ISSN 2723-9195

CERIDAP

Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche

Estratto

Fascicolo
2/2024

APRILE - GIUGNO

The evolving regulation of blockchain smart contracts looking at public services resilience for the sustainability of the healthcare and agrifood sectors

Giuseppina Lofaro

DOI: 10.13130/2723-9195/2024-2-41

Il perseguimento degli obiettivi di resilienza e sostenibilità delle comunità e dei mercati passa attraverso la transizione digitale dei servizi pubblici. Gli smart contract basati sulla tecnologia blockchain a registri distribuiti (DLT) mostrano un ampio potenziale applicativo nell'ambito dei servizi pubblici rivolti alla sanità, all'agricoltura e alla filiera agroalimentare. Inoltre, la funzionalità della tecnologia blockchain potrebbe migliorare grazie alla confluenza degli algoritmi di intelligenza artificiale (AI). Il lavoro, privilegiando gli aspetti del diritto amministrativo dei servizi pubblici come quelli riconducibili al principio di trasparenza, analizza tale scenario e focalizza il percorso di regolamentazione degli smart contract in Italia alla luce del complesso e dinamico quadro regolatorio comunitario. Alcuni dibattiti, compreso l'inquadramento dottrinale degli smart contract, rimangono aperti. Nel 2021 AgID ha lanciato un progetto di infrastruttura blockchain; nel 2023 AgID, in applicazione del nuovo Codice dei contratti pubblici, ha richiamato gli smart contract nel fissare i requisiti tecnici e le modalità di certificazione per le piattaforme di approvvigionamento digitale, mentre l'UE ha attivato una "regulatory sandbox" riguardante la blockchain ed ha recentemente approvato l'atto regolatorio sull'intelligenza artificiale inizialmente proposto nel 2021. Gli sforzi profusi ai fini della regolamentazione standardizzata degli smart contract sono notevoli, sia a livello comunitario che nazionale, ma essi devono confrontarsi con la velocità dell'innovazione tecnologica e la parallela necessità di tenere tutti gli aspetti giuridici e amministrativi sotto un armonico, sicuro, trasparente ed efficiente controllo.

The pursuing of resilience and sustainability goals of communities and markets *involves the digital transition of public services. Blockchain smart contracts by Distributed Ledger Technology (DLT) show a wide applicative potential within public services addressed to healthcare as well as agriculture and agri-food chain. Additionally, blockchain functionality could improve by the confluence of artificial intelligence (AI) algorithms. The work, privileging the aspects of administrative law of public services such as those leading back to the principle of transparency, analyses this scenario and focuses the regulation path of smart contracts in Italy in the light of the complex and dynamic EU framework. Some debates, including the doctrinal framing, remain open. In 2021 AgID launched a blockchain infrastructure project; in 2023 AgID, according to the new Public Contracts Code, recalled smart contracts within the published technical requirements and certification methods for digital procurement platforms, while the EU activated a blockchain regulatory sandbox and recently approved the AI Act proposed in 2021. Many efforts towards a standardised regulation of smart contracts, either at EU or national level, are being profused, but they must hardly compare with the technological innovation speed and the parallel need to keep all the legal and administrative aspects under harmonic, secure, transparent and efficient control.*

1. Introduction[1]

The evolving digitalisation initiatives within the worldwide public sector's services reflect the on-going transition through the increasing exploitation of electronic or digital components and technologies[2]. Technological innovation affects either the organization and activity of the administration or the relationships with citizens, due to the recognition by the legislator of a bundle of new rights arising from digitalisation according to the so-called "digital citizenship". In Italy an hystorical turning regulatory point, with respect to the formal recognition of informatic and telematic tools, can be found in the Law n. 241/1990[3]. The Legislative Decree n. 29/1993[4] addressed the computerization of public offices, regulating the methods of adoption of technological tools by the offices. In 1994 a governmental address recognised the principles of public services provision[5]. In 1995 some simplification and efficiency measures addressed to public administrations were introduced[6]. With the Law n. 59/1997[7], the relationship of the public administration with the use of technology has been further strengthened, as a communication tool with citizens in order to simplify the use of the bureaucratic services provided by the public administration. According to the Law n. 15/2005, which amended and integrated the Law n. 241/1990, the use of informatic and telematic tools represents the way to increase the efficiency of public administrations[8].

The provision by the Law n. 15/2005 has also feeded the codification of digital administration[9]. Later on the regulation principles and dictates of the Legislative Decree n. 33/2013[10], as modified the Legislative Decree n. 97/2016[11], rely with: transparency[12] in general, publicity and right to knowledge, transparency in the use of public resources, right of access to data and documents, access for scientific purposes to the collected databases for statistical analysis, obligations to publish data, information and documents of wide interest, with a dedicated evidence to some "special areas" (public contracts[13] of works, services and supply; planning, realisation and evaluation of public works; transparency in the activities of territory planning and government; environmental information; transparency of the national health service – art. 41), the coordination with the prevention plans of corruption[14]. The Legislative Decree n. 97/2016, at art. 32 (paragraph 1), confirms that public administrations and managers of public services are required to publish the chart of services or the document with the quality standards of public services[15]. The codification process of digital administration has been progressively up-dated by the Law n. 124/2015[16], the Legislative Decree n. 217/2017[17] and the Law Decree n. 76/2020[18] (simplification decree). More recently, within the Governance discipline of the National Plan for Recovery and Resilience, the Law Decree n. 77/2021[19], converted with modifications by the Law n. 108/2021[20], provided some further measures aimed at strengthening the digital transition of the public administration[21].

The more recent smartness dimension marks the ambitions of the public sector to become more agile and resilient in terms, among other, of transparency, interconnectedness, efficiency, effectiveness.

The development and progressive implementation of blockchain within the public administration is wide expression of that transition effort and the blockchain smart contracts based on the Distributed Ledger Technology (DLT) are a finalised example, starting from Szabo's intuition in the 1900s[22]. The potentialities of blockchain-based smart contracts subsequently find a strong interest within the public sector[23] according to the potential applications within the public services, ranging from public registers to the management of information, data and documents, identity mapping, tenders and calls for funding.

In Italy two relevant economic pillars with significant links with the public services[24] are represented by healthcare and the agrifood productive and distribuion chain[25]. The expenditure for health services (public plus private) as a share of italian GDP of 2019 has been estimated in 8,7% (6,4% the public only), resulting at the twelfth position, just below Spain (9,0%), slightly beyond the average of 8,3% of the 27 EU countries[26].The estimated weight of italian agrofood industry as a share of GDP of 2022 is over 15%, with a very high level of exportations, similar to that of Spain[27]. Today the two sectors also interact within the so-called "One Health" approach, originating in 1984 as the "One Medicine" concept according to which «*the critical needs of man include the combating of diseases, ensuring enough food, adequate environmental quality and a society in which humane values prevail*»[28]. The developing core idea looks at an holistic approach to human, animal and environmental health, to better protect the system health. The ever growing human populations and the resulting environmental degradation from expanding land use, intensified agricultural and animal husbandry methods, and closer habitation between humans and both domesticated and wild animal species, are also recognized as key factors increasing shared risk across the animal-human-ecosystem interfaces[29]. The One Health approach was officially launched in 2004 as an integrated, unifying approach to balance and optimize the health of people, animals and the environment. The approach mobilizes multiple sectors, disciplines and communities at varying levels of society to work together. One Health[30] involves the public health, veterinary and environmental sectors, and is particularly relevant for food and water safety, nutrition, the control of zoonoses (diseases that can spread between animals and humans), pollution management and combatting antimicrobial resistance (the emergence of microbes that are resistant to antibiotic therapy). Government officials, researchers and workers across sectors at the local, national, regional and global level are required to implement joint responses to health threats. This includes developing shared databases and surveillance across different sectors, and identifying new solutions addressing the root causes and links between risks and impacts. Community engagement is also critical to promote risk-reducing habits and attitudes, and to support early detection and containment of disease threats. The World Health Organisation (WHO) formed a One Health initiative to integrate work on human, animal and environmental health across the Organization. WHO is also working with the Food and Agriculture Organization of the United Nations (FAO), the United Nations Environment Programme (UNEP) and the World Organisation for Animal Health (WOAH) as a One Health Quadripartite. The Quadripartite is promoting multi-sectoral approaches to reduce health threats at the human-animal-ecosystem interface. The transformations required to prevent and mitigate the impact of current and future health challenges at global, regional and country levels is outlined in the Quadripartite One Health Joint Plan of Action (OH-JPA). The One Health High-Level Expert Panel (OHHLEP) was formed in May 2021 to advise FAO, UNEP, WHO and WOAH on One Health issues. This includes recommendations for research on emerging disease threats and the development of a long-term global plan of action. The panel will also have a role in investigating the impact of human activity on the environment and wildlife habitats, and how this drives disease threats. Critical areas include food production and distribution, urbanization and infrastructure development, international travel and trade, activities that lead to biodiversity loss and climate change, and those that put increased pressure on the natural resource base. One Health has become one of top concerns globally, as it entails the essential global public health challenges from antimicrobial resistance over zoonoses, to climate change, food security and societal well-being. Research priorities in One Health include the study on interactions of human-animal-plants-nature ecology interface, systems thinking, integrated surveillance and response systems, and the overall One Health governance as part of the global health and sustainability governance[31].

The applicative potential of blockchain-based smart contract appears, at first sight[32], destined to strengthen by the confluence of blockchain tecknology and Artificial Intelligence (AI) algorithms[33].

Looking at public services resilience for the sustainable development of healthcare and agrifood chain sectors, the works aims to deepen the promising scenario so far depicted concerning the blockchain smart contracts exploitation and analyse the regulation path in Italy, in the light of the complex and dynamic EU rule framework, paying particular attention to some aspects of administrative law applied to public services, such as those leading back to the broad principle of transparency.

2. The blockchain-based smart contracts environment

Blockchain can be defined as a DLT which secures and records transactions in a *peer to peer* network. Records are stored on many interlocked systems keeping identical information. Numerous transactions of value exchange are grouped into several interconnected blocks. By the assurance mechanism and cryptographic trust, each block immutably records information, preserving a rational state agreed by all the participants or individuals without any central or trusted authority. Blockchain technology is different from database technology. In blockchain systems, new entries are added at the end of the ledger and no one is allowed to edit or delete the data. On the other hand, data can be modifed or deleted by a central administrator in a relational database. Blockchain has many features, such as transparency, immutability, disintermediation, redundancy and many others. Since there are many users or individuals in the network of blockchain, who are distributed over several places, there are many issues, namely complexity, network size, network speed and unavoidable security faw. There are mainly three types of blockchain, namely the public or permissionless, the private or permissioned and the federated blockchain. In the permissionless blockchain, anyone can join the network and operate. In the permissioned blockchain, anyone cannot join the network. Decentralized blockchain supports to remove the central authority or middle-man, which can decrease the cost and risk.

Transparency in a blockchain network means that all the data are public; these data cannot be easily tempered and auditing of these data is very difcult. In a blockchain network, data are published on a common platform and other interested party and regulator can easily get a real-time view of the platform. With respect to redundancy, every user or individual keeps a copy of a file; therefore, it is challenging to hack the file by a hacker or attacker or by a third part, when the user is off-line. According to immutability in blockchain, record changing is diffcult and the consensus algorithm is developed by a protocol; therefore, the record integrity is ensured by the properties of the code. Blockchain provides many advantages[34]. According to the security aspect in blockchain, all the validated or executed transactions are permanently saved in the blocks that cannot be deleted or altered by anyone. Blockchain is a distributed technology, supporting numerous computers spreaded around the world, which can increase in real-time the efficiency of the network. Blockchain technology is resilient, even with the massive number of participants or individuals and the increased robustness of data with longer life. According to trust advantage, a majority of individuals or participants have to be agreed on data before adding it in the blockchain network, which is diferent from the centralized network. Thus, trust is increased for writing, altering or even reading any data. There are also some disadvantages and perplexities[35]. Blockchain is wasteful, because each node has to run or maintain the consensus algorithm, which gives fault tolerance ability and guarantees zero downtime and, however, all these are wasteful because each node follows the same task to reach consensus. One more disadvantage concerns the network speed and cost; in a blockchain network, it is difficult to manage large numbers of nodes. Blockchain increases the database size. According to the performance, blockchain network is always slower than the centralized database. When a transaction is executed, blockchain executes all the processes of a regular database along with many additional burdens like signature validation, consensus algorithm, etc.. A reliable standard can improve the security of the blockchain network.

The smart contract is one of the most popular blockchain applications. According to Szabo's initial definition, «*A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as* *payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs».*

Today blockchain-based smart contracts are self-executing agreements with their terms directly inscribed in code that will automatically execute when predetermined conditions are met. In principle, they are developed to offer transparent, tamperproof and cost-effective alternatives to traditional contracts. In other words, the blockchain is like a ledger, in whose system operations are recorded, shared between multiple nodes, which cannot be altered or tampered with in any way. The smart contract uses the formula "if this/then that occurs", according to which, upon the occurrence of a given event (this), certain effects (that) are produced, as predetermined by the parties themselves, on the basis of rigid instructions. Subsequently, the parties insert the smart contract into the chosen blockchain, which, in turn, becomes the guarantor of the contract and ensures that the instructions given to it can no longer be modified. At this point the smart contract becomes part of a block (identified by a hash code), which is validated by the nodes, i.e. by the participants in the blockchain, who are asked to give their consensus. Once the latter is obtained, the block is added to the chain, immutable and certified. The contract, in this way, acquires the ability to enforce its clauses and to have prompt and immediate execution, as soon as the agreed conditions occur, without, however, the parties having to carry out checks or activate paper or manual procedures.

