Towards IoT and Blockchain Framework for Product Authentication

Short Paper - Research in Progress

Introduction

Product authentication is crucial for producers and retailers to bring trust among their customers, maintain their brand reputation as well as their profitable business model. The process of identifying counterfeit product items is complex due to multiple complex factors (such as lack of transparency, the dearth of resources and enforcement capabilities). The counterfeit and pirated items now constitute up to 3.3% of total global trade volume [1]. The impact of the counterfeit product has hampered the quality of products as well as damages the reputation of the producers (Nia and Zaichkowsky 2000; Wilcox et al. 2009). The range of product categories varies a lot and all most all the expensive product categories are susceptible to counterfeiting. Now consumers are willing to buy the products online and internationally due to competitive prices (Wilcox et al. 2009). Due to the affordable cost of international shipping, companies are increasingly selling their products at the global level. Thus, the market for counterfeits products is also increasing. Now, consumers are interested to verify the authentication of products and the sustainability-related claims. Therefore there is an imminent need for the development of a robust, scalable product authentication methods, using which brands and product manufactures can protect their intellectual property rights (IPR) by fighting (essentially by detecting and taking measures) against the counterfeiting. This research project, supported by the federation of industries, aims to increase the knowledge and perform experiments with newer technologies for product authentication (among other use cases) within small and medium enterprise (SME) segment. Large enterprises are investing heavily in product authentication by using new technologies to leverage a competitive advantage for their products. In contrast, SME does not have opportunities to make substantial investments into new technologies since the risk of failures is relatively high compared to other business investments. The research project aims to contribute with knowledge on Internet-of-Things (IoTs) and blockchain technology for product authentication and traceability. Thereby delivering increased value for the end-users/consumers and involving at least 87 SMEs in the project (at various stages of testing and evaluation process of the IoT-blockchain based product authentication in the whole product lifecycle using Action Design Research (ADR) methodology (Sein et al. 2011)).

Complementing IoT with blockchain has the potential to change how stakeholders share information via more trust, security, and accessible distributed ledger (Mackey and Nayyar 2017). Blockchain offers immutability and transparency for storing as well as accessing the product/consumer information/digital assets (Faber et al. 2019). Combining IoT and blockchain technology have been addressed by several authors within information system (IS) research domain (Shim et al. 2019), but the research is limited to electronic products as a relevant category for IoT devices. Our research focused on exploring IoT and blockchain for product authentication in the general consumer products category especially for fashion design and home interior (eg. furniture). The above discussion leads to our research question: *How the Internet of Things and blockchain technology can be used to support product authentication and sustainable product lifecycle management?*

This paper is organised as follows: first, we present the current state of the art in the Literature Review section followed by a description of our research methodology. In the Conceptual Framework section, we provide the theoretical elements behind our research, followed by a description of our framework and of the prototype implementation in the next section. Finally, we discuss our future research plans and conclude in the final section.

[1] https://www.oecd.org/newsroom/trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm

Literature Review

IoT devices are being used by various industries (such as transport and logistics, public sector, smart cities, industrial automation and consumer electronics) (Shim et al. 2019). The application of IoT devices for the industrial use has been identified through a literature review includes in smart homes/offices, transportation, gastronomy, water quality monitoring, elderly care, and in the airport (Thangavel et al. 2019). In food supply chains, the uses of passive Radio Frequency Identification (RFID) devices are well documented for food traceability (Cao et al. 2009). Tian (2017) have been extended the concept with active sensors and with the use of blockchain technology, where they proposed a solution based on blockchain with IoT for traceability in the food supply chain. However, their system is still in an initial stage of implementation. The use of IoT devices for consumer products are only predominant in consumer electronics, but not in any other categories. Therefore the use of IoT devices for consumer products (such as furniture and fashion goods) is a new and emerging phenomenon. According to Shim et al. (2019), "by providing the transparency across different stakeholders and across borders, the IoT implemented in combination with blockchain technologies can help to reduce misrepresentation and fraud in the entire supply chain". Huh et al. (2017), in the proposed solution, use the blockchain only to control and configure IoT devices, where they predicted that blockchain technology with its ability to create a distributed and tamper-proof digital record system, blockchain can turn IoT data traces from a security hazard into a reliable source of valuable data. Leveraging blockchain technology, IoT devices can send data to a private blockchain-based tamper-resistant database. Thereby, allow only authorized stakeholders to access and contribute IoT data without the need for central control and management (Shim et al. 2017). Thereby blockchain can become a solution to data security issues, identity management since blockchain technology can authenticate the identity of the nodes in a network and verify that only by authorized nodes can access data and thereby, maintain data privacy and access control (Shim et al. 2020). Beyond the apparent technological challenges, IoT and blockchain convergence poses organizational adoption challenges as well. Choi (2019) proposed an analytical model to study the blockchain-based supply chain operations for diamond authentication and certification process whereas Sidorov et al. (2019) presented an RFID protocol targeted for blockchain-based supply chain management system. In terms of product fake identification, Alzahrani and Bulusu (2018) proposed supply chain framework based on blockchain that can track products, detects modification, cloning and/or tag re-application attacks. Toyoda et al. (2017) proposes an RFID-attached products ownership management system which makes the efforts of counterfeiters to clone genuine tags redundant. With the action design research approach as a backbone, the focus of our research project is to advance the concept of IoT-based blockchain framework for product authentication, complemented with several iterations of prototype development, piloting to learn from a wide range of use cases in collaboration with the active participation of a large number of organisations. In addition to that, our research focuses on documenting product lifecycle in a holistic perspective using circular economy (CE) (Geissdoerfer et al. 2017) principles to keep track of product sustainability, serviceability, and recycling to promote environmental friendliness in the product manufacturing processes.

Research Methodology Approach

In this research project, we use the Action Design Research (ADR) methodology to develop an IoT and blockchain-based prototype for the interventions through iterations of build, measure and learn. ADR is an evolution and combination of the methods Design Science Research and Action Research (Cole et al. 2005). It specifies that evolutionary development cycle with iterations of Build, Intervention and Evaluation (BIE) and learnings from the cycles are used to improve the design of the next version of the IT artefact (Sein et al. 2011). With reference to our research project, Figure 1 illustrates the iterations for the prototype development using blockchain and IoT, which starts with the producers linking their product and authentication devices. Next, adding the suppliers with certificates of sustainability practices related to the material for the products. Further retailers are added to exhibit the information to the consumers. IoT devices will be included to track the supply chain activities, product authentication and the information will be pushed to the blockchain for maintaining the product lifecycle and history. The evaluations of artefact in each iteration will provide inputs to the design of the prototype in the subsequent

iterations. The aim of the project is to gradually involve more and more SME so that in total at least 80 SMEs will prototype and pilot the use of the new technologies within the two-year duration of the project (all contributing to the outcome of the project).

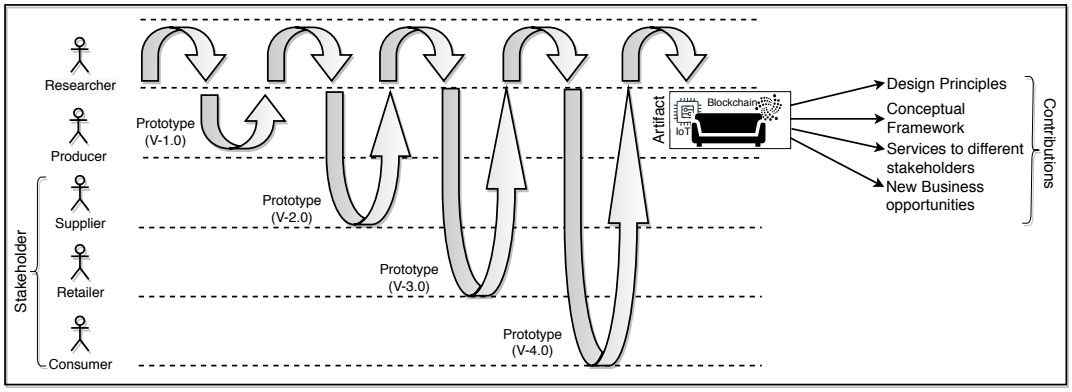

Figure 1. Project methodology based ADR principles (Sein et al. 2011)

Conceptual Framework

As depicted in Figure 2, product authentication can involve at least four high-level concepts: *1)* physical product, *2)* attached authentication device, *3)* digital information about historical records related to the product lifecycle (information that identify and authenticate the user and/or organisation providing the information, e.g. claiming the current (or previous) ownership(s)), *4)* different stakeholders who deal with the product lifecycle. The coupling between physical product and the authentication device in the physical space and the coupling between digital information and organisations and other stakeholders in the digital/virtual space is a novel aspect in the framework.

