# Blockchain: Riding the Rollercoaster towards a Standard***[[1]](#footnote-1)***

Adrian McCullagh[[2]](#footnote-2)

# Abstract

Nakamoto proposed a new solution to transact value via the internet. The internet prior to the advent of bitcoin was primarily a communications environment for non-face-to-face interaction. It was a global publishing environment. In order to carry out a commercial transaction it was necessary to involve some third party who would validate the financial aspects of the transaction. The heart of the bitcoin solution was the blockchain construct.

The blockchain as originally proposed with its proof of work consensus protocol has been shown to have some uncommercial aspects to which researchers globally are attempting to solve. Further, since the blockchain is a distributive environment, commercial compliance requirements can impact the architecture of a blockchain. The architecture of a blockchain must meet the regulatory compliance which could be industry specific such GDPR, financial and health regulatory obligations.

An important issue with the development of new technology that has international reach is that such technology should not become siloed. This is where standards especially international standards can assist. Of course, standards by themselves will not necessarily obviate the impediments to interoperability, but if standard interfaces, data structures and standard communication structures can be developed then the uptake of blockchain environment will be more likely to be achieved, which could financially benefit the global economy.

This paper will look at some of the issues confronting the further development of blockchain technology.

# Introduction

The technology underlying blockchain deployments had been known for more than 30 years but it took the eclectic thinking of Satoshi Nakamoto in November 2008[[3]](#footnote-3) to build the jigsaw puzzle to create a new kind of data repository[[4]](#footnote-4) that solved a very important missing link in e-commerce. Prior to the Nakamoto paper the internet had the principal characteristic of being a global information publishing environment[[5]](#footnote-5). All financial transactions relied upon the intervention of a trusted third party[[6]](#footnote-6).

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 described a method which would allow untrusted parties to transact value without the intervention of a third party. In fact, the parties did not even need to know the identity of the other party to the transaction. Much like what occurs when a consumer purchases an item from a grocery store using fiat currency. All that is required is some accepted form of consideration without the need to authenticate either party to the transaction.

Nakamoto’s solution for bitcoin is elegant though, there are issues that have caused many organisations to investigate ways of improving the commerciality of the blockchain concept[[7]](#footnote-7). Even though the Nakamoto paper was initially published on a narrow group list-server which was dedicated to cryptography, what set the Nakamoto paper apart from other technical papers was that Nakamoto and his/her collaborators eventually implemented the bitcoin concept which was first released in January 2009. The concept was slowly advanced within the cryptography environment, but by mid-2012 a group of bankers in New York became aware of the Nakamoto paper and immediately identified that instead of a so called “coin”[[8]](#footnote-8) being transacted a simple value concept could be substituted.

Both law and economics[[9]](#footnote-9) have each for more than 100 years understood that all property from a conceptual perspective comprises a bundle of rights. The rights can be either rights in rem or rights in personam[[10]](#footnote-10). These rights are intangible but can be represented conceptually through language and enforce by law. For example, Honore in 1961 explained that private property comprised 11 intangible incidents[[11]](#footnote-11). Being able to be expressed in language allows these rights to be metaphorically expressed as value rights which can be transacted via a blockchain. Hence, there has been increasing interest in the possibilities of blockchain deployments globally across many industries.

Interestingly, 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 what a blockchain is. There are various definitions as to what a blockchain is. For the purposes of this paper the NIST definition will be adopted[[12]](#footnote-12):

*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.*

Mark Carney the Governor of the Bank of England has stated the blockchain is the start of the fourth information revolution that will eventually impact every economy globally[[13]](#footnote-13). Having such potential, it is important that the technology does not get hijacked and become siloed through a lack of interoperability. Further, the technology is still developing through the advancement of research from both private enterprise and universities. For example, there are new consensus protocols being published weekly which have some advantage which the researcher has developed. If all of these protocols were deployed in various blockchains then an interoperability problem could arise which in turn could defeat the open structure of the technology.

