Journal of Pharmaceutical Innovation
https://doi.org/10.1007/s12247-023-09748-z

ORIGINAL ARTICLE

Blockchain for Data Originality in Pharma Manufacturing

Marta Durá[1] · Fátima Leal[2] · Ángel Sánchez-García[1] · Carlos Sáez[1,3] · Juan M. García-Gómez[1] · Adriana E. Chis[3] · Horacio González-Vélez[3]

Accepted: 4 June 2023

Abstract

Purpose This paper analyses the feasibility of tracking data originality for pharmaceutical manufacturing in a tamper-proof manner using a geographically distributed system. The main research question is whether it is possible to ensure the traceability of drug manufacturing through the use of smart contracts and a private blockchain network.

Methods This work employs a private Ethereum network with a proof-of-authority consensus algorithm to allow participating nodes to commit the medicament manufacturing originality as transactions in blocks. We use smart contracts to assess the "Original" principle of the ALCOA+ data integrity principles for full sensor-enabled production lines within pharmaceutical manufacturing plants. We have evaluated our data originality assessment approach employing a temporal series of 1300 reports generated based on real datasets from pharma production lines. Out of these reports, 300 reports have been randomly tampered with to make them "unoriginal" (i.e., falsified).

Results Evaluation consistently shows that the proposed approach systematically detects all the manufacturing records whether original or not, together with any source of falsification. By randomly injecting four common data falsification types, their approach effectively detects tampering and ensures the authenticity of the data originality acquired by sensors within manufacturing lines.

Conclusion The approach of using a private blockchain network with a proof-of-authority consensus algorithm and smart contracts is a feasible method to track data originality for pharmaceutical manufacturing in a tamper-proof manner. In addition, this approach effectively detects tampering and ensures the authenticity of the data originality acquired by sensors within manufacturing lines.

Keywords Blockchain · Production line · ALCOA · Ethereum · Data integrity · Data quality

✉ Marta Durá
marduher@upv.es

Fátima Leal
fatimal@upt.pt

Ángel Sánchez-García
ansan12a@upv.es

Carlos Sáez
carsaesi@upv.es

Juan M. García-Gómez
juanmig@upv.es

Adriana E. Chis
Adriana.Chis@ncirl.ie

Horacio González-Vélez
Horacio.Gonzalez-Velez@ncirl.ie

[1] Biomedical Data Science Lab, Instituto Universitario de Tecnologías de Información y Comunicaciones, Universitat Politécnica de Valéncia, Camino de Vera, Valencia 46022, Spain

[2] REMIT, Universidade Portucalense, R. Dr. António Bernardino de: meida, Porto 541, 4200-072, Portugal

[3] Cloud Competency Centre, School of Computing, National College of Ireland, Mayor Street, IFSC, Dublin, D01 K6W2, Ireland

Published online: 07 July 2023

Introduction

The EU Falsified Medicines Directive [1] "introduces harmonised European measures to fight medicine falsifications and ensure that medicines are safe and that the trade in medicines is rigorously controlled". Such obligatory safety features, legal framework, and record-keeping requirements have arguably imposed stricter controls for the manufacturing of medicines.[1] While the pharmaceutical[2] industry has consistently improved its manufacturing processes in compliance with good manufacturing practices, and it is well documented that falsification of medicines continues [2] and has led to disastrous consequences worldwide [3]. Consequently, different organisations including the World Health Organization have long called for distinct remediation strategies [4].

There have been a number of technology-centric approaches to hinder the proliferation of fake medicines [5] including mobile apps for drug authentication and tracking, packaging enhancements such as digital tagging, radio-frequency identification, and web portals to verify pharmacies. However, such approaches have mostly concentrated on the distribution and packaging of medicines rather than on the quality and reliability of their production. That is to say, scant research has been conducted on organically ensuring the traceability and originality of medicines from the perspective of their manufacturing data.

From an industrial perspective, the current gold standard for data management is comprised in the FDA's "Data Integrity and Compliance with current Good Manufacturing Practices" [6], where the term "ALCOA+" is defined. As a set of principles that should be followed throughout the data life cycle for achieving data integrity, ALCOA+ states that data should be **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal, and **A**ccurate, along with complete, consistent, enduring, and available, the "(+)" side.

This paper advocates the use of blockchain networks to better ascribe and ensure the manufacturing originality of drugs as comprised in the O of ALCOA+, which establishes the *Original principle*, as the assurance of data origin as the primary source. While blockchains are well-established in the cryptocurrency domain, their systematic application in the pharma industry remains an open problem, particularly from a regulatory perspective.

The main contributions of this paper are: ı) demonstrate the feasibility of using blockchain technologies to univocally assess originality—as defined by ALCOA+*—via raw data from pharma manufacturing batch records; and, ıı) systematically ensure traceability and end-to-end verification in a scalable manner within the drug manufacturing process.*

The proposed method includes a private Ethereum network with proof-of-authority (PoA) consensus and *smart contracts*, privacy-preserving verifiable programme stored on a blockchain that automatically enforce its components without the assistance of a trusted authority. Specifically, our smart contracts programmatically allocate the hash and the identifier of pharma records in a blockchain. They also enforce the originality principle by comparing the data committed to our blockchain network, e.g., a report that has the same identifier holding a different hash ought to be detected as unoriginal. That is to say, since the logged data and the business logic are tamper-proof and blockchain-embedded, they detect the originality infringement and identify the corresponding type of falsification. Running our ALCOA+ front-end in Valencia and the Ethereum network in Dublin, we have evaluated our approach employing a temporal data series of 1300 reports generated based on real pharma production lines. Out of these reports, 300 were *randomly* tampered with, i.e., made unoriginal (i.e., falsified) with four common data falsification types being randomly applied to each falsified report.

The results of the ALCOA+ evaluation show that our approach accurately detects all the manufacturing records whether original or not and, for those unoriginal, it also explains their source of falsification. It is also noted that this empirical evaluation has also studied the latency and performance implications of the geographically distributed system, as the assessment tool front-end has been executed in Valencia and the blockchain backend in Dublin.

This paper is organised as follows. In "Related Work" section, we describe the relevant related work for data integrity applications within the pharma industry. Then, in "Originality Assessment Approach" section, we introduce the proposed approach for assessing the originality of drug manufacturing records through blockchain technologies. In "Evaluation and Results" section, we present our evaluation methodology and the empirical evaluation results of our originality assessment approach and corresponding tool. Finally, in "Conclusions" section, we provide the concluding remarks of this work.

Related Work

The World Economic Forum (WEF) has recently coined the term *TradeTech* to denote the technologies and innovations that enable trade to be more efficient, inclusive and

[1] We have used the terms "medicines" and "drugs" interchangeably throughout this paper to refer to fully approved potions for the treatment of a clinical condition.

[2] Following industry conventions, the Instituto Universitario de Tecnologías de Información y Comunicacionese terms "pharma" and "pharmaceutical" are also used interchangeably.

equitable, and ultimately harness the innovations of the Industry 4.0 technologies to support the public good [7]. More specifically, the WEF suggests the continual improvement and optimisation of manufacturing processes by relying on digital sensing, machine learning, and blockchain, among other technologies. While sensors have been widely employed in manufacturing for well over 2 decades [8], their enhanced computing capabilities and connectivity and their full integration with other technologies continue to be an active area of research and innovation.

The use of blockchain for data integrity assurance is still in its infancy; however, its potential is widely accepted to augment the capabilities of dynamic distributed network environments. Blockchain technologies can securely enable storage, sharing, and data analytics in data-driven computer networks while preserving user privacy, trustworthy network control, and decentralised resource management [9]. Such a network-oriented approach can be useful for fraud prevention and for real-time analytics with significant impact on data integrity. Relevant examples of blockchain for data security in distributed networks have also been provided in Kumar et al. [10], where blockchain technology is used for robustly detecting copyright infringement thanks to its independence from any third party arbitration and in Ch et al. [11] where privacy is ensured via blockchain-enabled virtual circuits for device data.

It is widely accepted that smart connected sensors and connected manufacturing components can be linked to a central computing system, but security and privacy constraints have limited data exchange particularly in pharmaceutical companies and, consequently, the adoption of so-called Pharma 4.0 techniques [12]. That is to say, Pharma 4.0 techniques ought to integrate smart sensors with advanced data science, as has been proposed for smart factories [13].

Given the diverse dynamic nature of the data generated, pharma companies have mostly adopted trusted technological approaches in compliance with regulatory frameworks and safety and sustainability guidelines [14]. Nonetheless, the pharmaceutical industry aims to fully digitise manufacturing processes by using data-driven technologies. It aims to solve well-defined obstacles in their industrial data-processing life cycle, such as the analysis and tracing of high-dimensional data sets or the assessment of multivariable changes in the supply chain [15]. This is a new challenge for regulatory frameworks, due to the need to ensure data integrity in a traceable and transparent fashion.

Moreover, disclosure risk assessment techniques in pharma manufacturing typically rely on background knowledge, the behaviour of intruders, and the specific value of the data. Often, only heuristic arguments are used without quantitative assessment. However, the pharmaceutical industry has arguably become a large distributed data-intensive environment, where large amounts of data are generated and accessed regularly by different internal and external stakeholders including international and domestic regulatory bodies. Such an environment requires confidentiality, privacy, and security such that data authenticity and end-to-end tracking are consistently ensured throughout their different industrial processes. Consequently, the Smart Pharmaceutical Manufacturing (SPuMoNI) project is developing a novel approach to establish and assure constant proof of the authenticity of pharmaceutical manufacturing data to ultimately underpin data quality, compliance, and auditability [16].

Regulatory bodies are continually increasing their auditing requirements from traditional manual exercises to automated ALCOA+ trails, where detailed transactions capture complete traces of sensor and production lines to ultimately track the fabrication of pharmaceutical drugs at scale. This is not a new problem to solve. Rattan [17] discusses the large amount of regulations that, since 1963, have been put forward by several regulatory bodies. To assess data integrity, their proposed methods have initially been simple checklists, self-audits, and self-inspection techniques—mostly focused on self-prevention for random audit trails—instead of continuous monitoring and evaluation of manufacturing data.

More recently, regulatory bodies have identified the need to ensure data integrity in "The GAMP Guide: Records and Data Integrity" [18]. It comprises guidelines for the implementation and management of good practices (GxP)-regulated records and data, where the GxP are the accepted gold standard and framework for all automated manufacturing industries. It also provides a framework for regulatory focus, data governance, data life cycle, culture and human factors, and the application of quality risk management to data integrity. Pharma manufacturing industries are mostly automated, which implies full compliance with GxP and a large amount of data continuously generated.

> *Efficiently addressing* ALCOA+ *requirements arguably calls for novel technological solutions to dynamically analyse all generated data to assist qualified personnel and auditors to trace the originality of medicines.*

Emerging domains, such as Pharma 4.0, are facing privacy risks and security vulnerabilities. Since manufacturing lines involve more connected devices in the information network, it becomes a big data reality with a decentralised topology. Therefore, such heterogeneity requires quality assurance as well as security mechanisms to prevent attacks or data threats. In this context, blockchain has been proposed as a solution for these scenarios [19, 20].

