Trusteeship in a Post-Trust World: Property, Trusts Law & the Blockchain

Robert Herian – The Open University

Introduction

> What is it that determines this progression today? We can no longer argue that it is an economic or social condition, or education, or any other human factor. Essentially, the preceding technical situation alone is determinative. When a given technical discovery occurs, it has followed almost of necessity certain other discoveries. Human intervention in this succession appears only as an incidental cause, and no man can do this by himself. But anyone who is sufficiently up-to-date technically can make a valid discovery which rationally follows its predecessors and rationally heralds what is to follow[1].

This article will explore potential impacts to the practices and principles of trusts law as a consequence of rapidly evolving blockchain technology and other technologies associated with it, namely "smart property" and the "internet of things". The relevance of the blockchain to trusts law that this article with argue for, is based on widely-held yet generic characterizations of the technology that can be summarized in the following way: the blockchain is a decentralized and disintermediated system based on cryptographic proof instead of trust, a "peer-to-peer network using proof-of-work to record a public history of transactions"[2] that creates a post-trust paradigm in which there is no need "for participants to be trusted", and which provides "no centralized, single point of failure"[3].

There is already good cause to believe that blockchain architecture can be mapped onto trusts, or *vice versa*. Evidence of this comes from an existing, if still somewhat immature, post-trust paradigm facilitated by the blockchain in the growing legal domain of smart contracts. Comparable with smart contracts, "smart trusts" would, for example, involve trusteeship (in terms of duties and obligations etc.), being distributed across a public computer network involving varying numbers of anonymous nodes all working to securely facilitate and verify property transactions. A distributed "trustee" architecture could, in theory, remove the need for continuous human intervention in and monitoring of, for example, trust fund investments by a single trustee, group or board of trustees, and thus remove key issues relating to accountability

[1] Ellul, J. (1964), *The Technological Society*, New York: Vintage, p.90
[2] Nakamoto, S. (2008) "Bitcoin: A Peer-to-Peer Electronic Cash System", [online] Available at: https://bitcoin.org/bitcoin.pdf (accessed 18th January 2016), p.8
[3] IBM Institute for Business Value (2015), *Device Democracy: Saving the Internet of Things*, [online] available at: http://public.dhe.ibm.com/common/ssi/ecm/gb/en/gbe03620usen/GBE03620USEN.PDF? (accessed 16th February 2016), p.9

robert.herian@open.ac.uk

Working Paper

and, more importantly, the potential for any breach of trust[4]. Moreover, the potential for increased security and efficiency of smart trusts and distributed trusteeship would arguably improve the overall investment strategy of the trust, thereby creating better returns for beneficiaries. As a tentative early exploration into the compatibility of blockchain architecture and trusts, this article will explore these ideas in relation to basic principles of express trusts and trusteeship.

Blockchain: a brief history and introduction

The aim of this article is to focus on elements of trusts law in relation to the blockchain, rather than on a detailed examination or technological assessment of the blockchain as such. What can be extrapolated from the general architecture of the blockchain of relevance to the paradigm of trusts and trusteeship is the concern here. Moreover, how exactly blockchain architecture is given legal definition, meaning and, above all, (recognizable) authority in terms of existing trusts law rules, doctrines and principles; or, conversely, how the blockchain may demonstrate a new paradigm for trusts and trusteeship that renders exiting rules and doctrines obsolete.

Before turning to look at trusts however, is it first necessary to introduce some of the fundamental aspects of blockchain technology. It must be noted that many of the technical aspects fall outside of the scope of this article. To that end the following discussion will certainly fall short of the expectations of computer scientists. It will, however, hopefully prove enlightening for lawyers. Following a (very) brief history of blockchain technology, this section will discuss two aspects of the general blockchain architecture that determine how the network is run, and thus, given a smart trusts context, could potentially determine any impact upon the formulation and structure of trust arrangements, and the decision making activities and management and administration of trust property by trustees. The two aspects, based on those originally outlined by Nakamoto, are as follows: *proof-of-work* and *privacy*[5].

