Do Blockchain and IoT Architecture Create Informedness to Support Provenance Tracking in the Product Lifecycle?

Mazumdar, Somnath ; Jensen, Thomas; Mukkamala, Raghava Rao; Kauffman, Robert J.; Damsgaard, Jan

Document Version
Final published version

Published in:
Proceedings of the 54th Hawaii International Conference on System Sciences

DOI:
10.24251/HICSS.2021.181

Publication date:
2021

License
CC BY-NC-ND

Citation for published version (APA):
Mazumdar, S., Jensen, T., Mukkamala, R. R., Kauffman, R. J., & Damsgaard, J. (2021). Do Blockchain and IoT Architecture Create Informedness to Support Provenance Tracking in the Product Lifecycle? In *Proceedings of the 54th Hawaii International Conference on System Sciences* (pp. 1497-1506). Hawaii International Conference on System Sciences (HICSS). Proceedings of the Annual Hawaii International Conference on System Sciences https://doi.org/10.24251/HICSS.2021.181

Do Blockchain and IoT Architecture Create Informedness to Support Provenance Tracking in the Product Lifecycle?*

Somnath Mazumdar[a], Thomas Jensen[a], Raghava Rao Mukkamala[a,c], Robert J. Kauffman[a,b], and Jan Damsgaard[a]
[a]Copenhagen Business School, Denmark, [b]Singapore Management University, Singapore,
and [c]Kristiania University College, Norway
{sma,tj,rrm,rk,jd}.digi@cbs.dk

Abstract

Consumers often lack information about the origin and provenance of the products they buy. They may ask: Is a food product truly organic? Or, what is the origin of the gemstone in the ring I purchased? They also may have sustainability concerns about the footprint of a product at the end of its life. Producers and sellers, meanwhile, wish to know how longitudinal tracking of the provenance of products and their components can boost their sales prices and after-market value, and reveal new business opportunities. We focus on how the product lifecycle (PLC) can be leveraged to track information that typically has not been available to support distributed activities. Instead, they have been supported by the manufacturers that create new products. We propose an architecture that utilizes blockchain and the Internet of Things (IoT) to support a range of PLC use case scenarios – from production to marketing and consumption, to maintenance and refurbishment, as well as recycling and disposal. We also offer design thinking about blockchain-IoT architecture to support products such as textiles, furniture and food. Our contribution is an architecture for cross-PLC management support and an explanation of its potential to enhance value through stakeholder informedness.

1. Introduction

Consumers, buyers and users of products face many problems and issues, for example, whether they are authentic, support environmental sustainability, and are brought to market through business processes that reflect fair trade [32]. Manufacturers and resellers are similarly concerned with how to address these things while servicing their customers and gaining advantage over their rivals. Both sides of the market are also interested in establishing the origin of a product at any time in its lifecycle – in development/marketing, purchase/resale, use/reuse, maintenance/refurbishment, and recycling/disposal across the full spectrum of the **product lifecycle** (PLC) [21].

We propose the PLC [28] as a means to address the leading issues with product information tracking. Current PLC solutions are based on collecting all information needed in a central repository [22]. But today, most devices (e.g., mobile phones, circuit boards, kitchen appliances) are manufactured with components sourced from a distributed network of suppliers.[1] So, a central repository solution does not mirror the distributed supply chain in terms of how information can be best brought together. Further, post-manufacturing PLC information is unlikely to include product purchase, use, and maintenance information – much less that for disposal activities.

If it can be collected though, such information is likely to be useful to improve and develop future products [8], and enhance product informedness for lifecycle participants and for which the related theory of informedness suggests there should be new value to appropriate [18] – all the way to product remanufacturing, recycling and disposal. Economic theory further affirms that this should be a source of business value for firms to appropriate, affecting the price of manufactured goods they sell, as well as consumers' willingness-to-pay for them. Supply chain players with PLC information capabilities should be able to build new power for their positions in the market and competitive sustainability as a result too [7].

Blockchain technology is especially interesting and novel for this context, based on our scan of prior interdisciplinary literature and industry practice. A feature is its ability to support distributed information sources. We propose using blockchain technology with IoT for PLC

*This research is supported by Industriens Fond (The Danish Industry Foundation). Any opinions, findings, interpretations, conclusions, or recommendations expressed in this paper are those of its authors and do not represent the views of the Industriens Fond.

[1]Electronic devices like what you're using to read this are identified with a manufacturer, product ID, version and serial number, all documented in a manufacturer's system. This also typically includes the build materials and components with serial numbers and specifications for their software versions.

URI: https://hdl.handle.net/10125/70793
978-0-9981331-4-0

information mirroring to match the distributed nature of product information across multiple stakeholders. We further propose to combine this with IoT technology to enable easier product information sharing (e.g., GPS position or accelerometer records of movement). With these technical bases, we will also lay out how the product authentication component in our proposed architecture works, as a means of supporting provenance tracking for a range of possible PLC applications.

2. Relevant Literature

We next discuss appropriate literature to identify the intellectual foundations for our work.

2.1. Blockchain in the supply chain context

Many authors have explored blockchain-based product tracing and monitoring in supply chain management (SCM) systems – for example, for agricultural products [24], IoT combined with blockchain for food products [30], and RFID and blockchain-based [26] and near-field communication blockchain authentication [2]. Other applications are more basic, like managing cardboard boxes for supply chains [1], and globally tracking shipping containers through their locations using IoT devices with GPS [13]. Manufacturers source material and components from a range of suppliers that often obtain them from another level of international suppliers, so their supply chain networks are actually globally distributed.

