Service assurance in the transport of goods, to encourage the optimization of processes related to transport logistics and the reduction of waste

Paulo Matos
Research Centre in Digitalization and Intelligent Robotics (CeDRI)
Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC),
Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
Email: pmatos@ipb.pt

Pedro Filipe Oliveira
Research Centre in Digitalization and Intelligent Robotics (CeDRI)
Laboratório Associado para a Sustentabilidade e Tecnologia em Regiões de Montanha (SusTEC),
Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
Email: poliveira@ipb.pt

2023 International Conference on Engineering and Emerging Technologies (ICEET) | 979-8-3503-1692-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICEET60227.2023.10525735

***Abstract*—The transport of goods is one of the main economic activities today and an essential pillar of many other activities, with a well-defined growth trend and with increasingly demanding needs, namely in terms of quality of service, whether this is related to meeting deadlines or the conditions of carriage. This is particularly relevant when we talk about delicate, perishable goods of high commercial or even sentimental value. The paper proposes an architecture for carriers to provide a service with guaranteed transport conditions without major changes to the operating model and at a lower cost. Currently, this quality assurance is essentially based on validation, often empirical, of the state of the goods after delivery. It is not even possible to speak of confirmation upon delivery, as in reality, most operators avoid this confrontation. The existence of services with a guarantee of compliance with the agreed conditions for transport not only conveys the necessary confidence to the end customer, but can even promote other businesses, but above all promotes the accountability of all actors in the value chain, fostering process optimization and waste reduction. On the other hand, as this is a goods tracking solution, knowing the actual flow of goods helps identify opportunities for improvement. The architecture is based on IoT, cloud, and blockchain technologies.**

***Index Terms*—transport, delicate goods, IoT, smart-contracts**

I. Introduction

Transporting goods is a vital economic activity with a growth rate of 3% per year [1]. However, it has a significant ecological impact due to transportation and cargo losses.

The service provided is based on the premise of transporting goods between two locations, charging for this service. The dimension of this activity is so large that it gives rise to very diverse contexts and requirements. Getting to the point of supporting commercial circuits of intercontinental transport with deadlines and periodicity that are quantified in hours. But other requirements are imposed, such as transport conditions. Either as a result of the end customer's quality requirements; that is, simply as a way of making certain transactions (businesses) viable that would not be feasible without these transport conditions. Current practice is based on the assumption that the service provider complies with the transport conditions. However, even when such conditions refer only to deadlines, the practice is that in most cases the deadlines are effectively met, but it is also accepted that the service is not guaranteed in all cases. When transport conditions include temperature or humidity requirements, confirmation that the service was provided as agreed often results in an empirical verification of the state of the goods upon delivery or, at most, in auditing the delivery service on a regular basis.

Presently, the guarantee that the service is provided under the agreed conditions is based on merchandise insurance, which, in the event of loss or degradation, safeguards the customer against potential damages. But that doesn't avoid undesirable costs, either for the insurance itself or for compensation in case of loss. Besides costs of non-compliance with contractual obligations of supply or stock failure, which may have repercussions on the corporate image or even lead to the loss of business opportunities. As if that were not enough, there are also the environmental costs – a commodity that is spoiled/unusable, is basically garbage from something that required resources to produce, which required transport resources and logistical resources in general, and which now turns into garbage, most likely with a direct environmental impact or with increased costs to be recycled. The very principle that there is insurance that protects in situations of damage or loss of goods, particularly as a result of not safeguarding transport conditions, is antagonistic to current social demands that encourage a sustainable and circular economy, whose main premise is to avoid or minimize the production of waste.

Certain goods, like food, require specific transport condi-

979-8-3503-1692-6/23/$31.00 ©2023 IEEE

tions due to their delicate nature. This includes temperature, humidity, and ventilation regulations. These goods are traded globally in various forms.

