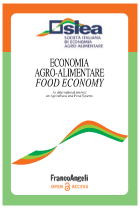
Economia agro-alimentare /
Food Economy

An International Journal on Agricultural and Food Systems

Vol. 25, Iss. 2, Art. 8, pp. 97-114 - ISSN 1126-1668 - ISSNe 1972-4802
DOI: 10.3280/ecag2023oa14958



Blockchain in the agrifood sector: From storytelling to traceability fact-checking up to new economic models

Francesco Rampone[*,a], Fabio Lecca[a], Paolo Giolito[a], Massimo Romano[a]

[a] Associazione Blockchain, Italy

Abstract

This paper aims to demystify a lot of misconceptions still widely circulating today about the alleged properties of blockchain and then illustrate the real opportunities that this technology offers for "food system" and how it must be correctly implemented for it to be truly useful, for producers and consumers, particularly in the agrifood sector. The concepts of blockchain opportunities and incompleteness of agri-food chain projects based on blockchain technology are then explained, setting out the minimum and necessary characteristics required to make the use of this technology useful and effective (Minimum Viable Ecosystem). The process governance levels for the development and maintenance of a blockchain traceability project are then illustrated, focusing on the role and responsibility of each player in the supply chain. Finally, the structure of a blockchain solution is described, focusing on a number of structural and technological solutions by outlining the concepts of consistency checking for the validation of input data with appropriate smart contracts, and of information frameworks for the subsequent scrutiny of data in audit operations and the assignment of levels of reliability. These are essential prerequisites for a collaborative blockchain data management to pursue the objective of actual reliability and transparency of information.

Article info

Type:
Article
Submitted:
17/11/2022
Accepted:
07/06/2023
Available online:
14/09/2023

JEL codes:
Q12, Q16, Q55

Keywords:
Blockchain
DLT
Supply chain
Precision agriculture
Sustainability

Managing Editor:
Lucia Briamonte
Biagio Pecorino
Angelo Frascarelli

* *Corresponding author*: Francesco Rampone - Lawyer - Associazione Blockchain Italia. E-mail: francesco.rampone@associazioneblockchain.it.

Introduction

Countless agrifood supply chain projects were announced and developed on blockchain platforms (hereafter, also "BC") of which, after a successful initial promotional launch, no further word has been heard. Maybe they failed to keep their promises, or maybe, when they have, they have not contributed in any appreciable manner to strengthening consumer confidence in the high quality and origin of products.

Blockchain solutions in the agrifood sector have in fact mostly remained anchored to producers' narrative and thus confined at the traditional evocative level of advertising and corporate branding. They therefore did not significantly impact the relationship between businesses and consumers.

As a result, some questions arise about this technology's actual suitability to be usefully applied in non-purely fintech sectors.

The reason for this is mostly to be found in the misconception that blockchain would not be able to solve problems other than those of a mathematical nature. The challenge is, in short, to be able to apply blockchain's original ability to reconcile accounting items without relying on a third-party trustee to food chains. This requires a logical leap and a technology adjustment so that it may solve informative and not merely arithmetical problems[1].

1. Innovations provided by blockchain technologies

1.1. *Blockchain in a nutshell*

Blockchain technology makes it possible to decentralise accounting transactions involving – at least in cryptocurrency protocols – debit-credit relationships between several parties. Prior to 2008, no one had succeeded in designing a computerised system whereby a single set of accounts would be kept in digital format between several operators without one of them necessarily having to take on the role of ledger keeper. In other words, it was not possible to run a shared accounting system without someone taking on

1. The application of distributed ledger technologies to new consortium forms of information management enabled by BC could become one of the most interesting economic levers for the development and valorisation of agrifood products. In a global competitive environment, strongly altered by large investments in marketing, blockchain, when properly applied, makes it possible to provide guidance to consumers by shifting from a market approach dominated by advertising storytelling, where consumers are a passive target of mass communication, in favour of a fact-checking approach, where consumers take an active and conscious role in their purchase choices.

the role of trustee, i.e. ensuring the correct and regular posting of debit and credit entries in the ledger.

Blockchain, therefore, introduced for the first time the possibility, in general terms, of settling relations between traders without necessarily having to rely on an intermediary who would ensure the correct execution of payment orders. It is precisely this ability of blockchain to overcome the traditional approach of information or commercial hierarchies that makes it the ideal tool to make the data uploaded and processed on it reliable without recourse to any third-party authorities.

For this reason, BC is defined as "trustless", in the sense that it does not require for trust to be placed in a particular entity that takes up the role of ledger keeper.

1.2. *What blockchain does not do*

Two myths are most commonly referred to in emphasising the useful nature of blockchain solutions. These are unfounded concepts that lead one to believe that the adoption of a DLT solution consists essentially in uploading data and documents into it in order to certify and authenticate them.

