

Article

IGR Token-Raw Material and Ingredient Certification of Recipe Based Foods Using Smart Contracts

Ricardo Borges dos Santos ^{1,*}, Nunzio Marco Torrasi ¹  and Erick Reyann Kasai Yamada ¹
and Rodrigo Palucci Pantoni ²

¹ Center of Mathematics, Computing and Cognition, Federal University of ABC, Campus São Bernardo do Campo, São Paulo 09606-070, Brazil; nunzio.torrasi@ufabc.edu.br (N.M.T.); erick.yamada@aluno.ufabc.edu.br (E.R.K.Y.)

² Department of Eletrical Engineering and Computer Science, Federal Institute of São Paulo, Campus Sertãozinho, São Paulo 14169-263, Brazil; rpantoni@ifsp.edu.br

* Correspondence: ricardo.borges@ufabc.edu.br; Tel.: +55-11-97699-8217

Received: 24 November 2018; Accepted: 28 February 2019; Published: 11 March 2019



Abstract: The use of smart contracts and blockchain tokens to implement a consumer trustworthy ingredient certification scheme for commingled foods, i.e., recipe based, food products is described. The proposed framework allows ingredients that carry any desired property (including social or environmental customer perceived value) to be certified by any certification authority, at the moment of harvest or extraction, using the IGR Ethereum token. The mechanism involves the transfer of tokens containing the internet url published at the authority's web site from the farmer all along the supply chain to the final consumer at each transfer of custody of the ingredient using the Critical Tracking Event/Key Data Elements (CTE/KDE) philosophy of the Institute of Food Technologists (IFT). This allows the end consumer to easily inspect and be assured of the origin of the ingredient by means of a mobile application. A successful code implementation of the framework was deployed, tested and is running as a beta version on the Ethereum live blockchain as the IGR token. The main contribution of the framework is the possibility to ensure the true origin of any instance or lot of ingredient within a recipe to the customer, without harming the food processor legitimate right to protect its recipes and suppliers.

Keywords: food traceability; smart contracts; ingredient certification; Ethereum token; commingled foods; supply chain; intellectual property; recipe management; full chain traceability; solidity; ERC-20

1. Introduction: The Need for Traceability of Food Ingredients

The European Union ([1] p. 8) defines “food traceability” 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”. Traceability is needed to enable consumers, regulators, production and marketing actors in the foods supply chains to react to potential risks in food and feed, and to make sure that all food products within a certain territory are safe for consumption. A significant number of food poisoning related cases are investigated by official health departments and reported each year, affecting dozens of million people. Food services and restaurant chains suffer every year from lost sales through loss of consumer confidence as a result of such outbreaks.

Another common problem which may put consumers at risk and that could be reduced by reliable food traceability systems is food fraud [2]. Food fraud is a common type of crime which typically abuses the consumer by mislabeling food items in order to induce consumer purchase

but uses ingredients that are not the ones indicated or by making misallegations on the sources of the ingredients.

It is paramount that, when food businesses identify potential risks to customers or brands, these can reliably and quickly be traced back to its sources and the suspect materials be segregated thus avoiding them from reaching consumers.

Efficient traceability allows for targeted recalls, reducing the eventual cost of the recall of false positive items. It also allows for more accurate information to the public, reducing damage to the brand image. These costs can be very high as has been demonstrated in recent cases, such as with the European dioxin contamination, Chinese milk products contaminated by melamine [3] and the horse meat salami scandal in Europe [4]. In several cases [5–8], food unsafe for human consumption was, according to their manufacturers, quickly identified and isolated. This protected consumer health from food poisoning risks and consumer good faith from counterfeit, malicious information or fraud, albeit without a third party certification and with significant costs.

Recurring examples are available from “Monthly Summary of Articles on Food Fraud and Adulteration” (<https://ec.europa.eu/jrc/sites/jrcsh/files/jrc-food-fraud-summary-september-2017.pdf>). Additionally the FDA publishes several of the known food recall actions in their web site. A brief analysis of this list typically shows one dozen cases every month for recall actions. The direct and brand damage costs involved in a recall action cannot be overestimated.

Both in the food poisoning and the food fraud cases, a recall action of the suspect items is mandatory by law and necessary to maintain brand confidence. Any recall intervention should be as fast and as precise as possible, avoiding as much as possible the undue cost of recalling products that are safe.

The increasing discussion on genetic modified organism (GMO) labeling spurs the public to question the origin and the reliability of the track record a food product. The final consumer has the right to know not only where the ingredients and associated products come from, as well as the processing methods, but also the reliability of the sourcing information made available to the consumer on labels.

Consumers have not only shown increasing concern with the origin of the ingredients in their food, but some are apparently willing to pay more for quality. According to ([9] p. 1) “A portion of consumers display traceability consciousness, and are willing to pay a premium for traceable food products”.

For recipe based foods, i.e., foods that derive from processes of commingling a fixed proportion of ingredients, due to the complexity of tracing all ingredients, the focus has been on the traceability of some premium ingredients.

Case studies for full chain traceability, i.e., from farm to consumer, are available for foods in general [10] but none for recipe based foods was found. This is due to opposed needs between consumer and processor of recipe based food brands. A direct conflict of interests between consumer and food processor requirements arises. The increasing interest of consumers in tracing specific ingredients in the recipe, rather than just believing in the claims on the labels, clashes with the manufacturer’s legitimate right to protect their business sensitive information concerning these recipes and suppliers. An efficient method that can be used for certification of ingredients without jeopardizing the commingler’s interests is needed. This method must reliably capture data on each transformation and transfer of custody of these specific ingredients along the food chain without hurting the requirements of each stakeholder in a transparent and trustworthy manner.

Blockchain technology (BCT) has been identified as advantageous for many applications requiring public verifiable certification and integrity as in postal and lottery services [11,12]. Applications requiring also transparency and privacy such as Supply Chain Management (SCM) adopted BCT as did Skuchain (Skuchain, 2017. <https://www.skuchain.com/>), Provenance (Provenance, 2017. <https://www.provenance.org/>) and Everledger (Everledger, 2017. <https://www.everledger.io/>) as well as applications for traceability of goods in complex distributed business environment [13–15].

One of the blockchain's attributes that may help solve this conflict is the open nature of the code of the smart contracts [16,17]. A further property is the tamper proof and universal access nature of information recording method [18].

The method also needs to detect if these valuable ingredients are used in a fraudulent manner, i.e., avoid double-spending [19] of these ingredients. In this manner, the method builds trust among the stakeholders and particularly the consumer about the origin of key ingredients used. Since the certified products and the certified ingredients they use will probably reach higher end prices, and BCT tends to reduce transaction costs, all the actors in the supply chain would be encouraged to use the method.

In summary this research was motivated by the conflict between:

- Increasing interest of consumers in tracing any type of goods, including foods, particularly the specific case of recipe based foods, rather than just believing in the claims on the labels;
- The commingler's legitimate right to protect their business sensitive information concerning these recipes and suppliers.

This paper investigates the traceability requirements in recipe based foods and proposes an alternative solution to full chain traceability. It proposes a food ingredient certification framework capable of maintaining the non disclosure of business sensitive data for foods that derive from commingling operations using the blockchain.

This paper is organized as follows: Section 2 describes the key definitions and requirements for traceability, data collection and organization along with some available solutions and their main characteristics. Section 3 details the traceability aspects related to ingredients within recipes. Section 4 summarizes BCT as currently applied to Supply Chain Management. Section 5 justifies the use of BCT in the case of ingredient certification. The Section 6 presents the supply chain to token synchronization concept. Section 7 addresses the algorithms and steps for the certification. Section 8 discusses the smart contracts and implementation of the IGR token used to demonstrate the feasibility and usage of the certification framework. Section 9 summarizes the results obtained and finally Section 10 presents conclusions.