Smart contracts based on DLT blockchain allow to disintermediate/decentralize[36]. Independence from intermediaries in the verification and approval phase of the contract represents a potential notable advantage, as, by devaluing the importance of the fiduciary element, it allows the negotiation processes to be simplified and accelerated, as well as reducing costs, such as, for example, those relating to the granting of guarantees. This, however, is true to the extent that it is simple for the parties to translate the contractual clauses into computer language. In fact, it should be noted that, in this case, we are witnessing a real inversion of the normal relationships between man and technology. While in contracts stipulated on-line via computer it is the machine that uses human language, on the contrary, in the context of smart contracts it is man who has to make use of computer language. But the parties are not always able to independently translate human and legal language into native computer language, especially when some general clauses come into play, such as, for example, good faith, fairness and diligence. In such cases, therefore, some form of intermediation may be always essential. So the issue of trust leaves the legal sphere to enter that of the developer, which, in reality, realizes an intervention by a third part. In light of the above, it can be concluded that the smart contract determines greater utility and benefits only in the presence of agreements with a high rate of standardization and characterized by low levels of complexity. Smart contracts have the advantage of reducing the possibility of non-performance between the parties, with subsequent recourse to the judge for legal protection. These contracts are executed on the basis of the computer program, which uses blockchain technology and the "if this/then that" formula, deriving from the rigid and unchangeable instructions dictated by the parties. It follows that the execution of the contract and the consequences of non-fulfilment are entirely governed in a computerized way, based on the occurrence of certain events and the production of given predetermined, as well as immutable, effects. And then, since everything is predetermined electronically and the transaction, once entered, is unchangeable, just as the related instructions become irretractable, it is clear that the risks of non-compliance are reduced. Furthermore, the architecture of a system conceived in this way, compared to traditional contractual mechanisms, contributes more to increasing the degree of certainty, security and stability. However, it must be specified that, when mandatory obligations *ex lege* to modify the system come into play, they cannot be fulfilled by the parties, who, as mentioned, cannot intervene on the system and modify the information contained therein, being the same radically intangible and immutable. On the other hand, the technologies under consideration are characterized by the lack of a central register and an administrator who manages a database, as well as by the presence of strong decentralization. They are based on distributed registers, in which the databases are managed in a decentralized way, by individual users, who, moreover, are not even easily identifiable, since they often use pseudonyms or computer addresses that are not always easily traceable to the real identity of the user. Some more advanced blockchains[37] have tried to solve this problem by inserting a specific function, the so-called kill or self-destruct function, which causes the smart contract to fail. Due to the critical issues and technical-legal limits previously described, the current applicability of smart contracts is restricted to very simple and linear contracts. Smart contracts, as highlighted above, operate based on the "if this/then that" logic, which is typical of the condition. The latter, pursuant to the articles 1353 and following of the italian Civil Code, constitutes a future and uncertain event, on which (suspensive) or until which (resolutive) the effects of the contract depend. Although the institution in question may contain a condition, it is not at all necessary for this to happen. And in fact, the "if/then" logic, in addition to the contemplation of a condition, could well have as its object an exception of non-compliance. Furthermore, if it is true that the effects of the smart contract are immediate, it is also undeniable that this automatism cannot be total. This is because each smart contract requires an input, which is provided by an oracle, which can be either a man or an IT tool (such as an application). The oracle allows the smart contract to communicate with the world outside the network, alerting it if fact A has actually occurred, resulting in event B. The input provided by the oracle is objective and automatic if it comes from an IT tool. The input is subjective, however, when it requires an evaluation that must necessarily be carried out by man, through his own judgement. It is true that there is nothing to prevent the parties from concluding a smart contract with external evaluative input. However, if this were to happen, the logic of automatism and disintermediation typical of such an institution would end up being betrayed, due to the external interference of a subject, i.e. the oracle-physical person, to whom the delicate and decisive task would be entrusted evaluative, on which the production of effects depends. Precisely in light of this consideration, it is believed that the natural scope of application of smart contracts is that of objective input, which postulates standard, simple and automatic transactions, dependent on the verification of an unquestionable objective fact. From the above, further confirmation is obtained that not all conditions and not the entire conditional discipline is compatible with the smart contract. And indeed, first of all, the computer program is not able to understand whether a condition is merely potestative (i.e. based on the mere arbitrariness and whim of a party) or pure potestative (i.e. dependent on a choice which, despite being voluntary, occurs as a result of a balance between opposing interests). To this it must be added that automatism and disintermediation would appear to be incompatible with the assessments concerning the conduct of the parties in good faith, pending the condition pursuant to the art. 1358 of the italian Civil Code and the consequent fiction of fulfillment pursuant to the art. 1359 of the Civil Code. Even where, in fact, the parties had foreseen in the initial instructions clauses similar to that of good faith pending the condition and, in the case of failure to comply with this obligation, that of the consequent fiction of fulfillment, a significant problem would still arise. The latter would derive from the fact that this input would have to be communicated by an oracle-natural person, who would carry out an extremely questionable activity, which would seem to exceed the limits of the permitted subjective input, thus excessively betraying the logic of automatism and disintermediation typical of the institution in question. As an alternative to the traditional procedure of concluding paper contracts, these tools have led to the creation of a new space for concluding electronic contracts based on binary information, data-oriented contracts, and finally smart contracts. In order to conclude smart contracts, the parties need to obtain a license.

Despite the similarity of smart contracts and traditional contracts in most of the governing rules, the emergence and expansion of electronic commerce have caused a new challenge in current contract law. Aside from the general ambiguity of electronic relations, the contracts made in this setting also include some legal questions and uncertainties. The introduction of new financial instruments into the legal system of any country requires the approval of new laws in order to identify and recognize the different aspects of these instruments in the legal system. Smart contracts are viewed as a very acceptable replacement for traditional contracts because of their security, speed, high accuracy and low cost. Due to their self-executing capabilities, transparency and correctness, smart contracts are effective in lowering legal claims. Smart contracts[38] prevent the occurrence of many legal and criminal lawsuits, as well as the occurrence of crimes such as financial frauds, the sale of other people’s property, and the conclusion of fraudulent transactions. These contracts reduce the costs of concluding transactions, avoid wasting time, and prevent the occurrence of some legal claims, such as the necessity of preparing official documents, enforcement of ownership, etc., because they are self-executing in relation to the implementation of the provisions of the contracts. Additionally, they are an obstacle to numerous financial abuses by transparency features. However, due to the unique characteristics of the electronic environment and in order to be able to assign legal actions, some minimal formal requirements have been established. The replacement of traditional contracts with smart contracts not only saves money by reducing the costs of concluding and registering transactions but also leads to more supervision by the competent authorities over the financial transactions of individuals. It is wide opinion that popularizing such contracts has many advantages and greatly increases the security and strength of transactions. This will reduce lawsuits, increase speed and accuracy in the markets, and, in general, lead to security and economic growth. It is possible to justify the various aspects of these contracts, but in any case, the foundation of a new process in any legal system requires the approval of laws to formalize the validity of these contracts in that system and create a general obligation for individuals to respect the form of these contracts. In the context of substantive rules, the principles of technical neutrality and functional equality are the basis for establishing laws governing smart contracts so that a person can understand that changing the constituent elements of the contract does not change the legal regime governing it and smart contracts also have the same protections as traditional contracts. The use of smart contracts depends on overcoming obstacles like educating the general public, defining the contract-closing procedure, resolving conflicts between national and international laws, harmonizing national and international laws to avoid conflicts, ensuring that third parties do not have access to the parties' private commercial and non-commercial information, and improving information security. The issue of trust is the biggest concern for organizations requesting to use "electronic" or "smart" contracts. Smart contracts have special qualities that contribute significantly to the growth of the exchange system and also popularizing such contracts has many advantages and greatly increases the security and strength of transactions. This will reduce lawsuits, increase speed and accuracy in the markets, and, in general, lead to security and economic growth.

3. The potentialities of smart contracts for the public

services in the health and agrifood sectors

3.1 Health sector

In Italy the Law n. 273/1995 introduced the obligation of public health agencies to publish the chart of services. Today, services charters cover general aspects dealing with the presentation of the public agency and its fundamental principles, the information on the health and socio-health services offered, the methods of access to the services, on their use and the continuity of care, the publicisation of the commitments undertaken to guarantee the main quality factors of the services, in particular with regard to the relationship with citizens, the publicization of protection procedures. The charters pursue fundamental principles such as: equality, impartiality, continuity, participation, effectiveness and efficiency[39], right to choose. The key principle of the health services charter is that according to which the provider adopts standards of quantity and quality of the service which it is required to ensure compliance with. The provider body publicizes the standards adopted and informs the citizen of them. The provider verifies compliance with the standards and the level of user satisfaction, guarantees compliance with the adopted standard, ensuring specific protection for the citizen, through forms of reimbursement in cases where it is possible to demonstrate that the service provided is not aligned, in quality and timeliness, to the published standard. According to the phylosophy of the charter, the service quality standards must concern the entire experience of the citizen who comes into contact with healthcare facilities (for example, the hospital or the specialist clinic) and must touch on all the factors perceivable by the user, distinguishing the technical quality of healthcare provision from the issue of service quality which, in healthcare[40], revolves around the following factors: time, understood as timeliness (speed of service, shortness of waiting lists and queues, etc...), punctuality, regular compliance with pre-established and communicated programmes, simplicity of procedures, understood as the possibility of making requests by telephone or ease of administrative obligations, information relating to healthcare treatment, understood in the sense of comprehensibility, clarity and completeness, orientation and welcome upon entry into healthcare facilities, understood in reference both to signs and to the reception service and to the necessary general information on services (times and location of services, names of managers, request methods, etc.), physical structures, in reference to the comfort and cleanliness of hotel facilities, services and waiting rooms, social and human relationships in relation to the personalization and humanisation of treatment, the ability to provide reassurance, courtesy and respect for dignity, etc. In the event that the aforementioned principles are disattended, the service charter provides for the methods, to be publicized in the most appropriate ways, through which the citizens themselves can easily access the complaint procedures. And here not only the providers come into play, but also the regional administrations as institutionally responsible entities for the planning, financing, organisation, management and control of activities aimed at health services. In the same direction, if the quality standards set out in the service charter are not respected or in the event of a disservice, act or behaviour that has denied or limited the usability of the services, the citizen can lodge a complaint with the Public Relations Office established at each institution. The latter, in addition to information and orientation tasks, also deals with the collection and management of reports from citizens, with the aim of improving the services provided by the structure.

Blockchain-based smart contracts show a number of key benefits to the health sector and the connected public services. These beneficts concern with clinical data sharing, global data sharing, patient monitoring, mantaining patient medical history, research and clinical trials, data access control, supply chain management, billing/payments. For example, with the blockchain approach, medical information is easily obtained and shared with different entities. Patients will give consent and at the same time have control over the data held. Some blockchain smart contract systems were proposed to support real-time patient monitoring and medical interventions by sending notifications to patients and medical professionals, while also mantaining a secure record of who has initiated these activities[41]. The knowledge of the medical history of the patient allows to receive medical treatment elsewhere. The blockchain can face trial research, that helps in the tracking process at each phase, then the data can be processed and analyzed without a lot of waste of resources. Blockchain can help the patient right to control his own data by the promised privacy as well as distributing it to trustworthy entities. With blockchain, the payment process can be easier by sharing information to the entities involved while providing security for payment data, so that payments will be more valid, effective and efficient in terms of time and cost. One more significant benefit is the removal of intermediaries. By relying on secure, tamper-proof code, smart contracts can simplify the claims process, reduce the time it takes to process claims, and eliminate the need for manual intervention. This results in cost savings for both insurance companies and policy holders. Smart contracts can provide greater security and privacy for sensitive health and personal information. Since the information is stored on a decentralized blockchain, it is protected from unauthorized access, tampering, and other forms of cybercrime. This is particularly important in the health insurance industry, where the security of personal health information is a top concern. Another benefit of smart contracts is their ability to promote transparency and trust. Policy holders can have greater confidence in the claims process, knowing that their information is being handled in a secure and transparent manner. Insurance companies can also benefit from the increased trust and transparency, as it may result in higher customer satisfaction and increased customer loyalty. This can also help the developing implementation of the One Health approach, i.e. through the secure and transparent management of intersectorial data.

But there are still some challenges to overcome due to the lack of standardization and interoperability. The use of smart contracts in these environments is promising and is likely to become increasingly important in the coming years.

The italian healthcare sector is recently provided with the law n. 62/2022[42], otherwise known as the “Sunshine Act”. The objective pursued by the new law is to prevent corruption[43] and combat conflicts of interest that affect the sector to the detriment of the interest in collective and individual health protected by the system. This objective is achieved by the legislator with the introduction of the principle of transparency of economic interactions between all healthcare operators: payments in cash (or in kind), shareholdings and proceeds deriving from industrial or intellectual property rights must all be communicated via an electronic public register kept by the Ministry of Health. The new register introduced by the Sunshine Act is an electronic platform prepared by the Ministry of Health in which all the information on economic relationships between operators in the healthcare sector must flow. This register will therefore be fed by the same information that operators will have the obligation to communicate to the Ministry of Health.

The art. 2 of the Sunshine Act specifies the addressed entities of the healthcare sector, such as production companies[44], entities operating in the health sector[45], health organisation[46].

All economic operators in the sector, therefore, will have to evaluate their economic relationships to verify whether or not they assume one of the three roles outlined by the Sunshine Act. The complexity lies in the fact that this role may vary depending on various factors, such as, for example: the activity carried out, the type of relationship, the onerousness or otherwise of the service, the identity of the contractual counterparty and/or the intended purpose.

The art. 3 of the Sunshine Act clarifies the types of data to be communicated to the Platform[47]. Even in this case, the interested operators will therefore have to verify whether their agreements with contractual counterparties fall within one of the defined operations. The obligation to communicate will fall on the subjects that fall within the notion of "producing company" and must be fulfilled within the terms and in the manner that will be definitively established by the Ministry of Health. Although the obligation is borne only by the manufacturing companies, entities operating in the health sector and healthcare organizations must ensure that the agreements contain this communication obligation to avoid signing contracts that differ from the requirements required by law and that in any case could be harmful to both parties.

The art. 6 of the Sunshine Act provides for pecuniary administrative sanctions for the "producing company" that fails to comply with its communication obligations[48]. The sanctions imposed will be published in the Healthcare Transparency Register, so as to identify the manufacturing company, the violations committed and the details of the sanction. In addition to proceeding *ex officio*, the Ministry of Health may become aware of violations of the communication obligation also through reports sent by natural persons made through the whistleblowing regulations. The Ministry, in fact, will prepare an "internal reporting channel" for the presentation and management of reports; in the event of elements that support the reporting of failed, incomplete or incorrect transmission of data in the Registry, the violation will be notified to the company producing the violation and the necessary measures will be adopted.

