LUT University

THE POSSIBILITY OF USING A DECENTRALIZED INTERNET OF THINGS NETWORK IN THE TRANSPORTATION SYSTEM

Lappeenranta–Lahti University of Technology LUT

Master’s Programme in Software Engineering

2022

Malysheva Tatiana

Examiner(s): 1st Examiner: Assistant Professor Annika Wolff

2nd Examiner: Research Assistant Mehar Ullah

ABSTRACT

Lappeenranta–Lahti University of Technology LUT
LUT School of Engineering Science
Software Engineering

Malysheva Tatiana

The possibility of using a decentralized internet of things network in the transportation system

Master’s thesis
2022
86 pages, 40 figures, 2 tables and 0 appendices
Examiner(s): Assistant Professor Annika Wolff, Research Assistant Mehar Ullah

Keywords: IoT, IoV, Blockchain, Decentalization, Smart Transportation, Smart Port

Digital transformation allows the transport sector to continuously develop, using various modern technologies in its processes, such as the Internet of Things, blockchain, artificial intelligence, etc. Thanks to these technologies, autonomous traffic and traffic flow management is gradually becoming a reality. In view of the fact that a huge number of different devices can interact on the Internet of Things, the data warehouse must cope with the task of storing the data that such devices generate. In addition to the problem of scalability of devices, the issue of security of such storage is also quite acute. This thesis presents a systematic review of the literature on the integration of blockchain technology in the IoT network in order to address network security and scalability issues. The thesis considers aspects of an intelligent road transport system, as well as a smart port.

ACKNOWLEDGEMENTS

It was a rather difficult, but interesting way of studying at the university for 6 years. I want to express my gratitude to LUT University and the entire teaching staff for giving me a chance to study at your university, learn something new and in any case become a little better.

I also want to thank my supervisor Annika Wolff for the allocated time, support, always constructive dialogue and interest in getting final result.

I also express my great gratitude to my family, especially to my mother for always supporting me in everything, providing me with an environment where I can develop, gain new knowledge and discover the world in every sense of the word.

Writing this work fell at a time when at times it seemed to me that the future that I dreamed of and to which I was going would no longer exist. But if you don't make an effort, there will never be a result.

I want to believe that the world will soon be ruled by the peace, so that every person living on this planet can use all the scientific achievements and technologies that I wrote about in my work and learned about during my studies. After all, historically, empires always collapse, and hatred, anger and war never bring anything good.

TABLE OF CONTENT

1 Introduction

Technology is radically changing people's lives. Today, a person cannot imagine his or her life without all those products and services that can instantly meet their needs. But with the development of technology, users’ requests for faster services, without interacting with real people, are also growing, and as a result, business must adapt to these changes.

The number of traditional enterprises is decreasing, more and more companies are implementing modern technologies into their activities [1]. Customers need faster receipt of services, which is why certain processes at enterprises are automated. With the advent of technologies, most of which are data-driven, new problems have appeared that are related to data storage and transmission, for example, data leakage, hacking of data warehouses, and so on.

One example of an industry that is continuously undergoing digital transformation is transportation. Technologies used in the field of passenger transportation allow people to build convenient routes, track transport and much more. [2] This applies to both air and rail transport, as well as city transport. At the same time, the technologies used in the field of cargo transportation are rapidly ahead of the previous ones. Cargo transportation by autonomous vehicles (drones), warehouse systems, autonomously operating unloaders, various robots – all these are modern means used in seaports today. All this is possible thanks to various technologies, such as artificial intelligence (AI), Internet of Things (IoT), blockchain and big data technology will serve as the main entry points and fundamental pillars for the promotion of new innovative solutions that will change the existing transport system. Separately, I would like to highlight the technology of the Iot, since thanks to its use and the introduction of various sensors both on the ships themselves, cars, and in the seas and on land, the functionality of the port itself increases at times, and savings at the same time can amount to thousands of dollars. But its use also has other not always positive sides.

2 Background

Currently, the sphere of trade is rapidly developing, and this creates a great need for a fast and reliable way of sending these goods. Cargo often needs to be sent from eastern countries to Western countries and vice versa, with the need to cross the ocean, and therefore there is a continuous development in the field of transportation, and in particular by sea vessels. In order for port operations to become more cost-effective, reliable and fast, information and communication technologies (ICT) are being used, which currently leads to the creation and implementation of highly automated processes and more cost-effective solutions [3]. The introduction of modern technologies into processes identifies the course of the Fourth Industrial Revolution, commonly referred to as Industry 4.0 (I4.0). Currently, port representatives are automating part of their processes with technology, in order to increase productivity, efficiency and effectiveness, as well as to strengthen the security of port operations and making ports more and more sustainable [4].

With the advent of technologies in which data means a lot to the functionality of systems, and with them the enterprise, there is a great concern about the safety of data and their inviolability. In recent years, cybersecurity has attracted increasing attention from port and maritime transport managers, and with them scientific researchers, because it is one of the main risks of the port, on which active research work continues [4].

Each smart port is equipped with a variety of sensors, the activities of which are controlled and monitored using Internet of Things technology. The technology has a huge number of advantages, but along with them there are some difficulties and risks. All data also needs to be securely stored and transmitted, so it is necessary to control the infrastructure and access to restricted areas [5]. Security and privacy are the main problems, since connecting various devices to the Internet opens up the possibility of unauthorized access and control, as well as theft of valuable information [6].

Currently, most IoT ecosystems have centralized interaction models called client-server architecture. All devices on the network interact with each other through cloud servers, which have huge data processing and storage capabilities. But the popularity of the technology is growing, and with it the scale of its use. Figure 1 shows the number of connected devices to the network from 2016 to 2024 (the projected number). Cloud servers do not always cope with the expansion of data sources at the present time, and based on the trend of network scalability, in order to ensure the smooth operation of servers, huge financial investments are needed. But even after overcoming financial difficulties, cloud servers will still remain a bottleneck and a point of failure that can disrupt the entire network. [7].

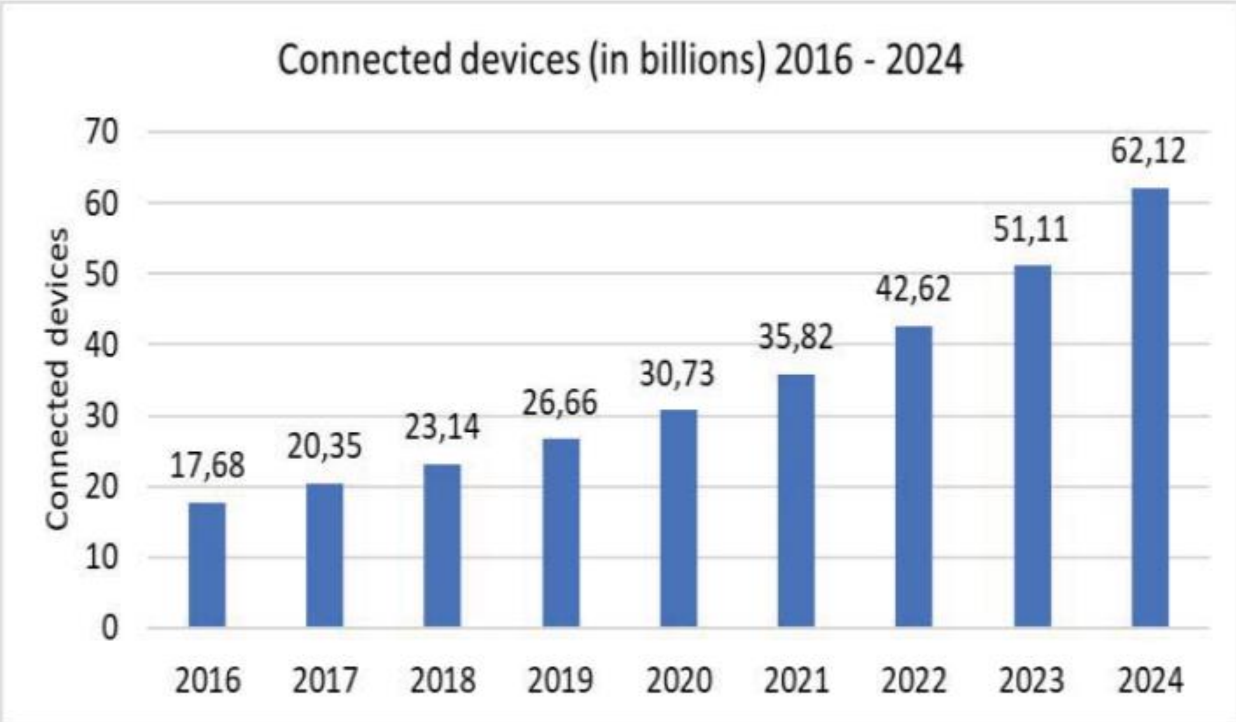

Figure 1: Connected devices in billions 2016 – 2024 [8]

Researchers are also considering building an IoT network using edge computing, that is, data processing should take place not in cloud storage, but on intermediate nodes. Despite the fact that this approach is really able to increase the security of the entire network, vulnerabilities also remain on the localized points of the border network themselves. In addition, due to the lack of authentication of edge devices, they can also be susceptible to hacking, although the deployment of such an approach is also quite expensive. Also, due to the fact that only the processed data gets into the storage, and if the edge devices delete the useful data, it will be impossible to restore them.

Based on all of the above, the Internet of Things network needs some changes and improvements, due to the growing problem of working with data. Enterprises and scientists have been dealing with this issue for more than a year, continuously developing and adapting new concepts. This work is aimed at studying existing solutions to the problem of Internet of Things data security in the transport sector, as well as their adaptation in various enterprises engaged in both cargo and passenger transportation, as well as studying and identifying new trends in the development of secure data transmission between stakeholders and process participants.

2.1 Problem statement

In the modern world, technologies bring huge benefits to society, contributing to the automation of some processes, significantly reducing the time of certain operations and the number of errors. The main tool when using technologies is information and data that are used for statistics, analysis, forecasts and decision-making. The analyzed data are of great value for companies and their activities in the context of digital transformation.

But in addition to the value, data also brings a lot of problems associated with their storage and transmission. History knows many examples when data has been stolen, leaked and completely lost. The problem of data security becomes especially relevant when using Internet of Things technology, because the more devices are connected, the more vulnerabilities and security threats there are. The financial consequences of such attacks can also be very painful — according to the World Economic Forum, in addition to the high costs of deploying and managing IoT platforms, in the case of hacking a cloud provider alone, the damage can range from $ 50 to $ 120 billion [9].

The data used in the field of transport is used by a huge number of users. In this connection, another problem arises related to the reliability of the data used, because it is impossible to completely trust outside the scope of responsibility of one owner, since it is not possible to verify that they have not been changed before sending, selling or using by other parties.

For instance, the IBM company [10] highlights the following IoT growth problems:

- Broken business models;
- Lack of functionality;
- Lack of prospects;
- Lack of information protection;
- High cost.

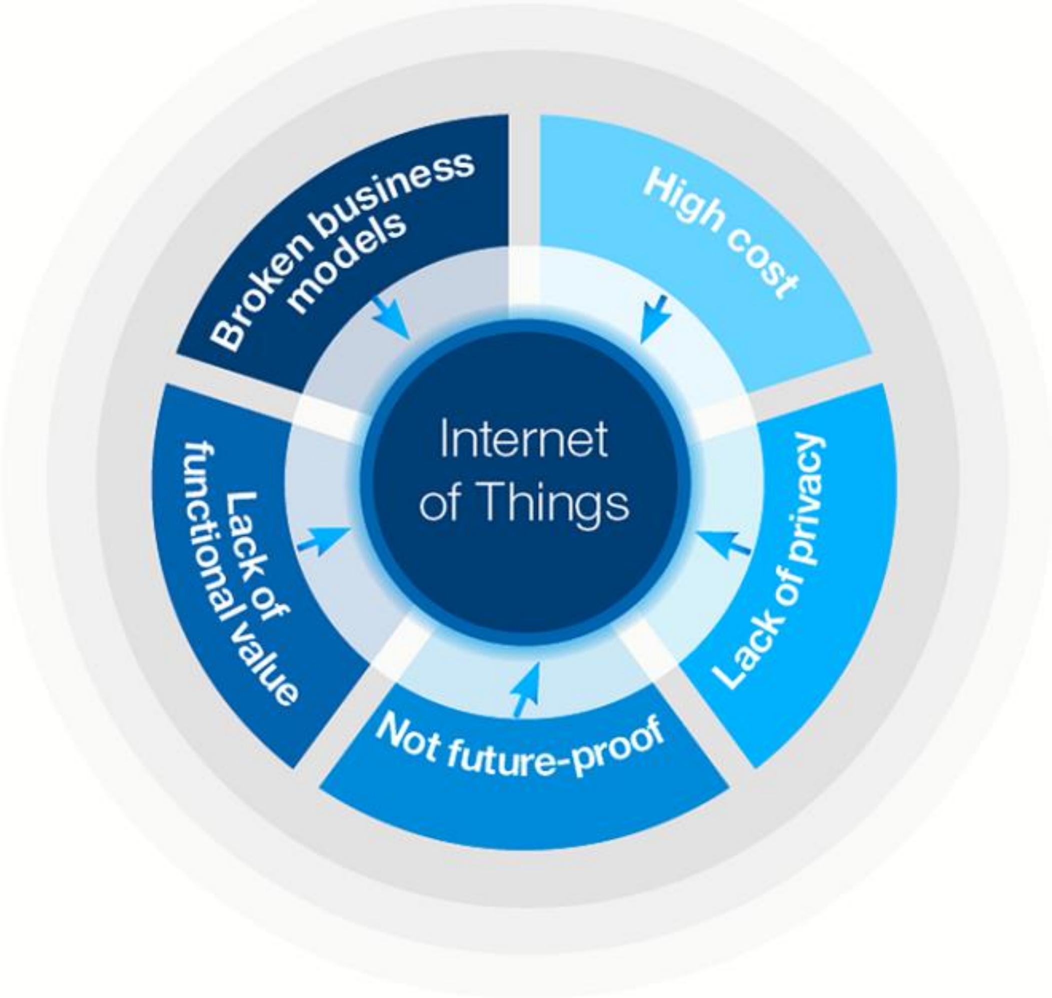

Figure 2: IoT growth problems [10]

The next issue related to data received and sent by devices connected to IoT is scalability. According to various estimates of IT giants, 30 - 50 billion devices are connected to the Internet of Things. IoT has a wider overall scope than the regular Internet. Therefore, the scalability of the IoT space will be more complex than that of conventional web applications.

The search for solutions to the above-mentioned problems is the main and relevant today, because then it will be possible to use this technology without fear of any security-related problems. And one of the possible solutions is to use this network without a centralized source, namely, using it in tandem with blockchain technology [11].

2.2 Research objectives

In this thesis, the use of decentralized Internet of Things technology in a transportation sphere is considered. The purpose of this thesis is to study the processes that have undergone digital transformation due to the decentralized Internet of Things in the field of maritime cargo transportation, and as a result, search and analysis of new solutions in the digital transformation of the urban transport sector.

Based on this goal, 4 research questions were developed:

RQ1: What is the essence of smart transportation?

To answer this question, it is first necessary to define the term "Smart", as well as to define the main provisions of Smart Transportation, and smart Port.

RQ2: What advantages does decentralization give to the Internet of Things?

As part of the answer to this question, first it is needed to determine the main provisions of IoT and Blockchain technologies. Then understand the specifics of their joint use, as it is possible in infrastructural and architectural terms. Then identify the key advantages and disadvantages both in their offline use and in sharing.

RQ3: Which Smart transportation processes already use the decentralized Internet of Things.

To answer this question, it is first necessary to identify the main stakeholders of the port and transportation system, identify the main business processes, describe use cases in which the technology of the decentralized Internet of Things is already used, with a detailed description of these business processes.

RQ4: Which Smart Port processes can still be improved with the help of these technologies.

Based on the results of the research identified on the previous research question, to draw an analogy with Smart Port and its processes and the sphere of digital transformation.

RQ5: What is the future of the decentralized Internet of Things in smart transport?

To identify the main trends in the development of decentralization in the Internet of Things and how it can be applied in the future.

Based on the questions posed, the research plan of the thesis is:

- Define the concepts of "Smart", “Smart Transportation", "Smart Port";
- Study of blockchain and Internet of Things technologies, as well as the benefits of their joint use;
- Study of Smart transportation system processes that use decentralized Internet of Things technology;

- Identification and analysis of key infrastructure, process and stakeholder requirements for technology deployment;
- Identification of smart city transportation problems that can be solved using decentralized Internet of Things technology;
- Search for new trends in the field of smart transport.

3 Background information

This chapter contains detailed information about various technologies and concepts that will be necessary to get answers to research questions and to disclose the topic of using a decentralized Internet of Things network in the transport sector. This section contains information and architecture of centralized systems, in order to further comparation it with a decentralized version of data storage.

3.1 Smart explanation

Information and communication technologies cover all spheres of human life, annually increasing the pace of digital transformation, introducing an increasing number of technologies in various fields. Recently, people are increasingly hearing the prefix "Smart" to many different everyday words, for example, "Smart kettle", "Smart refrigerator", "Smart vacuum cleaner" and much more. For big city citizens of developed countries, this is no longer something unusual and new, a self-turning kettle and an autonomously working robot vacuum cleaner entered people's lives several years ago and became routine. Figure 3 shows the forecast of the number of smart home devices shipped worldwide. As it can be seen from this graph, the number of these smart home devices will increase exponentially every year.

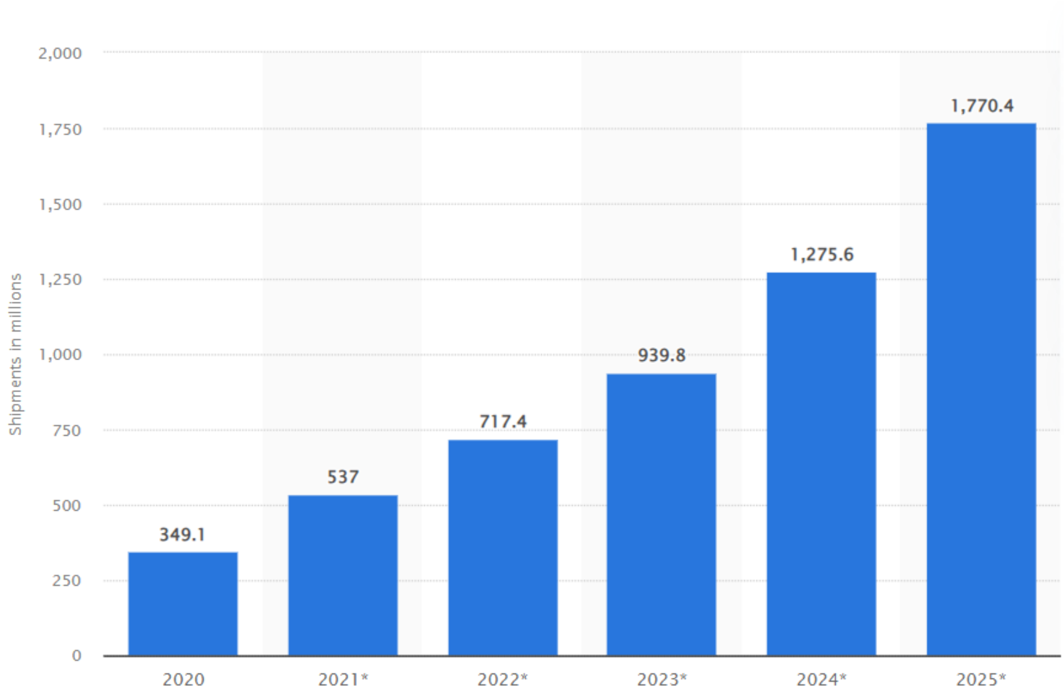

Figure 3: The number of smart home devices shipped worldwide [12]

In general, the prefix "Smart" for inanimate objects can be described as independent, intelligent. The main difference between smart objects and ordinary ones is that they are able to "communicate" with a person and each other and controlled remotely via Bluetooth, LTE, Wi-Fi and cellular communication. Applications or voice is a gateway through which a person is able to send a command to a device. From such devices, a broader infrastructure is being built, which is called a "Smart home". A smart home is the use of computer or control technologies, image display technologies and communication technologies that will be connected through a network of various objects together to meet the automation requirements of the entire system in order to provide more convenient control and management [13]. In this case, all smart devices and sensors that are located inside one house begin to communicate and exchange data with each other using cloud data storage. Such systems are much easier to manage and monitor their activities. A traditional smart home is often implemented within a centralized architecture, as shown in Figure 3. Household appliances are connected by a home network and controlled by a home gateway, which is a platform for service providers who provide services to residents.

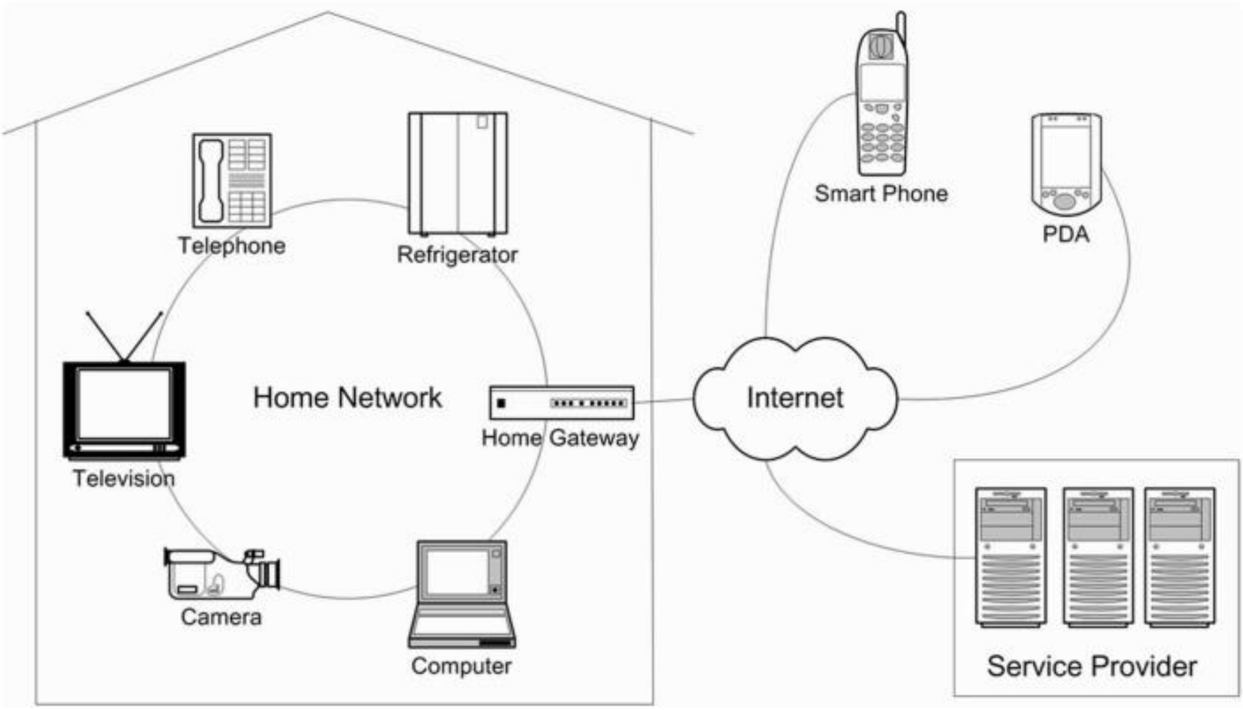

Figure 4 - Typical architecture of traditional smart home [14]

As can be seen from Figure 4, the architecture of a smart home in terms of the number of devices connected to the network is quite simple. In the following sections of the work, networks much larger than the specified one will be presented, since thousands of different devices and sensors will interact in it.

