A blockchain-based confidentiality-preserving approach to traceability in Industry 4.0

Valentin Mullet, Patrick Sondi, Éric Ramat

▶ **To cite this version:**

Valentin Mullet, Patrick Sondi, Éric Ramat. A blockchain-based confidentiality-preserving approach to traceability in Industry 4.0. International Journal of Advanced Manufacturing Technology, 2023, 124 (3-4), pp.1297-1320. 10.1007/s00170-022-10431-9 . hal-04182400

HAL Id: hal-04182400
https://hal.science/hal-04182400

Submitted on 17 May 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A Blockchain based Confidentiality-Preserving Approach to Traceability in Industry 4.0

Valentin Mullet[1], Patrick Sondi[1*†] and Eric Ramat[1†]

[1*]Université du Littoral Côte d'Opale, LISIC EA 4491, F-62228 Calais, France.

*Corresponding author(s). E-mail(s): patrick.sondi@univ-littoral.fr;
Contributing authors: valentin.mullet@univ-littoral.fr; eric.ramat@univ-littoral.fr;
†These authors contributed equally to this work.

Abstract

Industry 4.0 involves major changes in manufacturing process management. Both the Internet of Things and cloud computing allow online interactions between third parties, such as providers, customers and suppliers, with the traceability system of a factory. Several blockchain based approaches have been proposed to increase confidence in traceability data, and reinforce trust. However, the transparency brought may be at the cost of risks to factory's confidential data exposure. This paper investigates the way these critical data, that are necessary to post-assembly audit, could be included into traceability data, and validated through the related transactions by the third parties, without compromising their confidentiality. Accordingly, this proposal includes the description of a blockchain based traceability system, and its implementation using the Multichain platform. In addition to its confidentiality-preserving feature, we discuss the way energy consumption and storage volume induced could be managed so as to favor its effective adoption by manufacturing factories.

Keywords: Traceability, Industry 4.0, Confidentiality, Blockchain

1 Introduction

With industry 4.0, new technologies have been brought into the supply chain environment, where they still contribute to improve efficiency. Various equipment using these technologies generate an increasing amount of data during their operations related to traceability. Traceability can be defined as the ability to access any or all the information concerning a product which is under consideration throughout its entire life cycle by means of recorded identifications [1]. The growing number of normative and qualitative constraints to manufacturing factories, and customer requirements for high-quality products often lead to the verification of traceability data in order to determine the origin of the defects. Therefore, maintaining detailed, up-to-date and well-stored traceability data is a key strategy for manufacturing factories in order to accelerate product defect verification, and determine the causes. Moreover, manufacturing companies may be compelled to reveal confidential data to investigators in order to prove their point of view regarding the cause of the defects. To be completely convincing, this point of view should rely on data which were transparently exposed to the partners through the traceability system at the moment when the product's manufacturing occurred. Therefore, an effective way of including confidential data into traceability processes without compromising industrial secrets is required.

In this paper, we propose an approach which uses the blockchain technology in order to store traceability data, which are monitored and validated by the manufacturing company's partners with full transparency. However, so as to preserve confidentiality, the confidential data involved are not directly inserted into the blockchain, but only the derived information allowing to prove the unicity, integrity and authenticity of the actual confidential data to the investigators in case of litigation. Instead of a complete Industry 4.0 traceability model, the proposed approach focuses on a product-centred traceability regarding the interactions occuring inside the factory perimeter only, which is enough to demonstrate both confidentiality-preserving and transparency properties. The presentation of this paper is organized as follows: section 2 introduces the related work and points out the main issues addressed in our contribution; section 3 presents our approach to product-centred traceability and how it can achieve both transparency and confidentiality using a blockchain. An implementation of the proposed approach with the Multichain platform is presented as the main result in section 4, along with some discussions regarding performance indicators in section 5, before the conclusion.

2 Related work

2.1 On general aspects regarding traceability

A description of the three major components of a traceability system is proposed by [2]: identifying Traceable Resource Units (TRUs), documenting transformations and connections between TRUs, and recording TRUs

attributes. A TRU can be a trade unit (case, bag, box...), or a logistic unit (pallet) or a production unit (lot, batch). Multiple aspects of traceability data are highlighted in [1], such as their heterogeneous nature or the challenges related to interoperability and integration. Regulation and requirement aspects are also mandatory, since they actually drive traceability policies. All these aspects are taken into account in [1], in which the authors proposed an ontology-based modelling description of an intelligent traceability system. In order to evaluate the suggested model, they proposed a cloud-based application whose description focuses on the system's accuracy and benefits. Another notable work [3] introduces the concept of Smart Manufacturing Objects (SMOs) in a traceability platform in order to achieve real-time production within a smart factory. A combination of technologies such as the Internet of Things (IoT)[4], Radio Frequency Identification (RFID) and laser-scanner, helps converting any resource into a SMO. In this way, production operations and behaviour can be monitored in real-time, thus allowing a detailed and up-to-date traceability. A review of the benefits of traceability regarding supply chain resilience is proposed in [5], while a global cyber security analysis of traceability in supply chain is reported in [6]. Most of these works consider confidentialiy regarding data disclosure, which leads to solutions which mainly focus on confidential data protection, thus removing them from the traceability data exchanged between the partners. In this work, we consider that confidential data must be included, in an appropriate way which is still to be defined, in the traceability data exchanged when they can contribute to accelerate retrospective investigations.

2.2 On product-centred approaches

A product is a set of attributes, called characteristics, compounded in an identifiable way [7]. Those characteristics determine the value which is produced. Product traceability is defined by ISO 8402 as "the ability to access the history, the use or location of an article or an activity, or similar articles or activities by means of recorded identification" [8]. In manufacturing, it comes down to the recording of the specific movements and modifications of a product throughout its life cycle in the supply chain. A product-driven ontology developed in [9] proposes a methodology which formalizes the technical concepts and data embedded into the product itself, thus favouring interoperability with other applications. The conceptualization of the information model is based on standards such as ISO 10303 and IEC 62264. Another recent work [10] can contribute significantly to these efforts, through the elaborated product design lifecycle information model that they propose. More specifically, product traceability landscape can be heterogeneous, and thereby requires multiple technologies (QR Code, barcode, RFID) which make traceability integration very complex. In this context, a systematic approach for product traceability was designed by [8], with insights into the ceramic industry. This approach combines several technologies at different stages of a product

cycle, and supports traceability integration at the different levels required by Industry 4.0.

The methodological approach in [7] is proposed in order to characterize the products, the requirements, and the players involved in a traceability system by using a blockchain-based approach. In order to trace the spare parts aggregated in a manufactured product, [11] presents a blockchain-based approach which addresses some traditional issues faced by a supply chain management, such as transparency and active monitoring of the operations which affect the conformity and safety of spare parts' components. Due to its immutable feature, the blockchain technology cannot only help identifying defective or counterfeit parts, but also determine the assets' origin in the traceability context. The system proposed in [11] includes a decentralized storage of files based on the InterPlanetary File System (IPFS) for spare parts' data, smart contracts algorithms, security and cost analysis. An evaluation is proposed in order to demonstrate the reliability of the spare parts ownership tracking solution. However, this solution focuses only on the interactions inside a single company. Therefore, the challenges related to maintaining confidentiality of critical data as well as transparency in an interoperability context with external partners were not addressed.

Another example of blockchain-based product traceability is proposed by [12] for additive manufacturing. The objective announced was to ensure secure and reliable traceability, as well as accessibility and immutability. The proposed architecture uses Ethereum smart contracts and IPFS as a distributed file storage solution. The authors propose an evaluation focusing on security requirements such as integrity, accountability, non-repudiation and authorization. However, the questions related to the management of critical data, transparency and trust between stakeholders are not mentioned in the study. Yet, the cost introduced by the use of IPFS as a storage solution complementary to the blockchain is not analysed. About the evaluations, a survey on blockchain solutions for sustainable manufacturing and product lifecycle management empowerment is proposed in [13]. Various metrics related to the trust in using blockchain solutions in manufacturing are introduced, regarding transparency, decentralized decision, reputation, and customer relationship. From the manufacturing perspective, blockchain could be used as an enabler to drive already existing systems for workshops, such as Enterprise Resource Planning (ERP) and Manufacturing Execution System (MES).

From the product management perspective, the blockchain could offer a unified database to share product information. The fact that new proposals are still presented in various manufacturing sectors [14], including textile [15], emphasizes the importance of practical blockchain solutions to traceability in Industry 4.0. Indeed, other technical challenges such as satisfying privacy protection needs, energy consumption and storage scalability issues are among the primary problems which prevent manufacturers from rising their blockchain solutions beyond proofs-of-concept [16]. They are still pointed out in a very recent work [17], and will be part of the issues investigated in this paper.

2.3 On security, storage and transparency aspects

Traceability is not just about recording data. Other aspects are involved in traceability, such as ensuring confidentiality and efficient storage, and also transparency to other supply chain players. Besides security concerns[18], several papers in the literature investigated the use of the blockchain technology to address these aspects [17]. Blockchain is defined as a distributed ledger of the digital events or transactions executed between different parties, and that can be verified at any time in the future. For instance, [19] presents a list of blockchain solutions to traceability problems, essentially related to individual activity coordination, decentralized validation, and transaction legitimacy and preservation. By providing transparency and immutability, the blockchain paradigm offers a unique level of credibility for all stakeholders, and contributes to strengthen the relationship with the customers, and attract new ones.

Security and safety are other challenges mentioned, but not actually addressed in that work. In order to provide deep insights into this technology, [20] proposes a review about the implementation of blockchain-based solutions to various applications in which security remains paramount. It outlines the way the blockchain technology could solve the issues faced by traditional systems regarding transparency, centralization, scalability, trust, and security. The way a blockchain can be used to support smart manufacturing is also discussed in [21]. The authors propose a middleware which enables secure, trustable, traceable and reliable applications. The blockchain-secured smart manufacturing system presented by [22] uses blockchain to address some common issues in manufacturing systems, such as operation traceability, confidentiality and trust. Moreover, it also allows to avoid the failure of key nodes which could occur in centralized platforms. This system is based on the international standard ISA95 (www.isa.org), widely referenced in industry 4.0 regarding information technologies. The paper also introduces some metrics related to the use of blockchain in manufacturing, namely data provenance transparency, system flexibility, system sustainability and cost savings [23]. Privacy protection is only mentioned as a future research direction for blockchain in manufacturing.

In order to investigate the accuracy of the blockchain technology for real-time transparency and cost savings in the manufacturing industry, [23] proposes a comparison of the profits made by two manufacturing firms. Several aspects are considered in this study, notably blockchain start-up costs which are often ignored, and some other limitations related to this technology. These implementation cost and profit issues are also examined by [24] in their supply chain game composed of two firms, namely a supplier and a retailer, using blockchain and smart contracts. The studied aspects include business risks, transaction costs and stochastic cases in which blockchain deployment is not worth it. Another proposal from[25] was a three-level blockchain architecture for cyber-physical systems (CPS) to tackle the challenges associated with 5C-CPS structure implementation. In terms of security and storage, the

architecture tries to achieve integrity, fault-tolerance, resiliency, privacy and transparency.