Reports will be treated in accordance with the provisions of Legislative Decree 10th March 2023 n. 24, which implements the Directive (EU) 2019/1937 (the so-called whistleblowing decree). Before making a report, therefore, it will be necessary to ensure that this activity is carried out in compliance with the new Legislative Decree n. 24/2023. The whistleblowing procedure, that manufacturing companies are required to adopt according to the Legislative Decree n. 24/2023, must therefore also take into consideration the reporting methods that will be established by the Ministry of Health to implement the Sunshine Act. The adoption of an effective MOG (Organization, Management and Control Model) allows companies not only to be transparent but also to prevent corruption crimes, which have been included in the catalog of predicate crimes by the Legislative Decree n. 231/2001. The provisions of the Sunshine Act recall some principles usually indicated in the code of ethics of companies that adopt the MOG (it is intended to refer, for example, to the duty for all recipients of the model to avoid situations of conflict of interest or to provisions that regulate relations with the Public Administration in general). Furthermore, from a preventive perspective, companies regulate in detail within their models and with specific procedures the permitted behaviour suitable for avoiding the commission of corruption crimes, defining in detail the amount of permitted disbursements, the necessary authorizations, the methods reporting, the information flows to the supervisory body. For all those subjects who are therefore already equipped with a MOG and operate daily in compliance with the procedures and principles of the Legislative Decree n. 231/2001, the adaptation to the provisions of the Sunshine Act will require a revision of the model in order to adapt it to the new requirements imposed by law. Conversely, the adaptation for all those subjects who do not adopt a model will certainly be more complex, also and above all with a view to making operators aware of the new obligations with the risk for production companies, without a well-defined internal flow, of not even being aware of the disbursements made and therefore omitting their advertising, incurring the relevant sanctions. Although the Sunshine Act has already entered into force, the obligations that all interested operators must comply with will be applicable with a postponed deadline[49]. The notice referred to in art. 5 paragraph 1 will be published in the Official Journal and should coincide (or in any case be subsequent) with the publication of the

"Transparent healthcare" register in the website of the Ministry of Health. To date, the register has not yet been established as the public consultation launched by the Ministry of Health with all the stakeholders to issue the "implementation decree" and the "technical specifications" necessary for the establishment of the new database is still in progress. While awaiting the results of the consultations, it is to be assumed that there is very little left for the issuing of the implementing decree and the technical specifications and, consequently, for the establishment of the "Transparent healthcare" register. From that moment onwards, the double term of 6 months and 1 year will begin to run. Despite the perplexities and fears that this legislation raises in all the economic operators involved, from companies to healthcare professionals, it is necessary to take note of it and accept the idea that the ethical and "compliant" management of these relationships could be a significant step towards more genuine transparency in the sector, as well as a useful tool to avoid incurring sanctions and other legal risks. It will therefore be necessary for companies and other interested operators to begin now to evaluate the adoption of adequate measures.

3.2 Agriculture and agrifood sector

The digitalisation of the agri-food sector, public services included, has potential reflections over multiple segments of the value chain. It allows the use of digital technologies and data created on-farm (e.g. by machines and sensors about the status of soil, crops, animals and work processes) and off-farm (e.g. economic information, transactions, weather data and satellite data). This can help the decision-making process of the stakeholders such as farmers, input and output suppliers and policymakers. Therefore, the digitalisation of the agri-food sector is generally viewed as a positive means to strive towards sustainable development goals. The technological innovation is expected to increase the efficiency of food production at the firm and value chain levels and provide social and environmental benefits in food systems. These expectations also emerge from policy documents envisioning potential futures of agriculture[50], food production and food systems[51]. For example, the use of emerging technologies could in general improve the transparency of the food value chain[52]. Similarly, farmers' adoption of data-based technologies has the potential of improving their market power in relation to the input suppliers of the value chain[53]. According to the largest umbrella organisation of farmers in the EU, increased data exchange will raise several challenges in the domains of «*privacy, data protection, intellectual property, data ownership, relationships of trust/power, storage, conservation, public data, and usability*»[54]. The lack of interoperability between different machines, equipment and software places farmers at the risk of being locked into a relationship with one specific hardware or software developer without the real possibility to change to another system or aggregate data from different systems[55]. In addition, data infrastructure and connectivity in farms need to be further developed and geared towards sharing larger amounts of data. Upgrading farmers' skills to become «*informed data consumers as well as co-creators and curators of data*» to exploit the potential of data and information is crucial for better decision-making[56]. In its efforts to ensure the agri-food sector's compliance with societal demands (reduced environmental pressure, improved product and process traceability, etc.), public policies are from time expected to encourage technological development[57]. Aiming to reduce bureaucracy and overcome market failures, the public policies could promote the availability of new technologies and mitigate excessive market concentration of technology providers[58]. Public policies are also major contributors to well-functioning innovation systems by assuring quality regulations and institutions concerning data ownership, privacy and liability[59]. They support delivering upgraded research and extension services[60]. New technologies have significant potential in terms of measuring and comparing the results of different agricultural and environmental practices and policies in the agri-food sector and assessing the progress of moving towards set goals[61], a notion that is also reflected in several strategic initiatives of the EU, for example, "Farm to Fork Strategy". According to the literature[62], public policies should aim to ensure equitable digitalisation of the sector, protecting the public interests, the interests of farmers and other supply chain actors. Public policies should also be receptive towards the technological innovation opportunities, allowing equitable data exchange, supporting dedicated R&D activities as well as open-source and open-databased technologies.

Institutional infrastructure plays an important role in facilitating the free flow of goods, services, investments and labour in the agricultural sector[63]. The lack of effective institutional infrastructure is a key factor that causes trade barriers and low productivity in many developing countries. DLTs serve as a digital institution of trust that provides a more transparent and efficient system for transactions and recordkeeping than traditional private and public institutions. Through the disintermediation of transactions, DLTs replace inefficient verification, contractual and settlement processes provided by institutions to execute transactions. This eliminates the need for some forms of institutions to intermediate transactions in agricultural supply chains, which are costly in general and typically even more so in developing countries. In addition, smart contracts strengthen the institutional infrastructure by reducing the number of parties involved and by removing the need for some types of institutions that currently safeguard the contractual process. Smart contracts and DLTs automate the contractual process in real-time and provide savings for supply chain actors in transaction fees and legal costs. Ultimately, lower transaction costs enabled by DLTs and smart contracts can support policy goals to increase productivity and efficiency in agricultural supply chains, resulting in lower operational costs and higher incomes for smallholders, MSMEs and other actors, and lower food prices for consumers. The efficiencies that are generated by these technologies can strengthen rural incomes and thus improve food security. In addition, the technologies can enhance accountability and transparency in government transactions, such as subsidy programmes, taxes (VAT, customs tariffs, etc.), environmental programmes, social protection, governmentled development programmes and international agreements, among others. A common public policy goal in the agriculture sector is to ensure the safety and quality of agricultural products both in trade and domestic production. DLTs provide a platform for enhanced traceability and transparency for food safety and compliance with SPS standards. The ability of DLTs to trace a product's origin carries detailed attributes in each transaction, ensuring huge improvements for food safety, such as: a more quick response to disease outbreaks and contaminated agri-food products; environmental and sustainability certifications; combating food fraud; and potential reduced friction at the border. Market transparency and enhanced market information are recognised as key factors to strengthen food security around the world. DLTs provide a platform integrated with the large amount of data generated from transactions in agricultural supply chains. Apart from the huge efficiency gains for agricultural supply chain actors, greater access to more accurate market information can strengthen the global food system and reduce the incidence and impact of price surges that are a major threat to food security. The combination of lower transaction and legal fees, automated contractual processes with real-time settlement and enhanced traceability and transparency for food safety and markets can improve trade facilitation.

Blockchain can provide several significant features in the course of activities for agricultural production and the organization of the trading process. It can help to deal with the authenticity of the product origin, the guarantee of the process transparency for consumers, the speed-up of settlement and payment operations and the reduction of the commission benefit of intermediaries, the real-time control of the programmed process. The functionality of the blockchain has been considered [64] [65] easily expandible to contracts and operations such as tracking of the global supply chain and, in the precision agricultural context, implementable to enable new farm systems and e-agricultural schemes.

In agricultural production, the interest in the blockchain exploitation is due to its usefulness for various market agents. In particular, manufacturers are usually not interested in using environmentally friendly and expensive technologies because consumers do not have access to the entire supply chain when forming the final product. The blockchain also makes it possible to reduce the number of intermediaries from producer to consumer due to the transparent fixation of all transactions in the logistics chain. Distributors usually receive only unconfirmed assurances from manufacturers about the quality of products, technologies that were used, the harvest. However, they are interested in receiving accurate information about the origin of the product, in order to face financial risks when there is a change in supply and demand.

Of particular concern may be the protection of a specific smart contract code. These features are still responsible for the non-proliferation of such contracts in everyday business life. The blockchain technology allows optimizing and simplifying the process of moving products from the place of production to that of consumption, to monitor the cultivation, collection, processing of the product and calculations in real time. It has obvious benefits for all participants in the food supply chain. This technology, having passed the necessary accreditation in various sectors of the economy, is quite capable of becoming habitual also for small farms engaged in the production of specific or organic products. Now information about the blockchain is worth spreading among manufacturers for a clear demonstration of practical use. Based on this, the final decision on economic feasibility will be made. Thus, under favorable conditions, blockchain would be a powerful means to encourage the development of agriculture.

In the food industry, for example, blockchain is increasing food traceability, with visibility of products back to their source, to ensure food authenticity and safety. At the end of the 1990s, food safety began to be at the centre of European Community food policies. The publication of the "White paper on food safety" in 2000 posed the base for the approval, occurred two years later, of the first EU framework related to the food sector by the Regulation n. 178/2002[66], widely considered as the general food law regulation in Europe. This regulation, in force since the 1st of January 2005, lays down rules for food traceability, defined as the «*ability to trace and follow a food, feed, food-producing animal or substance intended to be, or expected to be incorporated into a food or feed, through all stages of production, processing and distribution*». Food business operators must therefore have systems and procedures to provide, when requested, information to the competent authorities about:

- who supplied them with a food, feed or any substance incorporated into a food;
- the identity of the businesses to which they have supplied their products («*traceability ... shall be established at all stages of production, processing and distribution*»).

Furthermore, foods and feeds that are placed on the market in the European Community must be adequately labelled or identified to facilitate their traceability. The possibility of tracking products along the whole production chain in order to guarantee their safety and quality is recognised as a key, priority element in European Union policies. The general principles and obligations established by the EC Regulation n. 178/2002 and subsequent evolutions within the EU (i.e. the Commission Regulation n. 931/2011[67], the Regulation n.

1169/2011[68] and the Commission Regulation n. 16/2012[69]) made traceability mandatory for all foods and feeds in order to guarantee the safety of food and the quality and transparency of data. Thus, traceability and transparency in supply chains for agricultural and forest commodities are from time of major concern[70]. Accordingly, much attention has been reserved to the use of blockchain for agri-food traceability and transparency goals with some best practices suggested to overcome the limitations of the smart contract tools[71]: parties entering any type of contractual arrangement would be best served using a hybrid approach that combines text and code; given the constraints of code in representing business realities and nuances of real contract terms, the text-based contract can act as a backup; the text should clearly describe the behaviour of the contract and give full visibility into content such as variables and event triggers; both parties should decide on a clear method of resolution upon contract failure or misbehaviour; third-party technical experts and insurers can be engaged to check for errors and reduce the risks involved. The value of blockchain technology in this case concerns smart contracts between trading partners, improving product data security, disintermediation of the supply chain, and improving visibility and traceability. Smart contracts, on the other hand, automate and facilitate the execution of contractual agreements, allowing automatic payments once certain criteria are met. This significantly reduces processing times and costs associated with contract management, freeing up valuable resources for other strategic activities. Ultimately, the adoption of blockchain and smart contracts in procurement not only optimizes operational efficiency, but also promotes greater trust and transparency within the global trade ecosystem.

4. The expected developments of blockchain-based smart contracts by the confluence of AI algorithms

As it is well known, AI technology can perform complex tasks previously thought possible only for humans and in much less time. There is a growing landscape of use cases where DLT technology and AI applications can converge to get new and high levels of smart contract development, automation and efficiency. The coupling of DLT with AI algorithms can significantly improve data management, giving to providers the opportunity to share their data while keeping it confidential as needed and maintaining the right to manage data access, enabling businesses to safely and efficiently train algorithms on the data to derive insights[72].

From one hand, blockchain DLT has gained widespread attention for its ability to promote transparency and trust among network participants, providing distributed consensus over a shared ledger in untrustworthy networks, which may contain, for example, unreachable or maliciously behaving nodes. From the other hand, AI has brought high strides in natural language processing, machine learning and data analysis.

Blockchain technology develops static smart contracts for decentralized operations, lacks dynamic decision-making capabilities that limit the possibilities of everincreasing demands of modern applications. Blockchain networks, as decentralized, ensure no single point of control of failure, presenting many scalability and efficiency challenges. One notable limitation of blockchain technology is its sluggish transaction speed compared to traditional payment systems. AI algorithms can come to the rescue by predicting and prioritizing transaction processing, enabling faster confirmation times and a seamless user experience. AI can also bolster blockchain network integrity by detecting and preventing fraudulent activities. Machine learning algorithms can analyze transaction data to identify suspicious behaviour and flag potentially malicious actors. This proactive security approach can not only deter bad actors but also strengthen the network's trustworthiness. Smart contracts, rigid by design, can struggle to process complex transactions and don't easily adapt to evolving circumstances, while AI can step in to enhance smart contract execution and functionality according to its potential to dynamically adjust smart contracts, allowing them to adapt to shifting conditions and assimilate new information as it arises. AI-assisted smart contracts can gain expertiveness and responsivity, facilitating intricate and context-aware agreements that cater to the involved parties' needs. AI has also the potential to greatly improve the dispute resolution process as it should be able to evaluate and interpret smart contract terms and independently evaluate and potentially resolve issues before contract execution. AI can enhance the decision-making process for smart contracts. By tapping into predictive analytics, AI can scrutinize large datasets, identifying trends, patterns and potential risks that could affect a contract's outcome.

Blockchain tecknology coupled with AI "expertise" can cover the gaps of individual technologies and can mutually benefit from one another to develop a decentralized machine learning architecture that promises to yield better security, automation, and dynamism of the application[73]. Some privacy-preserving solutions for smart contracts using blockchain and AI framework are proposed to simplify human interaction, system activities, service alerts, security risks, and fraudulent claims[74].

Thus, the interconnection of blockchain and AI holds the potential of radically changing smart contract execution and enhance blockchain network funcionality, paving the way for more expert, secure[75] and streamlined smart contract ecosystems. This brings a high potential of improving AI and machine learning driven applications and data management functions, opening to a new era of rapid improvements in blockchain-based smart contracts. On the other hand, it is, for example, expected[76] that AI Oracles, specific mechanisms which can be, among others, highly sophisticated autonomous systems, may provide failures in the contractual liability (i.e, breach of a smart contract, unjust enrichment, conclusion of a voidable smart contract that should not have been concluded, non-conclusion of a smart contract that should have been concluded). The very recent approvalof the «AI act»[77] and its forthcoming publication in the EU official journal, as the first specific EU regulation «*laying down harmonised rules on artificial intelligence*», starting from the initial proposal of 2021[78], could be a relevant step torwards the regulation and development of AI-assisted blockchain platforms and systems addressed to the smart contracts environment.

