Abstract

The aim of this paper is to demonstrate the disruptive potential of Blockchain, namely the technology behind BitCoin. As Blockchain is a distributed, shared, encrypted-database that serves as an irreversible and incorruptible public repository of information, it is possible to apply such an innovative technology on many legal grounds, like Contract Law, Property Law, Corporate Governance.

In particular this paper is focused on two main features of the said technology: to provide (an algorithmic) trust which can deeply reduce (and sometimes remove) the need for a third enforcing party, such a central authority; to produce better and much more verifiable information through a complex cryptographic mechanism which makes every Blockchain-based ledger incorruptible.

The paper is divided into five sections. Section 1. refers to a short description of the Blockchain technology. Sections 2.1. and 2.2. introduce the main applications of Blockchain, with a specific focus on the idea of Smart Contracts. Sections 3.1 and 3.2., by referring to the meaning of trust in relation to the notions of risk, uncertainty and transaction costs, describe Blockchain as a new form of legal institution, according to Douglas C. North’s theory of the impersonal exchanges.

*The Author graduated in Law at University of Pisa in September 2015 with a thesis on Private Law (Tort Law) and Environmental Law. At the moment he is writing a research project for a Doctorate in Law focused on the legal implications of the Blockchain technology, in particular in relation to a better definition of Property Rights on digital assets. For a better knowledge of the Common Law system, the Author is conducting his research in Ireland (from January to June 2016) thanks to an Erasmus Traineeship Program for post-graduate students.
Blockchain: a further step in the evolution of the impersonal exchanges

Giacomo Vergallo

Introduction
During the last two years, the deep impact that BitCoin had for the traditional definition of currency has greatly increased the attention of the economists on such a cryptocurrency; while the same has not yet happened for jurists. However, even the economists are in error when they concentrate their efforts on the application rather than on the technology behind it, namely Blockchain. Hence, the first goal of this paper is to shift focus on the latter.

Blockchain, indeed, can be seen as the pivot of a new technological revolution that has the potential, as the previous ones, to completely overturn our understanding of the world and, as a consequence, of the law. One of the main legal grounds interested by this revolution is Contract Law: the best evidence is represented by the idea of Smart Contracts (namely self-enforcing contracts which are governed by an algorithmic code that removes any risk of a breach). What was only theory in the 1997, now, thanks to Blockchain, could become reality. Given the many implications, first of all in terms of a massive reduction of the transaction costs, the second goal of this paper is to synthetically illustrate the main elements of such a new revolution.

However, the core of the paper, sections 3.1. and 3.2., consists of a dissertation about the interrelated economic and philosophic implications related to new Blockchain-based institutions, especially in the perspective of a renewed cooperation amongst the citizens which can lead to more efficient impersonal exchanges.

1. What is Blockchain

Blockchain, the technology behind the Cryptocurrency known as BitCoin, is a distributed, shared, encrypted-database that serves as an irreversible and incorruptible public repository of information. By using the type of cryptography called SHA-256, which is a one way cryptography where the disguised message can never be encrypted back to the original message, Blockchain can record...

---

1 This paper is part of a research project which has the aim to point out why the Blockchain technology should be applied to many traditional legal institutions of private law. Such a project requires a multidisciplinary research that involves Private Law, Law & Economics and Philosophy of Law. This paper, in particular, is based on the general part of the project which consists of the emphasis on a new concept of trust.
4 This is called the collision resistance.
chronologically every transactions into a smaller datasets referred to as “blocks”. Every block contains information about a certain number of transactions, a reference to the preceding block and an answer to a mathematical puzzle (known as “challenge string”) which is required to validate the data associated with that block.\(^5\)

Once a class or network participants (called “miners”) has found the answer (the “proof string”) to the said mathematical puzzle, the new block is broadcasted to all other active miners in the system. As a result, the other active miners start to verify that the proof string really solves the puzzle. In particular, the proof string is that one that, hashed\(^6\) with the challenge string, generates a specific number with certain mathematical properties, such as a specified number of zeroes at its start. The number of verifications a proof string receives acts as votes and the block with the most votes is added to the Blockchain; these votes are based on the amount of computational power (CPU) devoted to the system, meaning that the block with the most CPU associated with it will be the one that other miners accept as being the most accurate and verified block.\(^7\)

The first miner to solve the mathematical problem is rewarded, for example, by giving him a certain amount of BitCoin which did not exist before\(^8\) or through transaction fees.\(^9\) Of course, the reward represents an incentive for the miners to invest computational power: following their self-interest, at the same time they realize the purpose of the collectivity.\(^10\)

