Research Article

Oldřich Kodym*, Lukáš Kubáč, and Libor Kavka

Risks associated with Logistics 4.0 and their minimization using Blockchain

https://doi.org/10.1515/eng-2020-0017
Received Oct 30, 2019; accepted Dec 18, 2019

Abstract: Currently we are saying that we are at the dawn of the fourth revolution, which is marked by using cyber-physical systems and the Internet of Things. This is marked as Industry 4.0 (I4.0). With Industry 4.0 is also closely linked concept Logistics 4.0. The highly dynamic and uncertain logistic markets and huge logistic networks require new methods, products and services. The concept of the Internet of Things and Services (IoT&S), Big Data/Data Mining (DM), cloud computing, 3D printing, Blockchain and cyber physical system (CPS) etc. seem to be the probable technical solution for that. However, associated risks hamper its implementation and lack a comprehensive overview. In response, the paper proposes a framework of risks in the context of Logistics 4.0. They are here economic risks, that are associated *e.g.* with high or false investments. From a social perspective, risks the job losses, are considered too. Additionally, risks can be associated with technical risks, *e.g.* technical integration, information technology (IT)-related risks such as data security, and legal and political risks, such as for instance unsolved legal clarity in terms of data possession. It is therefore necessary to know the potential risks in the implementation process.

Keywords: Logistics 4.0, risks, risk management

1 Introduction

The current Industry 4.0, *i.e.*, the fourth industrial revolution, is characterized by the major role played by new information technologies in processes and ways of working, inevitably shaped by globalization and the internationalization of companies [1]. Logistic 4.0 as a concept is based on these same principles and refers to logistics management defined by interconnection, digitalization of information and cloud-based computer applications. The complexity of the information to be handled increases, based on advances in robotization and the standardization of processes that has become mandatory due to the expansion of international trade.

Logistic 4.0 is the use of Cyber-Physical systems (CPS) that monitor and control the physical processes, usually with feedback where physical processes affect computations and vice versa [2]. This CPS use RFID technology in order to identify, sensing and locate the items, and send the data to a computer which can collect and analyze this relevant information. These systems are able to communicate with other systems or with humans using the internet as a mean of communication and data storage, so that it can be shared data in real time and processes can be coordinated. This is possible through the use of IoT&S, Big Data, Data mining and last but not least, cloud computing technologies.

Use of these technologies will greatly reduce the work that requires human's intervention in each step of the supply chain. Technologies are replacing the process which is operated and decision-making by the humans. The supply chain management will be a big network where all the stakeholders in the supply chain form suppliers to customers are able to access it. All the process from the customers or suppliers can be managed online in real time. All activities in logistics will come from the information received from the internet platform used by all the stakeholders. The warehouses expense can be reduced to the minimum or might disappear completely because the customers' orders and the orders to the suppliers are processed at the same time, or alternatively due using 3D printing, when products are created after the orders is created. This saves not only storage space but also the amount of raw materials used. Another technology with great potential is Blockchain. Blockchain is bringing "trust" because it allows keeping the record throughout the flow of physical goods. Thanks to a reliable record in Blockchain, com-

***Corresponding Author: Oldřich Kodym:** Department of Master Studies, College of Logistics, Přerov, 750 02, Czech Republic; Email: oldrich.kodym@vslg.cz
Lukáš Kubáč: Technical University of Ostrava, Department of Control Systems and Instrumentation, Ostrava, 708 33, Czech Republic; Email: lukas.kubac@vsb.cz
Libor Kavka: Department of Bachelor Studies, College of Logistics, Přerov, 750 02,Czech Republic; Email: libor.kavka@vslg.cz

panies can establish measures quickly and transparently. With Blockchain, physical (paper) records can be fully replaced with trusted digital records throughout the supply chain. It also allows to make full use of the Smart Contract, thereby increasing the level of automation and digitization.

However, impacts of the implementation of new technologies are not clear. Companies are working towards a more digitized environment in which processes are automated, monitored real-time and self-configured. Companies are getting more transparent by the use of more data which is acquired, analyzed and used to make decisions. Logistics 4.0 also enables more flexibility which supports mass-customization. Besides this more data will be shared throughout the supply chain which will optimize transparency and Supply Chain performances. Important in this process is to take risks into account. On both side, cyber and physical, risks occur, and companies are getting more vulnerable. Risk assessment while using risk models should create awareness of risks.

One of the biggest hurdles that shippers, freight forwarders, and logistics managers need to overcome in order to build toward Logistics 4.0 adoption is the introduction of IoT devices into the value chain [3]. By equipping trucks, pallets, containers, etc. with devices RTLS (Real-time locating systems) that can provide real-time data streams for planners, we can create an environment in which all of shipments can be monitored in real-time and proactively adjusted in cases of potential disruption or uncertainty. These devices require large, dedicated initial efforts into researching, selecting, and implementing the right hardware options before we can achieve results. Logistics 4.0 provides value in a number of ways, from improved disruption management to increased flexibility across the entire value chain, each of which stems from E2E (end-to-end) visibility and process transparency. Without a high level of visibility and transparency, all the fancy technology in world won’t help us to improve logistics operations. In order to achieve the level of high visibility, each touchpoint on the value chain must be connected via digital infrastructure to every other point. The Logistics 4.0 aim is not to replace humans in their works, but to avoid inaccuracies and to have faster processes where the information can be shared effortless and in real time. It will be always needed the involvement of people controlling the processes and taking control of any system failure.

2 Risks of the implementation process

Logistics companies face and are exposed to several types of risk. The International Organization for Standardization (ISO) defined risk in ISO 31000 as “the effect of uncertainty on objectives”. Otherwise, the risk is expressed as a combination of the consequences of an event and the associated probability of occurrence [4]. Now let’s see what risks need to be assessed before we begin implementing the Logistics 4.0 concept (see Figure 1). The main types of risks are economic, technical / IT, social, environmental and legal / political.