The origin of the product, who produces it, and what certifications it has, are some of the important factors for its valuation, but also for the sustainability of the business, which requires investment and time, implying convincing and winning the consumer's trust. However, it is not enough to produce the best product, if the transport logistics conditions put this quality and recognition in question. The transport of this type of goods almost always involves road transport with refrigerated chambers, often operated by subcontracted companies or individual workers, who do not respond directly to those who contract the transport service and, as such, are less concerned with the quality of the transport and more with the profitability of their business. To save on expenses, they sometimes turn off or reduce the cooling system (reducing fuel consumption); they don't always resort to logistics warehouses to take breaks for rest/overnight stay (where the goods can be kept in proper conservation conditions); among other decisions that can easily lead to degradation or bacteriological contamination of the goods.

This being a reality that unfortunately occurs, neither the producer nor the consumer can have guarantees that the transport was carried out in the proper conditions and, without being directly guilty, they end up selling a product of inferior quality or even out of conditions for consumption. In short, it is urgent to provide better quality transport services with more guarantees than simply meeting the delivery deadline. The solution naturally involves the conditions created by carriers and other transport logistics operators, but it is up to the market to demand more effective guarantees that the service is provided under the agreed conditions. Whoever produces, who buys, and even who provides transport services wins, as there are almost always subcontracted companies (particularly in long-distance transport), so the need for guarantees also arises between the company that provides the transport service before the client and subcontractors.

In this article, the authors present an architecture that can be adopted by any carrier that wants to provide a service with guaranteed transport conditions, not requiring significant changes to the operating model, with reduced initial investment and low operating costs.

To provide service as per the contracted conditions, the transport of goods is monitored and reliable information is provided about any non-conformities, crucial to identify non-compliant parties and assign responsibilities.

In reality, from the author's perspective, the idea is not to persecute those who do not comply, but to encourage compliance, that is, if everyone involved has the perception that there is an effective control system, with identification of those responsible for non-compliance and with the imputation of responsibilities, so it makes no sense to accept providing the service if it is not to comply with the agreed conditions. Because the costs of non-compliance are usually much higher than the amounts charged by the transport service. There are several indirect gains with liability:

- Encourages compliance with transport conditions and, as such, prevents the occurrence of situations that may degrade or even make the goods unusable;
- Allows to detect situations that might not normally be detected, allowing to act in good time to avoid the total loss of the goods; or at least prevent the same from occurring for other goods;
- Identifying that the transport conditions were not ensured and quantifying the impact of this, can allow assess the state of the goods;
- If the condition of the goods is considered to be inappropriate, it allows to choose to stop the transport - avoiding transport costs (with the natural environmental impact).

On the other hand, the presented solution tracks the goods. The potential that exists in this area of activity to reduce commercial costs and the environmental impact is well known, because it is an activity that makes intensive use of subcontracting, which on a global scale leads to a huge lack of knowledge of how transport is effectively carried out. The solution presented here promotes transparency, knowledge, and control over the situation - supporting more effective and intelligent decision-making processes.

The paper has five sections: introduction, State of the Art, Technological Context, Architecture, and Conclusions.

II. State of the Art

Ambrosus [2] is a commercial solution that provides integration services for Internet of Things (IoT) devices to record data on blockchains [3], [4], supported by *Ethereum* technology [5], [6]. They allow customers (transport companies) to develop their own quality assurance solutions for transport conditions, with the necessary transparency and veracity. The company provides APIs in several languages, the customer can create through these smart contracts [7], [8], implement user interfaces, including dashboards; integrate monitoring devices and, of course, record the collected data. Compared to the main goal of the proposed architecture, which is to provide guarantees of the quality of the service provided, *Ambrosus* is a reference work. However, it is only focused on part of the process (cloud integration). By leaving fundamental parts of the process open, such as data collection, it immediately compromises the entire solution, namely the two greatest values: transparency and veracity of information.