3.2 Internet of things technology as the main tool of smart infrastructure development

The main technology thanks to which a person is able to "communicate" with devices, transmit commands to them to perform an action, and also thanks to which communication between inanimate objects is possible, is the technology of the Internet of Things (IoT). There is no precise definition of the term IoT, many researchers and companies involved in the implementation of this technology interpret it differently, depending on what kind of goal and problem the technology should solve. Kevin Ashton is the creator of the IoT concept, and in 1999 he presented it as "a uniquely identifiable inter-ship network of objects controlled using radio frequency identification (RFID) technology" [15].

Shancang Li in [16] notes that, as a rule, the term IoT has the following definition: "dynamic global network infrastructure with self-tuning capabilities based on standards and interacting communication protocols; physical and virtual "things" in IoT have identifiers and attributes, are able to use intelligent interfaces and integrate to the information network" [17]. Another definition is given in [18] here it is argued that the words "Internet" and "Things" mean an interconnected worldwide network based on sensory, communication, network and information processing technologies that can be a new version of information and communication technologies (ICT). Despite the fact that the technology does not have a specific definition and description, its development does not stand still, an increasing number of companies are taking on the task of implementing such a network in homes, businesses and cities, in order to improve their performance, as well as improve human living standards. In order to implement an IoT network, many related technologies are used, the development of which also does not stand still, as a result of which the definition of IoT may also vary. But despite this, the key idea around which the entire infrastructure is built, and what is static in the definition, is that all things within the same network can exchange data with each other, and if there is a certain algorithm, process them.

In order to ensure smooth interaction between devices with the gateway, there are several different options and implementation models [19]:

- Direct connection via Ethernet or Wi-Fi using TCP or UDP;
- Bluetooth with Low Power Consumption;
- Near Field Communication (NFC);
- Zigbee or other cellular radio networks;

- SRF and point-to-point radio channels;
- UART or serial lines;
- Wired SPI or I2C buses.

Figure 5 shows the diagrams of the two most common connection methods.

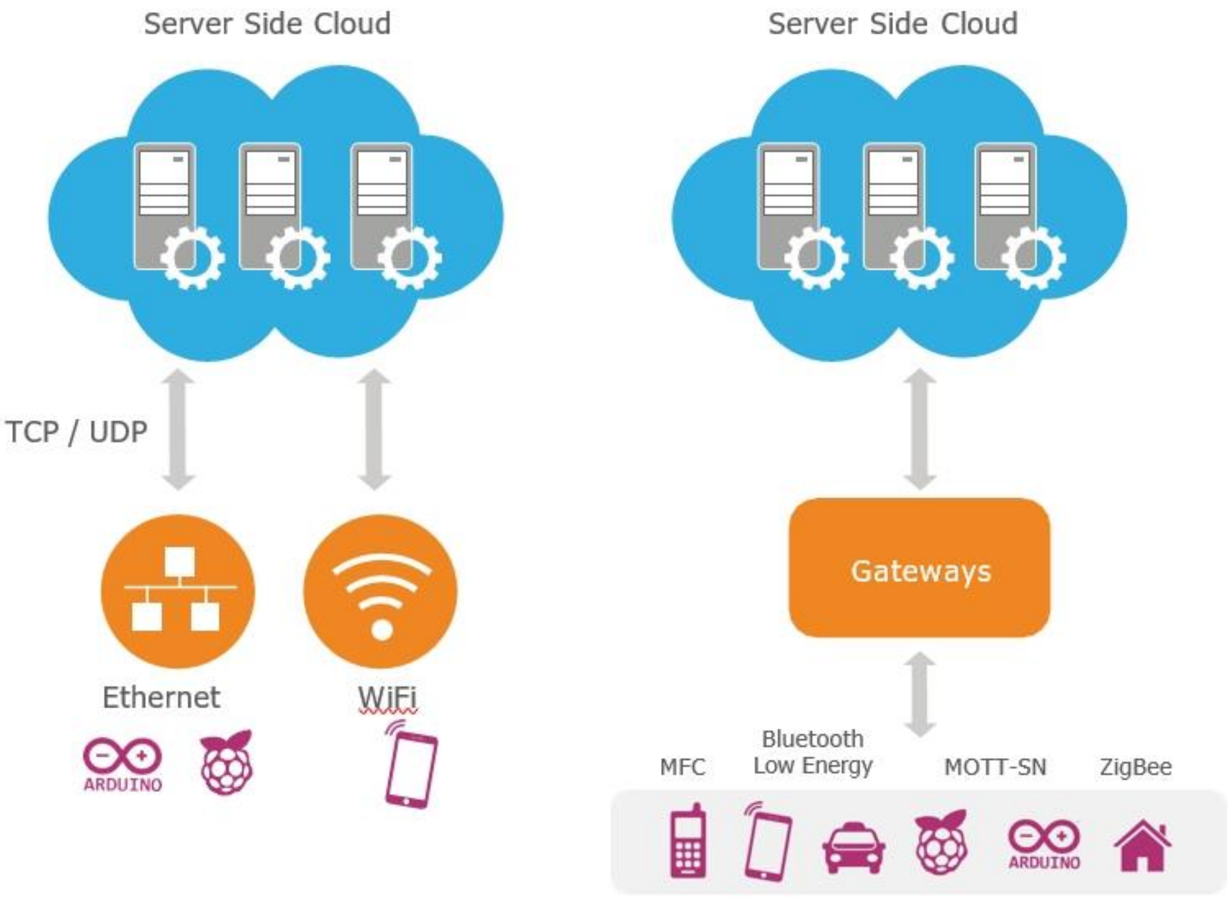

Figure 5 - Two major modes of connectivity

3.2.1 IoT centralized architecture development process

In order to combine many different devices and sensors together, creating the same network, it is necessary to carefully consider its architecture. The task of developing an architecture is quite difficult, since it is necessary to make sure that a lot of heterogeneous devices, as well as their business models, merge together, organizing a chain where each of them could convey the necessary information to each other. In other words, it is necessary to bridge the gap between the real and virtual worlds. Researchers have been studying this issue for many years since the appearance of the first such networks. At the moment, there are many different protocols that define their interaction.

3.2.2 Issues

There are a number of other difficulties that need to be carefully analyzed at the stage of preparation for the construction of the architecture [20]:

1. **Identification and scalability**: this problem arises due to the fact that there can be a huge set of devices and sensors connected to the network, it is also necessary to take into account the fact that their number is not finite, and their list may expand. It is also necessary to think over such points as naming devices, ways of transmitting and processing data, and later identifying useful information.
2. **The ability to self-organize**: the key advantage of IoT is that devices should be able to work autonomously, without human involvement in the process, or with minimal human involvement.
3. **Compatibility**: Development of a common standard to facilitate the interaction of devices within the same network.
4. **Data management**: it is necessary to develop algorithms for processing the data received by devices.
5. **Security and personal privacy**: one of the main and most difficult tasks of network development, since data in this case is of the highest value.
6. **Energy efficiency**: it is necessary to consider how each of the devices will receive the necessary amount of energy to maintain its operability.

3.2.3 Enabling Technologies

Developing an IoT network is possible only with the use of assistive technologies. Below is a brief description of the technologies that are used in the network most often.

RFID.

RFID is a technology that allows to automatically identify objects and read from them the necessary data for RFID tags. The label is a kind of chip in which information about the object and its environment is stored. The reader scans such a label and processes the received data. It is also necessary to have software that is able to connect everything together.

The process of using this method is as follows: the data obtained thanks to the reader, which was originally stored in the chip, and that already transmits the data to the system itself, which contributes to the rapid and autonomous recognition of objects. Most often, this technology is used for accounting and inventory management, that is, each item in the warehouse is a kind of smart object.

Wireless Sensor Network (WSN)

Wireless sensor networks, which are widely used in IoT networks and are capable of connecting the physical and computer worlds, consist of many miniature nodes equipped with a low-power transceiver, microprocessor and sensor [75]. Wireless Sensor Network (WSN) refers to a group of spatially dispersed and specialized sensors for monitoring and recording physical environmental conditions and organizing the collected data in a central location. NSW measures environmental conditions such as temperature, sound, pollution levels, humidity, wind, etc. [21].

NSHV are spatially distributed autonomous sensors for monitoring physical or environmental conditions, such as temperature, sound, pressure, etc., and jointly transmitting their data through the network to the main location. More modern networks are bidirectional, they collect data from distributed sensors [22] and allow monitoring the activity of sensors [23].

The NSHV consists of "nodes" - from several to several hundred or even thousands, where each node is connected to one (and sometimes several) sensors. Each such sensor network node has, as a rule, several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interacting with sensors and an energy source, usually a battery or a built-in form of energy collection. "WSNs" [24].

Machine-to-Machine (M2M) Communication

This technology is aimed at transferring data directly between devices. The M2M system includes peripheral nodes where sensors are located that are able to read this or that information. After that, this information is converted into digital signals, which are transmitted thanks to various communication equipment. Currently, the GSM network is mainly used as a data transmission medium, which is suitable in almost any case, and is also inexpensive and reliable, and is capable of transmitting data both to objects at rest and to moving ones. The software in this technology allows to work with data, process it and transmit commands to devices.

M2M systems are autonomous, and therefore there is practically no human intervention.

M2M systems are autonomous, and therefore there is practically no human intervention, which is undoubtedly their advantage. But at the same time, M2M lacks generally accepted standards for machine-to-machine interaction at the application level, which can be called its main drawback, since it interferes with the interaction of DRG devices with each other [25].

LiDAR

Lidar (Light Detection and Ranging) is a technology that can measure distances by itself using light (pulsed laser). Lidar mainly consists of a laser, a scanner and a specialized GPS receiver. This technology is able to measure distances both in water and on land, which is why it is often used in the field of maritime navigation [26].

3.2.4 IoT architecture

Since the set of tools and technologies in the Internet of Things network may differ depending on the scope and purpose of using such a network, creating an architecture template that could fit any request is quite a difficult task. In [27] the author, having conducted a study based on the study of various types of Internet of Things architectures, as well as having derived a list of the main requirements for the architecture of such systems, compiled an architecture that he calls "reference" in his report. According to the author, the proposed reference architecture has no dependence on the service provider and the technologies used in the network.

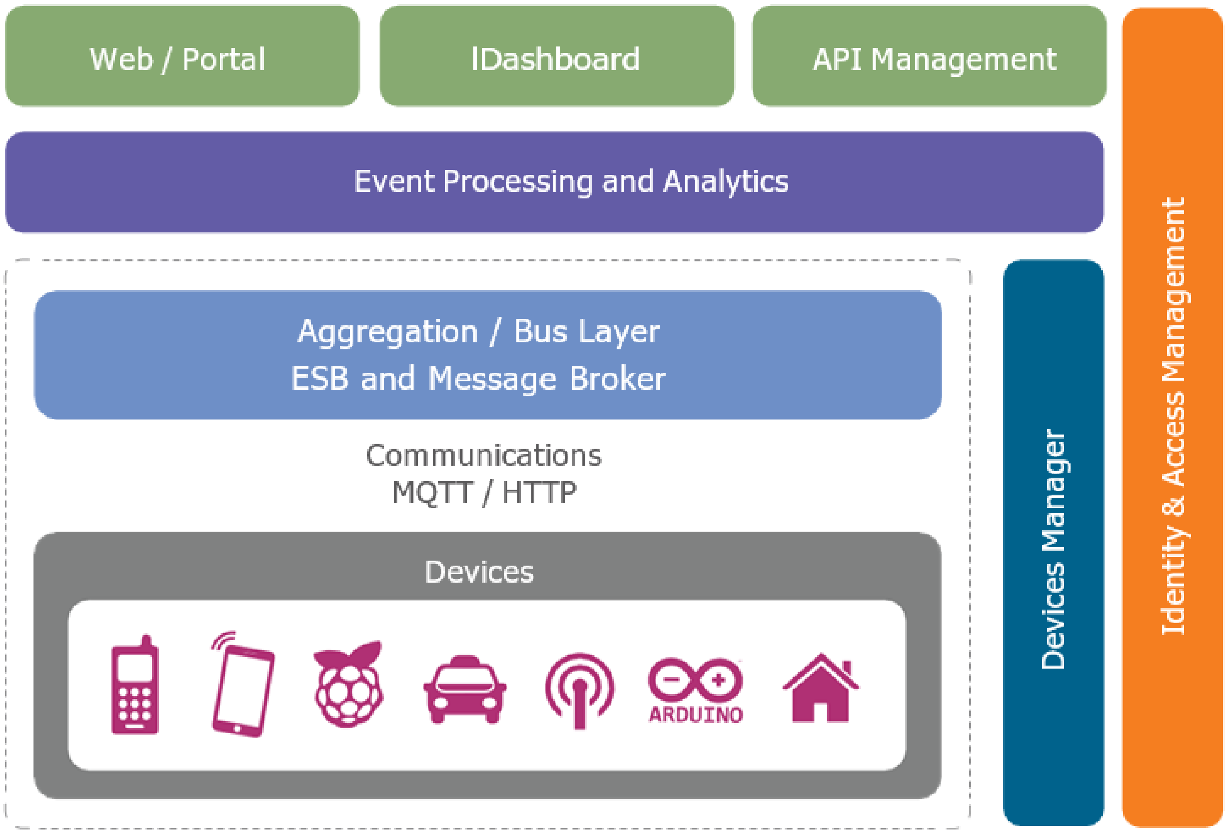

Figure 6 - The reference architecture develiprd by the author in [27]

Figure 6 shows the reference architecture developed by the authors in [27]. This architecture consists of the following layers:

1. ***Device layer.*** At this level of architecture, all devices that are capable of generating the data necessary for the user are represented. In order for a device to be able to exchange this data with other devices and systems, they need to have some means of communication, which are described in the next level of architecture.

2. ***Communications layer***. This level is aimed at maintaining a connection for real-time data exchange. There are many different protocols that support this exchange. In this case, the authors suggest using the MQTT protocol as the main one, due to having the following properties necessary when connecting to the Internet of Things [28]:

   - Neutral to the content of the message
   - Ideal for distributed one-to-many communications and disconnected applications
   - Equipped with the LAST (Last Will and Testament) function to notify the parties of an abnormal disconnection of the client

- Relies on TCP/IP for basic communication tasks
- Designed to deliver messages according to the templates "maximum once", "minimum once" and "exactly once".
- It is also assumed to use the HTTP protocol as an alternative variant.

3. **Aggregation / Bus layer**. This level is one of the most important, because thanks to it, the data transfer protocols mentioned above are supported, as well as data aggregation and integration between devices. Also at this level, the user's access to the system is checked by checking tokens.
4. **Event processing and analytics layer**. This level is designed for analytics and processing of all the data that comes from devices. They are processed through various programs designed for Big Data analysis. The main possibility here is the requirement to save data in the database.
5. **Client/external communications layer**. This level is aimed at providing the user with processed data in an intuitive way. The author suggests that the level should consist of three components:
   - Web interface, a platform on which charts and other dashboards will be displayed;
   - Dashboards, information panels, where all information will be presented in a human-readable form (graphs and other visualized data);
   - Managing the APIs that will be used between authorized systems.
6. **Device management.** At this level, devices that are connected to the network are managed using the device manager. The Device Manager also remotely manages the software and applications deployed on the device. If necessary, it can lock and/or erase the device. Also, the task of the dispatcher is to control device ids and their addressing with each other.
7. **Identity and access management.** The main task is to provide and control access to the system, issue and verify tokens, and so on.

It cannot be argued that such an architecture is suitable for any Internet of Things network, but it fully describes all the necessary requirements for a centralized network.

3.3 Smart transportation system

As mentioned above in the case of a smart home, the interaction of devices among themselves contributes to the improvement of monitoring and management of processes occurring in the same infrastructure, in connection with which humanity has gone further, and has begun to apply this kind of technology on a larger scale. This approach is particularly widespread in the field of transport, in particular transport networks within the city. The extremely rapid pace of urbanization encourages the city authorities to resort to the development of smart cities, the main advantages of which are to increase the efficiency, reliability and safety of human life in the city. One of the most important problems of cities with millions of people is endless traffic jams, which have a negative impact on the life of a city dweller, as well as on the development of urbanization in general. Thus, an important aspect of the development of smart cities is the development of smart transport systems that can provide citizens with faster, cheaper and more environmentally friendly ways of moving around cities [29].

In order to build a smart transport network inside the city, it is necessary to equip all vehicles, as well as roadside infrastructure with intelligent sensors and communication units, which will allow collecting traffic data in real time, using information, computing, communication and control technologies, and then using vehicle communication networks (V2V) and vehicles and infrastructure (V2I) to exchange them. This approach will make it possible to provide users (drivers) with analyzed information in real time, which will contribute to improving road safety, as well as reducing traffic congestion. [30], [31]. Systems that use various technologies for data collection and analytics are able to independently manage the following issues [76]:

- travel and traffic management;
- public transport management;
- electronic payments;
- management of commercial vehicles;
- emergency management;
- advanced vehicle safety systems;
- maintenance.

The figure 7 [32] shows a general model of urban smart transport components that interact with each other and exchange useful data within the same Internet of Things network.

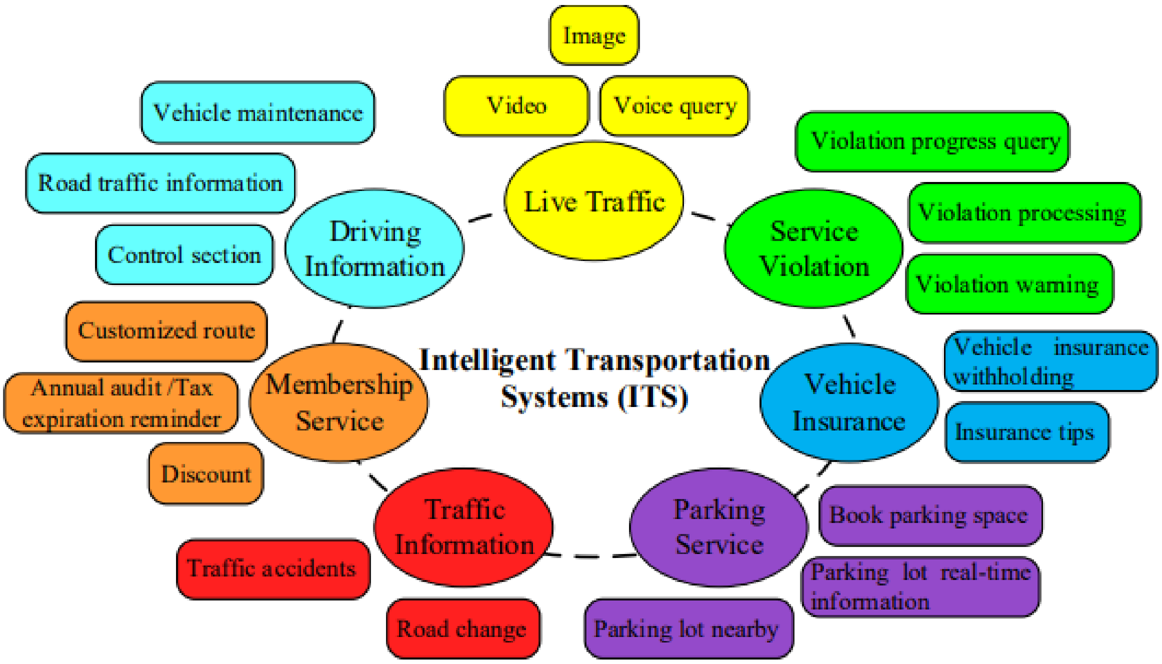

Figure 7 - Smart Transportation System model [32]

All these components are part of the movement of people from one point of the city to another, analyzing and tracking the data received, there are a huge number of opportunities to build a smart city whose residents will be able to move comfortably, safely and quickly within its borders.

3.4 Vehicle-to-Vehicle (V2V) Technology

V2V is a technology that contributes to making the transport system autonomous, where cars are able to exchange data on the state of the road in real time, which will improve road safety, as well as make the process of moving inside the city faster and more comfortable. Unlike M2M, M2M is aimed at integration into intelligent transport systems, and is being developed as part of intelligent transport systems (ITS) [33].

This method of data transmission from vehicle to vehicle allows to reduce the bandwidth between road infrastructure facilities and the vehicles themselves, and also helps to reduce operating costs. [34].

V2V networks allow to provide both another vehicle and the driver with a complete picture of the situation on the road, for example, about accidents, traffic jams and other things, which is much more useful information in comparison with parking sensors and other things [35].

3.5 The basic architecture of an intelligent transport system

In [36] the authors assume that the basic architecture of an intelligent transport system consists of three main levels: the physical layer, the communication layer and the service/application layer, as shown in Figure 8.

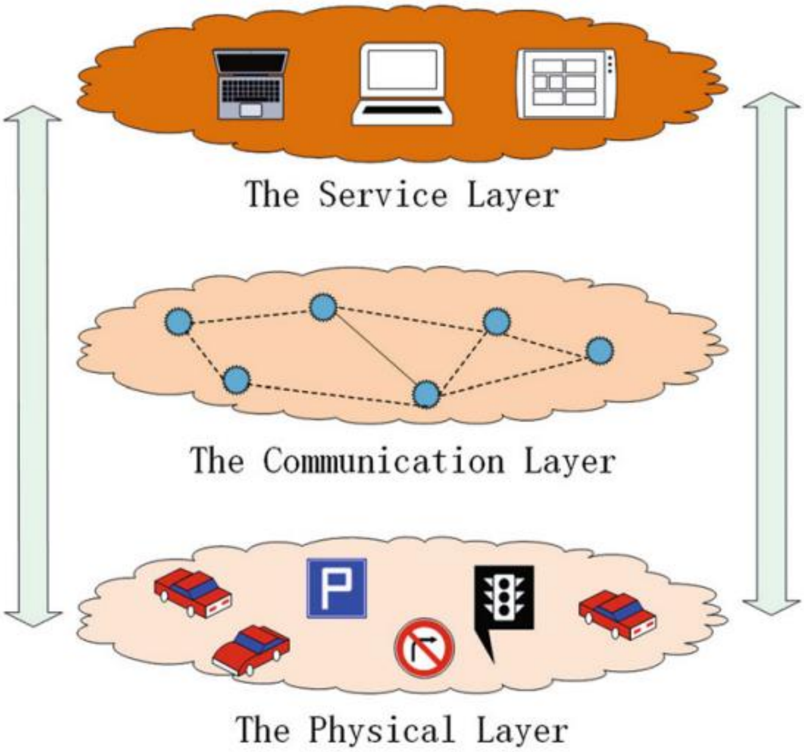

Figure 8 - Basic architecture of an intelligent transport system

Physical layer: this level includes the physical components and subsystems of the transport system. It includes various kinds of intelligent sensors located in vehicles and in road infrastructure facilities (traffic lights, road signs, etc.). Control units are integrated into these sensors, whose task is to process the generated data, as well as communication units, thanks to which data is transmitted to the communication level.