Thanks to the huge amount of CPU required by the mechanism of validation,\(^11\) Blockchain is considered an incorruptible database\(^12\) which can provide the society many advantages in terms, first of all, of transparency. Indeed, not only every transaction or event can be chronologically

\(^5\) Id. at 7.
\(^6\) A hash (output) is the result of a transformation of the original information (input). A hash function is a mathematical algorithm that takes an input and transforms it into an output.
\(^7\) This is the so called “Proof of Work”. But there are other mechanisms, like the so called “Proof of Stake”.
\(^8\) See Larissa Lee, New Kids on the Blockchain: How Bitcoin’s Technology Could Reinvent the Stock Market, Hastings Business Law Journal, Forthcoming; University of Utah College of Law Research Paper No. 138, p. 25. Available at SSRN: http://ssrn.com/abstract=2656501, “The reward released as a new block is added to the chain is called a coinbase reward […] Just like mining for gold or any other precious metal, the more Bitcoin that is mined the more difficult it is to receive a reward. At Bitcoin’s inception, a new block resulted in a 50 Bitcoin reward. Today, a new block results in a 25 Bitcoin reward. The coinbase reward will halve every few years until all 21 million Bitcoins are released, which is expected to happen in 2040”.
\(^9\) They can consist of an amount of Euro and, for this reason, the mechanism is possible even outside the BitCoin system. Furthermore, the miners can be administrative officers whose main function could be to validate the transactions without any necessity of a particular reward.
\(^10\) See Marc Pilkington, Bitcoin through the Lenses of Complexity Theory: Some Non-Orthodox Implications for Economic Theorizing, Handbook of the Geographies of Money and Finance, Pollard, J. & Martin, R.(eds.), Edward Elgar, Forthcoming, “Miners are self-interested in the sense that they hope to derive a future gain from their mining endeavor. Yet, the viability of the crypto-currency implies a sense of altruism amongst miners, ensured when individual and systemic incentives are aligned. Notwithstanding the existence of personal motives, there might exist a cooperative behavioral dimension in sharp contrast with a neoclassical economic arena dominated by Darwinian principles”.
\(^11\) This is due to two main reasons. First of all, the level of difficulty in generating a new block changes every two weeks so that each transaction takes an average of ten minutes to process: the more people are mining, the higher it becomes the level of difficulty of the challenge string, so that, to date, it takes around forty billion attempts to come up with one correct proof of strings. Moreover, given that every new added block contains a reference to the preceding block, it is impossible to hack a single block without rewriting all the Blockchain: this fact, of course, multiplies exponentially the CPU required.
\(^12\) To deeply understand this property it is necessary to know perfectly how Blockchain works: for a detailed exposition, see Larissa Lee, supra note 8; UK Government Scientific Adviser, supra note 2; Chris DeRose, Behind the Ingenious Security Feature that Powers the Blockchain, available at http://www.americanbanker.com/bankthink/behind-the-ingenious-security-feature-that-powers-the-blockchain-1074442-1.html.
recorded in an incorruptible database, but also, being the said database a shared one, a copy of the Blockchain is stored on every computer (known as “node”) in the network. These computers periodically synchronize to make sure that all of them have the same shared database. As a consequence this property produces many advantages, but surely the best one\textsuperscript{13} is to remove (or at least drastically reduce) the problems of adverse selection: if the records associated are in connection with any service provided by or any data certified by a public officer or even a private vendor, every citizen can directly and costless verify the truth of all the information provided;\textsuperscript{14} furthermore, all the members of the network can consult the data just through their own computers, with a massive reduction in terms of cost of information.

Moreover, the other advantages associated with Blockchain are: security and privacy;\textsuperscript{15} involvement of the citizens in providing services for the collectivity;\textsuperscript{16} the removal of many trusted intermediaries within traditional hierarchical organizations (such as banks or government departments);\textsuperscript{17} massive reductions of transactional costs.

As a consequence, there are many potential fields of application for the Blockchain technology.

2.1. Potential Applications: Smart Contracts

One of the most fascinating application is represented by the so called \textit{Smart Contracts}\textsuperscript{18} which have the potential to drastically reduce friction in both commerce and society by providing greater clarity and speed to transactions. Such a feature depends on the fact that they are drafted by using source code, so that they can be standardized and executed at nearly no cost like other programming languages.\textsuperscript{19} In other words, a Smart Contract is designed to assure one party that the counterparty will fulfill his promises with certainty.

\textsuperscript{13} A further advantage is represented by the capacity of the Blockchain, as a shared database, to be recreated in its entirely even if a certain number of computers have lost the data.

\textsuperscript{14} See the UK Government Scientific Adviser, supra note 2, p. 22.