5. The EU rule framework with implications on smart contracts regulation

In the near past the European Union has been promoting the development of blockchain technology and its diffusion and applications. Some non-regulatory significant trace can be found in a report of the European Parliament Scientific Foresight Unit published in 2017[79]. On the regulatory side, the consideration should focus the Regulation n. 910/2014[80] (eIDAS - electronic IDentification Authentication and Signature), the Regulation n. 679/2016[81] (GDPR - General

Data Protection Regulation), the Directive n. 2018/843[82], the Resolution of the 3rd October 2018[83], the Resolution of 20th October 2020[84], the AI act being published.

Regarding the eIDAS regulation, a particular attention should be addressed to the role it can play in smart contracts. A contract is the agreement of two or more parties to establish, regulate or extinguish a relationship between them. Although it does not contain specific provisions for smart contracts, the eIDAS regulation deals with electronic identification and therefore any type of identification that happens in a non-analog way.

As it regards the GDPR[85], the legal world has suddenly raised some doubts about its compatibility with the use of blockchain and DLT technologies. The field of applicability of GDPR is established[86]; in terms of territorial extension, it emerges that the scope is decidedly broad, not necessarily requiring the data controller or data processor to be established in the Union. The standard defines some important terms, essential to understand whether its scope of application influences the programming of smart contracts. The first important element is that "personal data" (article 4, point 1) refers to any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or imposed, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more elements characteristic of his physical identity, physiological, genetic, psychological, economic, cultural or social. It is certainly possible to avoid the inclusion of names and identifiers within a smart contract, limiting oneself to the use of hash codes and account addresses. By doing this, one is protected from the application of the GDPR? The answer would be negative, as although pseudonymized, the public key of an account is also personal data. In order to understand the scope of application of the regulation, the definition of "pseudonymized" data and "anonymous" data are also important. In fact, only if this last type of information were to be processed would the GDPR not apply. The data protection principles should therefore not apply to anonymous information, i.e. information that does not refer to an identified or identifiable natural person or to personal data made sufficiently anonymous to prevent or no longer allow the identification of the interested party. This regulation therefore does not apply to the processing of such anonymous information, even for statistical or research purposes. According to article 4, point 5, of GDPR, "pseudonymisation" refers to the processing of personal data in such a way that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such information additional data are stored separately and subject to technical and organizational measures to ensure that such personal data is not attributed to an identified or identifiable natural person. As can easily be deduced from the previous considerations, operating with a smart contract on blockchain cannot correspond exactly to the use of anonymous but pseudonymized data, therefore the provisions of the GDPR regulation must apply. Therefore, given that the legislation applies, what are the main points of friction with it? The legislation was designed for a vertical structure in which there is a subject who collects and uses user data for certain purposes, also using informatic structures provided by external parties. A decentralized and distributed network is a purely horizontal structure and difficult to coordinate with the principle of accountability contained in the legislation. Accountability is essentially a synonym of "responsibility" and is embodied in compliance with the principles indicated in article 5 paragraph 1 of GDPR, and in the ability of the owner to demonstrate that he has respected them. In fact, data protection does not only concern with the moment of violation but also with the whole management process of the data, starting from the collection and archiving phases. A first difficulty regards the possibility of identifying the figures that article 4, in points 7 and 8, defines as "holder of treatment" and "responsible of treatment"; the holder of treatment is intended as the natural or legal person, the authority public authority, the agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; the responsible of treatment is intended as the natural or legal person, public authority, agency or other body which processes personal data on behalf of the holder of treatment. The identification of a similar figure could be problematic if one thinks to a public blockchain[87], while it could be easier in a private permissioned blockchain or in DLT. In doctrine there have been several attempts to reconstruct a scheme of responsibility but to date it cannot be said that a unanimously recognized model has been found[88] [89]. Further problematic profiles could concern the storage, rectification and deletion of data[90]. The immutable nature of recorded data on blockchain could be a problem. With respect to article 5 of GDPR, it could however be argued that this type of conservation is necessary for the functioning of the architecture and therefore for the "achievement of the purposes". Looking to articles 16 and 17, the difficulty is due to the fact that, although it is possible for the user to request the insertion of updated data, since it is an append-only structure, this can only take place as a new registration without obtaining the deletion of existing data. From the smart contracts point of view, this requirement appears to be less problematic, concerning only the recording of the exercise of the functions and any events emitted. Worthy of attention is also the chapter V of GDPR which deals with the transfer of data to third countries. The above considerations apply again; the most problematic aspects are to be identified in the use of public blockchain networks, for which anyone can create a full node, and therefore contain the data that is recorded within the blockchain. With the resolution of 20th October 2020, the European Parliament invited the Commission «*to evaluate the development and use of distributed ledger technologies, including blockchains and, in particular, smart contracts*». The European Parliament recognized on that occasion the use of smart contracts and the lack of a legal framework; some first proposals were therefore presented, including the definition of rules regarding their use, the possibility of intervening in transactions in the event of suspicious financial transactions and specific protection measures for small and medium-sized enterprises. The resolution adopted by the European Parliament is part of the blockchain strategy. The European Commission has also established the "European Blockchain Observatory and Forum" pilot project, managed by the Directorate General for Communication Networks, Content and Technology, with the aim of: (i) accelerating the development of blockchain innovation in Europe; (ii) monitor blockchain initiatives in Europe; (iii) make recommendations on the role the EU could play in blockchain. Among the reports produced by the Blockchain Observatory and Forum, there is also a specific one on smart contracts of 2022. The document lists the benefits for the large-scale adoption of smart legal contracts compared to ordinary contracts; at the same time, it highlights its limitations and proposes solutions. In order to insert a smart legal contract into the blockchain, the report underlines the need for the legal language to be entirely translated into computer code. This could represent a problem when considering the fact that lawyers typically do not have the technical skills of code developers and viceversa. However, it is «*necessary to maintain a certain level of trust and competence to ensure that all parties can trust that the smart contract code truly reflects the content and legal purpose* [of the smart contract]»[91]. Among the critical issues, it emerges the difficulty of evaluating real world events; the report of 2022 identifies the oracle as a tool for connecting reliable data to the blockchain. Other critical issues are found with respect to cybersecurity and vulnerability to attacks, as well as to the risk of fraud and the field of privacy protection; the report proposes specific techniques to prevent operational risks, starting from security auditing tools estimates and attack simulation tests ("penetration tests"). The oracle has the purpose of guaranteeing the connection between what happens on the blockchain and what happens outside, "certifying" the originality and correctness of the data entered on the blockchain. In particular, in cases of the so-called oracle objective, the input provided by the oracle comes from a software or informatic tool, which postulates standard, simple and automatic transactions, dependent on the verification of an unquestionable objective fact (whether that fact A actually occurred, resulting in the event B). From a regulatory point of view, for the integration of smart legal contracts on a large scale, the report highlights the challenges posed for consumers by the language used, for which it seems useful: (i) to ensure the usability of the information, whatever the language applied and identify mechanisms that allow the legal position of the consumer to be taken into account; (ii) apply rigorous procedures and controls. Furthermore, given the semi-irreversible nature of recorded data in the blockchain, the correction of any error in the code can take time and be onerous. From a legal point of view, it is therefore necessary to bring the contractual meaning of specific legal concepts (e.g. good faith) to the attention of the contractor and leave room for flexibility.

On the 6th December 2022 the European Council reached an agreement for a general approach on that (negotiating mandate). On the 14th February 2023, the European Commission launched a regulatory "Sandbox" (European Blockchain Regulatory Sandbox) for innovative use cases involving distributed ledger technologies and/or blockchains. In essence, the Commission will make use of the operators to delve deeper into the technical aspects of these technologies, while the operators will contribute to identifying the best practices for the market, according to the participatory regulation process.

The AI act moves from the need of a key policy to promote the development and adoption of safe and lawful AI respecting fundamental rights[92] across the single markets. It went hand in hand with other initiatives, including the coordinated plan on AI, aiming to accelerate investment in AI in Europe. The agreement effectively addresses a global challenge in a rapidly evolving technological environment that affects a key sector for the future of european economies and societies[93]. The matter has been managed to maintain an extremely delicate balance between the opportunity to stimulate innovation and the adoption of AI across Europe, and the need to fully respect the fundamental rights of citizens. The main idea was to regulate the use of AI based on its ability to cause harm to society following a "risk-based" approach: the greater the risk, the more stringent the rules. As the first legislative proposal of its kind in the world, the AI act sets up a global standard for the regulation of in other jurisdictions, as the GDPR did[94]. To ensure that the definition of AI system provides sufficiently clear criteria to distinguish AI from simpler software systems, the compromise agreement aligns the definition with the approach proposed by the OECD. The AI act also clarifies that the regulation does not apply to areas which fall outside the scope of EU law and should not, in any case, affect Member States' competences in matters of national security or any entity competent in this area. Furthermore, the AI regulation will not apply to systems used exclusively for military or defense purposes. Similarly, the agreement provides that the regulation does not apply to AI systems used only for research and innovation purposes or to people who use AI for non-professional reasons. The compromise agreement establishes a horizontal level of protection, including a high risk classification, to ensure that AI systems that do not pose a risk of causing serious violations of fundamental rights or other significant risks are not included. AI systems that pose only limited risk would be subject to very light transparency obligations, such as disclosing that content was generated by AI, so that users can make informed decisions about further use. A wide range of high-risk AI systems will be subjected to a number of requirements and obligations to gain access to the EU market. These requirements have been clarified and adapted by the co-legislators, in such a way to make them more technically feasible and less burdensome for stakeholders, for example regarding data quality or in relation to the technical documentation that SMEs should draw up to demonstrate that their high-risk AI systems comply with the requirements. As AI systems are developed and deployed across complex value chains, the compromise agreement includes amendments that clarify the allocation of responsibilities and roles of various actors in such chains, in particular suppliers and users of AI systems. It also clarifies the relationship between responsibilities under the AI regulation and responsibilities already existing under other pieces of legislation, such as relevant EU data protection legislation or sectoral legislation. For some uses of AI, the risk is considered unacceptable and, than, such systems will be banned by the EU. The provisional agreement bans, for, example, cognitive behavioural manipulation, untargeted scraping of facial images from the Internet or CCTV footage, emotion recognition in the workplace and educational institutions, social scoring, biometric categorization to infer sensitive data and some cases of predictive policing for people. Taking into account the specificities of law enforcement authorities and the need to preserve their ability to use AI in their vital work, several amendments to the Commission proposal relating to the use of AI systems for law enforcement purposes have been agreed. Subject to appropriate safeguards, such changes aim to take into account the need to respect the confidentiality of sensitive operational data in relation to their activities. For example, an emergency procedure has been introduced that allows law enforcement authorities to use a high-risk AI tool that has not passed the conformity assessment procedure in case of urgency. However, a specific mechanism has also been established to ensure that fundamental rights are sufficiently protected from possible abuses of AI systems. Furthermore, as regards the use of real-time remote biometric identification systems in publicly accessible spaces, the provisional agreement clarifies the situations in which such use is strictly necessary for law enforcement purposes and law enforcement authorities should therefore be exceptionally authorized to use such systems. New provisions have been added to take into account situations where AI systems can be used for many different purposes (general purpose AI) and those where general purpose AI technology is subsequently integrated into another high-performance system risk. The provisional agreement also addresses specific cases of general purpose AI systems. Specific rules were also agreed for basic models, large systems capable of competently carrying out a wide range of distinctive tasks, such as generating video, text, images, speaking in lateral language, calculating data or the generation of computer codes. The provisional agreement stipulates that basic models must comply with specific transparency obligations before being placed on the market. A stricter regime has been introduced for "high impact" base models; these are basic models trained with large amounts of data and well above average advanced complexity, capacity and performance, which can spread systemic risks along the value chain. The AI act under publication[95] aims to promote the development and uptake of safe and trustworthy AI systems across the EU's single market, by both private and public actors, to ensure respect of fundamental rights of EU citizens and stimulate investment and innovation on AI in Europe. It confirms the regulation and supervision of artificial intelligence systems[96] subjected to sector regulations and related supervisory authorities. Among the requirements that the AI Act places for high-risk systems are data governance, automatic logging, risk management, transparency and human supervision requirements. In the context of smart contracts, it is significant the transparency requirement, functionally connected to the human supervision requirement. As for transparency, the AI Act requires that systems be structured in a way that allows users to «*understand and use the system appropriately*». Therefore, the AI Act requires the adoption of systems that allow "understanding" the logic behind a released output. Consequently, the transparency requirement places the burden on companies to choose the AI system to integrate into smart contracts on the basis of a cost-benefit analysis, which weighs the costs of the "obscurity" of the system against efficiency. The reference to "understandability" for the user contained in the regulation requires the knowledge of the system by a common subject/user. This involves linking the comprehensibility requirement with the context in which the model is used. However, the absence, in the AI Act, of a right to information directly actionable by the user, qualified for example as a right of access to information relating to the system used, prevents the user from having effective control over the information provided by the model for the purpose of its "understandability". The lack of individual transparency rights into the AI act can be filled, in cases of processing of personal data, by rights recognized pursuant to the GDPR. The articles 12-15 and 22 of the GDPR, in fact, provide specific access rights to «*significant information on the logic used*» in automated personal data processing systems. These rights apply, for example, to social scoring models used in the financial sector, which rely to a large extent on the processing of personal data. Following the new rules on general purpose AI models and the clear need for their application at EU level, an AI Office is established within the Commission to oversee these more advanced AI models, help promote testing standards and practices and enforce common standards across all Member States. An independent scientific panel of experts will advise the Office for AI on general purpose AI models, contributing to the development of methodologies for assessing the capabilities of underlying models, advising on the designation and emergence of high impact base and monitoring the possible material safety risks associated with the base models. The AI Committee, composed of representatives of Member States, will remain a coordination platform and advisory body of the Commission and will give an important role to Member States in the implementation of the Regulation, including the design of codes of good practice for basic models. Finally, a consultative forum for stakeholders, such as representatives of industry, SMEs, start-ups, civil society and academia, will be established to provide technical expertise to the AI Committee. Sanctions for violations of the AI Regulation are set as a percentage of the global annual turnover in the previous financial year of the offending company or, if higher, a pre-determined amount. This would amount to EUR 35 million, or 7% for breaches relating to prohibited AI applications, EUR 15 million or 3% for breaches of AI Regulation obligations and EUR 7.5 million or 1.5% for providing inaccurate information. However, the provisions provide for more proportionate ceilings for administrative sanctions for SMEs and start-ups. The compromise agreement also clarifies that a natural or legal person can submit a complaint to the relevant market surveillance authority regarding non-compliance with the AI Regulation and can expect that such complaint will be dealt in line with the specific procedures of that authority. The provisional agreement provides for a fundamental right impact assessment before a high-risk AI system is placed into the market. The regulation also provides for greater transparency regarding the use of high-risk AI systems. In particular, some provisions of the Commission proposal have been amended to indicate that certain users of a high-risk AI system who are public entities will also be required to register in the EU database for high-risk AI systems. Furthermore, new provisions place emphasis on the obligation for users of an emotion recognition system to inform natural persons when they are exposed to such a system. In order to create a more innovation-friendly legal framework and promote evidence-based regulatory learning, the provisions on measures to support innovation have been substantially changed compared to the Commission proposal. In particular, it is clarified that regulatory testing spaces for AI, which should create a controlled environment for the development, testing and validation of innovative AI systems, should also enable testing of innovative AI systems in real-world conditions. Furthermore, new provisions have been added that allow AI systems to be tested in real-world conditions, under specific conditions and safeguards. In order to ease the administrative burden on smaller businesses, the regulatory provisions include a list of actions to be taken to support such operators and provide for some limited and clearly specified exemptions. The AI act will apply two years after its entry into force, with some exceptions for specific provisions.

