to record changes in ownership of an asset, it has the potential to replace patent and trademark registries and land title registries (such as the Bitcoin 2.0 registry program in development by *Factom* with the Honduran government). Other examples of such non-financial utility of the blockchain include *Viacoin*, which provides a digital 'notary' service to time-stamp, verify ownership and transfer documents, and *Storj*, a decentralised cloud storage system using the blockchain as base infrastructure.[25]

As the utility of the blockchain is extended into further industries, lawyers will the relevant skill-sets in these industries will need to gain specific knowledge on how these Bitcoin 2.0 platforms have the potential to increase efficiencies and create risks. For example, the Bitcoin blockchain has other technical considerations that lawyers should be aware of. These include the need to use actual Bitcoins when anchoring into the Bitcoin blockchain, which may lead to additional risks around the cost of transactions; as well as speed and capacity considerations given that transactions currently require approximately 10 minutes to confirm and that Bitcoin cannot handle at present more than 7 transactions per second.

Smart Contracts and their impact on legal practice

Smart contracts are decentralised self-executing contracts on the blockchain that 'facilitate, verify, execute and enforce the terms of a commercial agreement'[26] where programmed conditions are met. Given that they are automated to fulfil programmed obligations once a counter-party performs its obligations, these contracts reduce verification costs and risk of non-performance of the contract. They include 'smart stock, self-enforcing derivatives, 'trustless' letters of credit and proof of existence',[27] and ‘invoices that pay themselves when a shipment arrives’.[28]

This added certainty to smart contracts gives it an advantage over other digital contracts where the law is still unsettled. For example, while electronic execution of contracts published on Bitcoin's blockchain

provides a hypothetical application of the smart contract to a connected car that would remain inoperable unless the security protocols embedded in the smart contract were met.

[24] Marc Andressen, as quoted in Olga Kharif, above n 19; and Joe Dewey and Shawn Amuial, 'Blockchain Technology will Transform the Practice of Law' (25 June 2015) *Bloomberg BNA* <https://bol.bna.com/blockchain-technology-will-transform-the-practice-of-law/>.

[25] For a more complete list capturing the wide variety of Bitcoin 2.0 platforms, see Adam Hayes, 'Bitcoin 2.0 Applications' (3 November 2015) *Investopedia* <http://www.investopedia.com/articles/investing/042015/bitcoin-20-applications.asp>; see also Antonis Polemitis (11 March 2014) *The Mega-Master Blockchain List* <http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list>.

[26] Tim Swanson, *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management* (2014) 11; cited in Trevor Kiviat, 'Beyond Bitcoin: Issues in regulating blockchain transactions' (2015) 65 *Duke Law Journal* 569, 605.

[27] Miles Cowan and Zachary Smith, 'Law as Code. Reality, Possibility and Potential' (April 2014) presentation given at Columbia Law School <http://blogs.law.columbia.edu/slst/files/2014/04/Law-as-Code-Presentation-Slides.pdf>.

[28] The Economist “The great chain of being sure about things” (2015) *Briefing Blockchains*, 23.

(supported by a platform such as *DocuSign*) are likely to be effective, there may be issues with whether the electronic witnessing of these contracts are effective, particularly in relation to deeds.

Ethereum is a platform with a Turing-complete scripting language that allows an additional data layer to be built on the base infrastructure of the blockchain. This allows self-executing smart contracts to be programmed in this scripting language and coded into the blockchain. The Ethereum protocol was incorporated in the recent IBM-Samsung *Autonomous Decentralised Peer-to-Peer Telemetry* ('ADEPT'), allowing users to 'transact over the "internet of things"' using their connected household devices.[29]

Dewey and Amuial suggest that with greater use of smart contracts, lawyers may need to understand basic coding as part of drafting these contracts to ensure that they create or are implementing a smart contract that works as intended on the blockchain.[30] This ties in with Lessig's observations on the need for increased knowledge-exchange between developers and regulators and lawyers (see the section on regulating Bitcoins above). Dewey and Amuial note that as there is still a requirement to translate what a lawyer drafts in a contract to the programming language that is used in the smart contract, lawyers should gain familiarity with the relevant programming language to reduce risks around this translation process.[31] However, the future application of machine logic and speed to de-bug inconsistencies in the drafting of these smart contracts or to update clauses in reference to the changing regulatory environment offers distinct opportunities for lawyers.[32]

However, Lessig, Dewey and Amuial all express concern that automated smart contracts that are 'virtually irreversible' may mark the start of a slippery slope that '[erodes] equitable principles'[33] and the ability of the courts to strike out clauses that are against public policy and void contracts on grounds of duress, mistake, misrepresentation or unconscionability. This automation also impacts on remedies such as specific performance,[34] removing this from the purview of the courts, although arbitration and dispute resolution clauses can still be drafted into these smart contracts to address the consequences of the automated performance of obligations. Lawyers should also be aware that clients may not be able to cancel or breach smart contracts where these are not programmed with sufficient flexibility.

This picks up on the tension that exists between the ‘purpose of code to execute a set of instructions in a deterministic fashion’ and that of a contract, which is to ‘frame and regulate interactions between… entities’.[35] Lessig suggests that lawyers and regulators need to work with developers to provide sufficient 'obscurity' (or ambiguity) in what is characteristically inflexible code to make it responsive to individual

---

[29] Eyers, above n 6.

[30] Dewey and Amuial, (25 June 2015), above n 24.

[31] Dewey and Amuial, 'Where are we going? Exploring the Blockchain's Utility' (2 October 2015) *Bloomberg BNA* <https://bol.bna.com/where-are-we-going/>

[32] Ibid.

[33] Dewey and Amuial (25 June 2015) above n 24; see also Lessig, above n 6

[34] Andrew Hinkes, 'Blockchains, smart contracts, and the death of specific performance' (29 July 2014) *Inside Counsel* <http://www.insidecounsel.com/2014/07/29/blockchains-smart-contracts-and-the-death-of-speci>.

[35] Email from TJ Saw, co-founder of blockchain startup Ethcore and former King & Wood Mallesons lawyer, to Brydon Wang, 12 January 2016.

circumstances and prevent the 'tyranny of code'[36]. This risk of tyranny is exacerbated by the possible creation and use of distributed autonomous companies or organisation as envisaged by the Ethereum developers. These autonomous entities pose challenges for existing corporations law, particularly where responsibility for an automated action needs to be allocated.[37]

The risk of smart contracts that are against public policy is 'compounded by the pseudo anonymous nature of the participants in these types of marketplace'.[38] This raises privacy issues with contractual information captured on a dispersed ledger, particularly where there is potential for personal information derived from a separate source to be correlated with pseudonymous blockchain data to reveal transaction history, contracting party information and sensitive information. Lawyers should be aware of these risks when advising clients.

Conclusion

Despite the potential risks that accompany any innovation of code and expansion of the utility of blockchain technology, Lessig asserts that the technology is 'the most important innovation in fundamental architecture since the tubes of the internets were first developed' to potentially 'bypass corruption, to bypass fraud, to improve efficiency, and to enhance freedom'.[39] Lawyers will have to rise to the challenges and opportunities for solving the new legal problems that will accompany the further development of blockchain technology.

[36] De Filippi, above n 3.

[37] Stephen Mason and Timothy Reiniger, '"Trust" Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog?' (2015) 21(5) *Computer and Telecommunications Law Review* 135, 136.

[38] Dewey and Amuial (25 June 2015) above n 24.

[39] Lessig, above n 7.