Exploring privacy challenges of blockchain-based supply chains in the pharmaceutical industry

Author: Jean Gal Supervisor: Tianyu Li Responsible Professor: Zekeriya Erkin
, {Tianyu.Li, Z.Erkin}@tudelft.nl
Cyber Security Group, Department of Intelligent Systems, Delft Univeristy of Technology

27/06/2021

Abstract

Blockchain is an expanding technology that offers benefits when applied to supply chain management. This distributed ledger technology is combined with supply chains for its intrinsic characteristics. For instance, traceability, immutability, and more are discussed. In this paper, we first present privacy-related challenges encountered when applying blockchain technology to this work. These include dealing with immutable data, providing the anonymity of end-users, as well as their accountability. The risks associated with the leakage of medical data show the necessity of protecting patient privacy. For this sake, we delve into blood donation, clinical trial, PPE tracking supply chains and highlight their privacy requirements. We introduce anonymous signatures, mixing services, and other cryptographic techniques, which satisfy these requirements through local anonymity, unlikability, but also accountability in specific contexts.

1 Introduction

A supply chain can be defined as all the steps it takes to sell products to a customer from the acquisition of raw materials [1]. It includes the transformation of these materials and the transportation of finished products to customers and more (e.g., marketing and customer service). The discipline consisting of managing the flow of goods, revenue, and information in a supply chain while reducing the costs as much as possible is called Supply Chain Management (SCM). In the scope of this project, we limit ourselves to the information flow and discuss the challenges related to privacy. The flow of information can contain a company's private data, which can be sensitive information. Hence, specific attention should be taken to hide that private data. If privacy-preserving techniques are not implemented, external parties can unfairly exploit that information for personal benefits, which can be considered a source of competitive advantage in certain scenarios [2].

One of the recent technologies used in association with Supply Chains is Blockchain and has received more and more attention from researchers and engineers in the last 10 years [3]. It offers the following relevant properties:

- Traceability brings the ability to trace back products from their origin.
- Immutability ensures the information has not been tampered with.
- Decentralization removes the reliance on third parties.
- Transparency allows information on a network to be transparent and accessible.

Thanks to Blockchain's decentralized structure and consensus mechanism, this technology is applied in supply chains to solve their challenges. These include increasing supply chain visibility, traceability and also reducing errors and attacks [4]. In addition, blockchain technology is used as "a source of verification for reported transactions." [5], which eases the audit process, also vital for SCM [6].

Blockchain technology combined with supply chains is used in diverse industries such as the food industry, logistics, and healthcare. To underline the

importance of privacy in blockchain-based supply chains, we decided to target a field where user privacy is more than a must: Healthcare. Data breaches in healthcare expose highly sensitive data, and this industry is one of the most common targets of criminals. Indeed, healthcare data can be sold on the dark web at the highest price, it can be used to charge a ransom and to carry out financial or identify fraud [7]. As a result of technology improvements, paper-based systems were replaced by electronic health records [8], which enable uninterrupted access to patient's health information. However, this new system also brings privacy-preserving challenges (e.g., hiding these records from unauthorized users).

This paper aims to answer the following 3 research questions. (1) What are the privacy-related challenges in supply chains based on distributed ledger technology? (2) In which scenarios of healthcare supply chains are privacy important (3) Which techniques can preserve user privacy of healthcare patients in blockchain-based SCM? To answer these research questions, we begin this paper with a methodology and preliminary section to explain our research procedure and define the main concepts of this work. Then, we describe the main identified privacy challenges of blockchain-based SCs before presenting pharmaceutical SC and their need for privacy measures. Next, we overview a list of techniques that preserve user privacy in the later section. Finally, we reflect on the responsibility of our research and conclude this paper by associating methods to the pre-established pharmaceutical supply chains.

2 Methodology

We chose to carry out a survey or literature review to answer the questions asked in this paper and find existing privacy-preserving techniques. At first, we identify the steps followed to gather sufficient knowledge of the concepts and organize the research. Secondly, we overview the methods and tools used to find relevant works.

2.1 Research Steps

In this paper, we identify privacy threats or issues provoked by blockchain technology in healthcare supply chain management. Accordingly, the objective is to offer solutions solving one of these identified challenges. Therefore, before presenting privacy-preserving techniques, we must understand the need for combining these technologies and what they require from another. Hence, the research was carried out through the following steps:

- Research about Supply Chain, Blockchain, and their association.
- Identify the current requirements of supply chain management and explore how blockchain could help fulfill those.
- Explore Supply Chain applications in healthcare and point out the importance of advanced privacy measures.
- Establish the majorly identified privacy challenges and research on existing solutions to theses.