A brief history

A system analogous to the blockchain was first described as a method for securely timestamping digital documents, which accurately recorded the order in which those documents were created[6], and thus "announced" an entire history of documents that were fixed, transparent and capable of public scrutiny[7]. It is the accuracy of the record keeping facilitated by timestamping that makes

[4] This was a particular outcome from discussions held between members of The Open University's interdisciplinary blockchain research group, 2nd March 2016.
[5] Ibid Nakamoto (2008)
[6] Haber, S. and Stornetta W. S. (1991) "How to Time-Stamp a Digital Document", *Journal of Cryptology*, Vol. 3, No. 2, pp.99-111
[7] Ibid Nakamoto (2008)

Working Paper

the system a highly "reliable witness"[8]. This early glimpse at the decentralizing and democratizing potential of this new technology was not, however, implemented in legal infrastructure nor given legal character in the same way as the blockchain, most notably, in recent years, in relation to so-called "smart contracts".

Today the story is markedly different, with technology now advanced enough to make implementation of document time-stamping in, for example, the domain of land registration a serious consideration. Indeed, the blockchain is already providing practical ways for nation-states lacking a sufficient or reliable land registry to securely define and enforce individual land rights[9]. Notwithstanding the remarkable increase in computational capability (and availability) in the years following the first, proto-blockchain, proposal, it was largely due to the solving of the so-called "double spend" issue by the somewhat mythical and likely pseudonymous Satoshi Nakamoto that can be credited with the characterisation and recent proliferation of blockchain technology[10].

The double spend issue Nakamoto was referring to was a problem rooted in electronic payments systems involving electronic coins – ostensibly a chain of digital signatures that were the forerunners of bitcoin and other analogous coins. The problem was defined in terms of a payee who could not verify whether the owner of a coin had double-spent or duplicated their coins, and in lieu of a trusted authority (the developers and coders of bitcoin were interested in a developing a system that would intentionally avoid or undermine centralized corporate control, and especially, what were viewed as, troublesome banks and financial institutions[11]) it was necessary to find a way in which the transactions could be checked to ensure they were not duplications. In accordance with economic norms and financial regulation this essentially meant that, prior to the blockchain, there was no definitive way of preventing the uncontrolled reproduction and proliferation of a measure of value, meaning there was no way in which levels of inflation could be controlled. In terms of the fundamental notions of property, it also completely undermined

[8] This was a further from discussions held between members of The Open University's interdisciplinary blockchain research group, 2nd March 2016.
[9] For example, see: http://cadasta.org/ (accessed 25th February 2016)
[10] Ibid Nakamoto (2008)
[11] Emphasis on autonomy and individual empowerment is a legacy of the blockchain's roots in anarchic and cyberpunk cultures that encouraged the development of systems uncoupled from state or corporate control. This extends to the open source character of, for example, bitcoin software which means that a community of individuals can collaborate in order to drive forward the progress of the software without having to rely upon technological development engaged with large corporate and financial institutions. Even though there is a team of core developers at the centre of bitcoin's development, the project remains "constrained by an informal self-imposed charter, which states that significant changes to any rules or protocols require broad consensus from the community" (Government Office for Science (2015), *Distributed Ledger Technology: beyond block chain*, [online] available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf (accessed 9th February 2016))

Working Paper

the ability of electronic coins to satisfactorily transfer rights of ownership, because, in theory, numerous stakeholders could claim and thus try and enforce a right of ownership of the same coin.

Whilst the problem of double spending was both identified and solved with regard to electronic payment systems, the chain of digital signatures that defined the "coins" in question were not exclusively monetary in nature. Indeed, recent litigation in the United States has finally moved the vexed legal question: "what is bitcoin?", away from the rather obvious yet wholly unsatisfactory conclusion that it is money; settling, for the time-being at least, on the conclusion that it is intangible property[12]. And this legal definition is important, not least because it reflects the fact that as a chain of digital signatures, "coins" can conceivably transact anything across a blockchain. They can, for example, represent documented yet still, to all intents and purposes, abstract notions of property rights. Accordingly this has seen the potential of the blockchain expand exponentially, especially in politico-economic and legal terms.

Aaron Wright and Primavera De Filippi describe some of the possible applications of the blockchain, as well as other key technologies facilitated by the blockchain, and importantly how this translates into the potential reach the blockchain may have in various socio-legal, economic and political domains:

> Blockchain technology enables the creation of decentralized currencies, self-executing digital contracts (smart contracts) and intelligent assets that can be controlled over the Internet (smart property). The blockchain also enables the development of new governance systems with more democratic or participatory decision-making, and decentralized (autonomous) organizations that can operate over a network of computers without any human intervention. These applications have lead (*sic*) many to compare the blockchain to the Internet, with accompanying predictions that this technology will shift the balance of power away from centralized authorities in the field of communications, business and even politics or law[13].