Hence, since this is nascent technology there are many issues that require further research and settlement. It is not possible to canvass all issues that require further research hence this paper will only discuss the following issues and even then, there is not the space to delve into minutia of the matters that should be investigated. In fact, the International Standards Organisation has formed TC 307 to investigate 10 areas concerning blockchain and distributive technology standards development[[14]](#footnote-14).

It is not possible to delve into all 10 areas[[15]](#footnote-15) consequently this paper only discusses at a high level three research issues which, it is submitted, are the most pressing issues from a practical perspective as opposed to a technical perspective though of course in each of the selected areas there are technical issues that need to be resolved:

* Blockchain governance both internal governance and external governance warrants substantial investigation and how standardisation may assist in advancing the uptake of blockchain deployment especially with private blockchains and their members continued involvement;
* Smart contracts and what characteristics they could have to assist commerce by improving the efficiency of commercial transactions, noting that the term “smart contract” is really a misnomer and in many respects does not actually result in an enforceable contract;
* Interoperability between blockchains is going to be a persistent issue from a commercial perspective. There are many blockchain deployments that support smart contract execution such as Cardano, Ethereum, and EOS to name a few. How interoperability is settled remains outstanding. It is clear that no one blockchain will dominate the market. It is not like the “Lord of the Rings” where one blockchain will rule them all. Consequently, interoperability needs to be resolved and this can be assisted through standards development. A group within TC 307 is positioned to investigate possible approaches to interoperability and it is expected that this investigation will have a flow on effect to smart contracts and data governance.

Prior to dealing with these issues, it is important to understand the benefits and importance of standards and how they can substantially advance the diffusion of new technologies especially technologies that have the potential of being able to change society globally.

# The Benefit of Standards

Standards[[16]](#footnote-16) are voluntary documents that set out specifications, procedures and guidelines that aim to ensure products, services, and systems are safe, consistent, and reliable[[17]](#footnote-17). Allen and Sriram define standards as documented agreements containing technical guidelines to ensure that materials, products, processes, representations, and services are fit for their purpose[[18]](#footnote-18). Basically, standards can be categorised into three types as either being Regional, National or international. A Regional standard is a standard that is prepared by a specific region like Australia and New Zealand as a combined region[[19]](#footnote-19); whereas a National standard is a standard that is developed by an accredited standards body like Standards Australia for a specific jurisdiction and an international standard is a standard that has international standing where global harmonisation is beneficial. Since blockchain is a global issue then clearly it is beneficial that international standards are developed.

International Standards offer strategic answers for policy makers and businesses in attempting to decrease costs, increase productivity, access new markets, and facilitate freer and fairer global trade. These standards also embody universally agreed procedures or practices to enhance the diffusion of new technologies that have the potential to impact the global economy[[20]](#footnote-20).

A benefit of standards is that they allow products and services that correspond to their relevant standard to be supplied across different markets potentially reducing market inefficiencies and facilitating uniform regulatory compliance. That is, with an international standard a supplier that meets that standard should not have to redesign their product or service to meeting different market requirements and all markets can adopt uniform standard.

A substantial issue at hand with blockchain diffusion is that the technology is still developing and is currently in a substantial state of flux. For example, initially the consensus protocol for bitcoin and Ethereum involved proof of work. This protocol takes advantage of the random characteristic of cryptographic hashes[[21]](#footnote-21). 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 predetermine which document produced the hash. Further, every hash should amount 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[[22]](#footnote-22). To solve this issue, there have recently been proposed several alternative consensus protocols such as (to name a few):

* Algorand Proof of Stake by Professor Silvo Micali;
* Ouroboros Proof of Stake by Professor Aggelos Kiayias; and
* Redbelly Proof of Stake by Dr. Vincent Gramoli
* Casper Proof of Stake by Ethereum especially Vlad Zamfir; and
* EOS Proof of Stake solution.

The principal benefit of a Proof of Stake (PoS) solution is that it is energy efficient with substantial throughput of transaction capacity. For example, in the Ouroboros proof of stake protocol that 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[[23]](#footnote-23) whose combination would control greater than 50% of the block determination capacity.[[24]](#footnote-24)

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 which is dependent upon the Intel SGX chip. The advantage of the Proof of Elapsed Time is that most of the calculations occur within the security of trusted hardware chip.

