European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 2, pp. 37-43
ISSN 2724-5969 - ISBN 979-12-5994-752-9 - DOI 9791259947529 05

*Blockchain Technology and Regulatory Compliance: Towards a Cooperative Supervisory Model**

Miriam Allena
(Associate Professor of Administrative Law at Bocconi University in Milan)

ABSTRACT This Article assesses the impact that blockchain technology could have on monitoring compliance with public law regulations, in particular by rendering it more cooperative, thanks to the possibility to involve in the monitoring process various non-public actors, including specifically the regulated entities and the general public. Focusing in particular on permissioned platforms (as opposed to permissionless ones), the Article shows how blockchain technology could potentially open up new horizons for a number of currently available compliance mechanisms - whether based on more traditional direct regulatory models, on self-monitoring and auditing mechanisms or on market mechanisms - thanks to the direct involvment of regulated entities and citizens in the performance of functions that have previously fallen within the purview of public agencies.

1. *Introduction*

The idea that the use of technological solutions can facilitate compliance with and monitoring of regulatory requirements is not new. In the financial sector, where regulators have to deal with the challenges posed by the raise of financial technology (or “FinTech”), the expression “regulatory technology” (or “RegTech”) refers to the application of technology to compliance and supervisory activities.[1]

The expression “ReghTech” can however be used also in a broader context to encompass all those instruments that - usually by automation - can make reporting and regulation more transparent, efficient and effective, for the benefit of both the regulated entities and the regulator.

This article focuses on one of those instruments, i.e. blockchain technology (and distributed ledger technologies - DLTs - in general)[2], and the impact it could have on monitoring compliance with public law regulations, in particular by reinforcing and enhancing the efficacy of public supervision, but moreover by rendering it more cooperative, thanks to the possibility to involve in the monitoring process various non-public actors, including specifically the regulated entities and the general public.

Most of the current hype and hope associated with blockchain result from the fact that the said technology heralds a potential withdrawal of the State and public authorities in general from certain function traditionally performed by them: indeed, as a as a peer-to-peer digital database distributed across multiple computers or “nodes” (thus open to participants that do not need to know or trust each other to interact), this technology makes it possible to certify the completion of particular activities or compliance with certain formal requirements without involving a centralized administrator or an independent third party.[3] Thus, according to many, certain public functions and services traditionally performed by the State and public authorities in general could be redesigned according to an equalitarian system of governance, where individuals could reach consensus and coordination through cryptographically verified peer-to-peer procedures, without the intermediation of any independent party: in brief, within a context made up of “decentralized trustless

* Article submitted to double-blind peer review.

[1] Toronto Center, *FinTech, RegTech and SupTech: What They Mean for Financial Supervision*, in www.res.torontocenter.org, 2017. To be more precise, the term “RegTech” is sometimes used exclusively in relation to reporting and compliance activities by regulated entities, while the more specific expression “supervisory technology”, or “SupTech”, is used for the supervisory activities of the competent authorities.

[2] In common parlance, the term “blockchain” is used as an alternative to Distributed Ledger Technologies (DLTs). This article will follow this approach, subject however to the provision that a distributed register is also a blockchain only if it uses the blockchain data structure to record transactions.

[3] This is typically the perspective of crypto-anarchists and techno-libertarians: but see M. Atzori, *Blockchain Technology and Decentralised Governance: Is the State Still Necessary?*, in *Journal of Governance & Regulation*, vol. 45, n. 6, 2017, 26, highlighting the risks associated with the reduction in the authority of the State as a central point of coordination within society.

transactions".[4] Against this backdrop, the very perimeter of public law would shrink, confirming the prospect - envisaged by some scholarship - of a crasis between public and private law or, at least, of an increase of areas of regulatory hybridization.[5]

