01 December, 2022, Accepted: 07 February, 2022, Online: 22 February, 2023
DOI: https://dx.doi.org/10.55708/js0202003

Blockchain Tokens for Agri-Food Supply Chain

Ricardo Borges Dos Santos[*,1], **Rodrigo Palucci Pantoni** [2], **Nunzio Marco Torrisi**[1]

[1]UFABC, Center of Mathematics, Computing and Cognition, Federal University of ABC, Campus São Bernardo do Campo, São Paulo 09606-070, Brazil
[2] Department of Eletrical Engineering and Computer Science, Federal Institute of São Paulo, Campus Sertãozinho, São Paulo 14169-263, Brazil
[*]Corresponding author: Nunzio Torrisi, nunzio.torrisi@ufabc.edu.br

ABSTRACT: The aim of this research is to suggest and analyze a framework to give universal publicity to food properties certificates from any certification authorities. The focus is the certification of agro product instances, i.e. unique for every single harvest, using smart contracts and blockchain non fungible tokens minted by third-party authorities. The development and testing of a set of smart contracts used the newly established ERC-1155 Ethereum token standard to implement Non-Fungible Tokens (NFT)s. The ERC-1155 tokens allow for representing both the uniqueness, thus non-fungibility, between different harvests as well as the quantitative elements within a specific harvest, e.g. mass fractions of product from the same harvest, which can be interchanged, thus fungible. The framework was developed, deployed, and tested on the Ethereum test net blockchain and submitted to extensive testing. The blockchain data is accessible through general-purpose block scanners and can be read through an Android App used by regular consumers during a supermarket visit. The goal is to give consumers easy access to the Third-party Certificates (TPC) URLs available at the public Ethereum blockchain. The benefit for food safety of widespread TPC visibility through web applications can not be underestimated, since the use of blockchain tokens controlled by smart contracts injects trust in the traceability of the merchandise, reducing counterfeiting and green-washing. The broadcasting of the TPCs with the corresponding discipline of tokens transfer and smart contact restriction to possible abuses increases agro-food supply chain transparency. Trust and transparency foster sustainable buying habits by many consumers and transparency in the complete production and distribution links.

KEYWORDS Third Party Certification, Smart Contracts, Non-Fungible Tokens, Food Certification, Blockchain

1. Introduction

In 1990, the Organic Foods Production Act (OFPA) established standards for agricultural producers of commodities that claimed to use organic methods. The methods, practices and substances used in agricultural practice, including sowing; growing; and harvesting; as well as handling crops and processed agricultural products, restrict the wording on the product labels and marketing. Since OFPA, the US consumer has been continuously increasing demand for certified organic foods brands that claim to use organic production processes. Nevertheless, these organic farm certification methodologies have shown limitations and criticism: the authors of [1] conclude that the "current regulatory framework is not only inadequate to the task of regulating domestic organics, but also incapable of ensuring the integrity of imported organics. Thus, the USDA Organic seal misleads consumers.".

1.1. Justification

Several studies have recently claimed that the certification of products holds great beneficial potential, such that [2]: "Product certification is one of the most promising and developed instruments to reward the socially and environmentally friendly practices of market producers".

Third-party certification (TPC) differs from first and second-party certification mainly because the third-party authority that issues the certificate has no interest in the transaction. A TPC involves an "independent Organisation with expertise to provide an assessment and verification of the company's compliance with standards or legal requirements" [3].

TPC can be very useful to ascertain product physical, chemical, or organoleptic properties and is allowing bolder certification of social, environmental, and sustainability properties. According to the work in [4]: "TPC also offers opportunities to create alternative practices that are more socially and environmentally sustainable".

Although the farming procedures may be certified according to criteria such as quality, sustainability, or social fairness, there is no form of ensuring that certification of the typical farming methods, such as USDA Organic certification methodology, avoids specific harvests being stained by malpractices such as agrochemical exposure or used hidden child labor.

Each harvest of a specific crop is unique. The difference may lie in the seeds used for that particular season or in the total hours of sunshine in that specific location during the crop's growth.

One good example is the wine industry, where consumers know that the time and the different weather conditions between harvests of different years even from the same farm will influence the wine quality. Organoleptic tests of wine produced from grapes of different years and locations evidence these differences. The wine counterfeit problem can be summarized as avoiding that larger quantities of more valuable wine from grapes harvested on better years or regions reach retail than the volume actually produced. This fraud is academically known as the mass balance [5] or the double spending problem [6] and has a negative impact on the luxury goods business as it can hurt the reputation of premium brands. This fraud also hurts products that are geographically traceable to a specific region, i.e., reserved by local laws under the protected designation of origin (PDO) concept.