\textsuperscript{15} By a mechanism of private and public keys (either processed with the cryptography SHA-256) it is possible to establish by whom and under which circumstances the data, regarding for example sensitive information used to fill-in a form or an agreement, will be verified. \textit{Id.} p. 47-51; John H. Clippinger, David Bollier, \textit{The Rise of Digital Common Law. An Argument for Trust Frameworks, Digital Common Law and Digital Forms of Governance}. Available at https://idcubed.org/digital-law/the-rise-of-digital-common-law/.


\textsuperscript{17} See Marcella Atzori, supra note 16; the UK Government Scientific Adviser, supra note 2, p. 14, p. 61, “Hierarchies can have serious disadvantages: duplication, added cost, potential abuse of power, and opportunities for financial mismanagement”; Dmitri Kosten, \textit{Bitcoin Mission Statement Or What does it mean Sharing Economy and Distributed Trust?} Available at http://ssrn.com/abstract=2684256.

\textsuperscript{18} See Aaron Wright, Primavera De Filippi, supra note 3, p. 10-11, “digital, computable contracts where the performance and enforcement of contractual conditions occur automatically, without the need for human intervention”; Maria Letizia Perugini, Paolo Del Checco, \textit{Smart Contracts: a preliminary evaluation}. Available at http://ssrn.com/abstract=2729548.

\textsuperscript{19} See Aaron Wright, Primavera De Filippi, supra note 3, p. 24.
In particular, the role of Blockchain is to enable them, as the experiences of Ethereum\textsuperscript{20} (a Blockchain-based architecture derived from the BitCoin protocol and projected for writing Smart Contract provisions in the code of a system-coin, named \textit{ether}) and Colu\textsuperscript{21} have proved.

By using such forms of contracts the general improvement of the social welfare would be enormous.

First of all by the removal of the need for an \textit{ex post} legal enforcement: once the contracting parties have agreed to be bound by a particular clause, the source code binds them to that clause without leaving them any possibility of a breach.\textsuperscript{22} Indeed, the contractual provisions are translated into an executable digital code and inserted into the logic log, so that when a given condition (mathematically verifiable) takes place the system performs the digitally linked action.\textsuperscript{23}

However, it is basic to point out that there are some technical limits which strictly define the suitability of the contractual provisions: the \textit{smart clauses} can only be referred to good or services that may be binary expressed; when it is required a certain activity to the parties, the relative contractual provision can be embedded into a smart contract only in case of direct e-commerce; while in the other cases (or in the case of negative personal obligations) the smart clauses can only consist of a monetary equivalent to be paid automatically as the breach of contract is verified.\textsuperscript{24}

From a traditional point of view, the main contractual provisions involved are, first of all, those subdued to a specific deadline, with significant advantages in terms of speed of execution for the event associated with (like a digital trigger) could be immediately and unmistakably verified.\textsuperscript{25}

Further \textit{smart clauses} can be those referred to alternative obligations or those transferring a sum of money in case a given event takes place. In relation to the latter, it can be mentioned the experience of InsurETH, consisting of a proposal for an insurance contract for delays in flights, where the trigger event is verified by a software which cross-checks the data from the airport website with data retrieved independently.\textsuperscript{26}

In any case, by making automatic the execution of the contract, transaction costs drastically decrease.

Advantages in terms of speed of execution, therefore, can be achieved also by associating these contracts with the so called \textit{Smart Properties} (physical properties controlled by a source code, normally internet-enabled).\textsuperscript{27} On this ground, the role of Blockchain would be to store the relationship between Internet-enabled machines and Smart Contracts, and to let the latter to allocate the rights and obligations referred to such machines in real-time, according to the source code: for instance, a car could contain code that is tied to the Smart Contract, so that if the borrower becomes

\textsuperscript{20} See Larissa Lee, \textit{supra note} 8, p. 37-39; Maria Letizia Perugini, Paolo Del Checco, \textit{supra note} 18, p. 20; \url{https://www.ethereum.org/}.
\textsuperscript{21} See Maria Letizia Perugini, Paolo Del Checco, \textit{supra note} 18, p. 19.
\textsuperscript{22} \textit{Id.}, p. 26
\textsuperscript{23} \textit{Id.}, p. 10.
\textsuperscript{24} In these cases the Smart Contracts do not prevent the breach of contract, but they drastically reduce the costs of enforcement.
\textsuperscript{25} \textit{Id.}, p. 21-25.
\textsuperscript{26} \textit{Id.}, p. 22.
\textsuperscript{27} See Aaron Wright, Primavera De Filippi, \textit{supra note} 3, p. 33-36.
late on a car payment, the parties could agree on a code that would forbid the keys from opening the car until the default is cured.\footnote{See Larissa Lee, \textit{supra note 8}, p. 38.}

By using the source code, Smart Contracts can also determine another strong abatement of transaction costs: the ambiguity of the natural languages, in fact, does not affect such a code. As a consequence, the source code ensures parties that the original meanings of the contractual provisions (as originally considered by them in translating the said provisions into the relative executable digital code) will not change during the execution of the contract. At the same time, the source code prevents a party to strategically use such ambiguity for contractual conditions that, by the beginning, the same does not want to honor. By this way, not only contract would continue to be a Pareto optimum even in an \textit{ex post} perspective, but the costs referred to a hypothetical judicial interpretation would be avoided.

