BLOCKCHAIN TECHNOLOGY FOR ENVIRONMENTAL COMPLIANCE: TOWARDS A "CHORAL" APPROACH

By

Miriam Allena*

Blockchain technology is increasingly attracting the attention of governments and public institutions around the world. As a distributed ledger that is tamper resistant and available as a multiplicity of copies constantly updated in real time, it has the potential to profoundly innovate the way in which public registers are kept, enabling improved data management and faster data sharing. Above all, that technology heralds a potential withdrawal from the scene of the State and public authorities, by making 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.

This Article examines the impact that blockchain technology could have on monitoring compliance with environmental regulations, rendering the process much more efficient thanks to its greater involvement of various non-public actors, including regulated entities and the general public. Specifically, blockchain allows for "dispersed" checks to ensure that environmental data have been submitted on time and are complete. This is, in turn, a prerequisite for subsequent checks, including substantive ones, into their accuracy and more effective enforcement of environmental law. At the same time, the technology lays the groundwork for the active involvement by regulated entities and the general public in creating public databases, giving rise to a system which this Article will refer to as "notarized transparency" within which environmental information is already reliable when it is created and can be more easily shared. This Article argues that blockchain has the potential

*Associate Professor of Administrative Law at Bocconi University in Milan. This Article was written during my visiting fellowship at the Berkeley Law School, University of California (from January to July 2019). I am grateful to the Institution for hosting me. I would like to thank Daniel Farber for inviting me to Berkeley and for his invaluable support and comments to draft versions of this work. I am also very thankful to all the other colleagues and friends who have provided comments, reactions and encouragement on early versions, including especially Eric Biber, Giacinto della Cananea, Ethan N. Elkin, Fabrizio Fracchia, Francesco Goisis, Amnon Reichman, Josephine van Zeben and Marco Ventoruzzo.

to reconfigure environmental protection according to a multi-polar logic, preventing (or significantly reducing) instances of corruption, maladministration and regulatory capture. In this regard, it paves the way for a form of "choral participation" in the protection of the environment capable of generating higher levels of environmental compliance and transcending the juxtaposition between command-and-control and market-based tools. Under the entirely innovative approach brought about, dynamic forces within society become directly involved to perform functions that have previously fallen within the purview of public agencies and in reconfiguring certain traditional market mechanisms in innovative and potentially more effective terms.

I. INTRODUCTION

The 2018 Joint Economic Report submitted by the Joint Economic Committee (JEC) of the U.S. Congress dedicated a specific chapter to blockchain technology,[1] which "offers a decentralized, secure, and efficient way to store almost any form of data across multiple platforms."[2] The Report clarifies that "[d]evelopers, companies, and governments recognize the potential and [are] already starting to implement blockchains for many different uses," and recommends that "[g]overnment agencies at all levels . . . consider and examine new uses for this technology that could make the government more efficient in performing its functions."[3]

In the same year, the European Parliament passed a resolution on distributed ledger technologies (DLTs) and blockchain,[4] stressing they can significantly improve not only "key sectors of the economy" but also "the quality of public services."[5] After providing a detailed list of the possible applications of this technology, the document stresses "the profound impact that DLT-based applications could have on the structure of public governance and the role of institutions," in particular by cutting red tape and reducing administrative burdens for citizens, businesses and public administrations;[6] decentralizing governance and improving the capacity of citizens to hold governments accountable;[7] improving traditional public services, including *inter alia* the digitalization and decentralization of public registries, the procedures

[1] 2018 JOINT ECON. REP., H.R. NO. 115-596, at 201, 212 (2018). 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 proviso that a distributed register is also a blockchain only if it uses the blockchain data structure to record transactions (for this account, see *infra* Part II.A). On the fast-moving vocabulary around blockchain technology and the difficulties that it creates for regulators, see Angela Walch, *The Path of the Blockchain Lexicon (And the Law)*, 36 REV. BANKING & FIN. L. 713, 717 (2017).

[2] H.R. NO. 115-596, at 201, 212. The JEC was created when Congress passed the Employment Act of 1946. Under this Act, Congress established two advisory panels whose primary role is to review economic conditions and to recommend improvements in economic policy: the President's Council of Economic Adviser (CEA) and the JEC. *About*, U.S. CONGRESS JOINT ECON. COMMITTEE, https://perma.cc/5BBD-RFA7 (last visited Oct. 8, 2020).

[3] *Id.* at 212, 226. Shortly before this the document notes, significantly, "with all the headlines focusing on the financial applications, people may miss the digital revolution now happening with other blockchain applications." *Id.* at 212.

[4] Distributed Ledger Technologies and Blockchains: Building Trust with Disintermediation, Eur. Parl. Doc. 2017/2772 (RSP) (2018). Resolutions of the European Parliament are non-binding acts by which the European Parliament expresses a political position concerning various matters falling within the competence of the EU.

[5] *Id.* ¶ K.

[6] *Id.* ¶¶ 2, 47, 57.

[7] *Id.* ¶ 48.

for issuing permits, licenses and certificates; and enhancing the transparency and security of services provided to citizens.[8]

Along the same lines, in 2017 and 2018 various legislative initiatives were promoted in both the United States and several European countries to authorize the usage of blockchain technology to support governmental functions in various ways.[9] Finally, some developing countries see this technology as an opportunity for overhauling their economies and productive systems.[10]

These developments provide a flavor of the incredible attention that blockchain technology has aroused within both governments and public institutions around the globe.[11] This attention is due primarily to its promise to profoundly innovate how public registers are kept, enhancing security and transparency within the management of many activities and services provided by public bodies. In a nutshell, blockchain can be defined as a peer-to-peer digital database distributed across multiple computers (or "nodes"), thus not stored in a centralized repository but hosted by them all simultaneously.[12] The particular way data are recorded in cryptographically inter-linked blocks (hence the name "block-chain") ordered in temporal sequence, along with the comprehensive visibility of all operations, means that any attempt to interfere with an entry after it has been recorded will leave a trace.[13]

---

[8] *Id.* ¶¶ 48, 53; *see also* Virtual Currencies, Eur. Parl. Doc. (2016/2007(INI)) ¶¶ 5,8 (2016); DARIUSZ SZOSTEK, BLOCKCHAIN AND THE LAW 11–13 (2019) (providing an account of the various European instruments adopted in relation to DLTs and blockchain).

[9] *See, e.g.*, S.B. 086, 71st Gen. Assemb., 2d Reg. Sess. (Colo. 2018) (concerning the use of cyber coding cryptology for state records); S.B. 1091, 53d Leg., 2d Reg. Sess. (Ariz. 2018); S.B. 464, 154th Gen. Assemb., Reg Sess. (Ga. 2018) (intending to allow cryptocurrencies to be used in order to pay taxes); *see also* H.R.J. Res. 25, 100th Gen. Assemb., Reg Sess. (Ill. 2018) (exploring the possibility of using blockchain and DLTs to create a more efficient, integrated and trusted state service). In the EU, 21 Member States and Norway agreed to sign a Declaration creating the European Blockchain Partnership and cooperate in the establishment of a European Blockchain Services Infrastructure that will support the delivery of cross border digital public services. *European Countries Join Blockchain Partnership*, EUROPEAN COMM'N (Apr. 10, 2018), https://perma.cc/Y2RL-8BF7.

[10] For some examples in the popular press, see Roger Aitken, *Bitland's African Blockchain Initiative Putting Land on the Ledger*, FORBES: INVESTING (Apr. 5, 2016), https://perma.cc/99TT-4RYD (stating that blockchain will allow citizens in Ghana to survey land and record title deeds on the Bitland blockchain, bringing clarity to land ownership rights, reducing corruption, and opening up trillions of dollars in locked capital); *see also* Tatiana Koffman, *Blockchain—Africa Rising*, FORBES (Apr. 4, 2019), https://perma.cc/KHM7-DJHH (outlining organizations in Africa utilizing blockchain technology to invest in local economies).

[11] *See, e.g.*, U.K. GOV'T OFFICE FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCKCHAIN 5–6 (2016) (outlining the British government's potential uses for blockchain); IBM INST. FOR BUS. VALUE, BUILDING TRUST IN GOVERNMENT: EXPLORING THE POTENTIAL OF BLOCKCHAINS 1 (2017) (surveying 200 government leaders in 16 countries on their experiences and expectations for blockchain).

[12] Marcella Atzori, *Blockchain Technology and Decentralized Governance: Is the State Still Necessary?*, J. GOVERNANCE & REG., Mar. 2017, at 45, 45, 47.

[13] Stephen Jones, *Data Breaches, Bitcoin, and Blockchain Technology: A Modern Approach to the Data-Security Crisis*, 50 TEX. TECH. L. REV. 783, 800 (2018).

Second, the attention around blockchain results from the fact the technology heralds a potential withdrawal of the State and public authorities by making 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.[14] It is precisely the prospect of a future made up of "decentralized trustless transactions"[15]—whereby the requirement to trust qualified intermediaries to carry out certain activities, to provide certain services or to perform certain functions could be dispensed with on a wide scale[16]—that immediately attracted the attention of financial institutions and industries all around the world.[17] For the same reasons, blockchain technology could have major implications for activities managed by public authorities, and more generally for how they interact with the citizenry.[18] However, an analysis of this type would fall beyond the scope of this Article. Instead, this Article will focus on the impact this new technology could have on monitoring compliance with environmental regulations rendering it much more efficient thanks to its progressively increasing involvement in the monitoring of various non-public actors, including specifically regulated entities and the general public.

With this in mind, Part II of this Article starts by setting out the basic technical characteristics of blockchain technology, explaining why it guarantees more security, immutability, and data integrity than traditional centralized databases. Part III examines how the characteristics of blockchain technology make it possible to put in place a form of "dispersed verification" of environmental data under which the

---

14 *But see* Atzori, *supra* note 12, at 51–54 (highlighting the risks associated with the reduction in the authority of the State as a central point of coordination within society).

15 Melanie Swan, Blockchain: Blueprint for A New Economy, at x (2015).

16 *See* Kevin Werbach, *Trust, but Verify: Why the Blockchain Needs the Law*, 33 Berkeley Tech. L.J. 487, 493–94 (2018) [hereinafter Werbach, *Trust, but Verify*] (discussing the benefits, use, and security risks of the blockchain as a global system of trust, trade, and monetization); Kevin Werbach, Blockchain and the New Architecture of Trust 3 (2018); Bruce Schneier, *There's No Good Reason to Trust Blockchain Technology*, Wired (Feb. 6, 2019) https://perma.cc/H3CD-YHHJ (distinguishing between four types of "trust architecture": peer-to-peer trust, which is when individuals learn to trust each other based on morals and reputational systems; leviathan trust, which is institutional trust in governments and institutions; intermediary trust, which is trust in banks, notaries and third parties in general; and distributed trust, which is trust in the blockchain system).

17 *See* Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia 2–3, [hereinafter De Filippi & Wright, *Lex Cryptographia*] (discussing the drastic impacts the blockchain could have on institutional trade); Philip Boutcher et al., European Parliamentary Research Serv., How Blockchain Technology Could Change Our Lives 4 (Feb. 2017); Don Tapscott & Alex Tapscott, Blockchain Revolution: How The Technology Behind Bitcoin Is Changing Money, Business, and the World 8 (2016) (underscoring the capacity of blockchain technology to redesign human interactions in business and society at large).

18 *See, e.g.*, Steven Young, *Changing Governance Models by Applying Blockchain Computing*, 26 Cath. U. J.L. & Tech., no. 2, 2018, at 53, 53 (describing how blockchain could change government).

people who use that distributed ledger directly certify the completion of certain operations and associate them with a precise timestamp. In other words, blockchain technology allows the general public, and indeed, any interested party (including regulated entities), to verify the formal validity of environmental data. This, in turn, constitutes the essential prerequisite for the conduct of effective substantive checks at a later stage (i.e., concerning the accuracy of the data). Under that system, the traditional alterity between the controlling administration, the parties 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.

Part IV then uses this as a springboard to demonstrate how, building on a context in which developments in information technology have already established a framework for enhancing and promoting transparent environmental information, blockchain technology incorporates special features that make it even more conducive to achieving this goal. And, by enabling improved data management and faster data sharing, this technology has the potential to involve private individuals directly in creating public databases, thereby giving rise to an innovative system—which will be referred to in this Article as "notarized transparency"—under which data 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 individuals. Part V concludes by identifying some opportunities offered by blockchain, more generally, for public regulation.

The core claim made in this Article is that blockchain technology can operate as the basis for a more direct engagement of both regulated entities and the general public in the monitoring and enforcement of environmental law, thereby improving environmental compliance as a whole and, at the same time, ensuring alignment with the growing international consensus around the value of public participation in environmental matters. In this sense, blockchain technology will make it possible to conceptualize an innovative "choral" approach to environmental regulation to achieve higher levels of environmental protection.[19]

From a systemic viewpoint, the type of "dispersed verification" of data that can be achieved using DLT moves beyond the juxtaposition between command and control and market instruments,[20] giving rise to

---

[19] This reflects the traditional distinction within Greek lyric where the choral lyric (sung by a chorus, generally also dancing) was juxtaposed with the monody. *But see* Malcom Davies, *Monody, Choral Lyric, and the Tyranny of the Hand-Book*, 38 THE CLASSICAL Q. 52, 52 (1988) (raising doubts concerning the orthodoxy of that distinction).

[20] *See* Bruce A. Ackerman & Richard B. Stewart, *Reforming Environmental Law*, 37 STAN. L. REV. 1333, 1333 (1985) (arguing for the demise of command-and-control regulation); Richard B. Stewart, *A New Generation of Environmental Regulation?*, 29 CAP. U. L.

an entirely innovative approach under which dynamic forces within society become directly involved to perform functions that have previously fallen within the purview of public agencies and in reconfiguring certain traditional market mechanisms in innovative and potentially more effective terms. At the same time, in facilitating the disclosure and transfer of information with greater ease and rapidity—by enabling closer cooperation amongst public agencies, regulated entities, and the general public—the blockchain is an infrastructure particularly suited to the adoption of modular, flexible, and adaptable approaches to the management of environmental problems.[21]

Although this technology is becoming a matter of increasingly intense debate within the literature, an analysis of its potential implications for regulatory compliance is still lacking. This Article aims to fill this gap and to provide a preliminary assessment of the potential and benefits blockchain technology could have, with particular reference to environmental regulation in the United States and in Europe.

Naturally, the author is acutely aware that blockchain technology is still in its infancy and that additional technological developments are necessary before secure and wide-scale use is possible.[22] Nonetheless, the incredible economic[23] and intellectual investment already made in blockchain technology suggests that it will make its mark.[24] With this in mind, it is, perhaps, not premature to consider the new perspectives that the technology could also open up for environmental law.

II. Blockchain Technology

This Part introduces blockchain technology, placing specific emphasis on the characteristics that make it particularly suited to

Rev. 21, 27–38, 99–134 (2001) [hereinafter Stewart, *A New Generation*] (analyzing environmental command and control regulatory systems, and how they could change by using more accurate modeling and market-based solutions).

21 *See* Jody Freeman & Daniel A. Farber, *Thirty-Fourth Annual Administrative Law Issue: Modular Environmental Regulation*, 54 Duke L.J. 795, 798–99 (2005) (discussing modular environmental regulation).

22 *See* Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, Harv. Bus. Rev., Jan.–Feb. 2017, at 120 (arguing that blockchain is not a disruptive technology but rather "a foundational technology," since "[i]t has the potential to create new foundations for our economic and social systems." However, according to the authors, "while the impact [of blockchain] will be enormous, it will take decades for blockchains to seep into our economic and social infrastructure.").

23 For example, the European Union has budgeted five million euros to support blockchain initiatives through the research and development program Horizon 2020. *Prizes*, European Comm'n, https://perma.cc/C7Y9-RM53 (last visited Oct. 27, 2020). In addition, in February 2018 the European Commission launched the EU Blockchain Observatory and Forum and will invest some €300 million in projects supporting the use of blockchain. *Funding*, European Comm'n, https://perma.cc/DUT9-MTPC (last visited Nov. 4, 2020).

24 *See* Michèle Finck, Blockchain Regulation and Governance in Europe 3 (2019) ("Even if the promises currently associated with a distributed ledger do not deliver, current innovation efforts will still result in innovation, even if not in the form currently projected.").

reinforcing and enhancing the efficacy of environmental monitoring. In addition, this Part analyzes the characteristics of permissionless and permissioned blockchains to establish how that distinction might not be so significant within the area of environmental law were environmental non-governmental organizations (NGOs) and other groups representing the general public nonetheless to be recognized the right to operate on the distributed ledger.