Widely adumbrated as immutable time-stamped data structures, blockchains are built as peer-to-peer networks where participant nodes verify interactions concurrently using decentralised consensus protocols. Data is stored in blocks that are "chained", i.e., each block knows the hash

Table 1 Comparison of blockchain applications in pharma

Approach	Technology	Data integrity assurance	Smart contracts	Domain
Benčić et al. [30]	Ethereum	–	✓	Supply chain
Bocek et al. [31]	Ethereum	–	✓	Supply chain
Chiacchio et al. [35]	Not specified	–	✓	Packaging/ERP
Debe et al. [34]	Ethereum	–	✓	Supply chain
Tseng et al. [32]	Gcoin	–	✓	Supply chain
Zhu et al. [33]	Ethereum	–	✓	Supply chain
Our proposal	Ethereum	✓	✓	Manufacturing lines/sensors

of the previous block, thus creating a ledger. Because of its tamper-proof characteristics, blockchain has emerged as a solution to enable secure traceability of information and is therefore used to ensure information provenance in multiple domains. Its scalability and resilience have proven to be efficient, particularly in conjunction with PoA consensus mechanisms for the generation of new blocks [21].

There is scant research concerning the application of blockchain technologies in the pharma industry to assess data originality in its manufacturing lines. However, general big data projects [9, 22] including smart cities [23], smart transportation [24, 25], healthcare [26], smart grids [27], and WiFi networks [28] have explored blockchain for data quality and risk reduction [10, 11]. Such literature presents blockchain as an effective technology for data quality [29]. In this context, drug manufacturing stands as an ideal scenario in which blockchain can be employed to effectively address ALCOA requirements.

Blockchain has been employed as part of the pharma supply chain for electronic tagging [30] as well as to keep temperature records in sensor-enabled shipping pallets and containers of medical supplies and medicines in order to reduce operational costs [31]. Developed by Modum.io and the University of Zürich, this ledger-based solution has been documented as a pioneering option for the safe transportation of controlled substances and, potentially, any temperature-controlled goods.

As a governance mechanism, blockchain has also been proposed to keep track of the end-to-end supply chain and exchange of medicament using cryptocurrency in Taiwan [32]. Such an approach promotes a safe commercial exchange for government agencies, manufacturers, pharmacies, large wholesalers, hospitals, and potentially patients. A similar approach has been proposed for the detection of counterfeited medicines [33]. Finally, a distributed ledger approach has been put forward to facilitate the return and redistribution of unused drugs in multi-level supply chains, a highly controversial matter in most countries due to the associated health risks [34]. Blockchain technologies have also been trialled to trace the serialisation packaging process at an Italian pharma manufacturer [35], mostly linking the marking of each medicine box and its unique identifier with the existing enterprise resource planning system.

Contribution

Table 1 includes a comparison concerning pharma-related blockchain applications. To the best of our knowledge, there is not a comprehensive technological approach to ensure traceability, authenticity, security, and other data quality dimensions [36], *sine qua non* in pharma manufacturing. Therefore, this paper proposes the use of blockchain networks for reinforcing data integrity, specifically assessing data originality.

Originality Assessment Approach

Ensuring the authenticity and traceability of the pharma manufacturing processes should arguably be addressed by the preservation of original records and comparison of any changes. Due to the intrinsic (perceived) simplicity of the ALCOA+ originality principle, it has been a challenge to ensure the authenticity of an original batch manufacturing report, particularly when data sources are fully automated, multi-device production lines within large pharma facilities.

The proposed approach is hence to verify the originality by assessing the data using a blockchain network. In this context, we describe (*i*) a pharma-related use case where we are applying the assessment tool, (*ii*) the blockchain network, and (*iii*) the implementation of our approach.

Use Case: Pharma Manufacturing Records

The SPuMoNI consortium includes a leading pharma manufacturing partner, Instituto De Angeli (IDA). IDA produces more than 2000 drug batches annually in their Italian facilities. Their production lines generate a large number of datasets and data streams from real production lines of different

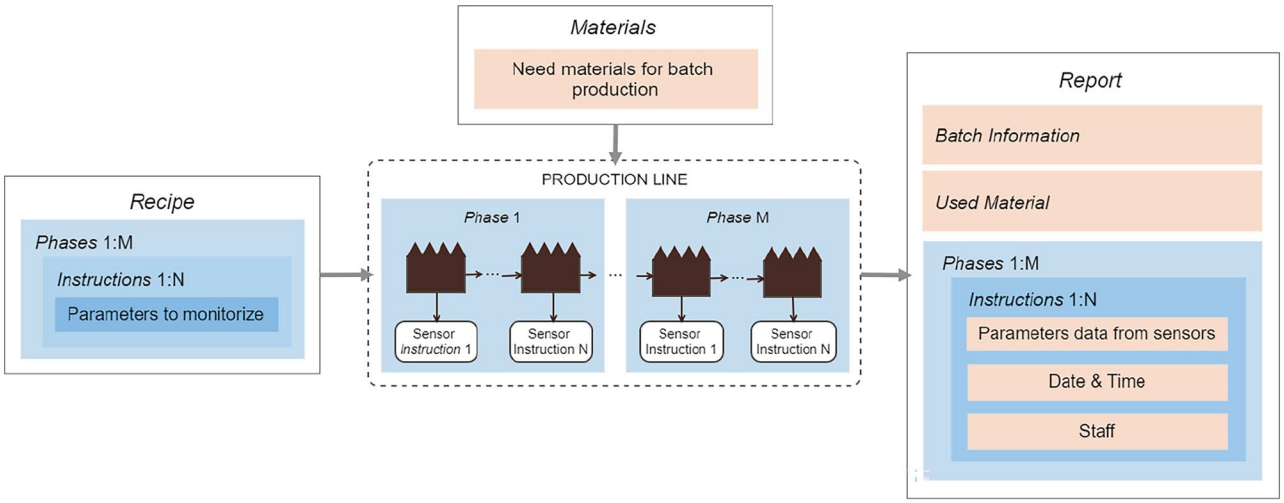


Fig. 1 Graphical representation of the workflow of manufacturing data. A *Recipe* includes *Phases* and *Instructions*. Each *Instruction* integrates the parameters to be controlled and monitored. The production line employs the required materials to execute the multiple phases. Finally, the *Report* is generated incorporating data related to the production. While orange boxes represent data from the manufacturing process, blue boxes illustrate the *Recipe* structure. The *Report* includes (*i*) *Batch information* (i.e., *Batch* code, *Recipe* code and its versions, and the *Qualified Person* responsible for the batch production), (*ii*) *Used Materials*, and (*iii*) the sensors data, i.e., date and time and the staff in charge

unit operations such as milling, granulation, coating, and tablet pressing.

During the manufacturing of a specific product, the production lines execute a set of steps based on a *Recipe*. A *Recipe* is the protocol that describes in detail the fabrication process of a certain product. It is composed of a set of *Phases*, and each *Phase* is formed from a set of *Instructions*. An *Instruction* is a single action implemented within the manufacturing process. There are various types of *Instructions*, such as setting a mixing machine, verifying the quantities of raw materials, transferring the product to the next step, checking the cleaning stage of a particular robot, *etc*. Complementing the action to be executed, each *Instruction* serves as a checkpoint within the manufacturing process. A *Recipe* may have some variations and/or updates; therefore, each *Recipe* also has an associated *Recipe Version*.

A *Recipe* describes the tasks that must be accomplished, including the optimal value and the range of acceptable values for each of the parameters. However, the production line routine may have deviations that must be controlled. Hence, all production lines are monitored by a network of sensors to not only automate the production but also to control the quality of the process. When an *Instruction* is executed, depending on its nature, some parameters must be checked, such as the temperature of some fusion, the mixing speed, the number of cycles, the amount of product processed, or to check that the *Instruction* has been completed according to the expectations. The sensors record data directly from the production lines including the start and finish date and time of each *Instruction*. These data must be collected, as well as the information about the person in charge of the *Instruction*. We explore the feasibility of tracking and ensuring the originality in pharmaceutical manufacturing by applying the proposed approach to the data recorded by these networks.

These production raw data are structured and organised as *Reports*. A *Report* contains all data related to the production of a single batch of a particular drug, and therefore, it includes all information that would be reviewed in an audit trail. At the main level of a *Report*, the attributes are related to the batch information, such as the batch code, the *Recipe* code, its version, and the *Qualified Person*. The *Qualified Person* is responsible for assuring the quality of medicines available on the market [37]; hence, this person reviews not only the overall batch production which is recorded in the *Report* but also the compliance of ALCOA+ principles. Moreover, a *Report* contains a list of used materials as well as the data recorded by sensors. It follows the *Recipe* structure: (*i*) a list of *Phases* that contains a set of *Instructions*; (*ii*) each *Instruction* item includes a list of parameters to be controlled (as indicated in the *Recipe*) and the data recorded during the process. Figure 1 is a representation of the process from the *Recipe* protocol to getting the *Report* object.

From the regulatory point of view, an audit trail evaluates random batch manufacturing records. These audits review all data generated during the process, whereby the sensor data are needed not only for quality control, but also for regulatory compliance. In this context, ensuring the originality of batch records may provide significant support for pharma manufacturing industries.