To certify or verify a datum (or information) is to give it the status of true information[2]. Well, no data will be of a higher degree of reliability merely because it is uploaded or managed on a blockchain[3]. Indeed, nothing prohibits participants from uploading incorrect data (the expression garbage-in-garbage-out is used to emphasise this property), so that deployment of a blockchain is unjustified where this technology is merely used as a data repository. Data's higher accuracy, from a statistical appreciability

2. **Certification** refers to a process whereby the "true nature" of data is acknowledged *indirectly*, i.e., through the intervention of an authority which we trust. By contrast, **verification** refers to a process whereby the "true nature" of data is recognised *directly*, i.e., by direct observation or deduction. Unlike certification and verification, data "true nature" in a blockchain is only obtained by **validation**, i.e., by exploiting the ability of the blockchain network to enable distributed consensus decision-making protocols in the IT environment, where no certifier or verifier is therefore needed. These are, however, at least in cryptocurrency protocols, mathematical "truths" consisting in the reconciliation of debit/debit accounting entries, as such not applicable, without appropriate considerations, to data of a logical nature. We will see in the following sections how validation can also be usefully employed in a production process, provided certain properties of the blockchain distributed structure are effectively applied.

3. As will be seen in chapter blockchain makes data both resilient and unchangeable. This is why reference is also often made to the concept of "notarisation". However, notarisation also implies a fiduciary element, the notary public or notarising public official, which by its very nature is completely absent in a blockchain protocol.

perspective, only depends on the system overall design, the controls that are implemented, and the reputation of the parties responsible for data entry, as well as the reliability of the IoT devices and other complementary technologies employed (*contra*, Tripoli & Schmidhuber, 2018, § 3.2.5, p. 15).

Authenticating some data (or documents) means identifying their specific origin or author. Well, blockchain does not confer any certainty as to the origin of data or documents (prior to entering the blockchain)[4]. On the contrary, in the digital environment, authentication is performed widely and very effectively, at least in Italy, by certified electronic mail (PEC) and digital signatures (or other types of qualified or advanced electronic signature or other process meeting the requirements laid down by AgID (Digital Italy Authority) in Article 20 of the Code of Digital Entities (CAD), paragraph 1-*bis*). However, only such systems may constitute evidence against perjury and thus bear a greater probative weight than data uploaded onto blockchain[5].

1.3. *When blockchain is not needed*

Often, when describing the benefits of using a blockchain solution, reference is made to its achievements and alleged prerogatives or characteristics which actually belong to any well-constructed computer system in comparison to which blockchain actually adds nothing. Document digitisation, data immutability, disintermediation, smart contracts, are some, among many, locutions misused when talking about BC.

1.4. *Blockchain Opportunities (BCOs)*

Ownerlessness. This is perhaps the most typical feature of blockchain. The platform performing the relevant protocol and storing transaction data may be a network of peer servers. Each server (node) is potentially owned by a different participant who has no greater privileges than the others (unless

4. Blockchain is used in Self Sovereign Identity (SSI) projects, i.e. in solutions that enable the identification of a party through verification of one or more verifiable credentials. However, these are implementations in which blockchain is neither necessary nor functional for identification per se, but used to enable a decentralised and autonomous management of statements.

5. We have been waiting for years for the Guidelines that AgID should have issued by May 2019 in performance of Article 8-ter of Legislative Decree 35/2018 (the *"Simplification Decree" 2018*) to make written smart contracts effective. These are technical rules that will probably never see the light of day until after this rule is reworded, as at present it creates quite a few interpretative doubts.

otherwise provided for under the shared protocol). In this perspective, in a blockchain solution there is no owner of the hardware/software infrastructure and the database, nor is there a governance pyramid structure, which results in enhancing the participants cooperation and empowerment.

Open execution. Data are processed according to a shared protocol (loaded on each node), which is as transparent and unchangeable as the data, so that observers outside the network can verify that the system's output is obtained by performing the rules stated by participants[6].

Irrevocable open data. The visibility of the data being processed on blockchains can be set in an irrevocable and verifiable manner by regulating the degree to which they can be displayed for the benefit of nodes, participants and third parties, while respecting the protection of personal data or the protection of confidential commercial information.

Resilience. The data cannot be removed or modified (except under some specific protocols)[7] as they are uploaded onto an indefinite number of nodes (servers) and managed by an equally indefinite number of autonomous and independent (and if necessary, also anonymous) players. Any opportunistic manipulation of data by a node will create a mismatch with the data held by other nodes and will therefore be rejected by the network[8].