In recent years, there also has been blockchain-based product authentication research, including zone-based identification [9] and diamond authentication [6]. Still other work has used blockchains to fight counterfeit product ownership [31] and capture chemical signatures for embedded particulates in OEM parts [16]. Liu et al. [20] further proposed a blockchain-based platform for information tracking in auto manufacturing [11]. For data sharing, blockchain-focused IS and smart contract support has also been considered for transaction execution. Our work is related, though the other work does not support product authentication for users and consumers or recycling, but mainly has been focused on production in the PLC.

With blockchains, records and information blocks are linearly-chained together. The primary elements are the append-only ledger, cryptography support, and shared ecosystem and distributed computing infrastructure. They offer trust via a hash-based integrity verification mechanism, which can be categorized as permissionless and permissioned. Permissionless blockchains offer true decentralization and transparency, but suffer from privacy and scaling issues. In contrast, permissioned blockchains offer higher throughput, better privacy and scalability, but at the cost of transparency.

There are other blockchain elements to note. *i)* One is *hashing*, a method of applying a cryptographic hash function to data to calculate a relatively unique output (message or digest) for input of nearly any size. *ii)* Another is a *transaction*, representing an interaction between users. *iii)* Yet another is *asymmetric-key* or *public key cryptography*, which is used to encrypt transactions similar to how private/public key approaches can be used to decrypt them. And *iv) ledgers* in blockchain networks support both distributed ownership as well as a distributed physical architecture.

With blockchain, users publish information in a block which contains a block header and block data. Such blocks are chained together with each block containing the digest of the previous block's header. Consensus protocol determines which user publishes the next block in the blockchain. Employing a mechanism consensus protocol forces multiple rational, distrusting users to publish blocks in the blockchain network. Smart contracts are one of the most important features added in blockchain implementations. They collect the business logic and associated input data which are executed based on a rule or after satisfying some preconditions that need to be met.

2.2. Informedness theory and PLC value

The *product lifecycle* (PLC) is related to the organization of "*the business activity of managing ... a company's products all the way across their lifecycles; from the very first idea for a product all the way through until it is retired and disposed*" [28, p. 1]. The potential value of bringing cross-PLC information together for firms is driven by the extent to which it creates beneficial impacts so managers can rethink how they design and handle products, to appropriate the highest RoI from the benefits that accrue to their stakeholders. This is often due to the price recovery effects of higher prices charged and the strength of business relationships that result.

Managerial use of information is typically driven by manufacturers that create new products and use their central ERP systems to record PLC information (e.g., information from suppliers and the supply chain network) related to the product manufactured. They typically do not collect PLC information after production is completed though, other than for product failures and consumer warranty claims. Building IoT into products enables them to communicate PLC information (e.g., with the IoT connectivity increasingly available in cars) to others, which increases informedness that enables valuable predictions of service and maintenance needs to be

addressed [10]. This theory of informedness guided our thinking about how to explain such information impacts in this research.

Today, such management practices are an integrated (albeit incomplete) part of the solutions offered by major ERP providers. The goal is to separate the product from information stored about it. Recorded information, meanwhile, is structured with predefined record types and versions, enabling historical background to be extracted. Such information captured by IoTs and implemented with blockchain can help to reduce misrepresentation and fraud in a firm's supply chain [12], thus creating the basis for improved value appropriation. Blockchain also can address data security issues and support identity management by authenticating network nodes and verify authorized users that can access information, thus maintaining distributed privacy and access control [25]. But a centralized repository of current management information solutions can hardly mirror the structure of the supply chain network and many suppliers. In contrast though, this is made possible by using a blockchain-IoT distributed architecture.

2.3. Authentication and product provenance

Product authentication is an up-and-coming technique to combat counterfeiting. In general, authentication can validate the authenticity of users and products when the appropriate systems support is available. Computer-supported, mathematics-based digital authentication – our focus – has significant promise for product provenance. This process usually requires a one-way hash function.[2] The input data is the message and the output data is the hash. This process represents the actions of suppliers that supply products to a manufacturer, and the manufacturer subsequently updates the information on invoices and parts supplied in its database.

Fig. 1 represents a way to represent a human actor to access legitimate services [3]. The authentication process begins with the registration process (on the left side of the figure). The person applies to a registration authority to become a subscriber after providing the required proof. Upon successful verification and receipt of approval, the subscriber receives a credential from the credential service provider (CSP) to access the appropriate services and facilities. The subscriber then must prove to a verifier for each session in which it participates via the issued credential that it is indeed an authentic subscriber. For example, Fig. 1 shows a product authentication process representing the actions of suppliers that supply products to a manufacturer, and subsequently causing an update to the information on invoices and parts supplied in the manufacturer's database.

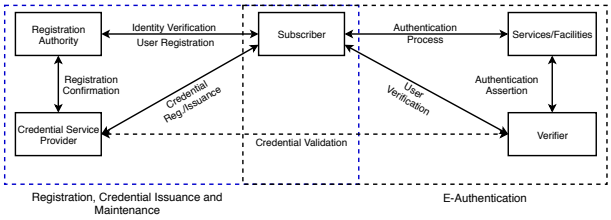

Figure 1. Generic authentication process using a service

During verification, the verifier makes a request to the CSP to validate the credential of the subscriber. Now, if the verifier is separate from the services and facilities, the former must present an assertion about the subscriber so the services and facilities offer further authorization for access. Upon successful validation, the subscriber will be permitted to access the services and facilities [4]. In Fig. 2, the user scans the QR-code to explore product authenticity from the manufacturer's website or a third-party authentication service.