Proof-of-work

The blockchain is most commonly defined as a digital ledger which is distributed across a network of computers or nodes. Each node securely verifies the events and transactions that occur, are "broadcast" or "published" across the blockchain, and records them, permanently, on

[12] See the decision in the February 2016 California bankruptcy case, *In re Hashfast Technologies* (Case No: 14-30866 DM)

[13] Wright, A. and De Filippi, P. (2015) "Decentralized Blockchain Technology and the Rise of Lex Cryptographia", [online] available at: http://articles.ssrn.com/sol3/articles.cfm?abstract_id=2580664 (accessed 8th February 2016)

Working Paper

the ledger. Unlike traditional ledgers however, and by virtue of its distributed and decentralized nature, the blockchain does not require a single authoritative intermediary, namely a person or institution (such as the bank in the double-spend example), in order to check, register or monitor transactions, events, or data associated with it at any one time. This is why the blockchain is described as both decentralized and disintermediated. In order to guarantee its inherent legitimacy and integrity, however, the blockchain must provide proof of the transactions and events that it facilitates. Proof-of-work is thus key, and assists with external and regulatory questions and issues of legitimacy and integrity, which in turn inform the relative authority and extrinsic enforceability of the blockchain. In other words, equivalent to the accounting obligations of trustees, the blockchain must be able to provide evidence of the transactions and events that it purports to facilitate. Proof-of-work is one of the ways the blockchain does this.

Due to the consensual basis on which blockchains operate, proof-of-work extends beyond the immutable timestamping and documenting facility that defines the blockchain as a ledger however. Proof-of-work is intimately related to the distributed nature of the blockchain insofar as it reflects the collective effort of nodes or numerous central processing units (CPUs) who build individual blocks, and ensure the proliferation of the architecture of the blockchain. Proliferation is achieved by what Nakamoto calls, "one-CPU-one-vote", which determines that an incentivised yet consensual, majority decision leads not only to the longest chains, but those most likely to be legitimate and "honest"[14]. Moreover, as each block is chained to the next, as well as the one prior to it, it becomes less likely that a "greedy attacker" looking to intermeddle with a chain, or more specifically the items contained within a block, and defraud as a consequence, would be able to undo or change a particular chain without effecting all the blocks associated with it. Incentives, insofar as they dovetail honesty, also play a significant role in this regard, adding a further layer of security and legitimacy to the system. "The incentive", Nakamoto claims, "may encourage nodes to stay honest", and thus a "greedy attacker […] ought to find it more profitable to play by the rules […] than to undermine the system and the validity of his own wealth"[15]. And whilst the account given here does not describe proof-of-work as such from a technical perspective, its importance as a process in structuring trust ought to be clear. In other words, it is a cornerstone of any consideration of new forms of trusteeship rooted in blockchain technology.

Privacy

Relatively few trusts are a public concern. So, whilst a key feature of the post-trust paradigm facilitated by the blockchain is the public announcement of transaction and event histories that occur across it, this would clearly conflict with the need for privacy demanded by, amongst others,

[14] Ibid Nakamoto (2008), p.3
[15] Ibid Nakamoto (2008), p.4

Working Paper

trust beneficiaries. As is the case with the particular blockchain that facilitates bitcoin transactions, each transaction or event is checked and validated using an encrypted digital fingerprint or hash to ensure that there can be no duplication of the information contained within a particular block, and that each block is unique.

Encryption is fundamental to blockchain technology. And encryption, or more specifically the use of two sets of keys, one public and one private, to validate transactions provides the possibility for secure, private spaces that nevertheless remain in public view. This means that on the blockchain, unlike existing methods for maintaining the privacy of transactions which shield the entire process from public view, including the identities of the transacting parties - a costly and potentially inefficient and ineffective process - "privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous"[16]. From a smart trusts perspective, adopting this type of privacy offered by the blockchain would necessarily involve a cost-benefit analysis in order to ascertain whether or not the potential increase in value and efficiency of the trust fund enabled by the blockchain merited the public scrutiny of the trusts dealings, although not its beneficiaries, which would accompany smart trusts.