With the advent of Industry 4.0, new manufacturing paradigms have emerged, such as cloud manufacturing. However they still suffer from some issues related to centralized industrial networks. Therefore, a blockchain-based peer-to-peer (P2P) network architecture was presented by [26]. The main objectives of this architecture were to secure data sharing, and improve cloud manufacturing reliability and flexibility. Ensuring data trustworthiness is a key issue to leverage big data analytics for supply chain efficiency. Thus, [27] highlights that it is essential to determine whether the collected information from sensors are valid or not. In order to address this issue, a combination of UAV (Unmanned Aerial Vehicles) and blockchain-based system is presented to handle inventory and traceability applications in big data driven supply chain management. However, though the blockchain technology is promising, the public disclosure of any transaction is considered as a security risk by most organisations [6].

A confidentiality-preserving blockchain-based system presented in [28] for transaction processing systems provides those issues with a few solutions. The main idea consists in finding a trade-off between the benefit of information sharing (transparency), and the cost associated to confidentiality weakening. Confidentiality preservation in the blockchain refers to the fact that only authorized parties can access sensitive or proprietary transaction data. The proposed system is based on homomorphic encryption, and a recent innovation called zero-knowledge proofs. We follow the same objectives, while avoiding zero-knowledge proofs which introduce higher processing costs and may not be practical for a wide range of data types involved in manufacturing processes.

3 A blockchain-based product-centred approach to traceability

The novelty and main contributions of this work are summarized as follows :

1. First, this work refers to the most general case, where the traceability system is accessible to all the third-parties involved in the manufacturing factory processes. Therefore, the blockchain based architecture is designed to include all of them. The only limitation is that anonymous nodes cannot join the blockchain network, which leads to the choice of a permissioned blockchain. Therefore, this proposal apply to most of the manufacturing factories seeking a blockchain solution for their traceability system.
2. Then, We consider that any data necessary to post-production investigations must be included in the traceability data, at least in an appropriate way for each of them. The proposed architecture offers a practical solution regarding confidential data, thus opening the road to the solution of the privacy/transparency challenge related to blockchain in Industry 4.0 [17].
3. Finally, practical issues such as those regarding data volume, energy consumption and additional costs related to blockchain deployment, are

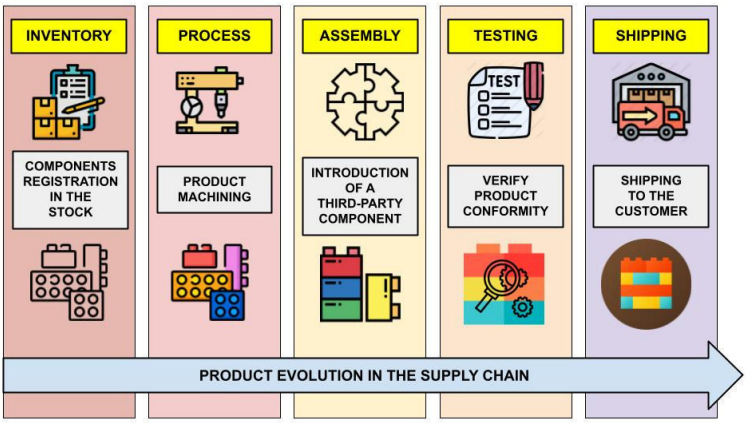

Fig. 1 Evolution of a manufactured product inside the supply chain

investigated concretely. We show that appropriate and justified choices performed case by case can lead to a situation where the blockchain is more a solution than a problem.

3.1 Overview of a product-centred approach to traceability

With the advent of Industry 4.0, the concept of traceability also includes a strategic purpose which goes beyond the mere identification of both the products and their location inside the factory. For instance, the concept of intelligent traceability ensures product monitoring alongside its tracing and tracking in order to enhance product quality and safety [1]. The importance of product traceability is emphasized in the quality management standard ISO 9001:2015 [8]. Different technologies and types of information are involved in the different phases of a product lifecycle, namely development, production, use and disposal. In this work, our approach focuses on the traceability of a product manufactured in a supply chain, which may include some components provided by external entities such as suppliers. A similar approach was adopted in [11] regarding the integration of different spare parts which compose a car engine. A more complete approach has been proposed recently in [10]. Our approach focuses on the product traceability all along the manufacturing process instead, and the integration of spare components is just one of the steps. Figure 1 illustrates a typical evolution of a manufactured product in the supply chain. This evolution considers five main steps, detailed as follows:

- **Inventory** when the different components of the product are recorded in stocks. At this stage, traceability data can be the components' reference number, serial numbers or any other information which could help track the products and components.

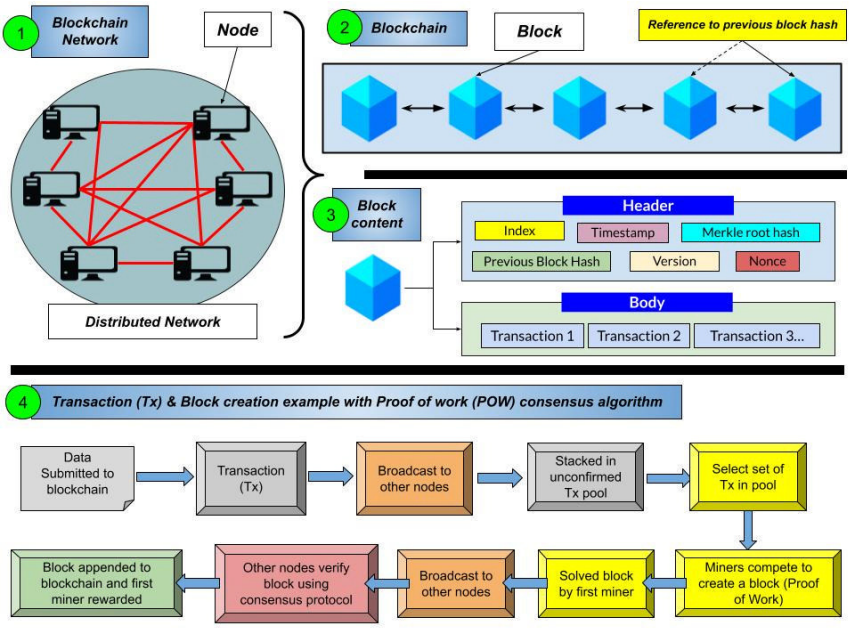

Fig. 2 Blockchain basics and main concepts overview

- **Process** when the product enters the supply chain, where it can be transformed multiple times through multiple substeps. Process and machine parameters are examples of traceability data generated at this stage, and which confidentiality can be critical.
- **Assembly** when a component manufactured by a third-party member is integrated into the product. Technical information about the component and the way it was used during the manufacturing process constitute the traceability data at this stage. They may be critical for post-assembly audit. A detailed work on assembly system in Industry 4.0 era is proposed in [29].
- **Testing** when the product's conformity is checked. Traceability data can be any information resulting from the tests (context, measures, etc.), which could help establish product conformity.
- **Shipping** when the product is ready to be sold and shipped to a customer. Examples of traceability data are : batch numbers, shipping numbers, or serial numbers so as to be able to trace the product back after it left the factory.

3.2 Blockchain basics and application to traceability

This section presents the fundamental principles of blockchain, and how they could be applied to traceability.

3.2.1 Blockchain basics

So as to better understand the blockchain basics, Fig.2 is proposed as a support for the following definitions.

Blockchain network

A network formed by the computers running the block-chain. Each member of the network is called a node. This network is also referred to as a distributed network or a Peer-To-Peer (P2P) network.

Blockchain

The distributed ledger consisting of a growing chain of blocks linked and secured using cryptographic tools. The idea of block connections by cryptographic chains was introduced by Haber and Stornetta in 1991 [20]. Every block in the chain contains the hash of the previous block, thus preventing any data modification and leading to immutability [12]. Thanks to this fundamental feature, a block cannot be altered retroactively without altering the subsequent blocks, thus revealing the manipulation attempt.

Block

The block is the main component of a blockchain. Its structure is divided into two parts : the header and the body. The header contains the index (position in the blockchain), the block timestamp in order to make existence-proof reliable[13], the Merkle root hash (hash of all transactions in the body by using a Merkle tree), the hash of the previous block which forms the relation between blocks, the protocol version used by the blockchain network, and the nonce which is the solution to the consensus algorithm when adding a new block to the chain. The body contains a list of transactions.

Transaction

The transaction represents the data submitted to the blockchain. They are stored in the blocks. A block can contain several transactions whose number depends on a limit defined by the maximum block size. When a user submits data to the blockchain, the latter generates a transaction and a transaction hash, which identifies this transaction in the blockchain uniquely.

Consensus Algorithm

As a distributed network, the blockchain does not have any central authority which could ensure a single version of the blockchain, a single truth. The consensus algorithm precisely allows reliability and trust between the peers in the blockchain network. Trust is built by using asymmetric cryptography, which allows the users to deal confidently with the other participants. It consists of several specific objectives, such as coming to an agreement, mandatory participation of every node in the consensus process, etc. Various consensus

algorithms exist, one of the most famous being the Proof Of Work used in the bitcoin blockchain [30].

Proof of Work (POW)

An example of consensus algorithm which is used to select a miner for the next block generation. The central idea is for nodes to compete in order to solve a complex mathematical puzzle. The solving process requires a lot of computational power. However, verifying the solution must be easy for the other nodes in order to reduce both processing time and additional energy consumption. The first node which solves the puzzle submits its solution to the network, and the other nodes verify it. If the solution is valid, the first miner gets a reward (for example, money in bitcoin blockchain). This reward aims at encouraging to follow the rules, as there is no gain in breaking them instead. Proof of Work also contributes in security reinforcement since because it makes it difficult to alter the data in the blockchain. Indeed, any alteration of any block would imply mining all subsequent blocks again, which would require a huge amount of computational power.

Blockchain transactions can be made irreversible and traceable by integrating the blockchain to smart contracts, thus forming a protocol, or more precisely a self-executing code which allows the performance of transactions in absence of a third party. It was first designed in order to avoid data tampering by using timestamps. Then, Bayer, Haber and Stornetta introduced transaction verification and validation by using the Merkle tree. In practice, a blockchain combines the chain data structure, consensus algorithms, cryptography techniques and automated smart contracts. The first blockchain network initialized in 2008 by Satoshi Nakamoto [30], used a hash function to create blocks in the chain, so that clients' or users' signatures were no longer necessary. This implementation gave birth to the cryptocurrency network called Bitcoin[20]. Then, smart contracts were introduced in 2010, leading to the development of Ethereum and Hyperledger. In 2015, the convergence with decentralized applications started, and multiple research areas were considered (IoT, supply chain, etc.). Since 2018, various services and databases have been evolving towards real-time, with the integration of Industry 4.0 applications.