1.2. Related Work

The work in [7] provides a comprehensive overview on the application of blockchain technology to agri-food value chains. These are in line with the work in [8] which concludes that the use of blockchain technology can improve sustainability from social, environmental, and market perspectives. Recent literature [9] presents a blockchain-enabled supply chain architecture to ensure the availability of a tamper-proof audit trail for foods free of COVID-19 contamination Further [10] conducts an extensive literature review on the integration of blockchain into traceability systems. Discussion on a blockchain strategy to trace organic food products is presented in [11]–[13] . Attempts to use less costly distributed data structures such as the interplanetary File System (IPFS) for food traceability are discussed in [14]. These and other articles are convergent in stating that blockchain tools are possibly the most appropriate technologies to meet the various requirements the rapidly expanding food value chains such as traceability, auditability, fault tolerance, and flexibility [15]–[17]. Research on certification using blockchain [18]–citecreydt2019blockchain has also evolved with many interesting sustainability findings and efforts.

Nevertheless, no research has been found where harvests are recognized as being unique, thus their yield not interchangeable between different harvests. This approach, where the produce or yield of the different harvests are not interchangeable except within the same harvest, leads this research to use Non-Fungible Tokens (NFT) of the type ERC-1155.

1.3. Proposed Solution

It is proposed to use Ethereum-based tokens and smart contracts pointing to TPC certificates for keeping track of certificates for individual harvests of each farm. In this manner, we show that it is possible to track the exact origin and quantity of each harvest from farm to consumer, offering the benefits of TPC available to the last links of the chain. Practical economic incentives to the chain participants are described allowing for effective productive usage. The focus is on information availability, reliability, synchronization to the physical flow of goods, and, above all, ensuring good publicity of the certificate at the consumer level.

This research paper is structured as follows. Section 2 presents relevant concepts and literature of traceability, blockchain, smart contracts, and distributed ledger technology (DLT) and the Ethereum-based non-fungible token (NFT). Section 3 discusses the requirements and implementation of a token passing TPC framework using the ERC-1155 token smart contracts and analyses the results obtained. Section 5 presents the conclusions pinpointing the research's main contributions and limitations.

2. Blockchain Key concepts applied to Certification

A chain of transactions, organized into cryptographically linked blocks, could, for the first time, reach a consensus, even within a (limited) number of unreliable (traitor) nodes. For a more detailed description of the data structures involved see in [22, 23]. Albeit the eventually synchronized nature of the protocol and possible temporary partitions in the network, the linear block of data is re-established after a partition and regains consistency and availability.

Consistency of distributed data within a predetermined time frame is achieved, avoiding the double spending [6] of the digital asset.

The technology behind blockchain successfully implements consistency and access discipline for collaborative data in a diffuse globally distributed accessible trustless environment. The consistency achieved by the underlying data structures and control mechanisms with validation through the consensus of third party validators or miners shows that this technology is an important step towards supply chain transparency and traceability data [24]–[26].

A blockchain is a cryptographically auditable, append-only, tamper-resistant, distributed and replicated data structure, accessible to anyone employing a web browser.

Blockchain can store proof of structured data as well as methods or programs to process this data according to deterministic program steps known as smart contracts. Blockchains require no central trust mechanism, thus there exists no central point of failure. The main strengths of Blockchain Technology (BCT) are listed below.

- Tamper resistance, i.e., cryptographic hashes to previous block, in practice, make it impossible to change data that has been recorded;
- Pseudo-anonymity, i.e., data are available publicly but encoded through hashed keys that allow for trust on the existence and on the authorship;
- Distributed presence, i.e., the data structures are replicated maintaining several copies with no single point of failure and keeping integrity between data sets;
- Software-driven, i.e., the Blockchain mechanism does not require human privileged operators to maintain the transactions, thus the system is not prone to bribery;

- Allows for certification of the tamper-proof storage of off-chain data by means of side blockchain. These are hierarchically hash-certified sub-database that can store larger volumes of data, including multimedia, and provide evidence and tools for more detailed analysis.

Ethereum [27] expanded the concept of the blockchain to distributed ledger technology by including tokens and programs called smart contracts that are executed independently of human intervention. These are open-source, human-readable high-level programs that are stored on the blockchain and run inevitably, without any human intervention, strictly as implemented thus avoiding any risk of downtime, censorship, or fraud [28]. The Ethereum Virtual Machine implements "unstoppable" and "unavoidable" Turing-complete computer processes. Smart contracts use open-source code and are developed to establish standard behavior between blockchain stakeholders and other contracts. They allow for extensive development and precise control, ensuring transparency of each data manipulation and thus trust. Digital blockchain tokens are capable of representing object properties, assets, or rights that have strict transactional behavior and ownership. The execution of smart contracts is immune to any human interference and therefore allows for transparent systematic transactions. Tokens can be used to represent supply chains, intellectual properties, voting, or identity management systems, among other objects. The associated smart contracts assure discipline to the corresponding state transitions of token balances and thus generate trust to the parties without a trusted third party thus no single point of failure. This assures transparency and prevents possible "double-spending" frauds in the certification system.