At first, we provide an overview of the key concepts in the background information section, which contain the results of the first research step. Then, in step 2, we research the requirements of Supply Chain Management, such as traceability and privacy, before exploring existing SC applications in the healthcare industry and finding why privacy is important. Finally, we extract the main challenges, present an overview of them, and for the last one, expose prominent solutions.

2.2 Guidance to lead the research

The research platforms or databases we used to find papers were most commonly Google Scholar (https://scholar.google.com) and World Wide Science (https://worldwidescience.org). Once on these platforms, we applied filters to narrow down the scope of the research and find relevant papers. A filter was the language of the articles, for which we only targeted ones published in English. Another filter was the period of the publications, which we choose to be between 2017 and 2021 for papers involving blockchain technology and current applications. However, we softened this filter for more general research on concept definitions, the healthcare industry, and some aged cryptographic techniques. Lastly, we also explored paper references to find the origin of the information some works present.

3 Preliminaries

Before we dive into the privacy challenges and their respective privacy-preserving techniques, we provide an explanation of this work's definitions. We clarify the concepts behind blockchain technology and finally describe a supply chain, their participants, and different flows.

3.1 Supply Chain

Figure 2 illustrates the general topology of supply chains and its five types of participants. We first have the suppliers who deliver the raw materials. Then there are the manufacturers who process these resources and transform them into products. Next, the distributors send the goods to retailers who sell them to the public, with the end consumers being the last entity in this process.

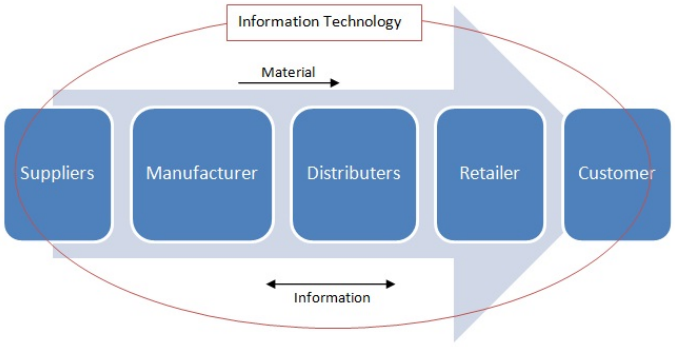

Figure 1: Supply Chain Entities [9]

Standard supply chains have three different flows or scopes. The financial flow is the flow of payments and currency exchanges. In addition, the flow of materials is all the processes of transferring and distributing goods, while the information flow includes all information generated in the supply chain activities. Privacy is particularly crucial when it comes to the exchange of information because it can be a consumer's personal data, sensitive product description, or even trade secrets [10]. The constant flow of information allows institutions to keep track of stock, production, and how the information is handled and accessed. However, stolen data or defects in the information flows can lead to companies losing great amounts of money (e.g., stocks are empty).

3.2 Blockchain

Ghiro et al. describe blockchain as a data structure used to register transactions. It is a distributed system that generally consists of the 2 following components [11]:

- A **peer-to-peer network** in which the nodes participate by reading and writing transactions to the blockchain. Each node owns copies of the registered information and makes blockchain a shared ledger of transactions.
- A **consensus protocol** that dictates if a transaction can be added to the network. Decisions are made upon a set of rules or policies enforced by all nodes [11], specific to a blockchain.

Digital information is stored in the network in the form of blocks that are chained together. Those blocks are made of the subsequent three different parts [12]:

- By the mean of digital signature, blocks store information on the author of the transaction.
- Blocks reveal information about the transaction, such as the time and date they got built.
- Each block has a unique hash code that helps differentiate one from another (e.g., new block or altered block)

The immutable cryptographic signatures make the recording of information practically impossible to alter or to hack. Blocks tampered by unwanted parties will no longer be recognized as the original ones, and thus, we can identify the acted changes. Additionally, every time a transaction takes place, every participant receives a record of that transaction in their ledger. Thus, if a hacker desires to corrupt the system, it would need to modify all the blocks across every distributed copy of the chain [13].

4 Privacy challenges for blockchain based supply chains

We can define privacy as someone's right to keep their personal information secret. It includes the right to "be able to control who can see or use information about you." [14] but also allows users to

withdraw from a study, organization, or the public view. As an example, the General Data Protection Regulations (GDPR) state that one has the right to erase its private data.