A. Data Integrity and Security

Discussion of blockchain started in 2009 when, in response to the 2008 financial crisis, an individual using the pseudonym Satoshi Nakamoto published a "white paper" in which he proposed an electronic peer-to-peer payment system called Bitcoin, which would allow "online payments to be sent directly from one party to another without going through a financial institution."[25]

Bitcoin is thus founded on blockchain technology, which incorporates distributed databases (or ledgers), cryptography, and consensus protocols to establish "a distributed, shared, encrypted database that serves as an irreversible and incorruptible public repository of information."[26]

A database is "distributed" where it is not physically hosted on one single server, but rather on a distributed network of computers, each of which holds an identical copy, which is updated in real time.[27] Data in such a database are aggregated into blocks which, once they reach a certain size, are chained to one another through a hashing process.[28] As part of this process, the data in each block are converted into a digital fingerprint (or a "hash") comprised of a string of characters and numbers with a fixed length,[29] which cannot be reverse-engineered (in

---

[25] Satoshi Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System* 1 (describing the bitcoin system). For a full technical description of the way in which Bitcoin operates, see Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction vii (2016) (providing a foundational understanding of bitcoin).

[26] De Filippi & Wright, *Lex Cryptographia*, *supra* note 17, at 2. *See also id.* at 5 n.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." *See also* Arvind Narayanan & Jeremy Clark, *Bitcoin's Academic Pedigree: The Concept of Cryptocurrencies Is Built from Forgotten Ideas in Research Literature*, ACM Queue, Jul.–Aug. 2017, at 1, 1 (arguing bitcoin was not a radical innovation—its technical components came from 1980–1990s academic literature).

[27] Dylan Yaga et al., Nat'l Inst. of Standards & Tech., Blockchain Technology Overview 1 (2018).

[28] *Id.* at 1, 7, 17.

[29] H.B. Pethe & S.R. Pande, *An Overview of Cryptographic Hash Functions MD-5 and SHA*, 5 ISOR J. Computer Engineering 37, 37 (2016). For example, the length for Bitcoin is still 256 bits (Secure Hash Algoritm-256), irrespective of the size of the data in-

this sense hashing is a "one-way" function because it is practically impossible to establish the content of any given body of data starting from its hash).[30] Each hash is uniquely associated with a specific block: this means that even a minimal change to the contents of the data block (i.e., changing one single character) would generate a completely different hash.[31]

To formulate the chain of blocks, the hash for each block is cryptographically signed with the hash of the previous block, timestamped, and published to the network.[32] Each of these three steps has an extremely precise function. Incorporating the hash from the previous block into the next one ensures the data from the various blocks cannot be manipulated without leaving a trace; in fact, any alteration of the data grouped together within a block will result in a change not only in the hash for that block but also all of the subsequent hashes in the chain.[33] The function of the timestamp is to establish that the data originating in that particular hash existed at a precise moment in time.[34] This is known as "notarization," which involves the allocation of a specific date and time to the data entry, establishing the point in time when any given operation was carried out, which can then be relied on against third parties.[35] Finally, hashes and timestamps are published to ensure anyone in the network can see at what time any specific data were entered and verify they have not been subsequently changed.[36]

Accordingly, this creates a transparent and "tamper-evident" database,[37] which permanently records transactions without necessarily revealing their content.[38] In fact, while the "block header" (which contains the hash for the data in the block, the timestamp, and the hash

serted. *See* Matt, *What Is SHA-256 And How Is It Related*, MYCRYPTOPEDIA, https://perma.cc/6EP3-TN9V (last updated Nov. 1, 2018).

30 Werbach, *Trust, but Verify*, *supra* note 16, at 502, 502 n.70 ("It is easy to compute the hash function of any file. An input string will produce the same output string every time. However, there is no known way to go from a hash back to the input string other than trial and error." For this reason, a cryptographic hash is said to be a one-way function.).

31 YAGA ET AL., *supra* note 27, at 7.

32 *Id.* at 15, 17.

33 Jean Bacon et al., *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers*, 25 RICH. J.L. & TECH. 1, 12 (2018) [hereinafter Bacon et al. I].

34 Nakamoto, *supra* note 25, at 2.

35 KC Tam, *Notarization in Blockchain (Part 1)*, MEDIUM (Aug. 28, 2018), https://perma.cc/YAL7-K79E.

36 *See* De Filippi & Wright, *Lex Cryptographia*, *supra* note 17, at 4–5 (noting that blockchains store data in a unique manner, at least compared to existing data structures); Nakamoto, *supra* note 25, at 2.

37 HOSSEIN KAKAVAND & NICOLETTE KOST DE SEVRES, DLA PIPER, THE BLOCKCHAIN REVOLUTION: AN ANALYSIS OF REGULATION AND TECHNOLOGY RELATED TO DISTRIBUTED LEDGER TECHNOLOGIES 6 (2017); Bacon et al. I, *supra* note 33, at 5, 9, 12; YANLING CHANG ET AL., BLOCKCHAIN IN GLOBAL SUPPLY CHAINS AND CROSS BORDER TRADE: A CRITICAL SYNTHESIS OF THE STATE-OF-THE-ART, CHALLENGES AND OPPORTUNITIES 11, 13.

38 KAKAVAND & DE SEVRES, *supra* note 37, at 6; CHANG ET AL., *supra* note 37, at 11–12.

from the previous block) is visible to everyone, the data within the block (the "block body") can only be inserted as plain text or encrypted text, depending upon its intended purpose.[39] If the data are encrypted, only a person with a specific encryption key for unscrambling them can read them; this means the blockchain can be configured in such a way as to permit differing levels of visibility and, if adequately designed, can enable any sensitive data to be kept secret.[40]

It is clear from the above the exceptional security of the blockchain results from the special arrangements for registering data described above and the use of distributed databases (or ledgers). Indeed, the fact that the database is shared between an indefinite number of computers (so-called "nodes," which must be distinguished from simple "users," the latter being those who request recording new data and who 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)[41] not only hugely complicates any attempt at interference but also makes it much more difficult to lose the information recorded in them.

The defining characteristic of the system lies not only in the dissemination of the actual data recorded (there is no central record, such as those usually kept by banks, internet service providers or public authorities) but also in the fact information is entered by a wide variety of actors.[42] This means when a "user" asks to register new data, the data must foremost, be validated by one of the nodes in the network.[43] Thereafter, 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 this validation occurred under clearly defined, pre-agreed rules, that is under the

[39] Zibin Zheng et al., *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, *in* IEEE, International Congress on Big Data, 557, 558 (2017); *see* Finck, *supra* note 24, at 90–91.

[40] The system used is that of "public-private cryptography" developed in the late 1970s under which the data provider holds a private key and can exercise control over its own data. For a full discussion, see Primavera De Filippi & Aaron Wright, Blockchain and the Law: The Rule of Code 14–15 (2018) (explaining the development and utility of public-private key cryptography). For an analysis of the risks and opportunities that blockchain technology could entail for the protection of personal data, focusing in particular on the tension between the EU data protection law and that technology, see Finck, *supra* note 24, at 88, 90–91.

[41] Yaga et al., *supra* note 28, at 2–3, 13.

[42] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 2, https://perma.cc/72AP-FB7N ("A common solution [to prevent double-spending of currency] is to introduce a trusted central authority . . . [to] check[] every transaction for double spending. . . . [W]ithout a trusted party, transactions must be publicly announced . . . and we need a system for participants to agree on a single history of the order in which they were received.").

[43] Paolo Tasca & Claudio J. Tessone, *A Taxonomy of Blockchain Technologies: Principles of Identification and Classification*, Ledger, 2019, at 1, 5 https://perma.cc/JA2S-4LJG ("The decentralised consensus on transactions governs the update of the ledger by transferring the responsibilities to local nodes which independently verify the transactions and add them to the most cumulative computation throughput.").

blockchain protocol which establishes which data can be recorded (and what characteristics the data must have).[44] This is called a "consensus protocol" because the rules enable the various nodes to reach agreement as to which blocks should be added to the chain.[45]

The most well-known consensus algorithm, previously considered the most secure option for networks with a large number of mutually unacquainted participants is Bitcoin's "proof of work" algorithm.[46] In this case, in order to avoid fraud, the blocks are validated according to complex, energy-consuming mathematical calculations for identifying a valid hash that satisfies certain properties for each new block.[47] 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.[48] The successful miner is then rewarded with a certain number of Bitcoins.[49]

The necessary energy investment to mine each new block makes it practically impossible for any one operator to control a number of nodes corresponding to 51% of the total computational capacity of the network (so-called "Sybil attack"),[50] which could corrupt the system.[51] On the

[44] 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. *See* Young, *supra* note 18, at 54 ("The algorithms that control this communication use cryptography to ensure that only the proper computers are making the decisions [and] that the blockchain does not record improper transactions . . . .").

[45] Chris Hammerschmidt, *Consensus in Blockchain Systems: In Short*, MEDIUM (Jan. 27, 2017), https://perma.cc/764V-RQ3K ("[I]t is necessary for the distributed operators of the blockchain to evaluate and agree on all addenda before they are permanently incorporated into the blockchain. . . . This review results in the 'consensus' I am examining here.").

[46] Tasca & Tessone, *supra* note 43, at 10 ("The most widely used cryptocurrency, Bitcoin, uses Proof-of-Work (PoW) to ensure the immutability of transaction records.").

[47] The nodes that compete with one another in order to validate new blocks are referred to as "miners." Bacon et al. I, supra note 33, at 24–25. Specifically, miners must identify a hash, which must start with a precise number of zeros according to the requirements of the Bitcoin protocol applicable for each new block at that given time. *Id.* The first node that finds the valid hash broadcasts it to the entire network. The other nodes then run a simple calculation in order to verify that the hash identified is compliant with Bitcoin protocol's specification (in fact, finding a valid hash requires a lot of work and energy, while checking whether the required properties are satisfied is very easy). *Id.* at 25. If a majority of nodes confirm it as valid, the block corresponding to the hash is chronologically added to the chain (i.e., each node adds that block to its own local copy of the blockchain), while the successful miner is awarded a certain number of Bitcoin. *Id.* at 20–21. The name "proof of work" is derived from the fact that the node that generates the valid hash thereby proves that it has put enough computing resources into the task. *Id.* at 23–24.

[48] YAGA ET AL., *supra* note 27.

[49] Bacon et al. I, *supra* note 33, at 20–21.

[50] For a technical explanation, see generally John R. Douceur, *The Sybil Attack*, *in* PEER-TO-PEER SYSTEMS 251 (Peter Druschel et al. eds., 2002) ("If distinct entities for remote entities are not established either by an explicit certification . . . certification authority . . . or by an implicit one . . . these systems are susceptible to Sybil attacks, in which a small number of entities counterfeit multiple identities so as to comprise a disproportionate share on the system.").

other hand, the very requirement of energy investment raises several critical issues on an environmental level and constitutes one of the main limits to the Bitcoin system—such limits discouraging its usage in other sectors, at least for the time being.[52] Over time, other types of consensus protocol have therefore been developed, which are more or less efficient and more or less resistant to potential Sybil attacks.[53]

It is not necessary in this Article to consider these mechanisms in detail. For now, it is sufficient to simply note that consensus protocols lie at the very heart of the blockchain by making 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.

B. Permissionless and Permissioned Blockchains

Whereas the model described above is the original form of blockchain technology, which operates using distributed ledgers, it should also be pointed out that databases may be decentralized to different degrees, depending upon the relevant requirements that need to be met (although data must in all instances be recorded in cryptographically interlinked blocks).

---

51 However, things might become different with the dissemination of quantum computers. Tiago M. Fernandez-Carames & Paula Fraga-Lamas, *Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks*, INST. ELECTRICAL & ELECTRONICS ENGINEERS ACCESS, Feb. 4, 2020, at 21091, 21093 https://perma.cc/STH5-AP63 ("[I]t is estimated that in the next 20 years such a kind of computers will be functional enough to be able to break easily current strong public-key cryptosystems.").

52 Miners are even competing with one another to locate sources close to cheap electricity. *See, e.g.*, Paul Roberts, *This Is What Happens When Bitcoin Miners Take Over Your Town*, POLITICO MAG. (Mar.–Apr. 2018), https://perma.cc/E27Q-L7J2 ("[In Wenatchee, Washington] [t]here was a growing, often bitter competition for mining sites that had adequate power . . . ."); *Lylian Teng, Chinese Bitcoin Miners Suffer in Iran Despite Cheap Power, BITCOIN MAG. (Apr. 10, 2019), https://perma.cc/6C8Q-QYS7* ("Many Chinese cryptominers have migrated to places with cheap electricity and favorable policies as a result of the escalated government crackdown on cryptocurrency . . . ."). *See also* Pasquale Giungato et al., *Current Trends in Sustainability of Bitcoins and Related Blockchain Technology*, SUSTAINABILITY, Nov. 2017, at 1, 9, https://perma.cc/SMH3-HGJ3 ("To maintain profitable mining revenues, miners use more and more powerful and less energy-demanding hardware, starting from the CPU, and passing through GPU, FPGAs, and recently ASICs to follow economic sustainability and placing bitcoin farmers in the countries with the cheapest electricity prices.").

53 For example, another system used within permissionless blockchains is "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. *See* Tasca & Tessone, *supra* note 43, at 11 ("The probability that a given *prover* is selected to verify the next block grows in relation to the share of assets that prover has within the system. The underlying assumption is that users with a large share of the system wealth are more likely to provide trustworthy information with respect to the verification process, and are therefore to be considered a more trustworthy validator.").

The first blockchains associated with cryptocurrencies were conceptualized as permissionless platforms enabling any person to register new data (thus acting as a "user"), to download the entire database (thus acting as a "node"), and to validate new blocks (thus acting as a "miner").[54] 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.[55] Security—in terms of tamper resistance—is guaranteed by coupling the anonymity of transactions with their full online visibility and traceability (i.e., these platforms are also, as a rule, public).[56] Thus, anyone can, for instance, see that a particular Bitcoin address sent a specific sum of money to another address, without, however, necessarily knowing to whom these addresses actually refer in the real world.[57]

However, financial and industrial operators are increasingly experimenting with using blockchain technology to meet with different needs.[58] These include for instance the need to share sensitive data between parties that know one another using a system that is overall more tamper resistant; the need to reduce costs and the time required to

---

54 This is the case not only for Bitcoin, but also for Ethereum (the second largest cryptocurrency in the word), which uses the same blockchain technology as Bitcoin, although also allows users to program "smart contracts." Smart contracts are agreements coded into the blockchain that execute obligations without any third-party intervention. *See* De Filippi & Wright, *supra* note 17, at 24.

55 Hence the slogan, which is used in relation to the technology under examination, "in code we trust" or "in crypto we trust," which imply 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. *See* Hammerschmidt, *supra* note 45; Michael Casey & Paul Vigna, *In Blockchain We Trust*, MIT TECHNOLOGY REV. (Apr. 9, 2018), https://perma.cc/8CBY-U6ZV.

56 *See* Jean Bacon et al., *Blockchain Demystified*, QUEEN MARY SCH. L. LEGAL STUD. RES. PAPER SERIES, Dec. 21, 2017, at 49–50 [hereinafter Bacon et al. II]; Nakamoto, *supra* note 25, at 6 ("The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.").

57 CHRIS JAIKARAN, CONG. RESEARCH SERV., TE10025, BEYOND BITCOIN: EMERGING APPLICATIONS FOR BLOCKCHAIN TECHNOLOGY 1–2 (2018). This is also the reason why every Bitcoin transaction must be digitally signed using a public-private cryptographic key, given that transactions are propagated through a peer-to-peer network and their origin cannot be proven. YAGA ET AL., *supra* note 27, at 14–15. As a result, each user must have his or her own alphanumeric address, enabling user anonymity, while at the same time ensuring security and transparency. Camila Sitonio & Alberto Nucciarelli, *The Impact of Blockchain on the Music Industry*, INT'L TELECOMM. SOC'Y, Aug. 2018, at 3.

58 *See* Jatinder Singh & Johan David Michels, *Blockchain as a Service: Providers and Trust*, QUEEN MARY SCH. L. LEGAL STUD. RES. PAPER SERIES, Dec. 21, 2017, at 4–5 (listing Amazon, Google, IBM, and Microsoft among those experimenting with blockchain).

synchronize different databases, also avoiding the risk of errors; and also the need to resolve some of the inefficiencies inherent within centralized databases.[59] In all of these cases, it is not 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. On the contrary, a permissioned blockchain, which operates as a "narrowly distributed" platform with a shared (as opposed to distributed) ledger, may prove more suitable for this purpose, as only some clearly identified operators store the database and validate new blocks.[60] Conversely, 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.[61] Blockchains of this type are used, for example, in the financial sector to make cross-border cash transfers.[62] They can also be used in a supply chain whenever there is a need to guarantee the origin, form of production, and transformation over time of a particular product.[63]

Several years ago, some countries used permissioned blockchains to ensure the integrity and security of their own public registers and databases.[64] This has been done in Estonia[65] and in other countries from

---

59 *Id.* at 4, 6, 15.