Communication layer: this layer consists of wired or wireless communication channels that support data exchange between devices and the transport system. V2V and V2I communication is also provided at this level. Also, various components and technologies (routers, Bluetooth, WiFi, and so on) that support data transmission are integrated.

Service layer: This layer is designed to output data to end users, providing them with safe and efficient travel services. In other words, this level can be called the application level, which is the main link between a person and intelligent road devices.

3.6 Smart Port as a part of Smart transportation system.

In the previous sections of this thesis, the urban transport system was considered, which is primarily aimed at improving the movement of urban residents. But passenger transportation is only a part of all transportation. Cargo transportation is also of great importance for a city dweller. The Internet of Things network can also be used for cargo transport both on land and on water.

Sea cargo transportation is the main link between Asia and Europe. So, for example, according to the sources of Eurostat [37] and the diagram shown in Figure 9, in 2020, despite coronavirus restrictions, which also had a detrimental effect on trade, an average of 7.4 tons of cargo per person was shipped in ports across the European Union.

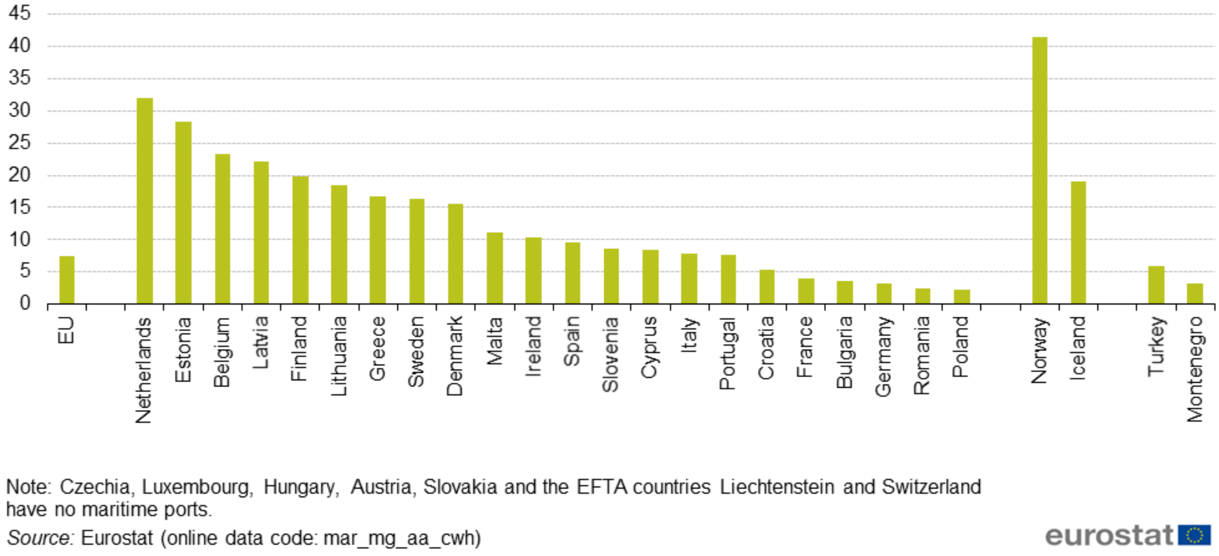

Figure 9 - Gross weight of seaborne freight handled in all ports, 2020 [37]

Due to the heavy workload of ports, especially the large ports of Rotterdam and Hamburg, it can be difficult for a person to accurately monitor all processes, serve the port in terms of loading and loading containers, moving them inside the port, as well as outside it. As a result, some of the processes inside the port were automated. Figure 10 shows a general diagram of the process of transporting goods by sea, how this process looks in general, without taking into account special cases. Port calls are complex logistics processes involving multiple stakeholders, where it is necessary to ensure the safety and efficiency of the ongoing processes. Modern technologies make it possible to increase the level of services provided by seaports, significantly increasing their productivity and efficiency. The innovations that are applied in modern seaports today make world trade more efficient and secure, making the supply chain more transparent.

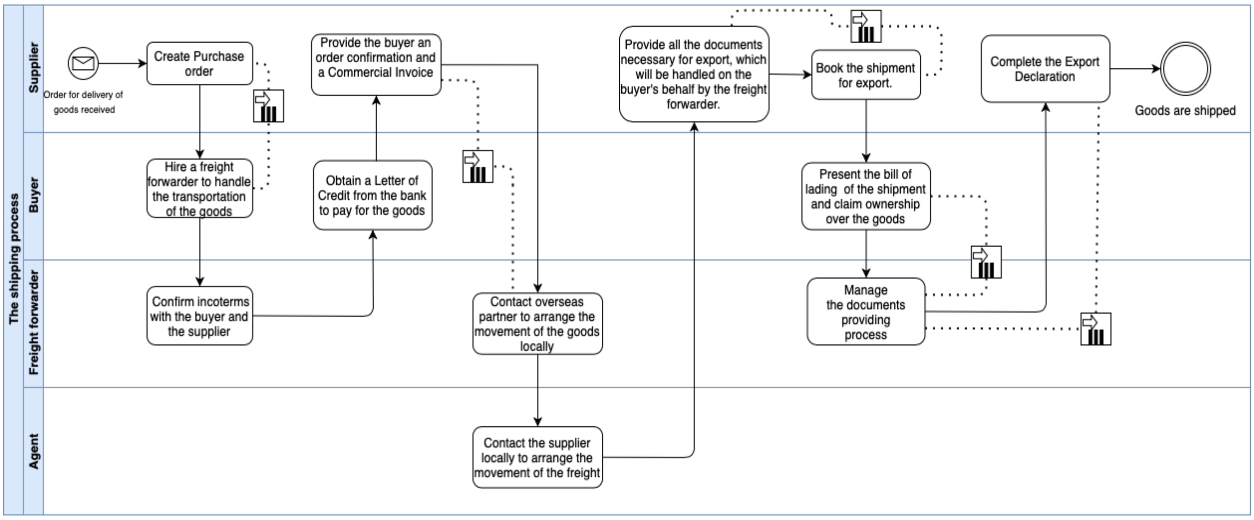

Figure 10 - The shipping process

Heilig, Schwarze and Voß (2017) in [38] presented their research on the topic of digital transformation of the seaport. In this study, the authors distinguish three generations of port operations and management, where the first generation is paper document management, the second is automated procedures and electronic documents, the third is intelligent procedures, where the machine is able to make certain decisions independently. But already at the first level of port construction in the 80s of the 20th century, managers were looking for solutions on how to reduce paper processing in inter-organizational business processes.

The processes of the second generation of seaports, which existed in 1990-2000, have already been partially automated, in particular, the first IT solutions aimed at automating container handling procedures at container terminals appeared in the port of Rotterdam. The ECT (Europe Container Terminal) terminal, located in the port of Rotterdam, was the first terminal in the world to use automated conductor vehicles at the terminal for container transportation [39].

The third generation of development, according to the authors [40] in seaports began in 2010 and continues to this day. Data is one of the main values of the enterprise, as a result of which the introduction of modern technologies such as machine learning, the Internet of Things began, which connected objects to which various sensors are connected, the use of which is aimed at improving the collection, processing, analysis and transmission of this data, of which a huge variety is generated. All this is done in order to eliminate inefficiencies and bottlenecks both in its port infrastructure and in transport flows. In addition to this, monitoring and data transmission in real time will increase the responsiveness and decision-making regarding events that deviate from their original schedule [39].

The Port of Rotterdam researchers have also developed a model of the digital maturity of the port, which is represented in the figure 11 [41]. This study is aimed at describing the development of a worldwide network of smart ports. Each port, in order to become smart, must go through a path consisting of 4 consecutive steps, which the authors recommend following, describing each of the steps in detail. The purpose of data exchange between ports is to make processes more intelligent, efficient and thereby increase the value of the supply chain [41]:

- *Level 1.* Digitization of individual sides in the port.

  The introduction of a Port Management System (PMS) is the first step towards becoming an intelligent port. This system is implemented separately on each side of the port. PMC assists parties in the administrative and financial processing of port calls, dock planning and cargo handling.

- *Level 2.* Integrated systems in the port community.

  The next step is to create a common system, the central platform of the Port Community System (PCS), which connects all the components developed in the first step, which allows the port to work as a whole. PCS forms a neutral base for digital information exchange within the port community.

- *Level 3.* A logistics chain integrated with the hinterland.

  Next, it is needed to connect PCS to the Internet of Things with the entire port infrastructure. This step is necessary either to create or to use tools to visualize the supply chain, network planning, tracking and tracing of shipments and conditions. Such a chain will allow to receive information about the location of the cargo, the transit calculation time, choose the fastest and most efficient route, as well as generally process the cargo more quickly.

- *Level 4.* Connected ports in the global supply chain.

  At this level, connected communications extend to other ports, and those, in turn, have a digital connection to their hinterlands. This makes possible the so-called digital door-to-door logistics chain on a global scale.

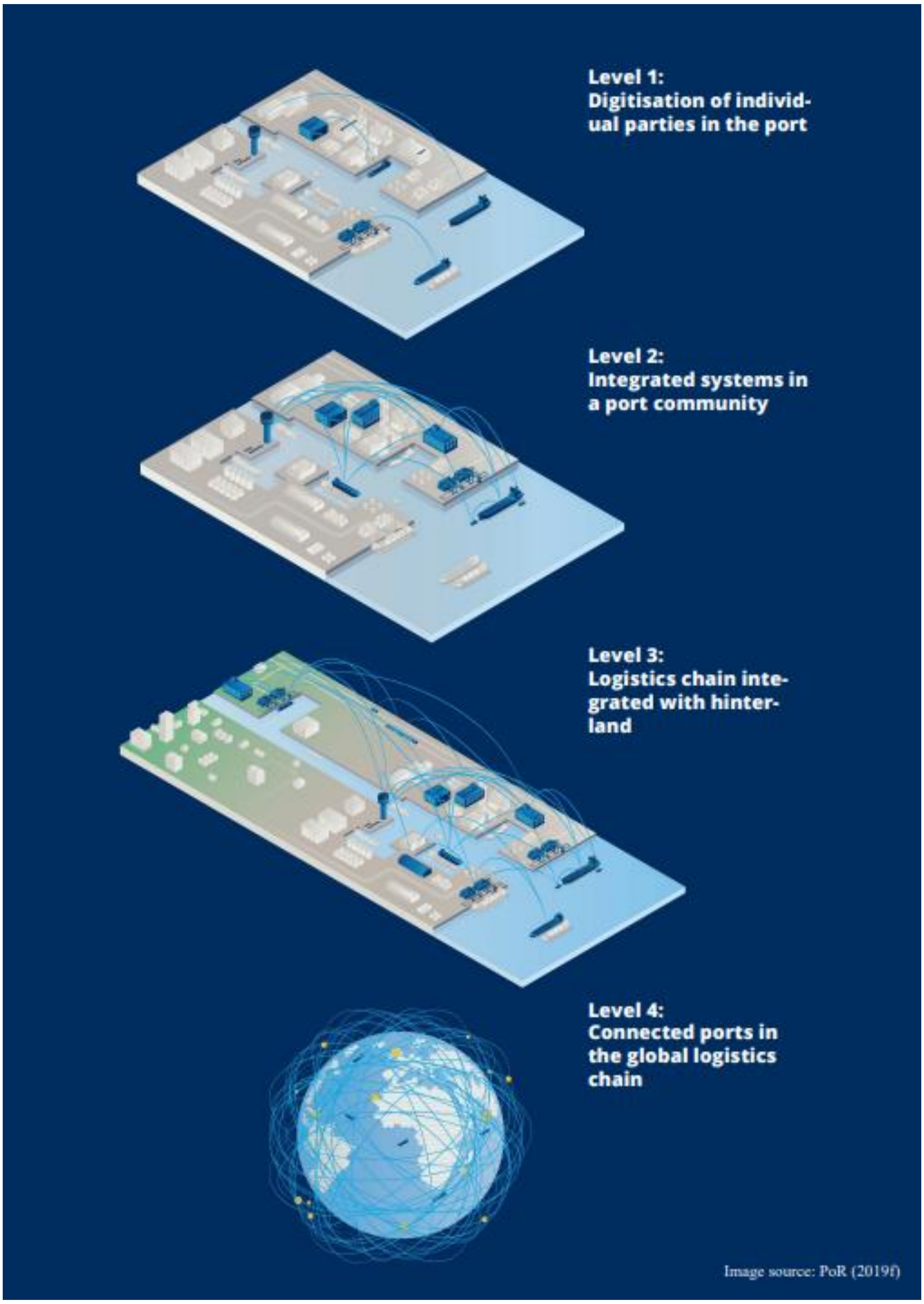

Figure 11 - Port digital maturity model

A good example of using the Internet of Things network in a seaport is a system that is deployed in the Port of Rotterdam, Pronto is a common digital platform for exchanging information about port calls in real time. Pronto receives information about the departure or arrival of the vessel from all connected stakeholders. Pronto creates a single point of truth based on this data [39]. In case any unforeseen circumstances have occurred, the vessel has deviated from the predicted schedule, Pronto sends notifications and warnings to all relevant stakeholders about this deviation and the new expected arrival or departure time. Thus, it tends to increase the efficiency of port entry and works on timely departure.

Various kinds of sensors send data to analytical panels, where the received data are processed and provide the necessary information to a person. An Automatic Identification System (AIS) has also been introduced, which is a signal emitted by ships that includes their location and speed..

In the port there is not only tracking of ships, but also trucks and other vehicles used on land. For example, RFID tags are installed on these machines, which are used to identify and monitor their activities. Container terminals are also equipped with optical character recognition systems (OCR) [42], which are able to independently read the code, which is the serial number of the container. Thanks to this, it is possible to get all the necessary information about its owner, contents, previous trips and much more. Thus, the container terminal can automatically identify the container and knows where this particular container should go or who is assigned to pick it up [39].

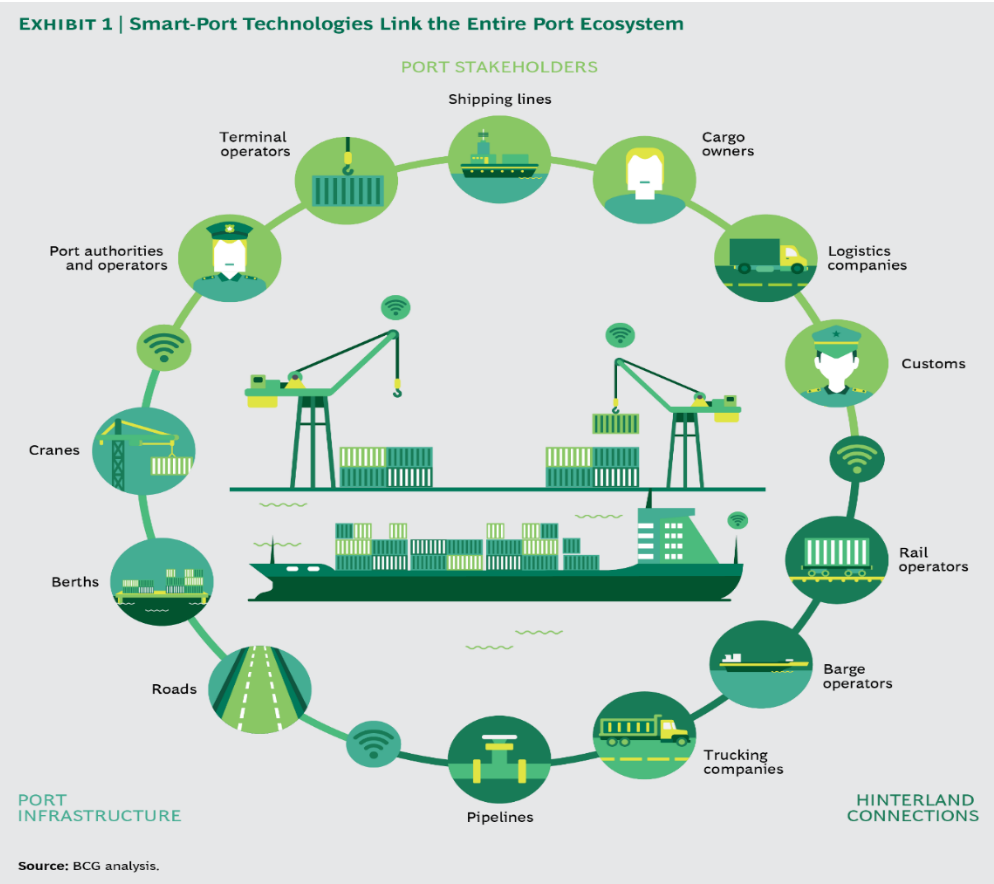

Figure 12 - Port Ecosystem [43]

In addition to the specific scenarios for the application of the smart port concept presented above, Figure 12 also shows other elements of the port that are part of its overall ecosystem and can be partially or fully automated.

4 Research methods

4.1 Grey literature

In order to answer the research questions posed, it is necessary to choose the correct research methodology. Undoubtedly, the best option of all possible would be to conduct interviews with representatives of companies (ports) that are already using the technology of the decentralized Internet of Things, in order to identify their current infrastructure, problems that can be solved with the use of this technology, as well as to identify their views on its future expansion beyond the smart port and transition to a smart the city.

Due to the fact that in Russia at the moment, blockchain technology is generally not widespread in ports and the impossibility of conducting interviews due to the different reasons, I chose a methodology called Multivocal literature review. Due to the fact that academic literature, due to its rather long publication process, is capable of incurring losses in terms of relevance and a small number of articles suitable for a particular study, so-called gray sources - unpublished or peer-reviewed sources of information will also be used in this work.

The main advantage of gray sources is that they carry practical knowledge and real experience. Practitioners often lack the time or desire to publish their work in academic sources, so they share their experience on various forums and websites by publishing blog posts and video presentations.

In his research, Vahid Garousi argues that the time and organizational efforts spent on conducting interviews go by the wayside, since an extensive database of public knowledge in the field of software engineering is already available online and can be quite conveniently analyzed and summarized by researchers. (The need for multivocal literature reviews in software engineering: complementing systematic literature reviews with grey literature) Each implementation of a particular technology for a particular enterprise is unique, and academic sources are often aimed at solving common issues.

4.2 Snowballing in Systematic Literature

There are several methods of literature search [44]:

- Protocol driven – compilation of the literature search protocol and the literature list itself before starting the study;

- Snowballing is a method in which literature is searched by finding the original source, and then using citation sources and vice versa. The process proceeds gradually;
- Personal knowledge – this method is suitable for conducting your own empirical research, relying only on your own research and research of acquaintances.

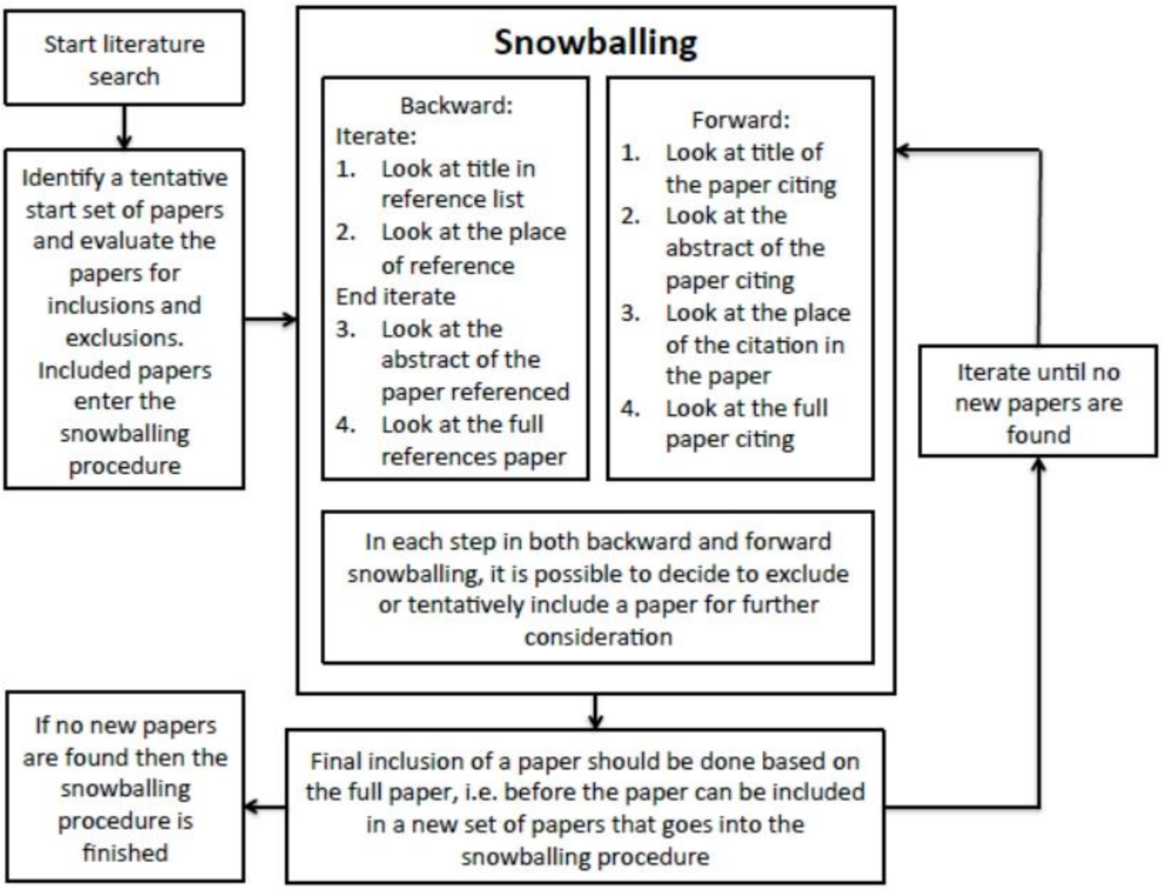

Figure 13 – Snowballing method description

In order to conduct this research, it is first necessary to determine the list of the literature being studied, as well as choose a method for searching for it.

The author chose the snowballing method for a number of reasons described below. The main advantage of using this method is the fact that the study is cross-disciplinary, so the use of different technologies and how they can work together is considered, as well as both technical and organizational characteristics. The fundamental advantage of using snowballing is that it focuses on cited or referenced articles, which reduces the noise level compared to the database approach. [45].

There are also a number of other reasons, for example:

- Difficulties in forming an accurate source search, due to the risk of obtaining a number of irrelevant articles;
- The ability to use multiple databases;
- The method is suitable for expanding existing literature reviews with new aspects.

In this research, the author adheres to the method and structure described in Wohlin's [46].