6. The on-going general regulatory process of smart contracts and debate in Italy

In Italy the smart contract regulation starts with the Law Decree n. 135/2018, better known as "simplification decree"[97], converted with modifications into the Law 11th february 2019, n. 12. The dictate of the art. 8-*ter*[98] presents some gaps and ambiguities which have attracted a wide debate in the italian context too[99]. To be schematic, the definition of the "tecnology based on distributed registers" (paragraph 1) concerns with the:

- register characteristics (*distributed*, *replicable*, *simultaneously accessible*, *architecturally decentralized register on a cryptographic basis*);
- possible actions with data (*both in clear text* or *further protected by encryption*);
- data characteristics (*verifiable by each participant*, non-alterable, non-modifiable).

It emerges that, for example, the character of "unchangeability" may result problematic for many aspects, if considering that the public blockchain can find difficult to ensure it absolutely (threshold of 51% of nodes), the possible conflict with the GDPR legislation, in particular with art. 17, providing for the right to obtain the cancellation of the communicated data.

The definition of the smart contract (paragraph 2) appears general, but in some way also generic. The definition only refers to the execution of the program, implicitely presupponing a preventive phase of formation of the agreement. The rule also qualifies the smart contract as binding the parties, leading many to believe that the legal source of the obligation is the smart contract itself. Some doctrine privileges the informatic interpretation of the term "execution", so that the smart contract can be the contract itself and not the (legal) execution of the willing expressed previously. Another problem[100] is that once the smart contract has been deployed it is immediately executed, at least in the part contained in the constructor. It will therefore be appropriate to pay particular attention during the development of the code to understand the exact moment in which the party is binding, always keeping in mind the content of the art. 1326 of the Civil Code (conclusion of the contract).

Particularly relevant is the so-called italian "Fintech Decree" implementing the EU Regulation n. 858/2022 (DLT Pilot Regime), which establishes a pilot regime for market infrastructures based on "Distributed Ledger Technology" and the simplification of Fintech experimentation. The provisions of the DLT Pilot Regime mainly introduce the necessary discipline for the issuance and trading of tokenized financial instruments. The possibility of tokenizing different types of goods, products or services and then generating a token in the virtual world and connecting it to a real good via a "smart contract"[101] could have a significant impact in terms of increasing speed and security, but also of reducing transaction costs. Specifically, the DLT Pilot Regime assumes smart contracts as one of the elements that the DLT market infrastructure can use in carrying out activities, and whose reliability must be guaranteed as much as continuity, transparency, availability, reliability and security of the services and activities that infrastructure managers offer through computing and cybernetic devices related to the use of their distributed ledger technology.

A prominent issue concerns the same legal nature of the instrument. Indeed, the second part of paragraph 2 establishes that «*Smart contracts satisfy the* *requirement of written form following informatic identification of the interested parties»*, according the specific requirements deriving to AgID (Agency for Digital Italy) guidelines which, however, are still in late. In absence of AgID guidelines, what validity can be attributed to the smart contract? It must be assumed left under discretionality? With respect to this, a view point comes from the *art. 20 - Validity and evidentiary effectiveness of electronic documents* - of the italian *digital administration code* of 2005[102] as modified by the Legislative Decree n. 179/2016. Generally, it is observed that smart contracts could not be qualified as contracts in a strictly legal sense, given that they present technical and technological peculiarities that do not allow the assimilation to the computerized or digitalized version of a contract. And indeed, in this case, the classic scheme of the contract concluded online between two subjects intermediated by a computer, where both parties mutually make declarations in human language, which are translated, first, into computer language, is not implemented and subsequently in human language for presentation to the other party. Rather, the definition pursuant to the Law Decree n. 135/2018 refers to a computer program that uses blockchain technology in order to allow the implementation of a contract already present upstream and to guarantee the production of stable effects to which the parties are bound. In particular, it can be noted how the identification of the contracting parties, based on the "pseudonymisation" mechanism typical of the blockchain, can be an obstacle to ascertaining the legal capacity of the party to the contract (with consequent possible cancellation); furthermore, the principle of "good faith" would not necessarily coincide with the literal execution of the transaction (qualitative evaluation pursuant to art. 1375 of the italian Civil Code), thus compromising coordination with civil law in the field of non-compliance; specifically, also regarding the interpretation of the wishes of the parties which cannot be seen in automatic fulfillment. In fact, in addition to part of the doctrine which states how the "tout court transposition" of the classic contractual case to that of the smart contract[103] can be defined as a "superficial and generalist" solution as it is contrary to the so-called principle of "technological neutrality" (according to which the legislator must not interfere in the development of a specific technology to favor it over others), the real critical issues are revealed in any interpretative forums regarding principles that are not easily (if not absolutely) convertible in software language, such as good faith, the principle of correctness, diligence, non-performance for just cause, the legal capacity of the parties and, in general, the so-called clauses. In reality, to exploit the potential of new technologies and, in particular of blockchain and smart contracts, it would be sufficient to simply create a closed system that maintains the "hierarchically superior" position of the public administration in order to constantly validate as certain and reliable the data present and the operations carried out in the system itself. The correlation between the transparency, certainty and immutability of data offered by blockchain technology makes the diffusion of the smart contract potentially relevant in the context of public administration action, as well as from a private point of view. We can, therefore, envisage a role for this technology, based on the already cited so-called principle "if this than that" (if this condition occurs, then do this), in the public administration sector, with the premise of their prior regulation aimed at producing legal effects similar to the figure of the traditional contract and, therefore, to define them as "smart legal contracts", as it would not seem to conflict with the private law capacity of public administrations (ex art. 1, paragraph 1-*bis* of Law n. 241/1990), regardless of the typical or atypical nature of the legal transaction (the art. 8-*ter* of Law Decree n. 135/2018 provides, indeed, the possibility of using technologies based on distributed registers). However, a critical issue in this aspect is illustrated by the European Parliament which notes that smart contracts, being devoid of «*flexibility and incapable of adapting to changing circumstances or to the preferences of the parties*», are insuitable to respond to all circumstances that, therefore, will necessarily require a further interpretation about the correct method[104] of application of the legal transaction; in fact, the code is simply too rigid to allow all contracts to be determined algorithmically. The appropriateness of the widespread meaning of "smart contracts" is consequently also called into question. Without prejudice to the possible future developments of the instrument in this sense, the expression, in fact, would presuppose an adaptive capacity, i.e. adaptation to evolving circumstances and contingencies, which smart contracts, however, do not possess. This is because the particular blockchain technology makes it impossible to alter and modify the transaction once the original instructions have been entered. Smart contracts do not allow any subsequent modification, nor do they allow any contingencies to be taken into account. Rather, they constantly refer to the instructions originally received, until the eventual occurrence of a “kill” instruction, which causes the contract to cease to be effective. Nonetheless, the use of smart contracts would guarantee advantages in terms of procedural guarantees such as transparency and traceability (as they are based on blockchain technology) and the automations could be used in those cases where the action of the public administration is bound by law or where the procedures are determined in ways and times that are not immediate (art. 32, paragraph 9, Law Decree n. 50/2016), so that the contract is automatically stipulated after a prescribed period of time. On the other hand, it is observed that, in principle, there are no impeding reasons to allow smart contracts to be used for the purposes of stipulating the contract. At the same time, however, problems of practicability arise, considering that, unlike the contract concluded online, which involves the translation by the computer of human language into computer language and back into human language, the parties should necessarily make use of blockchain technology, who only knows computer language. This, in other words, means that the parties should have specific technical-informatic knowledge and skills, not commonly possessed.

Although a structured intervention on the application level is not yet in force today, a first step in this direction was proposed by AgID with the drafting of “*Guidelines for the modeling of threats and identification of mitigation actions compliant with the principles of secure/privacy by design*”, and in particular in reference to the “*Secure design best practices for distributed ledger-based architectures*”. AgID proposes a high-level analysis of the integrity, availability and confidentiality requirements of a DLT system, with particular attention to the infrastructural components such as the network, the data structure and the consensus algorithms. These AgID guidelines identify smart contracts as the most critical component in the DLT field; however, they simply suggest a traditional secure-coding approach in software development, without delving into specific threats and vulnerabilities of smart contracts. In fact, in the recent intervention of 1th June 2023 in the field of surety guarantees, according to art. 26 of the Public Contracts Code[105] (Legislative Decree n. 36/2023)[106], the AgID published the provision that defines technical requirements and certification methods for digital procurement platforms[107]; in this provision, AgID recognizes among the conditions that surety platforms must use the writing of the surety guarantee by means of a smart contract. Also on this occasion, AgID provides a single condition concerning the characteristics that the subject must possess to issue surety guarantees, not also those dealing with the technology used. The only condition is that this operation is possible only by a person who is allowed to issue sureties, pursuant to Article 106, paragraph 3 of the Code, authorized to write in the distributed register, subject to electronic identification with a significant level of guarantee or high with reference to the eIDAS Regulation.

Paragraph 3 of the art. 8-*ter* also provides that - if the distributed registers comply with the technical standards identified by the Agency for Digital Italy - the storage of an informatic document through the use of distributed register technology «*produces the legal effects of temporal validation electronic information referred to in article 41 of the Regulation (EU) n. 910/2014 of the European Parliament and of the Council of 23 July 2014*» on electronic identification and trust services for electronic transactions in the internal market. According to the paragraphs 3, DLT technologies can be used for "electronic time validation", i.e. the so-called "notarization" of documents. This type of use is now common and there are many sites that provide this service for free or otherwise.

With respect to the paragraph 4, we fall into the same scenario waiting for the AgID guidelines.

The use of blockchain then seems particularly suitable for pursuing those specific institutional purposes for which transparency has recently taken on a new value: the reference, obviously, is to the legislation aimed at preventing and combating corruption phenomena, starting from the Law. n. 190/2012 and by the Legislative Decree n. 33/2013, the so-called consolidated law on transparency (as well as, subsequently, by the Legislative Decree no. 97/2016 - FOIA, and the ANAC[108] guidelines on the implementation of the obligations of advertising, transparency and dissemination of information contained in the Legislative Decree n. 33/2013, amended by the same Legislative Decree no. 97/2016): the use of "closed" transactions, which cannot be influenced or altered by external parties, would represent a Copernican revolution for the anti-corruption galaxy (already in 2019, the OECD Global Anti-corruption & Integrity forum identified the centralization of power - and the possibility of its misuse - as the most favorable preconditions for the birth and spread of the corruption phenomenon). Decentralized nodes would make the process impervious to external infiltration, as well as certified and *ex post* immutable: all characteristics that have led some to rename the blockchain as “Technology of “rust”. It seems natural, then, that among the most promising uses of blockchain there are those connected to the protection of the authenticity of the certification and traceability processes of the supply chain, also with regard specifically to the protection of what is “Made in Italy” (where the role of citizen trust- consumer is of extreme relevance): the first pilot project inaugurated by the italian Ministery of Economic Development - dated 2019 - expressly specifies the importance of the segregation of access and encryption techniques to «*prevent unauthorized access to the network*» and, at the same time, identifies the origin - and therefore the history - of the various assets, guaranteeing immutability and a Ground Truth to the entire process. Integrity and traceability of the transfer of information could also be used for publicly available procedures, such as those provided for by the Public Contracts Code. The direction taken by the legislator through the Procurement Code is - clearly - an ever-increasing search for transparency, precisely as a barrier and contrast to any corruption phenomena. The mechanisms of the blockchain, including the recognition and mandatory validation of each transaction, would not only allow a high degree of security - and therefore trust, and *ex ante*, but also be able to ensure, *ex post*, traceability and verifiability of the individual acts and individual phases of the public procedure, instantly determining, at the very moment of carrying out the operation, its immutability. They would gain, to an extent certainly unprecedented compared to the past, the genuineness of the procedure for choosing the contractor and evaluating the offer (which, let us remember, would be incorruptible and unchangeable), thus also impacting the discretion of the choice (and, therefore, on the possible concussive-corruptive conduct of the human agent). Similar blockchain development opportunities are already part of the IBSI (Italian Blockchain Service Infrastructure), in addition to others - such as the digital management of public certificates - and it is therefore reasonable to expect more marked and, above all, widespread future development on a large scale. But the use of blockchain technology is not limited to the pursuit of general interests only in the phase of identifying the contractor and can actually favor the quality of the administrative action[109], also in the subsequent phase of the conclusion of the contract with the public administration, through smart contracts (to which the Strategy of the italian Ministery of Economic Development also makes specific reference in the section dedicated to the IBSI). The express regulatory recognition of smart contracts, which initially occurred through art. 8-ter par. 2 of the Legislative Decree n. 135/2018, certainly represents a first, important manifestation of the legislator's openness to the new possibilities offered by the technological tool, confirming the opportunity of a generalized appeal; one would refer to the contraction of transaction times or the revisiting of the role carried out by the parties in developing the content of the contract; or again, for example, to any disputes in the execution of the contract, the - immediate - resolution of which would be entrusted to the informatic protocol and not (anymore) to the decision of the parties or, even, of an external party (above all, an arbitration or a Court). Of course, a smart contract should by its nature also include extra-informatic clauses, capable of covering the unforeseeable (the need for an analogical interpretation, in short, would not disappear *tout court*), but it is also true that the contractual risk would be reduced to a minimum (to the benefit of the speed and certainty of the operation, as well as a clear reduction in its hidden costs).