2. Traceability of Food: Key Definitions, Requirements and Review of Food Traceability Frameworks

The trustworthiness of the information concerning the ingredients of a food article and the nature of this information has been the focus of a large number of researchers.

For the purpose of this research, we use the concept of ingredient as being any of the components that are mixed to form a recipe. The concept of raw material is restricted to the components at their original state as of the moment they were extracted or harvested.

The Traceable Resource Unit (TRU), originally defined in ([20] p. 12) for batch processing of foods, was adapted by the ISO 22005/2007 (ISO 22005:2007 Traceability in the feed and food chain-General principles and basic requirements for system design and implementation (<https://www.iso.org/standard/36297.html>). "Traceable lot" is defined as the "set of units of a product which has been produced or processed or packaged under similar conditions". Further, the concept of granularity [21] describes the level and the size of the units in a traceability system have reached widespread agreement among models of food traceability and the analysis of food recall actions.

The literature shows various proposed solutions to trace the life cycle of food products.

Lo Bello [22] proposed a broad framework for a network for traceability of food supply chains, mostly focused on reducing the high latency time or uncertain response times for end-user traceability queries. The framework is capable of processing ad-hoc queries to the recipe based food chain traceability databases, although issues concerning Quality of Service, response times and above all the storage, processing costs and access rights to the server traceability database was identified as a setback.

Cimino [23] proposed, within the Cerere (Cerere website—<http://cerere2020.eu>) project, an information system supporting traceability using electronic business extensible Markup Language

(ebXML) (ebXML website—<http://www.ebxml.org>), that allows users to build loosely interconnected databases.

Similarly [24] introduced the “TraceFood” framework containing recommendations for “Good Traceability Practice”, common principles for the unique identification of food items as well as a common generic standard for electronic exchange of traceability information (TraceCore XML).

We understand that both these frameworks lacked practical usage due to the confidentiality and control of data issue inherent to the recipe based food chain.

Bechini [25] builds on the CERERE project to introduce a data model for traceability and a set of patterns to encode generic traceability semantics and a suitable technological standards to define, register, and enable business collaborations. The Unified Modeling Language (UML) activity diagram shown in Figure 1 includes the responsible actors and the transitions involved in a traceable ingredient processing system.

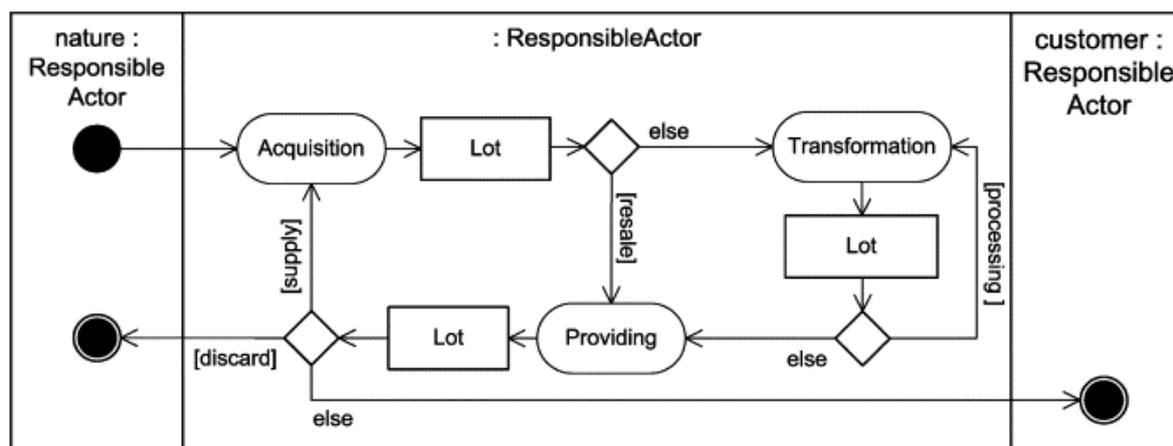


Figure 1. UML activity diagram describing the behavior of one instance of a food ingredient lot [26].

Traceability requires that an individual specific instance of a food ingredient: The TRU, lot or batch, be identified and positively followed. Since most industrial food packaging operations use the same date coding for production batches of typically one work shift per production line producing one specific package, this is chosen as the TRU. The date coding is required by law. Lots need to be individualized both externally, i.e., between businesses, but also internally, i.e., within a factory or warehouse. The traceability granulometry is thus one lot.

This calls for an information system able to manage an unique ID for each lot as well as some disciplined method to name and tag each lot unambiguously. The international standardization organization GS1 (GS1 official website—<https://www.gs1.org>), proposes an industry accepted internal and external traceability methodology by means of a well accepted criterion for individualization of lots and packages using the so-called stock keeping unit (SKU) code. The most important contribution of GS1 is the de facto individualization of each product instance by means of its unique SKU appended by the lot date code as seen by consumers on food labels.

Once a specific instance of a food item is identified, it is necessary to record data on the transitions that this item goes through, in order to keep record of its path from farm to consumer. Which pieces of data should be recorded as a minimum? The Institute of Food Technologists (Institute of Food Technologists official website—<http://www.ift.org>) (IFT) made significant advances to answer this question and provided a broad and powerful framework to apply traceability to food items in different segments [27]. These requirements were homogenized for the six major food supply chains families and sets forth a set of structured requirements for the six food chains segments: Baked foods, dairy, meat and poultry, prepared processed foods, produce and fruit as well as fish and seafood. Typical actors within each of the six main food supply chain families can be established as per Table 1.

Table 1. List of typical actors and stakeholders for different food chains [27].

Stakeholder	Recipe Based Foods			Non Recipe Based Foods		
	Bakery	Dairy	Processed food	Meat and poultry	Produce	Seafood
X = applicable stakeholder for that sector.						
Farm, grower, hatchery	X	X	X	X	X	X
Raw material, bulk supplier	X	X	X	X		X
Processor, manufacturer	X	X	X	X		X
Packer	X	X		X	X	
Distributor, wholesaler	X	X	X	X	X	X
Repacker	X	X		X	X	
Retailer, food service	X	X	X	X	X	X
Consumer	X	X	X	X	X	X

IFT (<http://www.ift.org/gftc/~media/GFTC/Events/BestPracticesinFoodTraceability.pdf>) analyzed requirements for traceability data in various stages of processing and consolidated the concepts of Critical Tracking Events (CTE) along with the corresponding Key Data Elements (KDE).

A CTE is described as any event along the chain of transformation or hand over of a food product instance where a supply chain actor makes changes to the nature or to the custody of the product lot.

Each CTE generates one particular record of data, the so called corresponding KDE, to ensure the flow of information is kept linked to the physical product flow.

The generic list of CTEs and associated KDEs is applicable to all food families as per Table 2. While some particular events do not occur in some food supply chains, or thus some KDEs need not be collected, and whilst nomenclature may differ from one food chain family to another, from a traceability perspective, “food is handled and distributed across the value chain in a fairly consistent manner.” [27].

The capture of each CTEs with their respective KDEs are understood to be the necessary and sufficient condition to assure traceability of one specific food lot across any of the food chain families.

Table 2. Typical Critical Tracking Events (CTE) and corresponding Key Data Elements (KDE) for food supply chain families (adapted from [27]).

