GRIFFITH UNIVERSITY

GRIFFITH LAW SCHOOL

Social Science Research Network Legal Scholarship Network

Griffith Law School Research Paper No. 19-09

Adrian McCullagh
John Flood

Blockchain's Future: Can the Decentralised Blockchain Community Succeed in Creating Standards?

Blockchain's Future: Can the Decentralised Blockchain Community Succeed in Creating Standards?

Adrian McCullagh* and John Flood^[1]

Griffith University

*Law Futures Centre and ^Griffith Centre for Social and Cultural Research

Abstract

Nakamoto proposed a new solution to transact value via the internet. And since 2009 blockchain technology has expanded and diversified. It has, however, proven to be inefficient in the way it achieves its outcomes, especially through the proof of work protocol. Other developers are promoting alternative methods but, as yet, none has superseded proof of work. The competing protocols illuminate a key feature of the blockchain community, namely, its inability to create consensus in a decentralised community. Because of this lack of consensus the formation of standards is particularly difficult to achieve. We examine three areas where some form of agreement over standards will be essential if blockchain is to evolve successfully. These three areas are blockchain governance, smart contracts, and interoperability of blockchains. We argue that because standards formation is such contested process the blockchain community will persist in creating difficulties for itself until it is able to overcome internal divisions.

1. Introduction

In 2008 Satoshi Nakamoto (2008) proposed a method which would allow untrusted parties to transact value without the intervention of a third party. The technology underlying blockchain deployments had been known for more than 30 years but it took the eclectic thinking of Nakamoto to create a new kind of data repository that solved a very important missing link in e-commerce (Haber and Stornetta 1990). All financial transactions relied upon the intervention of a trusted third party.[2] Prior to the Nakamoto paper the internet was principally a global information publishing environment.[3]

The missing link was whether it was possible to transfer value in non-face-to-face transactions over telecommunications infrastructure without the need of a trusted third party. Nakamoto's solution meant the parties did not even need to know the identity of the other party to the transaction.[4] All that is required is some benefit without the need to authenticate either party to the transaction (Catalani and Gans 2019). Although Nakamoto's solution for bitcoin is elegant, there are issues that have caused

many organisations to investigate ways of improving the commercial usefulness of the blockchain concept (Flood and Robb 2017).

Even though the Nakamoto paper was initially published on a narrow group list-server which was dedicated to cryptography, what set the paper apart from other technical papers was that Nakamoto and his or her collaborators eventually implemented the bitcoin concept, first released in January 2009. The concept was slow to develop, but by 2012 a group of New York bankers became aware of the paper and immediately identified that instead of a so called "coin" being transacted a simple value concept could be substituted.[5] Both law and economics have each for more than 100 years understood that all property from a conceptual perspective comprises a bundle of rights (Coase 1960). Hence, there has been increasing interest in the possibilities of blockchain deployments globally across many industries.

Nakamoto does not actually use the term "blockchain" in the paper but instead uses the phrase "chain of blocks". It is important in any discussion dealing with "blockchain", that there is a common understanding as to the meaning of a "blockchain". For the purposes of this paper the NIST definition will be adopted (Yaga et al 2018: ii):

> Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e. without a central repository) and usually without a central authority. At their most basic level, they enable a community of users to record transactions in a ledger that is public to that community, such that no transaction can be changed once published.

Since blockchain is developed through community protocols without a central authority, we can say there is an "anarchic" state of affairs—because of its Hydra like growth—with respect to blockchain raising questions about standards around interoperability. This is important as even the Governor of the Bank of England has said blockchain is the start of the fourth information revolution that will eventually impact every economy globally (Herian 2018).

This paper interrogates three key issues which are the most pressing from a practical perspective as opposed to technical. They are:

1. Blockchain governance through standardisation to assist in advancing the uptake of blockchain usage and security of keys
2. Smart contracts need defined or uniform characteristics to assist commerce by improving the efficiency and efficacy of commercial transactions
3. Interoperability between blockchains is a persistent issue from a commercial perspective. There are many blockchain deployments that support smart contract execution such as Cardano,

> Ethereum, and EOS. How interoperability is settled remains an open question and the development of standards will assist this process

In the next section we examine the sociological and economic aspects of standards and how they can substantially advance the diffusion of new technologies.