One main pending question runs between “smart legal contract” and “smart contract”.

As it overall emerges, the actual Italian legislation framework with implications on the use of smart contracts is at some starting point, with lack of detailed rules, laying the foundations for experiments, bringing to light the critical issues that the law will have to deal with.

7. Final considerations

Accordingly to literature deliverables, the upgraded features and the potentialities of the blockchain DLT encourage the effort in promoting smart contracts implementation into public services in the perspective of their resilience and adaptation to communities and markets demand and sustainable development.

It also arises from literature that blockchain-based smart contracts could, in presence of standardised rules, generally improve public services addressed to the healthcare and agrifood sectors[110]. In addition, blockchain-based smart contracts tools are expected to strengthen in the near future by the confluence of AI algorithms expertise and flexibility.

In Italy, as at EU level, the regulation path of smart contracts is still under way and appears characterised by complexity, even in doctrinal framing, because of the various interacting aspects posed by the on-going widespread digital transition[111], which certainly pertains also the public services. The administrative law issues concerning public services in the analysed sectors, i.e. with respect to the management of data and information as well as *transparency* in a broad sense, remain fundamental nodes from the regulatory point of view in order to guaratee effectively both public and private interests.

Relying on the computer code rather than on the fulfillment of the parties potentially generates significant advantages, such as the elimination of the risk of non-compliance, the use of intermediaries, the reduction of times and costs. According to the characteristics of immutability, confidentiality, traceability and transparency of blockchain coupled with the automation that smart contracts imply, it makes contracting procedures in the public sector the potential ideal field of implementation, which if, from one hand, would not eliminate corruption risks (which may affect different procedures, i.e. public procurement), would, from the other hand, allow its early detection so that corrective and preventive measures can be taken[112].

Exploiting the potential advantages offered by smart contracts requires the resolution of various legal issues. The definition of smart contract in the italian law (art. 8-ter of the Law Decree n. 135/2018, converted in Law n. 12/2019), which refers to the execution capable of automatically "binding" two or more parties on the basis of the effects predefined by themselves, opens, first of all, a controversial issue regarding the framework, the nature and the legal qualification of smart contracts, arising directly from the relationship that links the legal agreement to the computer code. Further legal problems emerge as arising from the coordination of smart contracts with the reference discipline, for example regarding the equivalence with real contracts and compliance with civil law. The fact that the smart contract configures an IT document entails the difficulties of conciliation with the rules posed by the positive law at European and national level, such as the EU eIDAS regulation n. 910/2014, the civil code, the Legislative Decree n. 82/2005 (Digital Administration Code) and the related technical rules. For example, a problem, related to the smart contract expression of a will, can be identified in the identification of the contracting parties, in the light of the operating mechanism of the blockchain, which is based on the "pseudonymization" of the subjects, and the legal requirements of the contract (the risk seems to remain that the subject is not who he claims to be and, therefore, of not being able to verify the capacity to act, which would lead to the annulability of the contract itself). The italian law does not neglect this problem, which it attempts to address by the procedure dictated by the AgID guidelines; however, significant gaps remain when moving from *permissioned blockchains*, where participants are previously identified, to *permissionless blockchains*; this highlights the need for an adequate preventive, proactive and technical approach, as required by the same EU regulation n. 679/2016 (GDPR); the preventive action on the technological architecture could allow adapting some distinctive characteristics of the blockchain, such as disintermediation and immutability, in order to respect the principles of personal *data protection*. Likewise, a need for "algorithmic transparency" emerges, which imposes to the owner the duty to govern the algorithm and the logical structures of its functioning to deal with legitimate requests for knowledge of rights by users according to the right to know, understanding and reviewing as well as contesting the system, ensuring conscious self-determination, the real possibility of control and authentic freedom of choice; this introduces the need to embrace a logic of *accountability* and responsibility of the subjects who manage the technologies, accompanied by the definition of the respective responsibilities, attention to safety, effectiveness (also of the related sanctionatory system), in the wake of the EU regulation n. 679/2016 (GDPR) regarding *data protection*. In the implementation phase, smart contracts, understandable to those who know the programming language, can create a sort of semantic barrier and raise problems of understanding and intelligibility of the content not only for the parties themselves, but also for a possible judge, who would need "an interpreter" to know its contents. Furthermore, the difficult transposition of contractual clauses into machine language also determines the concrete possibility that divergences may occur between the agreement (and the related will of the parties) and the translation into the algorithm, generating possible consequent defects. This aspect highlights the need for solid transversal legal and IT skills to be able to translate legal conditions into computer code and highlights the need and at the same time the danger of the simplification, required by the programming language, of complex clauses, with the real risk of undesidered or erroneous results. In these respects, the advantage of blockchain technology, consisting, among other things, in the elimination of intermediaries, could be significantly reduced by the help of third parties, with not only IT skills, in whom to place trust. On the other hand, the application of the tools relating to the negotiation phase, such as the defects of consensus, also appears to be critical. The use of the blockchain smart contract tool, eventually assisted by artificial intelligence algorithms, highlights the complex relationship between law and technology and the related need for an evolution of legal regulation, through the strengthening of principles, rules and remedies in technology, as in a "technical law". The absence of territorial barriers, as generally happens for the State in a technological society[113], means that the responses from a legal and administrative point of view cannot be limited to national borders, but must, in parallel with the matters they are called to regulate, take some supranational *governance* in order to be fully effective and not otherwise generate tensions between the global dimension of the issues and the territorial specificity of the rules.

The use of algorithms, especially of last generation as in the case of artificial intelligence, must fully comply with the principles that inform the reference legislation for the protection of rights, such as *data protection*, as well as the regulatory criteria that guide the public action in the field of administrative procedures, digital administration, *transparency*, *traceability*, *access to information and data*, particularly relevant either in the health sector[114] or the agriculture and agrifood one[115]. When introducing blockchain tecknology in the administrative procedures of the public sector, it requires its detailed analysis and to be preceeded by a review of the procedures on which they operate, a reflection on their needs and an assessment of the margins of simplification. Also, the question of the infrastructure on which the blockchain smart contract will be deployed should be addressed, but taking the different administrative levels into account[116].

More in general, it emerges from the analysis so far carried out that the on-going efforts to establish effective standards-supported regulations, at EU and national level, must compare with the difficulties deriving from the high speed of technological innovation and the parallel need to keep the evolving legal and administrative aspects under armonic, secure, transparent and efficient control. The most recent evolution of the troubled relationship between blockchain technology and Public Administration is only at the beginning and, despite being rooted on a regulatory basis, which could constitute a significant turning point, it already promises to be extremely challenging[117]. The challenge concerning the "new" digital administration also lies in the search of the right balance between the push towards the integral transfer of administrative functions to algorithmic automation[118] and the opportunity for technology to represent just an useful tool to support and improve ordinary administrative activities[119].

1. The work was funded by the Next Generation EU - Italian NRRP, Mission 4, Component 2, Investment 1.5, call for the creation and strengthening of Innovation Ecosystems, building "Territorial R&D Leaders" (Directorial Decree n. 2021/3277) - project Tech4You - Technologies for climate change adaptation and quality of life improvement, n. ECS0000009, Spoke 3 - PP 3.4.3 -Action 5.
2. R. Cavallo Perin – D. U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, Giappichelli, 2020, *passim*.
3. Law 7 August 1990, n. 241 - *New rules regarding administrative proceedures and right of access to administrative documents*.
4. Legislative Decree 3 February 1993, n. 29 - *Rationalization of the organization of public administrations and revision of the regulations regarding public employment, in accordance with article 2 of law 23 October 1992, n. 421*.
5. Directive of the President of the Council of Ministers 27 January 1994 - *Principles on the provision of public services*.
6. Law 11 July 1995, n. 273 - *Conversion into law, with amendments, of the legislative decree of 12 May 1995, n. 163, containing urgent measures for the simplification of administrative procedures and for the improvement of the efficiency of public administrations*.
7. Law 15 March 1997, n. 59 - *Delegation to the Government for the attribution of functions and tasks to the regions and local authorities, for the reform of public administration and administrative simplification*.
8. Law 11 February 2005, n. 15 - *Amendments and additions to the law of 7 August 1990, n. 241, concerning general rules on administrative action*; according to the art. 3-*bis*, *«to achieve greater efficiency in their activities, public administrations operate by informatic and telematic tools, in internal relations, between the various administrations and between these and private individuals»*.
9. Legislative Decree 7 March 2005, n. 82 - *Code of digital administration*.

10. Legislative Decree 14 march 2013, n. 33 - *Reorganization of the regulations concerning the right of civic access and the obligations of publicity, transparency and dissemination of information by public administrations*.
11. Legislative Decree 25 May 2016, n. 97 - *Review and simplification of the provisions on the prevention of corruption, publicity and transparency, corrective of the law 6 November 2012, n. 190 and the legislative decree of 14 March 2013, n. 33, pursuant to article 7 of law 7 August 2015, n. 124, regarding the reorganization of public administrations*.
12. G. Gardini, *La nuova trasparenza amministrativa: un bilancio a due anni dal "FOIA Italia"*, in *federalismi.it*, 19, 2018, p. 3.
13. F. Fracchia, P. Pantalone, *Verso una contrattazione pubblica sostenibile e circolare secondo l'Agenda ONU 2030*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 2-3, 2022, pp. 243-264, aims to capture the relevance of public procurement for the implementation of the 2030 Agenda for Sustainable Development, taking into account the transformation of the development model constituted by the ecological transition. Using this functional approach, in fact, public procurement may both represent «*a tool for achieving the goals of sustainability (not only environmental) embodied by the legal system at the various international, European and national levels (think, among others, of the National Recovery and Resilience Plan-NRRP) and be itself "sustainable" regardless of the goal it sets out to achieve*».
14. G.L. Albano, R. Cavallo Perin, G. M. Racca, *Public contracts and international public policies against corruption*, in *Transnational Law of Public Contracts*, edited by M. Audit, S. W. Schill, vol. 20, Bruxelles, Bruylant, 2016, 845-878.
15. A. G. Orofino, F. Cimbali, *L'uso delle tecniche informatiche nella prestazione di servizi pubblici*, in *Giurisprudenza italiana*, 6, 2022, pp. 1523-1527.
16. Law 7 August 2015, n. 124 - *Delegation to the Government regarding the reorganization of public administrations*.
17. Legislative Decree 13 December 2017, n. 217 - *Supplementary and corrective provisions to the legislative decree of 26 August 2016, n. 179, concerning amendments and additions to the Digital Administration Code, pursuant to Legislative Decree 7 March 2005, n. 82, pursuant to article 1 of law 7 August 2015, n. 124, regarding the reorganization of public administrations*.
18. Law Decree 16 July 2020, n. 76 - *Urgent measures for simplification and digital innovation*.
19. Law Decree 31 May 2021, n. 77 - *Governance of the National Recovery and Resilience Plan and first measures to strengthen administrative structures and accelerate and streamline procedures*.
20. Law 29 July 2021, n. 108 - *Conversion into law, with amendments, of the legislative decree of 31 May 2021, n. 77, containing governance of the National Recovery and Resilience Plan and first measures to strengthen administrative structures and accelerate and streamline procedures*.
21. D. U. Galetta, *Transizione digitale e diritto ad una buona amministrazione: fra prospettive*

aperte per le Pubbliche Amministrazioni dal Piano Nazionale di Ripresa e Resilienza e problemi ancora da affrontare, in *federalismi.it*, 7/2022, pp. 103-125, «*after considering the steps needed to reach the goal of digitalizing Public Administration, the analysis aims to verify whether and to what extent a public administration that makes use of ICT is (or could be) a better public administration in the sense of better responding to that right to a good administration referred to in art. 41 of the Charter of Fundamental Rights of the European Union and what role the National Recovery and Resilience Plan could play in this perspective*».

22. N. Szabo, *Smart Contracts: formalizing and securing relationships on public networks*, in *First Monday*, Volume 2, Issue 9, September, 1997, *passim*.
23. J.A. Triana Casallas, J.M. Cueva Lovelle, J.I. Rodriguez Molano, *Smart contracts with blockchain in the public sector*, in *International Journal of Interactive Multimedia and Artificial Intelligence*, volume 6, n. 3, 2020; G. Gallone, *Public administration and the challenge of contractual automation. Notes on smart contracts*, in *European Review of Digital Administration and Law*, Volume 1, Issue 1-2, June-December, 2020; F.C. Iaione, F. Da Silva Ranchordas, S. Hina, *Smart public law. Automation and decentralisation of public power: smart contracts and the blockchain as stepping stones for a digital and polycentric good administration?*, in *Italian Journal of Public Law*, Issue 2, 2021, pp. 1-32; P. La Selva, *Blockchain e smart contracts nella pubblica amministrazione: aspetti di un tentativo di digitalizzazione del settore pubblico*, in *Amministrativ@mente*, Issue 2, 2022, pp. 279-313; N.A. Sava, D. Dragos, *The legal regime of smart contracts in public procurement*, in *Transylvanian Review of Administrative Sciences*, Issue 66 E, June, 2022, pp. 99-112, doi: 10.24193/tras.66E.6.
24. S. Licciardello, *Profili della più recente evoluzione dei servizi pubblici locali*, in *Il Diritto della Regione*, 3-4, 2005, pp. 335-359.
25. M.T. P. Caputi Jambrenghi, G. Colella, *PPI for a sustainable economy: sustainable supply chain management in the agri-food sector*, in *Il diritto dell'economia*, 66, 3, 2020, n. 103, pp. 207-228, offers an analysis on the agri-food logistic chains with respect to the sustainability of management practices. The use of management and marketing tools and innovative legal and economic institutes, also in the agri-food sector, is fundamental to guarantee an increasingly "cleaner" agriculture. The creation of a network of companies through EU partnerships for innovation, aiming to provide companies in the agri-food supply chain with a high level of methodological and organizational innovation, makes it possible to draw guidelines relating to the development of territories through the use of public procurement for innovation.
26. *Health at a Glance: Europe 2020. State of health in the EU cicle*, Report OECD/European Union, 2020.
27. ISMEA - Istituto di Servizi per il Mercato Agricolo alimentare, *Rapporto sull'agroalimentare italiano, 2023.*
28. K. Lee, Z.L. Brumme, *Operationalizing the One Health approach: the global governance challenges*, in *Health Policy and Planning*, 28, 2013, pp. 778-785,

doi:10.1093/heapol/czs127.