Initially, it is needed to define keywords and search strings. In this case, it is necessary to develop search strings in such a way as to avoid the problem of ambiguity and inaccuracy in the context of the research questions posed, in particular, a full-fledged literature search is used to answer questions RQ3, RQ4 and RQ5. Firstly, the author has identified 3 main groups of topics that include this study, as well as keywords and phrases:

1. **RQ2/RQ5** Cross-industry use of the decentralized Internet of Things: BLOCKCHAIN AND INTERNET OF THINGS, BLOCKCHAIN FOR IOT, USE OF BLOCKCHAIN FOR THE INTERNET OF THINGS, BLOCKCHAIN-BASED ARCHITECTURE FOR IOT, BLOCKCHAIN AND IOT INTEGRATED APPROACH.
2. **RQ3** Using a decentralized Internet of Things network in smart port processes: BLOCKCHAIN FOR IOT IN MARITIME, IOT IN SMART PORT, DECENTRALIZED IOT APPLICATION IN SMART PORT.
3. **RQ4** Using a decentralized Internet of Things network in urban transport networks: BLOCKCHAIN AND IOV, DECENTRALIZED APPLIZATION IN SMART TRANSPORTATION, DISTRIBUTED LEDGER TECHNOLOGIES IN INTELLIGENT TRANSPORTATION.

The search string was compiled based on research questions and keywords derived from them, including synonyms and alternatives. The list of lines was developed iteratively and expanded along the course of the literature search process, by searching for certain combinations of words. The Google Scholar database was used as a source base, since its interface is suitable for searching for citation sources, and in the opposite direction, which is necessary when using the snowballing method.

Other limitations on the search for literature are the following searching parameters: scientific articles (including articles from grey sources, such as platforms describing use cases of already implemented projects in the field of smart transport), English or Russian language, open data sources, for RQ4 and RQ5 practical evidence.

5 Results

This chapter presents the results of the systematic literature review process, which was carried out using the forward snowball method.

According to the results of the search for articles in the Google Scholar database with the specified parameters, the system gave an average of about 4000 – 10000 results. In view of the fact that it is quite difficult to process such a huge array of information manually, it was decided to process only the articles on the first three pages, since the algorithms display them as the most relevant and most suitable for the specified query criteria. The first processing of articles took place by reading the title of the article, the abstract, as well as searching the document for the words "IoT" and "Blockchain".

After the first processing of the literature found, an initial list of sources was compiled, which will expand with each iteration. The Start set included 20 articles that were divided into three categories:

- Cross-industry use of the decentralized Internet of Things;
- The use of decentralized Internet of Things network in smart port processes;
- The use of decentralized Internet of Things network in urban transport networks.

In this study, at the iteration stage, the author used the direct snowball method, that is, citations in articles that were included in the Start set were considered. In the first iteration, a total of 176 articles were reviewed, of which only 64 were relevant for the current study. After the second iteration, where a fairly detailed screening of the entire article was carried out, 26 articles were selected, which are included in this work. These articles were also divided into 3 categories:

- The decentralized approach of the Internet of Things – 13 articles;
- The decentralized approach of the Internet of Vehicles – 11 articles;
- The decentralized approach of the Internet of Things in Smart Port – 3 articles.

Also, the category "The decentralized approach of the Internet of Vehicles" was also divided into 8 subcategories, the results are presented in Table 2.

The following chapters contain the results of the literature review, as well as answers to the research questions posed.

6 Blockchain and IoT integration

This chapter includes blockchain technology overview, and also possibilities of its integration with IoT network.

6.1 What is Blockchain technology and what is the principle of its operation?

This chapter includes basic information about the blockchain technology itself, its principle of operation and the main advantages compared to a standard database. The results of this chapter contribute to the continuation of research on the use of blockchain in collaboration with IoT.

6.1.1 Blockchain definition

Blockchain is a distributed database of records or a public registry of all transactions or digital events that have been executed and transferred to participating parties [47]. Each transaction in this approach must be confirmed by the consensus of the majority of system participants who have the authority to do so [47]. The information in this case is immutable [47]. The blockchain stores information about transactions in such a way that each record in the database can be verified [47]. The main purpose of implementing a distribution registry is to provide a trusting environment for each of the participants. Thanks to this approach, the possibility of forgery of information or documents contained within the database is almost completely excluded.

Table 1 presents the characteristics of three possible types of blockchain, which are based on accessing data in the system, viewing, downloading and supplementing them.

Table 1 - Types of blockchain overview [48].

Property	**Public blockchain**	**Consortium blockchain**	**Private blockchain**
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Public of restricted	Public of restricted
Immutability	Nearly impossible	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

6.1.2 Blockchain working principle

The blockchain is a chain of blocks, each of which contains one or another information, which includes data, the hash of the block and the hash of the previous block. The hash of a block is a unique code that serves as its identifier and is created during its creation. If one of the participants in the chain changes this or that information, the system will automatically reflect these changes in the hash. The creation of the chain itself is possible thanks to the hash of the previous block. Figure 14 shows the basic structure of the blockchain.

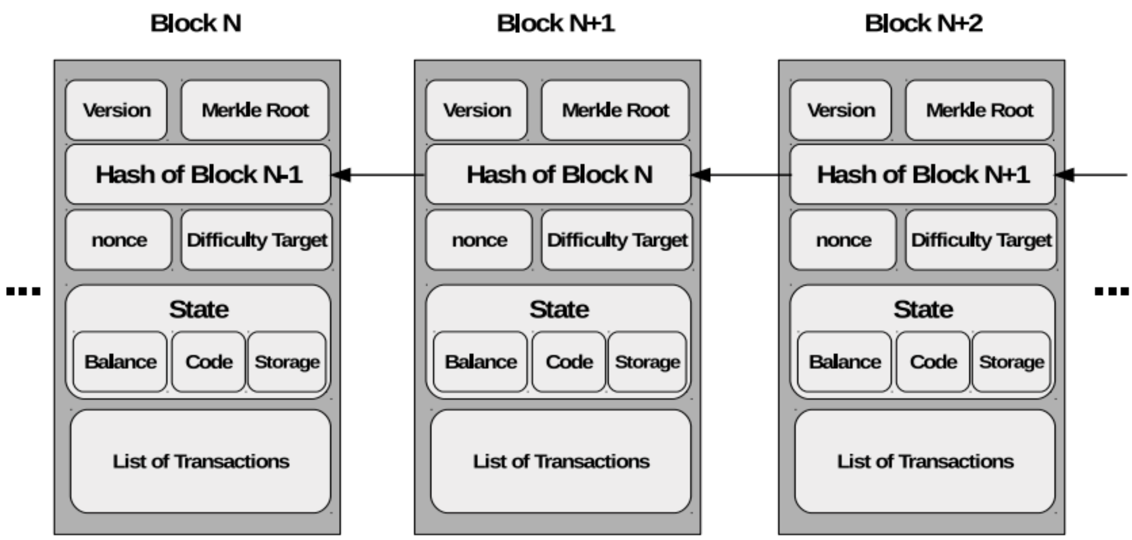

Figure 14: Blockchain design structure [49].

The "proof of work" mechanism serves to detect falsifications. Blockchain security is based on the combined use of hashing and proof of work.

The main and main way to protect data inside the blockchain is decentralization. As already mentioned in the thesis earlier, the centralized model is quite vulnerable, in the case of the blockchain, a peer-to-peer (P2P) network is used, accessible to everyone who can connect to it. When connected to the network, an authorized user receives a full copy of the blockchain, where a special node uses it to confirm the uniqueness of the chain.

6.1.3 Key Features and Advantages of Blockchain Technology.

The main features of the blockchain include: programmable, secure, distributed, immutable and time-stamped. Three of them can be called as a main – decentralization, traceability, immutability. Decentralization has the role of verification, storage, maintenance and transmission of data on the blockchain [50]. In this approach, mathematical methods ensure trust between distribution nodes [50]. Traceability ensures that transactions are arranged in chronological order. Communication between blocks is maintained using a cryptographic hash function [50], and a hash key allows to create a chain of blocks. When trying to change a transaction, different hash values will appear on the network and this will be detected by all other nodes performing exactly the same verification algorithm. That is why it is immutable [50].

It can also be noted the main advantages that the technology has are:

- Immutability of data and storage of all versions of documents in one place, while authorized and authorized users are able to view them.
- Ensuring full trust of all participants in the chain to the data stored in the database
- The absence of a database owner, each of the chain participants has the same authority
- This technology is able to create a common infrastructure of different scales, ranging from one company to the whole world

But the technology is not completely safe, and cases of cyber-attacks and fraud have already occurred. Undoubtedly, the introduction of such technology must be carefully considered, because often it is not able to solve specific problems.

6.1.4 Smart contracts

The general concept of smart contracts was proposed by Nick Szabo back in 1996 before the blockchain technology was created. Szabo proposed the following definition: smart contracts are digital protocols for transmitting information that use mathematical algorithms to automatically execute a transaction after the specified conditions are met and complete control of the process [51].

In comparison with the usual documentation, a smart contract is a code that is used to fill in all the necessary data and directly the signature of the chain participants. Smart contracts allow the system to independently confirm the conduct of certain transactions thanks to the "if – then" mechanism. That is, if one party fulfills its obligations, the system guarantees that the other party will also fulfill them. Other more complex algorithms can also be created. These contracts are stored in the blockchain and will allow to automate and betray greater trust to all stakeholders, and the personal data of users remains anonymous.

The advantages of smart contracts include the absence of the need for an intermediary, cost reduction (due to the absence of a third party), speed of registration (much faster than manually) and security (contracts in the blockchain cannot be lost, and the process of decentralized management eliminates the risk of manipulation).

6.2 Integration description

To date, there is a sufficient number of studies that are able to confirm the advantages of a decentralized Internet of Things network over a centralized cloud one. Thanks to the synergy of the Internet of Things and blockchain, the level of network security increases, which is the main point when deciding on the implementation of such a network.

To demonstrate the importance of this problem, consider the following example. In October 2016, the American DNS provider Dyn faced cyber attacks [52]. In this case, the attacks were directed from millions of different IP addresses. At the same time, the employees determined that some of them were sent from various kinds of Internet of Things devices, for example, from video cameras, refrigerators, routers, etc. It was found out that these attacks were of the "denial of service" type (DDoS), and they came from smart devices with the Mirai virus. The source of the infection was phishing emails, which contained this malware, which later spread to the entire home network.

The main security vulnerability for IoT applications is represented by centralized cloud storage. By applying blockchain technology, Internet of Things devices will become much more secure and this approach can be used in enterprises and networks of various scales.

The main obstacle to the development of the Internet of Things is the centralization of cloud services [53]. Huge amounts of data collected from IoT sensors and sensors have to, firstly, be transferred to a central cloud, which can lead to overload of transport communication networks, secondly, be processed in a centralized cloud, which requires huge capacities of servers and storage systems, thirdly, it is necessary to transmit back the results obtained, which may cause delays when managing online [53].

Distributed trust technology, which provides scalability, security and privacy, is the basis for the growth of Internet of Things applications [54]. This technology has been considered by business representatives in the last few years and IT researchers as a promising solution due to its internal properties that would be suitable for Internet of Things environments. As mentioned in the previous section, blockchain allows secure storage of confidential data and makes it available to Internet of Things devices [54]. Therefore, by its design, it can ensure security, confidentiality and the absence of single points of failure. At the same time, smart contracts will allow network participants to maintain and ensure consistency of operations between participants in accordance with predefined business logic. The main objectives of the introduction of blockchain into the IoT network is to ensure trust in the data stored on the network, as well as trust in the ongoing processes and their responsible parties. Thus, the decentralization of computing is an inevitable trend in the development of the Internet of Things [53].

According to IBM [55] the world is gradually moving to such a principle of data models, where all data warehouses are decentralized and a person no longer needs to independently verify the authenticity of information after all, every transaction is confirmed by all stakeholders. The model described above is the blockchain. Blockchain is able to provide the IoT network with full trust and security when interacting with various devices within the same network thanks to the confirmation and consensus model.

Figure 15: Transformation of device interaction models (source: IBM)

In addition, the blockchain allows to create a structure where it will be possible to safely store processed transactions, as well as coordinate devices located inside the network. Such devices together are capable of forming an "Internet of Decentralized and Autonomous Things", where the blockchain is a universal digital registry for performing transactions of various types between devices [53], for example:

- Device Registration;
- Authentication of devices and users;
- Device Security check;
- Real-time data exchange;

- And much more

6.3 Decentralized IoT architecture

Centralized cloud services have allowed the Internet of Things technology to become one of the main technologies used both in industry and in everyday life. But in order to ensure maximum transparency of data, the trust of all participants in the process and owners of devices located within the same network is necessary. Centralized cloud services can be called a kind of black boxes for IoT services, where IoT users do not have control over their data. In addition, centralized cloud services are vulnerable to failures and fatal security attacks [56] IoT can benefit from the decentralized network paradigm offered by blockchain, overcoming all the problems and obstacles mentioned in the work earlier. At the moment, the study and implementation of the integration of IoT and blockchain is still at an early stage of research and development, and there are still many problems associated with the seamless integration of IoT and blockchain [56].

Using blockchain to achieve absolute decentralization in IoT is problematic, given the variety of devices involved in IoT. Most devices on the IoT edge have limited resources to host a copy of the blockchain or participate in the verification of new blocks. Therefore, it is important to decide what role various objects (devices, gateways, etc.) will play at the IoT boundary.

To deploy public blockchains, alternative consensus algorithms, including Proof-of-Stake, are considered more suitable for deploying blockchains in IoT environments. Given the resource constraints faced by IoT devices, some design considerations are needed for their level of participation in the blockchain network. IoT devices do not have encryption capabilities, and also do not meet the requirements for computing and data storage when using blockchain consensus algorithms.

Many researchers have studied in their works possible options for how to connect the IoT network and the blockchain. In [56] the authors present the results of the analysis of alternative paradigms considered in the published literature.

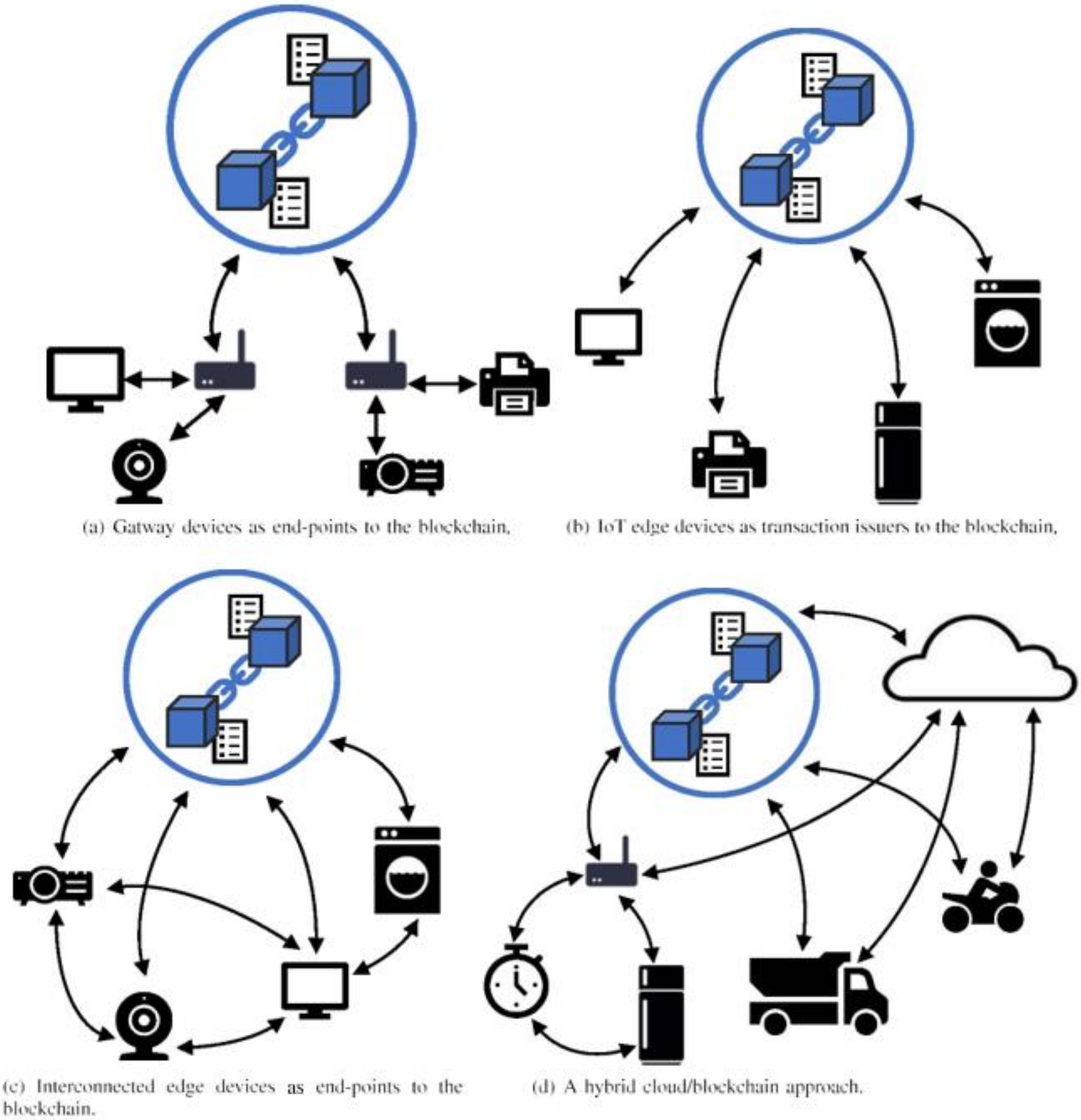

Figure 16: Possible options for the interaction of devices and blockchain

1. **Gateway devices as endpoints for blockchain**: Figure (a) shows an illustration of this approach. In this integration scheme, all communications pass through the blockchain, and the gateways of the Internet of Things act as endpoints for the blockchain network. This scheme can be used to authenticate devices connected to separate gateways with blockchain support [57]. At the same time, not all transmitted data should be stored in the blockchain. The blockchain carries a management function supported by smart contracts. In this case, data transfer is carried out using peer-to-peer technologies and data exchange occurs automatically.; but instead, reusable technologies for transferring documents or exchanging information between devices through a communication channel can be

implemented. However, recording all Internet of Things interaction events in the blockchain will increase bandwidth and storage requirements, and scalability will increase

2. **Devices as issuers of transactions in the blockchain**: Figure (b) illustrates this approach. This integration scheme is discussed in [58]. As in the previous approach, all events are logged by the blockchain to ensure a secure account. In this case, Internet of Things devices can be equipped with cryptographic functionality. The trade-off here is the higher autonomy of IoT devices and applications compared to the increased computational complexity of hardware.

3. **Interconnected edge devices as endpoints for blockchain**: Figure (c) illustrates this approach. In this approach, also described in [58], IoT gateways and devices send transactions to the blockchain and can interact with each other off-chain. Using routing and discovery protocols, it is possible to significantly reduce the latency between IoT devices. Such an integration scheme is more suitable for scenarios where interaction occurs much more often and requires high bandwidth and reliability of Internet of Things data.

4. **Hybrid of cloud and blockchain with IoT edge**: Figure (d) illustrates this approach. This approach allows users to use 2 methods of interaction, the first – through the blockchain, the second – between devices [58]. The choice of method depends on the setting of the event. When using this approach, it is possible to differentiate interactions according to the need for interaction with the blockchain. Hybrid approaches can use nebulous computing to overcome the limitations of blockchain-based IoT networks.

How the integration will be implemented, and which option is the most appropriate, depends on the requirements of a particular IoT application. For example, when immutable record keeping is required and a relatively small number of interactions occur, the first two schemes make more sense. In applications requiring higher performance, the use of blockchain alone may not be sufficient. In other use cases of the Internet of Things, devices and gateways should never be used as full-fledged nodes, since the overhead of data storage will not be able to justify the possible benefits [56].

In some cases, centralized models of the Internet of Things have certain disadvantages and limitations that can be canceled or mitigated by the decentralization properties of blockchains [59]. Blockchain creates the basis for the creation of decentralized Internet of Things platforms that provide secure data exchange and reliable message records.

7 Decentraliced Internet of Vehicles (IoV)

Many different researchers from different industries and spheres are studying the possibilities of using the decentralization of IoT networks, where the main idea is to protect the transmitted data. This section is aimed at reviewing the published literature, where the possibility of integrating Blockchain into IoT in the transport system is considered. In order to proceed to the applied analysis of the technology in question, the review contains literature that examines real use cases used in the technology called Internet of Vehicle (IoV).

IoV is a technology that ensures the interaction of vehicles, as well as objects of road and urban infrastructure in real time. This interaction is possible thanks to the use of intelligent terminal devices, vehicle navigation systems, mobile communication technologies and information platforms that allow to interact with information and exchange driving instructions, as well as control the network system [60]. This campaign greatly simplifies the processes of collecting, processing and exchanging data necessary for building an intelligent transport system.

This concept has become increasingly common in recent years, and building a fully autonomous transport system no longer seems like something fantastic. A significant number of IoT objects will fall on vehicles [15]. The popularity of the concept, as well as the rapid development of communication technologies, is the reason that many researchers and companies conduct a lot of research on this topic. Intelligent vehicles are connected to the Internet, thanks to which they can communicate both with other vehicles and with road infrastructure facilities. But despite all the advantages, the problem of data security is also acute in this concept. There are cases when attackers were able to hack into the Tesla control systems, and were able to gain access to the vehicle itself and its management. In order to avoid cases of hacking, researchers propose the introduction of blockchain technology to ensure the decentralization and hashing of information and data stored on the network.

Each of the following subsections is aimed at considering specific subject areas where IoV decentralization is able to solve certain problems. A brief overview of the articles under consideration is presented in table 2.

Table 2 – Possible application scenarios.

Application scenarios	Description	Paper
Vehicle communication	Opportunities for improving V2V and V2I communication, creating a secure network of interaction between all participants and traffic objects.	60
Vehicle Management	Autonomous vehicle control by creating a platoon of vehicles thanks to platooning technology.	61, 74
Data Management and Services	Methods of safe storage and exchange of data between road users, in which the provision of data is a service for which data owners can receive a monetary reward.	62, 63
Traffic contol	The use of a safe traffic control system will significantly reduce the number of traffic jams on the road, as well as the occurrence of traffic accidents.	65
Ride Sharing	Secure storage and data exchange between users of ride sharing services over the Internet.	67
Forensic application	Thanks to the IoV network, in which vehicles and transport infrastructure facilities are combined, as well as the storage and distribution of this data using blockchain technology, it will be possible to simplify decision-making in connection with the occurrence of a traffic accident.	68
Transportation Insurance	Creation of a new trust model of vehicle insurance, individual for each car owner.	69
Managing the transportation of dangerous goods	Due to the fact that the transportation of dangerous goods is regulated by law, stakeholders should receive up-to-date and authentic information about its transportation, which blockchain technology can provide in integration with IoV.	70

7.1 Vehicles communication

Vehicles exchange confidential information all the time, or messages, the delay in the transmission of which is unacceptable, for example, a warning about a dangerous section of road. It is difficult to provide security to VANETs networks, since they are capable of being subjected to various kinds of attacks, for example, "Man in the Middle" (MITM), which are aimed at wiretapping and distorting information throughout the network. DDOS attacks are used to disconnect users from the target network [60].