60 Bacon et al. II, *supra* note 56, at 21, 50.

61 *Id.* at 10–11. A distinction must therefore be drawn between permissioned blockchains and "fully private blockchains," which are databases stored in a centralized manner: this means that an individual organization verifies the data and ensures that they are registered on a fully centralized register organized into the block structure described. Ricardo Persiani, Development and Evaluation of Cryptocurrency and PSD2 Payment-Methods in an Ethereum-Based Loyalty Point System 16 (2017–2018) (published M.S. thesis, Politecnico di Torino) (on file with Politecnico di Torino).

62 Jorgen Brastad & Philip Alexander Stendahl, Blockchain in Financial Markets and Intermediation: A Qualitative Exploratory Study of the Impact of Blockchain Technology on the Financial Market Infrastructure and Financial Services 15–16, 57, 60–61 (unpublished M.S. thesis, Norwegian School of Economics) (on file with Norwegian School of Economics). This is the case, for example, for Ripple, the so-called banks' cryptocurrency, which was created by a private company with the aim of enabling money to be transferred (in any currency) in real time between banks participating in the network (thus on a peer-to-peer basis), thereby reducing or eliminating the costs of financial transactions. *Id.* at 61; *Our Story*, RIPPLE, https://perma.cc/75JS-JLNM (last visited Sept. 22, 2020).

63 *See, e.g.*, *Beyond Bitcoin: Emerging Applications for Bitcoin Technology: Joint Hearing Before the House Subcomm. On Oversight and House Subcomm. On Research and Tech. Comm. On Science, Space, and Tech.*, 105th Cong. 41, 52 (2018) (statement of Gennaro Cuomo, IBM Fellow, Vice President Blockchain Technologies, IBM Cloud) (statement of Frank Yiannas, Vice President of Food Safety, Walmart) (describing the benefits of blockchain use in over 400 projects, such as the traceability of mango production).

64 Rhys Gregory, *More Governments Will Use Blockchain Technology if it Adapts to Their Needs*, WALES 247 (Sept. 15, 2020) https://perma.cc/W2RX-32YJ; Jaan Priisala & Rain Ottis, *Personal Control of Privacy and Data: Estonian Experience*, 7 HEALTH & TECH. 441, 449–50 (2017).

65 Estonia started testing the use of cryptography to secure data and transactions in 2008, six months before the Bitcoin was created. At that time, Estonians referred to the technology as "hash-linked-time-stamping." *Frequently Asked Questions*, E-ESTONIA, https://perma.cc/KCH8-2U2B (last visited Sept. 22, 2019). *See also* Jaan Priisalu & Rain Ottis, *supra* note 64, at 449; Clare Sullivan & Eric Burger, *E-Residency and Blockchain*,

the former Soviet Union such as Georgia and Ukraine, which were amongst the first to experiment with blockchain-like technologies to improve their land registries and transfer processes.[66]

According to the current state of technological development, permissioned blockchains require less energy to operate because they use a traditional synchronous consensus protocol to establish agreement concerning the registration of new blocks, thus bypassing the costly "proof-of-work" or other similar asynchrony consensus protocols.[67] However, critics of these systems stress first that they do not amount to genuine blockchains, but rather simple "append-data only structures,"[68] which were, moreover, already broadly known and had been widely experimented with before the invention of Bitcoin.[69] Secondly, they stress that, while they are more efficient, they reintroduce forms of centralization.[70]

There is no need to consider in this Article whether so-called permissioned blockchains are genuine blockchains. However, it is sufficient to note the registration of blocks of data in distributed ledgers can be achieved in various ways associated with differing levels of anonymity and data visibility amongst the participants. Everything depends upon the objective set and the intended use of such platforms.[71]

33 COMPUT. L & SEC. REV. 470 (2017). *Cf.* Petteri Kivimäki, *There Is No Blockchain Technology in the X-Road*, NORDIC INST. FOR INTEROPERABILITY SOLS. (Apr. 26, 2018), https://perma.cc/WX9U-APR8 (arguing that the technology used in Estonia still operates according to a centralized data management system, and therefore is not an authentic blockchain).

66 Laura Shin, *Republic of Georgia to Pilot Land Titling on Blockchain with Economist Hernando De Soto*, *BitFury*, FORBES (Apr. 21, 2016), https://perma.cc/BC69-7Z7Q; Qiuyun Shang & Allison Price, *A Blockchain-Based Land Titling Project in The Republic of Georgia. Rebuilding Public Trust and Lessons for Future Pilot Projects*, INNOVATIONS: TECH., GOVERNANCE, GLOBALIZATION, Winter–Spring 2019, at 72, 73.

67 *See* Singh & Michels, *supra* note 58, at 8.

68 For example, databases that enable new transactions to be added but not existing ones to be removed or modified.

69 It is well known that the idea of cryptographically linking blocks in an append-only data structure was first developed in the paper written by Stuart Haber & W. Scott Stornetta, *How to Time-Stamp Digital Documents*, 3 J. CRYPTOLOGY 99, 99–111 (1991).

70 In this regard it is also important to clarify that, at least as far as Bitcoin is concerned, the computational capacity required in order to download the entire database and to validate new blocks is now so great that miners have to use specific hardware and operate in groups ("mining pools") in order to be more competitive. As a result, even the idea that anyone can act as a miner within permissionless blockchains is more a theoretical possibility than a reality. *See* FINCK, *supra* note 24, at 21 (discussing how this trend will inevitably entail a greater centralization because mining pools will end up controlling a significant percentage of the network's computational capacity, which is evidence of the fact that "there can be elements of stark centralization in allegedly decentralized networks."). *See also* Angela Walch, *In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains, in* REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES 60 (Philipp Hacker et al. eds., 2019) (discussing how decentralization plays a role in permissionless blockchains).

71 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 add-

Specifically related to environmental law, where the involvement of the general public in decision-making processes and the management of the related problems has always been of vital importance,[72] it would be consistent to imagine a system that allowed not only for the maximum visibility of the data registered in the blockchain, but also the broad involvement of the general public in the process of validating and registering data. This is also the position which appears to have been adopted within international instruments. It is sufficient to recall Principle 10 of the Rio Declaration on Environment and Development, drafted during the U.N. Conference on Environment and Development ("Earth Summit") in 1992 and adopted by 178 Member States (including the U.S. and the European Union).[73] That principle states "Environmental issues are best handled with the participation of all concerned citizens, at the relevant level" and requires that, for this purpose, each citizen must have "appropriate access to information concerning the environment that is held by public authorities, including information on hazardous materials and activities in their communities."[74]

A similar view has also been taken within the United Nations Economic Commission for Europe (UNECE)[75] Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (known as the Aahrus Convention), as the first international and legally binding instrument laying down detailed obligations for effectively implementing Principle 10.[76] Specifically, the Aarhus Convention clarifies right from the outset that,

ing 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. *See generally* Jean Bacon et al., *Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralized Ledgers*, 25 RICH. J.L. & TECH. 1, 6–19 (2018).

[72] *See* Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters, June 25, 1998, 2161 U.N.T.S. 447 [hereinafter Aarhus Convention] (discussing the principle that there is a long-standing connection between environmental law and public access to information).

[73] STAKEHOLDER FORUM FOR A SUSTAINABLE FUTURE, REVIEW OF IMPLEMENTATION OF THE RIO PRINCIPLES 1 (2011), https://perma.cc/WLF5-2B5S.

[74] U.N. Conference on Env't and Dev., *Rio Declaration on Environment and Development*, U.N. Doc. A/CONF.151/26 (Vol.1), annex I (Aug. 12, 1992) [hereinafter, *Rio Declaration*]*; see* STAKEHOLDER FORUM FOR A SUSTAINABLE FUTURE, *supra* note 73, at 68 (explaining that under principle 10, signatories to the Rio Declaration committed to recognizing the rights of people to hold their governments to account for environmental policies and laws).

[75] Aarhus Convention, *supra* note 72. The UNECE was established in 1947 as one of the five regional commissions of the United Nations with the aim to promote pan-European economic integration. There is a special section dedicated to the environment and social policies. UNECE includes 56 Member States in Europe, North America and Asia. However, all interested United Nations Member States can participate in the work of UNECE. *Mission*, UNITED ECON. COMM'N FOR EUR., https://perma.cc/C59Y-GYX7 (last visited Nov. 4, 2020).

[76] United Nations Econ. Comm'n for Eur., The Aarhus Convention: An Implementation Guide 24 (2d ed. 2014).

> in the field of the environment, improved access to information and public participation in decision-making enhance the quality and the implementation of decisions, contribute to public awareness of environmental issues, give the public the opportunity to express its concerns and enable public authorities to take due account of such concerns.[77]

In any case, the extent to which the system should be effectively open to active management by the general public is a question that will ultimately depend upon the specific regulatory choices made in the various jurisdictions. A middle way could be to leave the system open to consultation, while also allowing data to be validated only by certain specified environmental associations or other interested organized groups, which would once again have to be identified under the rules of the relevant legal systems.

Moreover, starting from the prerequisite that the public task of environmental protection is, in any case, a necessary one and cannot be suspended—and, it is inconceivable to provide for mandatory participation by interested individuals and NGOs—the data validation system put in place must be open, but must also be capable of functioning properly even if only public authorities are involved. Thus, involvement by public authorities should always be stipulated as a necessary prerequisite for operating the system. This would, to some extent, mark a return to a permissioned blockchain model, albeit a fully visible one (obviously subject to the permitted limits for environmental information under the various legal systems), which would above all be open to society, at least where NGOs and other associations representing social interests are involved in it. These NGOs and representative groups in general would naturally not receive any remuneration for their activities but would be motivated to cooperate, not only for ideological reasons, but also potentially to enhance their respective reputations, thereby further establishing their role within society.

III. BLOCKCHAIN TECHNOLOGY AND ENVIRONMENTAL MONITORING

This Part demonstrates how the characteristics of the blockchain described above render it particularly suited for efficiently and securely

[77] Aarhus Convention, *supra* note 72. The Aarhus Convention entered into force in 2001 and has to date been ratified by forty-seven parties in Europe and central Asia. *Status of Ratification*, UNITED NATIONS ECON. COMM'N FOR EUR., https://perma.cc/DJP2-5VU8 (last visited Oct. 8, 2020). The second pillar of the Aahrus Convention, which is dedicated to participation by the public in environmental decision making, was implemented in Europe by Directive 2003/35 of the European Parliament and of the Council of May 26, 2003, providing for public participation in respect of the drawing up of certain plans and programs relating to the environment and amending with regard to public participation and access to justice Council Directives 85/337/EEC and 96/61/EC. *Legislation*, EUR. COMM'N: ENV'T https://perma.cc/8MPZ-H56V (last visited Oct. 8, 2020).

coordinating a more effective system of environmental data verification capable of bringing about improved compliance and superior environmental outcomes. Specifically, it explains how, thanks to this technology, it is possible to achieve "dispersed verification" that environmental data has been lodged on time and in full. In doing so, this can exponentially increase oversight both over the effective conduct by public agencies of the controls for which they are responsible and over formal compliance by regulated entities with the provisions of environmental law. This Part then explains how the increased data reliability permitted by blockchain technology constitutes the basis for implementing more effective forms of monitoring, *inter alia*, of compliance with substantive environmental law.

The "dispersed verification" mechanism made possible by the blockchain is particularly important within a context, such as the current one, in which technological development already makes it possible to involve the general public and regulated entities on a broad scale in the collection of environmental data by facilitating the mechanisms for detecting pollution and those for processing, managing, and distributing the information concerned.[78] This will be discussed in the first instance in order to demonstrate how the exponential increase in the data available—concerning both environmental conditions and the degree of compliance with environmental law—within modern society has not yet however been accompanied by the implementation of effective systems for verifying the reliability of those data.[79]

A. Environmental Monitoring and Technological Development: Towards Greater Involvement of the General Public and Regulated Entities

It is generally recognized that the protection of the environment is an interest not only of each individual, but also, and above all, of the community. For this reason, the public authorities have historically been charged with this task, as the representatives of society. When performing this role, it is essential the authorities are, *inter alia*, adequately aware of the state of natural resources and the impact that particular human activities have on them.

Over the last few decades, technological advancements have made it possible to measure the state of particular natural resources (so-called ambient monitoring of environmental conditions) with an increasing

[78] *See* Robert L. Glicksman et al., *Technological Innovation, Data Analytics, and Environmental Enforcement*, 44 ECOLOGY L.Q. 41, 53 (2017) [hereinafter Glicksman et al., *Technological Innovation*] (analyzing the potential for improved monitoring capacity, advances in the dissemination of information, and improved data analytics in order to transform EPA enforcement programs).

[79] *See* ENV'T L. INST., BIG DATA AND ENVIRONMENTAL PROTECTION: AN INITIAL SURVEY OF PUBLIC AND PRIVATE INITIATIVES 3 (2014), https://perma.cc/TQ2F-8YFE (referencing some examples of the use of big data sets and analytics in environmental law).

degree of accuracy and continuity and at reasonable cost.[80] For example, the usage of highly advanced instruments such as satellite remote sensing, drones, and infrared devices, to mention but a few, can enable increasingly precise long-term assessments of pollutant levels and their concentration in various environmental media, thereby enhancing the ability of the public authorities to identify at an early stage any situations involving a risk for the environment and human health.[81] At the same time, it lays the foundations on which public agencies can base the regulatory strategies that are from time to time considered to be most suited to effectively implementing environmental law, and subsequently, adapt them over time in line with developments, based on data that more closely reflect the reality.[82] Similarly, the usage of highly advanced technological instruments can help to render more effective so-called compliance monitoring, that is the control of compliance with environmental law by regulated entities,[83] thereby laying the basis for more effective public enforcement.[84]

80 *See* Glicksman et al., *Technological Innovation*, *supra* note 78, at 45 (referencing some examples on ambient monitoring).

81 *See, e.g.*, Kenneth J. Markowitz, *Legal Challenges and Market Rewards to the Use and Acceptance of Remote Sensing and Digital Information as Evidence*, 12 DUKE ENV'T L. & POL'Y F. 219, 221 (2002) (including an overview of remote sensing technologies and its capacities for environmental assessment); Dave Owen, *Mapping, Modelling, and the Fragmentation of Environmental Law*, 1 UTAH L. REV. 219, 222 (2013) (noting that "increased data availability, new software systems, and exponentially greater computing power have combined to turn spatial analysis—that is, quantitative analysis of data coded to specific geographic coordinates—into the coin of the environmental realm."); Renee Schoof, *EPA Testing New Way to Measure Air Pollution Emissions*, 46 ENV'T REP. (BNA) 3244 (2015); Renee Schoof*, Infrared Camera Use Growing in Oil and Gas Sector*, 47 ENV'T REP. (BNA) 1007 (2016) (describing the experience of Colorado which has required the oil and gas industry to detect methane emissions using infrared cameras); *see* Glicksman et al., *Technological Innovation*, *supra* note 78, at 67–69 (referencing some examples of the use of advanced monitoring technologies by the Environmental Protection Agency).

82 *See* Daniel C. Esty, *Environmental Protection in the Information Age*, 79 N.Y.U. L. Rev. 115, 119 (2004) (providing a thorough explanation of the possibilities that the technologies of the Information Age could create for pollution control by making environmental protection "more data-driven, empirical, and analytically rigorous"); *see also* Bradley C. Karkkainen, *Toward A Smarter NEPA: Monitoring and Managing Government's Environmental Performance*, 102 COLUM. L. REV. 903 (2002) (arguing in favor of post-decision monitoring as a tool to improve the effectiveness of agencies' action and to enable continuous reevaluation and readjustment of the measures taken in order to protect the environment).

83 On the distinction between ambient monitoring and compliance monitoring, see Eric Biber, *The Problem of Environmental Monitoring*, 83 U. COLO. L. REV. 1, 10 (2011) (noting that "ambient monitoring generally measures conditions that are affected by a combination of both human and natural causes, while compliance monitoring generally measures specific human causes").