Validation. The entry of new data into a blockchain may be precluded if they conflict with data already on it or do not comply with certain input parameters or protocols. Data, in fact, may be subject to validation rules (actual smart contracts) that are transparent and cannot be circumvented or abusively modified, so they act as filters ensuring consistency of the data uploaded onto a blockchain. Validation is therefore the emerging property in the BC environment due to the application of smart contracts in open execution.

Unique data "historicising" *(append only)*. Data are uploaded onto blockchains in chronological sequence to form a single irreversible time

6. Open execution is therefore the possibility offered by blockchain to make data processing transparent by allowing anyone to verify the reliability of participants' statement. (see Salah, Damiani, Al-Fuqaha *et al.*, 2018).

7. There are some blockchain protocols that make it possible for specific nodes to delete data (Florian *et al.*, 2019, pp. 367-376). In such cases, however, this function is in any case shared among participants who find it useful to confer specific powers to some of them.

8. The data acceptance criterion on blockchain generally responds to majority principles (as is the case, for instance, in the bitcoin protocol), whereby data only enter the network where they are presented in an identical manner by the majority of nodes in the same time frame. Any "false" data entry therefore implies the existence of a fraudulent agreement between the majority of participants. This is the "51%" attack case. The sheer number of nodes, together with their autonomy and independence, has so far prevented the bitcoin network (by far the most popular and extensive blockchain) from being the target of such an attack.

vector[9]. Their temporal order, therefore, cannot be changed and develops a unique history-line of inputs and outputs as well as their processing protocol, all indelibly stored on blockchains. (Khaqqi *et al.*, 2018; Sharma, 2017).

Tokenisation (*uniqueness*). This is an effect obtained by combining the three previous requirements altogether. On blockchains, "unique" digital documents can be created, i.e. which cannot be duplicated or improperly modified. These characteristics, conferred on computer documents, represent the real novelty element introduced by blockchain and enable the creation of tokens and cryptocurrencies[10], the concept of originality and uniqueness is in fact introduced in the digital environment. Since nodes share the same information, such information may assign a right to someone in a clear manner, so that duplication of that right in favour of someone else is not possible[11].

1.5. *BCO in supply chain*

By virtue of the above-mentioned properties, the information "falling" into a blockchain may give rise to an invariable set of data (which we call tokens) that can only be updated or modified according to a shared protocol on the same blockchain. In a broad sense, we may call this protocol a "smart contract". Where these data are associated with supply chain products, i.e. they refer to actual or potential real-world objects (e.g. an EVO bottle or a load of tomatoes), we can by analogy consider them a "digital representation" of such products, of an informative and descriptive nature, which is reliable as it is shared, non-duplicable and non-falsifiable (i.e. not modifiable following its entry into BC). The degree of reliability, however, depends on the actual implementation of a BCO.

We shall examine in more detail in the next paragraph the blockchain's properties described above for a helpful application thereof in the agrifood supply chain.

As we have seen (§ 1.4), "validation" is an emerging characteristic of a blockchain environment. This refers to the protocol's suitability for execution in an automatic and transparent manner (open execution). In the

9. The "history" uploaded onto a blockchain is unique in the sense that no alternative data sequences may be written in the blockchain. By contrast, this is possible with other technologies with which the availability of data is in the hands of a single party that can opportunistically change the data history or the content of documents.

10. The success of bitcoin and the bitcoin protocol rests precisely on the resolution in a digital environment of the "double-spending problem", i.e. the impossibility, before then, of enabling credit circulation through an online cash system (Nakamoto, 2008).

11. A note receivable, like a banknote, is nothing more than a non-reproducible and non-falsifiable document that grants a receivable to its holder.

Bitcoin network, for example, data are subject to an accounting balance check (the transaction balance, net of change, must be zero). Similarly, in a food chain protocol we can execute a validation of a "material balance". Validation may also take the form of consistency checks, i.e. the comparison of data of different nature and origin, verification of their consistency against shared parameters, the subsequent attribution of a reliability index to the data submitted for verification, and the performance of inspection and audit activities in order to verify compliance with the specifications and fairness of the players' conduct. For example, the production data of a wheat field must be consistent with the upstream invoice data of the plant protection products used or with the weather data from sowing to harvest and, at the same time, with the downstream logistics data of the carrier and the retailer's sales data. If any inconsistency is identified, checks or requests for an explanation could be made by the consortium owning the quality mark that is using the relevant blockchain solution.

2. Transparency and consistency of information

We have seen that blockchain makes it possible to draw up a "story" of the supply chain that is trustworthy, immutable, transparent (on stakeholders' roles and obligations) and accessible to anyone provided that BCOs are properly implemented to the maximum extent.

Let us now see what are the minimum BCOs that must be implemented to justify the adoption of a supply chain BC project.