IFT Suggested Key Data Elements (KDEs) for Capture and Record Keeping at Critical Tracking Events (CTEs)						
	Critical Tracking Events (CTEs)					
	Transportation (Exchange of Goods)		Transformation (Creation/manipulation of Products)		Depletion (Exit from System)	
	Shipping	Receiving	Input	Output	Consumption	Disposal
Required KDEs						
Event Owner (firm submitting information)	X	X	X	X	X	X
Date/Time	X	X	X	X	X	X
Event Location	X	X	X	X	X	X
Trading Partner	X	X	X			
Item (the good)	X	X	X	X	X	X
Lot/Batch/Serial Nr.	X	X	X	X	X	X
Quantity	X	X	X	X	X	X
Unit of measure	X	X	X	X	X	X
Linking KDEs						
Activity Type (for example, Purchase Order, Bill of Lading, Work Order)	X	X	X	X		
Activity ID (number associated with PO, BOL, Work Order)	X	X	X	X		
Transfer typeb	X	X				
Transfer numberb	X	X				
Lot/Batch Relevant Datec	X	X	X	X	X	X
Carrier ID	X	X				
Trailer number	X	X				

The IFT methodology has been extended by GS1 through the “GS1 Global Traceability Standard” (https://www.gs1.org/sites/default/files/docs/traceability/GS1_Global_Traceability_Standard_i2.pdf) which focuses on the data management aspects of traceability. It identifies and references the necessary requirements for capturing and sharing data “for full chain traceability meeting practical regulatory and industrial requirements”. Albeit using slightly different nomenclature, GS1 and IFT are compatible with each other and with the ISO 22.000 (ISO 22000:2005 Food safety management systems: Requirements for any organization in the food chain) philosophy as well as Hazard Analysis and Critical Control Point (HACCP) systems.

The GS1 methodology is focused on the three main tasks: Identify, capture and share the instances of the food products and has achieved a widespread acceptance for the unique identification and the capture of the flow of industrialized product.

Today, most retail food products are marked with the GS1 coding. A typical food product instance can be identified through its SKU bar code plus Lot Number or Lot “best before” date.

Neiva [26] showed the logical architecture capturing the main activities, responsibilities, boundaries, and services involved in the traceability business process based on a use case model as proposed by the GS1 standard.

A comparison of the consolidated CTE-KDE with Cerere and with GS1 (https://www.gs1.org/sites/default/files/docs/traceability/GS1_Global_Traceability_Standard_i2.pdf) methodology for the different supply chain families can be seen in Table 3. It is noteworthy to mention that all three methodologies are fairly convergent.

Table 3. Comparison of consolidated CTE for the different supply chain families [27] with Cerere [23] and GS1 methodology.

Category	CTE	Cerere-UML Activity Diagram	GS1 Global Traceability Standard	Bakery	Dairy	Meat and Poultry	Processed Food	Produce	Seafood
X = applicable CTE for that sector.									
Creation	Harvest, hatch, grow, catch	Extracted	Receiving	X		X		X	X
Transformation	Separate, sort	Transformed	Transformation		X			X	X
Transformation	Combine, mix, commingle	Transformed	Transformation	X	X	X	X	X	X
Transformation	Process, production	Transformed	Transformation	X	X	X	X		X
Transformation	Batching	Transformed	Transformation	X	X	X	X		X
Transformation	Pack, package	Transformed	Transformation	X	X	X	X	X	X
Transportation	Load, order	Provided	Movement	X	X	X	X		X
Transportation	Ship, transport	Provided	Movement	X	X	X	X	X	X
Transportation	Receive, and unload	Acquired	Movement						
Transportation	Store, warehouse	Acquired	Storage	X	X	X	X		X
Transportation	Return	Acquired	Movement	X		X	X		
Depletion	Discard, dispose, loss	Damaged	Destruction	X	X	X	X	X	X
Depletion	Use or Sell to consumer	Consumed	Usage	X	X	X	X	X	X

Note that the bakery, processed food and dairy foods families deal mostly with recipe based, i.e., commingled food products. In these families, the tasks of keeping a traceability trail of one specific food lot is intertwined with that of other food lots due to the commingling of different ingredients each of which with their own traceability trail.

Nevertheless, the GS1 methodology requires further support for certification of recipe based foods due to the reluctance of the recipe owners to have their business sensitive data disclosed.

3. Traceability of Ingredients Within Recipes

For commingled foods segments such as recipe based, animal feed, processed and dairy foods, although internal CTEs with their KDEs are usually captured, they are rarely shared. This is probably due not only to the increasing complexity of recipes and products, the geographical dispersion of the

supply chain actors and the intense competition between recipe based foods producers, but also to the recipes being an important competitive factor within the business models of these producers.

Food products that have shown full chain traceability are mostly of the produce or meat or fish supply-chain. Within these families most of the supply chain processes are those of separating parts of a larger item into smaller pieces, and therefore the traceability procedure are reduced to an obvious sub itemization concept.

These three first families: Fruit, meat and poultry, typically involve operations where no recipes or commingling operations are involved. In the case of these families a number of full-chain traceability cases are reported. For fruit and produce traceability, software tools based on dedicated server-client hand held devices are available and reported to be reliable such as HarvestMark (<https://www.harvestmark.com/>). For the meat and poultry and the fish and seafood families, the literature reports a few successful use cases (Walmart and IBM will use blockchain to track pork from China, <https://finance.yahoo.com/news/walmart-and-ibm-will-use-blockchain-to-track-pork-from-china-142530691.html>).

On the other hand, very few full chain traceability use cases are reported for recipe based foods. In fact, businesses are extremely reluctant to, if not totally against, making their recipes or sub suppliers public. This data is considered to be business sensitive information and is typically kept internal to corporate databases. Protecting corporate recipes and suppliers data is a legitimate business goal. All recipe information is handled as classified information, almost as intellectual property and, as such, should not to be made available to external public or competitors.

Additionally, most large business use extensive marketing efforts to promote trust in their brands and recipes, pushing consumers to see their corporate name as the trustworthy element behind customer choices [28]. When a corporation claims to use some differentiated ingredient or raw material they support their claim through the trust that has been built by their marketing efforts.

Further, more and more recipe based food producers claim to use special socially, environmental or health related added value ingredients. Are these claims for the use of special added value ingredient trustworthy? How can a serious recipe based food processor evidence his claim without hurting his trade secrets? This impasse explains the small number of publications showing full-chain traceability of recipe based foods.

Nevertheless, we will show that with the use of the Blockchain and Smart Contracts it is possible to obtain, even for the recipe based foods, an alternative to traceability by means of the certification of specific ingredient value properties all the way from harvest source to the final consumer through third party certificates issued by any desired authorities.

The traceability of foods use case diagram [26] was extended to show the separation of the Business-sensitive-data from the Non-business-sensitive-data as shown in Figure 2.

As an alternative to full traceability of all ingredients, we will show that certification of a specific ingredient, from source to final consumer, is possible without compromising the business sensitive information of the commingler. This can be achieved by means of open source code and freely accessible data structure such as those inherent to BCT.