84 Public enforcement here refers to any process of enforcement controlled by administrative agencies as opposed to private enforcement, where a private individual (or a group representing the interest of its individual members) has a legal right to enforce violations of environmental law. *See* J. Maria Glover, *The Structural Role of Private Enforcement Mechanism in Public Law*, 53 WM. & MARY L. REV. 1137, 1140 (2012) (contrasting the American system, which relies heavily on enforcement by private parties to achieve public

Thus, the fact that "previously invisible pollution [has become] visible"[85] could have significant consequences both for ambient monitoring and for compliance monitoring, and also, in turn, for the enforcement and implementation of environmental law. More generally, there is no doubt technological development could also help to achieve a more complete implementation of some general principles of environmental law, including, first and foremost, the prevention principle and the principle that environmental damage should be rectified at the source, both of which require action to protect the environment to be taken at an early stage in order to prevent damage from occurring, rather than attempting to rectify it *ex post*.[86] It is no coincidence that the importance of using technology to monitor environmental conditions, emissions, and compliance was previously asserted by Principle 18 of the Stockholm Declaration of 1972 from the UN Conference on the Human Environment, which states "Science and technology, as part of their contribution to economic and social development, must be applied to the identification, avoidance and control of environmental risks and the solution of environmental problems."[87] More recently, the U.S. Environmental Protection Agency's (EPA) Next Generation Compliance initiative ("NEXT Gen")[88] of 2013

regulatory objectives, with the European system, which mainly relies on public enforcement by centralized state bureaucracies).

[85] Cynthia Giles, *Next Generation Compliance*, 45 ENV'T L. REP. NEWS & ANALYSIS 10205, 10207 (2015).

[86] For a clear statement of the principles of environmental law, see Consolidated Version of the Treaty on the Functioning of the European Union, art. 191, Sep. 5, 2008, (stating that "[u]nion policy on the environment shall aim at a high level of protection taking into account the diversity of situations in the various regions of the Union. It shall be based on the precautionary principle and on the principles that preventive action should be taken, that environmental damage should as a priority be rectified at source and that the polluter should pay."). *See generally*, in the EU scholarship, NICOLAS DE SADELEER, ENVIRONMENTAL PRINCIPLES: FROM POLITICAL SLOGANS TO LEGAL RULES 1 (2002) (stating that the precautionary and prevention principles are primary in European Community policy); ELOISE SCOTFORD, ENVIRONMENTAL PRINCIPLES AND THE EVOLUTION OF ENVIRONMENTAL LAW 1 (2017) (observing the European Court relying on the principles of prevention and the precautionary principle); LUDWIG KRÄMER & EMANUELA ORLANDO, PRINCIPLES OF ENVIRONMENTAL LAW 2 (2018) (stating that the preventive principle is a general principle of environmental law).

[87] U.N. Conference on the Human Environment, Principle 18, U.N. Doc. A/CONF.48/14 /Rev.1 (June 16, 1972) (commonly known as the Stockholm Declaration).

[88] *See Next Generation Compliance,* U.S. ENV'T PROTECTION AGENCY (2018), https://perma.cc/N7JF-C8PP (describing U.S. EPA's *Next Generation Compliance* said initiative). *See* Giles, *supra* note 85, at 10206–07 (noting that "[m]onitoring devices are becoming more accurate, more mobile, and cheaper, all of which is contributing to a revolution in how we find and fix pollution problems."). For some examples on how Next Generation Compliance approaches have been implemented in the National Pollutant Discharge Elimination System (NPDES), Clean Air Act (CAA), Resource Conservation and Recovery Act (RCRA), see *Compendia of Next Generation Compliance Examples in Water, Air, Waste, and Cleanup Programs*, U.S. ENV'T PROTECTION AGENCY (2020), https://perma.cc/25E5-SFTL (noting that the compendia allows states and the EPA to share information on creative ways to achieve environmental benefits).

identified the increased use of advanced monitoring (and reporting) technologies as one tool necessary to increase compliance with environmental regulations.[89]

This section sets out the limits within which the availability of innovative and low-cost technologies will allow for the greater involvement of operators other than public agencies in the collection of data concerning both environmental conditions and the compliance with environmental law by regulated entities.[90] This form of involvement is in keeping with the principles of so-called "environmental democracy" which, taking as their starting point the status of the environment as a collective resource, point to the need for the increasing involvement in its management of the general public and interested parties.[91]

1. The Involvement of Community and Local Groups in Ambient Monitoring

By using small, low-cost, mass-produced sensors, ordinary members of the public (often associated with local or community groups) can now collect enormous quantities of data in real time about, for example, the climate,[92] air and water quality,[93] the location of marine debris,[94] and

[89] *See* Robert L. Glicksman & David L. Markell, *Unraveling the Administrative State: Mechanism Choice, Key Actors, and Regulatory Tools*, 36 VA. ENV'T L.J. 318, 371–80 (2018) (analyzing the various tools identified by the EPA for increasing environmental compliance, specifically: improved communications achieved in particular by incentivizing e-reporting, increased transparency of compliance data, innovative enforcement strategies to be achieved in particular through third-party verifications, and better rules).

[90] *See* Giles, *supra* note 85, at 10207 (predicting that "changes, driven by new technologies, will encourage more direct industry and community engagement, and reduce the need for government action").

[91] *See generally* Gyula Bándi, *Introduction into the Concept of 'Environmental Democracy', in* ENVIRONMENTAL DEMOCRACY AND LAW: PUBLIC PARTICIPATION IN EUROPE, 1–20 (Gyula Bándi ed., 2014) (providing background on environmental democracy and its effect on public participation).

[92] *See, e.g.*, *What's Going On Here?,* CITIZEN WEATHER OBSERVER PROGRAM (Apr. 14, 2004), https://perma.cc/9H4J-MVZ5 (collecting weather data from more than 7000 stations across the U.S. daily).

[93] *See, e.g.*, *The Egg,* AIR QUALITY EGG (2018), https://perma.cc/XE3L-5M8A (describing "The Egg" as a wifi-device that connects to an app which allows the user to read and share the current, local air quality). *See also The Project,* CITI-SENSE (2020), https://perma.cc/KF3R-KGM2. The CITI-SENSE Project, co-funded by the European Union's Seventh Framework Programme for Research, Technological Development and Innovation, grant agreement no. 308524, which aimed to involve citizens in assessments of air quality, environmental quality of public spaces in cities, and indoor air quality in schools by developing "Citizens' Observatories" in these areas. The idea was to complete the "sensor-platform-product-users" chain, coupling technologies for distributed monitoring (to assess the air quality) and information and communication technologies (to disclose the information) with the aim of empowering citizens to participate in environmental governance). Another example is that of the "bucket brigades" that use inexpensive technologies to measure air quality in their community, often checking for the presence of specific pollutants produced by nearby industrial facilities. *See* Christine Overdevest & Brian Mayer, *Harnessing the Power of Information Through Community Monitoring: Insights from Social Science*, 86 TEX. L. REV. 1493, 1510–11 (2008).

bird migratory routes.[95] This can moreover be done with no need for specific expertise or supporting organizational structures (and for this reason is called "citizen science").[96]

The direct involvement of the general public in projects to collect, process, and disseminate data concerning environmental conditions has the potential to provide additional sources of information for public agencies, which have always found it difficult to carry out such monitoring effectively: ambient monitoring is a costly and complex affair, which must be carried out on a wide scale and over the medium to long term.[97] On the other hand, in many cases, agencies intentionally fail to carry out ambient monitoring, for instance, to avoid exposing particular problems or because the lack of information allows for greater flexibility and maneuvering in the management of complex situations, specifically those involving environmental issues.[98] In such a scenario, the data collected by private individuals are beneficial above all to enhance the accountability of both agencies and regulated entities, thus bringing specific, previously unknown problems within the spotlight of public opinion.

However, data of this type also raise a whole series of problems:[99] For example, it is a known fact that, particularly due to their low level

---

94 *See, e.g.*, *Debis Tracker: An Open Data Citizen Scientist Movement,* NATIONAL GEOGRAPHIC: MARINE DEBRIS TRACKER, https://perma.cc/7MJQ-77YP (last visited Oct. 8, 2020) (The mobile app Marine Debris Tracker makes it easy to report the existence of marine debris or litter anywhere in the world).

95 *See, e.g.*, *History of the Christmas Bird Count*, AUDUBON, https://perma.cc/67PL-V54P (last visited Oct. 8, 2020) (describing how the Christmas Bird Count, beginning in 1900, has involved thousands of volunteer birdwatchers. Audubon uses the data gathered by volunteers in assessing the health of bird population across northeastern North America and help to guide conservation action). *See also* Erica H. Dunn et al., *Enhancing the Scientific Value of the Christmas Bird Count*, 122 THE AUK 338 (2005) (noting that the Christmas Bird Count (CBC) is the most geographically widespread and longest-running Western Hemisphere survey of birds); Glicksman et al., *Technological Innovation*, *supra* note 78, at 80–83 (providing further examples of citizen science projects).

96 *See* JAMES MCELFISH ET AL., ENV'T L. INST., CLEARING THE PATH: CITIZEN SCIENCE AND PUBLIC DECISION MAKING IN THE UNITED STATES 5 (2016), https://perma.cc/59H6-YJ4H (defining citizen science as "a form of open collaboration where members of the public undertake scientific work, often in collaboration with professional scientists and scientific institutions, to meet real world goals"); U.S. GENERAL SERVICES ADMINISTRATION: CITIZENSCIENCE.GOV., https://perma.cc/4BPQ-72YR (last visited Oct. 7, 2020); *see also* Giles, *supra* note 85, at 10207 (predicting that "[a]s the price of monitoring devices drop, we are not far from the day when the public will have access to pollution monitoring tools").

97 *See* Biber, *supra* note 83, at 22–23 (noting the "complexity and uncertainty" of ambient monitoring).

98 *See id.* at 48–49 ("An agency might be reluctant to monitor . . . because monitoring data might prove troublesome in the future . . . The lack of information, on the other hand, generally gives an agency a tremendous amount of political or legal leeway.").

99 *See* Gregg P. Macey, *The Architecture of Ignorance*, UTAH L. REV. 1627, 1630–31 (2013) (arguing in favor of the development of a "data-intensive" approach to regulation, as opposed to the "data-starved world" that had characterized the first laws on the environment).

of technical and scientific training, various local or community groups overstate the importance of certain situations and also shift the focus of their attention quickly from one crisis to another.[100] On the other hand, since they are not always clearly independent from the interests in play, doubts can emerge as to the real priority of certain problem issues they bring to the attention of the public.[101] Finally, and above all, these groups are often unable to ensure continuity within data collection,[102] which makes it difficult to infer reliable information about actual changes in the state of certain natural resources and how they may have been affected by human activities. For all of these reasons, environmental agencies today use the data collected in this manner largely to support public monitoring, in the sense they only use them where they point towards the need to carry out further inquiries.[103] It is therefore solely within these limits that ambient monitoring can be said to be no longer the exclusive domain of public agencies. Technological change has in some sense brought about a paradigm shift,[104] making it possible to move from a model focused on the role of agencies towards a mixed model that at least takes account of the increasing sensitivity of the public at large to environmental protection. In other words, the availability of advanced technological instruments has not altered the fundamental nature of ambient monitoring, that is its "essentially public"[105] nature, because it is conducted by public authorities.

But it must be acknowledged that technological development and the experience of the direct involvement of the general public in ambient monitoring are, for the time being, the only options available, imperfect as they may be, for making up for the limits and mitigating the costs borne by the authorities (and ultimately by society) of a function that is generally managed exclusively by public agencies. In fact, it is

[100] Dara O'Rourke & Gregg P. Macey, *Community Environmental Policing: Assessing New Strategies of Public Participation in Environmental Regulation*, 22 J. POL'Y ANALYSIS & MGMT. 383, 384 (2003) (noting that community groups tend to "shift their focus from crisis to crisis").

[101] *See* Biber, *supra* note 83, at 59 (noting that "even if volunteer monitoring is methodologically correct, it may nonetheless be suspect in the eyes of the public or the regulator because of claims that the information was collected by groups with a hidden agenda.").

[102] *See* IAN SPELLERBERG, MONITORING ECOLOGICAL CHANGE 231 (2d ed. 2005) (noting that continuity must be construed not only as the collection of data over the long term, but also in terms of consistency of data collection protocols over time so as to enable for instance comparisons over time to be made).

[103] *See* Glicksman et al., *Technological Innovation*, *supra* note 78, at 81 (stressing that agencies have used data generated from nongovernmental sources largely "as a signal warranting their own further inquiries into compliance status or ambient conditions").

[104] Emily G. Snyder et al., *The Changing Paradigm of Air Pollution Monitoring*, ENV'T SCI. & TECH. 11369, 11369 (2013) (stressing that approaches to the monitoring of air pollution have been changing from the use of "expensive, complex, stationary equipment, which limits who collects data, why data are collected, and how data are accessed" to the "materialization of lower-cost, easy-to-use, portable air pollution monitors (sensors) that provide high-time resolution data in near real-time").

[105] Biber, *supra* note 83, at 9 (underlying that "monitoring is necessary, difficult, and essentially public").

notoriously difficult in this area to induce private entities (i.e. polluting industries) to cooperate: Since it is essentially impossible to establish a clear link between any improvements in the state of natural resources with the environmental performance of individual operators, this means operators rarely have any incentive to attend to the collection and analysis of the relevant data.[106] Consider, for example, how complicated it can be to prove air quality improvement in a given area results from the installation of more advanced technologies by one or more businesses operating there, rather than by contrast, a simple increase in rain or other events with nothing at all to do with operators' actions.[107]

2. The Involvement of Regulated Entities in Compliance Monitoring

On the other hand, experiments with the direct involvement of regulated entities in compliance monitoring have been ongoing for some time.[108] The limits to an exclusively public system of verification of compliance with environmental law are well known and have been debated in detail, as are the reasons that led to developing alternative and more collaborative approaches.[109]

It is sufficient to recall at this juncture (also) this form of monitoring is particularly pervasive and costly, given it can apply to potentially any form of polluting economic activity, including, for example, minor sources of pollution that, taken individually, are almost irrelevant but when considered as a whole can have a significant impact

---

106 *Id.* at 12.

107 In fact, it was precisely the difficulty in establishing a connection between problematic environmental conditions and particular sources suspected of violating emission limits that influenced the design of the Clean Water Act in the U.S. in 1972. Specifically, Congress introduced a system based on the measurement of emissions of point source discharges to surface water in response to the failure of the ambient-monitoring approach to water pollution control. *See* N. William Hines, *History of the 1972 Clean Water Act: The Story Behind How the 1972 Act Became the Capstone on a Decade of Extraordinary Environmental Reform,* J. ENERGY & ENV'T L., Summer 2013, at 80, 95–99.

108 Rena I. Steinzor, *Reinventing Environmental Regulation: The Dangerous Journey from Command to Self-Control*, 22 HARV. ENV'T L. REV. 103, 183–200 (1998) (analyzing the barriers faced by the EPA in implementing self-control programs and advancing several proposals to reorient reinvention initiatives).

109 *See* IAN AYRES & JOHN BRAITHWAITE, RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE 3 (1992) (discussing the "need to transcend" the debate over regulation and deregulation which has been "rerun so many times"); THINKING ECOLOGICALLY: THE NEXT GENERATION OF ENVIRONMENTAL POLICY 2 (Marian R. Chertow & Daniel C. Esty eds., 1997); Daniel A. Farber, *Triangulating the Future of Reinvention: Three Emerging Models of Environmental Protection*, 1 U. ILL. L. REV. 61, 69 (2000); Clifford Rechtschaffen, *Deterrence vs. Cooperation and the Evolving Theory of Environmental Enforcement*, 71 S. CAL. L. REV. 1181, 1220 (1998); Stewart, *A New Generation*, *supra* note 20, at 147 (discussing environmental audit and management systems); George B. Wyeth, *"Standard" and "Alternative" Environmental Protection: The Changing Role of Environmental Agencies*, 31 WM. & MARY ENV'T L. & POL'Y REV. 5, 11–13 (2006); *but see* Steinzor, *supra* note 108, at 184–96 (analyzing the barriers faced by the EPA in implementing self-control programs and advancing several proposals to reorient reinvention initiatives).

on the environment.[110] On the other hand, it is often blocked by the information asymmetry to which administrations charged with overseeing regulated entities are subject.[111] Finally, this form of monitoring is fundamentally "reactive in nature"[112] as it does not seek to put an end to any instances of non-compliance and is not primarily focused on the prevention of offenses (other than from a perspective of "general deterrence").[113] It is therefore not suited to environmental law, where it is, by contrast, essential to act at an early stage in order to, *inter alia*, avoid causing irreversible harmful effects.