Modum is a company that provides several solutions to monitor the conditions of transport of goods. As a commercial service/product, there are not many details about the implemented solutions or even about the maturity of these solutions. *ModSense One* [9] is *Modum's* award-winning solution to monitor temperature, comprising: physical device, which collects data; mobile application; blockchain; dashboards; and report generation. It is a complete solution, where the device is attached to the goods at the beginning of the transport, collecting data periodically and, as far as possible, ensures that the data is available in real-time. It is designed for transport companies or with logistics activities, in order for

them to monitor their own resources and goods, and not to provide service guarantees to third parties. Thus, it is not an open solution designed to be widely adopted, with reduced installation and operating costs, focused on providing guarantees to customers - as is intended with the architecture proposed in this article by the authors. It has, however, in common, many of the technological options and considerations addressed in the design of the solution presented in this article.

Roambee [10] is a company that provides a versatile solution to monitor goods, equipment, machines, and vehicles, among others, throughout the transport process, but also in warehouses or even in stores. It is focused on the business market (companies) and not on the individual customer. The solution is based on the *BeeBeacon*, which is the monitoring device that allows, as far as possible, to provide data in real-time. Among the collectable data are the temperature, humidity, pressure, geographic location, and others, and the *BeeBeacon* may even contain sensors for the detection of certain types of gases of an organic nature.

BeeBeacons uses Bluetooth Low Energy (BLE) gateway [11], to send data to the cloud (*Roambee* cloud) via the 3G/4G network. A gateway is fixed in the warehouse or transport vehicle and is the device that contains the Global Positioning System (GPS), which allows geolocation of the collected data. *BeeBeacons* are attached to merchandise, but can also be used in fixed locations such as warehouses or coolers. *Roambee* has chosen to have the *BeeBeacons* in continuous advertising (always on), thus being always available to accept connections from, for example, mobile platforms that have the *Roambee* application. The mobile platform itself lends itself to functioning as a gateway for sending data to the cloud. Through the *Roambee* Cloud Portal, customers can obtain reports and access various informative dashboards. As an architectural solution, *Roambee* is closest to the one presented by the authors, but the objectives, priorities, target market, and technical options are quite different. *Roambee* emphasizes access to real-time data and the relationship between time and geographic location of goods – a relevant approach for logistics management where the entire process is controlled by a single company and where distances and transport times are not very long. There is no specific concern with the veracity of the data and aspects such as the autonomy of the devices, investment, and operating costs were relegated to meet other requirements.

Several recent academic studies explore the use of blockchains, including for delicate goods [12] and there are several recent studies that address the theme of this article from a traceability perspective [13], [14].

III. Technological Context

Generally speaking, the solution consists of a monitoring module containing sensors, which collect data on transport conditions, and a processor that performs local control and ensures a way to communicate the data to those involved in the transport process, sender and recipient of the merchandise.

In the ideal solution, non-conformities would be reported in real-time. However, this solution has two major problems: energy autonomy and restrictions on communication technologies and topologies.

All the technologies that ensure communication on a global scale consume much more than is desirable. Monitoring devices are wanted to be small in the sense that they can be attached to all types of merchandise, which constrains the size of the batteries and, implicitly, their capacity. Thus, consumption with communication, 10,000 to 100,000 times more than the processor and sensors, is critical. Without the necessary autonomy, full monitoring of the transport route and, as such, all the added value of the solution may be at stake. But even thinking that a battery can survive more than one journey, it is fundamental to minimize the number of times it has to be replaced/recharged, whether due to cost, environmental impact, or unavailability of the devices. Then there are the technological limitations: in terms of communication, there is not always coverage on a global scale or even a single operator that provides such a service. The solution is to use satellite communications, but the cost of equipment and usage is too high for this type of application.

In short, having access in real-time is good, but given the implications it has in terms of limiting the scope of application (which we have already seen prevents its use on a global scale) and given the current state of technology (still expensive), it is an excessive solution.