Although the perspective outlined above seems fascinating and worthy of investigation, this paper takes a different view. Indeed, in the following Sections blockchain technology will be analyzed not as an instrument of potential withdrawal of the State and public authorities, but instead as an instrument which potentially allows a more direct engagement of both regulated entities and the general public in the performance of public functions: in other words, the thesis of this Article is that blockchain will not eliminate the role of public bodies, but it will make it possible to reformulate certain traditional public functions (and in particular, the supervisory/monitoring function) according to a multipolar logic, where public authorities, the regulated entities and the general public cooperate all together on a genuinely peer-to-peer basis: as a consequence, the traditional alterity between the controlling administration, the parties that are subject to checks and the general public fades away, leaving space for the performance by all parties of an active role and thus changing the very nature of the supervisory function.[6]

Against this backdrop, Section 2 of this article sets out the basic technical characteristics of blockchain technology focusing in particular on permissioned platforms (as opposed to permissionless ones) that, as "narrowly distributed" platforms, may prove to be more appropriate when specific public functions - that are intrinsically necessary (in the sense that they need to be performed by the State and cannot be suspended) - are at stake. Section 3 examines how the characteristics of blockchain make it possible to put in place a form of "dispersed verification" of data submitted by the regulated entities under which it is the people who use that distributed ledger (including the general public and the regulated entities) who directly certify the formal completion of certain operations and associate them with a precise timestamp. Section 4 concludes.

2. *Permissioned Blockchain as instrumental to the public supervisory function*

Blockchain technology was effectively defined as "a distributed, shared, encrypted database that serves as an irreversible and incorruptible public repository of information".[7] The database is "distributed" since it is not physically hosted on one single server, but rather on a distributed network of computers ("nodes"), each of which holds an identical copy of it, updated in real time.

Data in such a database are aggregated into blocks which, once they reach a certain size, are chained to one another through a cryptographic process (s.c. hashing process). The particular way in which data are recorded in cryptographically inter-linked blocks (hence the name "block-chain")[8] ordered in temporal

[4] See M. Swan, *Blockchain: Blueprint for A New Economy* Sebastopol, Calif, O'Reilly, 2015; P. De Filippi and A. Wright, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, 12 March 2015, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664; K. Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 *Berkeley Tech. Law Journal* 487, 494 2018; Id., *Blockchain and the New Architecture of Trust*, Cambridge (MA), MIT Press, 2018.

[5] Since, by virtue of the use of blockchain, many operations traditionally pertaining to public power would be entrusted to private individuals. In general, on the hybridization of public and private law see G. Napolitano, *Pubblico e privato nel diritto amministrativo*, Milano, Giuffrè, 2003 and, more recently, P. Cirillo, *Sistema istituzionale di diritto comune*, Padova, Cedam, 2021.

[6] For the idea that parity in the relationship between citizen and public administration is not achievable through the application of private law, but instead by virtue of public law transformed through procedural dialectics see for all F. Benvenuti, *Funzione amministrativa, procedimento, processo*, in *Scritti giuridici. Articoli e altri scritti* (1948/1959), vol. II, Milano, Vita e Pensiero, 2006, 1117 ss.; Id., *Per un diritto amministrativo paritario*, in S*critti giuridici, Articoli e altri scritti (1970/1983)*, vol. IV, Milano, Vita e Pensiero, 2006, 3223 ss.; Id., *L'amministrazione oggettivata: un nuovo modello*, *ibidem*, 3467 ss. The thesis that the application to the public administration of procedural guarantees (including participation of the citizenry) allows a more cooperative system has been subsequently further developed in particular by G. Pastori in the work *Introduzione generale*, in Id. (ed.), *La procedura amministrativa*, Vicenza, Neri Pozza, 1964. See also G. Gallone, *Blockchain, procedimenti amministrativi e prevenzione della corruzione*, in *Il diritto dell'economia*, vol. 3, 2019, 187, especially 199, who underlines, *inter alia*, the potential of blockchain to impact on the very concept of authoritativeness of the public administration.

[7] P. De Filippi and A. Wright, *Lex Cryptographia*, *supra* note 4, at 2 and note 15, where it is stated that, precisely due to its combination of various existing technologies that are already being used in isolation from one another, blockchain technology amounts more to an "incremental improvement" than "a huge technological advance".