2. The Development and Implementation of Standards in Blockchain

Timmermans and Epstein (2010: 71) define standardization as

> a process of constructing uniformities across time and space, through the generation of agreed-upon rules. The standards thereby created tend to span more than one community of practice or activity site; they make things work together over distance or heterogeneous metrics; and they are usually backed up by external bodies of some sort, such as professional organizations, manufacturers' associations, or the state.

Standards are voluntary statements that set out specifications, procedures and guidelines that aim to ensure products, services, and systems are safe, consistent, and reliable.[6] They often substitute for state action when states are reluctant to be involved, but they are now an essential and fully incorporated part of the global economy. Marx (1867) noted the relentless growth of world markets and their need to push away from distinctiveness towards homogeneity.[7] Institutional theory shows us that the very diffusion of standards across organisations leads towards eventual compliance with legal standards (Edelman 1992). Governments and courts can and do become involved in both the creation and enforcement of standards. Yet it is important to note the creation of standards is a social act and therefore is always contested because of competing interests. The crucial aspect is gaining consensus among the stakeholders in order for standards to emerge. But standards setting is not a one-time event as Lampland and Star (2009) have shown, "tinkering, repairing, subverting, or circumventing prescriptions of the standard are necessary to make standards work". This is especially so with blockchain.

A substantial issue at hand with blockchain diffusion is that the technology is still developing and is currently in flux. For example, the consensus protocol for bitcoin and Ethereum involves proof of work. This protocol takes advantage of the random characteristic of cryptographic hashes.[8] That is, knowing a document's structure, you cannot, by looking at the document, predetermine what hash will result. Likewise, in looking at a hash is it impossible to determine which document produced the hash. Furthermore, every hash should be equivalent to the "DNA" of the document in that every meaningful document must create its own unique hash and thus collisions should be mathematically improbable.

Finally, every document no matter its length or structure will result in a fixed length set of bits known as a hash. For example, the SHA256 algorithm will result in a hash length of 256 bits no matter what the length of the original input document may have been. That is, if the Bible and the Complete Works of Shakespeare were each operated on by the SHA256 algorithm, the result would be two distinct hash results other than each hash would be represented as a fixed length string of 256 bits.

The problem with the proof of work structure is that it is a brute force mechanism which is time consuming and thus energy inefficient (Vries 2018). To solve this issue, there have recently been proposed several alternative consensus protocols involving proof of stake.[9] The principal benefit of a proof of stake (PoS) solution is that it is energy efficient with an increased rate of transaction capability. For example, in the Ouroboros proof of stake protocol, which is being implemented in the Cardano blockchain, the network members elect a subset of members known as "Slot Leaders" to mine the next block. It is important that some form of entropy for the selection of slot leaders is achieved by having a randomisation factor included in the selection process. A further benefit is that if PoS is properly implemented it should overcome any possibility for the evolution of a dominant party or the collusion of several players,[10] whose combination would control greater than fifty per cent of the block determination capability.[11]

There are other new consensus protocols and, with certainty, more will be developed. For example, Intel has proposed its Proof of Elapsed Time consensus protocol (otherwise known as Sawtooth) which is dependent upon the Intel SGX chip.[12] The advantage of the Proof of Elapsed Time is that most of the calculations occur within the security of a trusted hardware chip.

Despite the uncertainty of settled consensus protocols, which is a fundamental component of most blockchain deployments, standards can still play a role in assisting in specifying a selection mechanism for each of the proposed consensus protocols. However, standards development can be slow and time-consuming and blockchain development waits for nothing. New developments arise weekly and it is not uncommon for standards to take years to be approved.

2.1 Governance, Standards and the Tragedy of the Anti-commons

As we have seen in the first decade of blockchain development, failures of governance in blockchain and associated cryptocurrency areas can hamper the advancement of distributed ledger technology. The Segwit issue within the Bitcoin environment is a prime example of this (Pepjin 2017). Heller (1998) illustrated in the "Tragedy of the Anti-Commons" that, if an asset is subject to multiple interests through which any party having an interest can veto or impede an advancement of the technology, then this will adversely impact the future development of the technology. And given

blockchain is a distributed ledger technology it is highly probable that contests over its bearing are inevitable.