We defined blockchain technology in section 3.2 and discussed its benefits, attributes, and why it is widely used. Yet, its inherent characteristics, such as traceability, transparency, and immutability, can lead to privacy-related challenges in supply chain management. In the following subsections, we describe some of the challenges encountered while conducting the research. The first challenge is to provide privacy when all data in the supply chain or blockchain should be traceable. How can we provide confidentiality and privacy when all transactions are made transparent? How can we make people accountable for their actions if we provide their anonymity? Finally, according to GDP Regulations, anyone should have the right to exercise over their data. To this extent, how can we provide privacy when all data posted on the blockchain is immutable, and more specifically, when it cannot be deleted?

4.1 Provide Information Privacy while making the supply chain traceable

With the tremendous amounts of data to handle inside supply chains, current and uprising supply chains strictly require a certain level of traceability. In real-time supply chain applications, it is necessary to find ways to trace back products to their origin and characteristics, that is, backward traceability. But it should also be feasible to find the location of products, namely forward traceability [15]. In both scenarios, the exchanged distribution information can happen to be private and still made public [21]. Thus, how and what techniques can be used to yield both traceability and privacy. That is, how can we ensure forward and backward traceability without leaking or giving access to private data (e.g., identity of a product owner).

4.2 Provide Transparency and Privacy of Transactions

Blockchain is a decentralized technology that does not rely on a trusted third party. However, trust is behind all business relationships and is especially important in supply chain management. A level of trust is required between the SC participants (e.g., medical patients trust the healthcare workers to send their medical records in time) such that the SC transactions happen right in time, as expected. Thus, how does blockchain ensure the intended level of trust? As stated by AlTawy & Gong (2019) [16], "transaction transparency is the powerhouse of trust in blockchains.". Transaction transparency is of great importance because it provides auditability to the blockchain. That is, it allows to perform audits of the ledger containing all transactions [31]. Nevertheless, this necessitates transaction privacy and is highly desirable in healthcare scenarios. We can't make all transactions fully transparent to every user, as some are desired to be kept unknown [17]. Thus, we must both provide transaction privacy and transparency.

4.3 Provide Information Privacy in an Immutable Blockchain

The next challenge we discovered is finding a middle ground between privacy and immutability. Article 17 of the General Data Protection Regulations, Right to erasure, states that "the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay." [29]. However, we previously discussed that immutability is one of the built-in characteristics of blockchain. This feature can "collide with the fundamental principles of the right to be forgotten" [30] imposed by the GDPR because it is what makes blockchain unique, that is, making all transactions or data unforgettable and unalterable.

4.4 Provide both Privacy and Anonymity of the involved entities

The last challenge we address and attempt to solve in section 6 is providing the privacy and anonymity of the participating entities. Privacy and anonymity are two different concepts, but the combination of both is often required. On the first hand, privacy hides your actions from the public but potentially lets participants know your identity. On the other hand, to yield anonymity does not imply hiding your actions but rather masking the person at the origin of his activities or transactions [19]. Thus, how can we ensure that the concerned entities are not identified through the exposure of information? In addition, accountability can be defined as the obligation to take responsibility for your actions. Hence, we deduce the need to find a compromise

between both characteristics. How can we at the same time dissociate the identity of someone from their actions and also make them take responsibility in the context of a dispute or problem?

5 Pharmaceutical Supply Chains and their relation with Privacy

Healthcare is a delicate field, and data breaches are even more dangerous in this sector. From 2005 to 2019, more than 60% of data breaches occurred in the healthcare (MED) department [8] which accounted for 3912 out of the 6355 data breaches. Hence, we orientate the focus of our work towards patient privacy, namely, the healthcare patients located at the end of the supply chain. Established patient privacy lets patients decide to what extent their health information can be accessed and when. They are the owners of their patient healthcare information (PHI), which should only be shared with entities that "need it to provide or improve medical care" [28], and patients should also have the right to withdraw (i.e., from a clinical trial).

Now that we explored the privacy challenges related to the use of blockchain technology in supply chains in the last section, we delve into use cases in the pharmaceutical industry. To underline its need for privacy, we target three prominent supply chains, Blood Donation, Clinical Trials, and Personal Protective Equipment Tracking. For each of them, we describe how they operate, identify the level of privacy they require, and relate to the challenges of establishing user privacy.