Despite this current uncertainty in a settled consensus protocol which is a fundamental component of most blockchain deployments, standards can still play a role in assisting in providing a selection mechanism for each of these proposed consensus protocols. In general standards are not designed to be prescriptive in nature but can provide guidance as to the variations within a technology framework so that the best solution is available for each situation. But in expressing this view, the development of standards can be fraught with danger especially when large multinational organisations become involved which it is not unusual. A further point is that standards development is a slow and time-consuming exercise and blockchain development waits for nothing. New developments arise weekly and it is not uncommon for a standard to take multiple years to be approved.

# Blockchain Governance

##  Tragedy of the Anti-commons

As we have seen in the last 12 months a failure of governance in the blockchain/cryptocurrency area can impede the advancement of any technology. The Segwit issue within the Bitcoin environment is a prime example of this. As Heller illustrated in his seminal paper: “Tragedy of the Anti-commons”[[25]](#footnote-25), if an asset is subject to multiple interests through which any party having an interest can veto/impede an advancement of the technology then this can adversely impact the future development of the technology. Further, it must be remembered that a blockchain is a form of distributed data repository.

It may be that majority arrangements can be implemented but even this can cause further concerns for anyone that does not agree. The creation of bitcoin and bitcoin cash is a clear example as well as ether and ether classic. If an organisation does not agree to the hard fork then this can give rise to the creation of new blockchain structures which may even compete.

## Data Governance

A distributed data repository can itself cause compliance issues for organisations. Care needs to be undertaken in the architecture of a blockchain environment to ensure confidentiality and privacy are not compromised. This distributed framework across multiple parties gives rise to the question of data governance. Data governance issues are of concern especially since the activation of the European Union’s General Data Protection Rules which came into force on 25 May 2018.

It is possible to comply with the GDPR by ensuring 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.

A commercial consideration is that since an organisation’s data may be held by multiple organisations it is likely to arise that a consortium agreement/membership constitution will be adopted to participate, especially for private blockchain deployments. Each member to the consortium will be required to agree to follow the rules of participation. These rules should cover such things as:

* Joining procedure;
* Exiting procedure;
* The impact on members and existing members after an exit has been completed;
* Minimum Security requirements;
* Establishment of a membership committee;
* Procedure to change the technical environment;
* Auditability of members security compliance;

In dealing with these top-level issues the impact on exiting members could give rise to compliance requirements. It really depends on what information is stored within the blockchain itself. This is where the blockchain architecture will need to be carefully designed and how any corporate sensitive information can be stored off-chain but accessed through the blockchain environment.

Due to the immutability of the blockchain data structure it is not possible for any exiting organisation to simply remove their reference data from the various instances of the blockchain under the control of the continuing members of the consortium. Nor is it possible for the continuing parties to request the exiting party to remove the continuing parties’ data from the exiting party’s instance of the blockchain up to the date of exit. It may be that the protection of all parties requires an exit agreement to be executed so that certain obligations carry forward for the benefit of all parties.

With a peer to peer network the exiting party’s instance of the blockchain will need to be excluded from further append data post exiting. How this is going to be done has not been settled. A further complicating factor will be any smart contract that may already be deployed. How can an individual instance of a smart contract be terminated without impacting the other instances of the blockchain? Consequently, data governance issues will be also affected by the advent and deployment of smart contracts which were first proposed by Szabo in 1996[[26]](#footnote-26).

# Smart Contracts

At the time of Szabo’s proposal concerning smart contracts the technology had not been developed for its deployment, but since the advent of blockchain and the introduction of the Ethereum platform[[27]](#footnote-27) in 2015 smartcontracts have become in part a reality. But, no smart contract has ever been litigated and as such there are substantial uncertainties as to the enforceability and recognition of smartcontracts from a legal perspective.