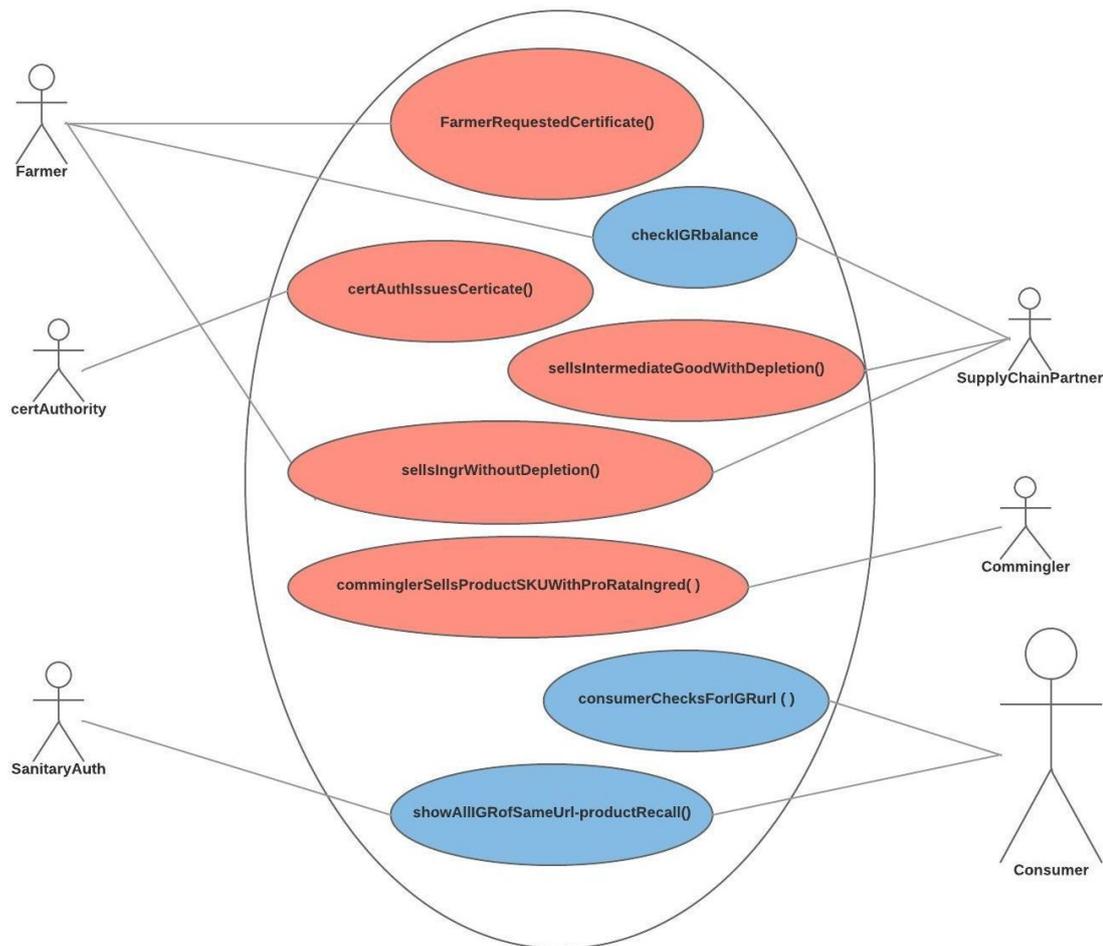


Figure 2. Traceability and Ingredient Certification use case (adapted from [26]).

4. Supply Chain Management and BCT

Recent research literature involving the keywords “supply chain management”, “traceability” and “blockchain” and “blockchain technology” [16,29–31] have shown that the traceability of pharmaceutical and foods, both recipe based type of products, are important fields that gain increasing researcher’s interest. Indeed BCT shows several advantages that can boost the information provenance to food ingredients. Nevertheless the references of those article do not address the recipe business sensitive concern.

Bitcoin [32], the first cryptocurrency, introduced the concept of a scarce digital objects and BCT to avoid double-spending of a digital asset. Ethereum [18] expanded the concept to include programs that are executed independent of human command, the so called smart contract and decentralized applications expanding the blockchain utility. These distributed technologies provide the needed transparency and prevention mechanism to possible double-spending frauds for the ingredient chain certification system.

“A central aspect of BCT is the distributed ledger, which contains a record of all previous transactions. It is called a distributed ledger because it is not stored in a central location, rather it is stored across a network of computers across the world. Key to the operation of a distributed ledger is ensuring the entire network collectively agrees with the contents of the ledger; this is the job of the consensus mechanism” (<https://hackernoon.com/consensus-mechanisms-explained-pow-vs-pos-89951c66ae10>).

The blockchain is a collaborative distributed ledger replicated in several physical locations, capable of maintaining its information integrity. This allows for companies doing business within

a production and marketing chain—such as raw material producers and crop growers, processing companies, re-packers, transportation companies, distributors and retailers—to record concurrent transactions securely on a global basis [14,33–35]. “The BCT as a foundation for distributed ledgers offers an innovative platform for a new decentralized and transparent transaction mechanism in industries and businesses. The inherited characteristics of this technology enhances trust through transparency and traceability within any transaction of data, goods, and financial resources.” [36,37].

The technology behind blockchain smart contracts successfully implements the access integrity for collaborative databases in the form of distributed ledgers for trust-less computing environment. The underlying data structures and control mechanisms with validation through proof of work stakeholders show that this technology is an important step towards supply chain transparency of traceability data [38,39].

Blockchains are cryptographically auditable, append only, tamper resistant, distributed data structures accessible to anyone by means of a web browser [17]. Blockchains require no central trust mechanism, hence no central point of failure. Smart contracts are intimately linked to BCT and allow for extensive development and control ensuring transparency of each data manipulation and thus trust.

BCT's main strengths are:

- Software driven, i.e., BCT does not require human privileged operators to maintain and operate the transactions, thus the system is not prone to bribery;
- Tamper resistant, making it impossible to change data that has been recorded;
- Pseudo anonymity: Data is available publicly but encoded through hashes of keys that allow for certification without disclosing trade secrets;
- Distributed presence: The data structures are replicated maintaining full integrity with each other data set in a perfectly smooth manner;
- Allows for certification of the tamper proof storage of large volumes of data in a side blockchain. through the use of hierarchically certified sub-blockchains database which can also hold much more data than what retailers get today, providing tools for more detailed analysis, including certification of multimedia content.

On the other hand, BCT, in its current proof-of-work implementation, has shown weakness in the aspect of scalability, slow speed of transaction validation and high energy usage ([40] p. 5), especially in the case where a larger volume of data needs be kept, the blockchain may not be the ideal solution. All of these issues are currently receiving a lot of improvement efforts.

Permissionless or Permissioned Blockchains

To store large data on the blockchain can be costly and cumbersome. Since BCT uses a replicated database, every single node on the network would have to manage all data.

The type of read and write access restrictions imposed on the data of a blockchain established the nomenclature: Permissionless and permissioned blockchains as opposed to private centralized database [41].

Permissionless blockchains are those that grant anyone read and write access, provided and validated by the corresponding smart contracts. These include the original Bitcoin, Ethereum, Rinkeby Testnet and several other blockchain projects accessible through web browser applications.

Permissioned blockchains are those that selectively grant anyone read and restrict write access, also provided and validated by the corresponding smart contracts or access methods. Some examples of permissioned blockchains are Hyperledger [13] and Corda [42].

5. Is Blockchain the Right Tool for Ingredient Certification?

Do we need BCT in the case of ingredient certification? Is blockchain appropriate? If yes, what type of blockchain can better address the valued ingredient recipe food certification problem?

The available options are to use: No database, traditional centralized database, public blockchain or permissioned blockchain. According to the requirements of each problem it is important to select the

appropriate tool for the job and avoid using unnecessary resources. For this purpose the literature ([43] p. 10, [41]) appoints some interesting methods to check if the tool to be used fits the problems requirements.

Classical Database or Blockchain selection steps

The selected methodology is shown in flow diagram in Figure 3 from ([43] p. 10).

In this case of ingredient certification, the application of this procedure leads to:

- a Do we need to store current State? Yes, each traceability partner needs to know the current state of each ingredient he is dealing with.
- b Can you use an always online Trusted Third Party? No, because there are no such entity or services available.
- c Need shared write access outside your organization? Yes, because all participants in the ingredient supply chain are from different companies, which are separate, not always trusted, legal entities.
- d Are all writers known? No, for the same reason as above.

This leads us to recommended data storage strategy 5: Permissionless blockchain, which is the *Public Ethereum Blockchain* chosen for the job.