Notwithstanding the need for such cost-benefit analyses, the anonymization of public keys and the resultant shielding of identities does open-up a number of possibilities for different and particular smart trusts on the blockchain. In other words, any number of private and privatized enclosed blockchains are possible, each capable of serving a dedicated purpose or assuming a particular form or particular characteristics, including those of a small family trust fund, or a major state-based investment strategy. Thus, whilst the general blockchain architecture ought itself to be considered generic, a blockchain can be individually tailored to suit a particular need by virtue of the manipulation of traditional methods of privacy.

Smart property and the internet of things

It is not really possible to conceive of smart trusts based on the blockchain alone. After all, whilst the blockchain, as a ledger system, is capable of generating immutable proof of transactions and the order in which these occur, thereby satisfying some of the aspects of trust management and administration, it cannot deal with trust property as such. Especially important to understanding the potential relationship between trusts and the blockchain, therefore, is how property, both intangible and tangible, personal and real, would be handled. A solution to this problem could lie in smart property and the internet of things, primarily because both of these technologies make dealing with physical property in a digital space possible. Moreover, they both make machine-to-machine or invisible transactions, management and administration of both tangible and

[16] Ibid Nakamoto (2008), p.6

Working Paper

intangible property possible. However, simply because it could in theory be possible does not mean it is yet entirely possible in a practical sense, nor desirable for that matter. The blockchain may be largely immutable as a distributed, disintermediated system, but, as a recent UK government report states, just like "real world" legal code that governs property rights, transfer of ownership etc., "technical code needs to be produced and maintained by humans who define the rule that the code embodies", and therefore it is a misconception to believe that unpermissioned distributed ledger systems exist independently of human rule-making[17].

It may be too soon to rely or insist upon the validity or desirability of smart trusts populated only by autonomous smart property networked to an internet of things, yet these two areas are now more advanced in terms of circumventing human interference. Indeed, IBM explain how invisibility is on the verge of becoming a normal function in the instrumented, interconnected and intelligent world of smart property and the internet of things: "Many machine-human interactions will be replaced by machine-machine interactions, and new machine-human interactions will emerge. A large majority of machine-machine communication will become invisible while machine-human communication will become highly interactive"[18]. Moreover, IBM propose and describe the treatment of physical property in digital terms, which they refer to as the "liquefying the physical world"[19]. Together smart property and the internet of things "creates the ability to digitize, sell and deliver physical assets as easily as with virtual goods today"[20].

Due to their inherent relationship with smart property, brief mention of smart contracts must also be made. Smart contracts are, after all, already demonstrating how smart property or even property in a more conventional sense can be effectively administered digitally, working both in relation to the internet of things – that is, in relation to a network specifically designed to facilitate invisible machine-to-machine transactions – as well as outside of it. Smart property has its roots in the existence of smart contracts; the two are intertwined, and if not exactly co-dependent, smart property is certainly bound to smart contracting in order to reasonably and effectively operate. This is how the former law professor, and one of the first people to define both smart contracts and property, Nick Szabo, describes the relationship between the two:

> Smart property might be created by embedding smart contracts in physical objects. These embedded protocols would automatically give control of the keys for operating the property to the agent who rightfully owns that property, based on the terms of the contract. For example, a car might be rendered inoperable unless the proper challenge-

[17] Ibid Government Office for Science (2015), p.43
[18] Ibid IBM (2015), p.19
[19] Ibid IBM (2015), p.13
[20] Ibid IBM (2015), p.13

Working Paper

> response protocol is completed with its rightful owner, preventing theft. If a loan was taken out to buy that car, and the owner failed to make payments, the smart contract could automatically invoke a lien, which returns control of the car keys to the bank[21].

As Szabo's outline suggests, by virtue of the relationship between smart contracts and property there is no need to limit the scope of property that could be handled by a smart trust. There would be no need, for example, to limit property to intangible rather than tangible types - something which further supports IBMs "liquefying" notion. Further, the inherent intangibility, abstraction and movability of property rights themselves means that the registered and documented rights to things could be recorded and transacted using smart contracts on the blockchain, while the physical property itself could be managed and administered via the internet of things, including providing access in accordance with changes to ownership and possession. Smart contracts, therefore, map across both property rights and the corresponding physical property, making it easily (and instantaneously) transferrable, and completing conveyance or transaction without the need for human intervention. Indeed, recent discussions concerning the property-like nature of bitcoin and cryptocurrency more generally may help to explain how the distribution of property rights is possible in precisely this manner[22].