The growing attention paid to forms of self-monitoring and auditing, at least since the 1980s, thus essentially sought to resolve these problems, while developing regulated entities' greater awareness regarding their impact on the environment, in line with so-called "reflexive approaches" to environmental law.[114] The aim of these approaches is to promote the internalization of environmental law, incentivizing self-analysis by regulated entities of the consequences of their activity for the consumption of natural resources, thereby disseminating a culture of self-responsibility, which is juxtaposed to the traditional regulatory model based on the authoritative setting of limits and the control of compliance with them by public agencies.[115] The idea underlying reflexive regulation is therefore that organizations are particularly complex self-referential social systems that can react to a variety of both external and internal stimuli.[116] As a result, to influence the behavior of organizations by imposing limits and mandating

110 For instance, small farms can be significant contributors of pollution to both water and air. *See* J.B. Ruhl, *Farms, Their Environmental Harms, and Environmental Law*, 27 Ecology L.Q. 263, 266 (2000).

111 Adam R. Fremeth & Guy L. F. Holburn, *Information Asymmetries and Regulatory Decision Costs: An Analysis of U.S. Electric Utility Rate Changes 1980–2000,* 28 J.L. Econ. & Org. 127, 128 (2010) (explaining that information asymmetry in public utility regulation increases costs).

112 Martin de Bree and Han de Haas, *Using Management Systems in Public Environmental Supervision*, *in* Elgar Encyclopedia of Environmental Law vol. VIII: Policy Instruments in Environmental Law § IV.2.2.1 (Michael Faure ed., 2017).

113 "General deterrence" is taken to refer to the punishment of one actor in order to deter non-compliant behavior by other potential offenders. *See* Kelli D. Tomlinson, *An Examination of Deterrence Theory: Where Do We Stand?*, Federal Probation J., Dec. 2016, at 33, 33; *see also* Jon D. Silberman, *Does Environmental Deterrence Work? Evidence and Experience Say Yes, But We Need to Understand How and Why*, 30 Env't L. Rep. News & Analysis 10523 (2000).

114 Eric W. Orts, *Reflexive Environmental Law*, 89 Nw. U.L. Rev. 1227, 1252–67 (1995); Stewart, *A New Generation*, *supra* note 20, at 127–34; *see also* Gunther Teubner, *Substantive and Reflexive Elements in Modern Law*, 17 Law & Soc'y Rev. 239 (1983).

115 *See* Orts, *supra* note 114, at 1232 ("[R]eflexive environmental law aspires to engender a practice of environmentally responsible management."); Stewart, *A New Generation*, *supra* note 20, at 130 ("Reflexive law concerns structure and process; it neither establishes formal rules of interaction nor directs substantive outcomes."). The theory of reflexive regulation has its roots in the social systems theory developed by the German sociologist Niklas Luhmann. *See* Niklas Luhmann, Social Systems 1–5 (1995).

116 Gunther Teubner, *Substantive and Reflexive Elements in Modern Law,* 17 L. & Soc'y Rev. 239, 255 (1983).

substantive outcomes is considered reductive and bring about results that, considered overall, are modest.[117]

Where construed strictly, "reflexive regulation" focuses exclusively on procedures, cooperation and, in general, structural mechanisms that enable self-regulation[118] in such a way as to influence results without, however, imposing them from the outside.[119] From this perspective, self-monitoring and reporting mechanisms can replace external controls with a more effective structure of internal controls,[120] thereby encouraging regulated entities to strive to achieve even very high environmental outcomes,[121] and in any case, generally enabling them to identify and correct in good time any regulatory violations, thus preventing irreparable harm to the environment. In reality, there is broad consensus regarding the fact these mechanisms work best where they are used alongside (and not as replacements for) more traditional command-and-control instruments.[122] Besides, it is well known that it is

[117] *See* Stewart, *A New Generation*, *supra* note 20, at 127 (illustrating the pitfalls of direct regulation due to limits on information and the broad range of organizational conduct).

> Any attempt at direct regulation of organizational conduct faces inherent limits on government information and administrative and enforcement resources, and suffers from inevitable lags, gaps and distortions in the development and application of legal controls in response to new problems and social needs. Furthermore, the conduct of organizations may be too far ranging and dynamic and the forces that generate organizational conduct too complex to be successfully contained by external controls.

Id. at 127–28.

[118] *See* Teubner, *supra* note 116, at 275 (defining reflexive law as a system that promotes internal controls over external regulation: "Reflexive law . . . will neither authoritatively determine the social functions of other subsystems nor regulate their input and output performances, but will foster mechanisms that systematically further the development of reflexion structures within other social subsystems.").

[119] On the shift from "direct outside intervention" to a more responsive and effective form of ecological regulation see Lindsay Farmer & Gunther Teubner, *Ecological Self-Organization*, *in* ENVIRONMENTAL LAW AND ECOLOGICAL RESPONSIBILITY: THE CONCEPT AND PRACTICE OF ECOLOGICAL SELF-ORGANIZATION 3 (Gunther Teubner, Lindsay Farmer & Declan Murphy eds., 1994) (noting that "externally induced, internal self-organization processes have come to be seen as the means of rendering organizations more sensitive to the demands of their environment.").

[120] *See* Teubner, *supra* note 116, at 278 (giving an example of how "constitutionalization" of corporate structures could lead to more effective internal controls).

[121] *See, e.g.*, Neil Gunningham et al., *Social License and Environmental Protection: Why Businesses Go Beyond Compliance*, 29 LAW & SOC. INQUIRY 307, 319 (2004) (stating that community pressures often lead pulp mills to go beyond the requirements of environmental regulation).

[122] *See* David L. Markell, *The Role of Deterrence-Based Enforcement in a "Reinvented" State/Federal Relationship: The Divide Between Theory and Reality*, 24 HARV. ENV'T L. REV. 1, 61–62 (2000) (discussing the National Environmental Performance Partnership System ("NEPPS") adopted by the EPA and the states); Sidney A. Shapiro & Randy Rabinowitz, *Voluntary Regulatory Compliance in Theory and Practice: The Case of OSHA*, 52 ADMIN. L. REV. 97, 155 (2000) (stating that deterrence-based enforcement will still have role in regulatory policy regardless of the extent voluntary compliance).

difficult to induce companies to cooperate in good faith and self-detect and report any breaches of environmental law;[123] on the contrary, they only fear the imposition of sanctions by public authorities, or otherwise negative responses from stakeholders and the general public.[124]

At any rate, there is no doubt technological change makes it possible, as a matter of principle, to also improve self-monitoring carried out by regulated entities. It is sufficient to consider the potential of continuous air emissions monitoring systems, or so-called "fenceline monitoring," which involves the strategic placement of monitoring equipment in areas in which facilities have been built or in surrounding areas, to detect and identify pollutant releases and any fugitive emissions.[125] On the other hand, the almost complete automation of many reporting processes has considerably reduced the risk of false or inaccurate declarations.[126]

However, technological development has not eliminated the ongoing need for checks by public agencies of the formal correctness and accuracy of the data presented by businesses (or, along the same lines, automatic data transmission systems, to ensure they have not been

[123] Cary Cognianese et al., *Seeking Truth for Power: Informational Strategy and Regulatory Policymaking*, 89 MINN. L. REV. 287–88 (2004).

[124] *See, e.g.*, Cognianese et al, *supra* note 123, at 278–79 (noting that unless it is required to do so, industry will have little incentive to reveal information concerning levels of compliance). However, programs seeking to incentivize self-monitoring have been operated for some time in a number of countries. For example, in the U.S. as early as 1995 the EPA adopted the so-called "Federal Audit Policy" (formally known as "Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations"), which provides for corresponding reductions in or exemptions from the applicable sanctions for any regulated entities that discover, voluntarily disclose, and correct any environmental violations. Incentives for Self-Policing: Discovery, Disclosure, Correction and Prevention of Violations, 65 Fed. Reg. 19,618 (Apr. 11, 2000). On May 15, 2018, EPA announced a renewed emphasis on encouraging regulated entities to voluntarily discover, promptly disclose, expeditiously correct, and take steps to prevent recurrence of environmental violations. *See Compliance: EPA's Audit Policy*, U.S. ENV'T PROTECTION AGENCY, https://perma.cc/T6L7-CC3H (last visited Oct. 8, 2020).

[125] *See* David A. Hindin & Jon D. Silberman, *Designing More Effective Rules and Permits*, 7 GEO. WASH. J. ENERGY & ENV'T L. 103, 116 (2016) (stressing that "regulators and sources are increasingly employing fenceline, remote, and ambient monitoring alongside, adjacent to, or further outside facility property lines."). *See also* Glicksman et al., *Technological Innovation*, *supra* note 78, at 73 (describing fenceline monitoring as required by some regulated entities and explaining EPA goals of fenceline monitoring).

[126] For example, in the U.S., the Acid Rain Program (ARP) implemented under the Clean Air Act Amendments of 1990 previously required larger businesses to equip themselves with continuous emissions monitoring systems that enabled specific measurements to be made of emissions over different periods of time, obliging them to transmit data directly to the EPA electronically at quarterly intervals. *See* Lesley K. McAllister, *Enforcing Cap-and-Trade: A Tale of Two Programs*, 2 SAN DIEGO J. CLIMATE & ENERGY L. 1, 4–7 (2010) (explaining ARP program and EPA's uses for the collected data).

interfered with).[127] Thus, environmental monitoring remains tied to a rigorously centralizing logic.[128]

However, the problem is that, within the context of a binary controller-controlled mechanism, instances of corruption, maladministration, or regulatory capture by the regulated entities themselves can always occur.[129] Thus, to give just one example, it is not infrequent to encounter in practice—especially at a local level—a form of blackmail by polluting businesses that are also particularly important in financial terms for a given area: in these cases, as is known, public authorities adopt a more tolerant approach to safeguard jobs and retain production facilities, so that the general public is represented by a body that does not faithfully defend their interests.[130]

The same problem arises, albeit on a more limited scale, where the data reported by regulated entities are verified by private third parties.[131] In fact, any certification work carried out by such bodies, even assuming they are genuinely independent, must be controlled by public agencies,[132] which, in turn, brings us back once again to the binary logic of the controller-controlled.

B. Environmental Monitoring in The Blockchain Age

Referring to the framework set out above, it is necessary at this juncture to consider what role blockchain technology can play and in what sense it can innovate traditional mechanisms for the monitoring and enforcement of environmental law, rendering them more effective to achieve an increased level of environmental protection.

This section therefore considers first how that technology interacts with the tendencies referred to above, which have gradually shifted the burden for collecting the data required for environmental monitoring to bodies different from environmental agencies. However, the blockchain is not a system for collecting data, but rather for recording them following validation by most nodes operating on the distributed ledger. In this sense, it enables the time of recording and formal completeness of the data to be verified in a manner referred to below as "dispersed," in

---

[127] *See* Giles, *supra* note 85, at 10208 ("And where government relies on self-reporting for compliance data, we also need ways to check for accuracy.").

[128] *Id.* at 10209.

[129] *See* Richard J. Lazarus, *The Tragedy of Distrust in the Implementation of Federal Environmental Law*, 54 LAW & CONTEMP. PROBS. 311, 316–17 (1991) (analyzing various instances of agency capture).

[130] *See, e.g.*, *id.* at 344 (providing an example of relaxed agency authority to enforce an environmental statute in response to concern over cost to industry).

[131] *See, e.g.*, *id.* (providing an example of industry control when EPA stops reviewing data).

[132] *Id.*

order to emphasize the fact that this process is carried out directly by the various subjects comprising the network.[133]

I shall then consider how the availability and full visibility (subject to the limits permitted under each legal system) of the data recorded on the blockchain is apparently capable of laying the groundwork for more effective substantive controls, while providing for the more effective enforcement of environmental law.

1. Towards a "Dispersed" Model of Environmental Data Verification

The mechanism described above for registering data that is typical of the blockchain could have significant consequences both on environmental monitoring and on compliance monitoring and the related self-monitoring practices by regulated entities.

As regards the former aspect, i.e. ambient monitoring, blockchain technology could enable the general public to verify the authorities have actually carried out checks into the state of certain natural resources as prescribed by law within the applicable time limits (and thus have not acted opportunistically). Consider, for example, data on levels of marine bacteria pollution, which in many countries must be provided at regular intervals by the competent authorities: their registration in a blockchain would make it possible to certify disclosure was formally complete and occurred on time, and thus avoid measurements being made exclusively during periods during which the sea is known to be less polluted (as occurs as a rule outside the bathing season or where there has been heavy rain).

As regards the latter aspect, i.e. compliance monitoring, the technology concerned would make it possible to certify regulated entities have complied with their statutory reporting obligations on time and in a formally correct manner. Consider the duty of a business to report certain data to the authorities about its own polluting emissions: before they can be registered on the blockchain, these data would have to be verified by the various computers from the network.[134] Specifically, these computers would have to certify, by majority, the business had complied at least formally with all requirements laid down by

[133] *See* Sinclar Davidson et al., *Economics of Blockchain* 15–18 (March 9, 2016) (unpublished manuscript), https://perma.cc/BXL5-KGKZ (arguing that blockchain technology, when combined together with already existing additional governance layers that are capable of regulating the interactions between people in a decentralized manner, is capable of enabling "massive open-source collaboration without any form of centralized coordination" and, regarding the aspect of particular interest here, is capable of implementing a system of distributed monitoring within which, "as opposed to the traditional model of governance based on *centralized monitoring*, where one central authority is in charge of monitoring and assessing the value of everyone else's action . . . [m]onitoring is achieved in a distributed manner, through collective action and peer-to-peer evaluation, thus incarnating the concept of *distributed monitoring* at the governance layer, and in addition to the distributed consensus algorithm that is found at the blockchain infrastructure layer.").

[134] Steve Cheng et al., *Using Blockchain to Improve Data Management in the Public Sector*, MCKINSEY (Feb. 28, 2017), https://perma.cc/HLE9-NC24.

environmental law (inserting all types of data and the documentation requested). Inclusion "on chain" would then constitute evidence the data that had been provided before the applicable time limit.[135] In this regard, the blockchain would thus make it possible to also verify that data relating to certain pollutants actually relate to a very specific period of time. This would be particularly useful where environmental law lays down a limit on emissions over a given period of time (such as a permit authorizing the emission of a certain quantity of polluting gas every hour). Under a scenario of this type, it is essential the businesses not only comply promptly and in full with the reporting obligations imposed upon them by law, but also that they be able to prove the sequence and distribution over time of their emissions in an incontrovertible manner.

In these cases an "initial push" would be required from the regulator, which should provide for the mandatory usage of the blockchain to record data relating to the environment, according to a classic command-and-control model.[136] However, it is clear a business called upon to engage constantly with a transparent IT system, which is thus potentially under the control of many operators (public administrations and 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 is because it would be aware effective compliance (at least) with the formal requirements of environmental law promptly would be subject to continuous, dispersed controls. As a result, it would know 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 environmental law would 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 or an 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 non-compliance 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 under environmental law.

On the other hand, any business would itself know that, since any negative environmental performance (even only in terms of a breach of

[135] *See id.* (explaining that once blocks are collected in a chain, they are verified by automation and shared governance protocols within the network). Part of the verification process, in this context, could be certifying that the data was submitted in accordance with appropriate deadlines.

[136] *See* Coglianese et al., *supra* note 123, at 278–79 (noting that unless it is required to do so, industry will have little incentive to reveal information concerning levels of compliance).

formal reporting obligations or failing to comply on time) would also be immediately visible to the general public, that outcome could have a significant adverse impact on its reputation and on consumer choices, given the heightened environmental sensitivity of consumers. As a result, it might act to be more compliant with regulatory requirements precisely to better respond to the social needs and expectations of consumers.[137] In this sense, blockchain technology could operate like a market-based tool. In particular, it could operate like eco-labels as instruments enabling consumers to assess correct environmental compliance, acting as a guide to their choices. Within this perspective, it is even conceivable full compliance with particular environmental requirements as certified by the blockchain system could operate as environmental certification, albeit limited to formal aspects. In other words, a prerequisite for the receipt and maintenance of particular environmental certifications would be full and timely compliance with reporting obligations as documented by the blockchain system.

This would resolve one of the principal limits to environmental certification, that is the fact 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 often chooses its own certifying body), are unreliable and also do not operate in a transparent manner.[138] On the contrary, the blockchain would give rise to a system of environmental certification also managed and controlled by the public, and it is thus likely it would be perceived by the public—or by those members of the public who are more sensitive to environmental issues—as more secure and more reliable.

Thus, the unprecedented collective and dispersed scrutiny achieved by the blockchain, at least in terms of the timeliness and formal regularity of environmental reporting, appears to open up new horizons for several available environmental protection mechanisms, whether based on the command-and-control model or on market mechanisms.