It is possible for majority arrangements to be implemented, but even this can create concerns for anyone that does not agree with the decision. The forking of Bitcoin and Bitcoin Cash is a clear example of consensus not emerging along with that of Ether and Ether classic (Zhang 2018). If organisations or individuals do not agree to a fork then new blockchain structures emerge which compete with the original one.

2.2 Data Governance

A distributed data repository itself causes compliance issues for organisations. They need to exercise care within the architecture of a blockchain environment to ensure confidentiality and privacy are not compromised. Distributed frameworks across multiple parties give rise to problems in data governance. And these are of special concern since the activation of the European Union's General Data Protection Rules (GDPR) which came into force in May 2018.[13]

One method of compliance with the GDPR is to ensure that the blockchain itself does not actually hold any personal identifiable information (PII). This can be achieved by having all PII stored off-chain in a separate data repository and for an application to be stored on the blockchain that can interrogate the off-chain repository for business purposes. This problem is further compounded when multiple organisations form a consortium to use private blockchain networks. Each member would have to agree to a common standard of data management and governance.[14] In dealing with these top-level issues the impact on exiting members would give rise to various compliance requirements depending on the information stored within the consortium blockchain itself. Thus blockchain architecture will need to be carefully designed so that any sensitive corporate information is stored off-chain but still accessible through the blockchain environment.

Exiting members are further restricted owing to the blockchain data structure which will prevent any single member from removing their reference data from the network. Nor would it be possible for the continuing member parties to request the exiting party to remove the continuing members parties' data from the exiting party's instance of the blockchain at the date of exit. Some form of exit agreement would be necessary to coordinate exits from the network and its dissolutions. With peer to peer networks the exiting party's instance of the blockchain will necessitate exclusion from further appending of data after the exit. Further complicating factors include what happens to smart contracts already deployed and destined to continue to transact (Szabo 1996). How would individual instances of smart contracts be terminated, if possible, without damaging the blockchain?

2.3 Key Security

The blockchain environment has been described as a "trustless" mechanism. The basis for this position is that neither party needs to necessarily know the other transacting party. Therefore, they do not need to trust the other party in order to effect the financial aspects of the transaction. This has a strong theoretical attraction, but each party must have confidence in the technology that is used in the transaction. McCullagh has argued that in electronic transactions, before parties can have confidence in any technology, they must possess an initial trust in the technology (McCullagh 1998). Thus trust is crucial in the successful deployments of new technologies.

In common with other forms of technology security is essential. Blockchain's use of public and private keys has the potential to intensify the problems associated with password protection that beset many individuals and organisations today. While the public key enables the pursuit of transactions, private keys are meant to be personal and wholly private. With the advancement and development of blockchain technology a fundamental aspect of the technology is the protection of the private key that is used to carry out transactions on the blockchain. Most implementations of blockchain whether bitcoin or other financially-based deployments do not adequately protect the private key which is essential for all transactions.

The problem of key security in blockchain is analogous to password security in online banking. The use of password managers and two-factor authentication provides extra levels of protection but ultimately it is the user's responsibility to ensure proper security. The crucial distinction between online banking and blockchain use is that banking deposits are brought under regulatory insurance mandates whereas, for example, Bitcoin deposits are not insured. As long as keys, however encrypted, are stored on machines connected to the internet, they are vulnerable to hacking attempts.[15] At present the most secure method of storing and isolating the private key from attacks to use offline hardware security modules or hardware wallets, but they too present their own security issues. There have been published incidents where hackers have cracked the security of a hardware wallet and surreptitiously copied the private key. To create confidence in the generation and storage of the key pair for blockchain usage the hardware wallet should meet a recognised standard so that transaction integrity is accomplished. One such standard is FIPS 140-2 level 3 certification, which is a US Government security module certification program with level 3 being dedicated to hardware security module security. Very few hardware wallet providers have this certification.[16]

2.4 Smart Contracts, Security and Enforceability

In 1996 when Nick Szabo published his proposal for smart contracts the underlying technology had not been developed (Szabo 1996), but since the advent of blockchain and the introduction of the Ethereum platform in 2015 smart contracts have become in part a reality.[17] Szabo saw smart contracts as a way of embedding security into hardware and software and have been described as "user defined programs running on top of a blockchain". As originally conceptualised by him (Szabo 1996)

> a smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitrations and enforcement costs, and other transaction costs.