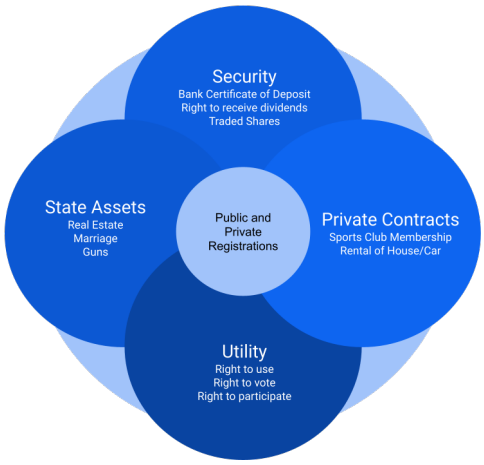

Figure 1: Families of assets and rights according to registration requirements.

2.1. *Digital Tokens*

Tokens are digital objects that represent specific rights or assets. They should be understood as assets that can be negotiated or used as guarantees. Note that the necessary and sufficient condition for full ownership of the balance of the token on a public address is the knowledge of its private key. Figure 1 shows a diagram for most common assets and rights, grouped into families along with their corresponding registration requirements.

The registration of the rights and property of assets, if required by law or regulation, will usually be centralized at a government-trusted centralized database. Because these data are maintained in centralized databases they are prone to corruption, fraud, censorship, downtime, or misuse. On the other hand, distributed registration schemes based on replicated databases, such as distributed ledgers, provide very high availability, are fraud-resistant, are fault-tolerant, and typically cannot be censored. Security and utility assets can reliably be represented, registered, and easily traded as cryptographic tokens. Automated processes through smart contracts allow high availability, low costs of the transaction, full traceability, non-repudiation, and pseudo-anonymity.

In order to be useful, tokens should not be copyable (i.e., should not be prone to double spending attacks) or suffer arbitrary changes. Thus, they need to follow strict discipline at each change of state to usefully represent real-world objects.

The development of digital objects to simulate real-world objects requires that the object's properties and behaviour are modeled through common data structures and coded procedures. Smart contracts manipulating tokens must respect some standard to allow for multiple users and contracts to share functionalities among different applications. Application independence and fungibility of digital objects could be achieved with a minimum set of functionalities. The ERC-20 token fungible objects standards are key to the success of many cryptocurrencies and many Ethereum decentralized applications. Because the ERC-20 token metadata structure holds all relevant property data within the blockchain, they can be freely transferred from one blockchain to another, allowing these to be exchanged for other ERC-20 assets.

It is important to note that like a real estate property record, which entitles the bearer to have full use and ownership of a real estate asset, the possession of a private key of a token on one blockchain entitles that person or smart contract to unrestricted use of that token for payment, exchange, deposit as warrant or collateral, lending or selling this assets at his discretion.

Further, it is important to recognize that objects can be categorized in fungible objects and non-fungible objects. Fungible objects are those that need not be distinguished from one another. The important question here is "How many of these objects?". Non-fungible objects, on the other hand, are those that are distinguishable from similar objects. The decisive question here is "Which of these similar, although unique, objects?"

The distinctive property between fungible and non-fungible tokens is that the former are fully exchangeable and thus can be added, e.g., coins of the same face type and value can be added or subtracted at will. The latter, not being exchangeable, can only be transacted as unique identifiable objects.

A non-fungible token (NFT) is a unique blockchain-based digital entity which can represent a non-fungible object. If this token follows a protocol such as the ERC-1155 or ERC-721, it can be traded as an asset between various stakeholders in possibly multiple applications.

The methods defined in the ERC-1155 standard assure consistent behavior, transparency, no double spending, and a verifiable auditable trail to families of similar, yet unique, objects. An ERC-1155 compliant NFT has one identifier that points to a specific URL, in which typically all properties and details are described. Additionally, an overview of these main differences is outlined in Table 1 and a numerical characteristic of the ERC-1155 object is also available (https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1155.md accessed on 26 November 2022).

Table 1: Comparison between ERC-721 and ERC-1155 tokens

	ERC-721	ERC-1155
Fungible	N	Y(within same family)
Non Fungible	Y	Y
Smart Contract	One instance	Multiple instances

2.2. Harvest TPC Algorithm

For decades, important crops have been traded as commodities. Commodities are intrinsically fungible. Once the product is classified in a certain grade, according to purity, size, or maximum cross-contamination levels, then, the lot is handled as a commodity. Global trading standards and procedures require that a certain measure of a commodity, say, a bushel of a certain grade of wheat, is fully fungible with the same measure of this same commodity, i.e. another bushel of the same wheat grade. However, a specific harvest should be regarded as a unique object. No other harvest possesses the exact same physical, chemical or organoleptic properties, therefore harvests should be handled as non-fungible physical objects. To track this object appropriately, it is necessary to record all relevant data which will individualize and keep the history of that specific harvest product.

Each harvest of a specific crop is unique. The difference may lie in the seeds used during that particular season or in the total number of hours of sunshine in that specific location during the crop's growth.

In several agricultural sectors, especially in the wine trade, expert consumers recognize the crop timing and the different characteristics between harvests of different years even from the same farm. The analysis of the organoleptic properties of the wine produced recognizes differences in the year and location of the harvest of grapes. In the wine sector, the wine counterfeit problem can be summarized as avoiding that larger quantities of more valuable wine from grapes harvested on better years or regions reach retail than the volume actually produced. This fraud is also known as the mass balance problem [5] or double spending [6] and is very deleterious to the business as it can stain the reputation of premium producers. Products that are geographically traceable to a specific region, i.e., reserved by local laws under the protected designation of origin (PDO) concept are also frequently affected by this type of fraud. A harvest TPC mechanism with tamper-resistant certificates which are easily available to any stakeholder via internet devices is very helpful to avoid double spending and can significantly boost trust along the supply chain stakeholders.