\subsection*{2.2. Other potential applications}

Having referred to Smart Contracts, it is now possible to introduce another potential field of application, namely \textit{Corporate Finance and Governance}.

Smart Contracts, indeed, have mostly been used to automatically execute derivatives, futures, swaps and options:\footnote{See Aaron Wright, Primavera De Filippi, \textit{supra note 3}, p. 11.} this is due to the significant gain in terms of speed of execution, as described above, in particular regarding to the immediate verification of the trigger event associated with.

However, the impact that such a gain could have on this ground is deeper than on the others: faster exchanges prevent, for example, phenomena like \textit{spoofing} and \textit{short selling}\footnote{See Larissa Lee, \textit{supra note 8}, p. 46.} which occur, to date, as the actual transfer of stocks takes up to three days; while Smart Contracts and Blockchain can verify every transactions in less than one minute.

Through the sole Blockchain, moreover, could be achieved many other advantages, especially in terms of transparency and reduction of transaction costs referred to third parties like brokers and transfer agents.

In relation to transparency, Blockchain, as an incorruptible and distributed ledger, can benefit: investors (through a better definition of the ownership positions of debt and less occasions of corruption on the part of regulators or listed companies); shareholders (through lower costs of trading and more transparent ownership records); regulators (as managerial ownership would become much more transparent too, with insider buying and selling detected by the market in real time).\footnote{See David Yermack, \textit{Corporate Governance and Blockchain}, available at \url{http://www.nber.org/papers/w21802}.}
Such a feature even implies the removal of the need for transfer agents, whose role is to record changes of ownership, maintain the issuer’s security holder records, cancel and issue certificates, and distribute dividends.\footnote{See UK Government Scientific Adviser, supra note 2, p. 58, “Over 90 per cent of corporate actions are distributed by data vendors, and then processed on behalf of investors by an agent such as a custodian or fund manager. Information is manually extracted from the original, interpreted and re-keyed by vendors. Levels of automation are low, errors frequent, and the process highly inefficient. One estimate puts the global cost of corporate actions processing at up to $10 billion per year. Custodians frequently reimburse clients for missed or incorrect execution of instructions. Block chain technology could make this process more efficient. Corporate actions represent contractual information and value, which can in principle be transferred directly between payers and payees without the need for intermediaries, provided the parties can trust the source data and have the necessary experience to act upon the information they receive. If a block chain was coupled to an application that captures and stores corporate action announcements in a structured format, it could be used to ensure that the data is from a verified source, and prove the time-stamped date that it was issued. This could be done in reverse for the execution of instructions. A distributed ledger based on such a block chain would reassure parties at every point in the process that their information is accurate, up-to-date, and unchanged since it was published by the issuer. In theory, it could eliminate all intermediaries between the issuer and the fund manager, guaranteeing the accuracy and timeliness of the information”.}

Blockchain can also be viewed as the path for innovative and much more efficient voting systems, given its nature of irreversible and incorruptible public repository of information whereby every data can be anonymously recorded (like BitCoin’s virtual portfolios). The huge abatement of transaction costs and the gain in terms of speed associated with, inspire the use of such a technology for a revolutionary idea of \textit{Distributed Real-time Governance}. Costless and real-time voting systems could lead to a further improvement in social welfare, namely through the resolution of many collective action problems: both for Corporate Governance\footnote{See David Yermack, supra note 31, p. 13-14.} and for the democratic systems overall.\footnote{See Aaron Wright, Primavera De Filippi, supra note 3, p. 37-40.}

The last potential application to be mentioned is that one referred to \textit{supply chains}.\footnote{See Jutta Steiner, \textit{Op-Ed | Blockchain Can Bring Transparency to Supply Chains}, available at \url{http://www.businessoffashion.com/community/voices/discussions/does-made-in-matter/op-ed-blockchain-can-bring-transparency-to-supply-chains}, “The open source, decentralised database blockchain allows consumers to check the authenticity and ethical standards of their products […], blockchains will entirely change the game for certifying, tracking and tracing the origin of our goods”.}

In particular, Blockchain could allow consumers to check the authenticity and ethical standards of products. Given the many implications in terms of health, pollution, overfishing and workers’ conditions associated with, more and more consumers are demanding genuine transparency on where and how their products are made. Even if such information can be provided by a third party, Blockchain represents a much more efficient instrument.