The testing issue with smart contracts is that they are neither smart nor a contract.[18] A contract is basically any agreement between two or more legal entities that will be enforced by law. Instead the smart contract code will be implemented and enforced by the blockchain. For public policy reasons smart contract code will, if there is a dispute, be reviewed by the courts to ensure that the code does not execute in a manner that offends current legal policy. For example, the courts will enforce a liquidated damages clause, but they will not enforce a penalty clause. An enforceable liquid damages clause is one where the parties agree at the time of contracting as being a genuine pre-estimate of the possible ensuing damage that could occur in case of a breach. Szabo's aim was to make a breach of contract expensive for the breacher (Szabo 1996). Such a position is not acceptable to the courts for public policy reasons. Firstly, it is not possible to oust the court's jurisdiction by encoding the contract to make it inaccessible. Secondly, as Keane J, in *Lucio Robert Paciocco & Anor v. Australian and New Zealand Banking Group Limited* stated:[19]

> Equity regards a collateral provision designed to provide an incentive to perform a principal obligation as objectionable on the ground that its enforcement was unnecessary to give the promise the benefit of the substance of the transaction.

Further, Lord Neuberger and Lord Sumption in *Cavendish Square Holding BV v Talal El Makdessi* [20] stated that:

> The true test is whether the impugned provision is a secondary obligation which imposes a detriment on the contract-breaker out of all proportion to any legitimate interest of the innocent party in the enforcement of the primary obligation. The innocent party can have no

> proper interest in simply punishing the defaulter. His interest is in performance or in some appropriate alternative to performance.

Consequently, for smart contract code to be enforceable at law it must not follow the Szabo proposal as such a position will be struck down as being unenforceable at law. Essentially the courts would not assist enforcement of contract provisions that are oppressive.

Since smart contract code is technically self-sufficient, once it has been invoked, it executes based upon certain events either occurring or failing to occur. If the result of a smart contract code is determined to be a penalty, and so unenforceable, there will need to be a way to correct the output written to the blockchain, taking into account the immutability of data written to the blockchain. The solution could be a court order compelling a party to prepare correcting code which will write a new record to the blockchain, without the need for a fork. In addition, there would have to be a termination mechanism incorporated into the code so no further records are written. But this too raises issues, especially if the contracts involve a one-to-many relationship and only one of the parties is actually disadvantaged, though it is difficult to see how this could in actuality occur.

The most basic issue with smart contract code is that there will be no errors in the code. Complexity, in any coded solution, always creates the possibility for errors to be included. In May 2016, the DAO code, a special smart contract that tried to establish the first Decentralised Autonomous Organisation, was released on the Ethereum blockchain and that code had some major vulnerabilities which caused the Ethereum stakeholders to implement a hard fork (Hinkes 2016). This was controversial at the time as many participants in the Ethereum blockchain believed code represented law and therefore it was against their beliefs that the Ethereum blockchain should be forked. The code contained a known bug which ultimately allowed one of The DAO's participants to divert 3.6 million ether (ETH), roughly valued at $50 million, into a "child DAO" controlled only by that participant. To the credit of the Ethereum hierarchy they decided to implement a hard fork so that all persons who were impacted by the vulnerability did not lose their investment. If such action had not taken place it would most likely had resulted in the first court case dealing with the failure of a smart contract.

There are real possibilities that smart contracts will not only interact with the particular blockchain in which they are embedded but could also interact with other blockchains. Consequently, interoperability becomes a potential major issue for commerce, since commercial contracts can be impacted by third parties who are not privy to the principal contract.