Considering the notable differences between contracts and trust instruments in traditional legal terms, it is arguably not possible or desirable to map one too closely atop the other, nor to blur the boundaries between the two unjustifiably. Further, as the legal status of smart contracts is still very much a live debate, namely whether they ought reasonably to be thought of as contracts at all, it is reasonable to be cautious about introducing further complexity and therefore uncertainly by marrying them to smart trusts[23]. However, because smart property is a key consideration for smart trusts; and smart property is largely defined by its use of smart contracts; any serious attempt to development a smart trust would inevitably involve a complex of "smart" elements. As mentioned previously however, from the legal standpoint this would largely involve applying legal character to computational processes that do not necessarily diverge in character themselves. From a technical or computational point of view, the process that facilitates a smart contract could be identical that which facilitates a smart trust.

Notwithstanding the fact that smart contracts are arguably not contracts as lawyers understand them, but are instead a series of useful and, importantly, proven computational processes that

---

[21] Szabo, N. (1994) Smart Contracts [blog] available at: http://szabo.best.vwh.net/smart.contracts.html (accessed 12th February 2016)
[22] See for example: Hoegner S. (ed.) *The Law of Bitcoin*, Bloomington: iUniverse
[23] See for example: Allison, I. (2015) "Norton Rose Fulbright considers the legal status of smart contracts", *International Business Times*, 14th December [online] available at: http://www.ibtimes.co.uk/norton-rose-fulbright-considers-legal-status-smart-contracts-1533313 (accessed 18th February 2016)

Working Paper

facilitate, verify and enforce machine-based commands in the guise of legal contracts, means that they could potentially offer a template for smart trusts. In other words, generic processes undertaken by smart contracts, such as the matching of private and public keys in order to unlock a contractual provision engendered by the code, which in turn releases payment for a particular contractual service, could be re-versioned to perform a "trust" instead of a "contract" from a legal perspective. Furthermore, smart contracts, as the vanguard of contemporary digitized legal products, provide a good model for assessing the evolutionary stages legal instruments or mechanisms, including trusts, must or will pass through on the road to becoming "smart". This includes a strong emphasis on the incorruptibility of the processes involved, including the use of cryptographic keys to make them more secure. To be precise, smart contracts make it more difficult to effect a breach in terms of, for example, withholding payment for a delivery or service, as the contract will only automatically transfer payment when the terms and conditions are partially of fully satisfied or performed. To conclude we will now apply some of these ideas to a basic express trust context.

Trusts law and the blockchain

The blockchain is no-longer science fiction. Instead it is an increasingly potent socio-economic, legal and political tool that has piqued the interest of powerful corporations, individuals and governments alike[24]. Analysis of the technology from the perspective of private law, and in terms of Common Law and Equity's rules, remedies and doctrines surrounding property and trusts in particular, is greatly lacking. From an Anglo-American and Australian Common Law perspective, consideration of the role Equity will play in the scene now being set by this new technology remains particularly vague, beyond a few tangential comments relating to specific performance of bitcoin contractual obligations, i.e. a contract to pay bitcoins[25].

It is beyond the scope of the present article to discuss all areas of interest or points of impact between the Common Law, Equity and the blockchain. But based on a large amount of commentary focusing on the relationship between the concept of trust and the blockchain alone, there is clearly a need to consider trusts law, and the role of trustees in particular (as well fiduciaries more broadly), in light of the technology. For present purposes we will explore the blockchain in light of some basic principles of express trusts and trusteeship. The fact that the blockchain has not been tested in terms of trusts and fiduciary law, and therefore lacks both

[24] For example: Robert J. J. (2016) "The Crisis in Bitcoin and the Rise of Blockchain", *Fortune*, March 4th, [online] available at: http://fortune.com/2016/03/04/crisis-in-bitcoin-rise-of-blockchain/
[25] Bayern, S. (2014) "Dynamic Common Law and Technological Change", *Washington and Lee Law Review Online*, 22:1, p.27

Working Paper

jurisprudence and jurisdiction, necessarily means that much of the discussion remains academic at this point in time.