The simplest solution would be to extract the data upon delivery to the recipient. In the event of non-conformities, the latter would immediately be aware of this and could request the appropriate compensation. The problem that arises is that the company providing the service, which is left with the burden of blame, has no way of identifying internally, or before the subcontracted companies, those responsible for non-conformities. The geographic contextualization of non-conformities, using GPS would be a possible solution, not least because it is available anywhere on the planet and is a free service (does not involve operators). It would be an excellent solution, were it not for the cost of the hardware and the high consumption it has.

Another possibility is to temporally contextualize the non-conformities, something much simpler and that has no relevant impact on the autonomy of the devices. This makes it possible to know when the non-conformities occurred, but it may not be enough to determine responsibilities, namely if the providing entity does not have records of the dates of receipt and delivery of goods between operators. In addition, providing data on non-conformities only when the goods are delivered has other disadvantages:

- Prevents recovering from minor non-conformities, which could be filled or corrected and thus minimize damage;
- The delay between the delivery date and the occurrence of non-conformities can make it difficult to understand the cause and effect. If the non-compliance results from a failure in the process, unknown to the operator, it may

mean that many other goods are subject to the same (non-compliant) transport conditions in the meantime;
- It also involves transporting the goods to the recipient, even if they are already in an irrecoverable situation.

A somewhat more reactive solution is desirable, which reports non-conformities as soon as they occur and thus allows not only to identify those responsible, but also to intervene to recover from this situation, but that will be technically and economically viable.

IV. Architecture

The solution idealized by the authors takes advantage of existing technology to provide a solution that fits the practical situation of transport logistics, whether in terms of device autonomy, acquisition, and operational costs, communication technologies, or simply the purpose of the solution. The monitoring modules contain sensors that assess transport conditions (temperature, humidity, displacement, etc.) Whenever there is an occurrence, the processor is woken up and registers the occurrence. Communication is carried out using BLE due to its low consumption, but mainly because this is a common technology, available on all mobile devices (smartphones, tablets, or laptops). BLE defines two roles: central and peripheral. The peripheral provides aggregated features in services, which can be writing, reading, and notification. The central behaves like a client that connects to a server (peripheral) and accesses those characteristics for reading and writing purposes. In the case of notification-type characteristics, whenever the value of the characteristic changes in the peripheral, the control panel is notified, and an event occurs for that purpose. The BLE operation is based on the following procedure:

- The peripheral, in advertising mode, transmits the indication that the device is available, eventually with some information, namely about the available services;
- The control panel, in scan mode, looks for advertisement radio signals, and may be pre-configured to look for peripherals that advertise certain services;
- If the desired device is found, the control panel can then request the connection;
- The connection may involve security procedures, with different levels of implementation – some of which are used in the proposed architecture;
- The control panel can read/write the characteristics;
- Peripheral can notify central;
- The connection can be terminated by either party.

The architecture considers three operational modes for monitoring devices, namely:

- **Mode A** – Advertise is activated by pressing a button on the monitoring device, thus opening a time window during which connection can be established;
- **Mode B** – The monitoring device is continuously advertising, that is, it is continuously available to connect with a central. It is idealized for situations in which it is not possible to activate advertising by pressing the button, such as when the device is inside the package; fixed on an animal, such as a bird or a feline, or inside a container;
- **Mode C** – Similar to mode A, the advertising is active if the button is pressed. Devices of this type serve to aggregate data from devices operating in A/B mode, establishing a local network with a star topology, where the device operating in C mode serves as a gateway for the devices operating in A/B mode.

The mode in use is chosen by software and the physical architecture (hardware) can be the same for all three modes. However, devices that operate solely in C mode do not need the sensors or the RTC. In terms of monitoring, the choices are between A and B, with the use of A being preferable, as it consumes less energy.

In Fig. 1 the procedures between the different actors of the system are represented. The customer/sender contracts the service with the transport service provider, defining the transport conditions, which include the limits of the relevant variables and/or deadlines. The service provider validates the possibility of providing the service under the requested conditions, which requires confirming that there are operators to perform all stages of the route, under the requested conditions, whether they are carriers, warehouses or others.