A smart contract has been described as “*user defined programs running on top of a blockchain*”. As originally conceptualised by Szabo “*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”.[[28]](#footnote-28)*

The difficult issue with smartcontracts is that overall, they are not smart nor are they necessarily a contract.[[29]](#footnote-29) A contract is basically any agreement between two or more legal entities that will be enforced by law. Instead the smartcontract code will be enforced by the blockchain. For public policy reasons smartcontract 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 a clause whereby 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 in his revised paper on smart contracts stated the following[[30]](#footnote-30):

“*The basic idea behind smart contracts is that many kinds of contractual clauses (such as collateral, bonding, delineation of property rights, etc.) can be embedded in the hardware and software …, in* ***such a way as to make breach of contract expensive*** *(if desired, sometimes prohibitively so) for the breacher.” (emphasis added)*

Such a position will not be accepted by the courts for policy reasons. Firstly, it is not possible to oust the court’s jurisdiction. Secondly, as Keane J, in the Paccioco case stated[[31]](#footnote-31):

*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 the Cavendish case[[32]](#footnote-32) 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 smartcontract code to be enforceable at law it **MUST NOT** follow the Szabo position as such a position will be struct down as being unenforceable at law. That is, the smartcontract code must not be structured “*in* ***such a way as to make breach of contract expensive*** *(if desired, sometimes prohibitively so) for the breacher”.* To do so will cause a court to review the code and issue a correction order known as an injunction mandamus.

Further Lords Neuberger and Sumption went on to state with approval the comments made by Mason J and Wilson in case of *AMEV-UDC[[33]](#footnote-33)* :

At least since the advent of the Judicature system a penalty provision has been regarded as unenforceable or, perhaps void, ab initio: …. In all that time it has been thought that no action could be brought on such a clause, no doubt because the courts should not lend their aid to the enforcement in any way of a provision which is oppressive.”[[34]](#footnote-34)

But since the smartcontract code is technically self-sufficient it will automatically execute based upon certain events either occurring or failing to occur. If the result of some smartcontract code is determined to be a penalty and thus unenforceable there will need to be some way to correct the output written to the blockchain, taking into account the immutability of the data written to the blockchain. It may be that a court order will be set against one of the parties to prepare some further correcting code which will write a new record to the blockchain, without the need for a fork. Also, it should be noted that some termination mechanism would need to be incorporated into the code so that no further records could be written; but this too has its issues especially if the contracts involves a one to many relationship and only one of the many parties is actually disadvantaged though it is difficult to se how this could in actuality occur.

Another aspect in dealing with smartcontract code is that hopefully there will not be any errors in the code and this is where a real problem can occur. Once complexity in any coded solution occurs there is always the possibility for errors/bugs[[35]](#footnote-35) to be involved.

In May 2016, the DAO code, a special smartcontract 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[[36]](#footnote-36). This was controversial at the time as many participants in the Ethereum blockchain believed code was law (which it is not) 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 initial 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 smartcontract.

There are real possibilities that a smartcontract will not only interact with the blockchain it is embedded buy will also interact with other blockchains. Consequently, interoperability could become a major issue for commerce, as commercial contracts can be impacted by third parties who are not privy to the principal contract.

# Interoperability

There will not be a single blockchain unlike the internet; though initially some multinational IT organisations did try to highjack the internet in its informative development. Multiple blockchain environments are being created such as Cardano, NEM, Ethereum, and Hyperledger to name a few. It is important that siloed structures are not the norm.

Interoperability across blockchains will become a core requirement both from a mechanical level and a value level[[37]](#footnote-37). NIST has defined “interoperable blockchain architecture”[[38]](#footnote-38) 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 an easy task to achieve because it will depend on how data are stored on the blockchain. Further, interoperability will need to contend with any off-chain data sources referenced and will be subject to any data ownership and access policies invoked by the owner of the data set[[39]](#footnote-39).