Physical Products

The products in this project mainly belong to two categories. The first category is home interior including furniture, where the physical circumstances are more spacious allowing devices to be attached even with batteries for power supply. Some products even already have the power supply built-in (such as lamps). The second category is fashion design within textile where the physical circumstances are limiting both with regard to physical size and available power supplies. Furthermore, the number of variants is relatively high, and the seasonal time window for collections (e.g. spring or summer) are relatively short compared to replenishing time. For both categories, there is a trend to include information about its provenance (such as certificates of fair trade and certificates of ecological materials). Many producers and retailers request options regarding the whole life cycle of the product as well.

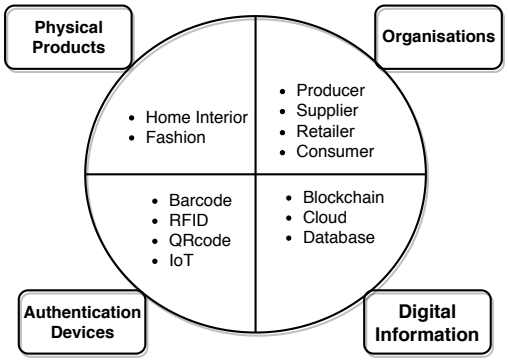

Figure 2. Conceptual Framework for Product Authentication

Authentication Devices

Authentication is one of the well-established technique to combat counterfeiting. First, the user scans the stock-keeping unit (SKU) code or other forms of code to explore the authenticity of the product and the authentication module generates a legitimate authentication request and sends it to the authentication service of the producer or brand owner, for further validation. The currently available product authentication solutions can be categorised into three segments (Power 2008). They are *1)* overt-technologies which are visible to the end-users for authentication verification (such as watermarks, holograms); *2)* covert-technologies which is not easily visible to the verifier but needs a special device to verify it (such as Security inks, digital watermarks); *3)* machine-readable technology where products can be tracked and/or traced (such as RFID).

Barcode is an inexpensive and faster way of tracking a product using an optical scanner. When a barcode optical reader scans the code, it turns the lines to text and sends the information to the backend systems, but one of the issues with barcodes is that they can be copied easily.

Radio Frequency Identification (RFID) provides unique identification/serial number to a product and it is one of the most popular/widely employed authentication mechanism for products (Juels 2006). It consists of a micro-chip to transmit the identification number and can only read by the devices using correct radio waves frequency. RFID can work either in *active* or *passive* mode. As the name suggests, the battery is needed to work as an active device which offers greater access range but active working hours primarily depends on the strength of battery-life. Passive RFID devices are used for smaller, cheap products with very long working duration (up to many years) while consuming the power from the reader itself. However, there is another hybrid form of energy consumption mode used in RFID devices.

Quick Response (QR) Code typically looks like multiple black squares arranged in a square shape on a white background. QR-code is a form of two-dimensional barcode. It offers instant access to the encoded information to users without using any special devices (unlike barcode reader or RFID scanner). QR code could either be static or dynamic type. In the static version, embedded data cannot be changed while the dynamic version allows data to be modified on the fly.

Internet of Things (IoT) devices provide built-in sensors features. However, the power supply and communication functions are critical for its practical use. There is a balance between power usage and communication possibilities, especially frequency. There are IoT devices with low power consuming communication capabilities that can operate for over 10 years. Communication also depends on the coverage which varies. In general, Wi-Fi and global system for mobile (GSM) networks are widely spread over the populated areas. Other dedicated networks dedicated to low-power consumption are available as well (e.g. Sixfox). The size and the weight of the IoT devices can be critical for attaching or embedding the device to/into a product.