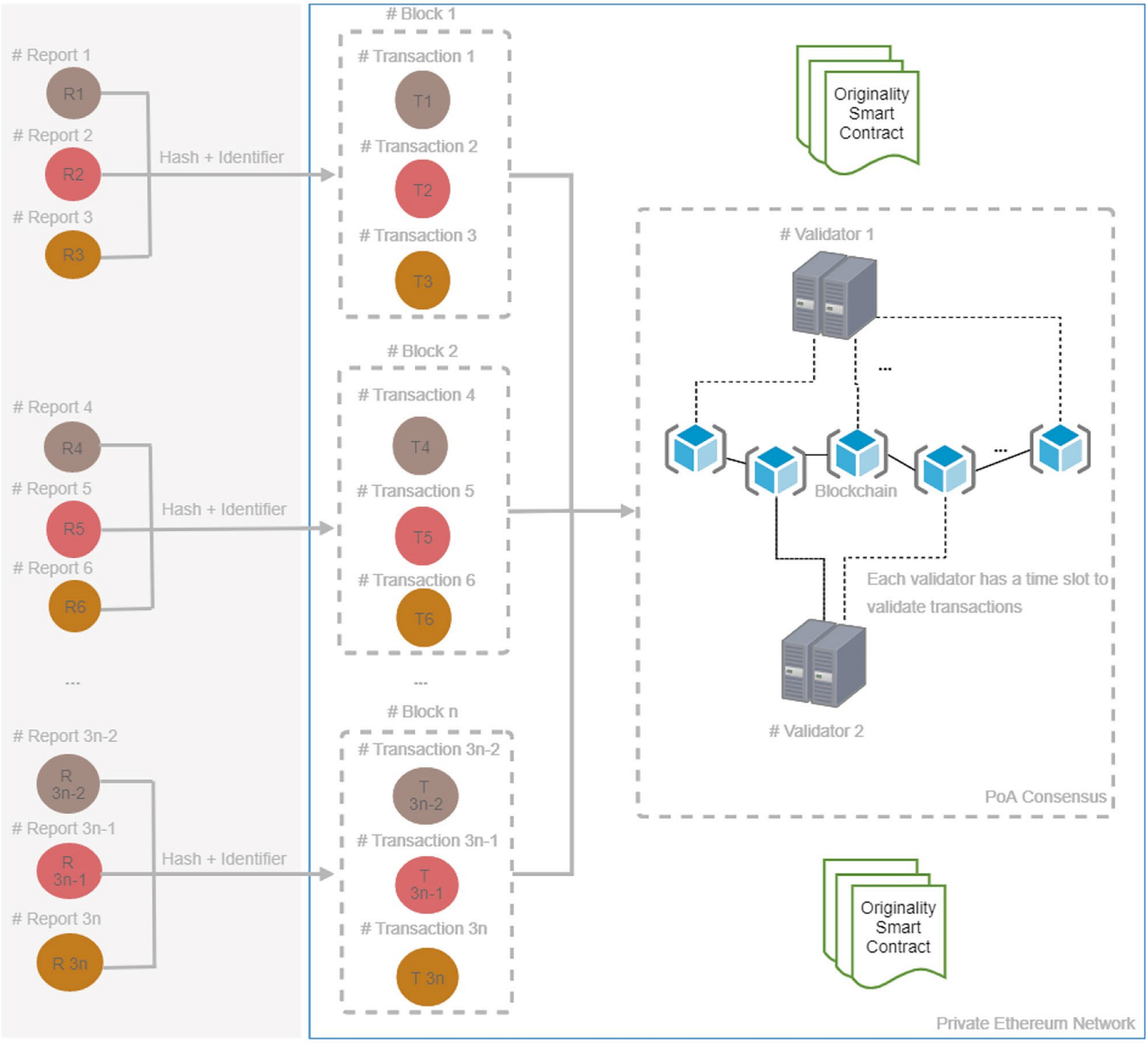


Fig. 2 Private Ethereum network configured with proof-of-authority consensus algorithm. The transactions are committed into blocks and mined by validator nodes. Once approved, the block is added to the chain. Currently, our private Ethereum network is composed of two validator nodes. The *Originality Smart Contracts* structure the data and evaluate the data originality

Blockchain Network in SPuMoNI

Blockchain has bee henticity, immutability, and transparency using decentralised environments. Decentralisation prevents single authorities from controlling the data. In this context, blockchain employs a distributed architecture eliminating centralised authorities and using immutability to prevent the alteration of past records. Moreover, by using Ethereum private networks and gas amounts, we have been able to empirically establish the feasibility to quantitatively marshal service levels and their associated quality of service for blockchain networks [38].

It is therefore possible to have an end-to-end verification of any process and, consequently, consistent verification of the corresponding data. In this scenario, we have adopted blockchain technologies to confidently ensure the originality of ALCOA+ principles taking advantage of such intrinsic properties. Specifically, our blockchain module involves (*i*) a private Ethereum network, (*ii*) PoA as consensus algorithm, and (*iii*) smart contracts. Figure 2 illustrates the behaviour of the network as transactions are received.

Private Ethereum Network Ethereum is one of the most popular blockchain technologies allowing us to implement decentralised and transaction-based systems. In addition, an Ethereum network supports smart contracts which are immutable pieces of code that enable to make intelligent decisions. Each Ethereum action requires an amount of *gas*, i.e., a computational fee required to perform specific Ethereum transactions. Our network is composed of two nodes working as miners which will receive and validate the transactions to be added into the blocks using the PoA consensus algorithm. The PoA consensus algorithm requires at least two nodes as miners to start chaining blocks in the network. Ethereum provides a JavaScript Object Notation (JSON) with Remote Procedure Call (RPC), i.e., JSON-RPC, which allows a front-end or an application to communicate with the Ethereum network. While JSON allows us to exchange data between a browser and a server, RPC allows us to perform requests in a network. Therefore, JSON-RPC defines the data structure, methods, and rules to communicate with the network.

Consensus Algorithm It is used to achieve agreement on data transactions in a distributed network ensuring that the next block to be added in a blockchain is unique and reliable. Our private Ethereum network relies on PoA, where miner nodes that work as validators are aware of all identities using a reputation-based approach. A node is able to validate transactions if at least $\frac{N}{2}+1$ network nodes have previously identified it as an honest node (where N represents the number of trusted nodes). Specifically, PoA works in our private Ethereum network as follows:

- Each validator holds a fixed time slot to validate blocks. During that time slot, the corresponding node is the network leader.
- Each node is enabled to validate transactions every $\frac{N}{2}+1$ blocks (with a mining frequency of $\frac{1}{\frac{N}{2}+1}$).
- A maximum of $N-(\frac{N}{2}+1)$ nodes are allowed to propose blocks in the same time slot. When $N = 2$, there are no simultaneous nodes validating blocks, just the leader. When N is greater than 2, multiple nodes can propose blocks within the same time slot as the leader, e.g., with $N = 16$, 7 nodes are allowed to validate blocks at the same time. If one node is down, the remaining network participants, which are able to mine transactions, will validate all transactions submitted to the network.
- The GHOST protocol [39] is applied if multiple nodes are validating the same transactions, simultaneously. This protocol privileges the leader.
- The nodes that constantly propose invalid transactions reduce their reputation and, consequently, can be excluded from the list of reliable validators.

Our PoA configuration requires a "master" miner responsible for adding new miners keeping the blockchain network fully private. Therefore, being hosted and managed by a private entity, it prevents dishonest nodes from participating in the network and, consequently, avoids potential security related attacks.

Smart Contracts The implemented private Ethereum network enables the deployment of smart contracts incorporating a dedicated data structure to manipulate transactions in the distributed network. When data is centrally stored, it can be easily manipulated to meet hidden interests. Given their tamper-proof nature, smart contracts aim to ensure complete data authenticity, i.e., avoid the manipulation from unethical stakeholders as well as user and data provenance. The proposed solution uses smart contracts to structure the data in the blockchain network and store the hash and *Identifier* values of pharmaceutical reports. Specifically, the smart contracts support a collection of transactions to access the stored information and assess the originality of the reports. Therefore, this work relies on smart contracts to evaluate the *Original* principle of ALCOA+ and, consequently, the integrity of data produced by pharmaceutical manufacturing lines. This originality is assessed by the smart contracts comparing the data stored in the blockchain network in the form of hashes and *Identifiers*. Thus, if a report with the same identifier is submitted into the network holding a different hash, the smart contract detects that report as being not original.

Implementation

The originality assessment tool aims to ensure the authenticity of data acquired and generated in pharma manufacturing lines. Towards this purpose, the tool is supported by blockchain infrastructure and provides a dashboard as the user interface.

Blockchain Infrastructure

Blockchain infrastructure is composed of a private Ethereum network that uses Go-ethereum[3] (Geth) as the Ethereum client and Solidity[4] as a smart contract language. The private Ethereum network was configured with a block period of 2 s to improve the network performance [40]. This network provides cost-free processing, i.e., the transactions are submitted using 0 as the gas price. Each OpenStack instance has 16 GiB RAM, 8 CPU, and 160 GiB of HDD. The originality

[3] https://geth.ethereum.org/

[4] https://solidity.readthedocs.io

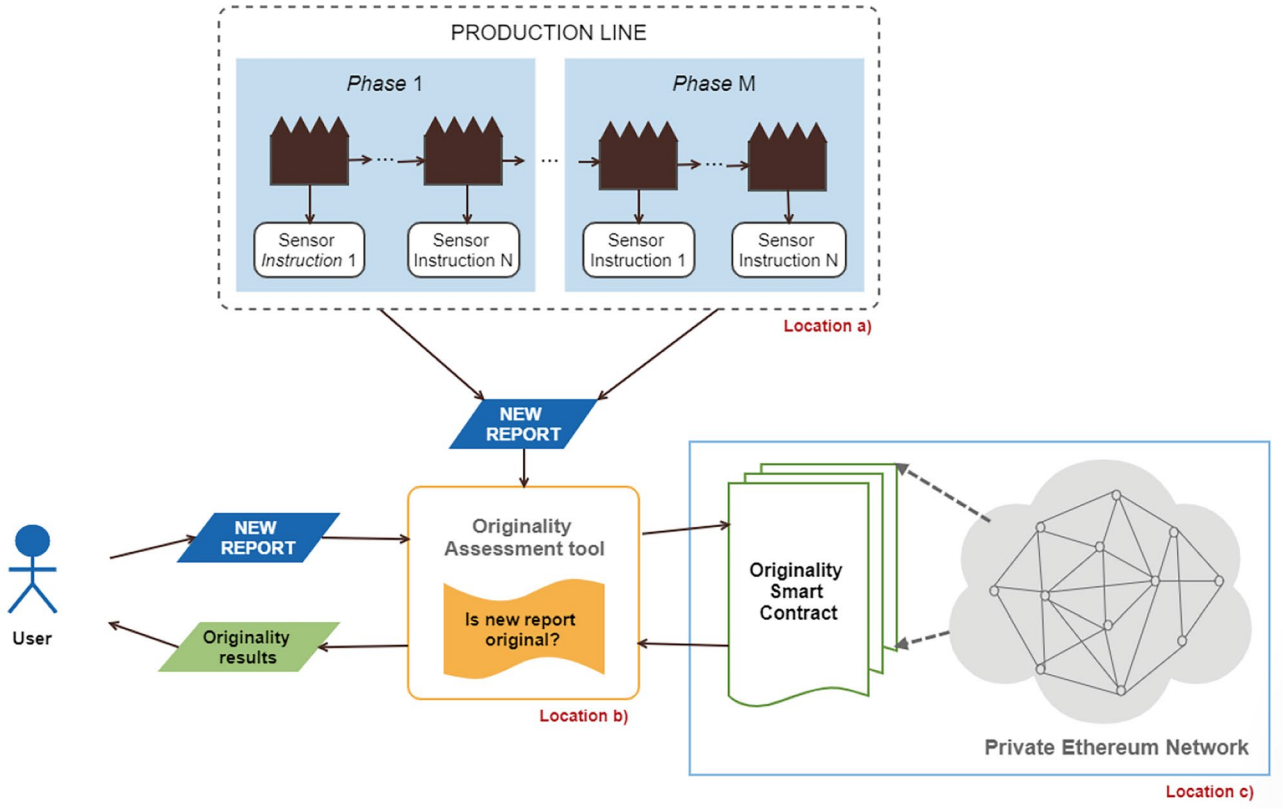


Fig. 3 Originality Assessment Workflow. The process starts by the input of a new report, likewise production line upload, or manually uploaded report by a user (here is depicted a generic user, which can be, for example, an auditor or any authorised person). The new batch is assessed by the Originality Smart Contract in the Ethereum network. The originality assessment is performed based on the previously uploaded reports on the Ethereum network, evaluating the uniqueness of the new data by comparing it with the existing stored information. The results of the assessment are visualised on the originality assessment tool, where the user can explore the reports, see whether they are original or not, and each report that is not original is provided a trace that includes the source of data falsification. This workflow schema is proposed for a distributed system; hence, the different components are labelled in red, as general locations

assessment tool uses 6.5 MB of storage and 1000 reports use 35 MB of JSON files and 139 MB of database information.