2.1. *Minimum Viable Ecosystem.*

When it comes to BC, it is crucial to remember that implementation of a BC system is not eminently IT-related: BC is not a new way of doing what was done before, but a technology that enables new conducts previously not possible in a digital environment. In other words, implementing a BC project means first of all deciding to organise information and its management on IT tools in a different way, involving other players, competitors even, thus pooling some resources and repositioning competition at a higher level with beneficial effects on the entire market segment in which the project operates.

In this perspective, the MVE not only concerns the structure of the IT platform on which the BC project rests, but shall also take into account the network of relationships and the value of individual network participants' contributions.

Let us see in the following three paragraphs the MVE elements in a BC project.

2.1.1. Multiple C-type stakeholders

The Bitcoin protocol bases its ledger trustworthiness on its peer-to-peer structure, i.e. a horizontal structure in which stakeholders' equal participation is the keystone that makes it possible to avoid having to rely on "middlemen", i.e. trustees tasked with ensuring the correct posting of accounting information relating to payment arrangements.

Such structure is fundamental in any BC project, and therefore also in a supply chain project. It is the first BCO – "ownerless" – without which there is no reason to deploy a BC solution. That is, it makes no sense to adopt a BC solution without taking decision-making power (transaction validation, data storage and "historicisation") away from a trustee and distributing it "on a democratic basis" to a large number of participants.

We can therefore say that the first element that the MVE in a BC project must certainly possess is of a structural nature: multiple C-type stakeholders.

2.1.2. Multiple W-type stakeholders

However, for BC to be useful in a non-accounting project – such as a supply chain – a data governance shall be implemented that includes a large number of W-type stakeholders. In such projects, implementing a protocol with only one W-type stakeholder would be just as irrational as implementing a BC platform consisting of only one node. A BC's strength specifically lies in its capacity to create equal relationships among participants where no economic, legal and informational hierarchies apply.

The second requirement of a non-purely-accounting BC project's MVE is therefore the large number of W-type stakeholders[12]. This is not a BCO specification, but a necessary precondition for executing validation smart contracts: only if the data subject to validation come from autonomous and independent sources does it make sense to cross-check the data, such that the write type stakeholders provide their contribution, in an uncoordinated but harmonious manner, to creating a chain of validations, in which each entry is consistent with the previous and subsequent entries (Di Cillo 2021).

12. The W-type stakeholder element is typical of non-accounting BC projects. On the contrary, in the Bitcoin protocol, which is a typical BC accounting protocol, there is no need for several W-type stakeholders as validation is only carried out as a result of a mathematical check (performed by smart contracts, or the C-type stakeholders' tools) and not of consistency with other data provided through previous C-type stakeholder inputs or resulting from the output of smart contracts.

2.1.3. Information consistency checks

The third and final MVE requirement – but no less important – that a BC system must possess to be worth using is the implementation of computer protocols (smart contracts) to assess the consistency of incoming information on a BC.

BC was created as a solution to get rid of the fiduciary aspect that all centralised management systems have. More generally, it allows for the regulation of financial, legal or informational relationships between participants without the necessary involvement of third party trustees (*middlemen*) (Pergamo, 2020). Therefore, adopting a BC solution while maintaining this fiduciary component makes no sense[13].

Therefore, limiting the MVE to type C and W-type stakeholders alone is not sufficient. Data entering BC must be subject to transparent and automatic IT protocols (open execution), which work as a "filter", preventing the entry of any incorrect data (because, for example, they do not comply with an accounting balance constraint) or automatically assigning them a reliability label showing their degree of consistency with respect to data already populated on the BC.

A third MVE requirement related to data governance may thus be identified: implementation of consistency checks on incoming data on the BC by means of appropriate smart contracts.

2.2. *Complete and incomplete BC systems*

On the basis of the considerations outlined in the previous paragraphs, a complete BC system may be defined as including an MVE consisting of:

- large number of C-type stakeholders;
- large number of W-type stakeholders (autonomous and independent);
- smart contracts that perform consistency checks on the information uploaded into BC.

Conversely, a system is defined as incomplete when it lacks at least one of the above-mentioned elements.

Of course, a BC system may be more or less complete depending on the number of stakeholders or the reasonable design of smart contracts. In

13. This is the main issue of the BC projects examined by the authors of this contribution. In all cases, while use is made of existing platforms that fulfil the first MVE requirement, data entry is then reduced to the initiative and responsibility of a single operator, which inevitably conflicts with the trustless goal that should drive the development of any BC project.

the following paragraphs we will therefore see some examples of how the complete nature of a non-accounting BC system may be maximised[14].

3. Verifiable information framework

In a BC project, validation is performed by smart contracts in open execution mode.

This makes it possible to any party with sufficient technical expertise to ascertain how a smart contract's algorithm performs validation of incoming data on BC.

However, without an *ex ante* statement of how the relevant smart contact should perform data validation, it is not possible to verify whether it does exactly what the compiler intended, nor whether the algorithm's inputs are timely, are of the expected type and come from the correct input point.