5.1 Clinical Trials

Clinical Trial Supply Chain management corresponds to the handling of clinical trials, that is, "research studies performed in people that are aimed at evaluating a medical, surgical, or behavioral intervention" [22]. They are conducted with the primary objective of testing new treatments or vaccines to research their effectiveness, safety and evaluate if there are any side effects. Logically, the main actors of these trials are the patients, and it would not be possible without them. Medical institutions collect the data at the end of the supply chain for analysis and analytic. Hence the priority of storing and exchanging their data privately for different reasons. One is the trust the patients give to an organization because if they find out their data gets leaked, medical patients will be less prone to participating again. As reported by the health company CROS NT [24], there are three levels of patient data:

- Level 1 - Direct identifiers such as biometrics information
- Level 2 - Indirect identifiers such as date of birth or body measurements.
- Level 3 - Risk of data linking by combining more than one data point.

To this end, we need a data anonymization process to keep patient data private, which can be first attained through de-identification at level 1. De-identification implies the removal of those direct identifiers to hide a patient's identity. However, we must also delete "the links between the de-identified datasets and the original dataset" [24], that is, a type of data anonymization (i.e., unlinkability).

5.2 Blood Donation

In the healthcare sector, blood is required to be available at all times and is not replaceable. It is vital for human life as it carries oxygen and nutrients to sustain and supply our body parts. The distribution of blood on demand is "directly or indirectly connected to its supply chain." [22]. Hence, blood donation supply chain management (BDSCM) involves safe storage, distribution, and tracing back information at each stage of the blood supply [22]. The use of blockchain technology for BDSC can allow for verification of blood origin through traceability and validation of blood quality. It can considerably benefit patient's health by ensuring blood safety and reducing the risks of infection. Regarding our identified privacy challenges and this type of supply chain, we pay specific attention to the privacy of the donors in the system, that is, patient privacy and anonymity. On the one hand, donors should have the right to keep their identity hidden, and undesirable entities should not have the possibility of linking personal information to donors. On the other hand, in unexpected scenarios such as donors providing inaccurate information, the circumstances might require revealing their identity and making them accountable.

5.3 PPE Tracking

Until now, we underlined the importance of healthcare patients' privacy, but we also need to keep an eye on the healthcare workers. Personal Protective Equipment (PPE) is what "protects healthcare workers from infection" and is a "critical component of infection control strategies in healthcare settings" [26]. The workers are indirectly or directly in contact with the patients and have high risks of exposure. Moreover, with the recent COVID-19 pandemic, PPE demand increased drastically and resulted in "critical shortages for healthcare and frontline workers." [27]. With everyone buying their products online, external parties can exploit the situation to disrupt the supply chain management, and for example, put counterfeits up for sale. These conditions make it compulsory to find efficient ways of privately sharing data across the supply chains and protect user privacy. Indeed, external parties should not manage to identify the ongoing owners of the protective equipment who should be anonymized.

6 Privacy-preserving techniques: Benefits and Drawbacks

We were able to overview the privacy-related challenges in the previous section, but we decided to choose one to assess more in-depth: anonymity. At first notice, one may think that complete anonymity is essential in Supply chains, but this is mostly not the case. Blockchain-based PPE Supply Chains can help us prove our point. When wanting to track equipment (e.g., it was lost) and to find which entity or institution possesses it, we need to identify the transaction parties in the blockchain. In similar scenarios, we need a solution that makes people accountable for their actions but makes it difficult or impossible for externals to track that data [16]. However, simple private-public key encryption models do not always hold up under GDP Regulations because, with the publicly available data and blockchain transactions, there exist methods to link public keys and individuals (Thomson Reuters, 2019). Yet, it should be impossible to prove that multiple outgoing transactions were sent by the same sender [33].

In this section, we review the existing techniques or cryptographic schemes that can satisfy some or all of the privacy requirements of the earlier described pharmaceutical supply chains. That is, not only anonymity but also unlinkability and accountability in some contexts. For each method, we emphasize its benefits and drawbacks. [33].

6.1 Pseudonymization

A simple technique approached in various papers is called pseudonymization and is used to mask the identity of a user. It consists of replacing the public key of the blockchain nodes with pseudonyms and "removing some of the information necessary to identify an entity." [19]. In PPE tracking scenarios, pseudonymization can allow identifying the current owners of medical equipment without storing their identifiers, which is the first step required to protect user privacy in the healthcare industry. However, this method guarantees anonymity but at a nonsufficient level. In a public blockchain where transactions are exposed, unlikability is not satisfied, and adversaries can unmask the users through their participation in transactions. Seh et al., (2020) reveal a list of attacks used to de-anonymize the users [17].