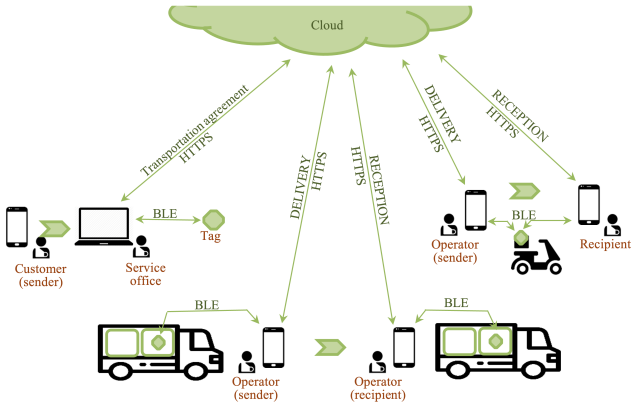

Fig. 1. Procedure between different actors.

If there is agreement, a key is generated, which only the sender should have access to (later this key will be provided to the recipient), and a key for the service provider. These keys lend themselves to consulting the merchandise's registration history, through the access portal to cloud services. They are separate keys, as the information provided to each party (service provider and sender/recipient) is different (the service provider contains internal information about operators). The key provided to the sender must be communicated to the recipient, so that he can formally receive the goods. Non-public identifiers are also generated for the device, merchandise, operators, sender, and recipient, as well as two pairs of keys for asymmetric encryption.

On the device is recorded: the public key of the first pair; the private key of the second pair; device, commodity, current, and next carrier identifiers; the conditions of carriage; descriptive information; earliest (EDD) and latest date/time of goods delivery (LDD) to the next operator. The device's RTC is reset and the universal time GMT+0 is saved. Depending on the

device placement on the goods, the device's operating mode and status are also defined. This state defines the condition of the goods relative to the operator and serves to control the actions that must be available for the operators to perform at any given time. In the context of this article, this status has two possible values:

- RECEIVED – which signals that the operator has received the goods;
- DEPOSITED – which indicates that the operator has deposited the goods to be received by the next operator.

To the cloud, it is sent the identifiers; private key of the first pair; public key of the second pair; identification of all operators involved in the transport by intervention order, with the respective earlier and later dates of goods delivery; maximum time after deposit/delivery that the next operator has to collect the goods; approximate location the place of transfer of the goods; and the universal RTC restart date.

The device is attached to the goods in front of the customer, with a physical lock that, once removed, triggers the procedure for delivering the goods to the recipient. And from then on, it starts to work collecting data, if any, of non-compliance. If the security lock is removed ahead of time, the procedure will not be closed or will be closed in an irregular situation, with responsibility for damage to the goods or loss of the same, the operator who officially had the goods in his possession. At any time, anyone with the mobile application installed can connect to the device as long as it is in advertising mode. And thus access the descriptive information of the device, the goods, the current and next operator, the earlier and later dates of delivery of the goods, and the status.