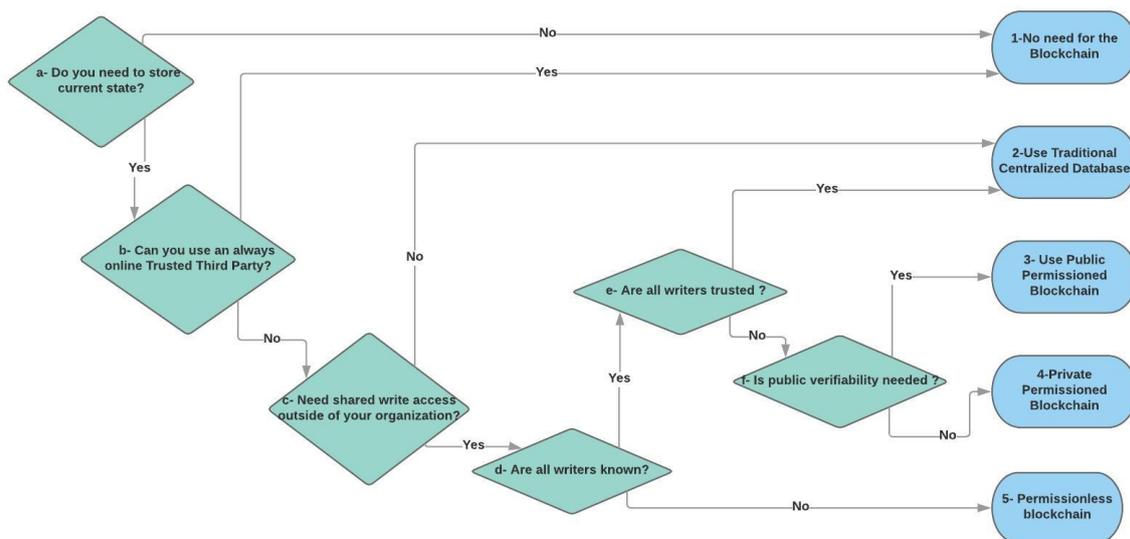


Figure 3. Defining if and what type of blockchain is the right choice for the problem: [43].

Application of Blockchain to Food Traceability

BCT has brought about a great deal of interest in several fields of applied research. Some recent academic reviews [44] evidence the broad range of use cases that can benefit from BCT. Figure 4 shows a structured classification of the many use-cases.

Recent work [29] analyzes 11 reported blockchain cases where five were traceability or supply chain management examples: Provenance, Ali Baba’s “Food Trust Framework”, “Everledger”, Walmart’s pork, intel’s “sawtooth”.

Whilst Provenance (Provenance website—<https://www.provenance.org/>) is a smart contract based decentralized application implemented as an Ethereum use case, focusing on the pedigree of historical data of physical assets for traceability and anti-counterfeit purposes, it lacks practical use for recipe based foods.

Provenance (from the french word “provenir”: to come from) relates to the chronological chain of ownership, custody or location of an historical object. Originally mostly used in relation to works

of art, the term is used today in a broader sense to denote backward traceability of objects in general including materials or intellectual property. To establish provenance is to keep precise and reliable documentation on the transfer of ownership of each asset.



Figure 4. Blockchain technology (BCT) Applications Taxonomy [44].

6. Tracing Ingredient Value Properties and Their Certificates with Tokens

Consumers are becoming more demanding and require different processes and raw-materials in food they consume. Claims such as non-genetic-modified seeds, organic crop cultures, agro-chemical free, gluten-free are often included in product advertisements, but manufacturers are seldom willing to provide evidence for those claims.

We here define such positive attributes of the raw materials used by a specific food product as an ingredient value property. The concept can also include claims of geographical origin such as “Oregon Potatoes”, “Champagne Sparkling Wine” or “Hallertau Hops”.

For the certification of ingredients we created an Ethereum token — the Ingredient Token (IGR). Making sure that for each change of custody of the food ingredient, the corresponding transfer of token takes place is the main challenge.

Figure 5 shows the synchronization between flow of food lots and the flow of information through the IGR token, in order to evidence to a final consumer that a certain instance of a recipe based food ingredient effectively contains a certain ingredient value property.

types of processing or changes of custody for each specific lot from farm to consumer: “Sale without depletion”, “sale with depletion” and “sale from commingler”.

“Sale without depletion” is the operation in which the delivered lot has exactly the same mass as the mass of the ingredient received or harvested. This is opposed to the “sale with depletion”, where the incoming lot will lose part of its mass, e.g., milling operation where the grain will lose part of its mass when the husk is separated from the grain that will be sold as milled grain. On the other hand, the commingling operation mixes this ingredient in fixed proportions with other ingredients. These states and transitions are pictured in the state diagram Food Ingredient Transition Diagram in Figure 6.

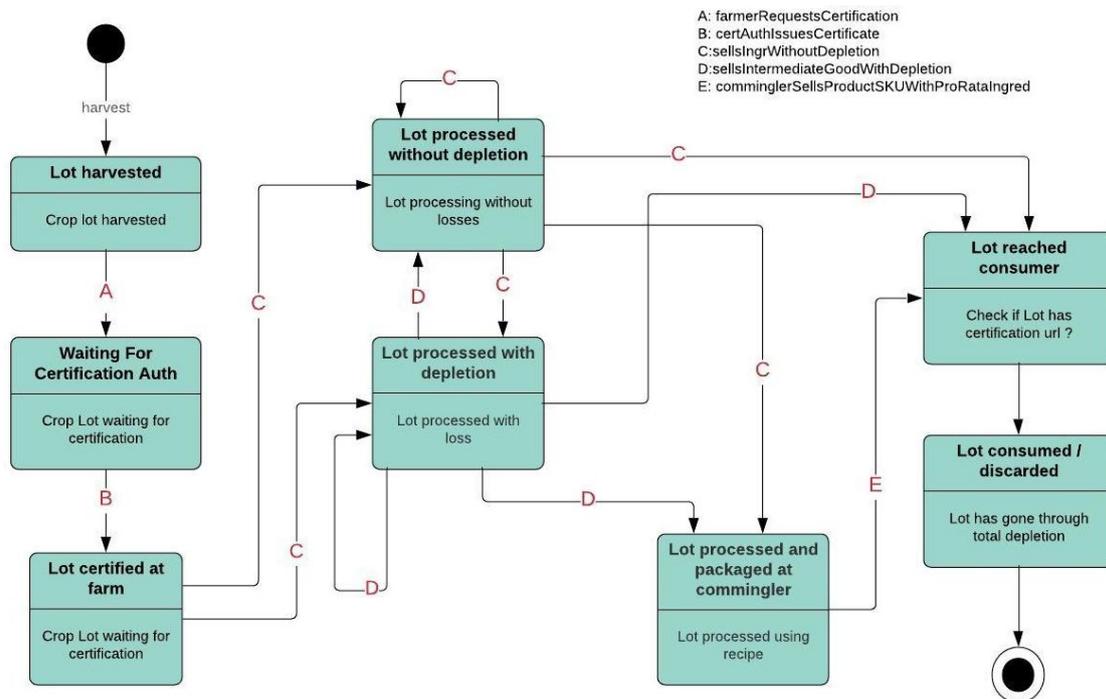


Figure 6. Food Ingredient State Transition Diagram.

In order to keep the provenance of the ingredients, it is necessary to use routines that will link six entities:

- Farmer
- Certification authority
- Reseller (sell without depletion)
- Processor (sell intermediate good with depletion)
- Commingler
- Consumer

The first five of these entities need to write to the Ethereum blockchain. The consumer and any other interested party may read from the blockchain, at any time without any difficulty, using a mere web browser (e.g., <https://etherscan.io>).

At the very start, a Farmer will request a freely chosen certification authority to certify one specific lot of an ingredient through the procedure “farmerRequestCertificate()”. The request to the certification authority requires information such as: Public address of certification authority, quantity of ingredient to be certified, name of ingredient, the property that the ingredient meets that will add value to this ingredient, location of harvest (typically the GPS coordinates of the harvest) and date of harvest.