3. Interoperability of blockchains

It is reasonable to forecast that there will be multiple blockchains because of their decentralised nature and multiple environments are already being created, e.g. Cardano, NEM, Ethereum, and Hyperledger. And interoperability across blockchains will become a core requirement both from a mechanical and value levels (Hardjono et al 2018). NIST (Yaga et al 2018: 1) has defined "interoperable blockchain architecture" as:

> An interoperable blockchain architecture is a composition of distinguishable blockchain systems, each representing a distributed data ledger, where transaction execution may span multiple blockchain systems, and where data recorded in one blockchain is reachable and verifiable by another possibly foreign transaction in a semantically compatible manner.

Interoperability is not simple because it will depend on how data are stored on blockchains. Further, interoperability will need to contend with off-chain data sources and will be subject to data ownership and access policies invoked by owners of data sets (Ribitzky et al 2018).

According to Vitalik Buterin (2016):

> The benefit of interoperability is that it should open up a world where moving assets from one platform to another, or payment-versus-payment and payment-versus-delivery schemes or accessing information from one chain inside another (e.g. "identity chains" and payment systems may be a plausible link) becomes easy and even implementable by third parties without any additional effort required from the operators of the base blockchain protocols.

Within this context the most likely mechanisms for moving assets will be smart contracts and we examine some of the many external factors that influence the performance of contracts and smart contracts.

3.1 Interoperable mechanisms and interference of contracts

The performance and outcome of any contract is affected by both internal and external factors. For example, even an instantaneous contract can be so affected. If an instantaneous contract is a sale of goods contract where a consumer purchases goods from a merchant, then for the most part the transaction is completed in a moment. The consumer usually pays over some consideration (money) and the merchant delivers and transfers title in the goods to the consumer. The basic terms of such a contract is that an offer is made by the consumer and the merchant accepts the offer and in consideration of payment title and delivery of the subject matter occurs instantaneously. In effect the contract is formed and completed immediately—buying a chocolate bar in a 711 store would be an instance of such a contract—but that is not the end of the contract.

There are occasions when regulators recall goods, post completion, which reverses the entire contract, e.g. children's toys being dangerously manufactured or food items that have been open to tampering. And usually consumer contracts have basic implied terms that the goods or services delivered will be of merchantable quality. The results are that the goods or services must be in good working order for a reasonable time post completion of the contract. If they are defective and such defects are discovered after completion, then the implied term will come into force which may result in requirements to rectify the defect or the merchant may be required to pay back the price to the consumer.

In addition to instantaneous contracts are longitudinal contracts sometimes known as executory contracts where performance is executed over a period. Examples of longitudinal contracts include loan agreements or mortgages where borrowers agree to pay the loan over a period and provide a security to support the loan. Other examples are contracts for services where a contract to build a rail tunnel over a 130 week period would be classified as longitudinal.

Longitudinal contracts by their nature are prone to external events occurring which can substantially impact performance. Because of that it is common for longitudinal contracts to contain force majeure clauses, also known as "Act of God" clauses. These clauses consider external events that are outside the reasonable control of either party. For instance, in dealing with a rail tunnel agreement the contract may provide for 24-hour tunnelling, but such tunnelling may adversely impact adjoining properties and the owners of these properties might obtain an injunction to restrict the tunnelling to 16 hours per day.[21] Since the external event would obviously impact the delivery of the tunnel the contract could be subject to the legal doctrine of frustration that would end the entire performance of the contract.

If smart contracts are to meet the business requirements of traditional transactional activity, then they should be designed to accommodate impacts of external factors. The question is how would a smart contract operating on Blockchain A be able to take into account external events that are recorded on another blockchain environment, Blockchain B. Suppose Blockchain B is an oracle operated by a trusted third party that collects trusted information like meteorological or geological data such as tremor data covering earth quakes. The smart contract on Blockchain A will want to be able to read data stored on Blockchain B as it would be important for determining whether force majeure events have occurred. Hileman and Rauch identified the current lack of interoperability between different blockchain frameworks as a major business concern (Hileman and Rauch 2018). They argue that interoperability generally falls into 2 major categories: Cross-chain interoperability, and Enterprise system integration and interoperability.