Thus, we researched the following main research questions (MQ1) and subsidiary research questions (SQ2, SQ3):

MQ1: "Is it possible to establish a harvest TPC mechanism with tamper resistant certificates easily available to anyone, even previously unknown food supply chain stakeholder via public blockchain access?"

SQ2: "If a TPC mechanism is possible, who will carry the data input and maintenance costs? In other words, how will each stakeholder be incentivized to use this mechanism?"

SQ3: "If a TPC mechanism is possible, what will a typical time of response for a certification query be, in other words what quality of service can be expected by the end consumer?"

To answer the Research Questions MQ1 and the subsequent research questions SQ2 and SQ3 a systematic method was used which involves designing all smart contracts needed, deploying and subjecting them to testing. The test evaluated compliance to functional and non functional design requirements. The procedure is depicted in the Algorithm 1 which shows a step-by-step description of the methodology for harvest TPC validation using a set of 7 smart contracts as a Proof-Of-Concept (PoC).

Algorithm 1: Methodology Systematic

```
Result: Write here the result
User Requirements;
while Register Request do
    SmartContract(ProofOfConcept);
    if TPC Authority exist then
        Token Transfer;
        Consumer Tracking Access;
    else
        Evaluate(ProofOfConcept);
    end
end
```

In summary, the algorithm develops a systematic methodology by means of the following steps:

- 1—Elicit and define user requirements (both Functional and Non-Functional).
- 2—Harvest Traceability - Define and Identify Traceable Units - Discipline data collection, i.e., when and what needs to be collected.
- 3—Design and implement proof-of-concept (PoC)—Deploy smart contracts.
- 4a—Analyze if third-party certification authority is capable of issuing tokens easily and transferring them along the Supply Chain Participants.
- 4b—Analyze if a token transfer allows the URL information to be made accessible to the token buyer along the Supply Chain Participants.
- 5—Analyze if consumers can access URL for TPC with internet applications easily, reliably, and fast (MQ1).

- 6—Evaluate PROOF OF CONCEPT and respective results and improve implementation.

Besides the blockchain immutability permit to trace of all the test runs and deployments of the smart contracts. This allows the research methodology and procedures to be easily reproducible and traceable (Examples of blockchain scanners are https://www.etherchain.org/, https: //www.EthPlorer.io or https://www.Etherscan.io accessed on 29 August 2022). In other words, both the smart contract source code as well as all the test runs of all tests performed to the PoC can be followed in detail on any browser.

2.3. Requirement Analysis

The desired functionalities of the system, i.e., the functional requirements are listed below.

- to allow for farmers to request any third person authority to inspect and certify properties that a specific harvest may have;
- to allow the inspection authority to issue a certificate on any website including quantitative data about the desired property of the yield;
- to allow the authority to create ("mint") tokens, i.e., digital objects representing the harvest and carrying the URL linked to the certificate, representing information about the mass of product inspected (yield);
- to allow these tokens to be "passed on" along the chain of buyers of the product (yield);
- to allow the buyer that applies the package, wrapper, or label to the food product to write the URL to an easily and freely accessible reliable database and
- to destroy ("burn") , after a predetermined time, these tokens once the food product is consumed, to avoid garbage accumulation or misuse.

As for the nonfunctional requirements, it is important to ascertain that the system satisfies the following:

(a) Universal access: allowing any supply chain participant, even previously unknown, to use the tool without previous registration;

(b) Tamper free auditabilty: enforcing tamper-free, auditable transactions between any parties;

(c) Robustness to faults: allowing the writing to a common persistent information layer in a robust manner;

(d) No double spending fraud: avoiding that token balances are used more than once;

(e) Universal read access: allowing any potential consumer to freely read the certificate by means of an internet device

(f) Interoperability: allowing usage with different systems and devices and

(g) Cost effectiveness: allowing information to be recorded in an inexpensive manner;

(h) Usability: allowing for comfortable user experience.

(i) Quality of Service: guaranteeing that response to a consumer query returns to the requesting device within a short time period;

(j) Scalability: allowing for a much larger number of transactions running within the acceptable quality of service i.e performance.

2.4. Persistence Layer Design: Do we need a Blockchain?

If harvests are to be certified for the benefit of the entire chain of potential stakeholders in the food industry, which type of data structure would be required to keep this information useful and trustworthy? Is it necessary to use a blockchain to record and make all relevant information consistently available to all stakeholders?