[8] In particular, the data contained in each block are converted into a digital fingerprint (or a "hash") comprised of a string of characters and numbers with a fixed length, which cannot be reverse-engineered (i.e., it is practically impossible to establish the content of any given body of data starting from their hash). Each hash is uniquely

sequence (a process known as "notarization") [9], along with the comprehensive visibility of all operations[10], mean that any attempt to interfere with an entry after it has been recorded will by definition leave a trace[11]. The result is a transparent and "tamper-evident" database, which permanently records transactions without necessarily revealing their content since it can be configured in such a way as to permit differing levels of visibility, including allowing any sensitive data to be kept secret.

Another important characteristic of the system lies in the fact that information is entered by a wide variety of actors ("users"): when a "user" asks to register new data, the data must first and foremost be validated by one of the "nodes" in the network. Thereafter, in order to be permanently recorded on the database (according to the system comprised of "chains of blocks" described above), the other "nodes" (or usually a majority of them) must confirm that the said validation occurred in accordance with clearly defined pre-agreed rules, that is in accordance with the blockchain protocol which establishes what data can be recorded (and what characteristics the data must have).[12] This is referred to as a "consensus protocol" because the rules enable the various nodes to reach agreement as to which blocks should be added to the chain[13]: consensus protocols lie at the very heart of the blockchain since they make it possible to remove the need for an intermediary and it is this, without doubt, that is one of the most fascinating and potentially transformative aspects of this technology.

The first blockchains associated with cryptocurrencies were conceptualized as permissionless platforms enabling any person to register new data (thus, act as a "user"), to download the entire database (thus, act as a "node"), and to validate new blocks (thus, act as a "miner").[14] This system meets with the need to enable cash transactions to be concluded in a "trustless environment", that is between participants who do not know and do not trust one another, bypassing any requirement for a specific, centralized, third-party intermediary: hence the slogan "in code we trust" or "in crypto we trust", which implies that, within a system operating between mutually unknown users such as Bitcoin, each of the various participants in the network simply places his or her trust in the fact that the various miners will follow the Bitcoin consensus protocol, and hence perpetuate the system.[15]

However, databases may be decentralized to different degrees and the registration of blocks of data in distributed ledgers can be achieved in various ways: everything is dependent upon the objective that has been set as well as the intended use of such platforms.[16]

As specifically regards public supervision, it

associated with a specific block: this means that even a minimal change to the contents of the data block (e.g. changing one single character) would generate a completely different hash.

[9] Each hash associated with a specific block is timestamped in order to establish that the data originating in that particular hash existed at a precise moment in time

[10] Indeed, both hashes and timestamps are published: thus in principle anyone in the network can see at what time any specific data was entered and verify that it has not been subsequently changed.

[11] In particular, the hash for each block is cryptographically signed with the hash of the previous block which ensures that the data from the various blocks cannot be manipulated without leaving a trace: in fact, any alteration at all of the data grouped together within a block will result in a change not only in the hash for that block but also of all of the subsequent hashes in the chain.

[12] As a matter of fact, everything is managed by an algorithm which establishes which nodes can validate the data and which data can be registered.

[13] There are various types of consensus: the most well-known (and that hitherto considered to be the most secure in networks with a large number of mutually unacquainted participants) is Bitcoin's "proof of work". In this case, in order to avoid fraud, the blocks are validated according to complex mathematical calculations for identifying a valid hash that satisfies certain properties for each new block, which are particularly energy-consuming (for this reason, the nodes that compete with one another in order to validate new blocks are referred to as "miners"): the greater the computational resources a node dedicates to resolving the problem, the more likely it will be the first to identify the hash in question. The successful miner is then rewarded with a certain number of Bitcoins. Over time, other types of consensus protocol have therefore been developed, such as for instance the s.c. "proof-of-stake", under which the node competent to validate new data is identified according to a randomized selection that takes account of actors such as the quantity of cryptocurrency held by each node and the period of time for which they have been held.

[14] This is the case for Bitcoin which was revealed to the world when someone using the pseudonym of Satoshi Nakamoto published a "white paper" in which he proposed an electronic peer-to-peer payment system (called Bitcoin), which would have allowed "online payments to be sent directly from one party to another without going through a financial institution": S. Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf.