In the following step, the certification authority will inspect the farmer and use the smart contract to confirm that the claimed ingredient properties are trustworthy. After inspection, the certification

authority will typically issue a public certificate on a webpage under its domain, i.e., URL. To make the certification data publicly available, the authority will perform the “certAuthIssuesCertificate()” procedure with parameters: Public address of farmer, amount of certified ingredients, URL in the web site, name of ingredient, ingredient value property, location and date of production. Once confirmed by the certification authority, the farmer can sell ingredients and transfer the corresponding IGR tokens certifying the trustworthiness of its property.

When selling ingredients, farmers should use the procedure “sellsIngrWithoutDepletion()” to transfer custody of the IGR tokens related to those ingredients. This requires the following parameters: Public address the new holder of tokens, quantity of ingredients, certificate URL. Typically the farmer transfers the ingredient to a first processor, typically known as a mill, although direct transfer to commingler or even to final consumer is also possible.

After the mill receives the custody of the certificates and the ingredients, he will typically process the food ingredients with some losses. The processed ingredient can be sold further, but, because the processing at the mill involves a depletion, it is necessary to specify the percentage of mass reduction involved. Typically the selling of ingredients with depletions requires the following procedure “sellsIntermediateGoodWithDepletion()” with these parameters: Public address of new custodian, quantity of ingredients, URL, mass ratio of output to input in percentage.

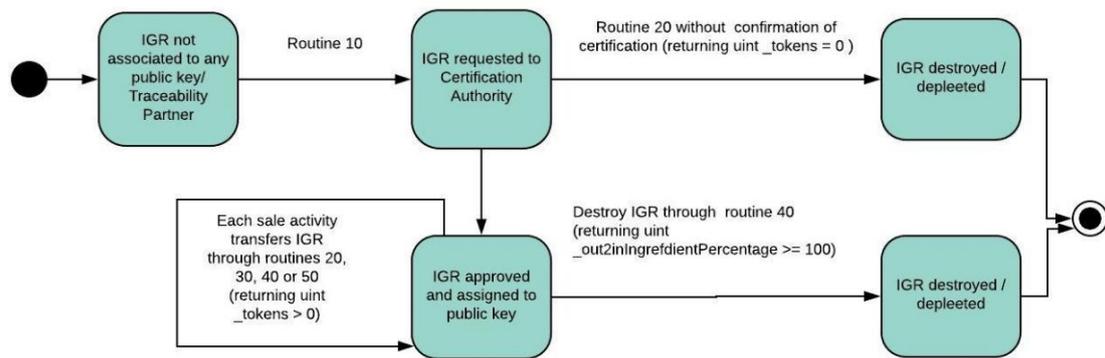
Once the ingredient is available to the commingler, the mass of the certified ingredient used in each SKU, according to the recipe, can be recorded in a manner that allows the end consumer to easily check for the presence of IGR tokens in the blockchain. In order for the final consumer to be able to check if a certain lot carries certified ingredients via IGR tokens, the SKU GTIN-13 identification, alongside the lot validity date will generate a public key in the Ethereum blockchain.

This blockchain public address will be credited with the corresponding tokens through the procedure “comminglerSellsProductSKUWithProRataIngr()” with the exact mass (in grams) of the certified ingredient. With the information that the consumer can read from the package, he can access the blockchain via a browser or via a dedicated Android application. The procedure needs as parameters: Public address of wholesaler or retailer, quantity of SKUs sold, URL, quantity of ingredient in the low level of SKU, GTIN 13 of package and “best consumed by” date.

Finally, for the consumer to confirm that the specific lot of food includes certified ingredients, the consumer only needs to read the SKU GTIN 13 and validity date of the product to access the blockchain. This will lead him to all the harvest data at the certification authority web page URL. The different states for the IGR token are pictured in the IGR token state transition diagram Figure 7. Food lots event transitions are followed by the IGR transitions every time change of ownership or custody takes place.

The implementation of the smart contracts followed the data flow diagram shown in Figure 8 which shows a generic case of ingredient provenance data being synchronized along its change of custody using the procedures of the IGR smart contract.

The motivation for the IGR changes of ownership is a probable higher sales price for the ingredient when certified, in the sense that a certified ingredient is more valuable than a non-certified equivalent. This mechanism is the driving force for the synchronization of the ingredients with the certification flow of data as shown in Figure 6.



Routines

- 10: farmerRequestCertificate (address _certAuth, uint _tokens, string _product, string _IngValueProperty, string _localGPSProduction, uint _dateProduction)
- 20: certAuthIssuesCertificate (address owner, address _farmer, uint _tokens, string _url, string _product, string _IngValueProperty, string _localGPSProduction, uint dateProduction)
- 30: sellsIngrWithoutDepletion (address _to, uint _tokens, string _url)
- 40: sellsIntermediateGoodWithDepletion (address _to, uint _tokens, string _url, uint _out2inIngreDientPercentage)
- 50: comminglerSellsProductSKUWithProRataIngreD (address _to, uint _numSKUsSold, string _url, uint _qtyIGRinLLSKU, string _GTIN13, string _YYMMDD)

Figure 7. IGR token Transition Diagram showing token states as triggered by smart contracts.

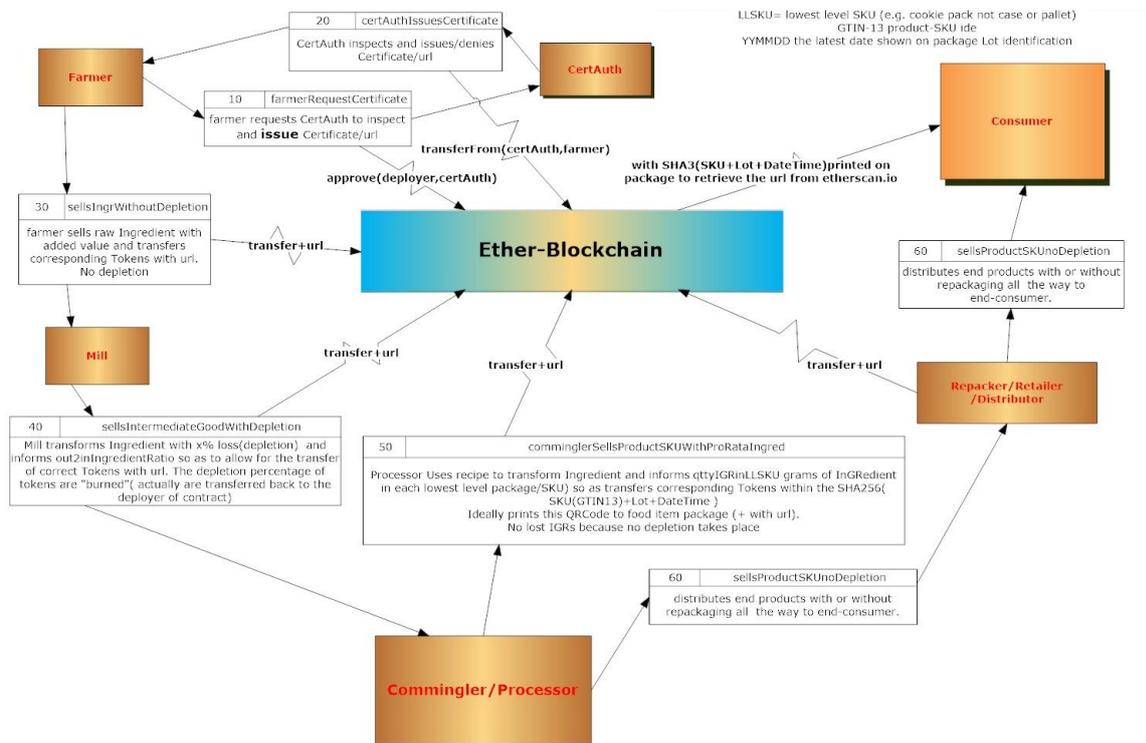


Figure 8. IGR token data flow diagram.