According to Buterin[[40]](#footnote-40): “*The benefits 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 (eg. "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.*

The development of interoperability is still in its infancy and much work remains to be undertaken. No one organisation will be able to solve this issue because, it is submitted, it will require the concerted effort of many industry organisations and academic researchers to provide a viable commercial solution that is robust in a commercial environment. Only time will tell if such a solution is forthcoming. It may arise that the International Standards Organisation is well placed to assist in this endeavour.

# Conclusion

The blockchain in its current design has a lot of potential but from a commercial position is substantially unsustainable. Further development is required but it will be like being on a rollercoaster. There are highs and lows, twists and turns which hopefully will result in a stable environment as there are some exciting benefits at the end of the tunnel. The blockchain due to its characteristics can transform how industry sectors transact business, but in doing so there remain some technical elements that need to be resolved.

This paper discussed only 3 aspects namely.

* **Blockchain Governance** This issueis impacted by both internal and external factors.
	+ Internal Governance

Concerning the issue of internal governance, the SEGWIT issue last year for bitcoin was an example of the tragedy of the anti-common. The tragedy of the anti-common arises when multiple stakeholders can impede a resolution. Much like what occurs in the UN Security Council where any of the permanent members being able to veto/impede the resolution of any issue put forward by any other member. The role of the core coders and miners caused many issues in 2017 in the development and deployment of SEGWIT.

* + External Governance:

External Governance primarily concerns data governance where multiple instances of information can be spread across multiple parties who may be party of a consortium. The introduction of new members or the exiting of existing members can cause compliance issues to arise. Many compliance issues arise from a regulatory perspective such as security, and GDPR. This is especially for industry sectors like health, gaming/casinos and finance.

* **Smart Contracts**

A smart contract is some code that is permitted to write to the blockchain. That is to append new records to the blockchain. In the Ethereum environment the code will be stored in the blockchain itself. This results in some interesting issues. Contracts can be classified as either an instantaneous contract (also known as an executed contract) or a longitudinal contract (also known as a executory contract). Instantaneous contracts are contracts that in effect conclude at the time of their creation; like the purchasing of groceries, whereas a longitudinal contract involve some post entering performance like a contract for the delivery of some services such as a software development contracts. Another example of a longitudinal contract would be a mortgage agreement which requires the regular repayment of principal and interest over a period of time. But it should be noted that the term smart contract is a misnomer. For the most part the code is neither smart nor does it represent a contract.

* **Interoperability**

There will not be a single blockchain unlike the internet; though initially some multinational IT organisations did try to highjack the internet in its informative development. Being multiple blockchain environments being created such as Cardano, NEM, Ethereum, Hyperledger and others it is important that siloed structured are not the norm. Solving interoperability standards should be a high priority.

Creating a siloed environment will defeat much of the benefits that blockchain can deliver. It is not like the Lord of the Rings whereby one blockchain will rule them all. Each blockchain will be structured to solve particular problems but in doing so it is highly likely that interoperability will form part of the solution. This is where standards can assist. The above can be assisted through the development of appropriate standards, but it will take time and that is the greatest impediment for standards development as they take time and blockchain development waits for no committee.

1. The author 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: Professor John Flood, Professor John Humphrey. [↑](#footnote-ref-1)
2. Ph.D. (IT Sec), LL.B. (Hons), B. App. Sc. (Computing), ODMOB Lawyers, Adjunct Research Fellow, Law Futures Centre, Griffith University, Queensland, Australia.

amccullagh@odmoblawyers.com [↑](#footnote-ref-2)
3. Nakmoto, S [*"Bitcoin: A Peer-to-Peer Electronic Cash System"*](https://bitcoin.org/bitcoin.pdf)

<https://bitcoin.org/bitcoin.pdf> <accessed 29 June 2018> [↑](#footnote-ref-3)
4. In fact, Nakamoto was not the first party to propose the solution. Haber & Stornetta had 17 years earlier proposed a similar solution in linking documents in order through successive hashes. Haber,S., and Stornetta, W.S., “How to Time-Stamp a Digital Document” in Advances in Cryptography, CRYPTO 90, LNCS 537m pp 437-455, A. Menezes and Vanstone, S.A. (Ed), Spinger Verlag, Berlin Heidelberg, 1991 [↑](#footnote-ref-4)
5. Testimony of Sir Timothy Berners-Lee, before the United States House of Representatives Committee on Energy and Commerce