29. A. Micello, *La tecnologia "blockchain" al servizio della gestione delle informazioni ambientali: verso un "Blockchained Green Public Procurement"?*, in *Rivista quadrimestrale di Diritto dell'Ambiente*, 3/2018, pp. 83-108, highlights the blockchain's potentialities in environmental data management. Legal arrangements of administrative documents digitization are firstly analyzed, highlighting the lack of instruments for environmental data dematerialization. The potential of environmental protection through the reference to experiences from other countries is tested. Lastly the possibilities of a blockchain-integrated Green Public Procurement for environmental management are shown, also through smart contracts.
30. G. Lofaro, *Innovación, digitalización y sostenibilidad de la salud pública entre el aprendizaje automático y el suave empujón (Innovation, digitalization and sustainability of public health between machine learning and nudging)*, in *Revista de la Facultad de Derecho de México*, 73(285), 31-60, Enero-Abril 2023, https://doi.org/10.22201/fder.24488933e.2023.285.85382.
31. X.-N. Zhou, M. Tanner, *Science in One Health: A new journal with a new approach* - Editorial, in *Science of One Health* - Elsevier (2022), doi.org/10.1016/j.soh.2022.100001.
32. V. Charles, A. Emrouznejad, T. Gherman, *A critical analysis of the integration of blockchain and artificial intelligence for supply chain*. In Annals of Operations Research,2023, 327:7-47, doi.org/10.1007/s10479-023-05169-w.
33. D. U. Galetta, G. Pinotti, *Automation and algorithmic decision-making systems in the italian Public Administration*, in *CERIDAP*, *Rivista Interdisciplinare sul Diritto delle Amministrazioni Pubbliche*, 1/2023, pp. 13-23. The Authors aim at analysing the decision-automation systems currently used by public administrations in Italy. After an overview of the legal framework, the different systems are classified and illustrated. The conclusions dwell on the reason for the scarce use of these tools in the Italian landscape, also due to the slow and uneven digitisation of the public sector. See also F. Fracchia, *Lo spazio della pubblica amministrazione. Vecchi territori e nuove frontiere. Un quadro d'insieme*, in *Il diritto dell'economia*, 2, 2023, pp. 247-303.
34. C. Robustella, C. E. Papadimitriu, *Spunti ricostruttivi in tema di "smart contracts", tra innovazione tecnologica e regola giuridica*, in *P.A. Persona e Amministrazione*, 1, 2022, pp. 963-995.
35. F. Di Ciommo, *"Blockchain, smart contract", intelligenza artificiale (AI) e "trading" algoritmico: ovvero, del regno del non diritto*, in *Rivista degli infortuni e delle malattie professionali*, 1, 2019, 1, pp. 1-36.
36. G. Remotti, *Possibili funzioni ausiliarie delle tecnologie "blockchain" per marchi e indicazioni di origine: tracciabilità della filiera agroalimentare, dinamica competitiva e meccanica mercantile*, in *MediaLaws*, 3, 2021, pp. 29-52.
37. W. D'Avanzo, "*Blockchain" e "smart contracts" per la gestione della filiera agroalimentare. Potenzialità, progetti e problemi giuridici dell'internet del valore*, in *Diritto agroalimentare*, 1, 2021, pp. 93-118.

[38] G. Gallone, *La pubblica amministrazione alla prova dell'automazione contrattuale. note in tema di "smart contracts"*, in *federalismi.it*, 20, 2020, pp. 142-170.

[39] G. Bottino, *Economicità, efficacia ed efficienza dell'azione amministrativa*, in *Lezioni di cultura amministrativa* (edited by), V. Italia, 2, Milano, Franco Angeli, 2004 - ISBN 88-464-6253-X. - pp. 247-260.

[40] C. Suraci, V. De Angelis, G. Lofaro *et al.*, *The next generation of eHealth: A multidisciplinary survey*, in *IEEE Access*, vol. 10, pp. 134623-134646, 2022, in https://ieeexplore.ieee.org/document/9996365.

[41] K.N. Griggs, O. Ossipova, C.P. Kohlios, A.N. Baccarini, E.A. Howson, T. Hayajneh, *Healthcare blockchain system using smart contracts for secure automated remote patient monitoring*, in *Journal of Medical Systems*, 2018, 42, pp. 42-130.

[42] *Law 31th May 2022, n. 62 - Provisions regarding the transparency of relationships between manufacturing companies, entities operating in the health sector and healthcare organisations.*

[43] E. Carloni, *Misurare la corruzione? Indicatori di corruzione e politiche di prevenzione*, in *Politica del diritto*, 3, 2017, pp. 445-466, doi: 10.1437/88492.

[44] According to art. 2 of the Law n. 62/2022 «*any entity, including those belonging to the third Sector, which, directly or in the role of intermediary or associated company, carries out an activity aimed at the production or marketing of medicines, instruments, equipment, goods or services, including non-healthcare services, including nutritional products, marketable in the field of human and veterinary health, or the organization of conferences and congresses regarding the same objects*».

[45] According to art. 2 of the Law n. 62/2022 «*subjects belonging to the healthcare or administrative area and other subjects who operate, in any capacity, within a healthcare organisation, public or private, and who, regardless of the position held, exercise responsibility in the management and allocation of resources or intervene in decision-making processes regarding drugs, devices, technologies and other goods, including non-healthcare ones, as well as research, experimentation and sponsorship. The professionals registered in the mandatory national register of members of the judging commissions in the procedures for awarding public contracts, referred to in Article 78 of the code referred to in Legislative Decree 18th April 2016, n. 50, managed by the National Anti-Corruption Authority, and selectable for public procedures for the purchase and production of goods and services in the healthcare sector*».

[46] According to art. 2 of the Law n. 62/2022 «*local health authorities, hospitals, university hospitals, scientific hospitalization and treatment institutes and any public or private legal entity that provides health services, university departments, specialization schools, public and private research institutes and associations and scientific societies in the health sector, professional associations of health professions and associations of health professionals, even those without legal personality, public and private entities that organize continuing medical education activities as well as companies, patient associations, foundations and other bodies established or controlled by the subjects referred to in this letter or who control them or hold*

ownership of them or who perform the role of intermediation for the aforementioned healthcare organisations».

47. Agreements and distributions, such as transactions in money, goods, services or other benefits made in favor of individuals operating in the health sector or healthcare organisations (in particular, transactions must be communicated if they exceed a certain economic threshold: over 100 euros - or an overall annual value greater than 1,000 euros - for individuals in the healthcare sector and over 1,000 euros for healthcare organizations - or an overall annual value greater than 2,500 euros); agreements between manufacturing companies and entities in the Health sector or Health organisations (these agreements will include direct or indirect benefits such as participation in conferences, training events, committees, consultancy, teaching or research); shareholdings: identification data of the individuals and healthcare organizations that hold shares, quotas or bonds of a manufacturing company; proceeds deriving from industrial or intellectual property rights: fees (and other forms of economic benefit) that healthcare individuals and organizations receive from a producing company.
48. The omission regarding «agreements, payments of money, goods, services or other utilities» is subject to an administrative sanction of 1,000 euros, increased by twenty times the amount of the payment to which the omission refers; the omission regarding «*shareholdings, bonds and proceeds from industrial or intellectual property rights*» is subject to a administrative sanction of 5,000 to 50,000 euros; if the communication contains "false" information, the administrative sanction may range from 5,000 to 100,000 euros.
49. In particular: the obligation to communicate «*agreements, payments of money, goods, services or other benefits*» will apply «*starting from the second semester following the one in progress on the date of publication of the notice provided for by article 5, paragraph 1*»; the obligation to communicate «*shareholdings, bonds and proceeds deriving from industrial or intellectual property rights*» will apply «*starting from the second year following the one in progress on the date of publication of the notice provided for by article 5, paragraph 1*».
50. R. Cavallo Perin, voce *Agricoltura*, in *Enciclopedia del Diritto*, Milano, Giuffrè, 2022, 24-46.
51. A. Lajoie-O'malleya, K. Bronsona, S. Van Der Burgb, L. Klerkxc, *The future(s) of digital agriculture and sustainable food systems: An analysis of high-level policy documents*, in *Ecosystem Services*, 2020, 45, 1011, doi.org/10.1016/j.ecoser.2020.101183. H. Barret, D.C. Rose, *Perceptions of the fourth agricultural revolution: what's in, what's out, and what consequences are anticipated?*, in *Sociologia Ruralis*, Vol. 62, Issue 2, April 2022, doi: 10.1111/soru.12324.
52. S. Fielke, B. Taylor, E. Jakku, *Digitalisation of agricultural knowledge and advice networks: A state-of-the-art review*, in *Agricultural Systems*, 2020, 180, 1027, doi.org/10.1016/j.agsy.2019.102763.
53. X. Pham, M. Stack, *How data analytics is transforming agriculture*, in *Business Horizons*, Volume 61, Issue 1, January-February, 2018, pp. 125-133,

doi.org/10.1016/j.bushor.2017.09.011.

54. COPA-COGECA (2016), *Main principles underpinning the collection, use and exchange of agricultural data*, in *https://ec.europa.eu/futurium/en/system/files/ged/main_principles_underpinning_the_collection_use_and_exchange_of_agricultural_data_.pdf*
55. S. Rotz, E. Duncan, M. Small, J. Botschner, R. Dara, I. Mosby, M. Reed, E.D.G. Frase, *The politics of digital agricultural technologies: A preliminary review*, in *Sociologia Ruralis*, Vol. 59, Issue 2, April 2019, doi:10.1111/soru.12233.
56. E. Jakku, B. Taylor, A. Fleming, C. Mason, S. Fielke, C. Sounness, P. Thorburn P., *If they don't tell us what they do with it, why would we trust them? Trust, transparency and benefit-sharing in Smart Farming*, in *NJAS - Wageningen Journal of Life Sciences*, 2019, 90-91, 1002, doi.org/10.1016/j.njas.2018.11.002.
57. M. Busse, A. Doernberg, R. Siebert, A. Kuntosch, W. Schwerdtner, B. Konig, W. Bokelmann, *Innovation mechanisms in German precision farming*, in *Precision Agriculture*, 15, 2014, pp. 403–426, doi 10.1007/s11119-013-9337-2.
58. R. Birner, T. Daum, C. Pray, *Who drives the digital revolution inagriculture? A review of supply-side trends, players and challenges,* in *Applied Economic Perspectives and Policy -* Wiley, 43, 2021, pp. 1260–1285, doi:10.1002/aepp.13145.
59. L. Wiseman, J. Sanderson, A. Zhang, E. Yakku, *Farmers and their data: an examination of farmers' reluctance to share their data through the lens of the laws impacting smart farming*, in NJAS - *Wageningen Journal of Life Sciences*, 2019, pp. 90-91 - Elsevier, doi.org/10.1016/j.njas.2019.04.007; A. Regan, *"Smart farming" in Ireland: a risk perception study with key governance actors*, in NJAS - *Wageningen Journal of Life Sciences*, 2019, doi:10.1016/j.njas.2019.02.003.
60. C. Eastwood, L. Klerkx, R. Nettle*, Dynamics and distribution of public and private research and extension roles for technological innovation and diffusion: Case studies of the implementation and adaptation of precision farming technologies*, in *Journal of Rural Studies* – Elsevier, 2017, 49, pp. 1-12, doi.org/10.1016/j.jrurstud.2016.11.008.
61. M.-H. Ehlers, R. Huber, R. Finger, *Agricultural policy in the era of digitalisation,* in *Food Policy*, 2021, 100, 102019, doi.org/10.1016/j.foodpol.2020.102019.
62. M. Kukk, A. Poder, A. Viira, *The role of public policies in the digitalisation of the agri-food sector. A systematic review*, in NJAS: *Impact in Agricultural and Life Sciences*, 2022, 94, 1, 217-248, doi.org/10.1080/27685241.2022.2147870.
63. M. Tripoli, J. Schmidhuber, *Emerging opportunities for the application of blockchain in the agri-food industry*. FAO and ICTSD: Rome and Geneva, 2018, Licence: CC BY-NC-SA 3.0 IGO.
64. F. Antonucci, S. Figorilli, C. Costa, F. Pallottino, L. Raso, P. Menesatti, *A review on blockchain applications in the agri-food sector*, in *Journal of the Science of Food and Agriculture*, 2019, 99:6129-6138, doi10.1002/jsfa.9912.
65. A. Shahid, A. Almogren, N. Javaid, F.A. Al-Zahrani, M. Zuair, M. Alam, *Blockchain-based agri-food supply chain: a complete solution*, in *IEEE Access*, April 2020,

doi10.1109/access.2020.2986257.

66. Regulation (EC) n. 178/2002 of the European Parliament and of the Council of 28th January 2002 that add *the general principles and requirements of food law*, establishes the Authority of the European Union for food safety and establishes *procedures in the field of food safety*.
67. Commission Implementing Regulation (EU) n. 931/2011 of 19th September 2011 on the traceability requirements set by *Regulation (EC) N. 178/2002 of the European Parliament and of the Council for food of animal origin*.
68. Regulation (EU) n. 1169/2011 of the European Parliament and of the Council of 25th October 2011 *on the provision of food information to consumers, amending Regulations (EC) n. 1924/2006 and (EC), n. 1925/2006 of the European Parliament and of the Council, and repealing Commission Directive 87/250/EEC, Council Directive 90/496/EEC, Commission Directive 1999/10/EC, Directive 2000/13/EC of the European Parliament and of the Council, Commission Directives 2002/67/EC and 2008/5/EC and Commission Regulation (EC) n. 608/2004*.
69. Commission Regulation (EU) n. 16/2012 of 11th January 2012 amending Annex II to Regulation (EC) n. 853/2004 of the European Parliament and of the Council as regards *the requirements concerning frozen food of animal origin intended for human consumption*.
70. E. Fripp, J. Gorman, T. Schneider, S. Smith, J. Paul, T. Neeff, F. Marietti, L. Vary, A. Zosel-Harper, *Traceability and transparency in supply chains for agricultural and forest commodities: a review of success factors and enabling conditions to improve resource use and reduce forest loss*, in *Report of World Resources Institute* - Washington DC, Version 1, October 2023, pp. 1-189, doi.org/10.46830/wrirpt.22.00156.
71. United Nations Development Programme - UNDP, Global Center for Technology Innovation and Sustainable Development- Singapore*, Blockchain for agri-food traceability*, 2021, p. 38.
72. T. Timucin, S. Birogul, *A survey: making "smart contracts" really smart*, in *Transactions on Emerging Telecommunications Technology*, 2021, 32:e4338, doi.org/10.1002/ett.4338.
73. S. Badruddoja, R. Dantu, Y. He, K. Upadhayay, M. Thompson, *Making smart contracts smarter*, in *Proceedings of IEEE International Conference on Blockchain and Cryptocurrency*, 2021, doi: 10.1109/ICBC51069.2021.9461148.
74. B.D. Deebak, F. Al-Turjman, *Privacy-preserving in smart contracts using blockchain and artificial intelligence for cyber risk measurements*, in *Journal of Information Security and Appliations*, 2021, 58, doi.org/10.1016/j.jisa.2021.102749.
75. M. Krichen, *Strengthening the security of smart contracts through the power of artificial intelligence*, in *Computers*, 2023, 12, 107. https://doi.org/10.3390/computers12050107.
76. V. Papadouli, V. Papakonstantinoub, *A preliminary study on artificial intelligence oracles and smart contracts: A legal approach to the interaction of two novel technological breakthroughs*, in *Computer Law and Security Review*, 2023, 51, doi.org/10.1016/j.clsr.2023.105869.
77. Council of the European Union, *Artificial intelligence (AI) act: Council gives final green*

light to the first worldwide rules on AI, in *Press Release General Secretariat of the Council of the EU* n. 409/24 of the 21th May 2024, Brussels, https://www.consilium.europa.eu/en/press/press-releases/2024/05/21/artificial-intelligence-ai-act-council-gives-final-green-light-to-the-first-worldwide-rules-on-ai/; «*The adoption of the AI act is a significant milestone for the European Union. This landmark law, the first of its kind in the world, addresses a global technological challenge that also creates opportunities for our societies and economies. With the AI act, Europe emphasizes the importance of trust, transparency and accountability when dealing with new technologies while at the same time ensuring this fast-changing technology can flourish and boost European innovation*».