8. Smart Contract Implementation and Usability

The above procedures were implemented in the Ethereum environment after being coded as smart contracts, using the Solidity programming language [45]. Solidity is a development language for smart contracts for the Ethereum platform created in 2014 by the Ethereum team [18] in order to facilitate the development of smart contracts. Similar to JavaScript, it uses the concept of contract-oriented programming.

To assure functionality, the code was tested in the Rinkeby (Rinkeby—<https://www.rinkeby.io>) Blockchain [46] environment using several datasets including public data [47]. After several improvements, the successful code implementation of concept was deployed as a live Ethereum smart contract application under the token IGR.

The IGR token contract (IGR token smart contract source code—[HTTPS://etherscan.io/address/igrtoken.eth](https://etherscan.io/address/igrtoken.eth)) shows the complete code for the current IGR preliminary implementation. Noteworthy is the code for the commingler which ascertain to the recipe owner that only the exact ingredient count within each SKU is made available to the public, not the full recipe.

The usage of this code within the testnet Rinkeby blockchain with practical examples such as peanuts, cocoa beans, apple juice and other ingredients to recipe based foods showed the feasibility of using the IGR token as a certification methodology of ingredients from farmer to consumer without exposing the recipe owner business sensitive information.

The proposed solution data storage requirement fits into one blockchain transaction structure, and provides efficient query response times and scalability. Since the blockchain is a linear data structure, the time needed to obtain the certification URL of any ingredient is linear and proportional to the number of links in the supply chain.

Thus the blockchain being a linear data structure, the search complexity for a query is estimated to be $O(n * i + m)$ where:

- n is the number of backstream CTEs, i.e., supply chain links, from farm to commingling operation,
- i is the number of ingredients for which value properties need be certified and,
- m is the number of upstream CTEs, i.e., links from commingled traceability partner to final consumer.

9. Results Obtained

The proposed research objective and methodology involves testing the following hypothesis:

IF a commingler, i.e., manufacturer of recipe based food, accepts to disclose the exact mass of one key ingredients, the so called value perceived ingredient, THEN consumers would accept to reduce the scope of the traceability to viewing a certificate of the value ingredient at a trusted third party (authority) web site. Nevertheless, it is also necessary to show to the commingler that the smart contracts are totally transparent and their recipe will not be requested, therefore never be disclosed.

To show the commingler that the information that will be made public about his recipe is limited to the mass, in grams, of the selected value ingredient we refer to the open source code of the smart contract *function comminglerSellsProductSKUWithProRataIngrd(...) public returns (bool success)* which shows that the parameters required by the function are limited to contract *qtyIGRinLLSKU*, i.e., the quantity of ingredient contained at the lowest level SKU. This is the only information that the commingler will release to the public.

The objectives of the research also involve implementing and testing the algorithms that discipline the generation and propagation of the certification URL as well as the public keys entries of this data within the blockchain.

10. Conclusions

This paper investigates the traceability requirements in recipe-based foods and proposes an alternative solution to full chain traceability by focusing on ingredient certification. It proposes a food ingredient certification framework capable of maintaining the non disclosure of business sensitive data for foods that derive from commingling operations. The certification starts at the farmer stage and allows for propagation of the certificate to the consumer using blockchain based smart contracts to push the URL of the certificate of any desired ingredient.

To achieve this, the methodology uses an integrated set of smart contracts to: Allow farmers to request an external authority to issue qualitative and quantitative certification of any consumer value perceived property; issue the corresponding quantity of IGR tokens; impose a disciplined transfer of these tokens along the supply chain transactions; provide consumers with a practical method to scan the food package SKU and lot number so as to visualize any corresponding certificate URL thus obtaining the desired assurance.

At each Critical Traceability Event (CTE) the corresponding certificate URL will be transferred through a token transfer transaction by the traceability partners involved in the transfer of custody. The open source nature of the code that implements these smart contracts assures the actors that no business-sensitive information will be disclosed. BCT disciplines the transfer of tokens such that no double-spending of these tokens would take place. Thus, the direct linkage from consumer to farm can be shown, without jeopardizing intellectual properties. In other words, the URL of the freely chosen certification authority will be synchronized with the physical exchange of custody or ownership of the food ingredients, without disclosing the proprietary recipe and supplier information. The framework can also be useful for tracking geographical certification of goods ensuring the proper transfer of ownership and no double spending.

The main contribution of the proposed framework for the certification of food ingredients of commingled products is to link the final consumer to the origins of the raw materials without disclosing the business sensitive information nor allowing the chain to double-spend the raw material value-certificates.

Author Contributions: R.B.d.S. conceived and designed the experiments; R.B.d.S. and E.R.K.Y. developed the Smart Contracts; all analyzed the data; R.B.d.S. wrote the paper, all reviewed the text.

Funding: This research received no external funding.

Acknowledgments: Acknowledgements to Zeppelin Systems Latin America Equipamentos Industriais Ltda for the support.

Conflicts of Interest: The authors declare no conflict of interest. Funding sponsors in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript.

Abbreviations

The following abbreviations are used in this manuscript:

BCT	Blockchain Technology
CTE	Critical Traceability Event as defined by [27]
DOAJ	Directory of open access journals
FDA	Food and Drug Administration
IFT	Institute of Food Technologists
IGR	Ingredient Token— HTTPS://etherscan.io/address/igrtoken.eth
KDE	Key Data Elements as defined by [27]
MDPI	Multidisciplinary Digital Publishing Institute
SCM	Supply Chain Management
TRU	Traceable Resource Unit as defined by [20]
UML	Unified Modeling Language
USDA	United States Department Agriculture

References

1. European Commission. Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety. *Off. J. Eur. Communities* **2002**, *31*, 1–24.
2. Aung, M.M.; Chang, Y.S. Traceability in a food supply chain: Safety and quality perspectives. *Food Control* **2014**, *39*, 172–184. [[CrossRef](#)]
3. Pei, X.; Tandon, A.; Alldrick, A.; Giorgi, L.; Huang, W.; Yang, R. The China melamine milk scandal and its implications for food safety regulation. *Food Policy* **2011**, *36*, 412–420. [[CrossRef](#)]
4. O'mahony, P. Finding horse meat in beef products—A global problem. *QJM Int. J. Med.* **2013**, *106*, 595–597. [[CrossRef](#)] [[PubMed](#)]
5. Mol, A.P.; Oosterveer, P. Certification of markets, markets of certificates: Tracing sustainability in global agro-food value chains. *Sustainability* **2015**, *7*, 12258–12278. [[CrossRef](#)]