6.2 Zero Knowledge Proofs

Zero-knowledge proofs (ZKP), first proposed in the 1980s, is one of the most commonly used cryptographic technologies to preserve privacy. This method allows verifying a transaction without revealing its content. For each transaction, someone (prover) wants to prove something that needs to be verified by someone (verifier). With zero-knowledge proofs, blockchain participants can verify transactions without having access to their data, thus guaranteeing privacy and anonymity. Furthermore, ZKP's adopt the 2 following essential properties, completeness and soundness [34]:

- **Completeness** is achieved when all valid statements are also provable. In other words, true statements leave verifiers convinced.
- **Soundness** is achieved when all invalid statements are not provable. Namely, it is not possible to persuade the verifier that a false affirmation is true.

Further improvements have been made to this method such as Non-Interactive Zero-Knowledge Proofs (NIZK), which conduct to "users not participating in the transaction not being able to access the original content of the transaction" [19].

6.3 K-anonymity

Sweeney (2002) describes a scenario in which a user is re-identified by establishing links on attributes shared through medical records. This same work then presents a protection model that ensures the unlinkability required, the k-anonymity model. For this sake, consider a table where each column is a record of data that belongs to a user. The k-anonymity model seeks to make all records indistinguishable from the table's other (k-1) records and is achieved by masking the user's sensitive information. Two simple methods are applied to achieve k-anonymity, generalization, and suppression:

- Generalization consists of swapping specific values by more general ones. For example, instead of keeping the age values directly on the table, they can be replaced by an age interval (e.g., under 20 years old).
- Suppression instead removes information from the table. Keeping the previous example, one might choose to remove the age values from the table. Depending on the situation, we decide which attributes are sensitive to show and remove them.

6.4 Mixing Services

Another mechanism used to tackle the linking of senders and receivers through public and transparent transactions is Mixing Services. This method was introduced by Chaum in 1981 and consists of blurring the relations between the transaction participants through a mixer. Mixers act as intermediaries that hide the content of a transaction, as well as the participants. This is achieved by outputting items or transactions in random patterns [17], which makes the linking complicated. This mechanism provides anonymity and unlikability but relies on a trusted third party, thus bringing other challenges. An example is an attack of a single mixer which can be solved by linking different intermediaries together.

We find two types of mixing services, centralized and decentralized ones. There exists available centralized mixing platforms that carry out the task just described, that is, mixing transactions anonymously. However, as stated by Seh et al., (2020) in a survey [17], the mixing server becomes a point of failure "vulnerable to denial of services (DOS) attacks" and a "bottleneck of the distributed blockchain network.". On the other hand, instead of having a third party do the job, decentralized mixing services tackle this issue by having a set of peers anonymously publish their transactions at the same time. Though common applications of decentralized mixing services such as CoinJoin can be more sensitive to de-anonymization [37].

6.5 Anonymous Signatures

The concept of digital signature was described for the first time by Whitfield Diffie and Martin Hellman but was not into practice. Methods for digital signatures were later introduced, such as the Rabin signature algorithm and RSA signatures which are based on the RSA public-key cryptosystem. Figure 2 presents the fundamental steps to authenticate an entity that signed a message. Through this mechanism, any modification to a message involves a change in its hash, which allows verifying the sender's authenticity.

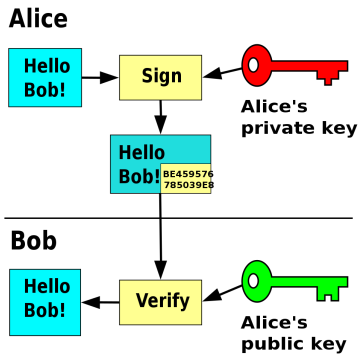

Figure 2: Digital signature scheme

In this subsection, we target two anonymous signature schemes that ensure anonymity, ring signatures, and group signatures.

6.5.1 Ring Signatures

Ring signatures work similarly to k-anonymity such that it selects a closed group of users with whom it is difficult to identify which participants originate the transactions. Compared to mixing services, there is no group manager, and participants can themselves create their "ring" of users [36]. It implies that this mechanism is suitable for public blockchains [36] and that complete anonymity is possible at the expense

of accountability. In the context of a patient deciding to remove his participation from a clinical trial, this type of digital signature can hide the patient's private data from both researchers and externals. On a related note, there exist ring signature schemes that sacrifice anonymity in exchange for traceability. Fujisaki Eiichiro and Suzuki Koutarou (2007) describe a traceable ring signature model in which identity can be revealed in specific scenarios and thus avoid "excessive anonymity" [39].