3.2.2 Blockchain application to traceability

Several work on blockchain application to traceability have already been mentioned in section 2.3. The blockchain technology is mainly known for its immutability and transparency, thus making it an accurate solution to address traceability challenges in Industry 4.0 [24]. However, those features alone are not enough to address all the concerns related to traceability. Instead, in our work, immutability will be used as a central feature around which other concepts gravitate to increase their strentgh. Our blockchain approach aims at ensuring trust among the participating stakeholders, and at providing tremendous advantages for product traceability regarding the following additional aspects:

Security

In manufacturing, traceability data are associated with privacy concerns, so it is important to maintain this privacy in our approach. Moreover, a factory needs to master the validation process of the blockchain participants who access its traceability system. Contrary to traditional public blockchain solutions in which participants may almost be anonymous, a permissioned blockchain such as the one used in this work, only allows a given number of authorized users to access and use the blockchain.

Transparency

In a blockchain, each transaction validated generates a transaction hash which can be reviewed by any participant. This allows verifying that a specific action was performed in the blockchain at a given moment.

Integrity

Integrity implies maintaining data consistency, accuracy and trustworthiness along their entire lifecycle. To ensure integrity, the traceability data are hashed, and the hash is stored inside the blockchain. Since the blockchain is tamper-proof, the hash can be considered as tamper-proof by extension. Integrity verification consists in computing the hash of the data, and comparing it with the original hash stored in the blockchain.

Confidentiality

Transparency does not mean that every information should be disclosed publicly. Indeed, traceability data may contain some private information related to the manufacturing process. Consequently, we consider that confidential data must be managed appropriately, for example by being encrypted prior to their insertion into the blockchain, or by inserting into the latter only some data derived from the confidential data, instead of the confidential data themselves. However, the data hash inserted into the blockchain regarding confidential data must be computed from the original data before encryption or any other operation. Indeed, the authenticity and integrity will have to be verified regarding the actual data. In this way, it will be possible to ensure both confidentiality (through data encryption) and transparency (through derived data and original data hash). When derived data is preferred to encryption, the protocol producing these derived data must be exposed in full transparency, and it must ensure that the original data cannot be retrieved from derived data. The protocols proposed in zero-knowledge approaches offer such guarantees. However, these approaches are complex and may not be practical in the context of manufacturing factory traceability due to the amount of data, and the fact that these latter are produced in real-time along with the product manufacturing.

Non-repudiation

It ensures that a participant cannot deny any of its actions regarding data and transactions in the blockchain. Since the participants are authenticated in a

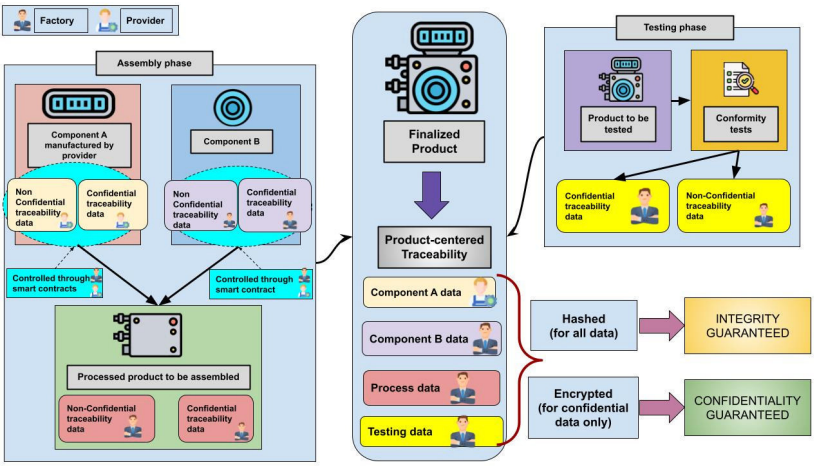

Fig. 3 Conceptual view of product-centred approach to traceability

permissioned blockchain, specific mechanisms should be introduced in order to verify and keep a track of data and transaction validation. Such a mechanism could be the use of digital signatures. Indeed, the latter offers the ability to sign the data with a private key, and the signature can be verified by anyone using the corresponding public key.

Fig.3 depicts an application of our approach to product-centred traceability. Two traceability stages are represented. During the assembly phase, two components are added to a compound product, where component A has been manufactured by a provider, while component B has been made inside the factory. During the testing phase, conformity tests are executed by the factory, and produce confidential data. In the middle of the figure, there is the finalized product which aggregates all its traceability data with different privacy concerns (confidential or not) and different participants (provider or factory). All of these data will be hashed in order to guarantee their integrity later in the blockchain. However, only confidential data will be encrypted (or derived).

Fig.4 proposes an overview of blockchain application to traceability in our approach. Firstly, traceability data are generated during the different phases of the proposed product-centred traceability approach implying different actors (customer, provider... etc.). Secondly, a processing layer validates, formats and aggregates the data in order to increase their value, and make their exploitation easier by the users. During this phase, the data are hashed to guarantee integrity, and encrypted to guarantee confidentiality. Once this stage has been completed, the data are submitted as transactions to the validator node, which represents the factory as well as any other member of the private blockchain.

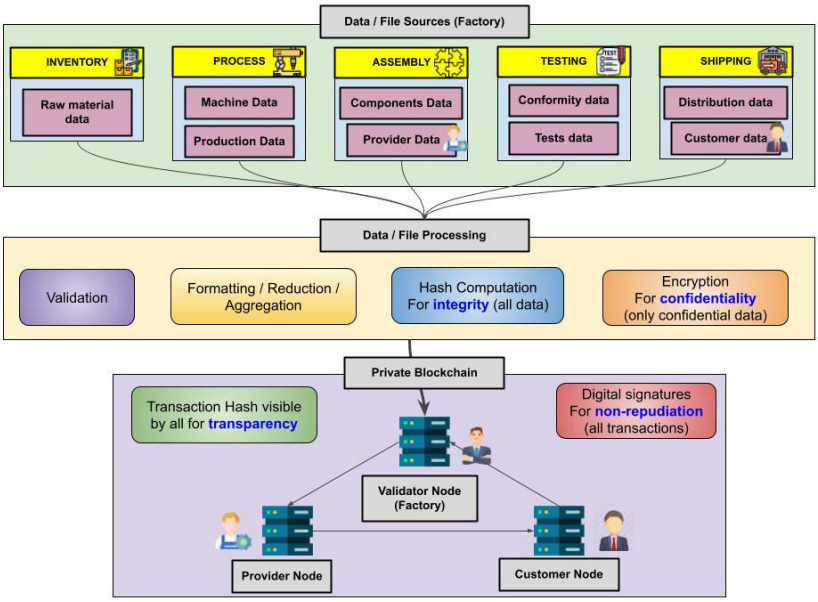

Fig. 4 Blockchain application to traceability overview

3.3 A Blockchain-based Product-Centred Architecture for Traceability

This section describes our Blockchain-based Product-centred Confidentiality-preserving Architecture for Traceability (BPCAT), and the concepts involved.

3.3.1 Architecture overview

BPCAT is an architecture covering two aspects : the product's traceability and its integration into the blockchain. This global architecture is depicted in figure 5, which will be described from top to bottom. Three blockchain nodes represent the types of players or participants, namely the validator (the company owning the traceability data), a customer (retailer, final user, etc.) and a provider (components provider, supplier, etc.) involved in the product's traceability. These nodes together form the blockchain network which can be controlled remotely by a node called the manager node. The latter aims at giving more control to the factory owner (or a designated operator).

In this blockchain network, a blockchain runs with a copy stored on every node. The product traceability data saved into the blockchain can be classified into multiple categories: mono-partner data which are only related to the manufacturing factory such as product machining data (see fig.1), third-party component integration data which involve the provider; and billing and shipping data which involve the customer. Some of these data can be confidential, and will require specific treatment, as detailed in the following sections.

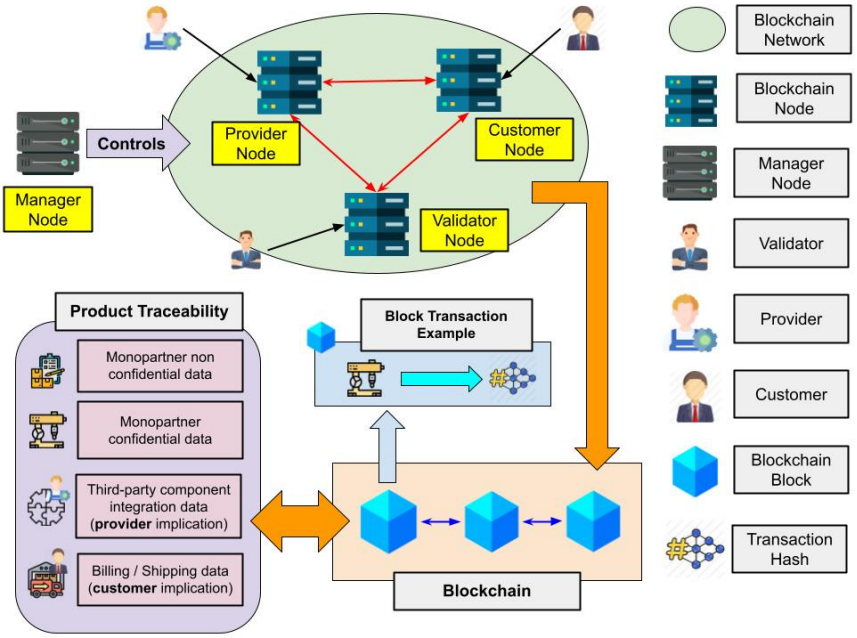

Fig. 5 BPCAT Architecture Overview

3.3.2 Data structure in the blockchain

In the blockchain, each time a new traceability piece of data is added to a block, a transaction is created. BPCAT has some prerequisites about how data should be structured (see fig.6). A typical blockchain transaction always includes a transaction hash and a timestamp so as to guarantee that an action was performed at a specific time in the blockchain. As mentioned in section 3.2.2, the transaction hash does not guarantee data integrity. For this reason, BPCAT also adds the data hash into the transaction. With the data hash, timestamp and transaction hash, both transaction transparency and data integrity can be guaranteed to the provider and the customer.