Digital information

The digital information includes many variants of information across the product life cycle (right from suppliers to consumers in form of historical events), which support product authentication (eg. the time and location of products and certificates regarding the sustainable use of materials and so on). This digital information can be stored in a database, in the cloud or on a blockchain depending upon the purpose. For instance, the need for immutable/mutable data storage, based on compliance to data regulations and based on access to information for different stakeholders. Blockchain can be considered as a distributed database with state replication using a peer-to-peer protocol, where the transactions are the atomic changes to the data store which are grouped into blocks (Kuhn et al. 2019; Sun Yin et al. 2019). Blockchain technology offers five key features: *1)* immutability (data written to the network cannot be changed or deleted), *2)* decentralization (no single entity can achieve control over the network), *3)* transparency (data available to all network participants), *4)* pseudonymity (privacy and security for participant's identity) and *5)* chronology (transactions are time-stamped, can be traced back). Due to immutability nature of the blockchain, the type of information stored on it will be the data related to all events of the product lifecycle and other information that is in compliance with respective data regulations, but the nature of the

information stored on the blockchain will mostly be transactional.

Organizations and Users

Our framework consist of several stakeholders (such as material and component suppliers, product producers, retailers and consumers), who will be interacting with the artefact by accessing as well adding digital information to the proposed system. It should be noted that our framework goes beyond the traditional track-n-trace IoT-blockchain models and let the user as well as the producer to detect the counterfeit product before purchase (by a consumer) and also to detect the fake (by the producer if any), supplied parts for the final production respectively.

Initial Prototype

Following our conceptual framework, Figure 3 represents an overall flow in a product lifecycle, example indicating different stakeholders, product authenticating devices and different types of digital information about events that will be interacting with the proposed IoT blockchain-based platform. The lifecycle of a product starts with the suppliers registering information and certificates (such as Fairtrade) about the product materials on the IoT-blockchain platform. The producer uploads all the information related to the product when the product is produced. At later stage retailers and consumers will interact with the system either by adding digital information for events or by retrieving the information. Of course, there will a lot of digital trace and information produced and updated during intermediate stages (such as transportation/shipping of materials/components/products between different stakeholders). At all the stages, product authentication using various authentication devices (such as IoT, RFID) plays a central role. Using IoT-Blockchain ecosystem, access to information can be provided based on disparate