6.5.2 Group Signatures

The second type of signature scheme we observed is group signatures. It was proposed for the first time in 1991 by David Chaum [40], and compared to ring signatures, this scheme relies on a trusted third party to supervise the group (group manager). Group signatures are relevant in terms of anonymity, unlikability and accountability because they follow the next three properties. At first, from Chaum's definition (1991), signing messages is only possible for the group members. Then, signatures are only verifiable by the group members who also do not know who is at its origin. Users are kept anonymous from both externals and group members. Finally, group signatures are unlockable in scenarios where accountability is required. They allow revealing a person's identity and would fit PPE tracking supply chains. Furthermore, Benoit Libert and Damien Vergnaud (2009) describe an extended solution of this scheme to preserve user privacy even after members leave the group, whether they are honest users or misbehaving users [41].

7 Responsible Research

By cause of conducting a literature survey, we came across many different works, and special care needs to be taken at each step of the process. We must have a responsible approach, that is, no impersonating authors of other studies, aligning the research outcomes with ethical values, having socially acceptable behavior, and more. For this sake, we adopted specific measures to execute a responsible research procedure. All found technical solutions or techniques were referenced and initially identified from the works cited in this paper. We do not pretend to be at the origin of the privacy-preserving methods analyzed. Finally, we adopted the latest version of the APA publication manual for citations and references, APA 7th edition. We show this information for easy access to the resources exploited and allow for cross-referencing.

8 Conclusion & Future Works

By contrast to ordinary supply chains, blockchain technology does not require trust in any third party. Instead, trust comes from the transparency of blockchain transactions. With most supply chain applications maintaining a constant flow of information, private data must be handled and shared carefully.

Healthcare supply chains are even more craving to protect user privacy due to the value and worth of healthcare information. This type of data is eminently sensitive and should remain hidden to external parties who can, as an example, make a profit out of it. Hence, privacy is critical when handling patient information in pharmaceutical supply chains, such as sharing Electronic Health Records (EHR).

In this paper, we have shown how to preserve user privacy through methods and techniques bringing anonymity. Pseudonymization is one of them but still allows externals to link participants to their transactions. In clinical trial Supply Chains where EHRs are often shared, the anonymity of users should be sturdier. Hence, techniques such as ring signatures would be more adapted due to their practically complete anonymity. However, different supply chain scenarios, being PPE tracking or Blood Donation, do not require complete anonymity for their patients. Blood donators or PPE owners should be traced back and made accountable when needed. For instance, group signatures allow revealing the identity in the context of a dispute and are more suitable in these scenarios. Finally, for future work in this field, we plan to tackle the risks related to third parties and centralized services. Group signatures or centralized mixing services may validate the requirements but, due to their need for a third party, these techniques can have higher risks and threats of leaking user data. The protection of private data is then dependent on the security level of the mediator or the services used.

References

[1] Larson, P., & Rogers, D. (1998). Supply Chain Management: Definition, Growth and Approaches. Journal of Marketing Theory and Practice, 6(4), 1-5. Retrieved June 27, 2021, from http://www.jstor.org/stable/40469931

[2] M. Ahluwalia, Z. CHEN, A. Gangopadhyay, & Z. GUO. (2007). Preserving Privacy in Supply Chain Management: A Challenge for Next Generation Data Mining. Proceedings of National Science Foundation Symposium on Next Generation Data Mining and Cyber-Enabled Discovery for Innovation NGDM 2007. 1-5. Research Collection School Of Computing and Information Systems.

[3] Chang, S., & Chen, Y. (2020). When Blockchain Meets Supply Chain: A Systematic Literature Review on Current Development and Potential Applications. IEEE Access, 8, 62478-62494. https://doi.org/10.1109/access.2020.2983601

[4] Hald, K. S., & Kinra, A. (2019). How the Blockchain Enables and Constrains Supply Chain Performance. International Journal of Physical Distribution & Logistics Management, 49(4), 376-397. https://doi.org/10.1108/IJPDLM-02-2019-0063

[5] Psaila, S. (2021). Blockchain: A game changer for audit processes? | Deloitte Malta | Audit & Assurance. Deloitte Malta. Retrieved 22 June 2021, from https://www2.deloitte.com/mt/en/pages/audit/articles/mt-blockchain-a-game-changer-for-audit.html.