The assessment is based on uploading a new batch record to the Ethereum network as a smart contract and verifying the uniqueness of all its information. The originality assessment is achieved by the verification of data authenticity, evaluating if the batch record has been corrupted. This software is designed for a direct interaction with the production line database. However, it is also possible to manually upload new batch reports. The workflow of the originality assessment tool is described in Fig. 3.

When a new batch is manufactured, its data is uploaded using the JSON format, and then it is parsed into a *Report*. After that, the *Report hash* is calculated by converting the *Report* into a map (or Python dictionary in this case), which will be converted into a `String`. Then, this string which contains the *Report* information is transformed into a bytes array when using the SHA256 algorithm and converted into a *hash*. In addition, the *Report Identifier* is also calculated, which is composed using a combination of *batch code*, *order code*, *recipe code*, *recipe version code*, and *product code*. The *Identifier* and the *hash* are uploaded into the Originality Smart Contract instance allocated in the Ethereum network. In this function, the *Report revision number* is also computed, which is calculated by checking if another report with the same identification data is already in the Ethereum network.

To obtain the Originality results, the following phases are verified: (*i*) if the *Identifier* is unique, the *Report* is considered *Original*; (*ii*) if the *Identifier* is not unique, but the *hash* is equal to the hash of a previously uploaded Report (i.e. with the very same *Identifier*), the current Report will be considered an *Original Report*—this case occurs when the very same *Report* is uploaded twice; and (*iii*) when the *Identifier* is not unique and the *hash* is distinct from the hash of a previously uploaded Report (i.e. with the very

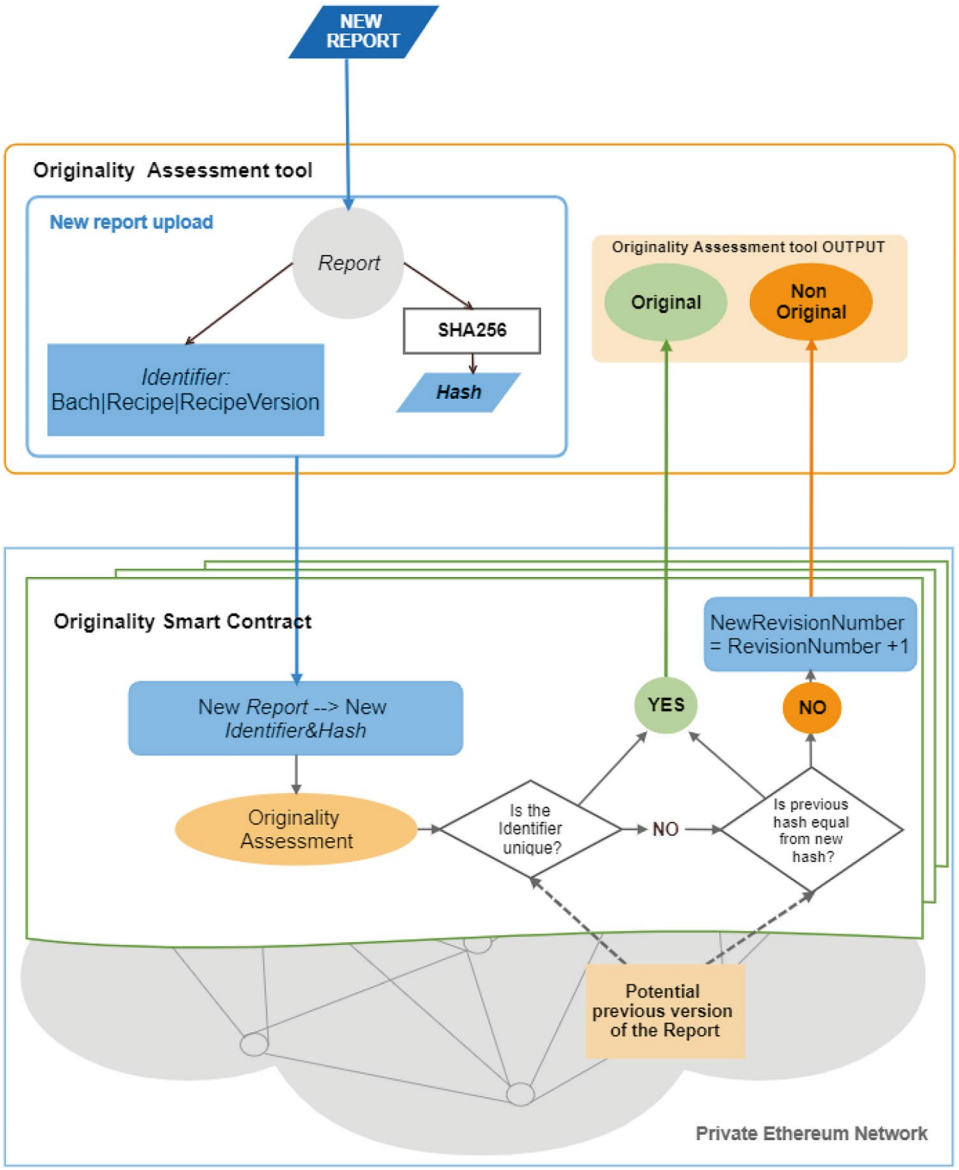


Fig. 4 Proposed Originality Assessment Process. The orange box represents the originality assessment tool, where *Identifier &hash* are calculated and the originality-related results (i.e., whether the report is original or not) are computed. The green box represents the Originality Smart Contract, where *Identifier &hash* are uploaded to the Ethereum network and the originality assessment is performed. The blue workflow illustrates the *Report* uploading, and the grey workflow represents the originality assessment. Also, the *Revision number* update is represented in a blue box, when the result of the assessment is "Non-original"

same *Identifier*), then the current *Report* is considered *Non-original*, and differences between these two versions are calculated and provided. The *complete Identifier* combines the *Identifier* with the actual *Revision number*. The *Revision number* is 0 when the *Report* is original; otherwise, it is a different version. Figure 4 summarises our approach for the originality assessment process.

Dashboard

For an easy interaction and comprehension of the results, the Originality Assessment tool has a user interface built using the Django framework and Python 3, in addition to the Bootstrap 4 web front-end framework. The main dashboard screen contains a summary table of the assessed reports including the batch code, the *Recipe* executed, the version of the *Recipe*, the *Revision number* and the originality assessment results. The tool also provides in-depth detailed information at report level, namely a user can explore the interactive view for a single Originality assessment result. Each batch information is represented in a table that includes (*i*) the batch code, (*ii*) the *Recipe* executed, (*iii*) the version of the *Recipe*, (*iv*) the *Revision number*, (*v*) the qualified person, and (*vi*) a breakdown of the assessment results. Additionally, the *Report identifier*, the *Report version number*, and the data trace (which identifies data disagreements between the current *Report* and its previous version) are included. Some examples of this interface are included in the "Results" section.

Table 2 Confusion matrix for the originality assessment results of 1300 *Reports* evaluated

		Detected situation					
		# Original reports	# Falsified reports				
			(1) Falsification of aualified person	(2) Falsification of staff	(3) Falsification of date and time	(4) Falsification of sensor data	(5) Multiple types of data falsification
Real situation	Original	1000	0	0	0	0	0
	Falsification of qualified person	0	12	0	0	0	0
	Falsification of staff	0	0	18	0	0	0
	Falsification of date and time	0	0	0	19	0	0
	Falsification of sensor data	0	0	0	0	12	0
	Multiple types of data falsification	0	0	0	0	0	239

Evaluation and Results

The originality assessment tool provides support for assessing and ensuring data originality in pharmaceutical manufacturing. A critical measure of the effectiveness of the approach is whether the originality assessment tool is capable of accurately detecting manufacturing records that are not original. In addition, another assessment of the usefulness of the approach is whether it correctly identifies the root cause (i.e., source of falsification) of the non-original records. To empirically evaluate our approach, we have designed an evaluation methodology which allows us to measure the originality assessment accuracy as well as the system performance.

Evaluation Setup and Methodology

To evaluate our approach, we will upload a set of batch reports where a subset of these are randomly falsified. We have defined five types of data falsification based on typical situations that should be detected in a real-world scenario:

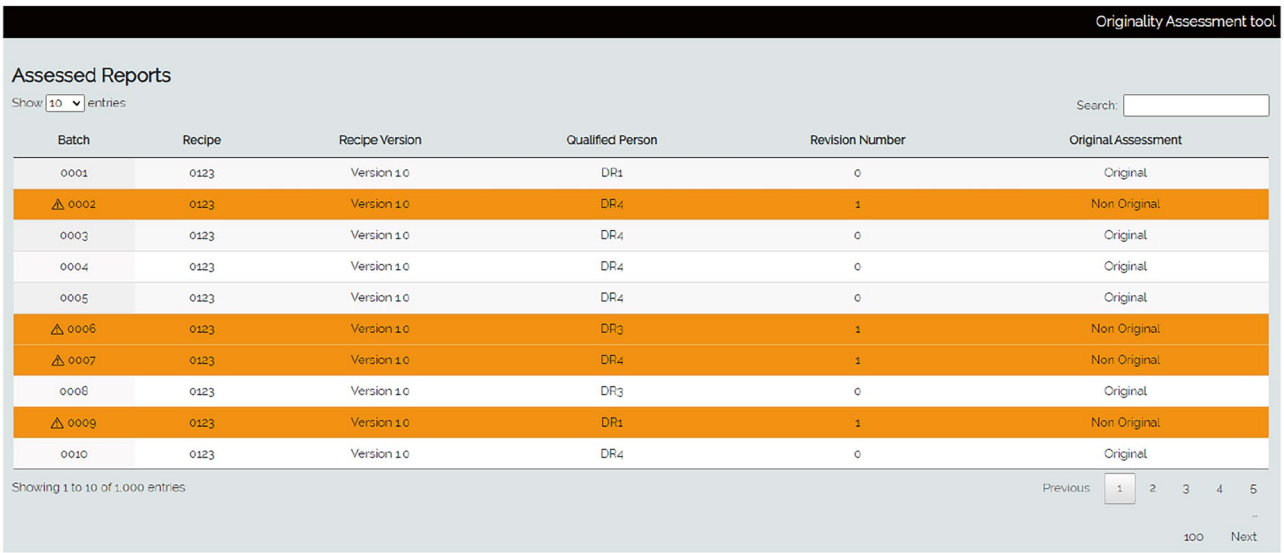
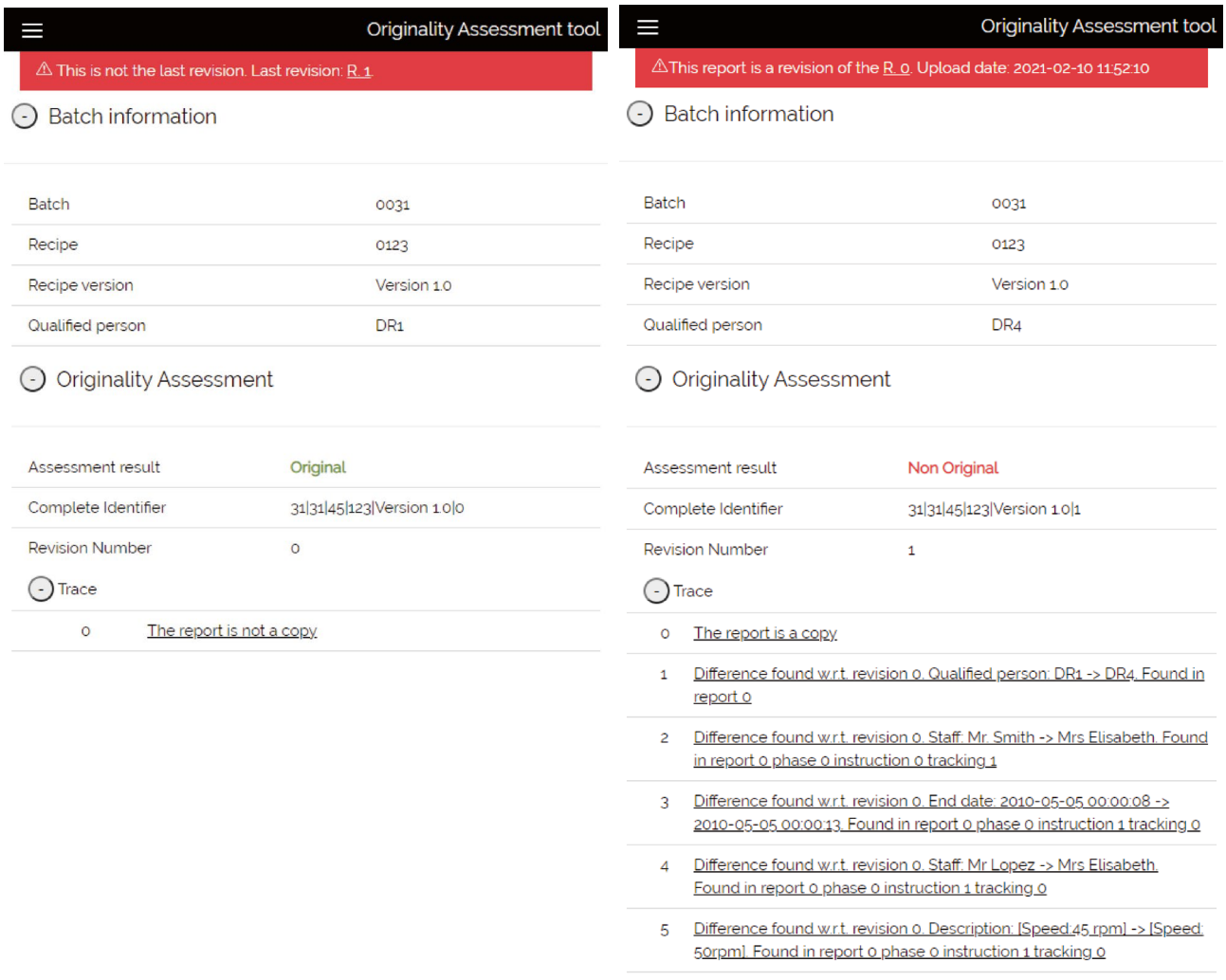


Fig. 5 *Dashboard of the Originality Assessment tool.* The dashboard provides a list of assessed reports. The reports identified as having originality-related issues are highlighted in orange. The columns represent the batch code, the *Recipe* executed, the version of the *Recipe*, the *Qualified Person* responsible for the batch data, the *Revision number*, and the original assessment result

(i) adulteration of the qualified person, *(ii)* adulteration of staff in charge of an instruction, *(iii)* adulteration of date and time of recording data, *(iv)* adulteration of the value of some sensor data, and *(v)* a combination of the former.

Due to privacy requirements of the Fareva-IDA facilities, we have employed data fabrication techniques to generate realistic temporal series for 1.000 *Reports* based on real raw data from their production lines, which account for some six months of their manufacturing operations. In addition, 300 reports were randomly selected to be generated as non-original, i.e., falsified. This set of non-original *Reports* may have one *(scenarios i–iv)* or multiple types *(scenario v)* of the data falsification scenarios defined above. The number and types of individual data falsifications applied in the fifth scenario to each non-original *Report* were randomly selected. The purpose of generating this random dataset of *Reports* was to simulate a real-world situation where data falsification occurs, i.e., without knowing which data has been falsified by design. It will allow us to evaluate our tool's capability to detect the source of such falsifications.



(a) Originality Assessment Revision 0

(b) Originality Assessment Revision 1

Fig. 6 *Multiple data modifications: Batch 0031*. This figure shows a comparison between the originality assessment results of Batch 0031 Revision Number 0 (**a**) and Batch 0031 Revision Number 1 (**b**), where result **a** is "Original" and result **b** is "Non-original". There are five types of data adulteration: (1) the qualified person has changed from Data Responsible 1 (DR1) to Data Responsible 4 (DR4); (2) in the *Instruction* 0 of *Phase* 0, the staff has been changed from Mr. Smith to Mrs. Elisabeth; (3) in the *Instruction* 0 of *Phase* 0, the recording date and time has been increased by 5 s; (4) in the *Instruction* 1 of *Phase* 0, the staff has been changed from Mr. Lopez to Mrs. Elisabeth; and, finally, (5) in the *Instruction* 1 of *Phase* 0, the original *Speed* data has been increased by 5 rpm. These data adulterations are summarised in the Revision 1 trace (**b**)

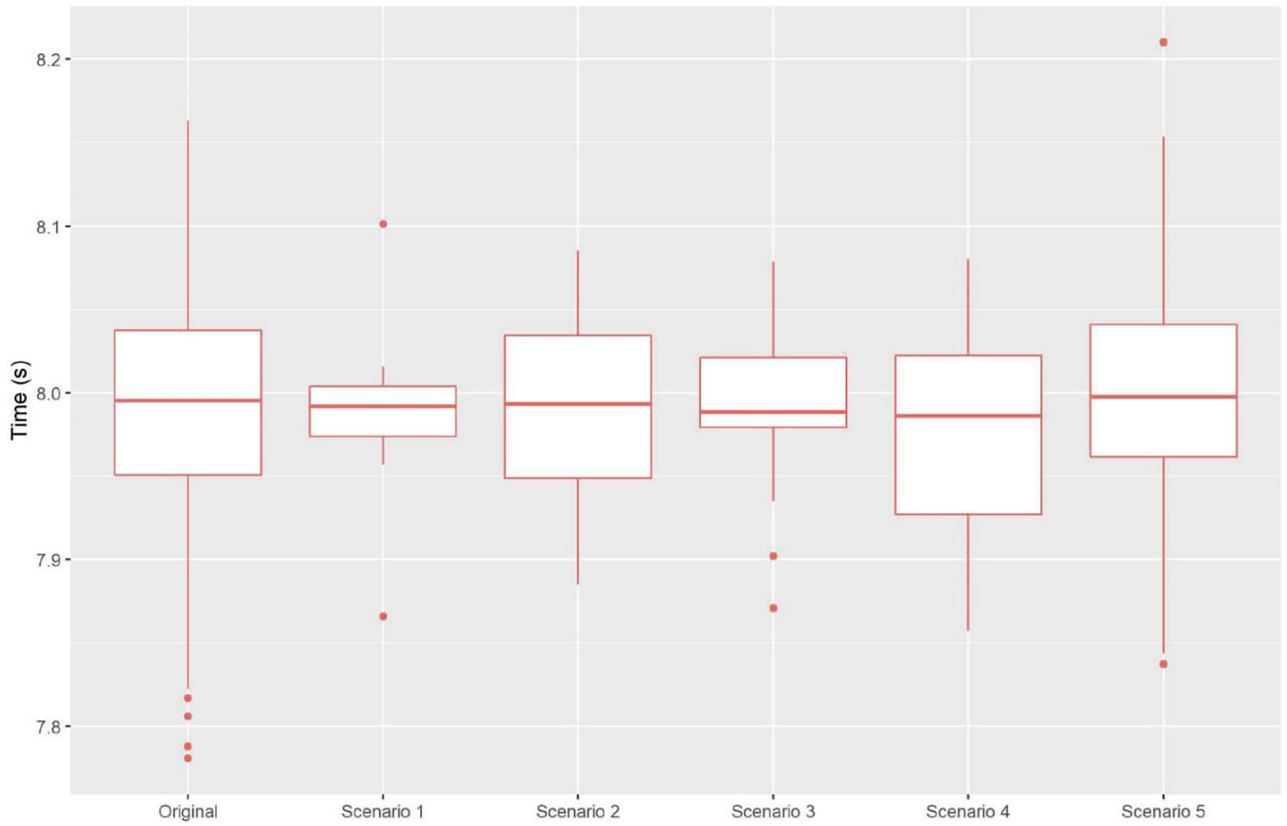


Fig. 7 System performance pertaining to the experiments included in Table 2: original reports, scenario 1, scenario 2, scenario 3, scenario 4, and scenario 5

Furthermore, the uploading and assessing time for each *Report* also has been measured, in order to characterise the overall distributed system performance as the Ethereum network is located at the NCI Cloud Competency Centre in Dublin and the Originality Assessment tool runs at the UPV facilities in Valencia. This distributed environment has allowed us to study the latency in the originality assessment process. Since the running time is recorded for each *Report*, we have also compared the times of evaluating the original and non-original *Reports*, distinguishing between the five *(i–v)* types of falsification, with the purpose of detecting potential performance variability due to the data falsification.

Results

Table 2 summarises these results and shows that the originality assessment tool has accurately detected as falsified reports all the *Reports* that were randomly altered, i.e., falsified (as compared to their originals). Therefore, our approach shows 100% accuracy in detecting non-original data. Furthermore, the tool has successfully identified, for each report, the source of data falsification.