Figure 2, derived from [29] summarizes a structured approach to optimize the data structure architecture to be used for a specific application. In this case, the particular requirements for the TPC of Harvest in the Food Supply Chain recommend the use of a public permissionless blockchain as the best architecture. The sequence of questions we would ask is:

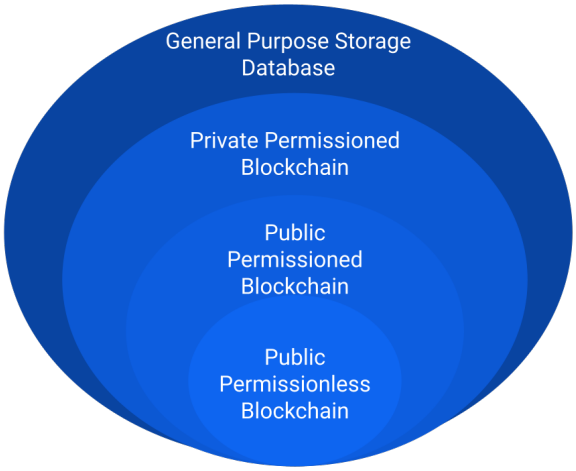

Figure 2: Scale of Requirements to define the type of data persistence layer (database or blockchain)

- Is it necessary to store current State (Current Custodian on Supply Chain)? YES;
- Is a Trusted Third Party available online? NO;
- Is WRITE access needed outside your organization? YES; (because of the possibly many unknown chain participants).
- Are all Writers known? NO.

Thus, the recommended architecture is Public Permissionless Blockchain. Because it is desired that the system maintains allows for new participants to join the supply chain such as new farmers, known farmers with new crops, new mills, new re-sellers, new comminglers or new retailers,

the choice of a permissioned blockchain such as Corda or Hyperledger was discarded[30, 29].

Because Ethereum tokens meet the non-functional requirements (a–i) listed above, the public Ethereum environment with the non-fungible token ERC-1155 standard protocol was chosen. Ethereum also meets all of the non-functional requirements today including (j): scalability.

3. Smart Contract Implementation

The smart contract code used for ingredient certification in [31] was modified to implement the non-fungible token (NFT) discipline that better represents each instance of a crop with the use of the ERC-1155 (https://github.com/enjin/erc-1155 accessed on 29 August 2022) objects and methods.

The fully documented source code for all the smart contracts in the Solidity programming language was published in the Ethereum main net where all variables and algorithms are fully commented on and documented. The code was developed, tested, deployed, and made available at https://rinkeby.etherscan.io/address/0x841c5c79d9ae35db8fb4f216a478cd184fdae634#code (accessed on 4 august 2021). The source code shown in the link is the full smart contract code and is divided as follows: The ERC-1155 standard code and the standard libraries used are shown up to line 772. The specific smart contract code responsible for the application is shown as of line 772 and comprises the following methods:

- *farmerRequestCertificate*- This routine allows for the sale of ingredients along with the respective IGR token transfer
- *certAuthIssuesCerticate*- This routine is used to allow for certification authorities to confirm that ingredients are trustworthy as well as quantity, URL where published, product, details of IGR value property, location, date of harvest).
- *sellsIngrWithoutDepletion* - This routine allows for the simple sale of ingredients along with the respective IGR token transfer (with URL).
- *sellsIntermediateGoodWithDepletion* - This routine allows for the sale of intermediate products made from certified ingredients along with the respective IGR token transfer (with URL) i.e.: allows only the pro-rata quantity of semi-processed InGRedient tokens to be transferred.
- *genAddressFromGTIN13date* - This is an auxiliary function to generate an ethereum address for the specific food item visible numbers GTIN-13 + date of validity in format YYMMDD. This is used by the method comminglerSellsProductSKUWithProRataIngred to allow anyone such as e.g. by a consumer with an App or block-scanner to query the exact blockchain address where the certificate URL is stored(Figure 4).
- *transferAndWriteUrl* - This is also an auxiliary routine to transfer the balance from the token owner's account to the 'to' account. Note that the owner's account must have sufficient balance to transfer, that zero value transfers are allowed.
- *comminglerSellsProductSKUWithProRataIngred* - This code allows for the sale of the final-consumer product with resp SKU and Lot identification with corresponding IGR transfer with URL. In other words, it warrants that only the pro-rata quantity of semi-processed InGRedient tokens be transferred to the consumer-level package(SKU)

The smart contract code described can be viewed also as a class UML diagram. Generation of UML class diagrams from published Solidity programming language source code on the Ethereum blockchain can be obtained by an automated functionality of the Etherscan blockchain scanner, as shown in (https://rinkeby.etherscan.io/viewsvg?t=1&a=0x841c5c79d9ae35db8fb4f216a478cd184fdae634.

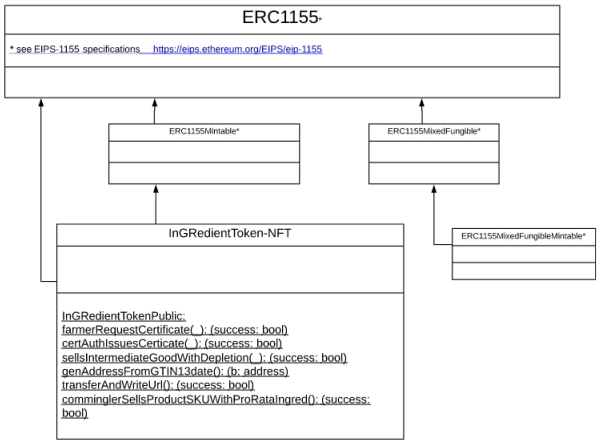

Figure 3: IGR Token class as a dependent class of the ERC 1155 class. (simplified by author from auto-generated UML class diagram from Etherscan).