<http://dig.csail.mit.edu/2007/03/01-ushouse-future-of-the-web.html> <accessed 2 July 218> [↑](#footnote-ref-5)
6. 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. [↑](#footnote-ref-6)
7. #  Blockchain is not a panacea for all commercial problems. A cost-effective investigation that an organisation should undertake is the FITS investigative model. FITS stands for: (a) Fraud; (b) Intermediaries; (c) Through-put; and (d) Stable data. See Flood, J., and Robb, L., “Trust, Anarcho-Capitalism, Blockchain and Initial Coin Offerings”

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3074263> <accessed 6 July 2018> [↑](#footnote-ref-7)
8. 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”. See Liversidge v. Sir John Anderson and another.  [1941] UKHL 1; [1942] AC 206 Lord Atkin at p244

*[A judges] function is to give words their natural meaning, …The words have only one meaning. They are used with that meaning in statements of the common law and in statutes. …I know of only one authority which might justify the suggested method of construction: “ ‘When I use a word’ Humpty Dumpty said is rather a scornful tone. ‘it means just what I choose it to mean, neither more now less’ ‘The question is’ said Alice ‘whether you make words mean so many different things’ ‘The question is’ said Humpty Dumpty, ‘which is to be the master – that all’’ (‘Through the Looking Glass”)*

It is not uncommon in the IT sector for common words to be adopted and be given peculiar new means such as “bit”, and ‘bitcoin”. One of the best descriptions of a bitcoin is that it is a number that represents a value in whole or in part or a combination of both that is noted as a line item in a distributed ledger that has the quality of ensuring each line item is immutable and the line item is set against a public key which can only be transacted by any entity that possess the corresponding private key. [↑](#footnote-ref-8)
9. Coase, R.H. *The Problem of Social Cost.* Journal of Law and Economics V.3: (1960) 1-44 [↑](#footnote-ref-9)
10. Hohfeld, W. *Some Fundamental Legal Conceptions As Applied in Judicial Reasoning,* 23 Yale L.J. 16 (1913) [Part 1]; and Hohfeld, W., *Some Fundamental Legal Conceptions As Applied in Judicial Reasoning,* 26 Yale L.J. 710 (1917) [Part 2]

As Professor Hohfeld noted, rights in rem are rights that third parties recognise at law concerning a thing whether that thing is a physical item that can be picked up and physically handled like a glass or chair or it might be a metaphysical item that cannot be physically held but is recognised at law as being property like land which cannot be moved but the legal construct of trespass can prevent third parties from transgressing and thus exclusive possession can be attained. In contrast to a right in rem, an in personam right is a personal right attached to a specific person, such as contract rights involving contracts for the delivery or supply of specific services. Hohfeld identified that in rem rights are property rights enforceable against the entire world, whereas in personam rights are only enforceable by the parties who are privy to the contract for services. [↑](#footnote-ref-10)
11. Honoré, A.M., *Ownership*, *in* OXFORD ESSAYS IN JURISPRUDENCE, FIRST SERIES 107-47 (A.G. Guest, ed., 1961).

	* the right to exclusive possession of the thing,
	* the right to exclusive use of the thing,
	* the right to manage of the thing,
	* the right to the income of the thing,
	* the right to the capital of the thing,
	* rights to destroy the thing in question but subject to certain overriding legal requirements like not destroying a thing in a manner that endangers others or their property,
	* the right to consume the thing;
	* The right to security; that is “immunity from expropriation, in that the thing cannot be taken from the right-holder. This has been in many cases been over ridden through the right of the State to compulsory acquire private property but, in most cases, due value must be provided to cover the acquisition. There are exceptions to this where criminality has been involved under for example the proceeds of crimes legislation.
	* transfer (bequeathing) the thing,
	* Liability to execution—liability for having the thing taken away for repayment of a debt.
	* Residuary character—the existence of rules governing the reversion of lapsed ownership rights”; for example, who is entitled to the property if the taxes are not paid, or if some other obligation of ownership is not exercised; [↑](#footnote-ref-11)
12. Yaga, D., Mell, P., Roby, N., and Scarfone, K., *Blockchain Technology Overview Draft NISTIR 8202, January 2018.*