Dashboard Results Visualisation

This subsection shows some examples of result visualisation on the developed dashboard. Figure 5 shows the main menu, which presents a sample list of the assessed reports together with a results summary. The non-original reports are highlighted in orange.

Once the user clicks in one of the assessed reports of Fig. 5, the dashboard shows the detailed results of its assessment. We present an example of this interface for assessment visualisation for *Scenario 5: Multiple sources of data falsification* in Fig. 6. For other examples of scenarios 1 to 4, please see the supplementary material.

Performance Characterisation

The mean time for uploading and assessing 1300 *Reports* was 8.00 s with a standard deviation of 0.221 (normal distribution, Shapiro-Wilk normality test, $\alpha = 0.05$).

To analyse potential discrepancies in the performance results between all five falsification scenarios and the original *Reports*, we have applied a one-way ANOVA test followed by a Tukey Honest Significant Differences post hoc test.

Statistically, there was no significant difference among the analysed scenarios ($\alpha = 0.05$). As such, there is no evidence of any effect of data falsification on the performance of the proposed original assessment tool. Figure 7 illustrates the six box plots for each group of *Reports*.

Conclusions

The pharmaceutical industry is a data-intensive domain. Its manufacturing lines continuously generate large amounts of data that must be collected and have to be ALCOA+ compliant. However, the risk of negligent or non-intentional falsification is high in pharma environments. In this context, the pharmaceutical industry requires effective solutions to improve its manufacturing process in terms of ALCOA+ compliance. Blockchain, together with smart contracts, has shown to be a promising technology concerning data authenticity. Towards this scenario, we propose a novel blockchain-based approach for assessing originality (i.e., the "O" in the ALCOA+). The proposed method is composed of a private Ethereum network incorporating smart contracts to detect data falsifications.

The proposed method has been evaluated using pharma batch records where multiple types of data falsifications were randomly applied using a geographically distributed system. The results show the feasibility of our approach to support the compliance of ALCOA+ principles, in particular, the originality principle, as our tool has accurately detected all records as to whether they are original or not. Furthermore, for the records that are not original, our approach provides a trace with the source of data falsifications. It is important to note that all experiments have been performed under a controlled scenario and with standard data; however, performance characterisation results suggest that the proposed method should be scalable for large datasets in distributed environments. To achieve a higher readiness level, an evaluation of the proposed tool in the pharma shop-floor environment is needed. Therefore, as future work, we aim to validate our originality tool in a real pharma manufacturing environment and integrate it within the SPuMoNI system.

Appendix

These appendices contain supplementary materials for the *Blockchain for Data Originality in Pharma Manufacturing* manuscript. In particular, Appendix A provides the pseudo-code pertaining to the algorithm to assess originality and Appendix B presents examples of Scenarios 1 to 4 described within the manuscript.

Appendix A. Algorithm: Originality Assessment

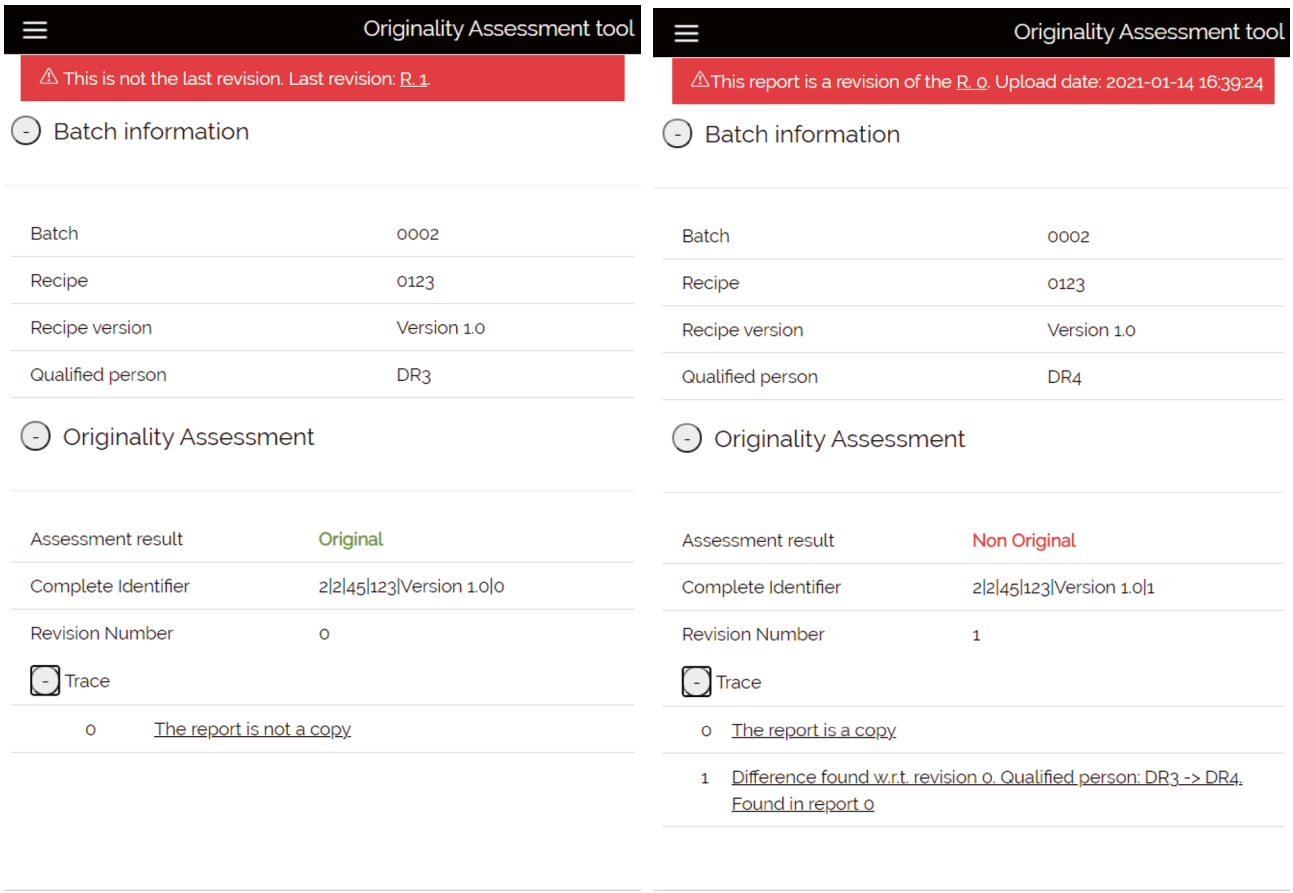
Algorithm 1 describes the Originality assessment process illustrated in Fig. 3. Specifically, it includes the steps to assess the originality of an updated manufacturing report. The comparison of *Identifiers ID* is executed within the Smart Contract *sc*. The *result* represents the evaluation to be displayed to the user in the Originality Assessment Tool dashboard.

Algorithm 1: Originality Assessment process corresponding to the workflow depicted in Figure 3

```
Input: Reports
Data: sc
Result: Originality evaluation: ORIGINAL or NON.ORIGINAL
begin
    // Receive a new report
    Report ← NewReport
    // Identifier composition
    ID ← Report.Batch + Report.Recipe + Report.RecipeVersion
    // Calculate the Report Hash
    Hash ← SHA256(Report)
    // Send Hash and Identifier to the smart contract sc
    if ID ≠ sc.ID then // Is the ID unique?
        sc.ID ← ID
        sc.ID.Hash ← Hash
        sc.ID.Revision.Number ← 0
        result ← ORIGINAL
    else
        if Hash = sc.ID.Hash then // Has ID the same Hash?
            result ← ORIGINAL
        else
            sc.ID.Revision.Number ← sc.ID.Revision.Number + 1
            result ← NON.ORIGINAL
    return result
```

Appendix B. Scenario Examples

The "Evaluation and Results" section describes five types of data falsification scenarios. Since the manuscript includes an example of Scenario 5 with multiple data falsification sources, this supplementary material furnishes four examples pertaining to Scenarios 1 to 4. Each result is shown in connection with its original batch report result.



(a) Originality Assessment Revision 0

(b) Originality Assessment Revision 1

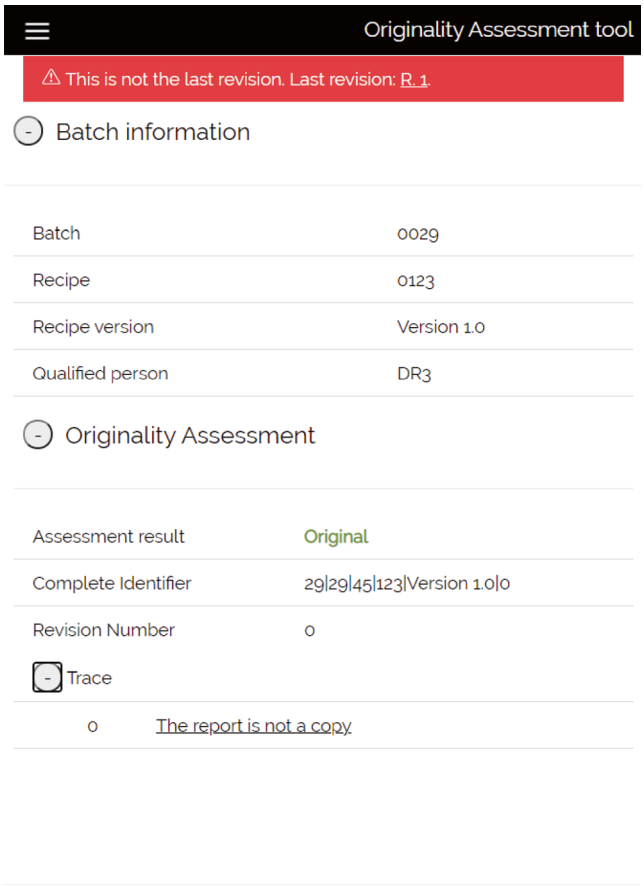
Fig. 8 *Modification of the Qualified Person: Batch 0002*. This figure shows a comparison between the Originality Assessment results of Batch 0002 Revision Number 0 (**a**) and Batch 0002 Revision Number 1 (**b**), where result **a** is "Original" and result **b** is "Non-original". The data adulteration is the *Qualified Person* field, which is DR3 in version 0 and DR4. The modification is also visualised on the trace of version 1 (**b**)

Scenario 1: Adulteration of the Qualified Person

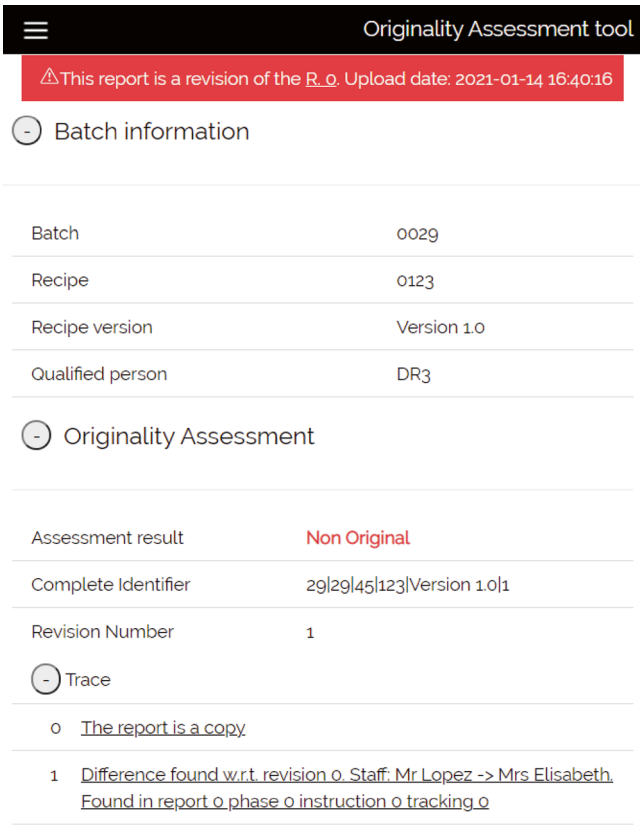
The Originality Assessment tool successfully detected all the reports with this data adulteration. The tool flagged as "Non-original" those reports in which the *Qualified Person* was modified. It also correctly identified the falsification, i.e., the relevant piece of data changed, as shown in Fig. 8.