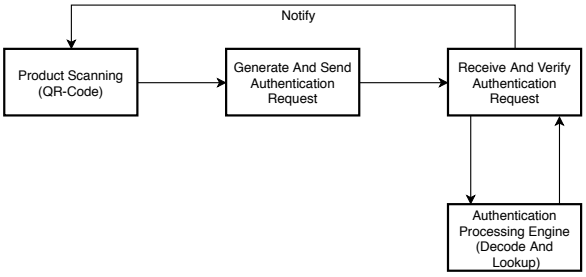

Figure 2. Product authentication steps using QR code

After this scan, the authentication module generates a request to the manufacturer's service for validation. In the service module, search occurs in the product database after successfully decoding the SKU code. If the product is made by the firm, then the scan will notify the user of a successful result. Product authentication supports manufacturers and retailers in building trust with their customers, and protects their brand and business model. Barcode identification of products is widespread and may involve RFID-based code scanning [14],[3] while authentication solutions occur in three technology forms: overt (watermarks, holograms); covert (digital watermarks); and

[2]This is often called a *secure hash algorithm* (SHA), with a variant, SHA-3, for blockchain encryption.

[3]RFID-based product authentication involves a micro-chip in a tag that transmits a unique product ID to a reader. The IDs can only be read by devices that use the correct radio-wave frequency. For related coverage of hash-based RFID reader-tag mutual authentication of products and passive RFID devices for food traceability, see Yang et al. [33] and Cao et al. [5].

machine-readable forms (RFID, QR codes) [23]. Historical records for product-related activities that are recorded and stored on the blockchain can provide confidence in the provenance of a product and thereby its authentication, yet must be accessible for all potential users. IoT devices attached to or embedded in products and blockchain-based provenance for product authentication will be discussed later with our proposed architecture.

3. PLC in design and manufacturing

The *product lifecycle* (PLC) was proposed for efficient management of the end-to-end lifecycle of a product, beginning from its conceptualization though its disposal [28]. We offer a representation of a product's PLC stages for the design and manufacturing industry context (see Fig. 3). While design, manufacturing and sales

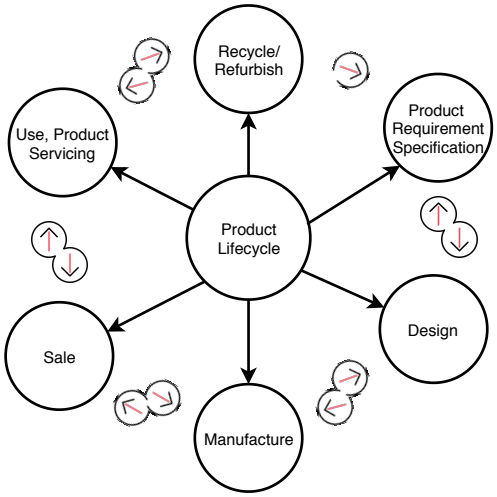

Figure 3. PLC stages of a product

are the most common product stages supported by commercial tools, ERP, CRM and inventory database capabilities typically are combined into a centralized suite of applications. We will consider an end-to-end product authentication sequence that involves an RFID microchip in a tag. An architecture that covers the PLC stages recognizes relevant services such as product authentication, recycling and so on – important in our work.[4]

[4] A simpler, general representation is one in which the PLC is divided into three product stages: the *beginning-of-life* (BOL), *middle-of-life* (MOL), and *end-of-life* (EOL) stages [29]. BOL covers the manufacturing process from design to a finished product, while MOL captures the process that brings the product to its users – from storing it in a warehouse, to its sale to users, and its subsequent use. Finally, EOL includes the post-usage stages, such as disassembly and recycling, reuse and disposal [15]. Commercial PLC tools typically support resource planning, and customer and supply chain management, which covers the BOL, but only some activities in the MOL stages. Across these more aggregated PLC stages, various stakeholders also play different roles.

During these stages, important information is generated about the product, including its usage. A challenge is that different stakeholders (e.g., manufacturers, retailers, distributors) contribute different kinds of information in different stages. It is usually stored in their legacy systems, and then distributed across the PLC to the extent that this is possible. Due to the vintage nature of the different stakeholders' systems though, it may be costly to share such information among them. Individual stakeholders only have access to a partial view of it also, which makes it hard to trace a product's history based on all relevant information, reducing the effectiveness of support for product provenance validation and other related activities.

4. Proposed blockchain-IoT architecture

We now turn to the proposed blockchain-IoT architecture and explain why it is suitable for supporting product provenance and facilitating a more holistic view of product-related information. We also show how the proposed architecture can efficiently and transparently support product authentication as a use case, to prove the genuineness of a product. As we noted, the PLC is not a new concept and there already are commercial tools available, but they mostly focus on just three out of the six PLC stages: design, manufacturing and retail. Singh et al. [27] noted seventeen factors responsible for successful implementation of traditional PLC systems in the manufacturing industry. The factors cover the areas of technology, business processes and people. We will emphasize the PLC's technological aspects, by focusing on infrastructure, interoperability and security.

With current advances in IoT and blockchain, communication protocols work well with robust peer-to-peer computing infrastructure, as well as with cryptographic security mechanisms built on blockchain. Our proposed architecture provides a secure and robust permissioned-ledger platform based on a permissioned-blockchain platform for sharing distributed product information among different stakeholders in a transparent and trustworthy manner. [5] We next introduce the stakeholders and then discuss the various components of the related technical architecture.