3.3.3 Confidential data management

Confidential traceability data refer to the data the factory owner does not want to reveal to all the blockchain participants, but that must be included anyhow in traceability data because they could be necessary as proofs during retrospective investigations. Indeed, in order to avoid a conflict with the transparency usually expected from a blockchain solution, BPCAT manages confidential data as follows (fig. 7):

- confidential data are encrypted using an encryption method chosen by the data owner in order to guarantee confidentiality;
- so as to guarantee transparency, BPCAT suggests that any encrypted data in a transaction should go with a linked information which could assess its

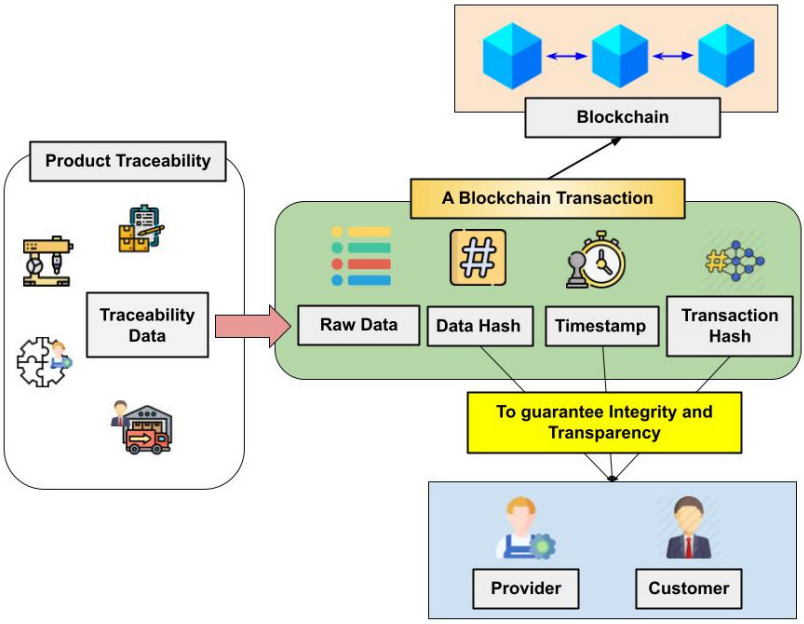

Fig. 6 BPCAT Data Structure Overview

authenticity and integrity when needed. The hash of the original data before encryption, or the hash of a piece of data derived from the original data in a predefined way, may be used to that end. All these data are inserted into the transaction, and both the timestamp and the transaction hash guarantee the authenticity and integrity of the entire transaction.

- in case of litigation, a participant can request decryption of the data so that it could be compared to the hash stored along with it in the blockchain, and thus establish its authenticity.

Figure 7 shows that encrypted data can only be decrypted by the owner (here the validator) in order to maintain confidentiality. However, both the provider and the customer have access to the original data hash, timestamp and transaction hash, which guarantees integrity, authenticity and transparency.

3.3.4 File management

In order to tackle traceability data volumetric problem which could require resorting to a cloud storage solution, BPCAT file management policy does not impose the storage of the files inside the blockchain. Each blockchain participant can use an external storage solution (see Fig.8). However, both the file hash and the file path are stored into the blockchain; the first one in order to guarantee file integrity and authenticity, and the other to retrieve the file easily. In this way, any of the players can resort to a Cloud storage if necessary.

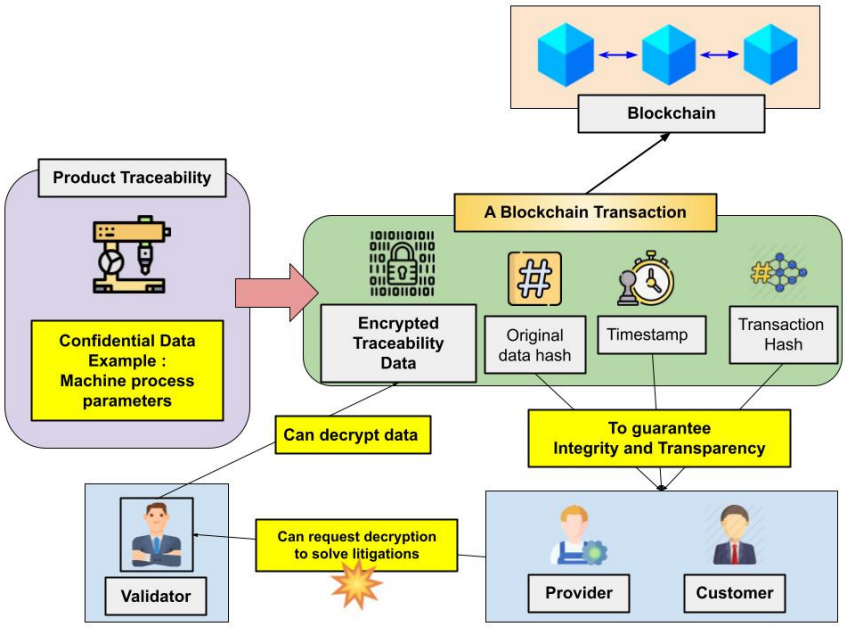

Fig. 7 Confidential Data management in BPCAT

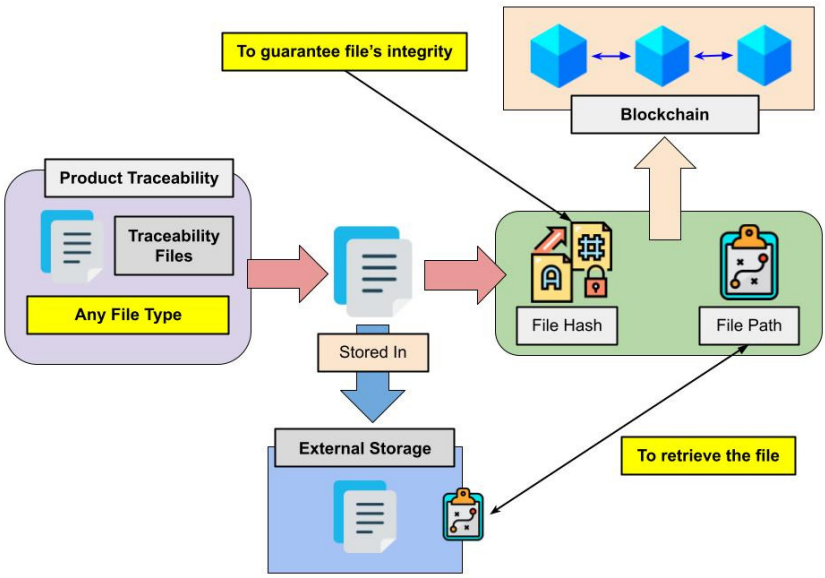

Fig. 8 File Management in BPCAT

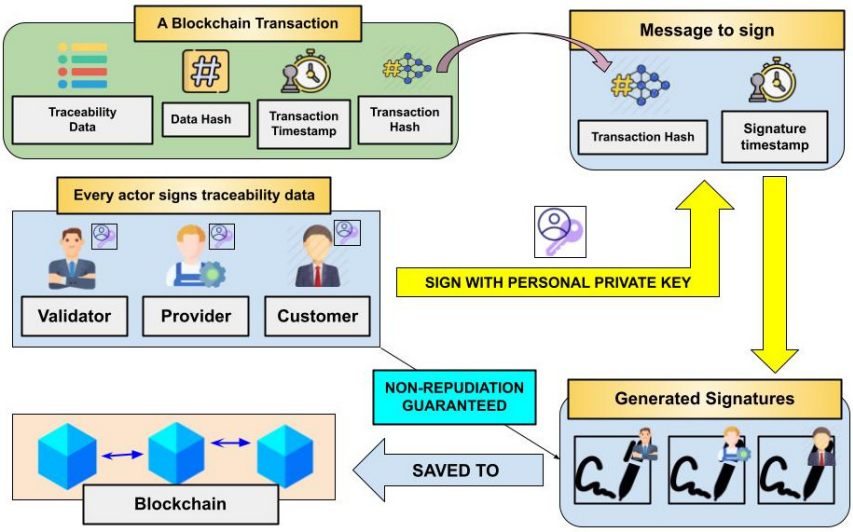

Fig. 9 Data signature and non-repudiation in BPCAT

3.3.5 Data signature and non-repudiation

Regarding traceability, it can be useful to solve litigations where the responsibility of one player is questioned. To that end, digital signatures can be used in the blockchain as depicted in figure 9. For every blockchain transaction involving traceability data, every player (validator, customer, provider) involved in the related product manufacturing stage must sign the transaction. Using their personal private key, each stakeholder signs a message containing the transaction hash and a timestamp in order to authenticate the signature. Then, once the digital signature has been computed, it is saved to the blockchain. Non-repudiation is guaranteed thanks to all the signatures, which can be verified by anyone using the signing player's public key.

3.3.6 Security, confidentiality, transparency and non-repudiation

This section summarizes the techniques used by BPCAT in order to strengthen trust among partners regarding product traceability. Trust can be considered as the sum of security, confidentiality, transparency and non-repudiation, which are the benefits provided by blockchain technology. Fig.10 illustrates the different techniques used in BPCAT to achieve this objective.

Regarding security, every blockchain participant has its own node with a dedicated address and private key in order to be clearly authenticated. A permissioned blockchain is used to perform access control to the blockchain, and other specific actions. For manufacturing companies, distributed systems such as blockchain can be difficult to maintain due to a lack of control. For that reason, BPCAT suggests to add a manager node so as to improve control.

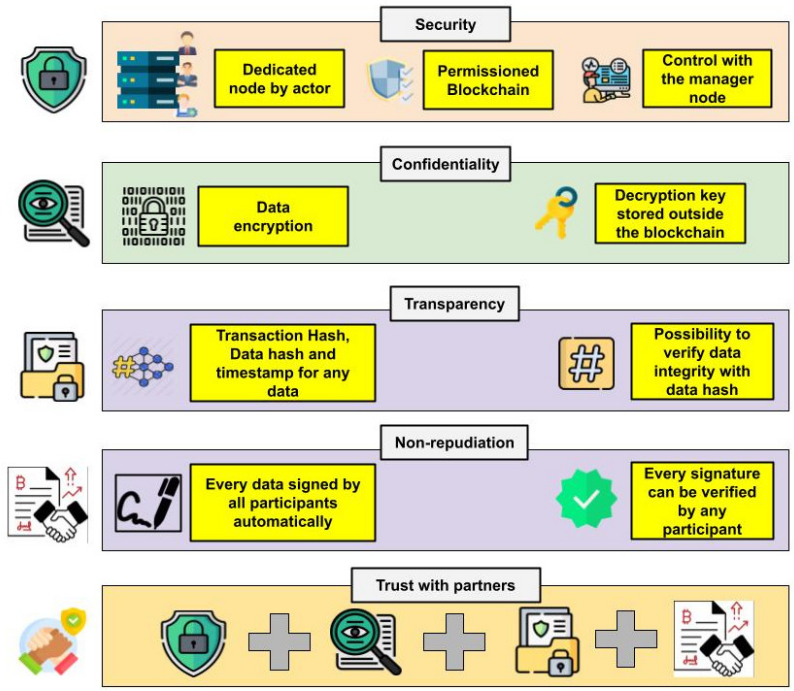

Fig. 10 Overview of security, confidentiality, transparency and non-repudiation in BPCAT

About confidentiality, the traceability data which are considered as private must be encrypted. The private key used to encrypt these data must be stored outside the blockchain in order to make sure that confidentiality does not entirely rely on the blockchain.