<https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf> <accessed 2 June 2018> [↑](#footnote-ref-12)
13. According to a *Financial Times* report on the World Economic Forum in Davos, Switzerland, in January 2018 ‘blockchain can no longer be ignored’

Noted in “Taking Blockchain Seriously**”,** Harian, R.,

Law Critique (2018) 29:163–171

<https://doi.org/10.1007/s10978-018-9226-y> <accessed 2 July 2018> [↑](#footnote-ref-13)
14. The areas concerning standards investigation are:

Terminology

Overview of privacy and personally identifiable information (PII)

Security risks and vulnerabilities

Overview of identity management using blockchain and distributed

Reference architecture

Taxonomy and Ontology

 Legally binding smart contracts

Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems

Security of digital asset custodians

Discovery issues related to interoperability

These areas have been allocated to 6 groups:

**WG1:** Foundations

**WG 2:** Security, privacy and identity

**WG 3:** Smart contracts and their applications

**JWG 4**: Blockchain and distributed ledger technologies and IT Security techniques

**SG 2:** Use Cases

**SG 6:** Governance of blockchain and distributed ledger technology systems

**SG 7:** Interoperability of blockchain and distributed ledger technology systems

Hence there are three working groups, one joint working group and three study groups. [↑](#footnote-ref-14)
15. To give justice to each area would require a chapter within a book hence only a high level discussion will be undertaken. [↑](#footnote-ref-15)
16. There are a number of international organisations that are investigating possible standards for blockchain development. These are:

International Standards Organisation (ISO) [TC307];

Institute of Electrical and Electronics Engineering [IEEE];

Internet Engineering Task Force (IETF); and

International Telecommunications Union (ITU); and

World Wide Web Consortium (W3C)

to name a few. [↑](#footnote-ref-16)
17. Standards Australia home page

<https://www.standards.org.au/standards-development/what-is-standard> <accessed 30 June 2018> [↑](#footnote-ref-17)
18. Allen R.H., and Sriram R.D., “*The Role of Standards in Innovation”* Technology Forecasting and Social Change, Vol 64, Issues 2-3, pp171-181 (2000)

[https://doi.org/10.1016/S0040-1625(99)00104-3](https://doi.org/10.1016/S0040-1625%2899%2900104-3) <accessed 30 June 2018> [↑](#footnote-ref-18)
19. An example of these are standards that are jointly developed for Australia and New Zealand only. [↑](#footnote-ref-19)
20. ISO (International Standards Organisation), “Economic Benefits of Standards” June 2011, [www.iso.org](http://www.iso.org) <accessed 2 July 2018> [↑](#footnote-ref-20)
21. In cryptographic terms a hash algorithm must possess the following characteristics:

First pre-image resistant;

Second pre-image resistant; and

Collision resistant [↑](#footnote-ref-21)
22. de Vries, A., *“Bitcoins Growing Energy Problem”,* Joule, Vol 2, Issue 5, 801-805. (2018)

<https://doi.org/10.1016/j.joule.2018.04.016> <accessed 30 June 2018>

also see: Bitcoin Energy Consumption Index

<https://digiconomist.net/bitcoin-energy-consumption> <accessed 5 July 2018> [↑](#footnote-ref-22)
23. 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. [↑](#footnote-ref-23)
24. 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. [↑](#footnote-ref-24)
25. Heller, M., “Tragedy of the Anti-commons – Property in the Transition from Marx to Markets”, Harvard Law Review, January 1998, Vol 111, Number 3. P.621 [↑](#footnote-ref-25)
26. ###  Szabo, N., *Smart Contracts: Building Blocks for Digital Markets* (1996)