[15] See A. Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains*, in P. Hacker et al. (eds.), *Regulating Blockchain. Techno-Social and Legal Challenges*, Oxford, OUP, 2019, 58 ss.

[16] Thus for example, if the main objective is security, this will increase the more widely a blockchain is distributed (in the sense that anyone can operate on the register by adding or validating new data). In fact, it is without doubt harder to corrupt thousands of users than to corrupt a single institution or a limited group of institutions.

may not be necessary for the particular form of data registration in blocks to be accompanied also by the ability for thousands of unknown users to operate on the database nor to operate in a "trustless environment", that is between participants who do not know and do not trust one another. On the contrary, a "narrowly distributed" platform with a shared (as opposed to distributed) ledger may prove to be more suitable for this purpose, as only some clearly identified operators store the database and validate new blocks, while the ability to propose the inclusion of new data and to consult the database as a whole can be open to all (or not) as required[17]: this is the model of s.c. "permissioned blockchains", which combine some of the characteristics of the first blockchains (for instance, data integrity, security, full visibility, decentralization on a peer-to-peer basis within the network of participants) with less costs in terms of maintenance, increased sustainability[18] and scalability.[19]

The characteristics above are at the basis of the success of permissioned blockchains in the financial and industrial sector (especially in supply chains whenever there is a need to guarantee the origin, form of production and transformation over time of a particular product)[20] and also explain why the said blockchains have started being used in some countries to ensure the integrity and security of public registers and databases.[21]

In the following Section, the scenario disclosed by permissioned blockchains, where public authorities necessarily operate as "nodes"[22], while the regulated entities and/or interested groups[23] (such as NGOs, consumer associations, groups of citizens, etc.) participate as "nodes" depending on the specific case, will be discussed to show how the technology at stake could potentially open up innovative forms of interaction between the public administration, the regulated entities and citizens.

3. *From a binary controller-controlled mechanism to a "dispersed verification of compliance model"*

The limits of a system of supervision/ monitoring of regulated activities essentially managed by public authorities, where the latter have the monopoly of the exercise of controlling power and basically are exclusively charged with overseeing the actions of others, are well known and have been debated in detail, as are the reasons that led to the development of alternative and more collaborative approaches.[24] Indeed, intrinsic limits on government information and administrative enforcement resources make it particularly challenging for regulators to develop legal controls in response to always new problems and social needs. At the same time, it is well known that it is difficult to induce companies to cooperate in good faith, and to self-detect and report any breaches of regulation.

Moreover, within the context of a binary controller-controlled mechanism, instances of - among others - information asymmetry, corruption, maladministration, and regulatory capture by the regulated entities themselves can always occur. A good example are polluting activities, where business almost always has more or better information than public authorities and the latter, in turn, have proved in

[17] As mentioned, those who request the recording of new data and can see what happens on the database, but do not store a full copy of the database and do not participate in the validation of new blocks are called "users".

[18] Permissioned blockchains require less energy to operate because they use a traditional synchronous consensus protocol in order to establish agreement concerning the registration of new blocks, thus bypassing the highly costly "proof-of-work" or other similar asynchrony consensus protocols (see nt. 13 above).

[19] In permissionless blockchains, the continuously growing number of nodes has resulted in the blockchain scalability problem which implies that the transaction throughput is reduced: for instance, permissionless blockchains process almost 7 transactions every second, while Visa processes almost 1700 transactions every second on average.

[20] It is worth noting that permissioned blockchains differ from "fully private blockchains", which are databases stored in a centralized manner, where an individual organization verifies the data and ensures that they are registered on a fully centralized register organized into the block structure described above.

[21] This is the case for instance of Estonia which started testing the use of cryptography to secure data and transactions in 2008, thus six months before the Bitcoin was created. See also the Italian experience where the Ministry of economy and finance (MEF) started testing the use of cryptography to secure data and transactions since 2015 (http://noipa.mef.gov.it./cl/en/sunfish; https://noipa.mef.gov.it/cl/en/Poseidon): on this experience see M. Bianchini and I. Kwon, *Blockchain for SMEs and entrepreneurs in Italy*, in www.oecd.org, 2020, 57.