Not only for the many reasons described above, but also (and mainly) because a shared, incorruptible and distributed ledger cannot be affected by problems like bribery, social engineering or targeted hacking\footnote{Id.} which, on the contrary, could be associated with a single third party, potentially exposed to conflict of interests.

Therefore, Blockchain could provide a better and much more verifiable information, with obvious and extremely important positive outcomes in terms of trust between consumers and markets (given
that trust on the vendors would be replaced by a sort of trust on Blockchain and, as a result, on transparency of markets.\textsuperscript{37}

At the same time, Blockchain-based supply chains could be used to face many illicit activities, given that certain goods of high value, like gems and diamonds, are very often involved in money laundering and terrorist financing on global scale. Indeed, the diamonds industry is beginning to implement a Blockchain-based system called Everledger, which establishes a digital ‘passport’ for each diamond; it also enables Smart Contracts, so that, through the ledger, the same contracts can be tracked and used to verify business relationships and agreements.\textsuperscript{38}

At the end of this short review, anyway, it is important to point out that the number of potential applications is unlimited, as Blockchain-based ledgers can be:\textsuperscript{39} distributed (public database spread across multiple site, countries or institutions) or shared (database shared within a certain range, like an industry’s ledger or a company’s register of shares and securities); permissioned (database with one or many owners, so that when a new record is added, the ledger’s integrity is checked by a limited consensus process carried out by trusted actors)\textsuperscript{40} or unpermissioned (like BitCoin, where anyone is allowed to contribute data to a ledger a copy of which is provided to everyone).\textsuperscript{41}

\section*{3.1. Providing trust}

Notwithstanding the previous applications, this paper is mainly focused on a fundamental Blockchain’s feature: to provide trust (albeit an algorithmic one).

This feature depends on, first of all, the capacity of the said technology to let unrelated people to reach consensus on the occurrence of a particular transaction or event without the need for a controlling authority. In other words, through cryptography, Blockchain can solve both a typical computer science problem, well-known as \textit{Byzantine Generals Problem},\textsuperscript{42} and the main concerns related to the need for a trustworthy third party, such as a central authority: the agency problem into every hierarchical structure,\textsuperscript{43} the so called \textit{Elected Official’s Dilemma}\textsuperscript{44} and the transaction costs directly or indirectly generated by these institutions.\textsuperscript{45}

\textsuperscript{37} See infra.
\textsuperscript{38} See UK Government Scientific Adviser, supra note 2, p. 56.
\textsuperscript{39} Id., p. 15-19 for a better taxonomy.
\textsuperscript{40} Letting more efficient Governments’ online services, such as registries of land, registries of birth or driving licenses (see Marcella Atzori, supra note 16, p. 21). Particular interesting is the management of democratic voting system (see the UK Government Scientific Adviser, supra note 2, p. 59 and p. 15, “Recommendation 7: Understanding the true potential of distributed ledgers requires not only research but also using the technology for real life applications. Government should establish trials of distributed ledgers in order to assess the technology’s usability within the public sector”), which can lead to a better political efficacy (in the sense described in Douglas C. North, \textit{Institutions, Institutional change and Economic Performance}, Cambridge, Cambridge University Press, 1990).
\textsuperscript{41} Unpermissioned ledgers can be used as a global record that cannot be edited: for declaring a last will and testament, or assigning property ownership.
\textsuperscript{42} See Aaron Wright, Primavera De Filippi, supra note 3, p. 16, “This problem questioned how distributed computer systems could reach consensus without relying on a central authority, in such a way that the network of computers could resist an attack from ill-intentioned actors”.
\textsuperscript{43} See Douglas C. North, supra note 40.
To refer to a central authority, of course, implies a meaning of trust as a vertical relation between Government and citizens. As stated above, the existence of a central authority into a hierarchical structure can be inefficient; nowadays, indeed, a central authority represents a SPOF (Single Point of Failure) on many legal grounds.

Blockchain can solve such failures by letting the private sector to provide traditional public sector’s services, but also by the removal (or at least a massive reduction) of the need for a third party.

The most significant evidence of such capacity is, of course, BitCoin: this cryptocurrency is not issued by a central authority nor a specific country and, on the contrary, the validation of every transactions does not require any third party. Certainly the wide complexity of the debate about BitCoin prevents any attempts to establish here if the associated pros exceed the relative contras, but it is important to underline how Blockchain was disruptive for the traditional idea of currency, in particular in relation to the need for a central authority, namely a central bank.