4.1. Stakeholders

Several stakeholders interact with the blockchain-IoT platform with varied kinds of information (see Fig. 4):

- **suppliers** are concerned about providing guaran-

[5] For implementing this architecture, we selected Hyperledger Fabric Platform (http://github.com/hyperledger/fabric).

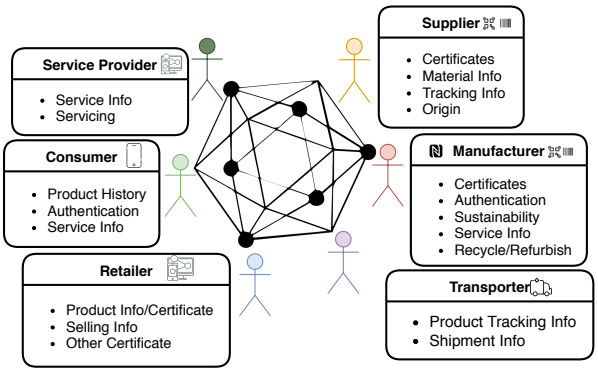

Figure 4. Stakeholders with different information exchanged via the blockchain-IoT platform

tees and certificates on sustainable materials and ecological practices;

- **manufacturers** care about product authentication, certificates for sustainable products, and recycling and refurbishing products;
- **transport providers** emphasize traceability and shipping-related information;
- **retailers** deal with product inventories, purchases and after-sale warranties and returns; and
- **consumers** are interested in product history, authentication and service information;
- **service providers** are concerned with post-sale servicing and maintenance.

Each stakeholder must deal with information related to products from different PLC stages and, in that process, necessary information will be added to, or retrieved from the platform in a decentralized and distributed manner. It is also worth noting that different stakeholders may employ different devices (e.g., barcodes, QR codes, and NFC) or use web and mobile services to add, update and access product- related information for PLC ecosystem participants. However, even though different stakeholders may do this, access to product-related information still will be controlled based on stakeholders' access rights, due to the permissioned nature of the blockchain platform. This way, information can be shared securely and privacy concerns respected. This feature is not available in existing PLC systems.

Most stakeholders still must maintain their own standalone ERP, CRM, and storage systems. But they typically will not need to communicate with each other while adding product-related information when the blockchain approach is used. Further, they can keep their data sources secure while they access product-related information from the distributed ledger of the blockchain-IoT platform.

4.2. Proposed architecture

Proposed permissioned blockchain-IoT architecture contains three layers (see Fig. 5). They are *legacy systems layer*, permissioned *blockchain-IoT layer*, and the *use cases and distributed applications layer*. The **legacy systems layer** is the left-most layer in the figure, consisting of traditional enterprise wide management tools (e.g., ERP, CRM and inventory databases of different stakeholders). It is designed to collect, process, and store information about a product, business and organization. An important characteristic is that its systems occur as siloes within the organizational boundaries of their respective stakeholders. The **blockchain-IoT layer** is the middle layer (refer Fig. 5), where the permissioned blockchain-IoT platform implements a permissioned distributed ledger. Blockchain-IoT ecosystem contains each module for cryptography-based security, consensus-making rules, and multiple protocols for safe peer-to-peer communication. They "guarantee" an immutable, tamper-resistant and append-only permissioned distributed ledger that provides transparent product-related information to ensure trust among the stakeholders. The middle layer also supports IoT devices, while connecting with physical products and generating additional information (e.g., traces of activity or geographic locations) for the platform.

A notable capability of the middle layer platform is its *off-chain storage* for primarily holding IoT sensor/device data or traces and other block related information. Blockchain is a distributed ledger replicated across many peer-to-peer nodes. So to maintain the stable performance (essentially the throughput) of the blockchain platform, it should not be used to store a huge information related to products. Moreover, blockchain ledgers are immutable, so once information is stored it cannot be changed. Thus, they are unsuitable for storing private information also (e.g., private identity and consumer information). Such information must be handled with compliance in mind (e.g., with Europe's General Data Protection Regulations (GDPR) and keeping other nations' regimes in mind).[6] As a result, some sensitive information will need to be relegated to the (encrypted) off-chain, offline storage. Only a hash pointer to the storage location will be retained on the blockchain. This way, a blockchain-IoT platform can be

[6]The issue with storing personal information on a blockchain is that, if someone wishes to exercise their *right to be forgotten*, then the related information has to be erased. But this is not trivial in an immutable blockchain ledger.