78. Proposal 21.4.2021 COM(2021) 206 final 2021/0106 (COD) for *a Regulation of the European Parliament and the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative acts*, Brussels.
79. P. Boucher, S. Nascimento, M. Kritikos, *How blockchain technology could change our lives: in-depth analysis*, Report of European Parliament Scientific Foresight Unit, STOA - Science and Technology Options Assessment, February 2017, pp. 1-24, doi: 10.2861/926645.
80. Regulation (EU) n. 910/2014 of the European Parliament and of the Council of the 23th July 2014 on *electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.*
81. Regulation (EU) n. 679/2016 of the European Parliament and of the Council of 27th April 2016 *on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*
82. Directive (EU) n. 843/2018 of the European Parliament and of the Council of 30th May 2018 amending *Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.*
83. European Parliament resolution of 3rd October 2018 on *distributed ledger technologies and blockchains: building trust with disintermediation (2017/2772(RSP)).*
84. European Parliament resolution of 20th October 2020 with *recommendations to the Commission on a Digital Services Act: adapting commercial and civil law rules for commercial entities operating online (2020/2019(INL)).*
85. G. Lofaro, *Dati sanitari e "e-Health" europea: tra trattamento dei dati personali e decisione amministrativa algoritmica*, in *MediaLaws*, 3, 2022, pp. 179-208, also in *Astrid Rassegna*, *Rivista Elettronica Quindicinale Sui Problemi Delle Istituzioni e Delle Amministrazioni Pubbliche*, Fondazione per l'analisi, gli studi e le ricerche sulla riforma delle istituzioni democratiche e sull'innovazione nelle amministrazioni pubbliche, in *https://www.astrid-online.it/static/upload/e-he/ehealth_02_2023.pdf.*
86. Art. 3 of the EU Regulation n. 679/2016 dictates: «*1. This regulation applies to the*

processing of personal data carried out within the scope of the activities of an establishment by a controller or processor in the Union, regardless of whether the processing is carried out in the Union or not. 2. This regulation applies to the processing of personal data of data subjects who are located in the Union, carried out by a controller or processor who is not established in the Union, where the processing activities concern: (a) the offer of goods or the provision of services to the aforementioned interested parties in the Union, regardless of whether a payment by the interested party is mandatory; or (b) monitoring their behaviour to the extent that such behaviour takes place within the Union. 3. This regulation applies to the processing of personal data carried out by a controller who is not established in the Union, but in a place subject to the law of a member State by virtue of public international law».

87. S. Caldarelli, *L'uso della tecnologia Blockchain nel settore delle pubbliche amministrazioni: tra "mito" e realtà giuridica*, in *Il Diritto dell'informazione e dell'informatica*, 4-5, 2020, pp. 857-896.
88. A. Razzini, *Blockchain e protezione dei dati personali alla luce del nuovo regolamento europeo GDPR*, in *Ciberspazio e diritto: rivista internazionale di informatica giuridica*, Enrico Mucchi Editore, 2018, vol. 19, Issue 60, pp. 197-208.
89. C. Brompezzi, A. Gambino, *Blockchain e proiezione dei dati personali*, in *Diritto dell'Informazione e dell'Informatica*, Giuffrè Francis Lefevre, 2019, 3, pp. 619-646.
90. According to article 5, par. 1, letter e) of GDPR «...*personal data are stored in a form that allows the identification of the interested parties for a period of time not exceeding the achievement of the purposes for which they are processed*»; while article 16, paragraph 1, of GDPR states «*The interested party has the right to obtain from the data controller the rectification of inaccurate personal data concerning him without unjustified delay*» and article 17 refers to «*...the right to obtain from the data controller the deletion of personal data concerning him...*».
91. European Union Blockchain Observatory and Forum, Report on *Smart contracts*, 1st November 2022, pp. 1-33, especially p. 29.
92. G. Lofaro, *La sicurezza dei dati sanitari nelle "smart technologies" quale strumento di realizzazione del diritto alla salute tra telemedicina ed intelligenza artificiale*, in *dirittifondamentali.it*, 2, 2022, pp. 120-141.
93. S. Licciardello, *Beni pubblici e generazioni future*, in *GiustAmm.it*, 9, 2016, p. 4.
94. F. Faini, *Blockchain e diritto: la "catena del valore" tra documenti informatici, smart contracts e data protection*, in *Responsabilità civile e previdenza*, 1, 2020, pp. 297-316.
95. Regulation (approved the 21th May 2024) of the European Parliament and of the Council *laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, as in the *draft document of the 14th May 2024 - 2021/0106(COD), PE-CONS 24/24* - submitted to approval, https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/EN/.
96. A. G. Orofino, G. Gallone, *L'intelligenza artificiale al servizio delle funzioni*

amministrative: profili problematici e spunti di riflessione, in *Giurisprudenza italiana*, 7, 2020, pp. 1738-1748: the Council of State (Consiglio di Stato, sez. VI, 4 febbraio 2020, n. 881) focuses on examining the validity of the use, in the context of administrative procedures, of computer algorithms, clarifying what are the conditions that make their application valid, even in the presence of discretionary measures: among them, in particular importance is played by the need for the activity conducted using telematic tools to be transparent, so as to allow full attribution of the act and the responsibilities resulting from its adoption, with a guarantee of knowledge of the logic that inspired the automated administrative action.

97. A. G. Orofino, *La semplificazione digitale*, in *Il diritto dell'economia*, 3/2019, pp. 87-112.
98. *«1. Technologies based on distributed registers are defined as technologies and informatic protocols that use a shared, distributed, replicable, simultaneously accessible, architecturally decentralized register on a cryptographic basis, such as to allow the recording, validation, updating and archiving of data both in clear text and further protected by encryption verifiable by each participant, which cannot be altered and cannot be modified. 2. A "smart contract" is defined as a computer program that operates on technologies based on distributed registers and whose execution automatically binds two or more parties on the basis of effects predefined by them. Smart contracts satisfy the requirement of written form following informatic identification of the interested parties, through a process having the requirements set by the Agency for Digital Italy with guidelines to be adopted within ninety days from the date of entry into force of the law converting this decree. 3. The storage of an electronic document through the use of technologies based on distributed registers produces the legal effects of electronic time validation referred to Article 41 of Regulation (EU) n. 910/2014 of the European Parliament and the Council of 23th July 2014. 4. Within ninety days from the date of entry into force of the law converting this decree, the Agency for Digital Italy identifies the technical standards that the technologies based on distributed registers must possess for the purposes of producing the effects referred to in paragraph 3»*.
99. C. Pernice, *Distributed ledger technology, blockchain e smart contracts: prime regolazioni*, in *InnovazioneDiritto*, Quarterly review of tax and economic law, Special Issue 5, December 2019; F. Longobucco, *Smart contract e "contratto giusto": dalla soggettività giuridica delle macchine all'oggettivazione del fatto - contratto. Il ruolo dell'interprete*, in *Federalismi.it*, 2021, 2; M.F. Tommasini, *Lo smart contract e il diritto dei contratti*, in*Juscivile*, 2022, 4. C. Robustella, C.E. Papadimitriu, *Spunti ricostruttivi in tema di smart contracts, tra innovazione tecnologica e regola giuridica (Reconstructive ideas on the smart contracts, between techonologica innovation and legal rule)*, in *P.A. - Persona e Amministrazione*, Volume 10, Issue 1, ottobre 2022,*passim*.
100. R. De Caria, *Blockchain and smart contracts: legal issues and regulatory responses between public and private economic law*, in *The Italian Law Journal*, 1, 2020, pp. 363-379.
101. G. Finocchiaro, C. Bomprezzi, *A legal analysis of the use of blockchain technology for the formation of smart legal contracts*, in *MediaLaws*, 2, 2020, pp. 111-135.
102. Legislative Decree 7th March 2005, n. 82 - *Digital administration code*.

103. G. Lemme, *Gli "smart contracts" e le tre leggi della robotica*, in *Analisi Giuridica dell'Economia*, 1, 2019, pp. 129-152.

104. S. Licciardello, *Metodo giuridico e sistema a diritto amministrativo*, in *Diritto e società*, 2, 2016, pp. 279-304: the methodologic question is a priority for jurists and concerns the conception of law. Today a study on the method is needed to build the administrative law system coherent. Vittorio Emanuele Orlando at the end of Eighteenth Century brings together order and scientific knowledge, alike Antonio Romano Tassone later on. The problem arises again today considering the crisis of law. The jurist must combine the law with the history, aware of a new ethical responsibility.

105. G. Lo Sapio, *Il tormentato rapporto tra blockchain e pubblica amministrazione nel prisma dei contratti pubblici*, in *federalismi.it*, 26, 1 novembre 2023, in https://federalismi.it/nv14/articolo-documento.cfm?Artid=49570.

106. D.U. Galetta, *Digitalizzazione, Intelligenza artificiale e Pubbliche Amministrazioni: il nuovo Codice dei contratti pubblici e le sfide che ci attendono*, in *federalismi.it*, 12, 2023, pp. 4-14.

107. L. Casini, *The Future of the (Digital) State*, in *BioLaw Journal - Rivista di BioDiritto*, 3, 2023, pp. 241-273, in this regard, wonders whether the digital revolution can transform the very idea of the State and its functioning? A first group of influences concerns the methods of exercising sovereignty and, in particular, the fundamental functions of the State. The techniques of the so-called direct democracy and their limits in pursuing the utopia of legislative production by the people, the use of algorithms by judges and the growing diffusion of automated administrative decisions are then examined. A second group of conditions refers to the effects that the technological revolution has on the other two elements of the State, the people and the territory. The issues concerning the protection of fundamental rights, the border crisis, the relationship between technology and information and, consequently, between democracy and truth are then analysed. From these constraints emerges a model based on "surveillance", in which big data, their use and their protection have acquired a strategic role.

108. S. Licciardello, *Prime note sulla funzione di regolazione dell'ANAC nel nuovo codice degli appalti*, in *federalismi.it*, 16, 2016, p. 4.

109. R. Cavallo Perin, I. Alberti, *Atti e procedimenti amministrativi digitali*, in *Diritto dell'amministrazione pubblica digitale*, edited by R. Cavallo Perin, I. Alberti, Torino, Giappichelli, 2020, pp. 119-158.

110. M. Mattalia, *I principi d'amministrazione pubblica in agricoltura tra libertà di circolazione, innovazione sociale e regolazione*, Edizioni Scientifiche Italiane, 2, 2019, XII-224, recognizes that the agricultural sector is one of the administrative models for financing, which recovers the studies of administrative law on subsidies and those on incentives in economics, but it also show what appears indispensable to meet the new challenges of environmental protection, management of the climate, of the cultures that claim biodiversity as a component of the identity of the peoples of the European Union.

111. R. Cavallo Perin, *Ragionando come se la digitalizzazione fosse data*, in *Diritto*

amministrativo, 2, 2020, pp. 305-328; The administrative algorithmic act represents «*the synthesis of this process and obliges scholars to revisit the traditional legal categories as well as to interpret existing legislation in a technological way: in any case, administrative law is responsible for defining the limits of validity that algorithm must follow*». A joint reading of the Italian law on the administrative procedure and the European law on personal data processing requires a guaranteed interpretation of the administrative algorithmic act by scholars: the "right to be heard" is the major guarantee as it allows to confirm, to verify and also modify the algorithm. Consequently, «*enhancing the right to participate and the right to be heard could be tool to overcome the criticism about the opacity and lack of motivation of the algorithms*». The increased predictability of decisions and the easy identification of "serious and manifest injustices" of such a systemic way of administering would ensure a positive effect both in terms of increased administrative capacity and in terms of increased assessment of the legitimacy of administrative action.

[112] J.A. Triana Casallas, J.M. Cueva Lovelle, J.I. Rodriguez Molano, cit., p. 68.

[113] L. Casini, *Lo Stato nell'era di Google*, in *Rivista trimestrale di diritto pubblico*, 4, 2019, pp. 1111-1148.

[114] A. Khatoon, *A blockchain-based smart contract system for healthcare management*, in *Electronics - Special Issue on Advances in Blockchain and Distributed Ledger Technology (DLT) for Industry 4.0 Technologies*, 9(1), 94, 2020, https://doi.org/10.3390/electronics9010094.

[115] P. Gallo, G. Capizzi, M. Timoshina, *SeedsBit: Blockchain per la tracciabilità agroalimentare multifiliera*, *in federalismi.it*, n. 2/2021; the paper highlights in particular the aspects of traceability, quality of data and intellegibility of smart contracts in the agri-food chains.

[116] J.A. Triana Casallas, J.M. Cueva Lovelle, J.I. Rodriguez Molano, cit., p. 70.

[117] G. Lo Sapio, *Il tormentato rapporto tra blockchain e pubblica amministrazione nel prisma dei contratti pubblici*, in *federalismi.it*, 26, 2023, p. 131.

[118] P. La Selva, *Blockchain e smart contracts nella Pubblica Amministrazione: aspetti di un tentativo di digitalizzazione del settore pubblico*, *in federalismi.it*, 2, 2022, p. 312.

[119] D.U. Galetta, J.G. Corvalan, *Intelligenza artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *federalismi.it*, 3, 2019, p. 19.