As for transparency, every transaction with traceability data includes the transaction hash, a timestamp, as well as the data hash, so as to guarantee data integrity. Thus, in case of litigation, it is possible to recompute the hash of any involved data, and to compare it with the hash stored in the blockchain.

Concerning non-repudiation, every transaction involving traceability data is signed by all the participants involved in the related manufacturing stage, using their private key to generate the signature. This process is performed automatically, and includes the transaction hash, a timestamp, and the participant's private key. This signature can be verified by any participant, which makes the authorship/validity of any traceability data impossible to dispute.

4 Implementation of our proposal with Multichain

In order to evaluate the feasibility of the proposed BPCAT, a prototype has been developed using the Multichain platform (https://www.multichain.com). It is an open-source platform mainly designed to build blockchain applications

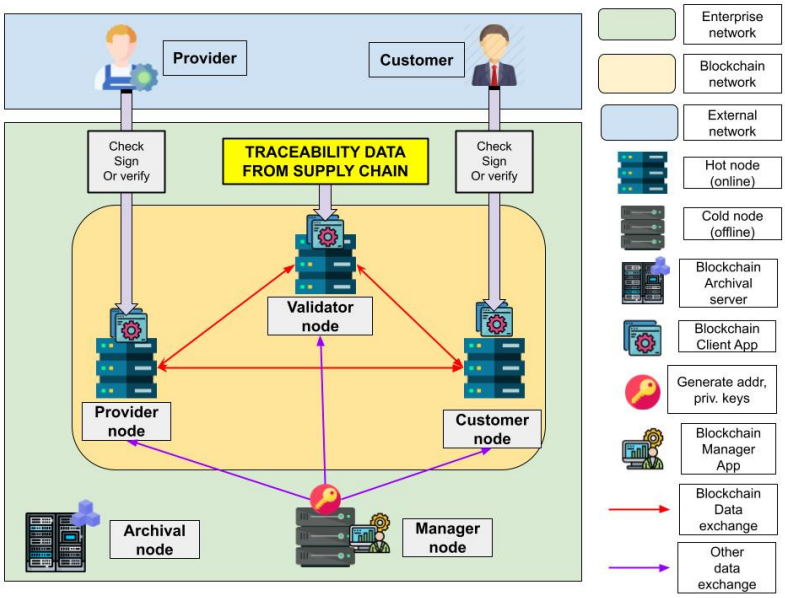

Fig. 11 Network architecture in BPCAT implementation

for companies in the context of a private or permissioned blockchain. The main advantages of this platform are the full control over every aspect of the blockchain (permission management, consensus algorithms, data storage...), the possibility to create multiple blockchains, and its ease of use for developers.

4.1 Network and actors

In Multichain, blockchain participants are called "nodes", and the blockchain network is made of connections between these nodes. In BPCAT, the nodes are like the players' avatars in the traceability system. The proposed implementation includes a total of five nodes:

- Validator: Avatar of the factory owning the traceability data;
- Customer: The customer's avatar;
- Provider: The provider's avatar;
- Manager: Node controlling the blockchain and the other nodes;
- Archival: Node storing old blockchains, and allowing their exploration.

Fig.11 is a representation of the network architecture including the interactions between the blockchain participants. Three networks are considered: the blockchain network formed by the blockchain nodes, the company network in which traceability data are generated and submitted to the blockchain, and the external network which is an abstraction of all the interactions with the entities outside the factory.

Hot nodes (validator, customer, provider) constitute the blockchain network and are connected to one another. As the main node, the Validator will

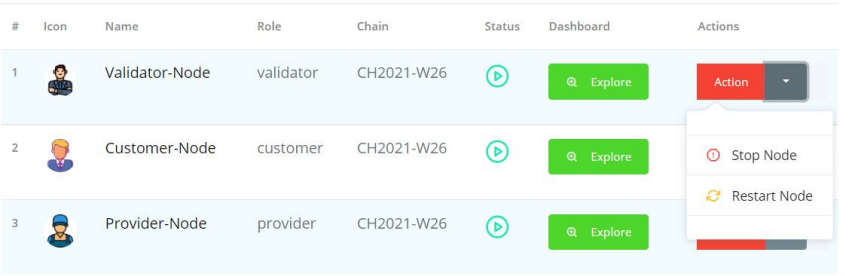

Fig. 12 Blockchain nodes overview in BPCAT implementation with Multichain

represent the manufacturing factory, and will publish the traceability data. The Customer and Provider nodes will be the entry points for transparency. Indeed, they will make it possible for the customer and provider to access traceability data.

Contrary to the previous nodes, the Manager node refers to a Multichain cold node: it is an isolated node which is not connected to the blockchain. From the blockchain's point of view, this node does not actually "exist". Its role consists in controlling the other hot nodes remotely, and therefore the running blockchain. The reason for its existence is to address one of the main issues often mentioned by companies about blockchain, basically: "blockchain is not easily manageable due to its decentralized characteristic". The remote control consists in starting and stopping other nodes, or more globally starting a new blockchain. Moreover, it is also responsible for the generation of other nodes' addresses, private/public keys for data encryption, decryption and signature. An external Public Key Infrastructure (PKI) chosen by every partners could ensure some of these features.

The Archival node is dedicated to the storage of old blockchains and gives the possibility to explore them later. Fig.12 shows the three blockchain nodes and how they are monitored from the Manager node in Multichain.

Finally, it should be noticed that due to the specific composition of the blockchain nodes, which gathers the factory and its partners, the consenus can be simplified in order to avoid useless energy consumption. The nodes are authenticated and the mining node for each transaction can be clearly identified through business processes and related smart contracts.

4.2 Chain and storage management

As mentioned previously, Multichain provides an easy way to create and start new blockchains. In BPCAT, this feature is used as a way to prevent another drawback of the blockchain technology for Industry 4.0 factories, namely its "constantly-growing" characteristic. For instance, we suggest a time criterion which would determine how long a specific blockchain should run before stopping it and starting a new one. In doing so: the size of the blockchains would be stable, and both data volumetry and storage cost would be easy to estimate and anticipate. Then, keeping the history of the old chains would be

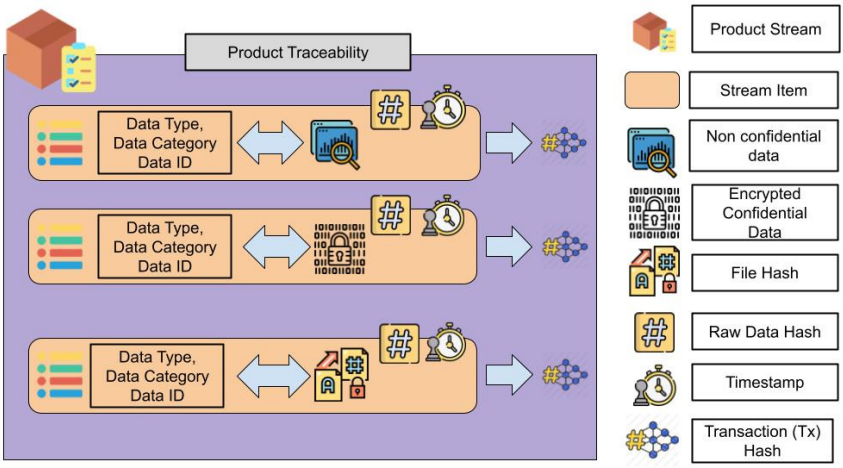

Fig. 13 Overview of traceability data in BPCAT implementation

handled by the Archival node, and data retention would consist in deleting the blockchains whose age exceeds a certain number of years according to the factory's traceability policy.

4.3 Product data storage

In order to manage and store the data, Multichain proposes an abstraction of blockchain mechanisms dedicated to data storage and management, which are called "streams". They are a kind of data container working like key stores. Each data is called an item, and an item is a key-value couple in which each key is used to index and retrieve a specific item. An item can have multiple keys, and the same key can be used multiple times. Fig.13 offers an overview of the way traceability data are organized into the implementation, and the different data types encountered. They will be detailed in the upcoming sections.

In BPCAT implementation, we use one stream per product in which the stream's name could be the product's serial number or any other unique attribute. Every product traceability piece of data is packaged as an item whose keys are its type or category. For every piece of data, the data hash is stored so that data integrity and authenticity can be verified.

4.4 Confidentiality

In our approach, we consider that the data can be divided into two categories: confidential and non-confidential data. To manage this difference, confidential data must be encrypted before their insertion into the blockchain. Figure 14 describes the way data confidentiality is preserved. In the BPCAT implementation, a hybrid encryption using symmetric encryption (AES 128) and asymmetric encryption (RSA 2048) is used. First, data are encrypted using

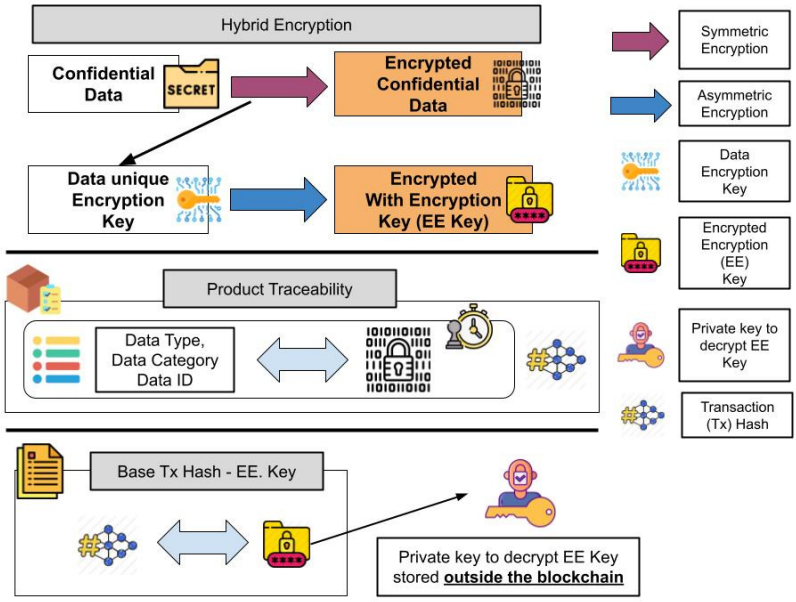

Fig. 14 Management of data confidentiality in BPCAT implementation

a unique random encryption key generated by the symmetric encryption system. Then, this encryption key is encrypted with the asymmetric encryption to produce what is called an Encrypted Encryption key (EE key). The EE key can only be decrypted by those who possess the related private key. The EE key is stored in a dedicated stream as a "Tx Hash-EE key" base, where "Tx Hash" is the transaction hash produced when the related encrypted data were stored into the blockchain. Thus, decrypting data consists in getting the EE key back from the transaction hash, decrypting it with the asymmetric private key, and decrypting the data with the decrypted key.