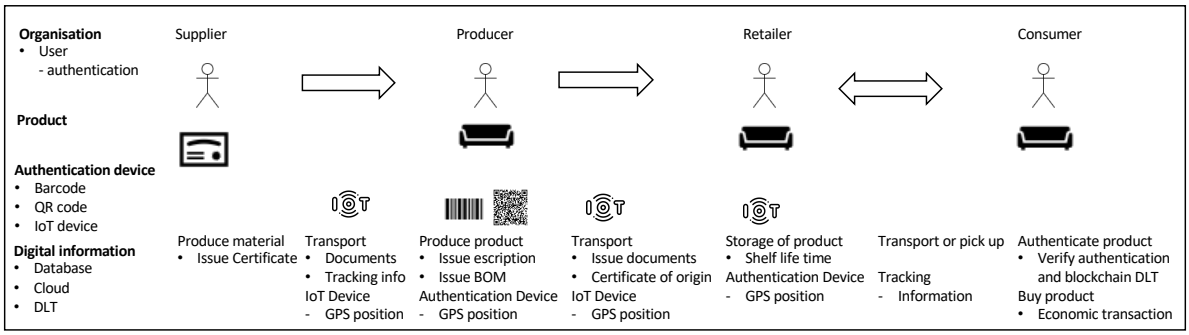

Figure 3. Flow indicating product lifecycle with authentication support

permissions. For example, buyers can have access to a portion of the stored digital information, while the producers, as well as the suppliers, can have access to their respective parts of the information. Such a way the entire stored digital information can be protected and simultaneously accessed by different stakeholders based on their access rights. It is worth to note that the personal information will not be stored into the blockchain due to the compliance with the personal data protection and regulatory mechanisms. However, such information will be stored in a secure location (such as local databases or cloud storage) and only the hash pointers to the personal information will be stored on the blockchain. As shown in the left part of Figure 4, digital information can have three protection levels: public, protected and private. As an example, in the case of the product purchase process, the public information can be available to any consumer who would like to buy the product which might include the informative text. The protected information would be available only when the buyer enters into an advanced state of the purchase process. Such protected information might have the authenticated certificates together with other pieces of information (such as designer name, patent's numbers and others). Finally, the private level holds confidential information (such as ownership, payment info and so on), only available after the purchase and authentication of the user. The types of information in these levels might vary from use case to use case. The right part of Figure 4 explains the working of the IoT-blockchain based authentication ecosystem from the consumer point-of-view. Suppose, a consumer wants to buy a product (sofa), then s/he

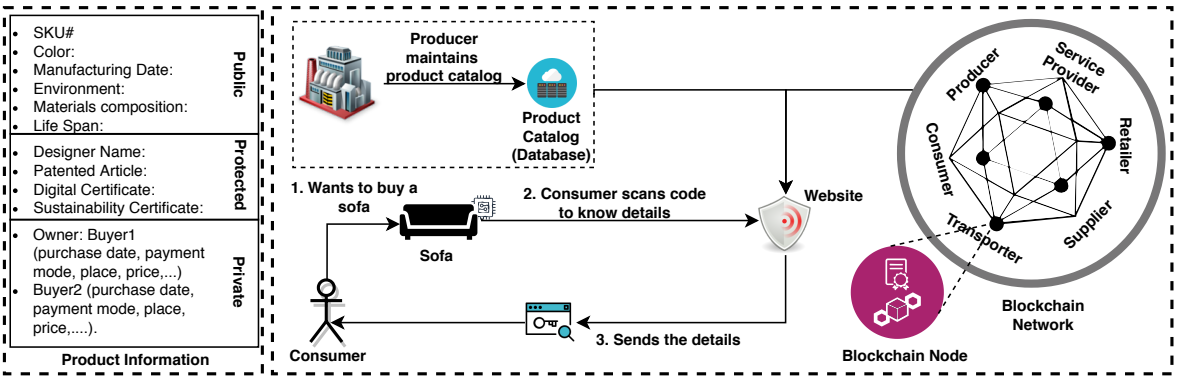

Figure 4. Product purchase: Information types (left), with authentication support (right)

scans the IoT device-generated QR code which is associated with sofa. The (authentic) product is already registered into the blockchain ecosystem (essentially to a product catalogue/database while the blocks of the distributed ledger will hold the reference to the database). An associated authentication process will be called and the code will be decoded/decrypted and searched in the database. If the product is an authentic item, it will return success. Furthermore, when the consumer scans code information will be available about a product's journey (including the certificates, ownership transfer history and others). Thus, the IoT-blockchain's use of dynamic QR codes to ensure that the product is authentic and has not been tampered with. Transaction metadata about the product (such as timestamps, owner id, transaction types (cash/card), product id, and place of purchase (or store location)) can be captured as well. The prototype has been implemented using the Hyperleder Fabric while using the Sigfox IoT devices as these authentication devices consume low power and can include a local channel (such as Bluetooth, Near Field Communication (NFC)) as per the need.

Discussion and Future Work

Product authentication is an novel research topic within IS research. This paper contributes to the research by providing a promising conceptual framework combining IoT and blockchain. As foreseen by prominent IS scholars (Shim et al. 2019; Shim et al. 2020; Shim et al. 2017), IoT and blockchain are promising technologies and in this research work, we proposed a conceptual framework based on these technologies for product authentication mainly targeting SME. The digital information about historical events on the blockchain complemented with authentication devices using IoT will increase the consumer's confidence by fighting against counterfeit products. Moreover, the product lifecycle historical events using product authentication are stored and accessible on blockchain. The blockchain is distributed across a huge number of nodes which makes it difficult to hack it and make it mutable. The initial prototype has been developed following the proposed conceptual framework based on ADR principles. The prototype helps the SME to understand and experiment the concept of product authentication using IoT and blockchain technologies which have proven to be crucial for their decision to engage themselves in the project and the testing of the prototype. Product authentication is crucial for producers and retailers to bring trust to their customers and maintain as well as to protect their brand together their profitable business model. Also it will support their sustainability claims (such as Fairtrade, ecological products). By providing the verifiable product authentication, the producers and the retailers can compete with fake and counterfeits products. The IoT devices are a crucial part of the conceptual framework because they relatively automatically create events on the blockchain (such as GPS signals about the product movement when transported from supplier to producer and later to retailer). For textile the IoT devices are currently too large to be part of the delivery to the end-user/consumer. For the home interior category, the IoT device can be part of and/or embedded in the product and sensor can provide information (such as statues and location (or removed outside the connected smart home)) that can be useful for the owner but also for service providers, producers and retailers which can prospectively become a new business opportunity.