The current operator, when delivering the goods, makes his physical deposit, activates the advertising mode (if necessary), and connects his mobile device to the monitoring device. The connection triggers an event on the peripheral side that forces it to encrypt in a single token, using the public key, all identifiers, the RTC time, the state, and non-conformities. Once connected, the mobile app will automatically read out descriptive information and monitor the device status. It is based on the latter that the possible actions to be carried out are enabled. As the goods were given as delivered to the current operator, the latter will now have available the action to request the formal delivery of the goods to the next operator (or, as the case may be, to the recipient). With this, the token generated on the peripheral is read, to which the identification of the operator of the mobile application is added, the GPS location obtained with the resources of the mobile device itself, and the identification of the action performed. It encrypts everything again in a second token with a second public key obtained when installing and configuring the mobile application (the respective private key is on the server side). This token lends itself to authenticating the entire context on the server, updating non-compliance records, and performing the requested action. The server decrypts the tokens and compares the data provided with the ones it has, namely the current time with the RTC value, the GPS location with the expected one, and the identifiers. If the tokens are considered valid, the non-conformity data is recorded and a third token is generated by the server, using the public key of the second pair of keys and encrypting: the indication that it is a response to a request for the delivery of goods; the identification of the goods; the elapsed time since the RTC was reset; and identification of the current operator requesting receipt of the goods. This token is returned to the mobile application following the goods delivery request. The mobile app uses the token to update the status of the monitoring device. Any operation that implies changing values in the monitoring module, from the open access BLE Service, implies authentication. Authentication is based on the token that the mobile application receives from the cloud. The monitoring device decompresses the token, using the private key of the second key pair, and compares identifiers, as well as the provided time with that of the RTC, and status. If the token is considered valid, the authentication is successful. Then, taking into account the identifier of the type of action, it performs the respective operations, which in this case is to change the status of the device from RECEIVED to DEPOSITED. The cloud server registers that the goods have been deposited and sends a notification to the next operator, with the maximum time that the latter has to receive the goods. The delivery operation does not always occur with the physical presence of the goods, current operator, and next operator, as a result of operational and physical constraints. Hence delivery and reception are two separate acts.

The next operator will carry out the same connection procedure, but in this case, as a result of the status of the device, the available action is to receive the goods. The second token is sent to the cloud service. After validating the second token, and considering the action to be performed, a third token is generated by the server, with the public key of the second pair of keys, containing: an indication that it is a response to a request for receipt of goods; the identification of the goods, the time elapsed since the RTC was reset, the identification of the current operator (who is requesting receipt the goods), and the identification, descriptive data and earlier and later dates of delivery to the next operator. That token is returned to the mobile application following the reception request, which uses it to authenticate and update the monitoring device. The device decompresses the token, using the private key of the second key pair, and compares identifiers as well as the provided time with that of the RTC. If the token is considered valid, it moves the records of the next operator (the one currently requesting reception) and updates the records of the next operator with those from the token. It also updates the status from DEPOSITED to RECEIVED. In both situations, delivery and reception, the mobile application, after the procedures, requests the condition of the goods so that the operators can have the perception of whether or not there has been a violation of the transport conditions. Depending on the conditions agreed between service providers, the recipient may reject the receipt. The goods thus pass from operator to operator, until they reach the recipient. Here, the delivery procedure is carried out by the last operator, and the formal receipt of the goods by

the recipient. For this purpose, the operator, in the presence of the recipient, requests the final delivery operation, being asked for the key generated during the contract and delivered to the sender. The operation can even be carried out by installing the application on the recipient's mobile phone, using the same code for this purpose.

V. Conclusions

The architecture is in advanced prototyping stage and has undergone partial functional and technical validation tests in controlled scenarios. More comprehensive testing requires cloud component and real-world context.

The authors had already had the opportunity to demonstrate the existing prototype to several transport service providers and it was evident that they were uncomfortable with the possibility of having to use this type of solution or providing the type of service that is envisaged here. In more than one situation, they simply rejected the idea of doing so, on the grounds that it is not economically sustainable. This reinforces the authors' motivation, as the challenge is not only technological but also one of changing mindsets. Currently, the authors are specifying the structure of the cloud, based on blockchain technology and smart contracts.

The proposed architecture offers a cost-effective solution for transporting fragile goods with guaranteed contractual conditions. It can be applied in various contexts to protect the interests of both customers and service providers, while providing a more valuable service.

The solution does not report non-conformities in real-time but reports when there is a transfer of responsibility, allowing the immediate identification of those who do not comply and thus determining responsibilities.