[22] As mentioned, being the supervisory power a necessary one, active involvement by public authorities should always be stipulated as a necessary prerequisite for the operation of the system.

[23] Such as, for instance, NGOs, consumer associations, groups of citizens in general that according to the law are entitled to participate to the system.

[24] *See*, *ex multis*, D.A. Farber, *Triangulating the Future of Reinvention: Three Emerging Models of Environmental Protection*, in *Univewrsity Illinois Law Review*, vol. 61, 2000, 323; R.B. Stewart, *A New Generation of Environmental Regulation?*, in *Capital University Law Rev.*, vol. 29, 2001, 27 and 99.

many cases to be willing to adopt a more tolerant approach towards business in order to safeguard jobs and retain production facilities.

The same problem arises, albeit on a more limited scale, also when well-structured self-monitoring and reporting mechanisms are in place (in line with the s.c. "reflexive approaches to regulation"[25]) and the data reported by the regulated entities are verified by private third parties (s.c. private certification systems). In fact, any certification work carried out by such bodies, even assuming that they are genuinely independent, must be (at least randomly) controlled by public authorities, which in turn brings us back once again to the binary logic of the controller-controlled: thus, from this perspective, public supervision still remains tied to a centralizing logic since the ongoing need for checks by public authorities on the correctness and accuracy of the data presented by businesses cannot be completely eliminated.

In the last decades, the increasingly pervasive reporting requirements imposed by the international and domestic regulatory framework have had further onerous consequences for both the regulated entities, which are required to ensure adequate methods for collecting, organizing and communicating relevant data, and the supervisory authorities, which are called upon to develop more efficient systems for managing and processing the enormous amount of data received, as well as to identify effective systems for verifying the reliability of those data.

Even though the almost complete automation of many reporting processes has considerably reduced the risk of false or inaccurate declarations, technological development has not eliminated the ongoing need for checks by public authorities of the formal correctness and accuracy of the data presented by businesses (or, along the same lines, automatic data transmission systems, in order to ensure that they have not been interfered with).

Against this backdrop, the strength of the blockchain lies precisely in its capability of enabling the time of recording and formal completeness of the data to be verified in a manner which I will referred to below as "dispersed", meaning that it is the people who use the blockchain ledger who directly certify the completion of certain operations and associate them with a precise timestamp. Consider for instance the duty of a business to report certain data to the authorities: in order for them to be registered on the blockchain, these data would have to be verified by the various computers from the network. Specifically, these computers would be required to certify, by majority, that the business had complied at least formally with all requirements laid down by a certain law (inserting all types of data and the documentation requested). Thus, any computer in the network (i.e., any party admitted to the permissioned blockchain such as, depending on the circumstances, the competent public authorities, other competitor businesses, the general public) would be in a position to verify the formal validity of the data inserted. Moreover, inclusion "on chain" would constitute evidence that the said data had been made available before the applicable time limit.

This leads to three many consequences.

First, blockchain technology has the potential to involve a number of subjects directly in the creation of public databases (indeed, data which has not been verified cannot be registered on the distributed ledger) thereby giving rise to an innovative system under which data that are made available to the public are already "secure" upon creation, thanks to the prior verification of their formal parameters by a potentially very large number of subjects. Within this context, the traditional alterity between the controlling administration, the parties that are subject to checks and the general public fades away, leaving space for the performance by all parties of an active role in checking data (subject to the limits mentioned above) on a genuinely peer-to-peer basis.

Second, it is clear that a business that is called upon to engage constantly with the said distributed ledger - which is potentially under the control of a large number of operators (public administrations, other competitor businesses as well as private individuals and groupings of individuals) - would almost naturally be inclined to improve its own self-monitoring and reporting practices. This because it would be aware that effective compliance (at least) with the formal regulatory requirements in a timely manner would be subject to continuous, dispersed controls. As a result, it would know that it could not rely for example on the inattentiveness of the public regulator, a lack of resources available to it, or even worse fraudulent collusion with it, since any conduct at odds with the regulatory framework would