In terms of Circular Economy (CE), the primary reduce, reuse and recycle concept of CE can be supported

using the IoT-blockchain based framework. Product recycling can be supported by the framework by alerting (eg. companies offering additional services as well as the current owner of the particular product when the time comes). Generally, such information (such as a specific day, month and year) can be encoded into the smart-contract of the blockchain via the input of the producer. Later, blockchain information can be used to send an alert to both of the consumer as well as the producer that time has come to recycle it. Such a way we can reuse some of the parts of the product and we can reduce the new resource requirements towards more sustainable production and product life. We believe that such an approach can reduce carbon (CO_2) emissions which further leads to innovative green technologies for climate change adaptation.

In addition to product purchase use case discussed previously, there are sevearal use cases where product authentication can be integrated to generate business value. They are re-sell, re-furbish, re-use, re-cycle, warranty, service, and insurance of products will be explored in future within the project. The use cases for furniture, fashion and the home interior have common elements eg. certificates of origin of materials but also different possibilities (about the options for IoT devices are more limited for fashion). Product authentication can be integrated into many activities in the product lifecycle. To integrate product authentication, we divided the product lifecycle into five parts: *1)* supply, *2)* produce, *3)* trade, *4)* use, and *5)* recycle and end of life. First, to add product authentication to the supply side to includes provenance of components and raw materials and their producers including their origin and authentication. Second, to add product authentication to the produce part includes authentication of producer(s) and the components and also the raw materials used concerning the supply side and tracking to the supply chain. Third, to add product authentication of the trade includes inventory storage, treatment and shelf life, and trade to new owners, who might re-trade/-sell the product. Fourth, to add product authentication for the use includes ownership, warranty, asset management of use. Fifth, to add product authentication at the end of lifecycle and/or recycle can include refurbishment/refresh and re-sell with a loop back to the trade part or dismantle into components or materials for either reuse to dispose of them in an environment-friendly manner. As stated earlier there is difference between fashion and home interior/furniture concerning if IoT device can be attached and/or embedded in the physical product. If an IoT device is embedded into furniture the possible use cases can be extended (such as enabling service offerings depending on the location of product which can create opportunities for new business models). The project is expected to generate innovations both in terms of use cases and new business opportunities that will help the SME to enhance their competitive advantage.

We plan to extend use cases and application of the conceptual framework for product authentication to other product categories either in subsequent projects or with research collaboration. Product authentication and fight against the counterfeits/fakes are increasingly getting important in the categories of medicine, food, and similar products. Similarly, authentication devices embedded in custom-build products (and variants) enables capturing of information which can be valuable feedback to the designers and developers for future improvements of the products. Another set of interesting business opportunities are in the product categories where IoT devices can be embedded, e.g. lamps where the IoT device can measure its capacity to light and that information can be used for generating a proposal for services which can be a whole new business model selling the services of light (instead of selling lamps) for example street light within a smart city. We expect to evolve the number of use cases to include asset management, refurbishment, recycle and scrapping products, based on the priorities of the more than 80 SME enrolled in the project. In the coming year, the prototype will be piloted to more and more SME and based on their feedback and evaluation both the prototyped solution, the conceptual framework and the use cases will be developed further using ADR guidelines. In this paper, we have proposed an IoT-blockchain based conceptual framework for product authentication and its sustainable product lifecycle. We have also shown how such a framework can improve the overall product traceability including information such as sustainability certificates, which further support product authentication. Furthermore, we want to complement with use cases for circular economy and support computing carbon emission data associated with each part used in a product, and much more depending on feedback from the piloting SME.