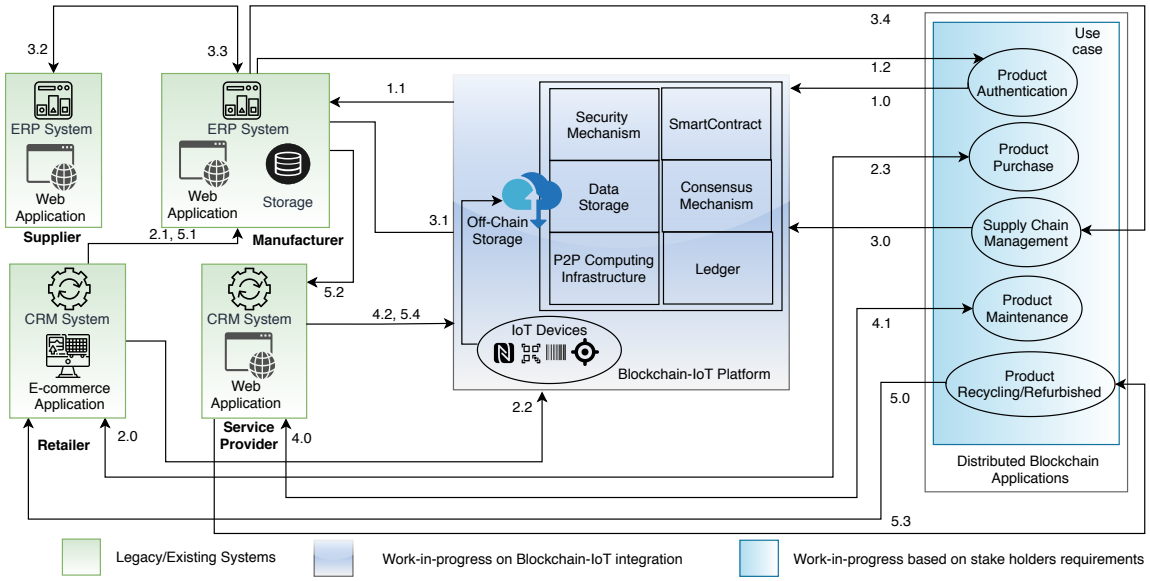

Figure 5. Blockchain-IoT platform architecture

compliant with almost any personal data privacy compliance requirements.

The **use cases and distributed applications layer** is the right-most part of the Fig. 5. It describes the various use cases and applications, such as product authentication and purchase, supply chain management, and product maintenance, recycling and refurbishing (and others) that cover various stages of the PLC. Apart from IoT devices, watermark, QR-code, bar-code and several other cutting edge mechanisms can also be attached to the proposed ecosystem. It is worth to note that this is a non-exhaustive use case list, as briefly explained below:

The **Product Authentication** use case involves verification by combining information from blockchain with other necessary information from the manufacturer to prove a product is genuine (covers sequence# 1.0–1.2). Normally, this will be used by consumers or other stakeholders who may be concerned about counterfeit goods or would like to have information about when a product was manufactured. This gives the original manufacturer a chance to respond with the authentication details directly to the user, thus enhancing product value.

The **Product Purchase** use case occurs with the economic exchange normally involving a retailer and a consumer (covers sequence# 2.0–2.3). When the retailer updates product-related information (e.g., inventory level), the manufacturer can be notified through an update to the blockchain representing a product's digital trace and history. This is especially useful with just-in-time auto re-supply of store inventories. It also is valuable for customer informedness, when a product they wish to buy has come back in stock at a store they wish to buy from. In contemporary retailing and wholesaling, this is an appropriate instance where our architecture creates the possibility of a new *service-as-a-service*.

The **Supply Chain Management** use case involves the complex job of managing a manufacturer's supply lines so the right products are available for sale and delivery at the right time and location (covers sequence# 3.0–3.4). The manufacturer and suppliers are the primary participants in this use case. In our proposed architecture, blockchain can add an extra information-interfacing capability to connect the stakeholders to each other and the means to store information related to products (e.g., authentication certificates) either on-chain or off-chain. This offers the benefit of enhancing an intermediary's value in a distributed supply chain network.

The **Product Maintenance** use case occurs during product usage, when the product may need regular maintenance (covers sequence# 4.0–4.2). To support this, the service provider needs to be notified and, after the task is completed, the appropriate maintenance and servicing information should be added to the blockchain. The service task will then become part of the product's history.

The **Product Recycling and Refurbishing** use case is intended to support these kinds of end-of-product life actions (covers sequence# 5.0–5.4). If a product is appropriate for recycling or refurbishing, a consumer would contact a designated retailer to handle the product in an environmentally-sustainable way. The manufacturer will be notified to carry out the process, and the designated service provider may be asked to actually perform the task locally. When the task is completed, the blockchain will be further updated, and the product's digital ledger will encode and store the new product information.

Thus, the proposed permissioned blockchain and IoT system will serve as a distributed and decentralised platform that will enable product-related digital traces of communication and exchange. They can be stored as information in a secure and transparent manner in coordination with stakeholders traditional systems, so that stakeholders can use it. Such trace data are immutable and secure, so altering information from any of the stakeholders will be very costly. In this way, our proposed architecture can enhance the functionality of existing systems, enhancing their informedness and value for stakeholders, and enabling the support of innovative services across the PLC.

4.3. A product authentication walk-through

Fig. 6 presents the information flow for the product authentication use case scenario. It has two parts that generate and consume information. The process starts by combining information from the permissioned blockchain-IoT platform with information from the traditional systems (e.g., ERP/CRM/database) of the manufacturer to verify the authenticity of the product (consumption part).

Assume that the product considered is a chair that can be recycled and has an attached QR code. If a consumer wants to buy that particular chair then the QR code has to be scanned and the product authentication service will be called using the designated web or mobile service. The request will be sent to the blockchain network, where it will be further combined with additional information from the manufacturer's traditional systems (information generation).

Now, using a QR code, the manufacturer will search its product catalogue. Once the product ID of the item is found, relevant information will be sent to the consumer in a response that may contain additional information such as product history, warranty and service information and suggestions about matching furniture (See the Sample Search Result in Fig. 6.).

For the product authentication process, the consumer and manufacturer are the primary stakeholders, while the suppliers and retailers could be secondary stakeholders in this particular use case. The quantity of information generated and consumed is implementation-specific and tied to the nature of the industry sector, consumer segment, and product type. For instance, expensive designer chairs and inexpensive commodity chairs have different warranties and after-market services (like add-on parts). This will enable a consumer to be guaranteed that the product is authentic, based on the immutability and security features of blockchain.