[6] Sezer, B.B., Topal, S., & Nuriyev, U. (2021). An Auditability, Transparent, and Privacy-Preserving for Supply Chain Traceability Based on Blockchain. ArXiv, abs/2103.10519.

[7] Schafer, A. (2021). Importance of Data Privacy in Healthcare + 3 Data Security Tips. Soscanhelp.com. Retrieved from https://www.soscanhelp.com/blog/importance-of-data-privacy-in-healthcare.

[8] Seh, A., Zarour, M., Alenezi, M., Sarkar, A., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare Data Breaches: Insights and Implications. Healthcare, 8(2), 133. https://doi.org/10.3390/healthcare8020133

[9] Maheshwari, N. (2021). Information Technology - Transforming Supply Chain | Business Article | MBA Skool-Study.Learn.Share.. MBA Skool-Study.Learn.Share. Retrieved from https://www.mbaskool.com/business-articles/operations/1241-information-technology-transforming-supply-chain.html.

[10] Bhargava, B., Ranchal, R., & Ben Othmane, L. (2013). Secure information sharing in digital supply chains. 2013 3Rd IEEE International Advance Computing Conference (IACC). https://doi.org/10.1109/iadcc.2013.6514473

[11] Ghiro, L., Restuccia, F., D'Oro, S., Basagni, S., Melodia, T., Maccari, L., & Lo Cigno, R. (2021). What is a Blockchain? A Definition to Clarify the Role of the Blockchain in the Internet of Things. Retrieved from https://arxiv.org/abs/2102.03750.

[12] Chibuzor, E. (2020). Basics of Blockchain and Cryptocurrencies. Retrieved from http://dx.doi.org/10.13140/RG.2.2.21818.54728.

[13] Blockchain Explained: What is blockchain? | Euromoney Learning. Euromoney.com. (2021). Retrieved from https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain

[14] What is privacy?. OAIC. (2021). Retrieved from https://www.oaic.gov.au/privacy/your-privacy-rights/what-is-privacy/.

[15] Jansen-Vullers, M., van Dorp, C., & Beulens, A. (2003). Managing traceability information in manufacture. International Journal Of Information Management, 23(5), 395-413. https://doi.org/10.1016/s0268-4012(03)00066-5

[16] AlTawy, R., & Gong, G. (2019). Mesh: A Supply Chain Solution with Locally Private Blockchain Transactions. Proceedings On Privacy Enhancing Technologies, 2019(3), 149-169. https://doi.org/10.2478/popets-2019-0041

[17] Feng, Q., He, D., Zeadally, S., Khan, M., & Kumar, N. (2019). A survey on privacy protection in blockchain system. Journal Of Network And Computer Applications, 126, 45-58. https://doi.org/10.1016/j.jnca.2018.10.020

[18] Maouchi, M., Ersoy, O., & Erkin, Z. (2019). DECOUPLES. Proceedings

Of The 34Th ACM/SIGAPP Symposium On Applied Computing. https://doi.org/10.1145/3297280.3297318

[19] De Haro-Olmo, F., Varela-Vaca, A., & Alvarez-Bermejo, J. (2020). Blockchain from the Perspective of and Anonymisation: A Systematic Literature Review. Sensors, 20(24), 7171. https://doi.org/10.3390/s20247171

[20] Sahai, S., Singh, N., & Dayama, P. (2020). Enabling Privacy and Traceability in Supply Chains using Blockchain and Zero Knowledge Proofs. 2020 IEEE International Conference On Blockchain (Blockchain). https://doi.org/10.1109/blockchain50366.2020.00024

[21] Uesugi, T., Shijo, Y., & Murata, M. (2020). Short Paper: Design and Evaluation of Privacy-preserved Supply Chain System based on Public Blockchain. ArXiv, abs/2004.07606.

[22] What Are Clinical Trials and Studies?. National Institute on Aging. (2020). Retrieved from https://www.nia.nih.gov/health/what-are-clinical-trials-and-studies.

[23] Team, M. (2021). Information Technology - Transforming Supply Chain | Business Article | MBA Skool-Study.Learn.Share.. MBA Skool-Study.Learn.Share. Retrieved from https://www.mbaskool.com/business-articles/operations/1241-information-technology-transforming-supply-chain.html.