According to the authors [60], the blockchain concept is able to cope with such problems, and the nominal IT solution for vehicle communication (DISV). This solution implies that the server will analyze a certain block and issue a decision on holding a smart contract.

The aim of the authors of this article was to develop an IoV solution with a real-time application (RTA). Its essence lies in the fast and secure transfer of information between transport and transport infrastructure facilities. The development and testing of the prototype was carried out with a scenario in which information about a sleepy bus driver was transmitted to the nearest road users. This solution contains three levels:

- ***The physical level***. It includes the collection and recognition of environmental data and the determination of the position of intelligent objects located nearby. This can be done using a number of devices equipped with sensors. Two Android apps are included in this level:
    - for vehicles, examines data about the vehicle, its route, the driver's driving style;
    - for infrastructure, creates a digital twin of road infrastructure facilities.
- ***Network layer***, which is aimed at creating communication between sensors and servers, and other devices. In addition, this layer is designed for transmitting and processing data generated by sensors.
- ***Application level***. At this level, communication is maintained between all participants of the transport system through a Blockchain application. This level also includes a central cloud server, with which all the information received is examined and invitations are sent to new devices.

Based on the results of test studies, the authors have deduced three main directions of DISV:

1. A safe real-time application for road users;

2. Maintaining safe and simple interaction between people and traffic objects;
3. Improvement of the driver assistance system.

7.2 Vehicle Management.

To date, there is a trend in the development of autonomous transport, where the vehicle can be partially or completely independently controlled. In view of the fact that there are not so many such vehicles, entrusting the car with independent control is not the best option. Platooning is a fairly common approach when transporting goods by trucks, when trucks are connected in a chain and move in a platoon on the section of road where their routes intersect. This concept is also applicable for passenger transport within the city. The platoon has a platoon leader and platoon members, where the first one controls his vehicle, and with it the entire chain. All members of the chain must keep a distance between each other, which is determined automatically.

The advantages of this approach is that it helps to improve traffic capacity on the roads, and with it reduce the number and length of traffic jams. Another advantage of platooning is the reduction of energy consumption, which is why fuel costs are reduced [61].

In order to choose a platoon head (PH), [74] provides a reputation value to help ensure an economic balance between the platoon members (PM). Each designated supervisor will have to travel a certain distance and receive a service fee from the PMs.

The authors claims in their work that the blockchain in this network can guarantee the confidentiality and integrity of shared information. The system should track how much fuel the platoon has spent and distribute the funds spent among the platoon members. In addition, the author suggests the use of smart contracts in order to establish automatic payments. The process of how smart contracts will be implemented inside the system is indicated in Figure 17, where MD is the matching degree, and under the specified circumstances, the application for joining the platoon must be approved.

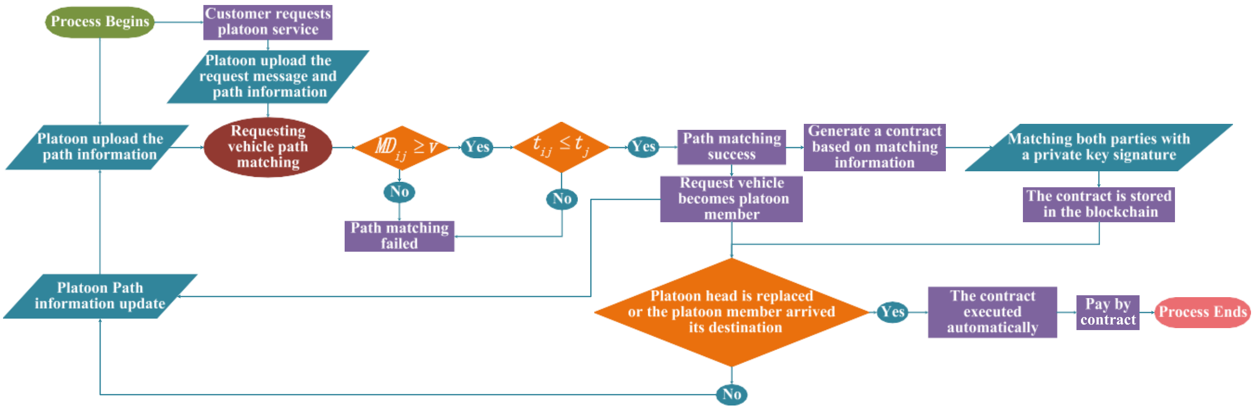

Figure 17: Process usage of smart contracts

The simulation results showed that the urban platoon mode is much superior to the individual vehicle mode in terms of fuel consumption.

7.3 Data Management and Services

Mirko Zichichi et al. in their article [62] consider the possibilities of using the architecture of a transport system using distributed registries in order to create, store and exchange data using sensors on users' devices or vehicles during their movement. The motivation of the authors of the creation and testing of such a system architecture is the fact that the transport system is developing in huge steps, and in the near future a situation is possible when the traffic flow will be controlled not by people, but by computers, thanks to the huge amount of data that the system receives and processes from various sensors, both from the vehicle itself and from infrastructure facilities. On this basis, it is necessary to create sophisticated intelligent services aimed at improving traffic management and transportation safety. Currently, there are many different technologies and systems that can ensure the operability of the transport network, but at the same time, due to the scalability problem, as well as the unreliability of the transmitted information, it can adversely affect the entire chain, since the transmitted data can be changed and is not authentic. In this study, the authors consider the use of Distributed Ledger Technology (DLT), as this will allow network users to trust the exchanged data, since there will always be an opportunity to verify their authenticity and immutability. The attractiveness of these technologies is mainly due to the fact that they exclude the possibility of downtime or interference by third parties. As a result, studies that have improved DLT and distributed data storage systems [63] have gained additional interest from researchers.

In the architecture proposed by the authors, data exchange services and user sensors can exchange data with each other. The proposed infrastructure is based on DLTS in combination with other decentralized file storage (DFS) technologies. Smart contracts regulate access to data for authorized users. Storage and use of data coming from vehicles are provided by IOTA [64] and DFS. In addition, the proof of zero knowledge is used as a scheme to ensure confidentiality while providing guarantees of location confirmation. Figure 18 shows the process of how the parties will exchange data within the network. Sensor owners receive data from their devices, after which they can provide it to consumers using DLT and smart contracts. Consumers can create new data or provide intelligent services available to individuals.

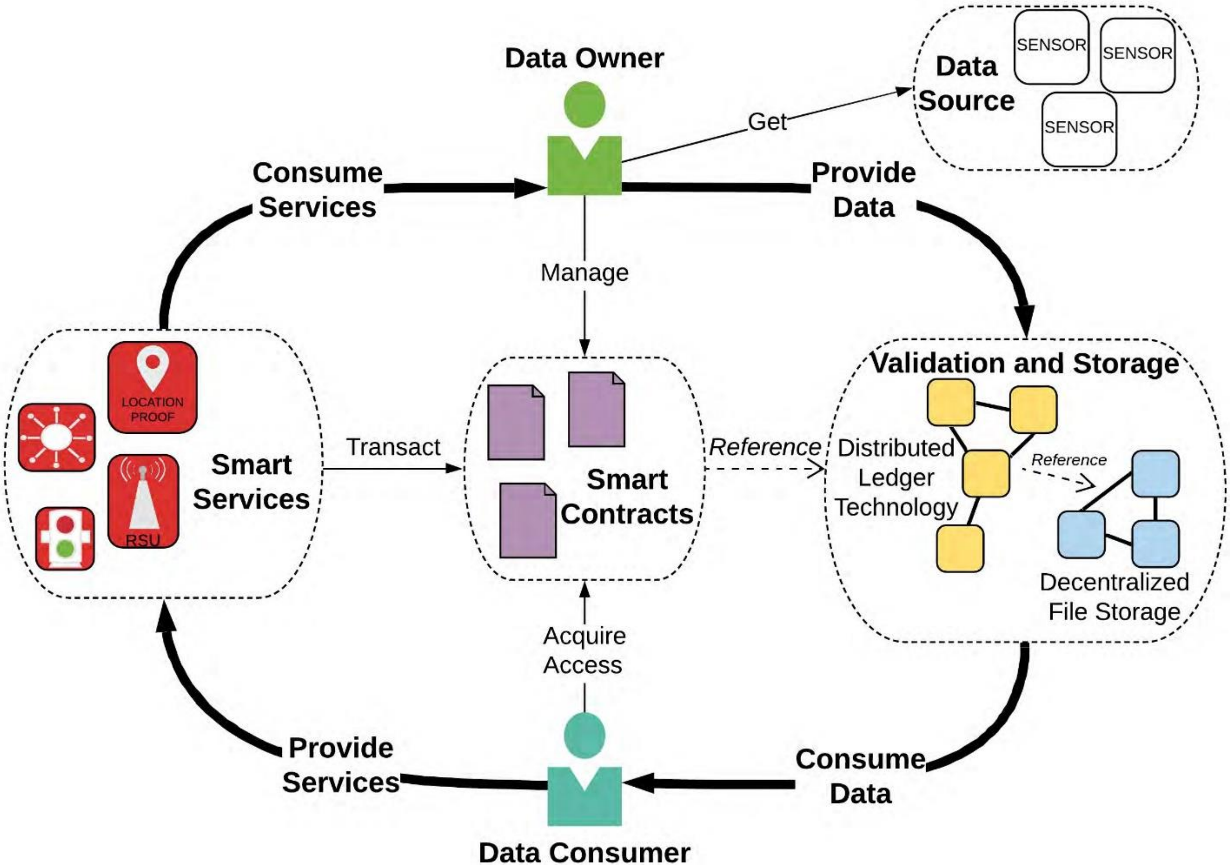

Figure 18: Data exchange flow

Figure X shows the layers of the architecture proposed by the authors, where:

- ***Presentation layer*** is responsible for implementing a clear interface between architecture and the real world;
- ***Service Layer*** is used to provide intelligent services to network users;
- ***Transaction Layer*** is designed to control access to data, which is carried out using smart contracts;
- ***Validation Layer*** ensures the integrity and authenticity of the data used through the use of DLT;

- ***Data Layer*** includes technologies that provide data storage through replication.

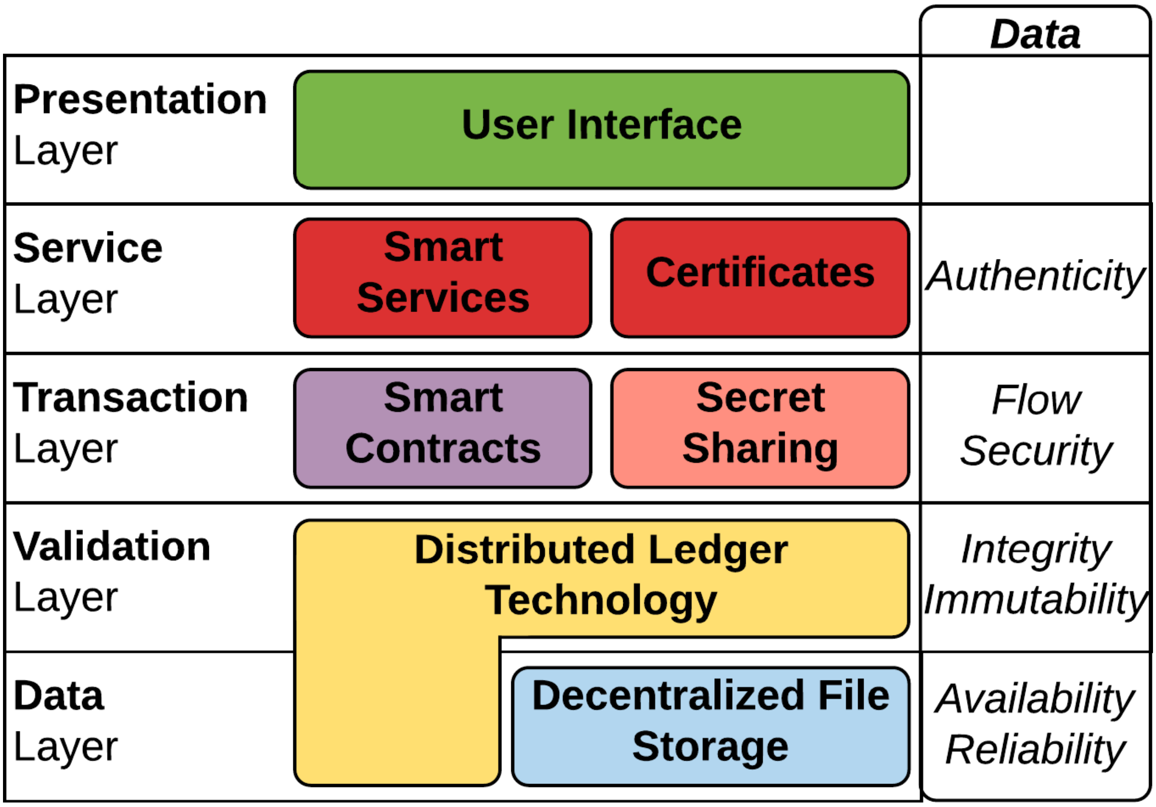

Figure 19: Architecture layers

This study is also notable for the fact that it was tested on generated data that mimics the movement of buses inside the city. In this case, only location transmission was considered, for which a Location Confirmation certificate was created and used. The main idea is that data owners can transfer their data to an aggregator, which identifies an array of useful data from them, and provides services for exchanging them with other users using smart contracts, while each participant receives a legitimate reward.

Having conducted an experiment, the author claims that despite the fact that at the moment the system's capacity is not enough to ensure uninterrupted operation on a large-scale infrastructure, the use of DLT together with DFS and complex cryptographic schemes allows to effectively control access to data and offer interesting services, while maintaining the authenticity and availability of data [62].

7.4 Traffic control.

Thanks to the data generated by vehicles and road infrastructure, on the state of traffic flow, road accidents and so on, it is possible to implement an intelligent system that will be able to independently monitor all processes on the road, while reducing the number of traffic jams and emergencies. But in order for all users to trust the data transmitted between each other and other objects, it is necessary to make the process of their transmission as safe as possible and closed from malicious attacks. Due to the presence of such problems, researchers are developing autonomous traffic control and management systems.

One example of such studies is [65]. In this article the authors consider the development of a system for intelligent transportation and control of the inner-city transport system. This system uses a blockchain, which is connected to the IoT by sensor nodes that are located in vehicles. The main purpose of such a system is to improve the safety of road users and reduce the number of traffic jams on the roads, which is achieved by automatically collecting data on the situation on the road and identifying road accidents. The blockchain, in turn, provides the implementation of transaction records so that vehicles can exchange secure and authentic data with each other.

In the course of the study, the authors identified a number of vulnerabilities of such a system, such as, for example, data transmission delay in time, as well as increased power consumption of Internet of Things devices.

But at the same time, provided that some vulnerabilities are eliminated, such a system will reduce the interference of the human factor, which allows vehicles and objects related to traffic to interact and automatically self-execute using a blockchain smart contract in accordance with traffic conditions.

Another option for using decentralized IoT on the road is suggested by the authors [66]. In their article, the authors focused on a scenario where vehicles can request the acquisition of lane ownership rights, that is, drivers can agree on who will move in which lane, while significantly reducing the number of accidents caused by incorrect and dangerous lane realignment. In this scheme, vehicles need to exchange information about location, speed and directly personal data to identify them. The right to use the strip can be obtained using a token. To rebuild, firstly, it is needed to get approval from the rest of the participants in the movement, while those participants who will allow to rebuild will earn the appropriate number of tokens. Then these tokens can be converted into a payment or insurance fee.

7.5 Ride Sharing

Carpooling or ridesharing is the sharing of a private car with the help of online travel companion search services. This approach implies a proportional distribution of fuel costs, while building an optimal route for all participants of the trip, which will be convenient for the driver of the vehicle.

At the same time, not only the economic component is important, but also the social and environmental one, since such a service allows to make new acquaintances, while reducing CO2 emissions.

In [67] , the authors developed a new model of how to provide this service, while protecting the data of all users participating in the trip. This model is based on blockchain, which is why it has the following advantages:

- The possibility of combining several service providers on a common platform where the parties can trust each other;
- It removes the restriction of centralized comparison of passenger and vehicle data while maintaining confidentiality by the service provider;
- Providing passenger privacy;
- Protection against cyber attacks.

The main role of the blockchain in this model is to verify the authenticity of passenger location data and their coordination. In addition, there are methods that serve to search for vehicles and compare destinations. Smart contracts, in turn, contribute to ensuring compliance of the Roadside Unit (RCU) with passengers and drivers. The payment process will also become more secure, as the authors have provided for the use of anonymous payments among users, drivers and service providers. The carpooling system is able to offer users more efficient vehicle sharing.

7.6 Forensic application.

Mumin Cebe et al. in [68] propose the use of blockchain and IoV integration in the field of traffic accident analysis. In this case, the blockchain serves to ensure an unbiased investigation by bringing together all stakeholders and providing data, while each of the participants in the process will be confident in their reliability. The data will be received from the vehicles involved in the incident, as well as from road infrastructure facilities.

This system is not aimed at completely excluding a person from such a process, it only provides additional information coming from the ports onboard diagnostics (OBD) and event data recorders (EDR), which represent valuable additional evidence to support dispute resolution.

The stakeholders in such a process are the drivers themselves, insurance companies, law enforcement agencies, in some cases also car manufacturers, if it is possible to prove the fact of a vehicle malfunction. That is why the authors want to create a system where absolutely all information about vehicles and related business components will be stored.

Thus, the system proposed by the authors should provide a blockchain chain, taking into account confidentiality, where the above-listed persons will participate, without the need for the introduction of a third party, as well as a forensic medical examination of vehicles, which contains all the necessary data for a comprehensive solution for the forensic medical examination of vehicles.

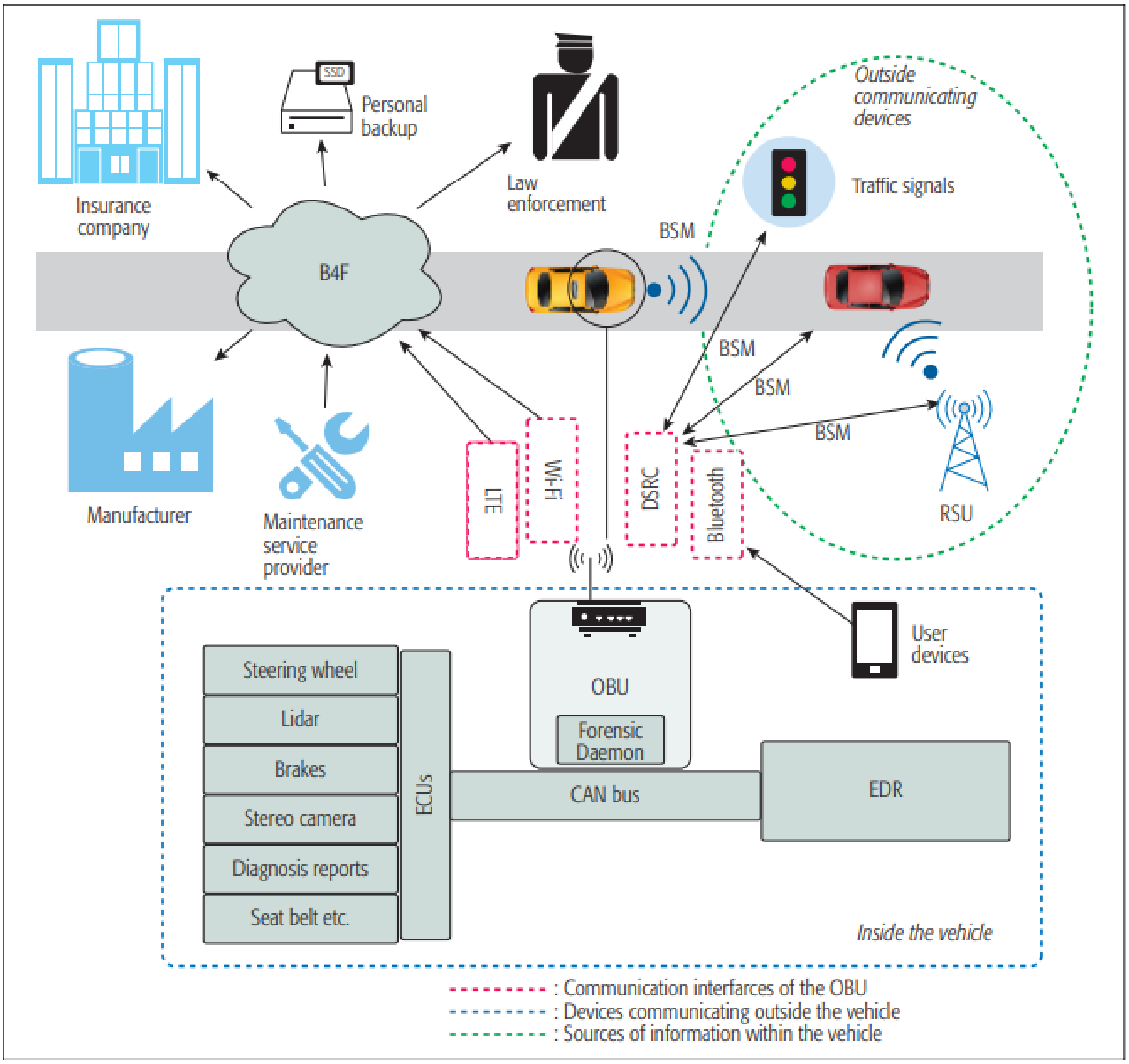

Figure 19: Forensic system model

Figure 19 shows a model of the platform being developed by the authors. Stakeholders are represented at it, B4F (Block 4 Forensic) is a blockchain-based vehicle management system. It is also based on a special forensic daemon that is located inside the OBU and constantly extracts data from EDR, BCM (i.e. messages received from other vehicles) and on-board sensors/IoT devices. This data is transmitted to stakeholders via encrypted channels. In turn, actors such as manufacturers and maintenance representatives also transmit data to the blockchain. The stored data will be used in post-accident scenarios, allowing the parties to selectively disclose their data to determine the guilty party.

7.7 Transportation Insurance

As identified in the previous section, processes related to vehicle insurance are also subject to a lack of trust between the parties. In [69], the authors propose a decentralized IoT model for the following purposes:

- fighting fraud;
- creation of a new insurance model in which the tripartite relationship should be simplified or completely eliminated;
- creation of a parametric insurance model in which possible accidents will be predetermined by collecting data from sensors of smart vehicles.

The main idea of the approach proposed by the authors is that the data on the driver and vehicles will be safely stored in the distribution register between the stakeholders, and thanks to the analysis of this data, more accurate insurance premiums will be calculated. This approach is aimed at creating a fair and honest environment between the participants in the process, as well as encouraging and encouraging drivers for a safe driving style. In addition, there are also advantages for business, since vehicle owners can safely give a vehicle to another driver to perform certain work tasks.