Scenario 2: Adulteration of Staff in Charge of an Instruction

The Originality Assessment tool successfully detected all reports where there was data adulteration. The tool flagged as "Non-original" those reports where any value of the staff in charge of an instruction was modified identifying the falsified data in question. Figure 9 shows an example of this scenario.



(a) Originality Assessment Revision 0



(b) Originality Assessment Revision 1

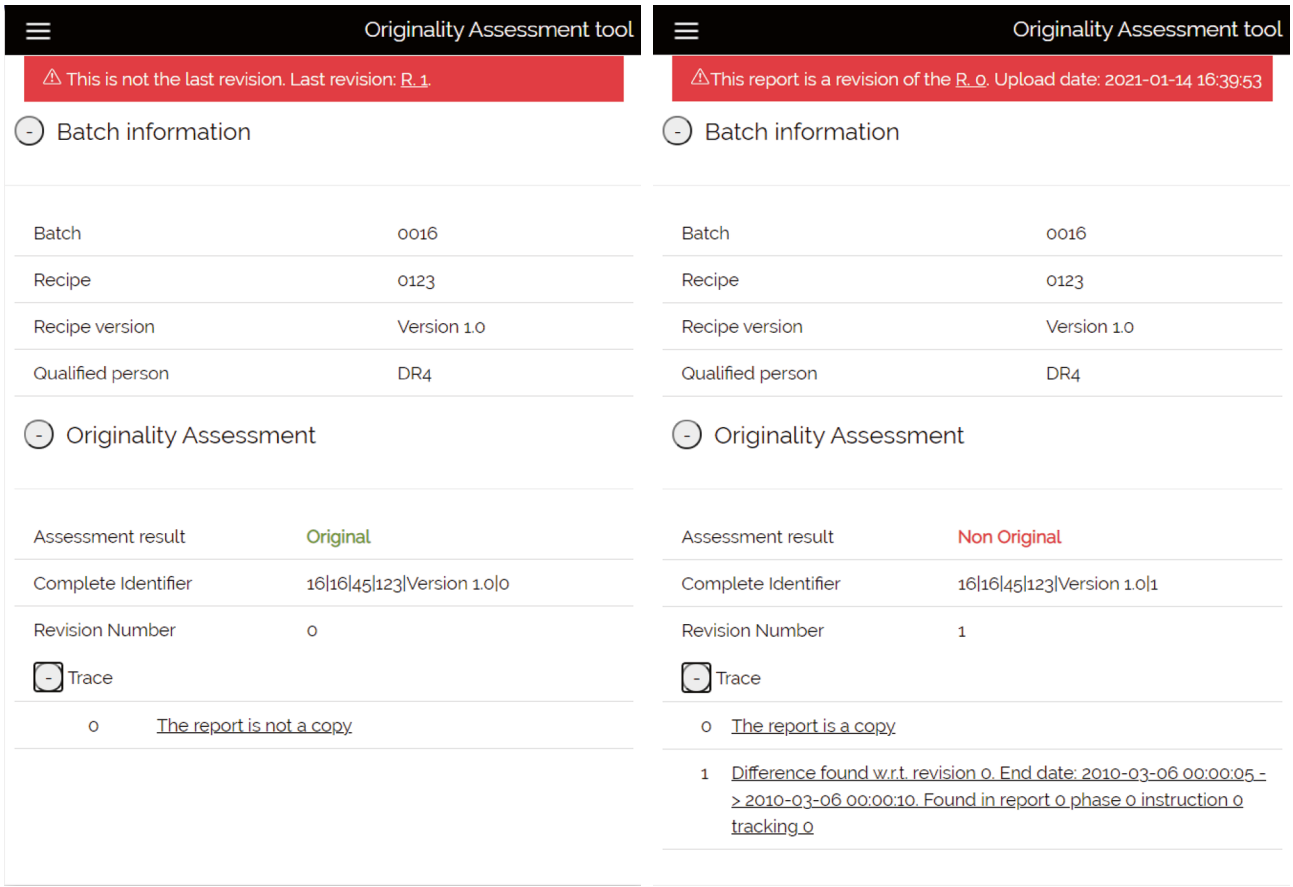
Fig. 9 *Modification of one of the Staff in charge of an instruction: Batch 0029.* This figure shows a comparison between the Originality assessment results of Batch 0029 Revision Number 0 (**a**) and Batch 0029 Revision Number 1 (**b**), where result **a** is "Original" and result **b** is "Non-original". The data adulteration is in the *Instruction* 0, where the original data has been changed for "Mrs Elisabeth", which is visualised on the trace of version 1 (**b**)

Scenario 3: Adulteration of Date & Time of Recording Data

In this case, the data adulteration has also been successfully detected. The tool flagged as "Non-original" those reports where any date &time value of the recorded data was modified, identifying the falsified data as shown in Fig. 10.

Scenario 4: Adulteration of Sensor Data

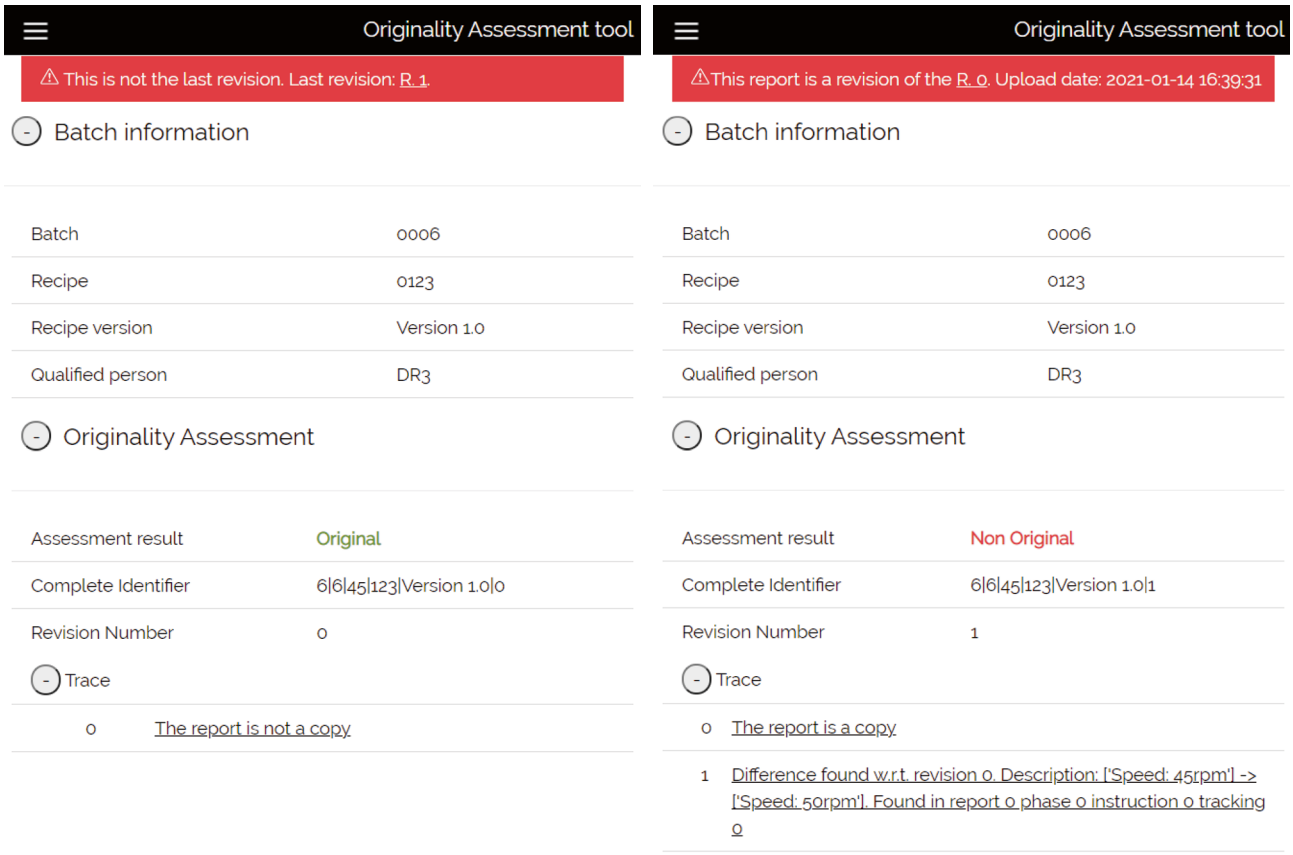
Similarly, in this case, the data adulteration has been successfully detected. The tool flagged as "Non-original" all reports where any data from sensors was modified. It also identified correctly the actual falsified data. Figure 11 shows an example of such detection.



(a) Originality Assessment Revision 0

(b) Originality Assessment Revision 1

Fig. 10 *Modification of one of the recordings of date & time of an instruction: Batch 0016*. This figure shows a comparison between the Originality Assessment results of Batch 0016 Revision Number 0 (**a**) and Batch 0016 Revision Number 1 (**b**), where result **a** is "Original" and result **b** is "Non Original". The data adulteration is in the *Instruction* 0, where the original *date& time* data has been increased by 5 s, which is visualised on the trace of version 1 (**b**)



(a) Originality Assessment Revision 0

(b) Originality Assessment Revision 1

Fig. 11 *Modification of a sensor in an instruction: Batch 0006*. This figure shows a comparison between the Originality Assessment results of Batch 0006 Revision Number 0 (**a**) and Batch 0006 Revision Number 1 (**b**), where result **a** is "Original" and result **b** is "Non-original". The data adulteration is in the *Instruction* 0, where the original *Speed* data has been increased 5 rpm; this is visualised on the trace of version 1 (**b**)

Author Contribution All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Marta Durá, Fátima Leal, Ángel Sánchez-García and Carlos Sáez. The first draft of the manuscript was written by Marta Durá and Adriana E-Chis, Horacio González-Vélez and Juan M. García Gómez commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. This work has been developed under the auspices of the SPUMONI research project (www.spumoni.eu) funded from 2019 to 2022 by CHIST-ERA, the Horizon 2020 Future and Emerging Technologies programme of the European Union through the ERA-NET Cofund funding scheme (CHIST-ERA BDSI Call 2017). In particular, this work has been funded by the Agencia Estatal de Investigación, Spain.