In other words, R-type stakeholders, to be able to verify that data validation has been performed accurately or according to a shared logic, must be able to understand the reasons behind the choice of rules and functions implemented through smart contracts. In fact, as we have seen, in a supply chain project, data validation checks do not pursue the purpose of preventing incorrect data from entering BC, but rather assigning them a specific degree of reliability. In order to ensure transparency and trust in favour of R-type stakeholders, not only do they require to be provided with information on what happens on a BC, but also on what *should* happen; that is, to state, in an immutable manner (on a BC precisely) the choices that have been made at the level of corporate governance and data governance with regard to the network's structure, the rules of the specifications to be complied with, the project objectives, and therefore the useful nature of the criteria and parameters adopted in the smart contracts validation operations in order to achieve these objectives.

14. Bitcoin is a complete system, as it is an open network in which anyone can participate with type write and type commit prerogatives without the need for authorisation from any higher authority and in which no transactions are allowed that do not comply with budgetary constraints (verification of the settlor's funds, sum of transactions net of commissions amounting to zero, change and mining). In contrast, other projects defined as blockchain-based, even though developed on open DLT ("permissionless") platforms, are incomplete systems as they do not involve the participation of multiple W-type stakeholders and the input data are uploaded by or under the authority of a single party (usually the owner of the brand that promoted the BC project), nor are the data subject to automated checks of any kind, thus addressing the market in a manner not different from the usual storytelling through advertising.

Therefore, in order to raise the level of completeness of a BC system, it is best to provide for more than mere transparency of the validation protocols of the relevant smart contacts and metrics (open execution), including by publishing declarative documents onto the BC, drafted in a structured form ("verifiable information framework" or "technical governance framework") so as to make them accessible on multiple applications.

In other words, the system objective is not only to provide consumers with information on "who did what", but also **verifiable information** on whether the "who" and the "what" are accurate, i.e. whether the process (the BC transaction) has been carried out in compliance with the roles, permissions and policies set out in the production specifications and supply chain contracts that ensure the products' quality and origin[15].

4. Digital twining

When describing the BC projects applied to supply and distribution chains, reference is often made to "digital twining" to imply that on a BC it is possible to create "digital twins" of physical assets (the expression "digital representation" is also often used). The underlying idea is that a sort of entanglement may be created between the two entities, the real one and the IT one, whereby the development of the former is reflected in an isomorphic manner on the latter (Notland, Hua, 2017).

In reality, twining and entanglement are two different aspects, and talking about digital twining is definitely misleading[16], often generating a series of erroneous deductions that do not help to accurately frame BCOs and risk pre-emptively making a project fail or be useless.

15. Only a few international working groups are discussing the development of governance frameworks similar to the one presented in this paper. These include the Hyperledger Aries RFC 0430, proposed commentary by Daniel Hardman (Chief Architect of Evernym, recently acquired by Avast, and technical board member of Sovrin) and the IEEE P2145 "Blockchain Governance Standards Working Group". The ISO/TC 309 "Governance of organisations" group as well as the groups related to Self-Sovereign Identity (SSI) technologies dedicated to the development of governance frameworks and data agreements on decentralised systems such as the Trust Over IP Foundation (ToIP) are of a less specific nature, but noteworthy.

16. The expression was invented well before the advent of BC (Gelernter, 1991) when it meant the digital modelling of a product and its components to manage the production stages, verify the assembly stages and test a product's strength and functionality already at the design stage.

4.1.1. Singling-out

In order to associate a product with a token, one must first distinguish it, i.e. make it unique, just as unique is the token with which it is associated, and thus make it different from all other similar products with which it might otherwise be confused.

A product may successfully be singled-out by identifying some intrinsic characteristics (e.g. the veins of a diamond), or affixing of a material tag on the product.

In all cases, the singling-out must lead to a stable outcome, i.e. it must be maintained until consumption or at least until sale to the final consumer, i.e. until the moment when the distinction is no longer necessary for tracking purposes.

A product singling-out obtained by reference to its intrinsic characteristics is by definition stable and is maintained throughout the life of the product until any alteration (due to consumption or damage). In this case, therefore, the unique connection between the product and its token is not problematic from a technical perspective, except for identifying the product unique characteristics, i.e. regarding the tool required to detect these characteristics.

Applying a QR-Code on a product – a solution often used in supply chain BC projects – in no way solves the singling-out problem since a specific QR-Code may be easily cloned and applied on an indefinite number of different products.

4.1.2. Entanglement

As for the reliability of the information associated with a product's digital twin (the second issue mentioned at the beginning of this paragraph), since there is no automatism between facts about a product and the information about those facts uploaded into BC, there is no guarantee that, even if the singling-out problem were solved, the information flow would not be intercepted and modified for fraudulent and opportunistic purposes.