Having developed a prototype of this system and conducted test studies on the data of GPS trajectories of vehicles in Singapore, the authors believe that such a model can really be working, provided it is refined and increased capacity.

7.8 Managing the transportation of dangerous goods.

As mentioned earlier, IoT devices are capable of generating data that, after processing them, can bring one or another benefit. This also concerns the monitoring of technological processes that are related to the transport sector. In [70] the authors propose to introduce blockchain technology into the process of transporting dangerous goods, where such goods need to cross state borders. Several stakeholders are involved in the process of transporting dangerous goods, which is why each of them needs to trust each other, as well as the data they provide. Such data must be verified before they are transmitted, as well as protected from any changes. In order to make the process transparent, it is necessary to ensure the consistency, reliability and integrity of the data received from IoT devices.

In this article, the authors consider the process of transportation of dangerous goods from the point of view of cooperation of stakeholders and information flow. Figure 20 describes this process.

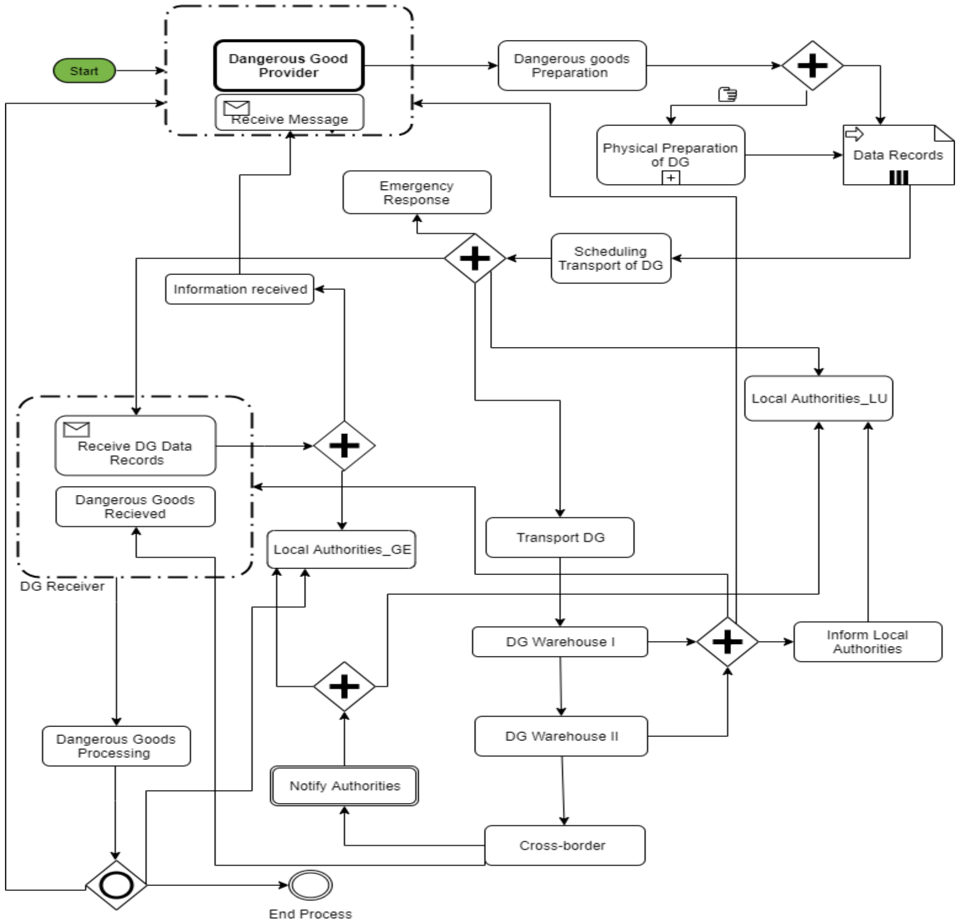

Figure 20: Dangerous goods transportation process flow

This diagram shows the technological process and interactions between stakeholders. The supplier of dangerous goods is the main figure in the process, which is responsible for preparing the cargo and entering all the primary information. Since this process is regulated by law, it is necessary to notify the local authorities and the recipient of the cargo about the beginning of the process. In case of unforeseen circumstances, the authorities should receive information in a timely manner and take the necessary measures. Each stage of movement must be marked in the system, regardless of the number of stops, crossing state borders, etc. When the cargo reaches its destination, the recipient of the cargo must notify all stakeholders that the cargo has arrived. The actions of the participants in the process, meanwhile, should not violate regulations and legal regulations.

It is needed to note that in this article, the authors presented stakeholders in the form of digital doubles, which allows to increase the level of security when using the system. The system also implies authentication of IoT devices, which gives it even greater transparency.

8 The possibilities of using the decentralized IoT network in Smart Port.

Due to the fact that the seaport is a huge ecosphere, where there is a place not only for sea transport, but also for land transport, which is designed for the transportation of containers inside the port, their loading and unloading, some scenarios for the use of decentralized IoT, which were described in the previous section, are also relevant for a smart seaport. This section discusses case cases that are both unique, suitable only for maritime transport, and for the entire supply chain as a whole.

8.1 Supply chain

In addition to the need to protect data in the processes of intra-city movements, the transportation of goods and all information related to such processes also needs protection. In [71], the authors consider several options for how the introduction of blockchain technology can bring benefits and efficiency to the supply chain.

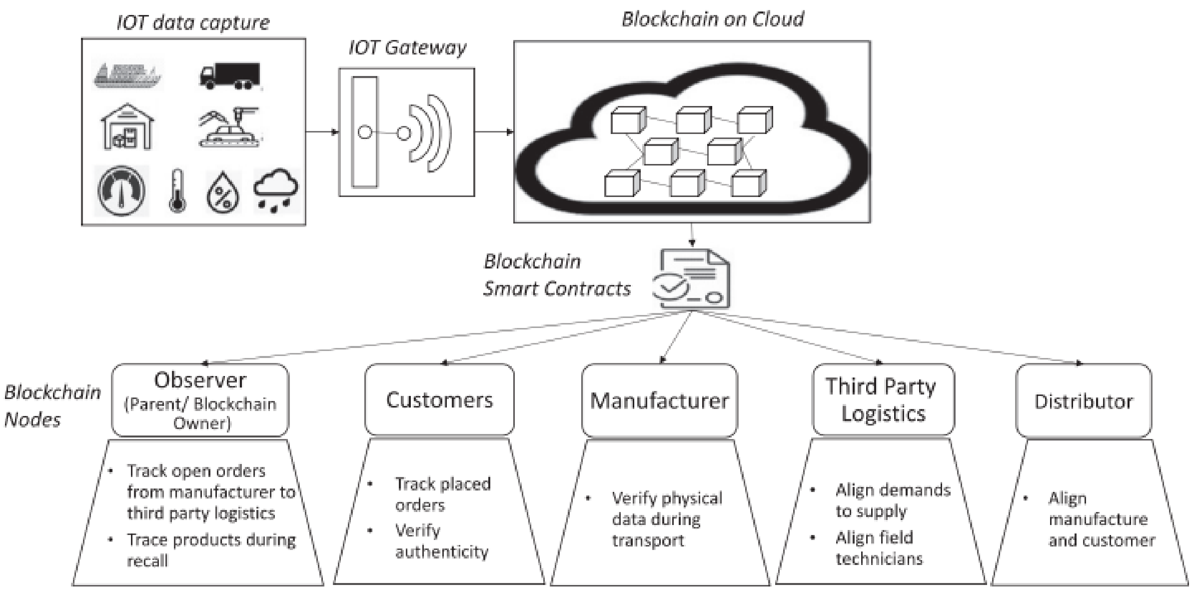

Figure 21: Supply chain with cloud blockchain architecture

Figure 21 shows the blockchain cloud architecture proposed by the authors. This system unites all stakeholders in a blockchain and data is collected from various devices connected to a common IoT network. Data from sensors is transmitted to the blockchain using a special gateway, without intermediate storage. This architecture is a kind of starting point when creating complex decentralized systems.

According to the authors, this approach contributes to solving a number of problems inherent in supply chains: Product tracking/Orders and Product Tracking/Review/Protection against counterfeiting. The solutions for the listed problems are quite similar. In the first case, the blockchain contributes to the creation of a single platform where each stakeholder will be able to receive information about the transported cargo in real time, while each of them will be able to trust the data received. The data will be generated from sensors located at various key points in the supply chain, and then transmitted to the gateway cloud system, and then to the blockchain network. End users will be able to receive data from the blockchain by using smart contracts, which provides control over the transfer of information. Smart contracts can determine the level of access and information for partners.

In Figure 21, the authors present a mechanism for coordinating supply chain partners using a combination of the Internet of Things blockchain. This mechanism will allow all end users to monitor a transparent supply chain, and in case of disagreement, will contribute to more correct decision-making. Such a system will store information about the full life cycle of the product – from its production to receipt in the hands of the buyer. At the same time, this approach helps manufacturers to constantly maintain the high quality of their products, since blockchain participants are also able to take into account errors during production.

In addition, employees of distribution centers will be able to predict the flow of shipments and correctly allocate work resources and places in warehouses. Also, thanks to IoT and sensors, all participants will be able to receive detailed information about the storage conditions of the product. Also, thanks to the approach presented by the authors in their study, it will be possible to receive feedback from the end user to the manufacturer directly.

Based on the description of the authors' approach described above, it can be concluded that such methods and technologies can be used both in cargo transportation by land vehicle and by sea. Sensors located inside the smart container are able to transmit data to users about physical characteristics, such as temperature, pressure, location, etc. in real time. For example, if the temperature of a smart cargo container suddenly starts to rise, a warning can be sent to the driver or other local logistics personnel, and they, in turn, will be able to take immediate action. Actually, it is the feedback and reaction capabilities that make it possible to consider the container smart.

In addition, it will also be useful to consider the scenario of the transport of dangerous goods presented in the last chapter. There is such a world practice when countries can conclude an agreement among themselves, where one country can transport such goods to another, outside the European Union. In this connection, such a process requires even more control and has a greater number of stakeholders and regulatory documents, as a result of which the blockchain is able to bring even greater benefits.

This approach can also be applied to the transportation of expensive goods, such as paintings, jewelry, military equipment, and so on. Due to the fact that all stakeholders, including the sender, recipient, intermediate logistics companies and customs, will be able to receive information about transportation in real time, theft attempts, changes in data in the system itself about the destination and so on, will be significantly reduced or completely disappear.

8.2 Port Video Terminals Security

Another possible scenario for using decentralized IoT in a smart port was proposed by the authors in their work [72], where they consider the security of the port itself. The video surveillance system located in the port uses IoT and AI technologies, which completely replaces human control, identifying people and vehicles that move inside the port. The intelligent port monitoring system is mainly divided into an intelligent video monitoring platform, a streaming media service module and a transaction processing service. But since the scale of video surveillance is really huge and a large number of devices are involved in the system itself, this can endanger the system. In order to avoid hacking the system and substitution of certain data, the authors propose the approach described below.

After the IoT device leaves the port territory, or some specific part of it, the system generates public and private keys, as well as a digital signature, which are transmitted to the blockchain identification system for publication. Next, the data is checked and recorded in the blockchain. For the interaction of the device and the blockchain authentication system, an edge computing node is used, and if the authentication process is successful, a secure data transmission channel is established. All stages of this process are supported by smart contracts.

8.3 Load planning

In [73], the authors propose the use of IoT and blockchain for the processes of planning the loading of RoRo vessels (vessels for the transportation of wheeled cargo). The main task of planning in this case is the competent distribution of cargo throughout the ship. To solve it, the authors propose the use of IoT sensors located on the scales and entrance gates, which will read the weight characteristics of the cargo and transmit information to the planning system. In this case, the blockchain will be used as a mechanism that will encrypt the received data in order to avoid their leakage. It is also proposed to use this method in order to prevent the use of ballast on board.

In order to test their theory, the authors developed and tested a simulation model. In order to obtain more accurate results, the authors checked the flow of the process both using IoT sensors and without them. According to the results of the data obtained, each vehicle loaded on board should be assigned a certain line for the location. According to the results of the study, where a lightweight version of the blockchain was used, the optimized planning process showed results where the use of ballast water was improved by 50-160%.

9 Future trends of decentralized IoT in transportation sphere

Each of the above options for using decentralization in the transport system is the future of humanity. Despite the fact that the transport system is actively developing, going through the process of digital transformation, at the moment the use of smart transport and intelligent systems that control the processes of movement of vehicles is not so much developed. Humanity is still moving in an environment where the human factor is decisive.

If we compare the spheres of sea transportation and traffic within the city, then seaports definitely have more development. For example, the port of Rotterdam is one of the most advanced in the world in terms of the use of various technologies. Loading and unloading of sea vessels, transportation of containers inside the port, the use of blockchain to settle legal processes – all this is a reality today. If we consider the smart port and the possibilities of increasing its efficiency, then the best option for using the technologies considered in the work will be the integration of smart port systems with a common urban transport system. This approach will automate the supply chain, where goods from the port will be automatically delivered to the customer's hands. Smart devices in this case, thanks to the use of smart contracts and an internal communication network, will be able to independently confirm the transfer of goods, as well as pay for the services provided.

As for urban transport systems, all the approaches being developed need to be combined into a single transport ecosystem, enabling drivers to choose all the services they need. At the moment, researchers conduct their work quite separately, without thinking about how to combine all their work into a common and unified concept. Thanks to this, it will be possible to create a sustainable model of the transport system, which will increase safety both on the road and in the system itself, increase capacity by reducing the number of traffic jams, while reducing the costs of both drivers and government.

In addition to the IoT and blockchain technologies discussed in this thesis, the use of artificial intelligence in such systems will bring enormous benefits and efficiency to transport systems as a whole, further increasing the level of its autonomy, thanks to decision support systems, as well as making the process almost error-free.

10 Economic evaluation

In order to identify the approximate cost of developing and implementing blockchain in the supply chain, as well as the payback period for investments, further research will be conducted based on the report of the Forrester Emerging Technology Projection series (Predictive Analysis of Promising Technology), which was performed by the Total Economic Impact™ methodology [74]. In this case, it is the calculation for the entire supply chain that is used, since this is the most common possible application for this work. In the Forrester study, the IBM blockchain was used, as well as various options for using the technology by various business lines. The article presents a generalized model of benefits and costs, which is why the following parameters may differ in the calculations of companies.

At a high level, benefit modules can be divided into two categories – benefits that create new opportunities (green) and benefits that solve existing problems (blue). It is quite possible that one or another organization will be able to receive more than one benefit from the set of benefits identified for a particular blockchain solution. Cost modules are divided into categories according to the stages of the solution lifecycle.

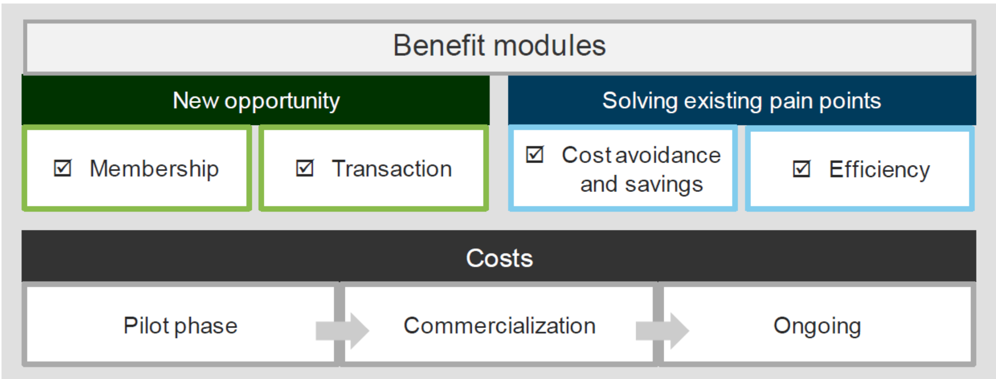

Figure 22: Benefit and cost modules

10.1 Advantage modules

Below are the methods for calculating the possible benefits that can be achieved by implementing blockchain in the enterprise

Subscription service income: This type of company income is created on the basis of membership fees paid by other companies participating in the network.

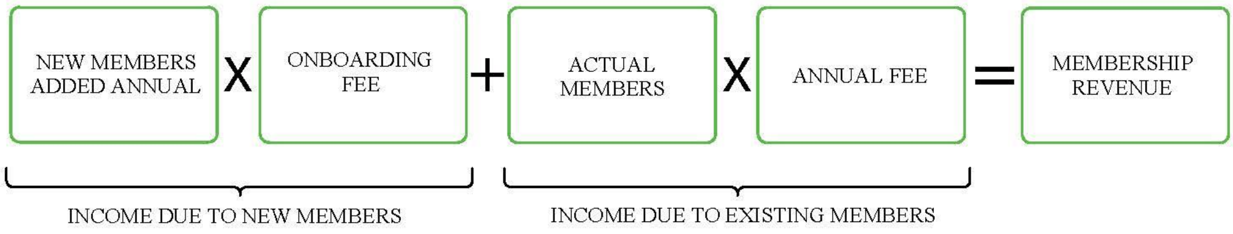

Figure 23: Subscription service income

Transaction Revenue: Some companies charge fees for transactions that pass through their network to make a profit.

Figure 24: Transaction Revenue

Savings due to capital costs and operating costs: due to the fact that the blockchain owner company has open access to the resources of other companies, this can allow saving on capital and operating costs.

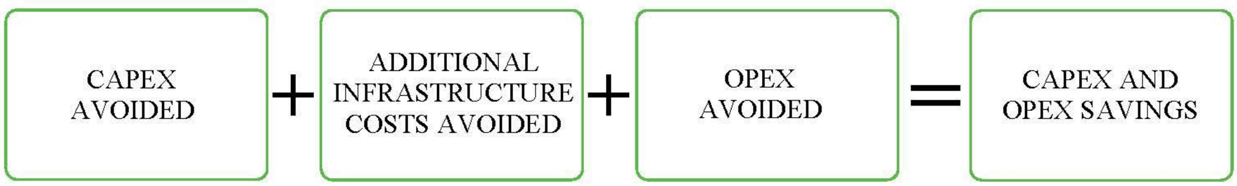

Figure 25: Savings due to capital costs and operating costs

Savings due to increased efficiency: in this case, efficiency can be achieved by combining all the company's services on one platform, simplified workflow, reduced time costs.

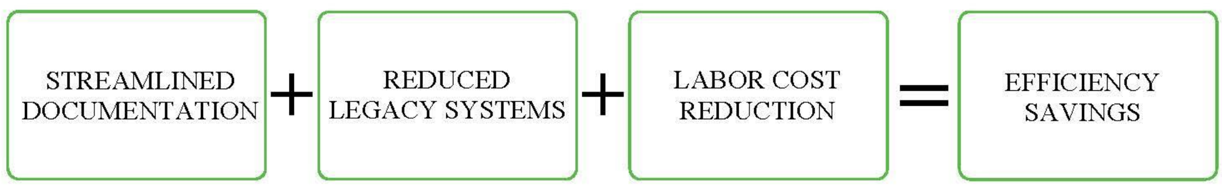

Figure 26: Savings due to increased efficiency

Fraud prevention: system security provides additional benefits to companies due to the fact that sometimes hacking the system brings additional costs for repairing and configuring software.

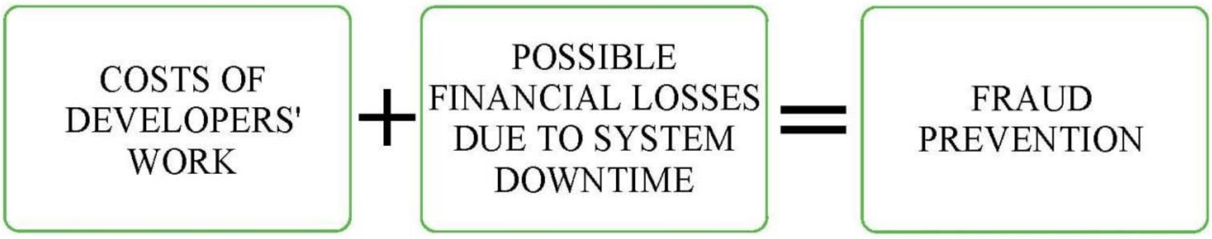

Figure 27: Fraud prevention

10.2 Cost modules

This part presents the possible costs of deploying the system, as well as its maintenance. The cost items may differ depending on the company, generalized modules are presented here.

Expenses at the pilot project stage: since in this case the deployment of the IBM system is considered, the services provided by IBM for consulting in the development of a viable idea, design or prototype of the system also fall under the expense item. As a rule, this stage lasts from six months to a year.

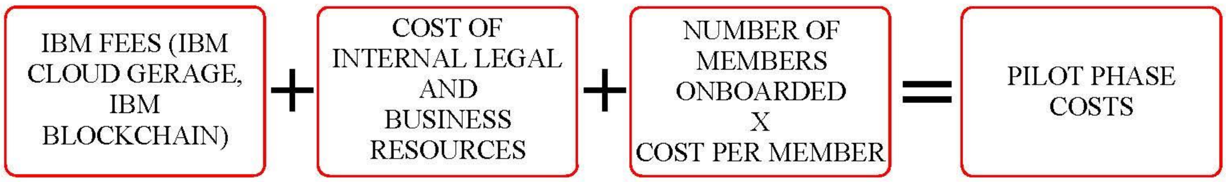

Figure 28: Expenses at the pilot project stage

Costs at the stage of commercialization: at this stage, the business logic of the blockchain is being configured, that is, at this stage, the forces of developers, employees involved in documentation and other administrative processes are needed, and consulting from IBM is also possible. Also, this stage is designed to connect all stakeholders to the chain. This stage lasts on average 1-1.5 years.

Figure 29: Costs at the stage of commercialization

Costs at the operational stage: this stage is supporting the functioning of the created blockchain network. All possible expenses proposed by Forrester are shown in the figure below.

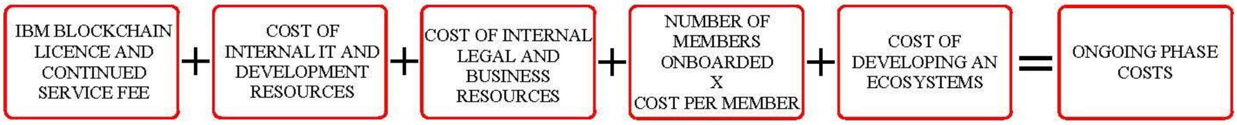

Figure 30: Costs at the operational stage

10.3 Calculation part

This section presents the calculation of the implementation of the blockchain, based on the logic of calculations presented in the work of Forrester and IBM. This model is not a representation of a specific use case, it is fictional and common to all companies. In order to make calculations more accurate, it is necessary to change the set of parameters, terms and cost of services. In the forehead is considered.