3.2 Interactions between cross chains

This section only discusses the first category as the second concerns issues extraneous to blockchains and therefore outside of scope of this paper. The first category involves the technical connection between separate blockchains that facilitate cross-chain communication, interaction and value transfer. For Hileman and Rauch (2018) the solution for implementing interoperability between separate blockchains is a Common Inter-chain Messaging Protocol, which involves the development of a common inter-chain messaging protocol, based either on an existing ISO protocol or an emerging dominant industry framework or application. Examples of the latter include Ripple's "Interledger Protocol", the Cosmos "Network Zones Project", and the Polkadot Project, which is a complementary protocol to Cosmos that allows different blockchains to leave their silos and interact seamlessly. It relies on relay chains and parachains which can be deployed through its protocol to build bridging chains for interoperability.

Cross chain capability is still in its infancy technologically. And if secure and trusted cross chain connectivity is not achieved, then this will become a major impediment in gaining the full benefit of blockchain technology.

3.3 Sidechains and interoperability

Sidechains are relatively new emerging mechanisms that enable digital tokens associated with one blockchain to securely interact with separate blockchains and then be moved back to the original blockchain if and when needed (Dilley et al 2017). Their essential property is that they are separate blockchains linked to parent blockchains via a two-way pegs, which permit digital tokens to be interchangeable and moved across chains at fixed deterministic exchange rates and operate by using simple payment verification proofs (Back et al 2014).

The development of interoperability is still in its infancy and much work remains to be undertaken. It is doubtful that one organisation would be able to solve this issue because it would require concerted effort by many industry organisations and academic researchers to specify a viable commercial solution that would be robust in a commercial environment. It is likely a solution will arise from both collaboration among and competition between different entities and institutions, some of which could be international standard setting organisations such as the ISO or the ITU.

4. Conclusion

Blockchain in its current configuration has much in its favour, given the creativity of the community, but because of its position within a decentralised community, agreements on future developments are

contingent on the community pulling together at crucial junctures. Thus far progress here is limited as we have indicated.

We identify three areas of concern where some form of standards will be necessary to enable future development. The first is blockchain governance which includes standards, data and key security. There are all kinds of problems with establishing standards. As we have emphasised, standards are constantly being contested, even in non-blockchain worlds, but the quintessential nature of the blockchain community increases the difficulty. Even when standards are established, and some accord exists, there is no guarantee they will remain stable. The second concerns smart contracts where the optimism for "code as law" in the blockchain community does not yet accord with the law of contracts and the lawyers' communities. To achieve some conformity between the two will require greater understanding between legal and blockchain communities, which remains open. The final area of concern is interoperability between blockchains. This is as much a technological problem as it is a social problem. With many differing solutions being promulgated, it is difficult to determine if consensus is feasible. How choices and selections will be made again remains open.

Blockchain is a community of contradictions, oppositions, alliances, and sometimes consensus. There is no way to bring the different factions together yet. The underlying political philosophy of blockchain is very much anarcho-capitalist (Flood and Robb), which places blockchain in the libertarian camp, one that is essentially anti-state and pro-individual. As business becomes more involved in developing and deploying blockchain, its roots will have less influence over its future.

5. References

Back, A, Corallo, M, Dashjr, L, Friedenbach, M, Maxwell, G, Miller, A, Poelstra, A, Timón, J, and Wuille, P, 2014. "Enabling Blockchain Innovations with Pegged Sidechains", https://pdfs.semanticscholar.org/1b23/cd2050d5000c05e1da3c9997b308ad5b7903.pdf?_ga=2.172033763.1563462457.1532138662-1341615866.1532138662.

Buterin, V, 2016. "Chain Interoperability", *R3 Report*, https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf .

Catalini, C and Gans, J, 2019. "Some Simple Economics of the Blockchain", Rotman School of Management Working Paper No. 2874598, https://ssrn.com/abstract=2874598

Coase, R, 1960. "The Problem of Social Cost" *Journal of Law and Economics* **3**: 1-44.

de Vries, A, 2018. "Bitcoins Growing Energy Problem", *Joule* **2** (5) pp 801-805.