If a product is not authentic, then the lack of product authentication can be communicated to the consumer, which is a way for the retailer to enhance consumer informedness in general through such actions. Further, the manufacturer can communicate about any product disclaimers that may result in a lack of warranty obligations on the manufacturer's part. Since the blockchain-based information cannot be tampered with, the consumer can be confident that they can purchase and be assured the product is not counterfeit.

5. Discussion

In this research, we proposed a blockchain-IoT platform that supports sharing of product-related information from various stages of the PLC in a decentralised and distributed manner among the stakeholders. To the best of our knowledge, there is not anything similar in the literature to our proposed architecture. The distributed architecture of blockchain promotes a holistic perspective about product-related information across the PLC, and IoT enables its autonomous creation to be shared via the blockchain. This leads to enhanced stakeholder informedness, and we believe it is a novel perspective and approach

5.1. Technological perspective

Technologically, the proposed architecture has several advantages when compared to the existing way of handling the PLC using legacy systems. First, blockchain provides immutable and tamper-resistant data storage in the form of an open and public distributed ledger. It has suitable privacy and access controls built on cryptographic security mechanisms that increase stakeholder trust in the information shared.

Since product-related information is stored in blocks with hash pointers as the links between them, it is easy to identify if the information has been tampered with. The immutable public ledger features of blockchain enhance trust among stakeholders based on their roles, and such information can be shared transparently with suitable permissions for the stakeholders' information access on the blockchain.

Second, product-related information is stored on the blockchain with time-stamps representing the chronological order of their addition. The immutability of time-stamped information leads to several interesting scenarios, especially product histories rendered from digital traces. These are able to cut across some of the PLC stages that support participant value co-creation, which makes it possible to perform data analytics about product quality and performance in ways that are permissible. This enables new use scenarios also, such as calculating the carbon footprint and others.

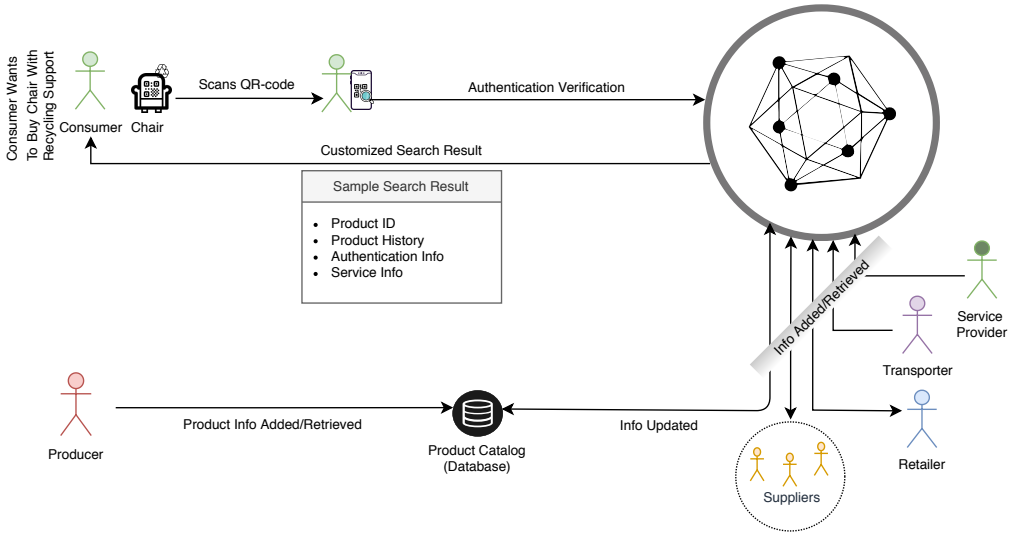

Figure 6. High level representation of product authentication use case

Product authentication by consumers and other stakeholders can also be used to fight against counterfeit products. The immutable time-ordering of information that is added can prevent dishonest manufacturers and suppliers from making false claims by providing fake certificates about sustainable products and eco-friendly materials. Relevant information and the necessary certificates must be added to the blockchain from the beginning. This encourages the participation of honest manufacturers and suppliers, since they will be able to present indisputable and verifiable certificates about the products they handle.

5.2. Business perspective

From a business perspective, the proposed blockchain-IoT platform will provide more information about products than what is available now to consumers and other stakeholders via the traditional tools. This will lead to increased informedness about the products of their interest – especially *consumer informedness* and *business partner informedness*, and will impact their behavior, increasing their willingness-to-pay. This will also impact the businesses involved with the products, since they can benefit from being able to develop new business capabilities, such as improving their products and building additional services since they can benefit from being able to charge higher prices and attract more purchases. As a result, the platform will serve consumers better and help manufacturers to gain competitive advantage over their rivals.

The increased informedness we have noted is likely to impact the potential value that consumers can obtain through their involvement with the informationally-enhanced products. This will apply to other major stakeholders too (e.g., suppliers, manufacturers and retailers), as well as secondary stakeholders (e.g., transport and other service providers). We foresee that the value-creation opportunities enabled by increased informedness will be useful in supporting the innovation and execution of new business opportunities.

For example, IoT devices attached to products can be used to develop new use case scenarios resulting in value-adding services. They may include: product search and identification support, reports that identify under-utilized and under-performing products and assets, and pushed-alerts when conditions for a product are unfavourable, for example, when products go outside of a pre-defined and geo-fenced area. This is similar to what we have seen with RFID sensors that identify events that result in cargo shocks in transit and out-of-range temperatures for stored food items that are not permissible. It also occurs with active IoT devices for which sensed events can be communicated in real-time. This increased informedness enables early and even preventive actions to be taken that can yield a surprising amount of business value.