10.3.1 Income

The figures below (31-33) show an approximate calculation of revenue from the implementation and deployment of blockchain within the company. All income was divided into four categories:

Transaction revenue: supply chain participants are required to pay for each of the transactions carried out, 50 cents is taken into account for each of the transactions. At the same time, an increase in the number of stakeholders is predicted every year, and with this an increase in the total number of transactions carried out;

Subscription service income: chain members must pay $5,000 for registration in the chain and $8000 as an annual membership fee;

Income due to savings on capital costs and operating costs: in this case, the savings will be calculated by adding operational and capital costs, and operating costs will be 30% of the capital;

Savings due to efficiency: this section discusses the advantages that blockchain gives in specific cases, as an example in the work considers improving document flow, replacing outdated equipment, labor resources and fraud prevention.

The period under review is 5 years.

Subscription service income					
Registration Fee	$5 000				
Ongoing Annual Fee	$8 000				
	6-12 Months	**12-24 Month**	**Year2-Year3**	**Year3-Year4**	**Year4-Year5**
New Actor	2	2	3	3	4
Total Actor	2	4	7	10	14
Revenue	**$26 000**	**$42 000**	**$71 000**	**$95 000**	**$132 000**

Income due to savings on capital costs and operating costs				
		Year2-Year3	**Year3-Year4**	**Year4-Year5**
	Shared Resources(worker,plant, warehouse) Saving	$50 000	$75 000	$100 000
	Transportation Saving	$50 000	$75 000	$100 000
	Reprocess or Testing Saving	$30 000	$50 000	$70 000
	Hardware or Technological Expenses Saving	$30 000	$50 000	$70 000
	Tax Saving	$50 000	$50 000	$50 000
	Capex Saving	**$210 000**	**$300 000**	**$390 000**
	Opex Saving	**$63 000**	**$90 000**	**$117 000**
	Total Capex And Opex	**$273 000**	**$390 000**	**$507 000**

Figure 31: Subscription service income and Income due to savings on capital costs and operating costs calculations

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1					**6-12 Months**	**12-24 Months**	**Year2-Year3**	**Year3-Year4**	**Year4-Year5**								
2				**Total Transacti**	720 000	1 920 000	2 544 000	3 432 000	5 520 000								
3	**Transaction Revenue**																
4	Transaction fee($)	$0,50		**Revenue**	**$360 000**	**$960 000**	**$1 272 000**	**$1 716 000**	**$2 760 000**								
5																	
6																	
7																	
8																	
9																	
10				Actor1	Actor2	Actor3	Actor4	Actor5	Actor6	Actor7	Actor8	Actor9	Actor10	Actor11	Actor12	Actor13	Actor14
11		**6-12 Months**															
12			Operations per actor	15 000	15 000												
13			Step per operation	1	1												
14			Transactions per step	2	2												
15																	
16			Transactions per actor (monthly)	30 000	30 000												
17			**Transactions per actor Year 1**	**360 000**	**360000**												
18																	
19		**12-24 Months**															
20			Operations per actor	25 000	25 000	15 000	15 000										
21			Step per operation	1	1	1	1										
22			Transactions per step	2	2	2	2										
23																	
24			Transactions per actor (monthly)	50 000	50 000	30 000	30 000										
25			**Transactions per actor Year 2**	**600 000**	**600000**	**360 000**	**360 000**										
26																	
27		**Year2-Year3**															
28			Operations per actor	30 000	30 000	15 000	15 000	8 000	4000	4 000							
29			Step per operation	1	1	1	1	1	1	1							
30			Transactions per step	2	2	2	2	2	2	2							
31																	
32			Transactions per actor (monthly)	60 000	60 000	30 000	30 000	16 000	8000	8 000							
33			**Transactions per actor Year 3**	**720 000**	**720000**	**360 000**	**360 000**	**192 000**	**96000**	**96 000**							
34																	
35		**Year3-Year4**															
36			Operations per actor	40 000	40 000	20 000	20 000	10 000	4000	3 000	3 000	1500	1500				
37			Step per operation	1	1	1	1	1	1	1	1	1	1				
38			Transactions per step	2	2	2	2	2	2	2	2	2	2				
39																	
40			Transactions per actor (monthly)	80 000	80 000	40 000	40 000	20 000	8000	6 000	6 000	3000	3000				
41			**Transactions per actor Year 4**	**960 000**	**960000**	**480 000**	**480 000**	**240 000**	**96000**	**72 000**	**72 000**	**36000**	**36 000**				
42																	
43		**Year4-Year5**															
44			Operations per actor	60 000	60 000	30 000	30 000	20 000	8000	6 000	6 000	3000	3000	1 000	1 000	1 000	1000
45			Step per operation	1	1	1	1	1	1	1	1	1	1	1	1	1	1
46			Transactions per step	2	2	2	2	2	2	2	2	2	2	2	2	2	2
47																	
48			Transactions per actor (monthly)	120 000	120000	60 000	60 000	40 000	16000	12 000	12 000	6000	6000	2 000	2 000	2 000	2000
49			**Transactions per actor Year 5**	**1 440 000**	**1 440 000**	**720 000**	**720 000**	**480 000**	**192000**	**144 000**	**144 000**	**72000**	**72 000**	**24 000**	**24 000**	**24 000**	**24000**

Figure 32: Transaction revenue calculations

	A	B	C	D	E	F
2	**R3 Efficiency Saving**			**Year2-Year3**	**Year3-Year4**	**Year4-Year5**
3						
4			**Total Efficiency Benefit**	**$703 200**	**$1 608 000**	**$2 512 800**
5						
6						
7						
8						
9	**3.1 Streamlined Documentation**			**Year2-Year3**	**Year3-Year4**	**Year4-Year5**
10						
11			Number of Document	30 000 000	30 000 000	30 000 000
12						
13			Percentage of Facing Conflicting Document	1%	1%	1%
14			Number of Facing Conflicting Document	300 000	300 000	300 000
15			Percentage of blockchain solution for conflicting transaction	10%	30%	50%
16			Cost for solving conflicting Document	$1	$1	$1
17						
18			**Saving Conflict Records**	**$30 000**	**$90 000**	**$150 000**
19						
20			Cost per documentation process	$0,05	$0,05	$0,05
21			Percentage reduction in cost per documentation process replaced by blockchain	30%	60%	90%
22						
23			**Saving Record Cost**	**$450 000**	**$900 000**	**$1 350 000**
24						
25			**Benefit Coming From Saving Streamlined Documentation**	**$480 000**	**$990 000**	**$1 500 000**
26						
27						
28	**3.2 Legacy System**			**Year2-Year3**	**Year3-Year4**	**Year4-Year5**
29						
30			Existing Legacy System (License) Cost	$100 000	$100 000	$100 000
31			Percentage of Legacy System replaced by blockchain	30%	60%	90%
32						
33			**Benefit Coming From Saving Software Licence of Tracking,Billing,Invoicing**	**$30 000**	**$60 000**	**$90 000**
34						
35						
36	**3.3 Labour**			**Year2-Year3**	**Year3-Year4**	**Year4-Year5**
37						
38			Number of Finance Employee solving conflict	3	3	3
39			Finance Employee Annual Compensation	$36 000	$36 000	$36 000
40			Reduction to finance employee dedicated to resolving conflicting records	20%	50%	80%
41						
42			**Saving Finance Employee solving conflict**	**$21 600**	**$54 000**	**$86 400**
43						
44			Number of Legal Employee solving conflict	3	3	3
45			Legal Employee Annual Compensation	$36 000	$36 000	$36 000
46			Reduction to Legal employee dedicated to resolving conflicting records	20%	50%	80%
47						
48			**Saving Finance Employee solving conflict**	**$21 600**	**$54 000**	**$86 400**
49						
50			**Benefit Coming From Labor Cost Reduction**	**$43 200**	**$108 000**	**$172 800**
51						
52						
53	**3.4 Fraud Avoidance**			**Year2-Year3**	**Year3-Year4**	**Year4-Year5**
54						
55			Number of Transaction with Supplier	5 000 000	5 000 000	5 000 000
56			Percentage of Facing Fraud in Transaction	1%	1%	1%
57			Number of Fraud Transaction	50 000	50 000	50 000
58			Percentage of blockchain solution for fraud transaction	10%	30%	50%
59						
60			Cost For solving Fraud Problem	$30	$30	$30
61						
62			**Benefit coming from reduction in Fraud Transaction**	**$150 000**	**$450 000**	**$750 000**

Figure 33: Savings due to efficiency calculations

10.3.2 Costs

As mentioned above, the costs of implementing the system must be divided into three stages:

- The pilot project stage – (Fig. 34) duration 6 months;
- Stage of commercialization – (Fig. 35) duration of 18 months;
- The stage of operation - (Fig. 36) the duration is 3 years.

	A	B	C	D
1	**Pilot Phase Cost**			
2	**$426 800**		**0-6 Months**	**6-12 Months**
3				
4		IBM Design Thinking workshop	$30 000	
5		Architectural consultancy	$10 000	
6		Software development fee paid to IBM	$250 000	
7				
8		**Design Cost**	**$290 000**	
9				
10				
11		Number of Technical Employees involved Pilot Phase	7	
12		Duration of the pilot phase engagement (Month)	6	
13		Percent of technical employees' time spent on the pilot	40%	
14		IT/dev/engineering employee monthly compensation	$6 000	
15				
16		**Cost of internal IT/developers' pilot efforts**	**$100 800**	
17				
18				
19		Number of Legal and Business Employees involved Pilot Phase	3	
20		Duration of the pilot phase engagement (Month)	6	
21		Percent of legal and business employees' time spent on the pilot	40%	
22		Legal, business owners, IT management monthly compensation	$5 000	
23				
24		**Cost of internal governance model/ legal employee pilot efforts**	**$36 000**	

Figure 34: Pilot project stage cost

	A	B	C
1			
2	**Commercialization Phase Cost**		
3	**$1 448 400**		
4			**6-24 Months**
5			
6		Blockchain full development fee to IBM	$1 000 000
7		IBM Blockchain license fee	$30 000
8			
9		**Blockchain Dev. And licence Cost**	**$1 030 000**
10			
11			
12		Number of Technical Employee Involved Commer. Phase	7
13		Duration of the commercialization phase engagement (months)	18
14		Percent of time dedicated to commercialization effort	40%
15		IT/dev/engineering employee monthly compensation	6000
16			
17		**Cost of internal IT/developers' commercialization efforts**	**$302 400**
18			
19			
20		Number of Legal and business Employees involved Commer. Phase	3
21		Duration of the governance model development and contract negotiation (months)	18
22		Percent of employees' time spent on the commer.	40%
23		Legal, business owners, IT management annual compensation	$5 000
24			
25		**Cost of internal governance model/legal commercialization efforts**	**$108 000**
26			
27			
28		Number of blockchain members onboarded for commercialization	4
29		Cost of onboarding one member	$2 000
30			
31		**Cost of member onboarding for commercialization (marketing, admin, contract negotiation)**	**$8 000**

Figure 35: Commercialization stage cost

	A	B	C	D	E	F	G
1							
2	**Operation Phase Cost**						
3							
4	**Year2-Year3**	**$436 800**					
5	**Year3-Year4**	**$436 800**					
6	**Year4-Year5**	**$438 800**			**Month24-Month36**	**Year3-Year4**	**Year4-Year5**
7							
8				Continued IBM blockchain software development fee	$200 000	$200 000	$200 000
9				IBM Blockchain license fee	$30 000	$30 000	$30 000
10							
11				**Blockchain Dev. And licence Cost**	**$230 000**	**$230 000**	**$230 000**
12							
13							
14				Number of Technical Employee Involved Ongoing Phase	3	3	3
15				Duration of the commercialization phase engagement (months)	12	12	12
16				Percent of time dedicated to ongoing effort	30%	30%	30%
17				IT/dev/engineering employee monthly compensation	$6 000	$6 000	$6 000
18							
19				**Cost of internal IT/developers' commercialization efforts**	**$64 800**	**$64 800**	**$64 800**
20							
21							
22				Number of Legal Employees involved Ongoing Phase	2	2	2
23				Duration of the governance model development and contract negotiation (months)	12	12	12
24				Percent of employees' time spent on the ongoing Phase	30%	30%	30%
25				Legal, business owners, IT management annual compensation	$5 000	$5 000	$5 000
26							
27				**Cost of internal governance model/legal ongoing efforts**	**$36 000**	**$36 000**	**$36 000**
28							
29							
30				Number of blockchain members onboarded for ongoing	3	3	4
31				Cost of onboarding one member	$2 000	$2 000	$2 000
32							
33				**Cost of member onboarding for ongoing (marketing, admin, contract negotiation)**	**$6 000**	**$6 000**	**$8 000**
34							
35							
36				**Ecosystem development (workshops, member relations, community boards, other)**	**$100 000**	**$100 000**	**$100 000**

Figure 36: Operation stage cost

Based on the results of the calculation of income and expenses, a calendar plan was drawn up for all 5 years, which clearly shows the amounts that the owner needs to spend on deploying the system, as well as the projected profit that he should have as a result.

BENEFIT	6-12 Months	12-24 Months	Year2-Year3	Year3-Year4	Year4-Year5
Blockchain Revenues	**$386 000**	**$1 002 000**	**$1 343 000**	**$1 811 000**	**$2 892 000**
Membership Revenue	$26 000	$42 000	$71 000	$95 000	$132 000
Transaction Revenue	$360 000	$960 000	$1 272 000	$1 716 000	$2 760 000
Capex Opex Saving			**$273 000**	**$390 000**	**$507 000**
Capex Saving			$210 000	$300 000	$390 000
Opex Saving			$63 000	$90 000	$117 000
Efficiency Saving			**$703 200**	**$1 608 000**	**$2 512 800**
Benefit Coming From Saving Streamlined Documentation			$480 000	$990 000	$1 500 000
Benefit Coming From Saving Software Licence of Tracking,Billing,Invoicing			$30 000	$60 000	$90 000
Benefit Coming From Labor Cost Reduction			$43 200	$108 000	$172 800
Benefit coming from reduction in Fraud Transaction			$150 000	$450 000	$750 000

COST	0-6 Months	6-24 Months	Year2-Year3	Year3-Year4	Year4-Year5
Pilot Phase	**$426 800**				
Design	$290 000				
Cost of internal IT/developers' pilot efforts	$100 800				
Cost of internal governance model/legal pilot efforts	$36 000				
Commercialization Phase		**$1 448 400**			
Blockchain Development And licence Cost		$1 030 000			
Cost of internal IT/developers' commercialization efforts		$302 400			
Cost of internal governance model/legal commercialization efforts		$108 000			
Cost of member onboarding for commercialization efforts		$8 000			
Operation Phase			**$436 800**	**$436 800**	**$438 800**
Blockchain Dev. And licence Cost			$230 000	$230 000	$230 000
Cost of internal IT/developers' ongoing efforts			$64 800	$64 800	$64 800
Cost of internal governance model/legal ongoing efforts			$36 000	$36 000	$36 000
Cost of member onboarding for ongoing			$6 000	$6 000	$8 000
Ecosystem development (workshops, community boards, other)			$100 000	$100 000	$100 000

Figure 37: Benefits and Cost overview

The calculation of the net present value of the project will allow investors to understand whether it is worth investing money for the implementation of the project, and how soon the investment will pay off. NPV (Net Present Value) is a financial indicator that demonstrates the expected future income of the project minus its initial cost. Simply put, NPV allows to compare current money with future money, which will cost less due to inflation [77]. In this case, the calculation is made by months. The annual discount rate is 12%, having performed the calculation ((1+12)^(1/12)-1), the monthly discount rate has become 0.95%. All values were calculated based on the duration of a particular stage.

The following is a calculation of the ROI (Return on Investment, return on Investment) indicator — this is the return on investment ratio [78]. In simple words — the return on investment. This indicator demonstrates how profitable or unprofitable a project or product is. The result of 321.26% gives reason to believe that this project is profitable for investment.

Next, it is necessary to determine the payback period of the investment. As can be seen from the table, the project will begin to pay off 27 months after the start of its implementation.

The total projected return on investments in 5 years is $13,428,000, and the total profit is $3,187,600. After applying the discount rate, it is reduced to $6,533,945.

Discount Rate Yearly	12,00%																					
Discount Rate Monthly	0,95%																					
Month	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**
Membership Revenue	0	0	0	0	0	0	4333,333	4333,333	4333,333	4333,333	4333,333	4333,333	3500	3500	3500	3500	3500	3500	3500	3500	3500	3500
Transaction Revenue	0	0	0	0	0	0	60000	60000	60000	60000	60000	60000	80000	80000	80000	80000	80000	80000	80000	80000	80000	80000
Capex Opex Savings	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Efficiency Benefit	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Revenue	0	0	0	0	0	0	64333,33	64333,33	64333,33	64333,33	64333,33	64333,33	83500	83500	83500	83500	83500	83500	83500	83500	83500	83500
Cumulative Total Revenue	$13 428 000																					
Pilot Cost	71133,33333	71133,33333	71133,33333	71133,33	71133,33	71133,33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Commercialization Cost	0	0	0	0	0	0	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67
Ongoing Cost	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Cost	71133,33333	71133,33333	71133,33333	71133,33	71133,33	71133,33	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67	80466,67
Cumulative Total Cost	$3 187 600																					
Profit	-71133,33333	-71133,33333	-71133,33333	-71133,3	-71133,3	-71133,3	-16133,3	-16133,3	-16133,3	-16133,3	-16133,3	-16133,3	3033,333	3033,333	3033,333	3033,333	3033,333	3033,333	3033,333	3033,333	3033,333	3033,333
Cumulative Profit	-71133,33333	-142266,6667	-213400	-284533	-355667	-426800	-442933	-459067	-475200	-491333	-507467	-523600	-520567	-517533	-514500	-511467	-508433	-505400	-502367	-499333	-496300	-493267
Total Profit	**$10 240 400**																					
ROI	**321,26%**																					
Discount Factor	1	0,990600398	0,981289148	0,972065	0,962928	0,953877	0,944911	0,936029	0,927231	0,918515	0,909882	0,901329	0,892857	0,884465	0,876151	0,867916	0,859757	0,851676	0,843671	0,835741	0,827885	0,820103
Discounted Profit	-71133,33333	-70464,70831	-69802,36809	-69146,3	-68496,3	-67852,5	-15244,6	-15101,3	-14959,3	-14818,7	-14679,4	-14541,4	2708,333	2682,876	2657,658	2632,677	2607,931	2583,418	2559,134	2535,08	2511,251	2487,646
Cumulative Discounted Profi	-71133,33333	-141598,0416	-211400,4097	-280547	-349043	-416895	-432140	-447241	-462201	-477019	-491699	-506240	-503532	-500849	-498191	-495559	-492951	-490367	-487808	-485273	-482762	-480274
NPV 5 Year	**$6 533 945**																					
Discounted Cost	71133,33333	70464,70831	69802,36809	69146,25	68496,31	67852,47	76033,85	75319,17	74611,2	73909,88	73215,16	72526,96	71845,24	71169,92	70500,95	69838,27	69181,82	68531,54	67887,37	67249,25	66617,14	65990,96
Cumulative Total Disc. Cost	$2 572 432																					
Discounted NPV ROI	**254,00%**																					

Figure 38: Implementation payback (part 1)

Discount Rate Yearly	12,00%																							
Discount Rate Monthly	0,95%																							
Month	**0**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**
Membership Revenue	0	3500	3500	5916,667	5916,667	5916,667	5916,667	5916,667	5916,667	5916,667	5916,667	5916,667	5916,667	5916,667	5916,667	7916,667	7916,667	7916,667	7916,667	7916,667	7916,667	7916,667	7916,667	7916,667
Transaction Revenue	0	80000	80000	106000	106000	106000	106000	106000	106000	106000	106000	106000	106000	106000	106000	143000	143000	143000	143000	143000	143000	143000	143000	143000
Capex Opex Savings	0	0	0	22750	22750	22750	22750	22750	22750	22750	22750	22750	22750	22750	22750	32500	32500	32500	32500	32500	32500	32500	32500	32500
Efficiency Benefit	0	0	0	58600	58600	58600	58600	58600	58600	58600	58600	58600	58600	58600	58600	134000	134000	134000	134000	134000	134000	134000	134000	134000
Revenue	**0**	**83500**	**83500**	**193266,7**	**193266,7**	**193266,7**	**193266,7**	**193266,7**	**193266,7**	**193266,7**	**193266,7**	**193266,7**	**193266,7**	**193266,7**	**193266,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**
Cumulative Total Revenue	**$13 428 000**																							
Pilot Cost	71133,33333	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Commercialization Cost	0	80466,67	80466,67	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ongoing Cost	0	0	0	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400
Cost	**71133,33333**	**80466,67**	**80466,67**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**
Cumulative Total Cost	**$3 187 600**																							
Profit	**-71133,33333**	**3033,333**	**3033,333**	**156866,7**	**156866,7**	**156866,7**	**156866,7**	**156866,7**	**156866,7**	**156866,7**	**156866,7**	**156866,7**	**156866,7**	**156866,7**	**156866,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**
Cumulative Profit	**-71133,33333**	**-490233**	**-487200**	**-330333**	**-173467**	**-16600**	**140266,7**	**297133,3**	**454000**	**610866,7**	**767733,3**	**924600**	**1081467**	**1238333**	**1395200**	**1676217**	**1957233**	**2238250**	**2519267**	**2800283**	**3081300**	**3362317**	**3643333**	**3924350**
Total Profit	**$10 240 400**																							
ROI	**321,26%**																							
Discount Factor	1	0,812394	0,804758	0,797194	0,789701	0,782278	0,774925	0,767641	0,760425	0,753277	0,746197	0,739183	0,732235	0,725352	0,718534	0,71178	0,70509	0,698462	0,691897	0,685393	0,678951	0,672569	0,666247	0,659985
Discounted Profit	**-71133,33333**	**2464,263**	**2441,1**	**125053,1**	**123877,7**	**122713,3**	**121559,8**	**120417,2**	**119285,4**	**118164,1**	**117053,4**	**115953,2**	**114863,3**	**113783,6**	**112714,1**	**200022,1**	**198142**	**196279,5**	**194434,6**	**192607**	**190796,5**	**189003,1**	**187226,6**	**185466,7**
Cumulative Discounted Profi	-71133,33333	-477810	-475369	-350316	-226438	-103725	17835,15	138252,4	257537,7	375701,8	492755,3	608708,4	723571,7	837355,3	950069,3	1150091	1348233	1544513	1738948	1931554	2122351	2311354	2498581	2684047
NPV 5 Year	**$6 533 945**																							
Discounted Cost	**71133,33333**	**65370,68**	**64756,22**	**29017,86**	**28745,1**	**28474,91**	**28207,26**	**27942,12**	**27679,47**	**27419,3**	**27161,57**	**26906,26**	**26653,35**	**26402,82**	**26154,64**	**25908,8**	**25665,27**	**25424,03**	**25185,05**	**24948,32**	**24713,82**	**24481,52**	**24251,4**	**24023,45**
Cumulative Total Disc. Cost	**$2 572 432**																							
Discounted NPV ROI	**254,00%**																							

Figure 39: Implementation payback (part 2)