4.5 File management

Product traceability data can take various forms, including that of a file. In BPCAT, the files are not directly stored into the blockchain. Indeed, the company is free to choose a storage method which best meets its needs. Fig.15 describes the way traceability files are managed, and how they are interconnected to the traceability data described in the previous section. In the BPCAT implementation with Multichain, the file information is stored in a dedicated stream. This stream contains items which are "file hash-file path" couples. Finally, to reference the file in the product traceability, the file hash is used. Every file is associated with a type for filtering purposes.

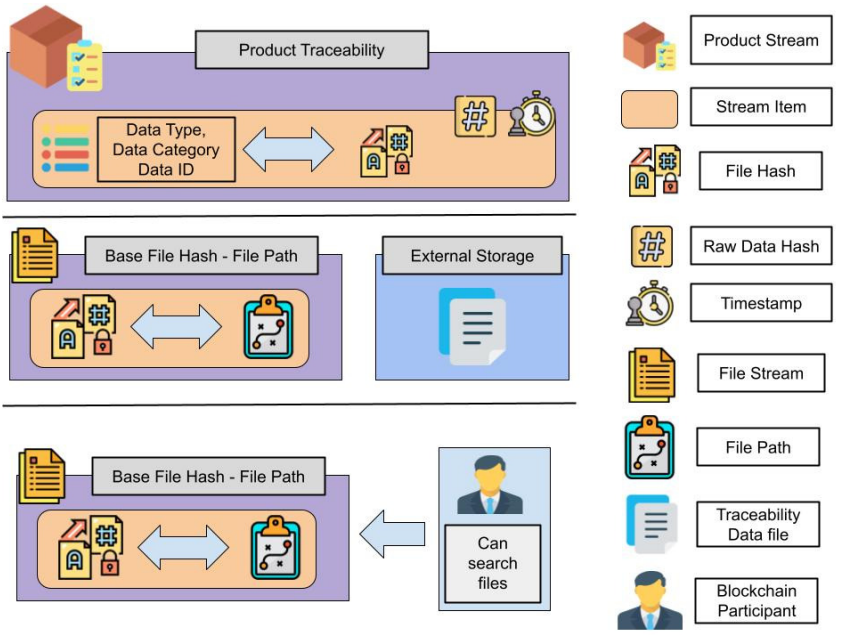

Fig. 15 Traceability file management in BPCAT implementation

4.6 Data signature

Multichain offers the possibility for a blockchain participant to sign data, and also the ability to verify a signature validity. In our approach, the signature represents the approval of a piece of data by a blockchain player which is different from the one who published it. Fig.16 shows how signatures are stored in Multichain, and how they can be made secure and reliable.

Signatures are stored in a dedicated stream, where every item is a "Tx Hash-Signature data" couple with "Tx-Hash" as the transaction hash of the data about to be signed, and "Signature data" is a combination of multiple information used to generate the signature. In order to keep the process secure, and to guarantee that all the signatures are unique, the signature generation is based on multiple parameters, which are the timestamp, the "Tx hash" of the data to sign, and the address of the involved node. To make sure that only valid signatures are added to the blockchain, a stream filter allows to verify the signature before adding it. This allows to keep trustworthiness in both the core blockchain and the blockchain client application. Fig.17 illustrates the way data are signed in the BPCAT implementation with Multichain.

4.7 Verifying data integrity

For every traceability data, the raw data hash is also stored. Therefore, it is possible to guarantee data integrity from the moment they were added to the blockchain, and any time they are monitored. In our approach, we give any

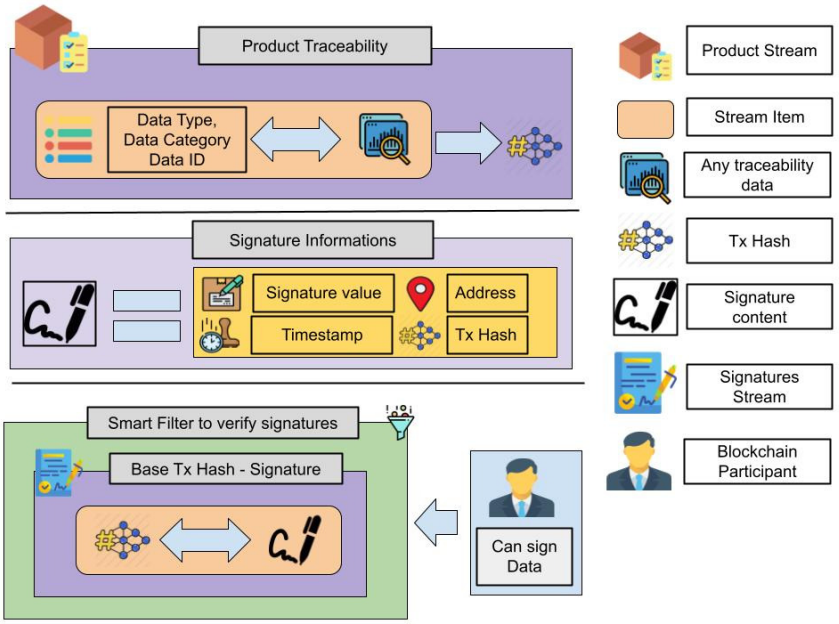

Fig. 16 Data signature management in BPCAT implementation

participant the ability to verify data authenticity. For instance, about non-confidential textual data, it is possible to copy-paste the data and to recompute the hash directly in Multichain panels. If the computed hash matches with the stored one, data integrity is verified. Regarding confidential data, two situations can occur:

- If the author of the request can decrypt the data, nothing differs from the previous example;
- However, if the author of the request cannot decrypt the data, he/she has to send a "decryption request" to the data owner, most likely the company owning the traceability data. Then, if the request is approved, all he/she needs to do is to copy-paste the decrypted data, and compare the computed hash with the stored one.

The process for checking file integrity (see fig.18) is quite similar. It requires the uploading of the file to be verified in order to compute its hash. Then, this hash is compared with the stored hash. If both hashes match, the file's integrity is guaranteed.

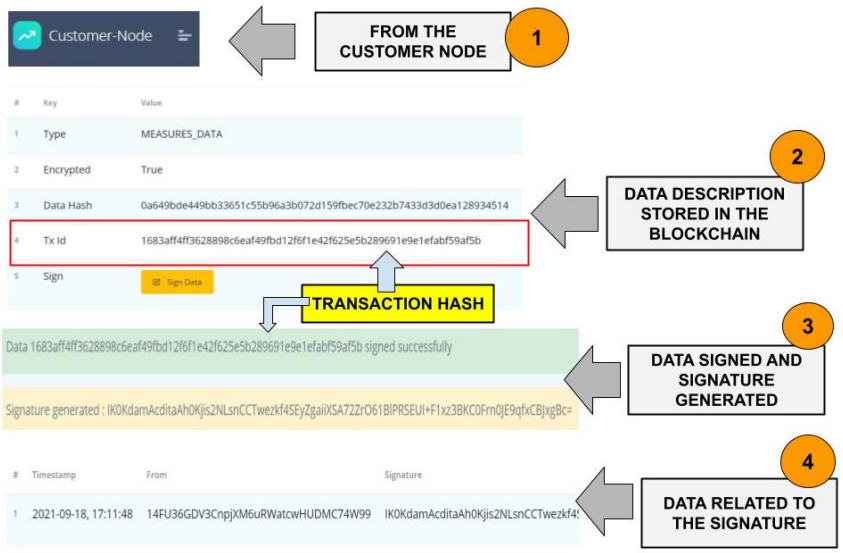

Fig. 17 Data signature in BPCAT implementation with Multichain

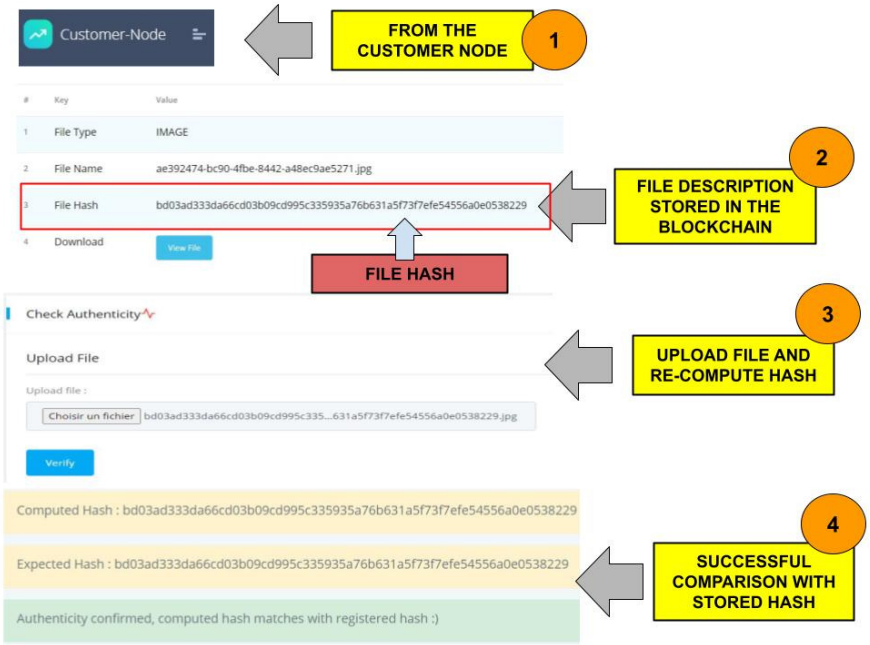

Fig. 18 How to verify file integrity in BPCAT implementation with Multichain

5 Discussion

5.1 Confidentiality of traceability data

BPCAT resorts to asymmetric cryptography and Public Key Infrastruture (PKI) in order to ensure confidentiality of the traceability data. These well-known techniques do not need further evaluations in order to convince of their efficiency. However, the overall architecture proposed through BPCAT may be evaluated regarding its efficiency in a manufacturing factory context. Firstly, though most modern manufacturing operators are familiar with PKI since they already use certificates for their servers and network, they will need to avoid internally managed autosigned certificates in order to resort to external PKI suppliers also acceptable for the other blockchain participants (providers, customers, etc.). Secondly, the Encrypted Encryption Key (EE key) generated by each participant for each confidential data will require a safe and historicized backup in order to guarantee both data protection and recovery. These additional costs could be avoided using homomorphic encryption, since the encrypted data would be able to be verified by any third party without the necessity of decrypting them. We plan to consider such contributions, and perform further evaluations in comparison with additional other approaches, notably zero-knowledge proof, in a future work. Finally, we provide in the following sections a preliminary evaluation of BPCAT itself regarding some of the main challenges raised by the use of blockchain in manufacturing: mining capability of the blockchain nodes, energy consumption, and storage volume.