The implementation of a blockchain-IoT platform such as we have discussed will not only be effective and less costly for manufacturers' current, central repository-focused IS. It also will transform the extent to which information becomes available about their product-related processes, how they conceptualize business and operational strategy, as well as their business partner relationships. Thus, our blockchain-IoT platform will be a strong complement to a firm's existing IS capabilities. The use of blockchain and IoT make it possible to capture so much more data about what happens across the entire PLC, which ought to be a game-

changer for the stakeholders. For business partners, for example, it will create *cross-organizational informedness* that is necessary to support the higher-level goals of Industry 4.0 innovation, while empowering auditors and regulators to develop a fuller understanding of a manufacturer' performance in different PLC activities and the effectiveness of their and their partners' compliance with regulation and fair market practices.

6. Conclusion

We proposed an architecture for information that documents the product lifecycle based on blockchain and IoT devices attached to physical products. The proposed platform is different compared to other state-of-the-art and commercial tools that aim to capture data across the PLC. Our most important overall contribution is to show how it is possible to map important information that needs to be captured, stored and made accessible for use by PLC stakeholders – wherever they are, and whatever the PLC stage they are involved with. The approach that we advocate is essentially aimed at reconsidering how to enhance the information endowment so it is possible to more fully track PLC activities and further integrate stakeholders' legacy systems into a commonly-accessible platform.

From an economics standpoint, changing the way that the information endowment can be leveraged is likely to support an information-driven transformation of the related business processes that the PLC covers. This is the essential insight from the theory of informedness we mentioned earlier. It will also change the competitive structure of the related supply chain ecosystem of firms. This will allow them to achieve stability in their businesses through their new capacity to create sustainable value for their partners and consumers in the market [7]. Another new aspect that we have considered is related to PLC end-of-life activities, and others that enable them to make heightened commitments to environmental practices. We hope this will prolong the product lifecycle for many products through timely services, and appropriate refurbishment, reuse and recycle activities. This way, industry-based product practices will come more into line with the agenda of UN, WTO and other global bodies for improving sustainability in the global economy.

Our blockchain-IoT architecture covers all six stages of the PLC to which a supply chain manufacturer and the wider set of stakeholders connect. It provides a distributed and decentralised public ledger for the sharing of product-related information amongmstakeholders in a transparent and secure manner. This makes it possible to enhance consumer informedness by increasing PLC transparency, and supports product authentication, fighting counterfeit products, ensuring fair trade, and building evidence of ecology-focused management practices.

The proposed platform offers enhanced informedness about products to all the stakeholders. This will open up a lot of business opportunities to the companies and support increased satisfaction for their customers. The architecture also is capable of offering any new services that are needed to be synchronised across the stakeholders' legacy systems and yet offers high security and transparency. We have shown how product authentication can be achieved using the proposed architecture, which supports an enhanced supply chain management while still using legacy systems. Such an architecture can improve the overall security level and increase the trustworthiness of the manufacturer and the product.

Several of the use case scenarios we discussed are supported by IoT solutions that aim to establish platforms to capture value created of IoT devices attached to product. The role of blockchain in the architecture is to add a standard ledger to the platform so it can operate across the PLC. This will create challenges for taking advantage of the business opportunities that arise in various contexts though. We also note that only meta-information and not the related detailed information need to be shared via the blockchain. Instead, it can be kept on the platform to support stakeholder value appropriation and promote opportunities for new business.

It is important to keep in mind that blockchain technology is still nascent in its development though. Indeed, it has a long way to go before it can become a more mature technology or an industry standard. And yet, the process of standardizing the blockchain platform already has started. Still, existing blockchain frameworks lack interoperability, which is a problem for connecting systems across firms. Toyoda et al. [31] have argued that public blockchains cannot prevent counterfeiters from impersonating the employees of other companies because a centralized, trusted third-party to enroll a manufacturer is required. Permissioned blockchains do not suffer from the same problem though. Nonetheless, blockchain platforms still face various vulnerabilities, such as non-ethical activity, transaction privacy leakages, network penetration due to consensus mechanism issues, stack overflows, and immutable bugs related to smart code [19]. In this context, heterogeneousIoT devices create readily-identifiable points of potential failure. Taken together, the still-weak status of their interoperability capabilities, less-than-best security protocols, and self-defense limitations can make IoT devices insecure [17]. To conclude, in our future research, we expect to involve more companies that provide more information on the utilization of our prototype.

References

[1] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," *Intl. J. Res. Eng. Tech.*, 5(9), 2016, 1–10.

[2] N. Alzahrani and N. Bulusu, "Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain," in *Proc. 1st Wkshp. Cryptocurr. and Blockchains for Distrib. Sys. New York: ACM Press*, 2018, 30–35.

[3] J. B. Bolten, "E-authentication guidance for federal agencies–memorandum to the heads of all departments and agencies," Technical report, Office of the President, Washington, DC, 2004.

[4] W. Burr, D. F. Dodson, E. Newton, R. Perlner, W. Polk, S. Gupta, and E. Nabbus, "Electronic authentication guideline," Special publication 800-63-2, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Boulder, CO, 2013.