Discount Rate Yearly	12,00%																						
Discount Rate Monthly	0,95%																						
Month	**0**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**
Membership Revenue	0	7916,667	7916,667	7916,667	7916,667	7916,667	7916,667	7916,667	7916,667	7916,667	7916,667	11000	11000	11000	11000	11000	11000	11000	11000	11000	11000	11000	11000
Transaction Revenue	0	143000	143000	143000	143000	143000	143000	143000	143000	143000	143000	230000	230000	230000	230000	230000	230000	230000	230000	230000	230000	230000	230000
Capex Opex Savings	0	32500	32500	32500	32500	32500	32500	32500	32500	32500	32500	42250	42250	42250	42250	42250	42250	42250	42250	42250	42250	42250	42250
Efficiency Benefit	0	134000	134000	134000	134000	134000	134000	134000	134000	134000	134000	209400	209400	209400	209400	209400	209400	209400	209400	209400	209400	209400	209400
Revenue	**0**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**317416,7**	**492650**	**492650**	**492650**	**492650**	**492650**	**492650**	**492650**	**492650**	**492650**	**492650**	**492650**	**492650**
Cumulative Total Revenue	**$13 428 000**																						
Pilot Cost	71133,33333	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Commercialization Cost	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ongoing Cost	0	36400	36400	36400	36400	36400	36400	36400	36400	36400	36400	36566,67	36566,67	36566,67	36566,67	36566,67	36566,67	36566,67	36566,67	36566,67	36566,67	36566,67	36566,66667
Cost	**71133,33333**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36400**	**36566,67**	**36566,67**	**36566,67**	**36566,67**	**36566,67**	**36566,67**	**36566,67**	**36566,67**	**36566,67**	**36566,67**	**36566,67**	**36566,66667**
Cumulative Total Cost	**$3 187 600**																						
Profit	**-71133,33333**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**281016,7**	**456083,3**	**456083,3**	**456083,3**	**456083,3**	**456083,3**	**456083,3**	**456083,3**	**456083,3**	**456083,3**	**456083,3**	**456083,3**	**456083,3333**
Cumulative Profit	**-71133,33333**	**2238250**	**2519267**	**2800283**	**3081300**	**3362317**	**3643333**	**3924350**	**4205367**	**4486383**	**4767400**	**5223483**	**5679567**	**6135650**	**6591733**	**7047817**	**7503900**	**7959983**	**8416067**	**8872150**	**9328233**	**9784317**	**10240400**
Total Profit	**$10 240 400**																						
ROI	**321,26%**																						
Discount Factor	1	0,698462	0,691897	0,685393	0,678951	0,672569	0,666247	0,659985	0,653781	0,647636	0,641548	0,635518	0,629544	0,623627	0,617765	0,611958	0,606206	0,600508	0,594864	0,589272	0,583733	0,578246	0,572811052
Discounted Profit	**-71133,33333**	**196279,5**	**194434,6**	**192607**	**190796,5**	**189003,1**	**187226,6**	**185466,7**	**183723,4**	**181996,5**	**180285,8**	**289849,2**	**287124,7**	**284425,9**	**281752,4**	**279104**	**276480,6**	**273881,8**	**271307,4**	**268757,2**	**266231**	**263728,5**	**261249,5738**
Cumulative Discounted Profi	-71133,33333	1544513	1738948	1931554	2122351	2311354	2498581	2684047	2867771	3049767	3230053	3519902	3807027	4091453	4373205	4652309	4928790	5202672	5473979	5742736	6008967	6272696	6533945,336
NPV 5 Year	**$6 533 945**																						
Discounted Cost	**71133,33333**	**25424,03**	**25185,05**	**24948,32**	**24713,82**	**24481,52**	**24251,4**	**24023,45**	**23797,63**	**23573,95**	**23352,36**	**23238,78**	**23020,34**	**22803,96**	**22589,61**	**22377,28**	**22166,94**	**21958,58**	**21752,18**	**21547,72**	**21345,18**	**21144,54**	**20945,79079**
Cumulative Total Disc. Cost	**$2 572 432**																						
Discounted NPV ROI	**254,00%**																						

Figure 40: Implementation payback (part 2)

11 Discussion and conclusions

This chapter is intended to summarize the work done and identify future research directions related to the main topic of the work. In addition, the content of this section indicates the results of the disclosure of all research questions presented at the beginning.

11.1 Key findings

The purpose of this work was to determine how decentralization using blockchain technology will be able to solve issues of security, trustworthiness and operability of the Internet of Things network. In this thesis, the use of this synergy in the processes of the transport system was considered. In order to affect the greatest radius of possible application of decentralization, the spheres of land transport logistics, as well as transportation using sea transport, were considered.

Since the study is a literature review, it was first necessary to collect all the sources necessary for the study. To search for literature, the snowballing method was used, which allowed us to find the maximum of relevant articles for research. In order to determine the necessary technical information for the study, the IoT technology itself with its centralized architecture was first considered. This approach was chosen in order to conduct a comparative analysis of a centralized model with a decentralized one.

In the next section, basic information about blockchain technology was presented, thanks to which it became possible to understand the construction of decentralization in various kinds of systems. Since smart contracts are one of the key achievements of the blockchain, it was necessary to present its main provisions.

The following sections represent the literature review itself. In order to describe the specific application of this model, the entire review was divided into possible scenarios for its use both inside the city (with ordinary residents and drivers) and in order to maintain and improve business processes. Since transport is one of the most important links in the supply chain, most of the review was devoted to this topic. Thanks to this approach, it has also become possible to describe the use of a decentralized IoT network within a smart port. In addition to improving the efficiency of the supply chain, the work also describes options for using decentralization to improve V2V and V2I communication, transport chain and traffic management, legal issues and decision support in case of emergencies, fraud prevention measures, and so on.

The following is a small part describing the future trends that are inherent in the transport system as a whole. I would also like to note that many of the scenarios described in this thesis are also not widespread, which is why they may also be trends of the future. In conclusion, I conducted an analysis of the cost-effectiveness of implementing such an approach in the supply chain, the entire analysis is based on a study by Forrester and IBM [74].

According to the results of the study, it was possible to provide theoretical evidence of an increase in the level of security and efficiency of operating things inside the network, where data is stored in a distribution database.

11.2 Contributions

At the beginning of the study, I identified the following research questions:

RQ1: What is the essence of smart transportation?

One of the main aspects of the development of a smart city is the development of its intelligent transport system, which will increase the capacity on the roads, make trips safer and more efficient. Thanks to the equipment of the transport infrastructure and the vehicles themselves of various sensors and other environment-reading devices, it will be possible to exchange things within the transport chain, and together with the analytics systems of this data, it will automatically perform the following functions:

- travel and traffic management;
- public transport management;
- emergency management;
- decision support in case of accidents;
- supply chain monitoring and management;
- etc.

RQ2: What advantages does decentralization give to the Internet of Things?

IoT in combination with blockchain technology allows to create an environment where device owners can trust the data received from the owners of other devices, as the blockchain allows you to ensure the immutability, integrity and protection of data. In addition, this approach allows to ensure the confidentiality of the owners. At the same time, smart contracts will allow network participants to maintain and ensure consistency of operations between participants in accordance with predefined business logic.

Another advantage of this approach is that the blockchain is a universal digital registry for performing transactions of various types between devices, which serves to register devices, authenticate them and verify security.

RQ3: Which Smart transportation processes already use the decentralized Internet of Things.

In the thesis, the author identified eight main directions of using decentralized solutions for IoV:

- Vehicle communication;
- Vehicle Management;
- Data Management and Services;
- Traffic control;
- Ride Sharing;
- Forensic application;
- Transportation Insurance;
- Managing the transportation of dangerous goods.

Each of the categories listed above is critical for creating a fully intelligent transport environment that allows vehicles and infrastructure facilities to safely exchange data, build the most suitable routes, reducing traffic density, regulate legal processes, provide insurance, and so on. Having implemented all this set of directions on the roads, residents of the city will be able to move much more comfortably and safely.

RQ4: Which Smart Port processes can still be improved with the help of these technologies.

At the stage of collecting scientific literature for review, the author found very little relevant literature for this review. But despite this, a review of the literature found was conducted, where a decentralized approach was used to monitor the security situation in the port, as well as planning the location of cargo on the ship.

In addition, thanks to the information received in the previous sections, the author suggested which approaches can also be used for the transportation of goods by sea. For example, smart containers can exchange information with their owners and other stakeholders, which will make the transportation process transparent and more efficient. Also, the information systems of the port, as one of the direct participants in the supply chain, with their decentralization, will be able to automatically send all the necessary data to stakeholders, receiving them from devices.

RQ5: What is the future of the decentralized Internet of Things in smart transport?

As mentioned earlier, at this stage of the development of intelligent road systems, most of the use cases described in this thesis are the future for humanity. In addition, the creation of a single ecosystem where it will be possible to interact all modes of transport within one system is key for all researchers in the future.

Researchers considered the main problems of using the symbiosis of blockchain and IoT to be difficulties in creating a model where devices can exchange data in real time, as well as problems of scalability of the blockchain registry. In this thesis, articles were analyzed that are also aimed at solving these problems, and each of them has practical validity, and real test cases are considered. The main significance of such a study is also that it covers all stages of building a decentralized IoT model in the transport sector, and 4 main options for integrating technologies that are applied in accordance with the requirements of specific applications were considered. In addition to the sphere of urban movements, movements inside and outside the seaport are also considered. The thesis proposes methods of data protection within the IoT network proposed by other researchers, as well as the use of new methods based on insights identified in previous sections. If we talk about what is missing in the work, it is a review of works that are aimed at researching the creation of a unified intelligent transport model within the city, where it is also necessary to consider issues of state regulation, huge scalability and the implementation of instant data transfer between those devices that need this or that information.

11.3 Limitations and future research

The key limitation of this study is the fact that it is entirely based on theoretical research, the author has not conducted a single practical experiment. In order to make the research applied, most of the articles considered in this thesis had sections where the authors tested the proposed theories on various kinds of data, thereby simulating real situations.

Another limitation is the fact that in the real world, a fairly small number of companies implement this approach into their systems, which means that the evidence base is extremely limited.

Future research related to this topic may be related to:

- Consideration of the possibility of applying decentralization to the entire IoT chain in a smart port;
- Creating a unified road infrastructure inside the city, where all devices, including residents' personal cars, will be connected to the same network;
- Research within the framework of creating a single transport ecosystem of various scales, including all types of transport;
- Studies aimed at combining existing scenarios for the application of decentralization in IoV.

References

1. Kurt R. Industry 4.0 in terms of industrial relations and its impacts on labour life //Procedia computer science. – 2019. – 158. – p . 590-601.
2. Melkonyan A., Krumme K. (ed.). Innovative Logistics Services and Sustainable Lifestyles: Interdependencies, Transformation Strategies and Decision Making. – Springer, 2019.
3. Ahmad R. W. et al. Blockchain applications and architectures for port operations and logistics management. Research in Transportation Business & Management, 100620. – 2021.
4. de la Peña Zarzuelo I. Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue //Transport Policy. – 2021. – T. 100. – C. 1-4.
5. To Get Smart, Ports Go Digital (2018). Available at: https://www.bcg.com/publications/2018/to-get-smart-ports-godigital.aspx
6. Jović M. et al. An overview of security challenges of seaport IoT systems //2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). – IEEE, 2019. – C. 1349-1354.
7. Banafa A. IoT and blockchain convergence: benefits and challenges //IEEE Internet of Things. – 2017. – T. 9.
8. IoT: number of connected devices worldwide 2012-2025 | Statista (2016).
9. IoT security: How we are keeping consumers safe from cyber threats/ Available at: https://www.weforum.org/impact/iot-security-keeping-consumers-safe/
10. Pureswaran V., Brody P. Device democracy: Saving the future of the Internet of Things //IBM Corporation. – 2015. – C. 23.
11. Dai H. N., Zheng Z., Zhang Y. Blockchain for Internet of Things: A survey //IEEE Internet of Things Journal. – 2019. – T. 6. – №. 5. – C. 8076-8094.
12. Smart home device shipments worldwide from 2020 to 2025. Available at: https://www.statista.com/statistics/1223274/smart-home-device-shipments worldwide/#statisticContainer

13. Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid — the new and improved power grid: a survey. IEEE Communications Surveys & Tutorials, 14(4), 944-980

14. Wu C. L., Liao C. F., Fu L. C. Service-oriented smart-home architecture based on OSGi and mobile-agent technology //IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). – 2007. – Т. 37. – №. 2. – С. 193-205.

15. Li S., Xu L. D., Zhao S. The internet of things: a survey //Information systems frontiers. – 2015. – Т. 17. – №. 2. – С. 243-259.

16. Li S., Da Xu L., Zhao S. 5G Internet of Things: A survey //Journal of Industrial Information Integration. – 2018. – Т. 10. – С. 1-9.

17. IERC. (2013). Coordinating and building a broadly based consensus on the ways to realise the internet of things in Europe; available from http://www.internet-of-things-research.eu/pdf / Poster_IERC_A0_V01.pdf.

18. Kranenburg, V. (2013). Moscow futurodesign lab co-create urban intelligence: designing smart interfaces between people and city; available from http://www.theinternetofthings.eu / content/moscow-futurodesign-laboratory-workshop-co-createurban-intelligence-designing-smart-interfa.

19. Fremantle P. A reference architecture for the internet of things //WSO2 White paper. – 2015. – С. 02-04

20. Sobin C. C. A survey on architecture, protocols and challenges in IoT //Wireless Personal Communications. – 2020. – Т. 112. – №. 3. – С. 1383-1429.

21. Ullo S. L., Sinha G. R. Advances in IoT and smart sensors for remote sensing and agriculture applications //Remote Sensing. – 2021. – Т. 13. – №. 13. – С. 2585.

22. Di Francesco M., Das S. K., Anastasi G. Data collection in wireless sensor networks with mobile elements: A survey //ACM Transactions on Sensor Networks (TOSN). – 2011. – Т. 8. – №. 1. – С. 1-31.

23. Xia F. et al. Wireless sensor/actuator network design for mobile control applications //Sensors. – 2007. – Т. 7. – №. 10. – С. 2157-2173.

24. Dargie W., Poellabauer C. Fundamentals of wireless sensor networks: theory and practice. – John Wiley & Sons, 2010.

25. Current state of M2M (machine-to-machine) systems. Available at: https://sudonull.com/post/104153-Current-state-of-M2M-machine-to-machine-systems

26. What is lidar? Available at: https://oceanservice.noaa.gov/facts/lidar.html

27. Fremantle P. A reference architecture for the internet of things //WSO2 White paper. – 2015. – p. 02-04

28. MQTT V3.1 Protocol Specification. Available at: http://public.dhe.ibm.com/software/dw/webservices/ws-mqtt/mqtt-v3r1.html

29. Ding Z. et al. Enabling smart transportation systems: A parallel spatio-temporal database approach //IEEE Transactions on Computers. – 2015. – Т. 65. – №. 5. – С. 1377-1391.

30. D’Orey, P., & Ferreira, M. (2014). Its for sustainable mobility: A survey on applications and impact assessment tools. IEEE Transactions on Intelligent Transportation Systems, 15(2),477–493

31. Elkosantini, S., & Darmoul, S. (2013). Intelligent public transportation systems: A review of architectures and enabling technologies. In Proceedings of international conference on advanced logistics and transport (ICALT)

32. Moazzami M. et al. Internet of Things Architecture for Intelligent Transportation Systems in a Smart City //2021 3rd Global Power, Energy and Communication Conference (GPECOM). – IEEE, 2021. – С. 285-290.

33. Daniel C. Smith, "Vehicle to vehicle communications: Readiness for application", National Highway Traffic Safety Administration, 2018

34. Bazzi A., Masini B. M. Taking advantage of V2V communications for traffic management //2011 IEEE Intelligent Vehicles Symposium (IV). – IEEE, 2011. – С. 504-509.

35. S. Sundaresan, K. Suresh Kumar, R. Nishanth, Y. Harold Robinson, A. Jaya Kumar, Chapter 3 - Artificial intelligence and machine learning approaches for smart transportation in smart cities using blockchain architecture, Editor(s): Saravanan Krishnan, Valentina Emilia Balas, E. Golden Julie, Y. Harold Robinson, Raghvendra Kumar, 2021, Pages 35-56

36. Xu H., Lin J., Yu W. Smart transportation systems: architecture, enabling technologies, and open issues //Secure and Trustworthy Transportation Cyber-Physical Systems. – Springer, Singapore, 2017. – С. 23-49.

37. Gross weight of seaborne freight handled in all ports, 2020 (tonnes per capita). Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=File:Gross_weight_of_seaborne_freight_handled_in_all_ports,_2020_(tonnes_per_capita).png

38. Heilig L., Schwarze S., Voß S. An analysis of digital transformation in the history and future of modern ports. – 2017.

39. Laas B. T. The new port infrastructure: strategic design of a container data platform for Port of Rotterdam. – 2020.

40. Heilig L., Schwarze S., Voß S. An analysis of digital transformation in the history and future of modern ports. – 2017.

41. Port of Rotterdam. (2019c). Move Forward: Step by step towards a digital port. White paper. https://www.portofrotterdam.com/en/port-forward/step-by-steptowards-a-digital-port

42. OCR in Ports and Terminals. (2013). A PEMA Information Pape. https://www.portofrotterdam.com/en/port-forward/step-by-steptowards-a-digital-port

43. To get smart ports go digital. Available at: https://www.bcg.com/publications/2018/to-get-smart-ports-go-digital

44. Sandelowski M., Barroso J. Handbook for synthesizing qualitative research. – springer publishing company, 2006.

45. Wnuk K., Garrepalli T. Knowledge management in software testing: a systematic snowball literature review //e-Informatica Software Engineering Journal. – 2018. – Т. 12. – №. 1.

46. Jalali S., Wohlin C. Systematic literature studies: database searches vs. backward snowballing //Proceedings of the 2012 ACM-IEEE international symposium on empirical software engineering and measurement. – IEEE, 2012. – С. 29-38.

47. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71.

48. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE.

49. Salah, Khaled & Khan, Minhaj. (2017). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems. 82. 10.1016/j.future.2017.11.022.

50. Chen, G., Xu, B., Lu, M. et al. Exploring blockchain technology and its potential applications for education. Smart Learn. Environ. 5, 1 (2018). https://doi.org/10.1186/s40561-017-0050-x

51. What Are Smart Contracts? Available at: https://www.cryptoninjas.net/what-are-smart-contracts%20/

52. Major cyber attack disrupts internet service across Europe and US. Available at: https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service

53. Viriyasitavat W., Anuphaptrirong T., Hoonsopon D. When blockchain meets Internet of Things: Characteristics, challenges, and business opportunities //Journal of industrial information integration. – 2019. – T. 15. – C. 21-28.

54. Panarello A. et al. Blockchain and iot integration: A systematic survey //Sensors. – 2018. – T. 18. – №. 8. – C. 2575.

55. Pureswaran V., Brody P. Device democracy: Saving the future of the Internet of Things //IBM Corporation. – 2015. – C. 23.

56. Ali M. S. et al. Applications of blockchains in the Internet of Things: A comprehensive survey //IEEE Communications Surveys & Tutorials. – 2018. – T. 21. – №. 2. – C. 1676-1717.

57. S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, “A blockchain connected gateway for BLE-based devices in the Internet of Things,” IEEE Access, vol. 6, pp. 24639–24649, 2018

58. Reyna A. et al. On blockchain and its integration with IoT. Challenges and opportunities //Future generation computer systems. – 2018. – T. 88. – C. 173-190.

59. Christidis K., Devetsikiotis M. Blockchains and smart contracts for the internet of things //Ieee Access. – 2016. – T. 4. – C. 2292-2303.

60. Jabbar R. et al. Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum //Sensors. – 2020. – T. 20. – №. 14. – C. 3928.

61. Xu Z. et al. Modeling relationship between truck fuel consumption and driving behavior using data from internet of vehicles //Computer-Aided Civil and Infrastructure Engineering. – 2018. – Т. 33. – №. 3. – С. 209-219.

62. Zichichi M., Ferretti S., D'angelo G. A framework based on distributed ledger technologies for data management and services in intelligent transportation systems //IEEE Access. – 2020. – Т. 8. – С. 100384-100402.

63. Benet J. Ipfs-content addressed, versioned, p2p file system //arXiv preprint arXiv:1407.3561. – 2014.

64. Popov S. The tangle //White paper. – 2018. – Т. 1. – №. 3.

65. Ren Q. et al. Intelligent design and implementation of blockchain and Internet of things–based traffic system //International Journal of Distributed Sensor Networks. – 2019. – Т. 15. – №. 8. – С. 1550147719870653.

66. Ren Q. et al. Using blockchain to enhance and optimize IoT-based intelligent traffic system //2019 International Conference on Platform Technology and Service (PlatCon). – IEEE, 2019. – С. 1-4.

67. Li M., Zhu L., Lin X. CoRide: A privacy-preserving collaborative-ride hailing service using blockchain-assisted vehicular fog computing //International Conference on Security and Privacy in Communication Systems. – Springer, Cham, 2019. – С. 408-422.

68. Cebe M. et al. Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles //IEEE Communications Magazine. – 2018. – Т. 56. – №. 10. – С. 50-57.

69. Li Z. et al. Blockchain and IoT data analytics for fine-grained transportation insurance //2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). – IEEE, 2018. – С. 1022-1027.

70. Imeri A., Agoulmine N., Khadraoui D. Blockchain and IoT integrated approach for a trusted and secured process to manage the transportation of dangerous goods //Revista de Sistemas e Computação-RSC. – 2020. – Т. 10. – №. 1.

71. Banerjee A. Blockchain with IOT: Applications and use cases for a new paradigm of supply chain driving efficiency and cost //Advances in computers. – Elsevier, 2019. – Т. 115. – С. 259-292.

72. Tang C., Ma Y., Yu X. Design and Implementation of Port Video Terminals Security Access Authentication System Using Blockchain Technology //E3S Web of Conferences. – EDP Sciences, 2021. – Т. 253. – С. 03086.Henesey L. et al. Improved load planning of roro vessels by adopting blockchain and internet-of-things //Proceedings of the 22nd International Conference on Harbor, Maritime and Multimodal Logistics Modelling and Simulation, HMS. – 2020. – С. 58-65.

73. Прогнозный анализ перспективной технологии: Применение методики Total Economic Impact™ (Совокупный экономический эффект) для анализа IBM Blockchain. (2018). Forrester company report. https://www.ibm.com/downloads/cas/GB6BQWM8

74. Chen C. et al. Smart-contract-based economical platooning in blockchain-enabled urban internet of vehicles //IEEE Transactions on Industrial Informatics. – 2019. – Т. 16. – №. 6. – С. 4122-4133.

75. Sorokin I. Wireless sensor networks for agriculture systems //IOP Conference Series: Earth and Environmental Science. – IOP Publishing, 2021. – Т. 686. – №. 1. – С. 012045.

76. WANG Y. et al. Intelligent Road Transport Systems. 2022

77. Net Present Value (NPV). Available at: https://www.investopedia.com/terms/n/npv.asp

78. Return on Investment (ROI). Available at: https://www.investopedia.com/terms/r/returnoninvestment.asp#:~:text=Return%20on%20investment%20(ROI)%20is%20calculated%20by%20dividing%20the%20profit,when%20expressed%20as%20a%20percentage.