We have already illustrated, however, how to solve (strongly mitigate) this issue in the preceding paragraphs, i.e. by resorting to an information hierarchy that is as horizontal (distributed) as possible, such that it is not necessary to place trust in one or a few players, but in which the various information sources (operators and IoT) contribute autonomously and independently to the writing of a single, coherent story. This means that it is impossible for the story to be made false without a fraudulent agreement between a large number of stakeholders (an agreement, moreover, that would require continuous fraudulent conduct in order to conceal the story inconsistency over time).

4.2. *Reversing the terms of the relationship*

Digital twining should not (only) be understood as a real-to-virtual operation, i.e. as if information from the real world would add to, and characterise the digital twin. This is certainly true and necessary, but does not constitute the essence of “twining”.

Entangling a physical asset with a digital asset (token) works in the opposite sense, i.e. in a virtual-to-real sense: only events affecting the token can have an instantaneous effect on the life of the physical asset associated with it.

From this perspective, a digital twin is nothing more than a token whose possession and transfer certifies the holder’s ownership (or other right) over the physical asset it represents. Product entanglement, therefore, takes place on a legal level[17].

4.3. *TAG features*

A tag, just like the token it refers to, must be durable, unalterable (not falsifiable) and non-duplicable. That is, it must be permanently associated with one product, and one product only: a tag that is easily reproduced on other products or easily modified or removed is not capable of conferring a unique trait to a product and, therefore, ensuring its unique association with a given token on BC.

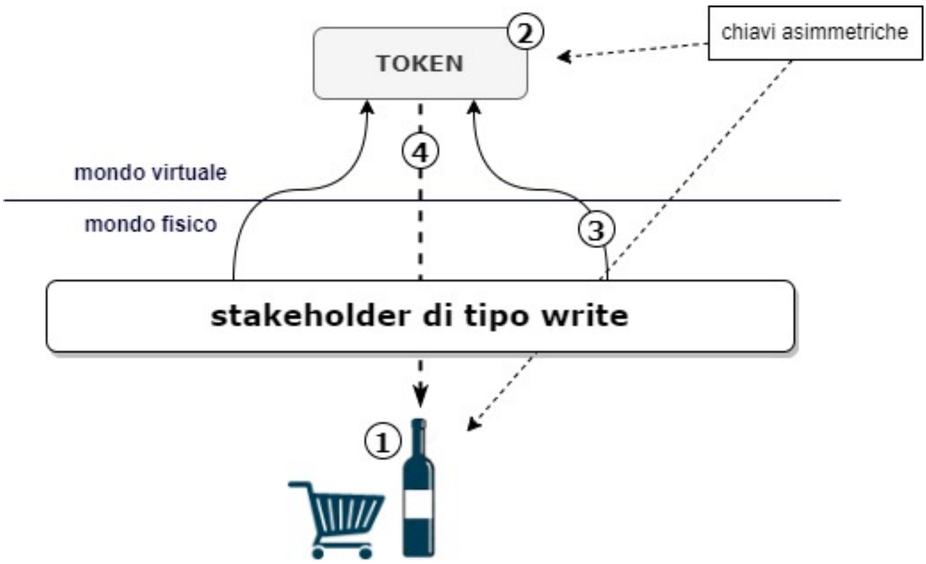
The features of material tags can therefore be summarised as follows:

- **Originality**. Tags must be produced through means that prevent the creation of two identical tags.
- **Uniqueness**. Tags must not be reproducible on other products (except at a cost that would make the reproduction operation unworthy)[18].

17. A token is a unique digital asset, i.e. a digital document, which, thanks to BC technology, is durable, and may not be subject to forgery, “historicisation” and duplicability. The concept has already been mentioned in about BCOs (tokenization item), and thus the possibility of obtaining a digital certificate having all the properties of traditional physical certificates. For digital twining to take place, the same unique characteristics of the token must be implemented in the physical product it is to represent.

18. The tag uniqueness (non-duplicability) can also be achieved “*ex post*”, i.e. through endorsement of the tag at the time of purchase when the product is checked out at the counter. In such a case, the cashier acts as the last W-type stakeholder and the endorsement basically consists of updating the information associated with the token by qualifying the product as “sold” (no longer saleable). Any fraudulent duplication of the token would prevent the counterfeited product from being successfully checked out at the counter and, therefore, from being sold (unless it is sold before the original product which would, in any case, reveal the fraud).

- **Immutability**. The tag must not be modifiable (except as provided for by any update protocol).
- **Incorporation**. The tag must not be removable from the product except at the cost of its destruction or identifiable alteration.



Singling-out. The product is identified by its intrinsic properties (e.g. the veins of a diamond) or marked with a **material tag** that makes it unique.