Even without resorting to global communication channels, the presented architecture manages to monitor and report data in a timely manner, simply using BLE and conventional smartphones/tablets, working anywhere. The cost of adopting a solution of this type essentially requires the acquisition of monitoring devices by the company providing the transport service. Based on the prototype's bill of material, it is realistic to think that the production cost could currently remain at $15 - a value that already reflects the enormous increase that has occurred in recent years for the hardware of this type of technology. All other operators only need to have a conventional smartphone/tablet, with the application installed and with access to data communications. Thus, there are no high-value structural investments, and the acquisition of monitoring devices can even be done gradually.

In operational terms, the operators have the costs of data communication and the operationalization of the protocol, in compensation of a service with greater added value. The company providing the service to the final customer will incur operating costs for access to cloud services, which must be provided by an entity other than the service provider itself, so as not to jeopardize the veracity of the data and the process. and other operators are sure that the transport was (or was not) carried out as agreed; and in the event of non-compliance, it is entirely possible to identify who the defaulters were and thus determine responsibilities. This is particularly relevant when the damage is not immediately identifiable on the goods. Furthermore, with the proposed technical solution and technologies, a simple CR2032 battery can last for years, probably beyond the useful life of the device itself. However, the great contribution of this architecture is actually contributing to the transparency and accountability of the entire transport logistics chain, promoting less waste and the optimization of the entire process, which should translate into lower operating costs and less environmental impact.

Acknowledgment

The authors are grateful to the Foundation for Science and Technology (FCT, Portugal) for financial support through national funds FCT/MCTES (PIDDAC) to CeDRI (UIDB/05757/2020 and UIDP/05757/2020) and SusTEC (LA/P/0007/2021).

References

[1] ITF, "Key Transport Statistics 2019 (2018 Data)," ITF, Tech. Rep., 2019. [Online]. Available: https://www.itf-oecd.org/key-transport-statistics-2019-2018-data

[2] "Ambrosus," https://ambrosus.io/, accessed: 2023-09-15.

[3] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, May 2016.

[4] S. C. S. Huh and S. Kim, "Managing IoT devices using blockchain platform," in *19th International Conference on Advanced Communication Technology (ICACT)*, Bongpyeong, South Korea, 2 2017, pp. 464–467.

[5] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[6] S. Tikhomirov, "Ethereum: State of knowledge and research perspectives," in *Foundations and Practice of Security*, A. Imine, J. M. Fernandez, J.-Y. Marion, L. Logrippo, and J. Garcia-Alfaro, Eds. Cham: Springer International Publishing, 2018, pp. 206–221.

[7] J. Montes, C. Ramirez, M. Gutierrez, and V. Larios-Rosillo, "Smart contracts for supply chain applicable to smart cities daily operations," in *2019 IEEE International Smart Cities Conference (ISC2)*, Casablanca, Morocco, 10 2019, pp. 565–570.

[8] S. Wang, L. Ouyang, Y. Yuan, X. Ni, and X. Han, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, pp. 2266–2277, 02 2019.

[9] "MODsense One | modum.io," https://modum.io/solutions/modsense-one, accessed: 2023-09-15.

[10] "Real-time Shipment Tracking and Monitoring | Roambee." [Online]. Available: https://www.roambee.com/shipment-monitoring/

[11] "Bluetooth Core Specification: 5.4," https://www.bluetooth.com/specifications/specs/core-specification-5-4/, Tech. Rep., 2019, accessed: 2023-09-15.

[12] L. Wang, L. Xu, Z. Zheng, S. Liu, X. Li, L. Cao, J. Li, and C. Sun, "Smart contract-based agricultural food supply chain traceability," *IEEE Access*, vol. 9, pp. 9296–9307, 2021.

[13] N. G. Muralidharan, V. Pantelic, V. Bandur, and R. Paige, "Integrating software issue tracking and traceability models," in *2022 IEEE International Conference on Software Maintenance and Evolution (ICSME)*, 2022, pp. 429–433.

[14] S. Guo, "Blockchain-based traceability system for trading pre-made food products," in *2022 2nd International Conference on Computer Science and Blockchain (CCSB)*, 2022, pp. 7–10.