Nevertheless, when a generic central authority is considered in relation to his role as a third party, then the main rationale of its very existence becomes to promote the exchanges through the guarantee for the enforcement. As the need for such a guarantee derives from the generalized mistrust between parties of an exchange, discussing on this role means to shift from a vertical to a horizontal idea of trust. Consequently, providing trust amongst the citizens means to remove the need for a third (centralized) party: there may be law even without a control authority.

44 See Dmitri Kosten, supra note 17, “The higher the level of governance, and the larger the constituency, the more abstract the concept of “public interests” becomes. The power of temptation grows higher with the proportion of assets under one’s supervision”.

45 See John H. Clippinger, David Bollier, supra note 15, “For many reasons conventional government policymaking is increasingly unable to provide timely, responsive, and effective governance and policymaking. The process itself is paralyzed by a political gridlock in the U.S. Congress that shuns evidence-driven policymaking; by complexity and delays in law-making, regulation and litigation; by the “pay to play” ethic that has tainted the legitimacy of governance; by cumbersome and ineffectual enforcement systems; and by the sheer expense of relying upon lawyers to protect one’s interests”.

46 Both from an economic and a political points of view.

47 The expression is taken from Marcella Atzori, supra note 16, p. 8, and it is an IT notion referring to any malfunctioning component which, as a consequence, causes a malfunction of the whole system.


50 See Dmitri Kosten, supra note 17, where the Author, referring to a so called “Crypto-socialism”, states “The (crypto-currency) network breaks down the banking pyramid of propagating fiat via economic channels. Thus it eliminates the competitive advantage of having access to newly printed cash, receiving disproportionate benefits from multiplier effect and fractional reserve system, which would then return system back to one of value creating completion […] The new tools created by technological advancements will trigger and force the changes of the socio-economic framework, just like it happened during transition from feudalism to capitalism”. The Author takes also in account the main concerns within the current financial system, pointing out, as a result, the deep and growing mistrust towards banks and other generic central authorities.

51 Douglas C. North, supra note 40.

52 The implications for a general theory of law are numerous, but, in particular, this suggests that law is based on mistrust, so that, according to Hobbes’ theory, not only the essence of legality must be coercion, but also there is not a (legal) society without a Leviathan. For a critique, see Tommaso Greco, Relazioni giuridiche. Una difesa dell’orizzontalità nel diritto, Teoria e critica della relazione sociale, 2014, p. 9-26.

53 This would confirm that there are legal grounds without the need for a Leviathan (coercion) and where legality involves just cooperation. Id. p. 25.
3.2. Blockchain as an Institution

Albeit algorithmic (and/or cryptographic), the trust provided by the Blockchain technology can deeply transform how people cooperates.54 In particular, by considering Blockchain as an institution, it could be said that this technology represents a further step in the evolution of the institutional change described by Douglas C. North.

The Author plainly explained that history has witnessed a gradual shift from the exchanges of the primitive or tribal societies (which were simple, territorially limited, personal and based on trust, guaranteed by moral rules and repeated)55 to the exchanges of the modern societies (which are much more complex, not territorially limited, impersonal, dominated by mistrust, guaranteed by a third party56 and not repeated).

Surely, is it indisputable that a much more complex exchange is better than a simple one, but the more the exchanges are complex in relation to time and space, the more complex and expensive the institutions (promoting cooperation) are.57 According to North, the need for an enforcing third party derives from the uncertainty between parties; the main reasons why such a mistrust is so spread within the modern societies are two: unlike the simplest ones, there are not moral rules whereby shirking, free-riding or lies are considered disadvantageous;58 furthermore, such modern exchanges are, in general, not repeated, so that both moral and social rules, like reputation, are ineffective and, as a result, people do not receive the right incentives to cooperation.59

Blockchain can deeply overturn this situation.

First of all, Blockchain provides trust by directly preventing any breach of contract. This is the aim which inspired Nick Szabo’s Smart Contracts in 1997.60 In particular, through the experience of Ethereum and thanks to the Blockchain technology behind it, such a kind of self-enforcing contracts, governed by an algorithmic code, has become reality.

Of course, it does not mean that contract law will become useless,61 but, however, removing such a risk means, on this ground, to drastically increase the exchanges: given that risk-aversion is an individual characteristic which can deeply affect the way how a person elaborates the information.