4. Results and Discussion

A set of public blockchain smart contracts govern the token synchronization framework to positively identify each harvest along the food supply chain to the end consumer.

At each transactional change to the product such as change of custody, mixing, usage, or depletion of the product, tokens are exchanged.

Using a modification of the IGR token set of smart contracts rewritten for ERC1155, in Figure 3, the farmer responsible for the harvest can freely choose the properties to be certified between:

- functional - e.g. minimum size of fruit or grade.
- organoleptic - e.g. color or aroma.
- social - e.g. free of child labor cultures.
- environmental - e.g. "grown in certified no forest devastation areas"or "organic—no xyz herbicide", or non Genetic Modified seeds only.

as well as the appropriate authority that will audit and issue the corresponding certificate for each harvest.

The authority is then invited to audit the farm at harvest time. After the appropriate auditing procedures, including inspection of the farm and qualitative and quantitative evaluation of crop yield, the authority formalizes the audit results by publishing the certificate as a web page at the authority's domain web server.

The link to this certificate, in the form of the URL is part of the minting process. Further, this smart contract will issue the exact number of tokens to match the numerical mass yield of that specific harvest in grams.

Thus the ERC-1155 unified resource identifiers (URL) descriptor will point to the web page containing the full technical details of the certified "consumer-valued properties", including the original mass of goods in grams. The number of IGR tokens issued will represent this specific mass of ingredients.

By using the delegated transfer "setApprovalForAll()" and "safeBatchTransferFrom()" primitive in the smart contracts, it is not possible for the farmer to issue or make first-person claims on the certificate. Only the Authority has this capability, thus enforcing strict true third-person certification (TPC).

Comparing the current approach to the previously published certification using the ERC-20 IGR Ethereum token, the main improvement was to avoid tokens obtained from different harvests, thus with different characteristics, being mixed. The ERC-1155 discipline allows for the farmer to sell part of the harvested product whilst avoiding possible attempts to mix tokens from distinct harvests.

Further, as in blockchain distributed ledgers, "double spending" frauds are not possible.

The necessary information in order to evidence to a final consumer that a specific harvest or food ingredient raw material was effectively inspected and certified by a third party to hold some "consumer value property" is handed over from one chain participant to the next, all the way to the recipe final processor.

The farmer, can freely define any property that may be useful or cherished by his consumers and the certifying authority by using the smart contract *farmerRequestCertificate()*. After an inspection of the farm, the certification authority will confirm the quality, quantity, and date of the lot harvested. He will then include all relevant information in the certificate web page at the authorityś web domain. *certAuthIssuesCert()* The smart contract mints for this specific lot of crop an equivalent quantity of IGR tokens such that one IGR token corresponds to one gram of that certified ingredient. The authority issues IGR tokens through the smart contract including nature, quantity, location, and time of the harvest. The token will hold the URL to the web page of the full TPC. Note that only the certification authority has permission to mint or not mint the tokens or determine the correct quantities. This assures a truly independent third-party certification and avoids potential conflicts of interest.

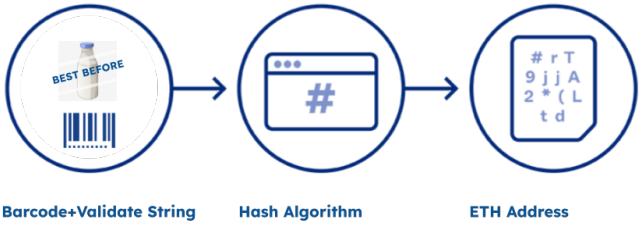

Figure 4: ETH Address generation from *genAddressFromGTIN13date*

The final processor, sometimes also known as commingler or packer, uses information printed on the product retail label to generate a public key which is linked to the certificate URL. The barcode (GTIN-13 SKU identifier) appended to the validity "best before" date on the wrapper are hashed to provide a unique public key in the Ethereum blockchain. Thus, the hash of the "GTIN-13 + Date" string is the public key on the Ethereum blockchain. Querying the blockchain at this address returns the URL link to the certificate.

This new ERC-1155 smart contract code retains the original functionalities while extending the framework to allow for non-fungible objects such as harvests of food products to be certified as unique objects. It has a major new focus on the conception, validation, and usability of smart contracts for TPC of non-fungible objects.

4.1. *Answers to Research Questions*

The research questions **MQ1** and subsidiary research question **SQ2** and **MQ3** can be answered as follows:

MQ1: Yes, the IGR token smart contracts after being modified to ERC-1155 are capable of truly evidencing harvest TPC with tamper-free certificates and are available to anyone, including new entrants to the food supply chain through simple internet devices, as shown by the PoC running on a test net as described.