---

[137] Furthermore, recent studies support the view that the adoption of more restrictive environmental practices can increase the competitiveness of and innovation by the most productive and technologically advanced businesses over the medium term. *See* SILVIA ALBRIZIO ET AL., DO ENVIRONMENTAL POLICIES MATTER FOR PRODUCTIVITY GROWTH? INSIGHTS FROM NEW CROSS-COUNTRY MEASURES OF ENVIRONMENTAL POLICIES 29 (Org. for Econ. Coop. and Dev., Working Paper No. 1176 2014) ("Industry-based evidence shows that the gain in productivity growth from a tightening in environmental stringency is highest for the most productive industries" and these positive effects are "likely to be reinforced by their technological advancement."). *See also* Michael E. Porter & Claas van der Linde, *Green and Competitive: Ending the Stalemate*, HARV. BUS. REV., Sept.–Oct. 1995, at 120 ("Properly designed environmental standards can trigger innovations that lower the total cost of a product or improve its value.").

[138] *See* Lesley K. McAllister, *Regulation by Third-Party Verification*, 53 B.C. L. REV. 1, 33–34 (2012) (describing the challenges inherent to holding third-party verifiers accountable for the lack of transparency that is common with any privatized regulatory scheme); Hindin & Silberman, *supra* note 125, at 115 (asserting that one of the most critical design challenges of third-party verification programs is assuring that the verifiers are truly independent from their clients so as to avoid conflict of interest).

2. Towards the Dispersed Monitoring also of Data Accuracy and the Increased Responsibility of all Parties Involved

This Article mentioned above the controls permitted by blockchain technology essentially involve a verification as to whether data have been recorded on time and in full. However, it is not any less important for this reason. In fact, 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 to request public authorities to carry out substantive checks as to their accuracy.[139] A further development could occur were powers of analysis, including substantive analysis, are granted to private persons. For example, environmental associations could send their own technicians to make measurements "in the field" where the blockchain system suggested any anomalies or any gaps in presented documentation. In addition, environmental associations already measure the status of certain natural resources and provide the results to the general public.[140]

But the automatic and immediate control mechanism described above could be enhanced by introducing automated data processing, which would also enable the plausibility of certain information registered on it to be ascertained.[141] Again, to further enhance the dispersed verification of environmental data, it is possible to envisage systems that immediately report any apparently situations that appear to be anomalous on either a formal or a substantive level.[142] Consider a situation in which a business has published on time data relating to its own emissions, which are however incomplete or report a breach of one or more limits. However, the incomplete nature of the data and the breaches should not only be theoretically visible but should also be clarified to the general public and society at large by dedicated alerts.

To ensure the system is efficient, individuals should be put in a position to verify their reports or any automatic alerts have actually been acted upon by the public administration, and what the results are (e.g., the legislator could require the authorities to publish a final report within a specified time limit that takes account of the problems identified and the choices made).

This aspect raises a further issue of particular significance: given the natural dynamism within environmental situations,[143] a database

---

139 *See infra* Part III.B.1.

140 *See, e.g.*, NATURE CONSERVANCY, *California Natural Flows Database*, https://perma.cc/LMD4-W7H6 (last visited Nov. 4, 2020) (estimating natural flows in California rivers and streams using data from the United States Geological Survey).

141 *See, e.g.*, OPENGATE SOFTWARE, *What is Microsoft Access Used For?*, https://perma.cc/2CE6-2QA7 (last visited Nov. 4, 2020) (providing benefits to using Access as an example of an online database).

142 *Id.*

143 *See* Eric Biber, *The Problem of Environmental Monitoring*, 83 U. COLO. L. REV. 1, 22 (2011).

that states with certainty when particular environmental data were obtained and how complete they are would put the public authorities in a position to act promptly if any anomalies or inconsistencies occur. Similarly, any omissions, inefficiencies, or delays in acting would also be immediately visible and could be documented by any individual. Blockchain technology would thus enable a fuller implementation of the prevention principle, which requires the public authorities to take action to protect the environment at an early stage and before any damage occurs. However, the formal and undisputed provision of data establishes not only the possibility but also a duty for them to act in situations involving a danger for the environment. This has obvious consequences in terms of the (political, but also legal) responsibility of any authorities that fail to act promptly, causing further damage to the environment.[144]

However, despite the above, there is no doubt the implementation of a system of wide-scale scrutiny such as that described above would have significant consequences for the enforcement of environmental law. Accordingly, depending upon the legal system, the enhanced capacity to identify anomalies or breaches could enable a more effective system of private enforcement, understood in a narrow sense, or as an opportunity for private individuals, generally organized into associations,[145] to take court action to enforce compliance with environmental law by regulated entities, either instead of or in addition to any action taken by public bodies. This is provided for under "citizen suits" rules in the United

[144] In fact, the inclusion of data in the blockchain incontrovertibly confirms the information available to the authorities at any given past moment in time. The existence of positive obligations on the state to protect the environment has often been made apparent within the case law of the European Court of Human Rights, which has inferred a duty to protect the environment from Article 8 of the European Convention on Human Rights (ECHR), which enshrines the right to privacy and family life. See, most recently, *Cordella et al. v. Italy*, Eur. Ct. H.R. App. No. 54414/13, 161–74 (2019) (concerning extremely serious damage to the environment and the health of local residents caused by the ILVA steelworks in Taranto in southern Italy). To read the ECHR Press Release in English, issued by the Registrar of the Court, see Press Release, European Court of Human Rights, Registrar of the Court (Jan. 24, 2019) (discussing the case of *Cordella et al. v. Italy*).

[145] The Aarhus Convention in particular enhanced the role of environmental associations by vesting them with standing—subject to the sole prerequisite of recognition as such within the various national legal systems—without any requirement to assert and prove a specific interest. *See* Aarhus Convention, *supra* note 72, art. 2(5) which, in defining the concepts underlying that international treaty, states that, "'The public concerned' means the public affected or likely to be affected by, or having an interest in, the environmental decision-making; for the purpose of this definition, non-governmental organizations promoting environmental protection and meeting any requirements under national law shall be deemed to have an interest." Conversely, in the United States, environmental associations can sue on behalf of their members if their members would themselves have standing. In *Hunt v. Washington State Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977), the Supreme Court stated that an association has "representational standing" when: "(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit."

States, which authorize "any person" (provided that the plaintiff satisfies standing requirements) to sue polluters allegedly acting in violation of statutory requirements.[146]

It could also enable mechanisms for the reporting of environmental problems to public agencies to be better used in support of traditional public enforcement, increasing the likelihood that any breaches can be identified and prevented, thus representing a greater deterrent for prospective polluters.[147] In other words, it could enhance what has been defined as the capacity of the general public to act as "fire alarms."[148] This is significant within systems in which the efficacy of reports of this type is enhanced by a duty for the public authorities to respond. This occurs for instance under European Directive 2004/35 on environmental liability, which provides an administrative or judicial right of action by the public authorities to obtain an order preventing environmental damage construed as a "diffuse" interest, along with an award of compensation.[149] According to that mechanism, private persons can only

---

[146] The first citizen suit provision appeared in section 304 of the Clean Air Act, 42 U.S.C. § 7604 (2012), allowing for enforcement against violations of "an emission standard or limitation" or "an order issued by the Administrator or a State with respect to such a standard or limitation." A similar provision has subsequently been incorporated into almost all federal environmental statutes adopted in the United States since the 1970s. *See, e.g.*, Jeffrey G. Miller, *Private Enforcement of Federal Pollution Control Laws, Part I*, 13 ENV'T L. REP. 10309, 10309–10 (1983) ("Every federal environmental statute enacted since 1970, except FIFRA, has included a citizen suit provision, and each provision has been modeled on § 304."). The various federal environmental statutes provide in general that the plaintiffs cannot commence any action prior to sixty days after having given notice of the violation to the relevant federal agency, the relevant state and the alleged violator of the standard, limitation, or order. The purpose of such notice is primarily to enable the public authorities to commence and diligently prosecute a civil action in court to require compliance with the environmental statute. *See* Barry Boyer & Errol Meidinger, *Privatizing Regulatory Enforcement: A Preliminary Assessment of Citizen Suits Under Federal Environmental Laws*, 34 BUFF. L. REV. 833, 835 (1985) (stressing that in cases in which citizen suits are brought, private litigants "step into the shoes of government enforcement staffs" on the assumption that the latter are, for whatever reason, unable or unwilling to enforce environmental law).

[147] *See* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 207 (1968) (providing an economic analysis to assist in the creation of public and private policies to help prevent crimes, using decision variables such as the probability an offense is discovered).

[148] David L. Markell & Robert L. Glicksman, *Dynamic Governance in Theory and Application, Part I*, 58 ARIZ. L. REV. 563, 625 (2016) (noting that "[j]ust as a citizen pulls a fire alarm to alert the fire department of the need for help, a citizen provides information to notify the government of the need for attention"). *See also* Yvonne Scannell, *Public Participation in Environmental Decision-Making in Ireland: The Good, the Bad and the Ugly*, *in* ENVIRONMENTAL DEMOCRACY AND LAW: PUBLIC PARTICIPATION IN EUROPE 193 (Gyula Bándi ed., 2014) (providing a thorough analysis of the relationships between access to information and public participation in the enforcement of environmental law).

[149] Directive 2004/35, of the European Parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage, 2004 O.J. (L 143) 56, 63–64 (stating that "[n]atural or legal persons: (a) affected or likely to be affected by environmental damage or (b) having a sufficient interest in environmental decision making relating to the damage or, alternatively, (c) alleging the im-

call for such an action to be brought by the public authorities (i.e., they cannot launch it directly themselves), but may seek judicial review of any refusal to bring or delay in initiating such an action.[150]

Finally, incontrovertible evidence that certain environmental data were available at a precise moment could serve as a basis for damages actions against public authorities due to any failure on their part to act.

IV. Blockchain Technology and Environmental Transparency

In the light of the characteristics described above, this Part examines the potential of blockchain technology to enhance the transparency and reliability of information relating to the environment. In doing so, this Part will first discuss how, at least since the start of the 1980s, information and communications technology (ICT), in particular the use of electronic databases, has provided the opportunity to manage more efficiently and to disseminate an enormous quantity of data relating to the environment held by the public authorities.[151] This Part will then show how these very same technologies have facilitated the "disclosure" by regulated entities of data relating to their environmental performance.

The purpose is not to offer a complete framework of developments in relation to these issues, but only to present some of the most significant experiences along with their limits, to clarify the context within which the blockchain operates. On this basis, the following paragraphs explain how that technology achieves an innovative system of "notarized transparency" in which private individuals are no longer simple passive recipients certain, disclosed information about the environment, but cooperate actively with the public authorities in creating public databases, these databases thereby become increasingly

pairment of a right, where administrative procedural law of a Member State requires this as a precondition, shall be entitled to submit to the competent authority any observations relating to instances of environmental damage or an imminent threat of such damage of which they are aware and shall be entitled to request the competent authority to take action under this Directive . . . . The request for action shall be accompanied by the relevant information and data supporting the observations submitted in relation to the environmental damage in question. Where the request for action and the accompanying observations show in a plausible manner that environmental damage exists, the competent authority shall consider any such observation and requests for action. . . . The competent authority shall, as soon as possible and in any case in accordance with the relevant provisions of national law, inform the persons referred to in paragraph 1, which submitted observations to the authority, of its decision to accede to or refuse the request for action. . . .").

[150] *Id.*

[151] Joshua Knauer & Maurice Rickard, *Internet Global Environmental Information Sharing*, *in* Information Systems and the Environment 185, 191–92 (Deanna J. Richards et al. eds., 2001) (discussing the efficacy of the EnviroLink Network, a global electronic database which collects and disseminates environmental information submitted by individuals, businesses and groups around the world).

reliable as they ensure the environmental information within them is registered both on time and in full.

A. Environmental Transparency in The Information Age: The Role of Public Databases

According to various legislative instruments adopted at both national and international levels, most environmental information held by public authorities should be incorporated into public electronic databases.[152] This infrastructure is essential to ensure effective transparency in relation to environmental matters.[153]

Thus, as early as 1998, the Aarhus Convention (Convention) mentioned "the importance of making use of the media and electronic or other, future communications,"[154] stressing the need for each signatory to "ensure that environmental information progressively becomes available in electronic databases which are easily accessible to the public through public telecommunications networks."[155] In this way, the Convention identified ICTs as the technical instrument necessary to complete the passage from access upon request to full transparency, understood as the proactive disclosure of environmental information to the public, in keeping with the guiding principle of the Convention that "public authorities hold environmental information in the public interest."[156] Within this perspective, the Convention provides, for example, that public authorities must "disseminate, on their own initiative and without a corresponding request from the public" a broad range of information relating to the environment, including reports, plans, monitoring results, and other materials.[157]

The European Commission gave effect to the Aarhus Convention by adopting Directive 2003/4/EC on public access to environmental information, which stresses the need for public authorities "to make all reasonable efforts to maintain the environmental information held by or for them in forms or formats readily reproducible and accessible by electronic means," as well as to "make available and disseminate

---

152 Aarhus Convention, *supra* note 72; Directive 2003/4, of the European Parliament and of the Council of 28 January 2003 on Public Access to Environmental Information and Repealing Council Directive 90/313/EEC, 2003 O.J. (L 41) 26, 30 (EC); *see* Electronic Freedom of Information Act Amendments of 1996, Pub. L. No. 104-31, 110 Stat. 3048, 3049 (codified as amended at 5 U.S.C. § 552 (2016)) (noting that government agencies hold valuable records and information and should utilize electronic telecommunications and other new technology to enhance public access to such records).

153 *See* Aarhus Convention, *supra* note 72, Rec. 10–12 (discussing that the Aarhus Convention was inspired by the need for further accountability and transparency within all branches of government by allowing the parties to participate in decision-making and have expanded access to information on environmental matters).

154 *Id.*

155 *Id.*

156 *Id.* art. 5.

157 Ludwig Krämer, *Transnational Access to Environmental Information*, 1 TRANSNAT'L ENV'T L. 95, 101 (2012).

information on the environment . . . by means of computer telecommunication and/or electronic technology," with a view to increasing "public awareness in environmental matters and to improv[ing] environmental protection."[158]

In the United States, the Freedom of Information Act (FOIA) of 1966, which provides access to information and transparency of information, including environmental information, held by federal agencies,[159] has been amended twice to bring it into line with the changes brought about by developments in ICT.[160] The first change came in 1996 with the Electronic Freedom of Information Act Amendment, which broadened the categories of records that the public agencies must provide without delay for immediate access on their website (or in the relevant agency's electronic reading room).[161] The law also sought to simplify access upon request, speeding up the provision of records.[162]

Subsequently, the FOIA Improvement Act of 2016 further enhanced government transparency by making proactive disclosure the general

---

158 Directive 2003/4, of the European Parliament and of the Council of 28 January 2003 on Public Access to Environmental Information and Repealing Council Directive 90/313 /EEC, 2003 O.J. (L 41) 26, 27 (EC) (implementing the first pillar of the Aahrus Convention on access to environmental information). *See also* Directive 2007/2, of the European Parliament and of the Council of 14 March 2007 Establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), 2007 O.J. (L 108) 1 (EC) (aiming to create a spatial data infrastructure to enable the sharing of environmental spatial information across Europe).

159 For instance, the information held by the EPA. On the other hand, FOIA does not apply to state government agencies that have their own freedom of information laws (the same applies for the District of Columbia). For an overview and links with each state freedom of information law, see *State Law Resources*, NAT'L FREEDOM INFO. COAL., https://perma.cc/4FZM-AZTM (2020) (providing a link to a page with each state's freedom of information law and a link to a page with an overview of each state's freedom of information law).

160 Freedom of Information Act of 1966, Pub. L. No. 89-487, 80 Stat. 250 (codified as amended at 5 U.S.C. § 552 (2016)). More generally, the FOIA has been amended several times over the years as a consequence of social or legal change, as well as technological changes. For a detailed discussion of the various changes, see *FOIA Legislative History*, NAT'L SECURITY ARCHIVE, https://perma.cc/UB7X-JRE9 (last visited Sept. 19, 2020) (explaining the changes made to FOIA through seven amendments).