6. Suk-Joo, L.; Ahn, C.; Song, K.M.; Ahn, H. Trust and Distrust in E-Commerce. *Sustainability* **2018**, *10*, 1015.
7. Vukatana, K.; Sevrani, K.; Hoxha, E. Wine traceability: A data model and prototype in Albanian context. *Foods* **2016**, *5*, 11. [[CrossRef](#)] [[PubMed](#)]
8. Ringsberg, H.A. Implementation of global traceability standards: Incentives and opportunities. *Br. Food J.* **2015**, *117*, 1826–1842. [[CrossRef](#)]
9. Sun, S.; Wang, X.; Zhang, Y. Sustainable Traceability in the Food Supply Chain: The Impact of Consumer Willingness to Pay. *Sustainability* **2017**, *9*, 999. [[CrossRef](#)]
10. Pigini, D.; Conti, M. NFC-Based Traceability in the Food Chain. *Sustainability* **2017**, *9*, 1910. [[CrossRef](#)]
11. Yanovich, Y.; Shiyarov, I.; Myaldzin, T.; Prokhorov, I.; Korepanova, D.; Vorobyov, S. Blockchain-Based Supply Chain for Postage Stamps. *Informatics* **2018**, *5*, 42. [[CrossRef](#)]
12. Liao, D.Y.; Wang, X. Applications of Blockchain Technology to Logistics Management in Integrated Casinos and Entertainment. *Informatics* **2018**, *5*, 44. [[CrossRef](#)]
13. Mao, D.; Wang, F.; Hao, Z.; Li, H. Credit Evaluation System Based on Blockchain for Multiple Stakeholders in the Food Supply Chain. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1627. [[CrossRef](#)] [[PubMed](#)]
14. Alcarria, R.; Bordel, B.; Robles, T.; Martín, D.; Manso-Callejo, M.Á. A Blockchain-Based Authorization System for Trustworthy Resource Monitoring and Trading in Smart Communities. *Sensors* **2018**, *18*, 3561. [[CrossRef](#)] [[PubMed](#)]
15. Yoo, M.; Won, Y. A Study on the Transparent Price Tracing System in Supply Chain Management Based on Blockchain. *Sustainability* **2018**, *10*, 4037. [[CrossRef](#)]
16. Kouhizadeh, M.; Sarkis, J. Blockchain Practices, Potentials, and Perspectives in Greening Supply Chains. *Sustainability* **2018**, *10*, 3652. [[CrossRef](#)]
17. Kirkman, S.; Newman, R. Using smart contracts and blockchains to support consumer trust across distributed clouds. In Proceedings of the 13th International Conference on Grid, Cloud, and Cluster Computing, WorldComp, GCC'17, Las Vegas, NV, USA, 17–20 July 2017.
18. Wood, G. Ethereum: A Secure Decentralised Generalised Transaction Ledger; Ethereum Project Yellow Paper; 2014; Volume 151, pp. 1–32. Available online: <https://gavwood.com/paper.pdf> (accessed on 24 November 2018).
19. Chohan, U. The Double Spending Problem and Cryptocurrencies. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174 (accessed on 27 January 2019).
20. Moe, T. Perspectives on traceability in food manufacture. *Trends Food Sci. Technol.* **1998**, *9*, 211–214. [[CrossRef](#)]
21. Karlsten, K.M.; Dreyer, B.; Olsen, P.; Elvevoll, E.O. Granularity and its role in implementation of seafood traceability. *J. Food Eng.* **2012**, *112*, 78–85. [[CrossRef](#)]
22. Bello, L.L.; Mirabella, O.; Torrisi, N. A general approach to model traceability systems in food manufacturing chains. In Proceedings of the 10th IEEE Conference on Emerging Technologies and Factory Automation, ETFA 2005, Catania, Italy, 19–22 September 2005; Volume 2, p. 8.
23. Cimino, M.G.; Lazzarini, B.; Marcelloni, F.; Tomasi, A. Cerere: An information system supporting traceability in the food supply chain. In Proceedings of the Seventh IEEE International Conference on E-Commerce Technology Workshops, Munich, Germany, 19 July 2005; pp. 90–98.
24. Storøy, J.; Thakur, M.; Olsen, P. The TraceFood Framework—Principles and guidelines for implementing traceability in food value chains. *J. Food Eng.* **2013**, *115*, 41–48. [[CrossRef](#)]
25. Bechini, A.; Cimino, M.G.; Marcelloni, F.; Tomasi, A. Patterns and technologies for enabling supply chain traceability through collaborative e-business. *Inf. Softw. Technol.* **2008**, *50*, 342–359. [[CrossRef](#)]
26. Neiva, R.; Santos, N.; Martins, J.C.; Machado, R.J. Deriving UML Logical Architectures of Traceability Business Processes Based on a GS1 Standard. In Proceedings of the International Conference on Computational Science and Its Applications, Banff, AB, Canada, 22–25 June 2015; pp. 528–543.
27. Zhang, J.; Bhatt, T. A guidance document on the best practices in food traceability. *Compr. Rev. Food Sci. Food Saf.* **2014**, *13*, 1074–1103. [[CrossRef](#)]
28. Farooq, U.; Tao, W.; Alfian, G.; Kang, Y.S.; Rhee, J. ePedigree traceability system for the agricultural food supply chain to ensure consumer health. *Sustainability* **2016**, *8*, 839. [[CrossRef](#)]
29. Kshetri, N. 1 Blockchain's roles in meeting key supply chain management objectives. *Int. J. Inf. Manag.* **2018**, *39*, 80–89. [[CrossRef](#)]
30. Tribis, Y.; El Bouchti, A.; Bouayad, H. Supply Chain Management based on Blockchain: A Systematic Mapping Study. *MATEC Web Conf.* **2018**, *200*, 00020. [[CrossRef](#)]

31. Francisco, K.; Swanson, D. The supply chain has no clothes: technology adoption of blockchain for supply chain transparency. *Logistics* **2018**, *2*, 2. [[CrossRef](#)]
32. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: <https://bitcoin.org/bitcoin.pdf> (accessed on 24 November 2018).
33. Tian, F. An agri-food supply chain traceability system for China based on RFID & blockchain technology. In Proceedings of the 2016 13th International Conference on Service Systems and Service Management (ICSSSM), Kunming, China, 24–26 June 2016; pp. 1–6.
34. Hofmann, E.; Rüscher, M. Industry 4.0 and the current status as well as future prospects on logistics. *Comput. Ind.* **2017**, *89*, 23–34. [[CrossRef](#)]
35. Cong, L.W.; He, Z. *Blockchain Disruption and Smart Contracts*; Technical Report; National Bureau of Economic Research: Cambridge, MA, USA, 2018.
36. Abeyratne, S.A.; Monfared, R.P. Blockchain ready manufacturing supply chain using distributed ledger. *Int. J. Res. Eng. Technol.* **2016**, *5*, 1–10.
37. Mao, D.; Hao, Z.; Wang, F.; Li, H. Innovative Blockchain-Based Approach for Sustainable and Credible Environment in Food Trade: A Case Study in Shandong Province, China. *Sustainability* **2018**, *10*, 3149. [[CrossRef](#)]
38. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [[CrossRef](#)]
39. Khan, S.; Haleem, A.; Khan, M.I.; Abidi, M.H.; Al-Ahmari, A. Implementing Traceability Systems in Specific Supply Chain Management (SCM) through Critical Success Factors (CSFs). *Sustainability* **2018**, *10*, 204. [[CrossRef](#)]
40. Pedrini, D.; Migliardi, M.; Ferrari, C.; Merlo, A. On The Case of Blockchain Adoption in the Internet of Things. *Proceedings* **2018**, *2*, 1231. [[CrossRef](#)]
41. Wüst, K.; Gervais, A. Do you need a Blockchain? In Proceedings of the 2018 Crypto Valley Conference on Blockchain Technology (CVCBT), Zug, Switzerland, 20–22 June 2018; pp. 45–54.
42. Brown, R.G.; Carlyle, J.; Grigg, I.; Hearn, M. Corda: An Introduction; R3 CEV: August 2016. Available online: https://docs.corda.net/_static/corda-introductory-whitepaper.pdf (accessed on 24 November 2018).
43. Wu, L. Blockchain Smart Contracts in Megacity Logistics. Ph.D. Thesis, The Pennsylvania State University, State College, PA, USA, 2018.
44. Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [[CrossRef](#)]
45. Dannen, C. *Introducing Ethereum and Solidity*; Apress: Berkeley, CA, USA, 2017.
46. Hu, Y.C.; Lee, T.T.; Chatzopoulos, D.; Hui, P. Hierarchical Interactions Between Ethereum Smart Contracts Across Testnets. In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, CryBlock'18, Munich, Germany, 15 June 2018; ACM: New York, NY, USA, 2018; pp. 7–12.
47. USDA. Organic Integrity Database—Oregon Tilth Certified Organic Certifier Profile. Available online: <https://organic.ams.usda.gov/Integrity/CP/CertifierProfilePage.aspx?cid=62> (accessed on 2 February 2019).



© 2019 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).