Twining 1. An association is created between a product, or the tag applied to a product, and a token.

Twining 2. W-type stakeholders (directly or through IoT) collect the product information and upload it piece by piece onto BC (information is associated with the token and data are validated through smart contracts);

Entanglement. The token not only contains or refers to a truthful and up-to-date history of a product (campaign journal), but also allows, by simply being circulated (by way of transactions), the establishment, modification or cancellation of specific subjective legal situations concerning the product.

5. Applicability: valorisation of the traditional agri-food chain in a blockchain-based traceability system

Current regulatory references provide for specific provisions concerning the traceability of foodstuffs along the entire production chain as well as defining mechanisms for food withdrawals and recalls. In particular, Regulation (EC) N. 178/2002[19] provides for the adoption of a traceability system that makes it possible to identify the origin and route of foodstuffs throughout the chain in order to guarantee food safety and consumer health protection. Food business operators are required to take appropriate measures to ensure food safety and to notify the competent authorities of any risk to consumer health. The competent authorities, in turn, are responsible for verifying compliance and managing food-related health emergencies.

6. From storytelling to fact-checking, process and system innovations

According to Cirianni *et al.* in ISTAT Working Paper 4/2021 - "Struttura produttiva e performance economica della filiera agroalimentare italiana" (p. 15): "*Farms within the agri-food chain and compared to the national average have low intermediate cost values on turnover, because they have very low sales volumes and are small in size, many of them are unable to adopt adequate marketing policies and, above all, to penetrate foreign markets*".

The shrewd and reasoned application of blockchain technologies and in particular of the new distributed governance models that can be financed through the funds earmarked for the implementation of market policies and the implementation of the Farm to Fork strategy, can counteract the competition contexts strongly altered by large investments in marketing to focus attention on product quality (excellence of Italian farms). The hoped-for technological and cultural transformation of agricultural enterprises could become the primary socio-economic enabler for transitioning from storytelling approaches to effective and comprehensive fact-checking, provided that it is accompanied by the planning of ministerial campaigns to raise consumer awareness about these aspects.

Following the realisation of this marketing transformation, the foundations will be formed to generate a virtuous circle along which the mere technical possibility of being able to verify and prove the truthfulness of traceability information should generate a demand for access to this information by shifting the consumer's attention to the qualities and values of the product rather than its narrative.

Indeed, we can say that blockchain technologies produce holistic[20] value within the food system, given their fundamental characteristic of being able

19. Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002R0178.

20. Whereby the overall system has value greater than the sum of its parts.

to organise and re-engineer the relationships among system actors through a technology that supports the disintermediation of the trust.

Through them, consumers, auditors, regulators, and other participants are thus empowered to use or produce information using verifiable, distributed, and independent mechanisms that would otherwise be impossible to achieve. From the improved control of processes and data, relying on *a single source of reliable information shared between the parties* (Single Source of Truth), will come an improvement in business efficiency, thanks to the automation, independence and speeding up of controls.

Acknowledgements

The authors of this paper would like to thank all the participants at the Supply Chain Working Table operating in the Italian Blockchain Association from 2018 to 2022. Many of the ideas and concepts herein presented were developed during the long and almost weekly meetings and discussions held in person and videoconference. A warm gratitude for their contribution to: Stefano Gatti, Filippo La Scala, Massimo Montecchi, Cesare Fabio Saccani, Michele Soavi, Mikaela Valan and Ivan Vitali.

References

Akgiray, V. (2019). The Potential for Blockchain Technology in Corporate Governance. *OECD, Corporate Governance Working Papers, No. 21*. Paris: OECD Publishing. doi: 10.1787/ef4eba4c-en.

Berryhill, J., Bourgery, T., & Hanson, A. (2018). Blockchains Unchained: Blockchain Technology and its Use in the Public Sector. *OECD Working Papers on Public Governance, No. 28*. Paris: OECD Publishing. doi: 10.1787/3c32c429-en.

Biggs, J., Hinish, S.R., Natale, M.A., & Patronick, M. (2018). *Blockchain: Revolutionizing the Global Supply Chain by Building Trust and Transparency*. -- Available at www.academia.edu/33180964.

Cirianni, A., Fanfani, R., & Gismondi, R. (2021). *ISTAT working papers: Struttura produttiva e performance economica della filiera agroalimentare italiana*. -- www.istat.it/it/files/2021/06/IWP_4-2021.pdf

Di Cillo, M. (2021). L'applicazione delle tecnologie smart contract e blockchain al settore agrifood: profili innovativi e criticità. *Camminio Diritto*, *11*. -- Available at https://rivista.camminodiritto.it/articolo.asp?id=7788.