161 Electronic Freedom of Information Act Amendments of 1996, Pub. L. No. 104–231, 110 Stat. 3048 (codified as amended at 5 U.S.C. § 552 (2016)). *See, e.g.*, Senator Patrick Leahy, *The Electronic FOIA Amendments of 1996: Reformatting the FOIA for On-Line Access*, 50 ADMIN. L. REV. 339, 341 (1998) (explaining how agencies have established websites and electronic reading rooms to comply with the Electronic FOIA Amendments of 1996); Michael E. Tankersley, *How the Electronic Freedom of Information Act Amendments of 1996 Update Public Access for the Information Age*, 50 ADMIN. L. REV. 421, 426–30 (1998) (providing a detailed explanation of the different provisions of the 1996 Amendment and noting that all of them were "driven and inspired by the pervasive growth in the use of computers").

162 *But see* Tankersley, *supra* note 161, at 423 (noting that the provisions in the 1996 Amendments "seek to address the most pervasive problem with FOIA, namely the chronic delays in the processing of individual FOIA requests. . . . [but] offer little that is new, and fail to provide any additional resources or enforcement mechanism to cure the delays").

rule unless "the agency reasonably foresees that disclosure would harm an interest protected by an exemption" or "disclosure is prohibited by law."[163] Within this perspective, the Act, for example, obligated federal agencies to make their disclosable records and documents, as well as records requested on three or more occasions (known as "frequently asked records"), available for public inspection in an electronic format.[164]

However, the law on the statute books is one thing, while the law in action is another. It is no secret public authorities are still often reluctant to publish certain environmental information due to political, electoral, or other considerations.[165] Thus, databases are rarely created or are not created quickly enough. This may also be due to a scarcity of resources and staff at the administrations, or simply the normal time-frame necessary to collect data, and thereafter to check it and record it in public registers.[166]

And yet, the value of environmental data is often inversely proportional to its age. For example, it makes little sense to know about the quality of marine water several weeks after the start of the bathing season if bathers have already gone on holiday to the location in question. Similarly, the timely provision of data is of fundamental significance for ensuring effective cross-checks on compliance with emissions and pollution limits (consider the checks carried out by public agencies on regulated entities, but also NGOs and the general public on both regulated entities and public agencies).

Second, the enormous quantity of data generated by modern society (termed "big data") is rendering increasingly critical the issue of how to store and manage that constantly increasing volume of information over the long term, while guaranteeing security and ease of access.[167] From

---

[163] FOIA Improvement Act of 2016, Pub. L. No. 114-185, sec. 2, § 552(a)(2), 130 Stat. 538, 539 (codified as amended at 5 U.S.C. § 552 (2016)).

[164] *Id.* sec. 2, § 552(a)(2), 130 Stat. at 538 (providing for the agency's proactive disclosure in an electronic form of copies of all records, regardless of form or format—"(i) that have been released to any person under paragraph (3)"; and "(ii) (I) that because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records"; or "(II) that have been requested 3 or more times"). For a summary of the Act's changes, prepared by the U.S. Department of Justice's Office of Information Policy, see *OIP Summary of the FOIA Improvement Act of 2016*, U.S. DEP'T JUST. (Aug. 17, 2016), https://perma.cc/PQ3A-3P2C.

[165] *See* Krämer, *supra* note 157, at 101 (noting that this tendency also persists in a number of countries that have ratified the Aarhus Convention); Peter H. Sand, *The Right to Know: Freedom of Environmental Information in Comparative and International Law*, 20 TUL. J. INT'L & COMP. L. 203, 203 (2011) (noting that since access to knowledge is about access to power, denial of access is often "the standard reaction of knowledge-holders," whether regulated entities or regulators).

[166] Melanie Dulong de Rosnay & Katleen Janssen, *Legal and Institutional Challenges for Opening Data Across Public Sectors: Towards Common Policy Solutions*, J. THEORETICAL & APPLIED ELEC. COM. RES., Sept. 2014, at 1, 3–9.

[167] Martin Strohbach et al., *Big Data Storage*, *in* NEW HORIZONS FOR A DATA-DRIVEN ECONOMY: A ROADMAP FOR USAGE AND EXPLOITATION OF BIG DATA IN EUROPE 119, 119–22, 127 (José María Cavanillas et al. eds., 2016).

this perspective, ICTs have in some sense exacerbated the problem in that, while they do admittedly make it easier for environmental information held by public authorities to be accessed, they give rise to even greater expectations by the public at large and industry that increasingly complete, understandable, and accurate information will be disseminated in real time. This means it is necessary to identify new and potentially more efficient arrangements for the management of this type of data.

Third, experience shows that, even where an electronic database is created, it does not itself offer any guarantee the information in it will be clear and accessible.[168] Even today, public databases are often incomplete, websites are outdated and links to various types of document are frequently invalid.[169] In other cases, where the massive volume of information is organized in a sub-optimal manner[170] or has not been adequately harmonized[171] it is difficult to consult.

It is sufficient to cite the affair of the Enforcement and Compliance History Online (ECHO) website in the United States, which was established by the EPA Office of Enforcement and Compliance Assurance in 2002, to provide integrated compliance and enforcement information for a wide number of regulated facilities.[172] During the first few years of its life, large numbers of regulated entities complained about the difficulties in searching data, low levels of accuracy and completeness, as well as the excessive amount of information which proved to be overwhelming for members of the general public without specific expertise in environmental matters.[173] The problem was

168 *See generally* Taryn L. Rucinski, *An Environmental Legal Practitioner's Guide to EPA's Website*, 42 ENV'T L. REP. 10416 (2012) (stressing the difficulty in searching for information posted on the EPA's website).

169 Sarah Lamdan, *Beyond FOIA: Improving Access to Environmental Information in the United States*, 29 GEO. ENV'T L. REV. 481, 492–93 (2017).

170 *See id.* at 492–95 (providing an overview of the difficulties in navigating between the different electronic sources of environmental information in the United States).

171 For an example of legislation seeking to harmonize the environmental data held by public agencies, see Directive 2007/2/EC, of the European Parliament and of the Council of 14 March 2007, establishing an Infrastructure for Spatial Information in the European Community (INSPIRE), 2007 O.J. (L 108) 1, 1 ("The problems regarding the availability, quality, organisation, accessibility and sharing of spatial information are common to a large number of policy and information themes and are experienced across the various levels of public authority. Solving these problems requires measures that address exchange, sharing, access. . . . An infrastructure for spatial information in the Community should therefore be established.").

172 *What's New*, U.S. ENV'T PROTECTION AGENCY: ENF'T & COMPLIANCE HIST. ONLINE, https://perma.cc/NA7X-PCGT (last updated Aug. 2020).

173 *Known Data Problems*, U.S. ENV'T PROTECTION AGENCY: ENF'T & COMPLIANCE HIST. ONLINE, https://perma.cc/YHZ5-PSLF (last updated Mar. 2020). For an account of the various problems that have affected the ECHO during the first few years following its implementation, see Clifford Rechtschaffen, *Enforcing the Clean Water Act in the Twenty-First Century: Harnessing the Power of the Public Spotlight*, 55 ALA. L. REV. 775, 802 (2004) (summarizing complaints about ECHO's website being hard to access); Lynn L. Bergeson,

partially resolved in subsequent years, although as late as 2016, the U.S. Inspector General published a report objecting, as it relates to control of major Clean Air Act facilities, that "inaccurate data hinder EPA oversight and public awareness."[174]

B. Disclosure-Based Regulation in the Information Age

Numerous provisions now require the mandatory disclosure of environmental information by regulated entities,[175] and there is a broad awareness that they are essential for effective environmental regulation. These practices fall within the broader context of "informational regulation," i.e. the regulatory strategy falling under the "third wave" within the evolution of pollution control policies, and operate alongside more conventional command-and-control and market-based approaches.[176] The idea underlying informational regulation is that, thanks to the pressure brought to bear by the market and public opinion, greater transparency regarding the environmental performance of regulated entities can promote more responsible behavior by them.[177]

ECHO: Enforcement Online, Up Close, and Real Personal, ENV'T QUALITY MGMT., Summer 2003, at 81, 81–83 (describing the evolution of ECHO and its main benefits and risks).

174 U.S. ENV'T PROT. AGENCY, REP. NO. 16-P-0164, CLEAN AIR ACT FACILITY EVALUATIONS ARE CONDUCTED, BUT INACCURATE DATA HINDER EPA OVERSIGHT AND PUBLIC AWARENESS (2016).

175 *See* Rónán Kennedy, *Rethinking Reflexive Law for the Information Age: Hybrid and Flexible Regulation by Disclosure*, 7 GEO. WASH. U. J. ENERGY & ENV'T L. 124, 124 (2016) (discussing how disclosure-based regulation has been, and is, a "significant feature" of environmental regulation of entities).

176 For examples in the legal scholarship, see generally *id.* at pt. I and II (discussing information regulation and offering a critique of "third generation" tools); Douglas A. Kysar & James Salzman, *Foreword: Making Sense of Information for Environmental Protection*, 86 TEX. L. REV. 1347, 1352 (2008) ("[A]gencies must depend on their own modeling or experimentation, on existing academic work, or on entirely new work that the agencies sponsor or support as sources of needed information, rather than leverage legal authority to require private actors to generate that information for them."); David W. Case, *The Law and Economics of Environmental Information as Regulation*, 31 ENV'T L. REP. 10773 (2001) (reviewing the legal and economic scholarly literature on informational regulation in the environmental arena); Bradley C. Karkkainen, *Information as Environmental Regulation: TRI and Performance Benchmarking, Precursor to a New Paradigm?*, 89 GEO. L.J. 257, 262 (2001) (stating that EPA's Toxic Release Inventory database is limited by the incompleteness and unreliability of its data, therefore impacting performance standards of facilities); Christopher H. Schroeder, *Third Way Environmentalism*, 48 U. KAN. L. REV. 801 (2000); Paul R. Kleindorfer & Eric W. Orts, *Informational Regulation of Environmental Risks*, 18 RISK ANALYSIS 155 (1998) (discussing the two frameworks of law and economics as applied to information regulation); Cass R. Sunstein, *Informational Regulation and Informational Standing: Akins and Beyond*, 147 U. PA. L. REV. 613, 613 (1999). Within the economic literature, see Mark A. Cohen, *Information as a Policy Instrument in Protecting the Environment: What Have We Learned?*, 31 ENV'T L. REP. 10425 (2001); Tom Tietenberg, *Disclosure Strategies for Pollution Control*, 11 ENV'T & RESOURCE ECON. 587, 588 (1998); ANTHONY I. OGUS, REGULATION: LEGAL FORM AND ECONOMIC THEORY 121 (1994).

177 *See* David W. Case, *Corporate Environmental Reporting as Informational Regulation: A Law and Economics Perspective*, 76 U. COLO. L. REV. 379, 383 (2005) (arguing that "[t]he primary purpose of informational regulation is to enlist the aid of non-governmental

It is no coincidence mandatory disclosure practices fall within the ambit of "reflexive regulation."[178]

The usage of information disclosure as a regulatory tool was first facilitated and then particularly enhanced by the development and dissemination of ICT.[179] Thus, from the end of the 1980s and onward, several pollutant release and transfer registers were created, which imposed reporting obligations in relation to toxic emissions, accidents or hazardous substances.[180] The aim of these was to increase public awareness of the harm to health and environmental damage caused by industrial activities and also to assist the public authorities and regulated entities in identifying non-compliance.[181]

The most famous case is that involving the Toxic Release Inventory (TRI) in the U.S., established by the Emergency Planning and Community Right-to-Know Act (EPCRA) to inform citizens of releases of toxic chemical into their communities.[182] The Inventory is held by the EPA and contains information about releases of over 300 chemicals into the air, land, and water by certain particularly polluting industries.[183] The data can be accessed freely by the public, primarily over the internet.[184]

forces, particularly economic markets and public opinion, to either complement or substitute for traditional regulatory strategies of government standard setting and enforcement.").

178 *See* Daniel C. Esty, *Next Generation Environmental Law: A Response to Richard Stewart*, 29 CAP. U.L. REV., 183, 197 (2001) (noting that "[b]etter information also supports reflexive environmental law.").

179 For a general perspective, see Braden R. Allenby, *The Information Revolution and Sustainability: Mutually Reinforcing Dimensions of the Human Future*, *in* INFORMATION SYSTEMS AND THE ENVIRONMENT 15, 19 (Deanna J. Richards et al. eds., 2001) (noting the "fundamental coevolution of the Informational Revolution and sustainability.").

180 *TRI Around the World*, U.S. ENV'T PROTECTION AGENCY, https://perma.cc/YG4H-EWKU (last visited Sept. 17, 2020).

181 *See, e.g.*, Lamdan, *supra* note 169, 487–91 (2017); Rechtschaffen, *supra* note 173, at 795–804 (providing many examples of successful regulation on mandated disclosure of data).

182 42 U.S.C. § 11023 (1986). TRI was enhanced by the Pollution Prevention Act of 1990, requiring facilities to report additional data on waste management and source reduction activities. *What is the Toxic Release Inventory?*, U.S. ENV'T PROTECTION AGENCY, https://perma.cc/6ETL-YBJJ (last visited Sept. 16, 2020). *See* Gary D. Bass & Alair MacLean, *Enhancing the Public's Right-to-Know About Environmental Issues*, 4 VILL. ENV'T L.J. 287, 297, 299 (1993) (indicating how TRI can be useful aid to regulatory programs aimed at reducing pollution); Cass R. Sunstein, *Informing America: Risk, Disclosure, and the First Amendment*, 20 FLA. ST. U.L. REV. 653, 662–63 (1993).

183 *What is the Toxic Release Inventory?*, *supra* note 182.

184 *Id.* In 2013, the EPA adopted a final rule requiring facilities to report non-trade-secret TRI forms to the EPA using electronic software provided by the Agency with the aim of making it simpler for facilities to report accurate information by expediting form completion, while at the same time reducing the cost to EPA of processing forms and making the information available to the public more quickly. Electronic Reporting of Toxics Release Inventory Data, 78 Fed. Reg. 52,860 (Aug. 27, 2013) (to be codified at 40 C.F.R. pt. 372).

Drawing on experience with the TRI, and as called for in the Aarhus Convention,[185] the UNECE Protocol on Pollutant Release and Transfer Registers (PRTRs) was adopted in 2003.[186] As the first legally binding international instrument in this area, the Protocol obligates the parties "to establish nationwide systems that report and collect pollution information" with the aim of enhancing public access to information, facilitating public participation in environmental decision-making and contributing to the prevention and reduction of pollution of the environment.[187] More generally, there are mandatory disclosure programs in several countries, which enable up-to-date, standardized and site-specific data relating to emissions and releases into various environmental media to be downloaded freely.[188]

Although, sometimes, these instruments have effectively reduced damaging emissions to the environment; however, they too, are not without their weaknesses.[189] The mere provision of information does not guarantee it will also be up-to-date and formally complete.[190]

In reality, while the computerized systems currently available largely enable the problems of costs and late disclosure to be resolved, their centralized structure means public agencies are still the only

[185] *See* Aarhus Convention, *supra* note 72, at art. 5(9) (stating that "[e]ach Party shall take steps to establish progressively, taking into account international processes where appropriate, a coherent, nationwide system of pollution inventories or registers on a structured, computerized and publicly accessible database compiled through standardized reporting. Such a system may include inputs, releases and transfers of a specified range of substances and products, including water, energy and resource use, from a specified range of activities to environmental media and to on-site and off-site treatment and disposal sites.").

[186] *See* Protocol on Pollutant Release and Transfer Registers, May 21, 2003, 2626 UNTS 119, https://perma.cc/SW72-MEL9.

[187] *Id.* The Protocol was adopted during an extraordinary meeting of the Parties to the Aarhus Convention held in Kiev in May 2003, was signed by 36 Parties and entered into force on October 8, 2009. The European Community signed it on February 21, 2006. Following ratification, the European Community adopted the European PRTR (E-PRTR), which was published as Regulation (EC) No 166/2006/EC on February 4, 2006 and entered into force 20 days later (Regulation 166/2006 of the European Parliament and of the Council concerning the establishment of a European Pollutant Release and Transfer Register (E-PRTR) and amending Council Directives 91/689/EEC and 96/61/EC, art. 22, 2016 O.J. (L. 33), 1 (EC).

[188] *See, e.g.*, Clean Water Act, 33 U.S.C. § 1318(a) (2018) (requiring requires industries, municipalities and other facilities discharging to surface water to periodically submit to EPA Discharge Monitoring Reports (DMRs)). The relevant data are fed into a database managed by the EPA and can be freely consulted on the Enforcement and Compliance History Online ("ECHO") website referred to above. *About the Data*, U.S. ENV'T PROTECTION AGENCY, https://perma.cc/N7AK-TCF7 (last updated Sept. 2, 2020).