[5] W. Cao, L. Zheng, H. Zhu, and P. Wu, "General framework for animal food safety traceability using GS1 and RFID," in *Proc. Intl, Conf. Comp. and Comp. Tech. in Agric.* Berlin: Springer, 2009, 297–304.

[6] T. M. Choi, "Blockchain technology supported platforms for diamond authentication and certification in luxury supply chains," *Transp. Res. Pt. E: Logist. Transp. Rev.*, 128, 2019, 17–29.

[7] E. K. Clemons, R. M. Dewan, R. J. Kauffman, and T. A. Weber, "Understanding the information-based transformation of strategy and society," *J. Mgmt. Info. Sys.*, 34(2), 2017, 425–456.

[8] J. Goldenberg, D. Mazursky, and G. Jacob, *Creativity in Product Innovation*. London: Cambridge University Press, 2002.

[9] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comp. & Sec.*, 78, 2018, 126–142.

[10] M. Holler, L. Barth, and R. Fuchs, "Trustworthy product lifecycle management using blockchain technology nist: Experience from the automotive ecosystem," in *Product Lifecycle Management : The Case Studies (Vol. 4)*. Springer, 2019, 13–19.

[11] M. Holler, E. Stoeckli, F. Uebernickel, and W. Brenner, "Towards understanding closed-loop PLM: The role of product usage data for product development enabled by intelligent properties," in *Proc. Bled eConf.* Slovenia, 2016, 13.

[12] S. Huh, S. Cho, and S. Kim, "Managing iot devices using blockchain platform," in *Proc. 19th Intl. Conf. Adv. Comm. Tech.* Washington, DC:IEEE Comp. Soc. Press, 2017, 464–467.

[13] T. Jensen, J. Hedman, and S. Henningsson, "How TradeLens delivers business value with blockchain technology." *MIS Qtrly. Exec.*, 18(4), 2019.

[14] A. Juels, "RFID security and privacy: A research survey," *IEEE J. Select. Areas in Comm.*, 24(2), 2006, 381–394.

[15] H. B. Jun, J. H. Shin, D. Kiritsis, and P. Xirouchakis, "System architecture for closed-loop PLM," *Intl. J., Comp. Integr. Mfg.*, 20(7), 2007, 684–698.

[16] Z. C. Kennedy, D. E. Stephenson, J. F. Christ, T. R. Pope, B. W. Arey, C. A. Barrett, and M. G. Warner, "Enhanced anti-counterfeiting measures for additive manufacturing: coupling lanthanide nanomaterial chemical signatures with blockchain technology," *J. Mat. Chem.*, 5(37), 2017, 9570–9578.

[17] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Fut. Gen. Comp. Sys.*, 82, 2018, 395–411.

[18] T. Li, R. J. Kauffman, E. Van Heck, P. Vervest, and B. G. Dellaert, "Consumer informedness and firm information strategy," *Info. Sys. Res.*, 25(2), 2014, 345–363.

[19] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Fut. Gen. Comp. Sys.*, 107, 2017, 841–853.

[20] X. Liu, W. Wang, H. Guo, A. V. Barenji, Z. Li, and G. Q. Huang, "Industrial blockchain-based framework for product lifecycle management in industry 4.0," *Robotics and Comp. Integr. Mfg.*, 63, 2020, 101897.

[21] McKinsey & Co., "The circular economy: Moving from theory to practice," Center for Business and Environment, New York, October 2016.

[22] PAT Research, "Top 19 product lifecycle management software," Toronto, 2020.

[23] G. Power, "Anti-counterfeit technologies for the protection of medicines," World Health Org., Geneva, 2008.

[24] K. Salah, N. Nizamuddin, R. Jayaraman, and M. Omar, "Blockchain-based soybean traceability in agricultural supply chain," *IEEE Access*, 7, 2019, 7273–7285.

[25] J. Shim, R. Sharda, A. M. French, R. A. Syler, and K. P. Patten, "The Internet of Things: Multi-faceted research perspectives," *Comm. AIS.*, 46(1), 2020, 21.

[26] M. Sidorov, M. T. Ong, R. V. Sridharan, J. Nakamura, R. Ohmura, and J. H. Khor, "Ultralightweight mutual authentication RFID protocol for blockchain enabled supply chains," *IEEE Access*, 7, 2019, 7273–7285.

[27] S. Singh, S. C. Misra, and F. T. Chan, "Establishment of critical success factors for implementation of product lifecycle management systems," *International Journal of Production Research*, 58(4), 2020, 997–1016.

[28] J. Stark, "Product Lifecycle Management," in *Product Lifecycle Management (Vol. 2)*. Berlin: Springer, 2016, 1–35.

[29] S. Terzi, A. Bouras, D. Dutta, M. Garetti, and D. Kiritsis, "Product lifecycle management: From its history to its new role," *Intl. J. Prod. Lifecycle Mgmt.*, 4(4), 2010, 360–389.

[30] F. Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of Things," in *Proc. 2017 Intl. Conf. Serv. Syst and Serv. Mgmt.* Washington, DC: IEEE Comp. Soc. Press, 2017, 1–6.

[31] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system for anti-counterfeits in the post supply chain," *IEEE Access*, 5, 2017, 17 465–17 477.

[32] United Nations Environment Programme (UNEP), "Sustainable production and consumption: A handbook for policymakers," Nairobi, Kenya, 2015.

[33] L. Yang, P. Yu, W. Bailing, Q. Yun, B. Xuefeng, Y. Xinling, and Y. Zelong, "Hash-based RFID mutual authentication protocol," *Intl. J. Sec. & Its Appl.*, 7(3), 2013, 183–194.