Express Trusts

It ought to be clear that the promise of the blockchain to "solve" issues relating to trustworthiness, or the inherent weaknesses of trust based models, means the technology is primed to disrupt the very foundations of trust constitution, including those surrounding the formalities required for a trust to be deemed valid. As stated in the introduction to this article, as well as during preceding sections, there is already good cause to believe that blockchain architecture can be mapped onto trusts, or *vice versa*. With evidence from existing, if still somewhat immature, post-trust paradigms facilitated by the blockchain in the growing legal domain of smart contracts.

A distributed "trustee" architecture could, in theory, remove the need for continuous human intervention in and monitoring of express trust funds by a single trustee, group or board of trustees, and thus remove problems of accountability and, more importantly, the potential for any breach of trust. Moreover, the potential for increased security and efficiency of smart trusts and distributed trusteeship would arguably improve the overall investment strategy of the trust, thereby creating better returns for beneficiaries. How realistic is it, however, to supplant existing trustee obligations and duties from a practical point of view?

Firstly, how would the trust that trustees must command in the minds of beneficiaries be supplanted? Traditionally the trustee accepts onerous duties as part of their office, including significant fetters upon their individual or personal autonomy when dealing with trust property, in order to prevent, for example, situations in which a trustee seeks to gain financial advantage or enrichment based on inside knowledge. Moreover, as a paradigm fiduciary relationship, the trustee owes the beneficiary loyalty and fidelity and must account for any situations in which these duties are called into question or breached, including where the trustee has acted outside of or beyond the limits imposed upon them by the trust arrangement. It is to that end that within the four corners of the trust instrument and in the eyes of the beneficiary a trustee engenders trust. However, the long-history of trust law is complicit in the fact that trustees, being at best infallibly human, at worst nefarious fraudsters, do breach trusts and do undermine the trust invested in them by their beneficiaries.

Given the outline of the blockchain discussed thus far, the short answer as to how the trust obligation of trustees would manifest itself differently in a smart trust context is that it would likely not be analogous. Primarily this is because trust in this context would not be predicated on any requirement for an individual trustee or board of trustees needing to be trusted as such. "Trusteeship", understood in the blockchain context, is both distributed across a whole network

Working Paper

and importantly reconfigured via at least two major conditions: the cryptographic and computation proof of the chronological order of transactions; and the running of the network (the process) itself, involving the building of chains by incentivized nodes able to generate more CPU power than "greedy attackers".

Together these factors inform the trustee-like character that could be mapped onto the processes performed by the blockchain, in order to produce trustee-like outcomes. It is clear, however, that whilst these processes can perform bare processes such as transactions, conveyances, investments etc., a point at which decisions are negotiated and made would still be needed - at least to the extent that the system could not intrinsically, for example, devise an investment strategy based on existing data held within the chronology of the blockchain. In the steps to running a network highlighted by Nakamoto, the first is that "new transactions are broadcast to all nodes"[26]. If we take "broadcast" in this case to mean the point immediately after a decision of what to broadcast has been made, then this would suggest that, at least in the majority of cases, human interventions would still be required; and, crucially, interventions that could carry the risk of unjust or unconscionable outcomes. A plausible if highly complex way around the issue of continued human trustee interventions would be for the trust arrangement itself – much like a smart contract – to be a series of protocols which, to all intents and purposes, embody the intentions of the settlor and execute different commands relating to trust property as coded to do so. This might describe a viable way in which, for example, an estate is settled in a will, property distributed and testamentary trusts established following probate.

Other than problems supplanting the decision-making of trustees, and especially insofar as they ultimately link to notions of trust, there is also the problem, touched upon earlier, of how to supplant the trustee's obligation and duties insofar as those relate to the physical management, handling or delivery of property. Present technology means that it is not possible for a network of computers to exclusively manage, handle or transact tangible property in the real-world. Delivery of physical, tangible property into the hands of a new owner could not be performed or completed purely in computational terms, yet[27].

Transfer of property rights and ownership in terms of legal and equitable title, as when a settlor declares their intention to create a "dumb" trust, could, however, be performed as soon as that intention is captured in coded form. This would notionally alter existing formalities relating to

[26] Ibid Nakamoto (2008), p.3

[27] IBMs notion of the "liquefying of the physical world" would clearly change the capability of computers to administer and "deliver" property as such. Transfer of ownership and the associated control assumed by a new owner of, for example, a house, car or other piece of physical property could be associated with an "unlocking" process or mechanism commanded by the blockchain via elements of the property that are connected to the internet of things, including door knobs and other modes of access and control.