5.2 Mining and energy consumption

Reducing energy consumption is one of the challenges regarding blockchain technology when it comes to big data. The main element related to energy consumption is the consensus algorithm used in the mining process. In the case of the bitcoin, for example, the consensus algorithm is the Proof Of Work. Multichain is a fork of bitcoin core, and has therefore the ability to use Proof of Work (POW) as well as the round-robin validation scheme. The round-robin is the default scheme of multichain, and it is based on mining diversity where the nodes hiring mining permissions will add blocks either randomly or one after the other depending on the diversity settings. Therefore, there is no competition in the case of this consensus algorithm. In the case of Proof Of Work, the nodes will compete to solve a complex mathematical puzzle, which explains the high energy consumption. In order to illustrate the impact of the consensus algorithm on energy consumption, a comparison of the CPU Core usage by Multichain when using Proof Of Work or round-robin scheme is proposed on fig.19. For every node, two curves are available: POW and Non-Pow. It can be observed through the benefit written next to the non-pow curve associated with each player. For instance, using non-pow makes a difference of -59% for the validator, -83% for the provider and -82% for the customer. A discussion can be engaged regarding energy consumption. Indeed, if some

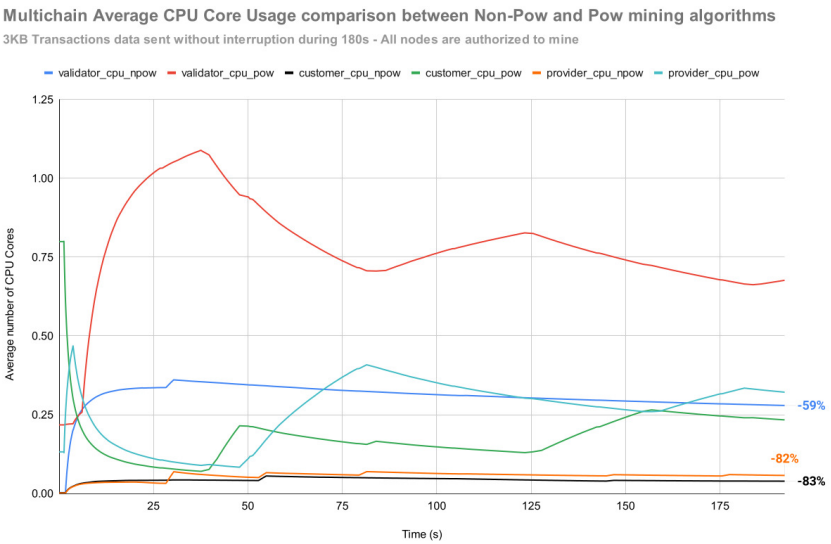

Fig. 19 Multichain Average CPU Core usage: comparison between Proof-of-Work (POW) and Non-Pow (round robin) mining algorithms

factory owners consider that a blockchain is necessary to its traceability policy, and that it justifies the related additional energy consumption, some of its providers and customers may not share their opinion. Currently, BPCAT uses the round robin scheme in order to save energy for every participating player, but it could be also decided that only the factory (validator) performs mining operations so as to spare for both the providers and customers any additional energy costs due to mining.

5.3 Storage volume optimization

Another challenge related to the blockchain technology is the storage volume. Since the blockchain is a distributed system, it implies that all participating nodes must store a copy of the blockchain, thus making the solution less efficient than a centralized system in which the data would be stored only once (in the factory infrastructure, for example). The following subsections describe a way for solving this issue through two parameters: reducing the data size itself, and reducing the volume stored in each node.

5.3.1 Data volume

Multichain provides the possibility to store data as offchain items, which means that data are stored outside the blocks and referenced by a hash. This choice is not neutral, as it can be observed in figure 20. Storing multiple itemps per transaction allows reducing the storage volume necessary, while on-chain storage requires almost the double of the volume in comparison with off-chain

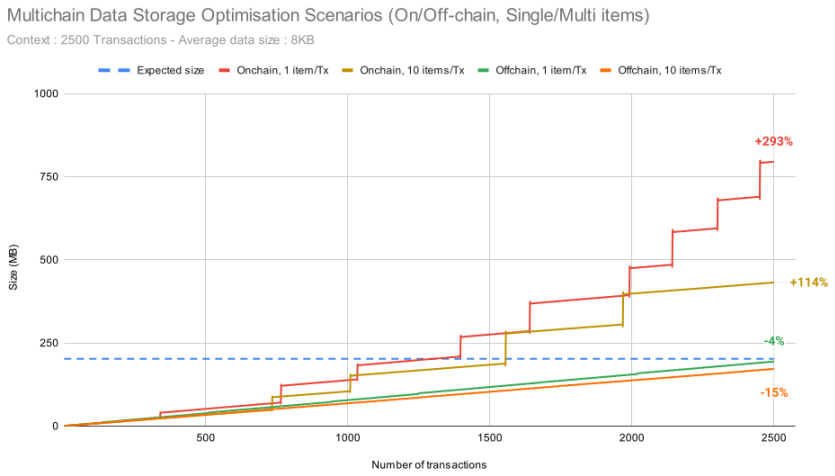

Fig. 20 Multichain Offchain vs Onchain storage volume with single/multiple items per transaction

storage. When data are submitted in offchain, they are internally split into chunks of fixed size and, for every chunk, a hash is calculated. This process is similar to IPFS functioning [11]. However, contrary to IPFS which is a distributed file storage system which can be associated with the blockchain, Multichain includes this feature natively. The most interesting feature in this process is that when a chunk with the same hash already exists, it is not stored twice, and a reference to the existing chunk is created instead. Consequently, storage space can be saved regarding data with a high similarity rate, since duplicated data are not stored multiple times. This is illustrated by Fig.21 for the storage volume optimization according to data variance between the files.

The context is the following: one thousand files of one Megabytes (1MB) are submitted to Multichain in offchain mode with the individual chunk size defined at 100 Kilobytes (10 chunks of 100KB for each 1MB file). The curve labelled as "Total volume reference" shows the total storage volume necessary for simply storing the files in a hard disk. The other curves represent seven situations where the variance between the files ranges from 5% to 100%. A 5% variance means that the 1000 files are only 5% different from one another, and a 100% variance means that the files are completely different from one another. The storage volume savings in each situation according to the Total volume reference is reported as a percentage of reduction on the corresponding curve. This saving ranges from -90% when the files have only a 5% variance and +1% when the files are completely different (a 100% variance). In this latter situation, the volume is higher than the total volume reference due to the supplementary information introduced by Multichain in file storage management.

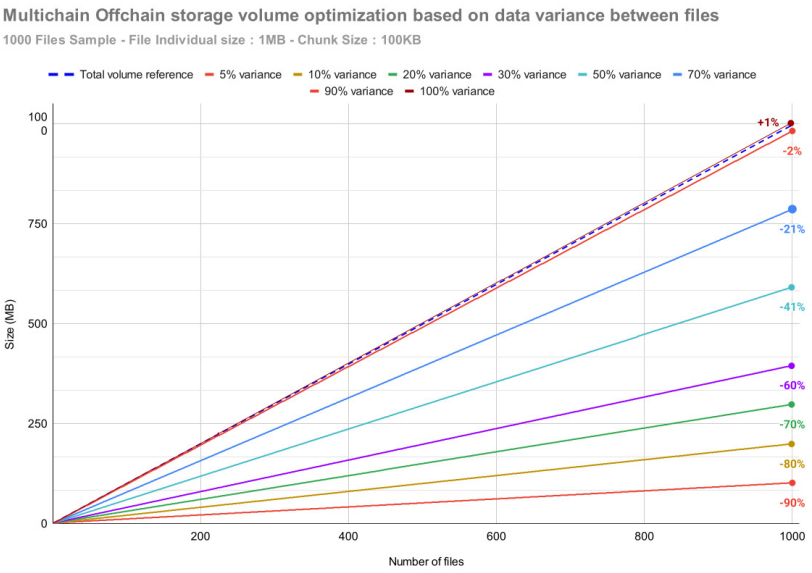

Fig. 21 Multichain Offchain storage volume optimization based on data variance between the files

The context of a manufacturing factory implies that the same processes are repeated over and over, for the same machines and the same products. Therefore, the probability of finding similiraties between data generated by product-centred traceability processes is very high. Consequently, the feature which consists in splitting data into chunks, and not saving twice the same chunk could allow to reduce the volume necessary to traceability data storage.

5.3.2 Node global storage volume

The other issue is the volume of data stored in every node. The idea that the blockchain is a distributed register could suggest that every node has to store exactly the same volume of data in its copy of the blockchain, which is not completely true. As it was previously mentioned, Multichain can save the data in streams, thus allowing the blockchain to be used as a general purpose append-only database providing timestamping, notarization and immutability. By default, every node has to store the blocks and transactions hashes. However, the data stored in the streams imply specific storage management due to the subscribing feature. Subscribing to a stream implies the indexation of the entire content of the stream on the node, including the offchain data. This means that each player has a certain flexibility when choosing the data to store in their local storage, which can allow to save some storage volume. To illustrate how far the extent of this flexibility is, fig.22 presents an optimization of the storage volume based on stream subscription in the BPCAT implementation with Multichain. The context can be described as follows :

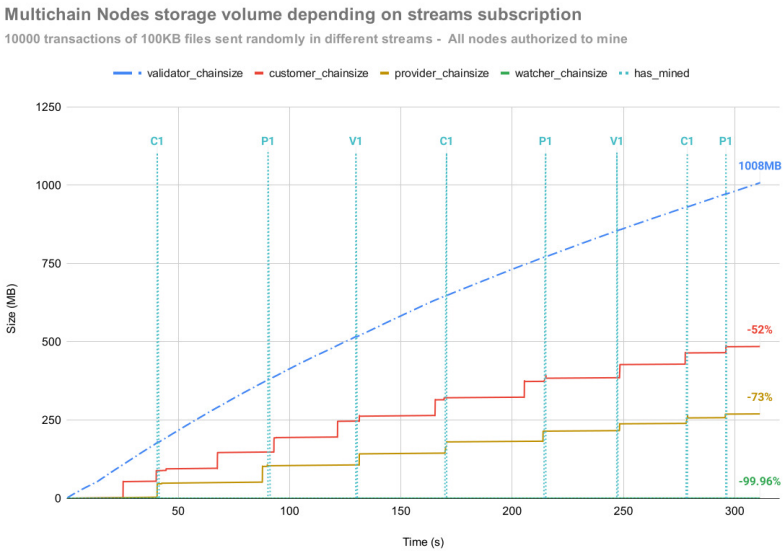

Fig. 22 Multichain node storage volume optimization depending on streams subscription

three specific streams were created for every player, and each one subscribed to its own stream (validator, customer, and provider). A fourth node called the "watcher node" was created, but with no subscription to any streams in order to show the mandatory volume storage needed by any node participating in the blockchain network.