SQ2: Yes, price incentive mechanisms are established for each stakeholder. The premium to the price that the final consumer is willing to pay for access to the TPC certification of products will be shared with the supply chain participants. The sum of the incentives along the links of the supply chain is approximately as large as the premium the consumer actually pays.

SQ3: The typical time for the response for an end consumer to a certificate query using the HTTP protocol is linear because it uses only one direct hashed access to the blockchain (linear data structure) plus one direct URL web access to the certificate, both of which are accessible in linear time. This is due to the fact that, at each change of custody, the URL to the certificate is "handed over" to the next in the chain all the way to the commingler or packer. The public key information (GTIN-13 + lot date) to the certificate URL saved on the blockchain can be scanned directly from the product label. This can be achieved conveniently using an Android App https://play.google.com/store/apps/details?id=com.igrtoken&hl=en&gl=US&pli=1

In summary, the modified IGR-token smart contracts suite using the ERC-1155 tokens allows for the synchronization of the transfer of custody of the crop with the corresponding IGR token representing each gram of the yield instantiated for each different harvest. The modifications to the IGR-token code to use the ERC-1155 have kept all original functionalities adding the necessary non-fungible discipline. The main enforcement is that yields from different harvests now may not be added.

The framework can not detect if a physical counterfeit of packaging, within a short period, i.e., re-utilization of original packaging material with counterfeit content, whilst the spent tokens are still "live".

5. Conclusions and Future Work

Farmers are systematically urged towards more sustainable farming methodologies whilst becoming more competitive. Some producers use the information on labels to induce customers to believe that their ingredients are harvested in environmentally and socially friendly manners without proper evidence. Third-party certification along with better availability of this information to the general public and supply chain actors can help fight this green-washing and promote consumer trust. Reliable publicity of the certificates with fast and easy access is paramount. A possible practical solution is the use of distributed ledger technology using tokens carrying the URL pointing to the certificate at the authority's website. This information is transferred at each change of custody from harvest along the chain.

This research shows that a TPC, via the certificate URL at the authority's website, can easily and publicly be made available through internet Apps. To allow for credibility among the target consumers, the certification authority can be freely chosen by the farmer. The authority is free to decide and has full control on whether or not to certify or deny certification. The architecture has a practical appeal because it allows economic incentives to be shared by stakeholders along the agro-supply chain links.

The major contribution of this research is to show a method for public access to URLs with TPC of harvests as unique objects, as opposed to a more generic certification of a farm.

Conflict of Interest The authors declare no conflict of interest.

References

[1] C. Liu, "Is usda organic a seal of deceit: The pitfalls of usda certified organics produced in the united states, china and beyond", *Stan. J. Int'l L.*, vol. 47, p. 333, 2011.

[2] F. DeClerk, J. F. Le Coq, B. Rapidel, J. Beer, *Ecosystem services from agriculture and agroforestry: measurement and payment*, Routledge, 2012.

[3] B. Tanner, "Independent assessment by third-party certification bodies", *Food control*, vol. 11, no. 5, pp. 415–417, 2000.

[4] M. Hatanaka, L. Busch, "Third-party certification in the global agrifood system: an objective or socially mediated governance mechanism?", *Sociologia ruralis*, vol. 48, no. 1, pp. 73–91, 2008.

[5] T. Hirbli, "Palm oil traceability: Blockchain meets supply chain", Ph.D. thesis, Massachusetts Institute of Technology, 2018.

[6] U. W. Chohan, "The double spending problem and cryptocurrencies", *Available at SSRN 3090174*, 2021.

[7] G. Zhao, S. Liu, C. Lopez, H. Lu, S. Elgueta, H. Chen, B. M. Boshkoska, "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions", *Computers in industry*, vol. 109, pp. 83–99, 2019.

[8] J. Kasten, "Blockchain on the farm: A systematic literature review", *Journal of Strategic Innovation and Sustainability*, vol. 15, no. 2, pp. 129–153, 2020.

[9] A. Iftekhar, X. Cui, "Blockchain-based traceability system that ensures food safety measures to protect consumer safety and covid-19 free supply chains", *Foods*, vol. 10, no. 6, p. 1289, 2021.

[10] K. Demestichas, N. Peppes, T. Alexakis, E. Adamopoulou, "Blockchain in agriculture traceability systems: A review", *Applied Sciences*, vol. 10, no. 12, p. 4113, 2020.

[11] X. Lin, S.-C. Chang, T.-H. Chou, S.-C. Chen, A. Ruangkanjanases, "Consumers' intention to adopt blockchain food traceability technology towards organic food products", *International Journal of Environmental Research and Public Health*, vol. 18, no. 3, p. 912, 2021.

[12] K. Salah, N. Nizamuddin, R. Jayaraman, M. Omar, "Blockchain-based soybean traceability in agricultural supply chain", *Ieee Access*, vol. 7, pp. 73295–73305, 2019.

[13] G. d. S. R. Rocha, L. de Oliveira, E. Talamini, "Blockchain applications in agribusiness: a systematic review", *Future Internet*, vol. 13, no. 4, p. 95, 2021.