[189] *But see, e.g.*, ARCHON FUNG ET AL., FULL DISCLOSURE: THE PERILS AND PROMISE OF TRANSPARENCY 20–31 (2007) (reviewing the development of targeted transparency policies in the United States since mid-1980s); MARY GRAHAM, DEMOCRACY BY DISCLOSURE: THE RISE OF TECHNOPOPULISM 137–41 (2002); Wendy E. Wagner, *Commons Ignorance: The Failure of Environmental Law to Produce Needed Information on Health and the Environment*, 53 DUKE L.J. 1619, 1668–69 (2004).

[190] Kennedy, *supra* note 175, at 124.

genuine "guarantors" of timely and complete disclosure.[191] This means that, where the authorities are corrupt, inefficient or otherwise willing to tolerate delays or other omissions by regulated entities, it is extremely difficult for the general public to identify those shortcomings. Similarly, it is difficult for the authorities to establish whether there has been interference with any automated mechanisms for controlling and reporting delays or formally incomplete information.

While external public scrutiny of the IT systems hitherto used has been theoretically possible, it has been informal and unsystematic. This depends partly on the fact that individuals have "limited time, energy and attention."[192] On the other hand, the complex and highly time-consuming nature of that scrutiny, especially if conducted systematically, also reduces the efficacy of the controls that can be carried out, for instance by NGOs. All of this means that the potential inherent within effective external pressure is not always exploited to the full.[193]

While ICT might (and, depending on the legislation, should) allow for the wide-scale, comprehensive, and timely dissemination of a potentially enormous quantity of environmental information, which should be easily accessible from home computers with no particular cost, these technologies do not, however, alter the essentially "passive" role of the users of that information.[194] Specifically, although users can request the disclosure of certain data and documents subject to a statutory publication requirement, they are not, however, directly involved in creating databases, and in particular, do not have any opportunity to verify environmental information (in terms of either its completeness of its formal regularity) before it is registered.[195]

C. Transparency of Environmental Information in The Blockchain Age: From Mere Transparency to "Notarized Transparency"

Blockchain technology operates within the context described above, on the one hand enabling more effective management of the increasing

---

[191] So much so, as was apparent for example in the TRI case in the U.S., even where data have been disclosed by businesses, there is an expectation on the part of society as a whole that the data will be correct and that any anomalies, gaps or mistakes will end up undermining public trust in public agencies and the legitimacy of their actions. *See, e.g.*, CHARLES J. SHEEHAN, MANAGEMENT ALERT: CERTAIN TOXIC RELEASE INVENTORY DATA DISCLOSED TO THE PUBLIC ARE INACCURATE REPORT NO. 19-N-0115 (2019), https://perma.cc/L6UD-7FD8 (noting that the public was not receiving timely and complete information in an agency audit by the Acting Inspector General).

[192] Stewart, *A New Generation*, *supra* note 20, at 141.

[193] Karkkainen, *supra* note 176, at 262 ("[B]ecause external monitoring under TRI is informal and unsystematic, external pressures may not be applied vigorously or consistently across the full range of facilities and firms. And, for a variety of reasons, facilities and firms may not be equally responsive.").

[194] *See, e.g.*, U.S. ENV'T PROTECTION AGENCY, *supra* note 182 (providing free electronic access TRI data to citizens after it has been received and published by EPA).

[195] *Id.*

volume of environmental information held by the public authorities, while allowing private individuals, regulated entities, and stakeholders in general to play a direct role in creating public databases, which has significant consequences in terms of enhanced data reliability and security.

Starting with the issue of the management of the increasing volume of environmental information, it must be recalled first that the decentralized form of data registration typical of the blockchain has the potential to create a more efficient and safer system of environmental ledgers, moreover at a reduced cost.[196] That technology would eliminate the need to use huge databases for data storage, which for instance require costly maintenance and need to be updated constantly.[197] The decentralized structure of the database would also render it more secure, in terms of its resistance to external attacks, as there would no longer be any single point of failure (which is also the case, albeit to a lesser extent, within permissioned blockchains involving few participants defined in advance),[198] and in terms of resistance to interference. This resistance results essentially from the way data are registered in blocks along with cryptography that ensures that previously registered data cannot be altered without leaving a trace.[199] However, the system of distributed ledgers would be make it relatively easy to discover any such changes, as they would appear in every copy of the database stored in the nodes (and would be visible to the general public).[200] This would also be a highly effective tool in combating corruption and crime.

Second, the very structure of distributed ledgers, which can be updated in real time, would facilitate sharing (non-reserved) information, both between different public authorities and between public authorities, regulated entities and private individuals.[201] Thus, the perfect synchronization of all databases would enable public authorities to avoid having to collect the same data multiple times (known as the “once-only principle”), thus significantly reducing costs

---

[196] *See* 2018 JOINT ECON. REP., H.R. NO. 115-596, at 201, 212 (2018) (noting that decentralized blockchain technologies provide safe and efficient data storage across multiple platforms).

[197] Stacey Peterson, *What You Need to Know About Blockchain Storage*, TECH TARGET (Apr. 10, 2019), https://perma.cc/UY3G-BVNQ.

[198] *See* De Filippi & Wright, *Lex Cryptographia*, *supra* note 17, at 108 (noting that governmental information has thus far been stored in highly centralized databases that act like digital fortresses and are thus vulnerable, like all fortresses).

[199] *See* Bacon et al. I, *supra* note 33, at 12.

[200] *Id.* at 9–12 (explaining the aim of blockchain technology as a tamper-evident data chain where an external observer can spot any change).

[201] Svein Ølnes et al., *Blockchain In Governments: Benefits and Implications of Distributed Ledger Technology for Information Sharing*, 34 GOV’T INFO. Q., 2017, 355, 357; FINCK, *supra* note 24, at 120 (noting that “ [d]ata is largely non-rivalrous in nature, meaning that sharing data does not decrease its value, as the same data can be used for various purposes and applications”).

for society and the bureaucratic burden for individuals.[202] At the same time it would be extremely useful, for instance within complex administrative procedures (as environmental procedures typically are) involving multiple public and private parties. In these cases, where participants in the procedure are generally clearly identified or otherwise identifiable, network participants (NGOs, other public authorities with interests affected by the procedure, and private parties with a direct interest) could validate data, while the general public could nonetheless read the data in full and submit any reports or comments (e.g. by flagging them).[203]

Third, the ability to share the information in full should, at least in theory, reduce the information asymmetry between regulated entities on the one hand and the administration and the general public on the other, favoring greater involvement in public decision-making processes relating to the environment. From this viewpoint, blockchain technology would then make it easier to complete the shift, which is desirable in relation to environmental matters, from transparency of administrative action towards open government, or in other words, from the "citizens' vision" to the "citizens' voice,"[204] the latter construed as the active involvement of the general public in the management of environmental problems. The structure of that technology appears to be particularly well-suited to managing the complex nature of environmental issues, which is due *inter alia* to a heightened "fragmentation of knowledge," in the sense that no single actor, considered in isolation, holds all information necessary to ensure the optimum management of the issues.[205] It could open up new forms of interaction between the public

[202] *See* Distributed Ledger Technologies and Blockchains: Building Trust with Disintermediation, *supra* note 4, ¶ 47 (referring to "the efficiency potential of DLT for public services and management as regard reducing bureaucracy, especially with a view to enforcement of the eGovernment Action Plan, with particular reference to the EU-wide adoption of the digital Once-Only-Principle," i.e. the principle that collecting the same data multiple times is more expensive than sharing and reusing data already gathered).

[203] Full visibility of data would moreover be compatible with any requirements of confidentiality since, as mentioned above, it is possible secure data registered on chain by using encryption.

[204] On the concept of open government, see, e.g., Daniel Berliner et al., *The Future of FOIA in an Open Government World: Implications of the Open Government Agenda for Freedom of Information Policy and Implementation*, 63 VILL. L. REV. 867, 871 (2018) (offering a systematic framework for understanding the political consequences of the open government agenda for Freedom of Information policy and implementation); Jing Zhang, Luis F. Luna-Reyes, & Theresa A. Pardo, *Information, Policy, and Sustainability: The Role of Information Technology in the Age of Big Data and Open Government*, *in* 20 PUB. ADMIN. & INFO. TECH. 1, 7–8 (Christopher G. Reddick ed. 2016) (analyzing the phenomenon of open government from a perspective that is not limited to the environment, but that embraces public institutions in general); Albert J. Meijer et al., *Open Government: Connecting Vision and Voice*, 78 INT'L REV. ADMIN. SCI. 10, 12–15 (2012).

[205] *See* Ølnes et al., *supra* note 201, at 356 (discussing the *Byzantine generals' problem* as it relates to *Distributed Ledger Technology* (DLT)).

administration, regulated entities, and private individuals to achieve more flexible, "reflexive," and "decentred" regulation.[206]

It is important to stress the blockchain would not alter the rules on access to environmental data, as governed under the various legal systems. Thus, to give an example, this technology would not impinge upon the provisions that restrict access to environmental information in both the U.S. and the E.U. in situations involving confidential business information.[207] If anything, that technology would affect the circulation of environmental information the disclosure of which is already permitted, thus giving effect to the rules on the transparency of environmental information.

Besides, the technology under examination would make it possible to involve interested parties directly in registering environmental data and thus in verifying it has been filed on time and is complete. Compared to the IT systems currently used, within the blockchain it would thus be the network participants that certified these operations, by majority, before the data can be inserted "on chain" as a new block. A centralized control by a public body, potentially followed by an ex post control by social operators and NGOs of data previously entered, would thus be replaced by a mechanism providing for the multi-nodal certification of data before its registration.

206 *See* Julia Black, *Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in A 'Post-Regulatory' World*, 54 CURRENT LEGAL PROBS. 103, 112 (2001) ("'Decentred regulation' thus involves a move away from an understanding of regulation which assumes that governments have a monopoly on the exercise of power and control, that they occupy a position from which they can oversee the actions of others, and that those actions will be altered pursuant to government's demand . . . Essentially, decentred regulation involves a shift (and recognition of such a shift) in the locus of the activity of 'regulating' from the state to other, multiple, locations, and the adoption on the part of the state of particular strategies of regulation.").

207 *See* Freedom of Information Act, 5 U.S.C. § 552(c)(4) (protecting "trade secrets and commercial or financial information obtained from a person and privileged or confidential" in the U.S.). As a result, "reverse" FOIA lawsuits allow the submitter of confidential business information to prevent the agency that collected the information from revealing it when requested by a third party. *See FOIA Guide, 2004 Edition: "Reverse" FOIA*, U.S. DEP'T JUST. (July 24, 2014), https://perma.cc/2VQ7-ZPDP (describing the reverse FOIA process and significant case law). Similarly, Article 4(4)(d) of the Aarhus Convention, *supra* note 72, provides that public authorities may refuse a request for environmental information if the disclosure would adversely affect "[t]he confidentiality of commercial and industrial information, where such confidentiality is protected by law in order to protect a legitimate economic interest." However, the provision also states that, "[w]ithin this framework, information on emissions which is relevant for the protection of the environment shall be disclosed" and more generally that all exceptions to access "shall be interpreted in a restrictive way, taking into account the public interest served by disclosure and taking into account whether the information requested relates to emissions into the environment." It should be pointed out that the European Court of Justice tends to interpret exclusively the concept of "emissions," and has on the other hand clarified on various occasions that exceptions to the principle of the broadest access possible to environmental information must be construed and applied narrowly. *See, e.g.*, Case C-673/13, Comm'n v. Stichting Greenpeace Neth. and Pesticide Action Network Eur., ECLI:EU:c:2016:213, ¶¶ 26–41 (Apr. 7, 2016).

This implies the data registered on the blockchain are secure at birth, so to speak, as they are checked before inclusion by network participants (which could be significant in number) rather than by an official responsible for their inclusion in an electronic register (or rather than by a single computer operated centrally by the public authority alone).[208] This mechanism would make it possible first to eliminate or reduce the risk of corruption or the regulatory capture of the public body by regulated entities and thus ensure the data registered "on chain" are more reliable. Second, it would enable private individuals, private organizations and non-governmental stakeholders in general to also play an "active role" in the creation and management of public databases. As a result, private individuals would no longer be the simple users or "negative terminals" of a database created by others but would have to contribute actively to its creation,[209] confirming how the blockchain is conceptually closer to the concept of open government than to that of transparency.

In this sense therefore the blockchain gives rise to a system of "notarized transparency" in which environmental information is not only freely visible to, and usable by, all interested parties, but also its reliability is guaranteed in terms of its formal completeness and the certainty as to the precise moment of its publication.

V. CONCLUSION

Blockchain technology lays the basis for "choral participation" by the general public, regulated entities, and all interested parties in the protection of the environment. Thanks to this technology, these actors could not only be put in a position to cooperate more effectively with public authorities in the monitoring and enforcement of environmental law but would also turn into genuine co-administrators capable of carrying out a dispersed verification as to the completeness and timely status of environmental data.

Under the system hypothesized in this Article, the blockchain would not therefore eliminate the role of public bodies but would make it possible to reformulate the function of formal verification of environmental data and their registration on public databases according to a multi-nodal logic, preventing potential cases of corruption, maladministration, and regulatory capture. But the joint 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 these operators' having an inherent tendency to be of low

208 The (at least) formal correctness of data is also essential, *inter alia*, with a view to their usage for regulatory purposes.

209 Werbach, *Trust, but Verify*, *supra* note 16, at 504 ("Distributed ledgers are active, not passive. In other words, they do not simply record information passed to them. They are part of a consensus system, so they must ensure that recorded transactions are actually completed to match the consensus.").

reliability owing to their pursuit (also) of their own specific interests. Accordingly, blockchain makes it possible to envisage a "third way" between state failure and market failure in which public and private bodies cooperate to promptly make available data that are, at least in formal terms, reliable.

Within this system, the data would not be reliable because of the identity of the individual charged with controlling them, but rather because of the cooperation or "choral participation" described above. By virtue of this cooperation, public and private bodies would thus become equally reliable: thanks to the mechanism of "notarized transparency" and the dispersed verification of data, it would be the system itself that, subject to the limits mentioned above, induced them to act properly. In fact, opportunistic and especially unlawful behavior could be discovered easily and quickly.

But the possibility to establish with certainty when certain data were provided along with their level of completeness would induce both private operators and public authorities to act in a more responsible manner. This is because the blockchain system would make it possible to subject to closer scrutiny not only the actions of businesses but also the manner in which public authorities manage environmental issues. The authorities could be more readily exposed to political responsibility before an increasingly aware and informed public, as well as legal liability if they fail to act. However, this could ultimately be a "double-edged sword." In fact, it is impossible to exclude that the public authorities might object to such a rigorous system that required them to seek a new balance between the often only notional efficacy of environmental protection and the attendant regulatory costs.

It may be noted once again that, since the system of absolute "notarized transparency" achieved by the blockchain increases overall compliance within the system, it might also offer a response to the problem of "slippage" which often affects environmental law and other branches of the law. While it must be accepted that a certain degree of "slippage" is to some extent inevitable and above all—as has been astutely argued—could in some cases even be useful to ensure the effective implementation of environmental law (for example in cases involving excessively rigorous rules that impose excessive and disproportionate costs on regulated entities), it must also be considered that it is associated with a cost, especially in terms of "damage to our concept of rule of law."[210] Within this context, by enhancing

[210] *See* Daniel A. Farber, *Tacking Slippage Seriously: Noncompliance and Creative Compliance in Environmental Law*, 23 HARV. ENV'T L. REV. 297, 305–11, 325 (1999) (providing a thoughtful analysis of the costs of "slippage," but also of its importance, under certain circumstances, in making environmental law more implementable and effective). *See also* Stewart, *A New Generation*, *supra* note 20, at 60 (noting that "[b]y its very nature, slippage must function interstitially. Even if it were capable of wider application, it would not be wise or desirable to attempt to use it more widely because of the threat that it poses to the rule of law and its low level of transparency and accountability").

transparency and accountability for all actors involved, the mechanism for registering data on the blockchain would help to reveal the contradictions and lack of coordination or consistency between the approaches of the public authorities. It would reveal many instances of "slippage" that are at present more or less tolerated, obliging lawmakers to resolve the problems associated with regulations that are often obscure, disproportionate, and unsustainable within the relevant places (rather than in the backrooms of public agencies). Therefore, blockchain technology would require environmental protection to be taken (more) seriously.

Recall that many considerations made above in relation to environmental protection could also be extended to other sectors in which, analogously, common goods—which as such are of interest for all—are at issue. To give just a few examples, these may include the financial markets, territorial protection, and food safety where, not by chance, individuals (acting either alone or, more frequently, within associations) are already very active and would therefore be ready to take on the new and more significant tasks blockchain now allows us to envisage.