Dilley, J, Poelstra, A, Wilkins, J, Piekarska, M, Gorlick, B and Friedenbach, M, 2017. "Strong Federations: An Interoperable Blockchain Solution to Centralised Third-Party Risks", https://arxiv.org/pdf/1612.05491.pdf.

Edelman LB, 1992. “Legal ambiguity and symbolic structures: organizational mediation of civil rights law”, *American Journal of Sociology* **97** pp 1531–76.

Flood, J and Robb, L, 2017. “Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings”, Griffith University Law School Research Paper No 17-23, https://ssrn.com/abstract=3074263.

Haber, S and Stornetta, WS, 1991. “How to Time-Stamp a Digital Document”, (1990) Advances in Cryptography, CRYPTO 90, LNCS 537, pp 437-455, A. Menezes, A and Vanstone, SA (Eds), Berlin Heidelberg: Springer Verlag.

Hardjono, T, Lipton, A, and Pentland, A, 2018. “Towards a Design Philosophy for Interoperable Blockchain Systems*”, MIT Connections,* https://www.researchgate.net/publication/325168344_Towards_a_Design_Philosophy_for_Interoperable_Blockchain_Systems.

Heller, MA, 1998. “Tragedy of the Anti-commons – Property in the Transition from Marx to Markets”, *Harvard Law Review*, **111** (3) p 621-688.

Herian, R, 2018. “Taking Blockchain Seriously**”** *Law and Critique* **29** (2) pp 163–171.

Hileman, G and Rauch, M, 2017. “Global Blockchain Benchmarking Study”, Cambridge Centre for Alternative Finance, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224.

Hinkes, D, 2016. “Legal Analysis of the DAO Exploit and Possible Investor Rights”, *Bitcoin Magazine,* https://www.nasdaq.com/article/a-legal-analysis-of-the-dao-exploit-and-possible-investor-rights-cm638561.

Lampland M, and Star SL, (eds.), 2009. *Standards and Their Stories: How Quantifying, Classifying, and Formalizing Practices Shape Everyday Life*, Ithaca, NY: Cornell University Press.

Marx, K, 1867. *Capital: A critique of political economy,* London: Penguin.

McCullagh, A, 1998. “E-commerce – A Matter of Trust” in *Proceedings of the 1998 Information Industry Outlook Conference.*

Nakamoto S, 2008. “Bitcoin: A peer-to-peer electronic cash sytem” https://bitcoin.org/bitcoin.pdf.

Pepijn, D, 2017. “What the fork is Segwit? Everything you need to know about Bitcoin scaling”, *The Next Web,* https://thenextweb.com/contributors/2017/09/13/fork-segwit-everything-need-know-bitcoin-scaling/.

Ribitzky, R, St. Clair, J, Houlding, D, McFarlane, C, Ahier, B, Gould, M, Flannery, H, Pupo, E and Clauson, K, 2018. “Blockchain in Healthcare Today: Pragmatic Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare.”, https://doi.org/10.30953/bhty.v1.24.

Shenhav, Y, 1999. *Manufacturing Rationality,* Oxford: Oxford University Press.

Szabo, N, 1996. “Smart Contracts: Building Blocks for Digital Markets”, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

Timmermans, S and Epstein, S, 2010. “A World of Standards but not a Standard World: Toward a Sociology of Standards and Standardization” *Annual Review of Sociology* **36** pp 69-89.

Yaga, D, Mell, P, Roby, N and Scarfone, K, 2018. Draft NISTIR 8202 “Blockchain Technology Overview*”, January 2018.* https://csrc.nist.gov/publications/detail/nistir/8202/final.

Zhang, E, "2018's Big Question: Can Bitcoin Forks Deliver Value?" https://www.coindesk.com/2018s-big-question-can-bitcoin-forks-deliver-value.

---

[1] The authors would like to thank the following persons for their useful comments in the preparation of this paper noting that the author takes full responsibility for any errors that may exist in this paper: Alan Davidson, John Humphrey, Mark Staples, Sandy Maitland, Burt Tregub, and Rick Skibo.

[2] Such organisations in Australia must comply with the non-cash payments facility provisions in the Corporations Act 2001 (Cth). These third parties are required to validate certain financial aspects of the transaction.