[14] D. Prashar, N. Jha, S. Jha, Y. Lee, G. P. Joshi, "Blockchain-based traceability and visibility for agricultural products: A decentralized way of ensuring food safety in india", *Sustainability*, vol. 12, no. 8, p. 3497, 2020.

[15] A. Upadhyay, S. Mukhuty, V. Kumar, Y. Kazancoglu, "Blockchain technology and the circular economy: Implications for sustainability and social responsibility", *Journal of Cleaner Production*, vol. 293, p. 126130, 2021.

[16] N. Kshetri, "1 blockchain's roles in meeting key supply chain management objectives", *International Journal of information management*, vol. 39, pp. 80–89, 2018.

[17] J. F. Galvez, J. C. Mejuto, J. Simal-Gandara, "Future challenges on the use of blockchain for food traceability analysis", *TrAC Trends in Analytical Chemistry*, vol. 107, pp. 222–232, 2018.

[18] F. Zhao, X. Guo, W. K. Chan, "Individual green certificates on blockchain: A simulation approach", *Sustainability*, vol. 12, no. 9, p. 3942, 2020.

[19] F. Casino, V. Kanakaris, T. K. Dasaklis, S. Moschuris, N. P. Rachaniotis, "Modeling food supply chain traceability based on blockchain technology", *Ifac-Papersonline*, vol. 52, no. 13, pp. 2728–2733, 2019.

[20] A. Kamilaris, A. Fonts, F. X. Prenafeta-Boldv, "The rise of blockchain technology in agriculture and food supply chains", *Trends in Food Science & Technology*, vol. 91, pp. 640–652, 2019.

[21] M. Creydt, M. Fischer, "Blockchain and more-algorithm driven food traceability", *Food Control*, vol. 105, pp. 45–51, 2019.

[22] J. Zhang, S. Zhong, T. Wang, H.-C. Chao, J. Wang, "Blockchain-based systems and applications: a survey", *Journal of Internet Technology*, vol. 21, no. 1, pp. 1–14, 2020.

[23] M. Choi, S. R. Kiran, S.-C. Oh, O.-Y. Kwon, "Blockchain-based badge award with existence proof", *Applied Sciences*, vol. 9, no. 12, p. 2473, 2019.

[24] A. Rejeb, J. G. Keogh, S. Zailani, H. Treiblmaier, K. Rejeb, "Blockchain technology in the food industry: A review of potentials, challenges and future research directions", *Logistics*, vol. 4, no. 4, p. 27, 2020.

[25] S. Khan, A. Haleem, M. I. Khan, M. H. Abidi, A. Al-Ahmari, "Implementing traceability systems in specific supply chain management (scm) through critical success factors (csfs)", *Sustainability*, vol. 10, no. 1, p. 204, 2018.

[26] R. Cole, M. Stevenson, J. Aitken, "Blockchain technology: implications for operations and supply chain management", *Supply Chain Management: An International Journal*, 2019.

[27] E. Wood, "A secure decentralised generalised transaction ledger, ethereum proj", *Yellow Pap*, , no. 151, p. 1.

[28] W. Ethereum, "Ethereum whitepaper", *Ethereum. URL: https://ethereum. org [accessed 2023-01-01]*, 2014.

[29] L. Wu, "Blockchain smart contracts in megacity logistics", 2018.

[30] K. Wüst, A. Gervais, "Do you need a blockchain?", "2018 Crypto Valley Conference on Blockchain Technology (CVCBT)", pp. 45–54, IEEE, 2018.

[31] R. B. dos Santos, N. M. Torrisi, E. R. K. Yamada, R. P. Pantoni, "Igr token-raw material and ingredient certification of recipe based foods using smart contracts", "Informatics", vol. 6, p. 11, MDPI, 2019.

Ricardo Borges dos Santos has completed his Bachelor in Mechanical Engineering degree from PUC-RJ University in 1984 with honors. He has obtained a Computer Engineer Degree from UNIVESP, Sao Paulo in 2020 as well as a MS degree in Mechanical Engineering at Penn State University in 1989. He has earned his PhD degree in Computer Science from the Center of Mathematics, Computation e Cognition of the Universidade Federal do ABC in 2019.

His research activities are mainly related to Distributed Systems, Cryptography, Blockchain and Energy. He has over 20 articles on Food Traceability, Distributed Systems, Energy Efficiency and Supply Chain Management.

Rodrigo Palucci Pantoni He received the Computer Science degree in 2000 and subsequently received the M.S. in 2006 and PhD in 2012 at the University of São Paulo (USP).

He now teaches "Industrial Informatics" at the Department of Electrical Engineering and Computer Science of Federal Institute of São Paulo. His research activities are mainly in the area of Industrial Informatics with focus on development activities including Internet of Things and Industry 4.0.

Nunzio Marco Torrisi He received the Master degree and the PhD in Computer Engineering from the University of Catania, Italy, in 2002 and 2006, respectively.

He registered a Brazilian patent, published his work in international journals and magazine and since 2009, he has been an associate professor at the Federal University of ABC in São Paulo (UFABC).