Working Paper

the creation of some express trusts, however. It would prevent, for example, smart trusts regarding personal property from being created orally. The need for "written" code would mirror other existing trusts where formal written documentation is required however, most notably trusts of land, meaning the creation of smart trusts would comply with recognizable and valid rules and principles of trusts law. This would in effect mean all smart trusts, involving all types of property, would require formalities and processes analogous to the writing requirements under s.53(1)(a) and (b) of the Law of Property Act 1925 ("LPA") for trusts of land, and s.53(1)(c) for dispositions of equitable interest. Whether code for the creation of smart trusts and for smart property transfers in this context would be considered "writing" for the purpose of tax liability is obviously yet to be tested. The closest HM Revenue and Customs ("HMRC") seem to have come to defining such liabilities was in relation to VAT for bitcoin transactions, and in a 2014 briefing the conclusion was that these transactions would not be subject to VAT[28].

With the advent of advanced voice recognition and biometric software, such as that now being used in the banking sector[29], it could be possible, in the not too distant future, to replicate the creation of "dumb" oral trusts. In such a circumstance, the settlor could orally declare their intention to create a smart trust and identify each item of trust property subject to the fund. This orally-captured intention could then be translated into a coded smart trust arrangement, broadcast or published to the blockchain, any potential beneficiaries could be notified, and the process of any investment or management of property on the beneficiary's behalf could begin seamlessly and without any delay. There would be no trustees as such, and the blockchain would instead act in a trustee-like capacity by securing, verifying and witnessing each transaction and investment made on behalf of the beneficiaries. Indeed, as we might expect in relation to bank transfers today, the whole process of creating a smart trust in this way could be almost instantaneous.

Conclusion

Generally-speaking there has been a notable lack of engagement, scholarly or otherwise, with trusts law and trusteeship in legal debates and discussions of the blockchain that are otherwise greatly informed, even obsessed by, the concept of trust. The 2008 Nakamoto white paper that spawned today's blockchains was predicated on the need for payment transaction system that did not suffer from "the inherent weaknesses of the trust based model"[30], and this signalled the

[28] HM Revenue and Customs (2014) *Revenue and Customs Brief 9: Bitcoin and other cryptocurrencies*, [online] available at: https://www.gov.uk/government/publications/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies/revenue-and-customs-brief-9-2014-bitcoin-and-other-cryptocurrencies (accessed 18th February 2016)
[29] For example see: "HSBC offers voice and fingerprint ID system to customers" (2016), BBC News [online] available at: http://www.bbc.co.uk/news/business-35609833 (accessed 25th February 2016)
[30] Ibid Nakamoto (2008), p.1

Working Paper

centrality of trust to the development of the blockchain architecture from the outset. This article was aimed, therefore, at responding, even if somewhat speculatively, to questions of how this rapid shift in technology that is already touching other legal domains, will likely touch and concern trusts and trusteeship.

At a more fundamental level, questions of the potential transformation of conceptions of property and property rights that the blockchain and other associated technologies, namely smart property and the internet of things, may facilitate also demand more attention. Bitcoin has already featured litigation in the United States, where the courts were forced to confront uncertainly over the category of property bitcoin ought to be included in[31]. There is reason to believe, therefore, that further challenges to the nature of property and property rights may not be far behind.

Many aspects of the blockchain, smart property and the internet of things, and especially how these relate to and potentially impact upon trusts and trusteeship, have been left untouched in this article. It is only realistic at this stage to approach the subject with a degree of generality that some may find frustrating. For others this article will hopefully shine a light on a matter of growing legal importance. Echoing the quote from Jacques Ellul that featured at the start of this article, it is surely incumbent on lawyers to remain sufficiently up-to-date technically in order to make a valid discovery which "rationally follows its predecessors and rationally heralds what is to follow"[32].

Working Paper

[31] For example, as a Texas District Court first suggested in 2014 in *Securities and Exchange Commission v Trendon T. Shavers and Bitcoin Savings and Trust*, Civil Action No. 4:13-CV-416, bitcoin ought to be considered money; more recently, following the decision in the February 2016 California bankruptcy case of *In re Hashfast Technologies* (Case No: 14-30866 DM), bitcoin was referred to as a commodity and not currency. The law in the United States has, for the time-being at least, settled on bitcoin as intangible property.
[32] Ibid Ellul (1964), p.90