[24] Conducting Clinical Trials in the Era of Data Privacy and Anonymisation. CROS NT. (2021). Retrieved from https://www.crosnt.com/clinical-trials-in-the-era-of-data-privacy-and-anonymization/.

[25] Sadri, S., Shahzad, A., & Zhang, K. (2021). Blockchain Traceability in Healthcare: Blood Donation Supply Chain. 2021 23Rd International Conference On Advanced Communication Technology (ICACT). https://doi.org/10.23919/icact51234.2021.9370704

[26] Patel, A., D'Alessandro, M., Ireland, K., Burel, W., Wencil, E., & Rasmussen, S. (2017). Personal Protective Equipment Supply Chain: Lessons Learned from Recent Public Health Emergency Responses. Health Security, 15(3), 244-252. https://doi.org/10.1089/hs.2016.0129

[27] Omar, I., Debe, M., Jayaraman, R., Salah, K., Omar, M., & Arshad, J. (2020). Blockchain-based Supply Chain Traceability for COVID-19 PPE. https://doi.org/10.36227/techrxiv.13227623.v1

[28] (RSNA) Patient Privacy and Security of Electronic Medical Information. Radiologyinfo.org. (2021). Retrieved from https://www.radiologyinfo.org/en/info/article-patient-privacy.

[29] Art. 17 GDPR Right to erasure (ŕight to be forgotten)́ | General Data Protection Regulation (GDPR). General Data Protection Regulation (GDPR). (2021). Retrieved from https://gdpr-info.eu/art-17-gdpr/.

[30] The right to be forgotten as the main risk for blockchain technology. Medium. (2021). Retrieved 2 June 2021, from https://medium.com/coinmonks/the-right-to-be-forgotten-as-the-main-risk-for-blockchain-technology-4f6a7ecca14b.

[31] KRITIKOS, M. (2021). What if blockchain offered a way to reconcile privacy with transparency? | Policy Commons. Policycommons.net. Retrieved from https://policycommons.net/artifacts/1335700/what-if-blockchain-offered-a-way-to-reconcile-privacy-with-transparency/.

[32] Hardjono, T., & Smith, N. (2016). Cloud-Based Commissioning of Constrained Devices using Permissioned Blockchains. Proceedings Of The 2Nd ACM International Workshop On Iot Privacy, Trust, And Security. https://doi.org/10.1145/2899007.2899012

[33] Singh, K., Heulot, N., & Hamida, E. (2018). Towards Anonymous, Unlinkable, and Confidential Transactions in Blockchain. 2018 IEEE International Conference On Internet Of Things (Ithings) And IEEE Green Computing And Communications (Greencom) And IEEE Cyber, Physical And Social Computing (Cpscom) And IEEE Smart Data (Smartdata). https://doi.org/10.1109/cybermatics_2018.2018.00274

[34] Lindell, Y. (2010). Foundations Of Cryptography 89-856. https://u.cs.biu.ac.il/l̃indell/89-856/complete-89-856.pdf.

[35] SWEENEY, L. (2002). k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY. International Journal Of Uncertainty, Fuzziness And Knowledge-Based Systems, 10(05), 557-570. https://doi.org/10.1142/s0218488502001648

[36] Zhang, R., Xue, R., & Liu, L. (2019). Security and Privacy on Blockchain. ACM Computing Surveys, 52(3), 1-34. https://doi.org/10.1145/3316481

[37] Mikhelidze, G. (2021). Bitcoin Mixers: Centralized Vs. Decentralized Mixers - The Cryptonomist. The Cryptonomist. Retrieved from https://en.cryptonomist.ch/2020/08/15/bitcoin-mixers-centralized-decentralized/.

[38] Understanding Digital Signatures | CISA. Us-cert.cisa.gov. (2021). Retrieved from https://us-cert.cisa.gov/ncas/tips/ST04-018

[39] Fujisaki, E., & Suzuki, K. Traceable Ring Signature. Public Key Cryptography - PKC 2007, 181-200. https://doi.org/10.1007/978-3-540-71677-8_13

[40] Chaum, D., & van Heyst, E. (1991). Group Signatures. Advances In Cryptology - EUROCRYPT '91, 257-265. https://doi.org/10.1007/3-540-46416-6_22

[41] Libert, B., & Vergnaud, D. (2009). Group Signatures with Verifier-Local Revocation and Backward Unlinkability in the Standard Model. Cryptology And Network Security, 498-517. https://doi.org/10.1007/978-3-642-10433-6_34