References

Alzahrani, N. and Bulusu, N. (2018). "Block-supply chain: A new anti-counterfeiting supply chain using NFC and blockchain," in *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems,* pp. 30–35.

Cao, W., Zheng, L., Zhu, H., and Wu, P. (2009). "General framework for animal food safety traceability using GS1 and RFID," in *International Conference on Computer and Computing Technologies in Agriculture,* Springer, pp. 297–304.

Choi, T.-M. (2019). "Blockchain-technology-supported platforms for diamond authentication and certification in luxury supply chains," *Transportation Research Part E: Logistics and Transportation Review* (128), pp. 17–29.

Cole, R., Purao, S., Rossi, M., and Sein, M. (2005). "Being proactive: where action research meets design research," in *ICIS 2005 proceedings,* vol. 27, pp. 325–336.

Faber, B., Michelet, G. C., Weidmann, N., Mukkamala, R. R., and Vatrapu, R. (2019). "BPDIMS: A blockchain-based personal data and identity management system," in *Proceedings of the 52nd Hawaii International Conference on System Sciences,*

Geissdoerfer, M., Savaget, P., Bocken, N. M., and Hultink, E. J. (2017). "The Circular Economy–A new sustainability paradigm?," *Journal of cleaner production* (143), pp. 757–768.

Huh, S., Cho, S., and Kim, S. (2017). "Managing IoT devices using blockchain platform," in *2017 19th international conference on advanced communication technology (ICACT),* IEEE, pp. 464–467.

Juels, A. (2006). "RFID security and privacy: A research survey," *IEEE journal on selected areas in communications* (24:2), pp. 381–394.

Kuhn, R., Yaga, D., and Voas, J. (2019). "Rethinking distributed ledger technology," *Computer* (52:2).

Mackey, T. K. and Nayyar, G. (2017). "A review of existing and emerging digital technologies to combat the global trade in fake medicines," *Expert opinion on drug safety* (16:5), pp. 587–602.

Nia, A. and Zaichkowsky, J. L. (2000). "Do counterfeits devalue the ownership of luxury brands?," *Journal of product & brand management* (9:7), pp. 485–497.

Power, G. (2008). *Anti-counterfeit Technologies for the Protection of Medicines*. Tech. rep. World Health Organization, Geneva, Switzerland.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. (2011). "Action design research," *MIS quarterly* (35:1), pp. 37–56.

Shim, J., Avital, M., Dennis, A. R., Rossi, M., Sørensen, C., French, A., et al. (2019). "The transformative effect of the internet of things on business and society," *Communications of the Association for Information Systems* (44:1), pp. 129–140.

Shim, J., Sharda, R., French, A. M., Syler, R. A., and Patten, K. P. (2020). "The Internet of Things: Multi-faceted Research Perspectives," *Communications of the Association for Information Systems* (46:1).

Shim, J. P., Avital, M., Dennis, A., Sheng, O., Rossi, M., Sorensen, C., and French, A. (2017). "Internet of things: Opportunities and challenges to business, society, and is research," in *ICIS 2017 Proceedings,* vol. 2017.

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

Sun Yin, H. H., Langenheldt, K., Harlev, M., Mukkamala, R. R., and Vatrapu, R. (2019). "Regulating cryptocurrencies: a supervised machine learning approach to de-anonymizing the bitcoin blockchain," *Journal of Management Information Systems* (36:1), pp. 37–73.

Thangavel, G., Memedi, M., and Hedström, K. (2019). "A systematic review of Social Internet of Things: concepts and application areas," in *ACIS 2019 proceedings,* vol. 2019.

Tian, F. (2017). "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," in *2017 International conference on service systems and service management,* IEEE, pp. 1–6.

Toyoda, K., Mathiopoulos, P. T., Sasase, I., and Ohtsuki, T. (2017). "A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain," *IEEE Access* (5), pp. 17465–17477.

Wilcox, K., Kim, H. M., and Sen, S. (2009). "Why do consumers buy counterfeit luxury brands?," *Journal of marketing research* (46:2), pp. 247–259.