---

55 From a philosophical point of view, this is the description of a society where gift, trust, reputation and social stigma are the only factors of Law. See Lorenzo Scillitani, Fiducia, diritto, politica. Prospettive antropologico-filosofiche, G. Giappichelli Editore, Torino, 2007. In particular, pp. 20, 28, 65, 138.
56 See supra note 52.
57 Keep in mind that very often the institutions are not only extremely expensive, but also inefficient.
59 As Douglas C. North underlines, this is easily understandable by using the Prisoner’s Dilemma.
61 For instance, if someone wants an agreement (even a smart contract) to be declared void then he will be required to seek such a declaration from the Court. Furthermore, as described above, there are some technical limits which strictly define the suitability of the contractual provisions.
and the subsequent calculation of utility, the removal of a source of risk implies a reduction in the likelihood of sub-optimal outcomes (in the sense described by the rational choice theory).  

For a better comprehension, it is important to underline that uncertainty, risk and transaction costs are profoundly interrelated. If less-than-fully rational behaviors are due to the existence of non-quantifiable uncertainty (from which the very existence of the concept of risk originates), so that, in order to eliminate (or reduce) uncertainty, you need trust (where trust can be considered the propensity to transact regardless the existence of a given lack of knowledge), then it is necessary to point out that within the modern societies (and in a world of impersonal exchanges) to provide trust is expensive. As a result, trust is like a transaction cost. By removing any uncertainty referred to the performance of the contract, Blockchain removes the need for such an expensive trust-building (which implies a waste of resources); as a consequence, by reducing the transaction costs referred to uncertainty and risks, Blockchain promotes the exchanges.

As an incorruptible ledger, Blockchain can also provide trust through more, better and verifiable information. This is what happens when Blockchain records every step of a supply chain, which not only leads to a better protection of the consumers (through much more conscious choices) and to an increased trust on Markets, but can also heavily reduce the costs of information regarding to a certain product.

Furthermore, this feature can prevent many principal-agent problems associated with a sequence of contracts by making available for the last potential party, through a Blockchain-based registry of the origorative and of all the subsequent contracts, the information referring to all the previous agreements.

Blockchain can also be used for better public registries of real estates: this way, the costs of information associated with would be validly lessened; many concerns relating to phenomena of double-spending would be avoided too, given that Blockchain, as the BitCoin system proved, eliminates ex ante any possibility of double-spending.

Finally, the algorithmic nature of this trust cannot be ignored.

As stated above, trust implies less-than-fully rational behaviors. Only where there is uncertainty (in the sense of imperfect knowledge), there can be trust (in the sense of a complementary form of

---

62 It can also produce some distributional consequences. Given that to trust someone implies to run a risk, it is important to note that risk-aversion is often an inverse function of wealth, so that normally a poor person is more risk-adverse than a rich one: this could prevent poor people, more than the richer ones, to trade. From another point of view, risk-aversion could also affect poor people as they could be considered, because of their paucity, less trustworthy (see Cathy Reisenwitz, Smart Property’s Promise. Available at https://bitcoinmagazine.com/articles/smart-properties-promise-poor-1390852097). From a philosophical point of view, this is expressed by the link between trust and wealth (see Lorenzo Scillitani, supra note 55, p. 29, p. 15).

63 From a philosophical point of view, it is important to underline the link between trust and truth (see Lorenzo Scillitani, supra note 55, pp. 16, 104).

64 See Benito Arruñada, Registries, Universitat Pompeu Fabra, Economics and Business Working Paper Series 1456. Available at SSRN: http://ssrn.com/abstract=2535958. For other aspects of the registries of contracts, see Aaron Wright, Primavera De Filippi, supra note 3.

knowledge), so that, normally, to trust (or mistrust) someone requires to take into account, first of all, feelings and other subjective elements which can produce \textit{sub-optimal} outcomes.\textsuperscript{67}

This situation can be deepened by the way how people elaborate the information (which is one of the main reason why North justifies the existence of institutions). In a world of impersonal exchanges, the uncertainty referred to the counterpart is wider than before. But the bigger the uncertainty, the more trust is called for; this means that impersonal exchanges can directly raise the negative impact of \textit{sub-optimal} outcomes and/or indirectly, given the necessary waste of resources in trust-building, cut down a considerable part of the gain in social welfare that the same realize.

On many legal grounds, these negative effects could be removed (or at least lessened) if trust becomes an algorithmic one. The \textit{ex ante} mechanism whereby Blockchain prevents the breach of a Smart Contract removes uncertainty; the same happens when a consumer trusts the supply chain instead of the vendor, because, being aware of the incorruptibility of Blockchain, he knows that what is stated in the supply chain is true.

In other words, what Blockchain and its algorithmic provided trust do is to let people concentrate their efforts in seeking information on the attributes of the goods and services involved in the exchanges, regardless the personal qualities of their counterparts.\textsuperscript{68} Such a thing, of course, would have a huge impact in terms not only of \textit{sub-optimal} outcomes,\textsuperscript{69} but even in terms of trust-building.