[3] Testimony of Sir Timothy Berners-Lee, before the United States House of Representatives Committee on Energy and Commerce (1 March 2007), http://dig.csail.mit.edu/2007/03/01-ushouse-future-of-the-web.html.

[4] Some commentators have described the blockchain as being a trustless environment, but in reality, this is not the case. There may not be a trust structure between the legal entities to the transaction but there needs to be some base trust in the technology deployed.

[5] It should be noted that the term "coin" is actually a metaphor. There is no coin, as such. In legal parlance, the term "coin" as used for a crypto-currency would be known as a "Humpty-Dumpty-ism". The so-called coin is simply a number stored in a block that forms part of the blockchain ledger and as such represents some stored value'. Consequently, the coin nominal is simply a metaphor for the representation of a coin.

[6] Standards Australia home page, https://www.standards.org.au/standards-development/what-is-standard.

[7] Economic historians have argued that standards emerged because production and goods crossed borders. See Shenhav 1999.

[8] In cryptographic terms a hash algorithm must possess the following characteristics: 1. First pre-image resistant, 2. Second pre-image resistant, 3. Collision resistant.

[9] Alternatives proposed include: Algorand Proof of Stake, Ouroboros Proof of Stake, Redbelly Proof of Stake, Casper Proof of Stake, and EOS Proof of Stake solution.

[10] Vitalik Buterin has criticized the EOS Proof of Stake solution because instead of ensuring entropy of validators, EOS has a static allocation of 21 validators which could collude and be subject to risk of bribes among block producers operating across different jurisdictions, https://www.reddit.com/r/eos/comments/6qmpjt/vitalik_buterin_on_eos/ <accessed 21 July 2018>

[11] Even Nakamoto identified in her/his/their paper that the Proof of Work protocol would be susceptible to a 51% attack. It has been identified that currently there exists a few miners that in combination do possess greater than 50% of the computer power which could substantially disrupt the stability of the bitcoin blockchain.

[12] See https://sawtooth.hyperledger.org/docs/core/nightly/0-8/introduction.html.

[13] For the GDPR see https://eugdpr.org/.

[14] A consortium's rules would have to cover, at a minimum, joining procedures, exit procedures, impacts on members and existing members after an exit has been completed, minimum security requirements, establishment of a membership committee, procedures to change the technical environments, and auditability of members security compliance.

[15] An example of this was identified in the case of *USA v. Scarfo et al.* 180 F. Supp. 2d 572 (D.N.J. 2001). This case was the first published litigation involving a key logger to capture the PGP private keyring. The FBI used a keylogger to capture the passphrase used by a suspected criminal concerning an encryption program known as PGP. Further, the FBI had transferred a copy of the private keyring which held the private key used by Scarfo in his electronic communications. The PGP application was an open source encryption program, hence the FBI all of the necessary components. In having all 3 components, the PGP program, the private-keyring and the access passphrase the FBI was able to monitor all communications even encrypted communications sent or received by Scarfo.

[16] SPYRUS Inc is a hardware security module provider based in Silicon Valley, California, that has obtained FIPS 140-2 Level 3 certification. FIPS certification is an expensive exercise but from an end user's perspective it should be a high priority to have peace of mind that their private keys are safe from unauthorised copying. After all, the safety of the end user's digital assets must be an essential element.

[17] The Ethereum Platform was developed by the Ethereum Foundation, a Swiss non-profit organisation. The initial project was bootstrapped via an ICO for Ether in August 2014 and went live on 30 July 2015. The Ethereum platform is designed as a decentralised platform that runs smart contracts.

[18] There are now attempts to combine legal and smart contracts. See OpenLaw at https://openlaw.io

[19] *Lucio Robert Paciocco & Anor v. Australian and New Zealand Banking Group Limited*. [2016] HCA 28; paragraph 257. (Australian HC), http://eresources.hcourt.gov.au/downloadPdf/2016/HCA/28.

[20] *Cavendish Square Holding BV v Talal El Makdessi* [2015] UKSC 67 (UK SC)

[21] *Codelfa Construction Pty Ltd v State Rail Authority of NSW* (1982) 149 CLR 337 (Australian HC)