[25] The s.c. "reflexive approaches to regulation" assume that self-analysis by regulated entities may foster a culture of self-responsibility, as opposed to the traditional regulatory models based on the authoritative setting of limits and the control of compliance with them by public agencies.

become immediately visible to a wide range of people. These people could moreover potentially have considerable incentives to perform a controlling function (consider a competitor business, a consumer association or residents in an area exposed to the emissions of a particularly polluting industry). Given the high likelihood of being discovered, business would have a particular interest in preventing instances of non-compliance from occurring by putting in place an effective system of internal controls. From this viewpoint, blockchain technology could thus provide effective "teeth" in order to enhance the efficacy of self-monitoring and reporting practices, which are already widely provided for in many sectors.

Indeed, any business would itself know that, since any negative performance (even only in terms of a breach of formal reporting obligations or the failure to comply on time) could be immediately visible also to the general public (if the design of the specific blockchain so provides), that outcome could have a significant adverse impact on its reputation and on consumer choices (think for instance of the heightened sensitivity of consumers about environmental compliance or data protection requirements). As a result, it might decide to act in a manner that is more compliant with regulatory requirements precisely in order to better respond to the social needs and expectations of consumers.

Third, within this perspective, it is even conceivable that full compliance with particular regulatory requirements as certified by the blockchain system could operate as a kind of dispersed certification system of good compliance with sectorial regulations, albeit limited to formal aspects. In particular, a prerequisite for the receipt and maintenance of the said certification would be full and timely compliance with reporting obligations as documented by the blockchain system.

This would *inter alia* resolve one of the principal limits to private certification, that is the fact that it tends to be managed by private operators which, due to the obvious conflict of interest (their operations are remunerated by the controlled body, which not infrequently chooses its own certifying body), are not particularly reliable, and also do not always operate in a fully transparent manner. On the contrary, the blockchain would give rise to a system of dispersed certification that can in principle be managed and controlled also by the public at large, and it is thus likely that it would end up being perceived by the public as more secure and more reliable[26].

In conclusion, the unprecedented collective and dispersed scrutiny achieved by the blockchain, at least in terms of the timeliness and formal regularity of reporting, appears to be capable of opening up new horizons for a number of currently available compliance mechanisms, whether based on more traditional direct regulatory models, on self-monitoring and auditing mechanisms or on market mechanisms.

4. *Conclusions*

The implementation of a system of wide-scale scrutiny such as that described above would have significant consequences not only in terms of enhanced transparency and reliability of information submitted to the public authorities, but would also lay the groundwork for more effective substantive controls concerning the accuracy of the data submitted. Indeed, it is likely that, during formal checks as to the completeness of the data and whether they have been submitted on time, the system would enable interested parties to obtain any information required in order to request public authorities to carry out substantive checks as to their accuracy.

Therefore, a control system based on blockchain technology may in principle exponentially increase oversight over (formal and substantive) compliance by regulated entities with public law regulation.

Furthermore, from a systemic point of view, the type of "dispersed verification" of data that can be achieved using blockchain moves beyond the juxtaposition between "command and control" and market instruments, giving rise to an entirely innovative approach under which dynamic forces within society become directly involved both in the performance of functions that have previously fallen within the purview of public agencies as well as in reconfiguring certain traditional market mechanisms in innovative and potentially more effective terms.

As mentioned above, the blockchain would not eliminate the role of public authorities, but would make it possible to reformulate the function of formal verification of data submitted by regulated entities and their registration on public databases according to a multi-nodal logic, thereby preventing potential cases of

[26] On the philosophical implications of the production of certainty allowed by blockchain technology see G. Fracchia, Verum-factum. *La produzione della certezza ordinamentale a fronte della blockchain*, unpublished manuscript.

corruption, maladministration and regulatory capture. On the other hand, the joint public-private exercise of that control would make it possible to counter the limits that arise when that activity is carried out by private operators. These limits essentially result from the fact that these operators have an inherent tendency to be of low reliability owing to their pursuit (also) of their own specific interests.

The blockchain accordingly makes it possible to envisage a "third way" between "state failure" and "market failure" in which public and private bodies cooperate with a view to making available in a timely manner data that are, at least in formal terms, completely reliable.