During the evaluations, ten thousand transactions of 100KB-files were sent randomly to those created streams. The first curve shows the total volume stored in the validator which has the highest volume, since it is the one which has submitted all the transactions (the publishers of any transaction have no choice but to store their own data). However, the customer and the provider observe a lower volume in comparison with the validator, respectively -52% and -73%, since they are not subscribers of all the streams. The watcher node needs the lowest volume as expected (-99,96% according to the validator's storage volume). Thus, by defining clearly the relations between the data and the players, it is possible to organize them efficiently into streams in order to save a lot of storage volume on the different nodes. This could facilitate the participation of external players such as providers, suppliers and customers to a blockchain based traceability system of a manufacturing factory.

6 Conclusion

We presented a blockchain based traceability solution for manufacturing factories, which offers an efficient way of providing transparency to all the partners involved while preserving the confidentiality of their respective critical data.

The main idea consists in including encrypted confidential data, along with their hash calculated before encryption into blockchain transactions. In this way, in case of litigation, the investigators can ask the data owner to access the confidential data and compare them with the related data validated by all the blockchain participants in order to establish their authenticity during the product defect analysis procedure. In order to reduce the delay related to encryption, and avoid prohibitive storage consumption for traceability files, only the file hash must be included mandatorily in the blockchain transaction. The implementation of the proposed concepts and functionalities has been illustrated using the Multichain blockchain tool. We show that traceability file storage can be optimized in order to reduce data volume, and the total storage volume necessary to each node by using Multichain chunk and stream features, respectively. In our future work, we plan to perform further evaluation of this solution using real-world manufacturing factory traceability data, in a manufacturing factory simulator especially designed to evaluate blockchain based traceability system performance and drawbacks in various scenarios.

Acknowledgments

The authors acknowledge the support of ETAPLES 4.0 project which is co-financed by the European Regional Development Fund, and the Industry of the future program of the Hauts de France Region Council.

Statements & Declarations

- **Funding**: the authors declare that no funds, grants, or other support were received during the preparation of this manuscript.
- **Competing interests**: the authors have no relevant financial or non-financial interests to disclose.
- **Author contributions**: Valentin Mullet and Patrick Sondi conceived the BPCAT approach. Patrick Sondi formalized the confidentiality preserving mechanism. Valentin Mullet specified and carried out the BPCAT implementation with Multichain. Eric Ramat supervised the research work, and verified the implementation. All authors wrote and reviewed the manuscript.

References

[1] Bougdira, A., Ismail, A., Ahaitouf, A.: A traceability proposal for industry 4.0. Journal of Ambient Intelligence and Humanized Computing **11** (2020). https://doi.org/10.1007/s12652-019-01532-7

[2] Olsen, P., Borit, M.: The components of a food traceability system. Trends in Food Science and Technology **77**, 143–149 (2018). https://doi.org/10.1016/j.tifs.2018.05.004

[3] Zhong, R.Y., Xu, X., Wang, L.: Iot-enabled smart factory visibility and traceability using laser-scanners. Procedia Manufacturing **10**, 1–14 (2017). https://doi.org/10.1016/j.promfg.2017.07.103. 45th SME North American Manufacturing Research Conference, NAMRC 45, LA, USA

[4] Cohin, O., Sondi, P.: Internet of things for smart factory. IEEE COMSOC MMTC E-Letter **10** (2015)

[5] Razak, G.M., Hendry, L.C., Stevenson, M.: Supply chain traceability: a review of the benefits and its relationship with supply chain resilience. Production Planning & Control (2021)

[6] Syed, N.F., Shah, S.W., Trujillo-Rasua, R., Doss, R.: Traceability in supply chains: A cyber security analysis. Computers & Security **112**, 102536 (2022). https://doi.org/10.1016/j.cose.2021.102536

[7] Bettín-Díaz, R., Rojas, A.E., Mejía-Moncayo, C.: Methodological approach to the definition of a blockchain system for the food industry supply chain traceability. In: Gervasi, O., Murgante, B., Misra, S., Stankova, E., Torre, C.M., Rocha, A.M.A.C., Taniar, D., Apduhan, B.O., Tarantino, E., Ryu, Y. (eds.) Computational Science and Its Applications – ICCSA 2018, pp. 19–33. Springer, Cham (2018)

[8] Barata, J., da Cunha, P., Gonnagar, A., Mendes, M.: A Systematic Approach to Design Product Traceability in Industry 4.0: Insights from the Ceramic Industry. In: Paspallis, N., Raspopoulos, M., Barry, C., 0001, M.L., Linger, H., Schneider, C. (eds.) Information Systems Development: Advances in Methods, Tools and Management - Proceedings of the 26th International Conference on Information Systems Development, ISD 2017, Larnaca, Cyprus, University of Central Lancashire Cyprus, September 6-8, 2017. ISD (2017). Citations: dblp

[9] Panetto, H., Dassisti, M., Tursi, A.: Onto-pdm: Product-driven ontology for product data management interoperability within manufacturing process environment. Advanced Engineering Informatics **26**(2), 334–348 (2012). https://doi.org/10.1016/j.aei.2011.12.002. Knowledge based engineering to support complex product design

[10] Niu, X., Wang, M., Qin, S.: Product design lifecycle information model (pdlim). Int J Adv Manuf Technol **118**, 2311–2337 (2022). https://doi.org/10.1007/s00170-021-07945-z

[11] Hasan, H.R., Salah, K., Jayaraman, R., Ahmad, R.W., Yaqoob, I., Omar, M.: Blockchain-based solution for the traceability of spare parts in manufacturing. IEEE Access **8**, 100308–100322 (2020). https://doi.org/10.1109/ACCESS.2020.2998159

[12] Alkhader, W., Alkaabi, N., Salah, K., Jayaraman, R., Arshad, J., Omar, M.: Blockchain-based traceability and management for additive manufacturing. IEEE Access **8**, 188363–188377 (2020). https://doi.org/10.1109/ACCESS.2020.3031536

[13] Leng, J., Ruan, G., Jiang, P., Xu, K., Liu, Q., Zhou, X., Liu, C.: Blockchain-empowered sustainable manufacturing and product lifecycle management in industry 4.0: A survey. Renewable and Sustainable Energy Reviews **132**, 110112 (2020). https://doi.org/10.1016/j.rser.2020.110112

[14] Tönnissen, S., Teuteberg, F.: Analysing the impact of blockchain-technology for operations and supply chain management: An explanatory model drawn from multiple case studies. International Journal of Information Management **52**, 101953 (2020)

[15] Hader, M., Tchoffa, D., Mhamedi, A.E., Ghodous, P., Dolgui, A., Abouabdellah, A.: Applying integrated blockchain and big data technologies to improve supply chain traceability and information sharing in the textile sector. Journal of Industrial Information Integration **28**, 100345 (2022). https://doi.org/10.1016/j.jii.2022.100345

[16] Xu, X., Tatge, L., Xu, X., Liu, Y.: Blockchain applications in the supply chain management in german automotive industry. Production Planning & Control **0**(0), 1–15 (2022). https://doi.org/10.1080/09537287.2022.2044073

[17] Chen, S., Cai, X., Wang, X., et al.: Blockchain applications in plm towards smart manufacturing. Int J Adv Manuf Technol **118**, 2669–2683 (2022). https://doi.org/10.1007/s00170-021-07802-z

[18] Mullet, V., Sondi, P., Ramat, E.: A review of cybersecurity guidelines for manufacturing factories in industry 4.0. IEEE Access **9**, 23235–23263 (2021). https://doi.org/10.1109/ACCESS.2021.3056650

[19] Galvez, J.F., Mejuto, J.C., Simal-Gandara, J.: Future challenges on the use of blockchain for food traceability analysis. TrAC Trends in Analytical Chemistry **107**, 222–232 (2018). https://doi.org/10.1016/j.trac.2018.08.011

[20] Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., Alazab, M.: Blockchain for industry 4.0: A comprehensive review. IEEE Access **8**, 79764–79800 (2020). https://doi.org/10.1109/ACCESS.2020.2988579

[21] Mohamed, N., Al-Jaroodi, J.: Applying blockchain in industry 4.0 applications. In: 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), pp. 0852–0858 (2019). https://doi.

org/10.1109/CCWC.2019.8666558

[22] Leng, J., Ye, S., Zhou, M., Zhao, J.L., Liu, Q., Guo, W., Cao, W., Fu, L.: Blockchain-secured smart manufacturing in industry 4.0: A survey. IEEE Transactions on Systems, Man, and Cybernetics: Systems **51**(1), 237–252 (2021). https://doi.org/10.1109/TSMC.2020.3040789

[23] Ko, T., Lee, J., Ryu, D.: Blockchain technology and manufacturing industry: Real-time transparency and cost savings. Sustainability **10**(11) (2018). https://doi.org/10.3390/su10114274

[24] De Giovanni, P.: Blockchain and smart contracts in supply chain management: A game theoretic model. International Journal of Production Economics **228**, 107855 (2020). https://doi.org/10.1016/j.ijpe.2020.107855

[25] Lee, J., Azamfar, M., Singh, J.: A blockchain enabled cyber-physical system architecture for industry 4.0 manufacturing systems. Manufacturing Letters **20**, 34–39 (2019). https://doi.org/10.1016/j.mfglet.2019.05.003

[26] Li, Z., Barenji, A.V., Huang, G.Q.: Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. Robotics and Computer-Integrated Manufacturing **54**, 133–144 (2018). https://doi.org/10.1016/j.rcim.2018.05.011

[27] Fernández-Caramés, T.M., Blanco-Novoa, O., Froiz-Míguez, I., Fraga-Lamas, P.: Towards an autonomous industry 4.0 warehouse: A uav and blockchain-based system for inventory and traceability applications in big data-driven supply chain management. Sensors **19**(10) (2019). https://doi.org/10.3390/s19102394

[28] Wang, Y., Kogan, A.: Designing confidentiality-preserving blockchain-based transaction processing systems. International Journal of Accounting Information Systems **30**, 1–18 (2018). https://doi.org/10.1016/j.accinf.2018.06.001. 2017 Research Symposium on Information Integrity and Information Systems Assurance

[29] Cohen, Y., Naseraldin, H., Chaudhuri, A., et al.: Assembly systems in industry 4.0 era: a road map to understand assembly 4.0. Int J Adv Manuf Technol **105**, 4037–4054 (2019). https://doi.org/10.1007/s00170-019-04203-1

[30] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Cryptography Mailing list at https://metzdowd.com (2009)