Data Availability Data sharing is not applicable to this article as no datasets were generated during the current study.

Declarations

Ethics Approval Not Applicable.

Conflict of Interest I declare the absence of any conflict of interest for the publication of the named manuscript.

References

1. European Parliament–Council of the European Union, Directive 2011/62/EU of the European Parliament and of the Council of 8 June 2011 amending Directive 2001/83/EC on the Community

code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products, Official Journal of the European Union 54 (2011) Document 32011L0062. http://dx.doi.org/10.3000/17252555.L_2011.174.eng.
2. McManus D, Naughton BD. A systematic review of substandard, falsified, unlicensed and unregistered medicine sampling studies: a focus on context, prevalence, and quality. BMJ Glob Health. 2020;5(8):e002393. https://doi.org/10.1136/bmjgh-2020-002393.
3. Rahman MS, Yoshida N, Tsuboi H, Tomizu N, et al. The health consequences of falsified medicines - a study of the published literature. Trop Med Int Health. 2018;23(12):1294–303. https://doi.org/10.1111/tmi.13161.
4. Attaran A, et al. How to achieve international action on falsified and substandard medicines. BMJ. 2012;345:e7381. https://doi.org/10.1136/bmj.e7381.
5. Mackey TK, Nayyar G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opin Drug Saf. 2017;16(5):587–602. https://doi.org/10.1080/14740338.2017.1313227.
6. U.S. Department of Health and Human Services, Data integrity and compliance with CGMP guidance for industry, Draft Guidance Pharmaceutical Quality/Manufacturing Standards (CGMP), Food and Drug Administration, Silver Spring (Apr. 2016). https://www.fda.gov/drugs/guidance-compliance-regulatory-information/
7. Sotelo J, Fan Z. Mapping TradeTech: Trade in the fourth industrial revolution. Insight report, World Economic Forum, Geneva.(Dec. 2020).https://www.weforum.org/reports . Accessed 12 Aug 2021.
8. Tonshoff HK, Inasaki I. editors. Sensors in manufacturing. Weinheim: Wiley-VCH Verlag; 2001. ISBN: 3-527-29558-5.
9. Li X, Wang Z, Leung VCM, Ji H, Liu Y, Zhang H. Blockchain-empowered data-driven networks: a survey and outlook. ACM Comput Surv. 2021;54(3):1–38. https://doi.org/10.1145/3446373.
10. Kumar R, Tripathi R, Marchang N, Srivastava G, Gadekallu TR, Xiong NN. A secured distributed detection system based on IPFS and blockchain for industrial image and video data security. J Parallel Distrib Comput. 2021;152:128–43. https://doi.org/10.1016/j.jpdc.2021.02.022.
11. Ch R, Srivastava G, Gadekallu TR, Maddikunta PKR, Bhattacharya S. Security and privacy of UAV data using blockchain technology. J Inf Secur Appl. 2020;55:102670. https://doi.org/10.1016/j.jisa.2020.102670.
12. Lee SL, O'Connor TF, et al. Modernizing pharmaceutical manufacturing: from batch to continuous production. J Pharm Innov. 2015;10(3):191–9. https://doi.org/10.1007/s12247-015-9215-8.
13. Wang S, Wan J, Zhang D, Li D, Zhang C. Towards smart factory for industry 4.0: a self-organized multi-agent system with big data based feedback and coordination. Comput Netw. 2016;101:158–68. https://doi.org/10.1016/j.comnet.2015.12.017.
14. Ding B. Pharma Industry 4.0: Literature review and research opportunities in sustainable pharmaceutical supply chains. Process Saf Environ Prot. 2018;119:115–30. https://doi.org/10.1016/j.psep.2018.06.031.
15. Steinwandter V, Borchert D, Herwig C. Data science tools and applications on the way to Pharma 4.0. Drug Discovery Today. 2019;24(9):1795–805. https://doi.org/10.1016/j.drudis.2019.06.005.
16. Leal F, Chis AE, Caton S, González-Vélez H, García-Gómez JM, et al. Smart pharmaceutical manufacturing: Ensuring end-to-end traceability and data integrity in medicine production. Big Data Res. 2021;24(100172):1–12. https://doi.org/10.1016/j.bdr.2020.100172.
17. Rattan AK. Data integrity: History, issues, and remediation of issues. PDA J Pharm Sci Technol. 2018;72(2):105–16. https://doi.org/10.5731/pdajpst.2017.007765.
18. Wingate G, et al. GAMP guide: Records & data integrity, Guide ISPE GAMP 5, International Society for Pharmaceutical Engineering, Florida. 2017. https://ispe.org/publications/guidance-documents/.
19. Alladi T, Chamola V, Parizi RM, Choo K-KR. Blockchain applications for industry 4.0 and industrial IoT: a review. IEEE Access. 2019;7:176935–51. https://doi.org/10.1109/ACCESS.2019.2956748.
20. Wang Q, Zhu X, Ni Y, Gu L, Zhu H. Blockchain for the IoT and industrial IoT: a review. Internet Things. 2020;10:100081. https://doi.org/10.1016/j.iot.2019.100081.
21. de Oliveira MT, Reis LH, Medeiros DS, Carrano RC, Olabarriaga SD, Mattos DM. Blockchain reputation-based consensus: a scalable and resilient mechanism for distributed mistrusting applications. Comput Netw. 2020;179:107367. https://doi.org/10.1016/j.comnet.2020.107367.
22. Hu D, Li Y, Pan L, Li M, Zheng S. A blockchain-based trading system for big data. Comput Netw. 2021;191:107994. https://doi.org/10.1016/j.comnet.2021.107994.
23. Xie J, Tang H, Huang T, Yu FR, Xie R, Liu J, Liu Y. A survey of blockchain technology applied to smart cities: Research issues and challenges. IEEE Commun Surv Tutor. 2019;21(3):2794–830. https://doi.org/10.1109/COMST.2019.2899617.
24. Ahmed SH, Bashir AK, Ahmad A, Guibene W. Computer networks special issue on intelligent and connected transportation systems. Comput Netw. 2019;164:106895. https://doi.org/10.1016/j.comnet.2019.106895.
25. Singh M, Kim S. Branch based blockchain technology in intelligent vehicle. Comput Netw. 2018;145:219–31. https://doi.org/10.1016/j.comnet.2018.08.016.
26. Zhang P, Schmidt DC, White J, Lenz G. Blockchain technology use cases in healthcare. In: Advances in Computers, vol. 111, pp. 1–41. Elsevier. 2018. http://dx.doi.org/10.1016/bs.adcom.2018.03.006.
27. Alladi T, Chamola V, Rodrigues JJ, Kozlov SA. Blockchain in smart grids: a review on different use cases. Sensors. 2019;19(22):4862. https://doi.org/10.3390/s19224862.
28. Brincat AA, Lombardo A, Morabito G, Quattropani S. On the use of blockchain technologies in WiFi networks. Comput Netw. 2019;162:106855. https://doi.org/10.1016/j.comnet.2019.07.011.
29. Lu Y. The blockchain: State-of-the-art and research challenges. J Ind Inf Integr. 2019;15:80–90. https://doi.org/10.1016/j.jii.2019.04.002.
30. Benčić FM, Skočir P, Žarko IP. DL-Tags: DLT and smart tags for decentralized, privacy-preserving, and verifiable supply chain management. IEEE Access. 2019;7:46198–209. https://doi.org/10.1109/ACCESS.2019.2909170.
31. Bocek T, Rodrigues BB, Strasser T, Stiller B. Blockchains everywhere - a use-case of blockchains in the pharma supply-chain. In: 2017 IFIP/IEEE IM, pp. 772–7. Lisbon. 2017. http://dx.doi.org/10.23919/INM.2017.7987376.
32. Tseng J-H, Liao Y-C, Chong B, Liao S-W. Governance on the drug supply chain via Gcoin blockchain. International Journal of Environmental Research and Public Health. 2018;15(6):1055:1–8. https://doi.org/10.3390/ijerph15061055.
33. Zhu P, Hu J, Zhang Y, Li X. A blockchain based solution for medication anti-counterfeiting and traceability. IEEE Access. 2020;8:184256–72. https://doi.org/10.1109/ACCESS.2020.3029196.
34. Debe M, Salah K, Jayaraman R, Arshad J. Blockchain-based verifiable tracking of resellable returned drugs. IEEE Access. 2020;8:205848–62. https://doi.org/10.1109/ACCESS.2020.3037363.
35. Chiacchio F, D'Urso D, Compagno L, Chiarenza M, Velardita L. Towards a blockchain based traceability process: a case study from pharma industry. In: APMS 2019, Vol. 566 of IFIP Advances in Information and Communication Technology. Springer, Cham. 2019. pp. 451–7. http://dx.doi.org/10.1007/978-3-030-30000-5_56.
36. Sáez C, Martínez-Miranda J, Robles M, García-Gómez J. Organizing data quality assessment of shifting biomedical data. In: Quality of Life through Quality of Information, Vol. 180 of Studies in Health Technology and Informatics. IOS Press. 2012. pp. 721–5. http://dx.doi.org/10.3233/978-1-61499-101-4-721.
37. European Union, Good Manufacturing Practice (GMP) guidelines: Annex 16-certification by a qualified person and batch release. In:

EudraBook V1: Compendium of EU pharmaceutical law, Vol.4 of Guidelines for good manufacturing practices for medicinal products for human and veterinary use, Catalogue number : NB-06-15-186-EN-N. 2015, p. Version 1.3. http://dx.doi.org/10.2772/288501.

38. Leal F, Chis AE, González-Vélez H. Multi-service model for blockchain networks. Inf Process Manag. 2021;58(3):102525. https://doi.org/10.1016/j.ipm.2021.102525.
39. Wood G. Ethereum: a secure decentralised generalised transaction ledger. Yellow Paper Petersburg version 6424f7d: 2020-12-28. Parity.io. 2014.https://ethereum.github.io/yellowpaper/paper.pdf . Accessed 12 Aug 2021.
40. Leal F, Chis AE, González-Vélez H. Performance evaluation of private Ethereum networks. SN Computer Science. 2020;1(5):285:1–17. https://doi.org/10.1007/s42979-020-00289-7.