<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html> <accessed 29 June 2018> [↑](#footnote-ref-26)
27. The Ethereum Platform was developed by the Ethereum Foundation which is 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. [↑](#footnote-ref-27)
28. Opcit note 11 [↑](#footnote-ref-28)
29. There are now attempts to combine legal and smart contracts. See OpenLaw at <https://openlaw.io> [↑](#footnote-ref-29)
30. Szabo, N., “Formalizing and Securing Relationships on Public Networks”, First Monday, 1997

[http://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher=First](http://firstmonday.org/ojs/index.php/fm/article/view/548/469-publisher%3DFirst)

<accessed 6 July 2018> [↑](#footnote-ref-30)
31. Lucio Robert Paciocco & Anor v. Australian and New Zealand Banking Group Limited. [2016] HCA 28; paragraph 257.

<http://eresources.hcourt.gov.au/downloadPdf/2016/HCA/28> <accessed 6 July 2018> [↑](#footnote-ref-31)
32. Cavendish Square Holding BV v Talal El Makdessi [[2015] UKSC 67](http://www.bailii.org/uk/cases/UKSC/2015/67.html) [↑](#footnote-ref-32)
33. *AMEV-UDC Finance Ltd v Austin* (1986) 162 CLR 170, at p. 191 [↑](#footnote-ref-33)
34. Mason J and Wilson expanded this view by also expressing the following:

*However, this is not the only reason why the courts would refuse to lend their aid. In the majority of cases involving penalties, the courts, if called upon to assist in partial enforcement of the kind suggested by the appellant, would be required to undertake an unfamiliar role. They would need to rewrite the clause so as to permit the plaintiff to recover the loss he has actually sustained. Penalty clauses are not, generally speaking, so expressed as to entitle the plaintiff to recover his actual loss. Instead they prescribe the payment of a sum which is exorbitant or a sum to be ascertained by reference to a formula which is not an acceptable pre-estimate of damage. In either case the court, if it were to enforce the clause, would be performing a function very different from that which it undertakes when it severs or reads down an unenforceable covenant, such as a covenant in restraint of trade. In the ultimate analysis, in whatever form it be expressed, the appellant’s argument amounts to an invitation to the court to develop a new law of compensation, distinct from common law damages, which would govern the entitlement of plaintiffs who insist on the inclusion of penalty clauses in their contracts* [↑](#footnote-ref-34)
35. Admiral Grace Hopper is attributed as first using the term “computer bug” though the first use of the term in relation to a failure of operations is attributed to Thomas Edison.

<http://theinstitute.ieee.org/technology-focus/technology-history/did-you-know-edison-coined-the-term-bug> <accessed 6 July 2018> [↑](#footnote-ref-35)
36. Hinkes, D., “*Legal Analysis of the DAO Exploit and Possible Investor Rights*”

<https://www.nasdaq.com/article/a-legal-analysis-of-the-dao-exploit-and-possible-investor-rights-cm638561> <accessed 6 July 2018> [↑](#footnote-ref-36)
37. Hardjono, T., Lipton, A., and Pentland, A., “*Towards a Design Philosophy for Interoperable Blockchain Systems”*

*MIT Connections, MIT 16 May 2018.*

[*https://www.researchgate.net/publication/325168344\_Towards\_a\_Design\_Philosophy\_for\_Interoperable\_Blockchain\_Systems*](https://www.researchgate.net/publication/325168344_Towards_a_Design_Philosophy_for_Interoperable_Blockchain_Systems) *<accessed 2 June 2018>* [↑](#footnote-ref-37)
38. OpCit note 5 [↑](#footnote-ref-38)
39. Ribitzky, R., St. Clair, J., Houlding, D., McFarlane, C., Ahier,B., Gould, B., Flannery, H., Pupo, E., Clauson K., *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> <accessed 2 July 2018 [↑](#footnote-ref-39)
40. Buterin, V., “Chain Interoperability”, R3 Report, September 9, 2016

[https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf](https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain%2BInteroperability.pdf) <accessed 2 July 2018> [↑](#footnote-ref-40)