Indeed, in case of Blockchain-based institutions, the only costs referred to such an activity would be those regarding the creation and the maintenance of the said institutions, so that, as pointed out for the supply chains, there would be a sole (inevitable) waste of resources for a trustworthy Market. While the said costs would multiply if the same activity was aimed to improve trust between a party (like a consumer) and different counterparts (like the vendors). In this sense, on the ground of trust-building, Blockchain-based institutions reduce the relevant transaction costs, as well as, according to Ronald H. Coase’s \textit{The nature of the firm}, firms do within Market.

\textsuperscript{66} See Lorenzo Scillitani, supra note 55, p. 48.
\textsuperscript{67} See Georg Simmel, \textit{Soziologie: Untersuchungen über die Formen der Vergesellschaftung}, Leipzig: Duncker & Humblot, 1908; Lorenzo Scillitani, supra note 55, p. 70.
\textsuperscript{68} See the UK Government Scientific Adviser, supra note 2, p. 13, “trust is a risk judgement between two or more people, organisations or nations. In cyberspace, trust is based on two key requirements: prove to me that you are who you say you are (authentication); and prove to me that you have the permissions necessary to do what you ask (authorisation). In return, I will prove to you that I am trustworthy by delivering services or products to you in a secure, efficient and reliable fashion. Authentication and identification are interlinked but they are not the same thing. Authentication does not require that I know your identity but it does require that you provide me a token that is inextricably linked to your identity, for example the pin number associated with a credit or debit card, or a fingerprint allied to a biometric passport or other document. Equally, when I provide my authentication token to you, I need assurance that I am providing it to the correct individual or organisation, ie that you are who you claim to be. So it is equally important that organisations can provide authentication to their users, be they individuals, other organisations or government”.
\textsuperscript{69} This can be seen as a further step of what was defined “objectification of culture”. See Lorenzo Scillitani, supra note 55, p. 49.
The reasons why the legal systems should seriously consider the disruptive potential of Blockchain are various, but maybe the first one depends on the prime purpose of the modern State: to increase social welfare by letting people trade according to their personal preferences (i.e. by promoting exchanges). To do so, modern states (and their law) need to reduce the transaction costs and provide trust.

All these goals can be achieved by implementing law with Blockchain-based institutions, so that it is a duty, first of all for jurists, to modify the traditional ones. Not only because the primary rationale of the modern private law (since the nineteenth century) is to organize and support markets, but also because available technology continuously shifts (in the sense of improving) society’s utility frontier. Hence, a legal system which does not employ the best available technology leads society to sub-optimal results.

Lastly, according to North’s method, it is important to coordinate institutions with the evolution of society, in particular when history suggests a clear and peculiar direction. This direction is, nowadays, represented by horizontal subsidiarity, altruism (as proved, in this case, by the open-source movement within which Blockchain itself was born) and distributed governance. At the same time, not only Blockchain fulfils all these conditions, but even represents the definitive technology which can conduct society towards a revolutionary idea of law and trust: a further step in the evolution of the impersonal exchanges where, once again, institutions, technology and social changes will be perfectly interconnected.

71 See the UK Government Scientific Adviser, supra note 2, p. 71-83; Lorenzo Scillitani, supra note 55, p. 110.
74 See John H. Clippinger, David Bollier, supra note 15, “This platform abandons the classical-modernist system of bureaucratic oversight and control, and instead leverages the demonstrated capacity of people on open platforms to self-organize themselves into collaborative regimes that can organize stable communities, mediate conflicts, and get real work done”.
75 See Tommaso Greco, supra note 52; John H. Clippinger, David Bollier, supra note 15, “People are more likely to respect and participate in a system whose governance procedures are transparent and responsive, and that enables the positive externalities generated by a community to be captured for collective (and personal) benefit”.
76 Id., “In its most ambitious sense, we are talking about the next, great leap in the structure of the Internet and its socio-legal-economic evolution […] In a sense, law itself must be re-conceptualized if it is to function well in networked environments. Now is the time to engineer a great leap forward to digital, network-native forms of law, where the rule of law derives from the collective sentiments of a given community or network of users and functions in a more algorithmic, self-executing and self-correcting way”.
77 See the UK Government Scientific Adviser, supra note 2, p. 53, “Sufficiently radical technical innovations can lead to revolutionary changes, not only in business models or industries, but eventually in the way in which society is organised and governed […] Distributed ledger technologies (DLTs) […] have the potential to disrupt the whole economy, and society”.

Conclusions
BIBLIOGRAPHY