Florian, M., Henningsen, S., Beaucamp, S., & Scheuermann, B. (2019). Erasing Data from Blockchain Nodes. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. Stockholm, Sweden. doi: 10.1109/EuroSPW.2019.00047.

Gelernter, D.H. (1991). *Mirror Worlds: or the Day Software Puts the Universe in a Shoebox – How It Will Happen and What It Will Mean*. Oxford, New York: Oxford University Press.

Kamath, R. (2018). Food traceability on blockchain: Walmart's pork and mango pilots with IBM. *The Journal of the British Blockchain Association*, *1*(1), 3712.

Khaqqi, K.N., Sikorski, J.J., Hadinoto, K., & Kraft, M. (2018). Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. *Applied Energy*, *209*, 8-19.

Notland, J.S., & Hua, A.V. (2017). *Project Thesis Blockchain enabled Trust & Transparency in supply chains*. doi: 10.13140/RG.2.2.22304.58886.

Pergamo, R. (2020). La blockchain: la tecnologia e l'applicazione al settore agroalimentare. *Pianeta PSR*, *93*, July-August.

Perpete, S. (2020). *Challenges and opportunities of using blockchain technology in the food supply chain. Focus on organic food supply chain*. Liege University Library. -- Available at https://matheo.uliege.be/handle/2268.2/10227.

Pranata, A.R., & Tehrani, P.M. (2022). *The Legality of Smart Contracts in a Decentralized Autonomous Organization (DAO). Regulatory Aspects of Artificial Intelligence on Blockchain* (pp. 112-131). IGI Global.

Rampone, F. (2019). Smart Contract, né smart né contract. *Rivista Diritto Privato*, *2*, 241-258.

Salah, K., Damiani, E., Al-Fuqaha, A., Martin, T., Taha, K., & Khan, M.K. (2018). Open execution – The blockchain model. IEEE Blockchain Technical Briefs. -- https://blockchain.ieee.org/technicalbriefs/december-2018/open-execution-the-blockchain-model.

Schebesta, H., & Candel, J.J. (2020). Game-changing potential of the EUs Farm to Fork Strategy. *Nature Food*, *1*(10).

Sharma, S. (2017). *Climate change and blockchain*. -- Available at SSRN: https://ssrn.com/abstract=3088990.

Sylvester, G. (2019). *E-agriculture in action: blockchain for agriculture. Opportunities and challenges*. FAO/ITU.

Tripoli, M., & Schmidhuber, J. (2018). *Emerging Opportunities for the Application of Blockchain in the Agri-food Industry*. Rome-Geneva: FAO and ICTSD.

Van, Pelta R., Jansena, S., Baarsb, D., & Overbeek, S. (2021). Defining Blockchain Governance: A Framework for Analysis and Comparison. *Information System Management*, *38*(1), 22. doi: 10.1080/10580530.2020.1720046.

Wyoming - SF0038 - Decentralized autonomous organizations -- www.wyoleg.gov/Legislation/2021/SF0038, -- https://wyoleg.gov/2022/Enroll/SF0068.pdf.

Xu, J., Guo, S., Xie, D., & Yan, Y. (2020). Blockchain: A new safeguard for agri-foods. *Artificial Intelligence in Agriculture*, *4*, Elsevier.

Francesco Rampone
Associazione Blockchain Italia; La Scala Law Firm
E-mail: francesco.rampone@associazioneblockchain.it
Lawyer with over 25 years' experience in intellectual property, information technology and data protection. President of the Italian Blockchain Association. Head of the TMT department at La Scala Law Firm.

Fabio Lecca
Chief Technical Officer
Associazione Blockchain Italia; Araneum Group S.r.l.
E-mail: fabio.lecca@associazioneblockchain.it
Computer scientist with over 25 years of experience, he is the Chief Technical Officer of Araneum Group srl working on blockchain and open source projects and counsellor of Associazione Blockchain Italia.

Paolo Giolito
Associazione Blockchain Italia; CA Indosuez Wealth (Europe)
E-mail: paolo.giolito@associazioneblockchain.it
He has over 25 years in Wealth Management (Deutsche Bank, Credit Suisse, CA Indosuez), 10+ years in Italian innovative ecosystem as a Business Angel (IAG, Club degli Investitori, IBAN, A4I) and in partnership with most important players (LeVillage, Doorway, Spartan Capital, Pariter Partners, StartupWiseGuys). Vice President of the Italian Blockchain Association.

Massimo Romano
Associazione Blockchain Italia; Innova4 S.r.l.
E-mail: massimo.romano@associazioneblockchain.it
Bio-bibliographical note: Senior IT Consultant and R&D Manager with over 20 years of experience in designing, redesigning and integrating business information systems using blockchain technologies in recent years. Co-founder of the Italian Blockchain Association and Director of the blockchain-based traceability working group.