To express the risk of processes mathematically, we define total risk as the sum over individual risks R_i, which can be computed as the product of potential losses L_i, and their probabilities $p\left(L_i\right)$:

$$R_i = L_i p\left(L_i\right) \tag{1}$$

$$R_{total} = \sum_i L_i p\left(L_i\right)$$

Equation 1. Risk evaluation[1]

Even though for some risks R_i, R_j, we might have $R_i = R_j$, if the probability $p\left(L_j\right)$ is small compared to $p\left(L_i\right)$, its estimation might be based only on a smaller number of prior events, and hence, more uncertain. On the other hand, since $R_i = R_j$ L_j must be larger than L_i, so decisions based on this uncertainty would be more consequential, and hence, warrant a different approach.

2.1 Economic Risks

Automation, digitization, and networking technology requires large expenditures for infrastructure, implementation and maintenance costs. Investing in new technologies brings a high financial risk because we do not know which processes will be economically advantageous in the long term and which will not. Technologies are full of uncertainty that will be truly necessary and successful. Choosing the right time and method of investment to be divided between different technologies and different parts of the supply chain can be seen as a crucial success factor regarding Logistics 4.0 [5]. There is a risk of incorrect investment in poor or often immature technologies. On the other hand, there is a risk of postponing investments, where compa-

[1] Source: https://en.wikipedia.org/wiki/Risk_assessment

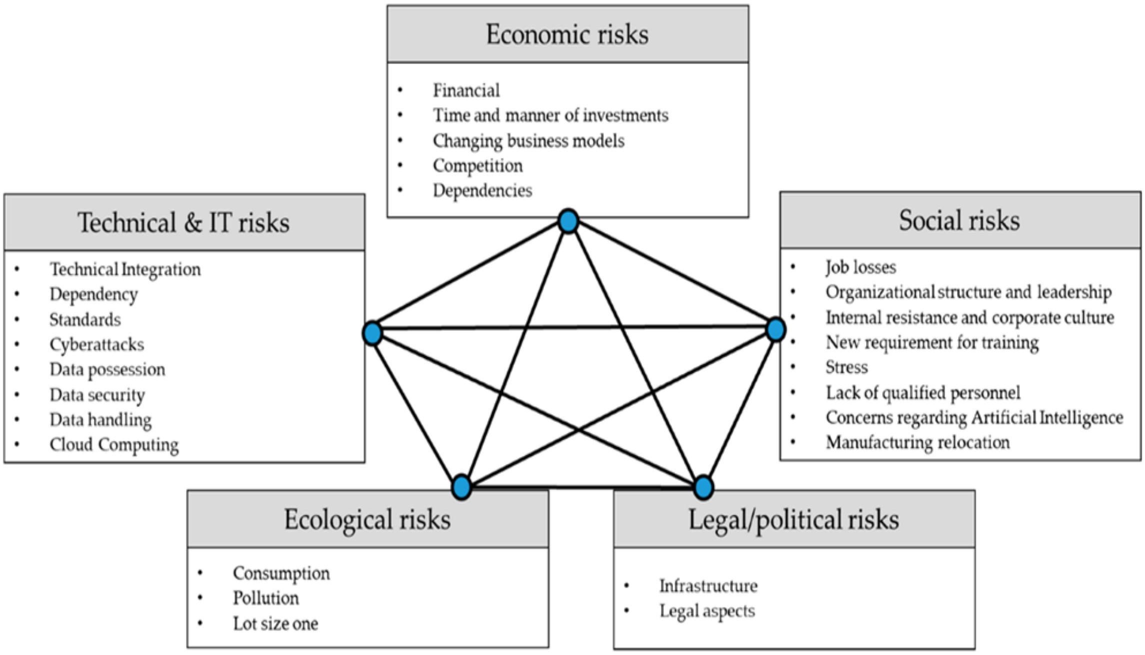

Figure 1: Industry 4.0 risk framework[2]

nies can miss trends and thus the opportunity to place themselves on the market.

Another economic risk is the adoption of technologies related to Logistics 4.0. One part of customers is increasingly focusing on new product and service options, but another group of customers may be reluctant to pay for new technologies. Another aspect is the emergence of new business models. Existing business models are focused on product marketing. Many current executives do not know how to generate value from data. Companies lack the expertise to develop data-based business models, or lack the resources to collect the necessary amount of data to generate their value.

The principle of Logistics 4.0 is related to the transparency of processes and data. However, there is a risk and concern that increased transparency of data in the supply chain might be used to their disadvantage, *e.g.* when negotiating price or other terms of trade, based on knowledge of key numbers such as transmission capacity, average delivery speed, etc. Great concern brings fear of possibly excessive dependence on suppliers of necessary technologies, for example, with respect to repairs, updates or maintenance of systems that the user cannot perform independently. The provider can then demand a high price for these services.

2.2 Technological and IT Risks

The implementation and use of Logistics 4.0 solutions involves technical risks. The technical complexity is increasing, resulting from a merging of mechanical and IT systems across several stakeholders in a supply chain. Logistics 4.0 might bring a great deal of potential, but also is associated with a high level of complexity in order to be implemented. Digital transformation can be accomplished in two ways. The first way is to use a new infrastructure, including a technical side in the form of a new information and communication technology (ICT), but also an employee who will use the new technology. This method requires a large investment but guarantees greater compatibility. The second way is to incorporate new technologies into existing infrastructure. This would reduce the cost of implementing Logistics 4.0. However, from a technical point of view, this poses large technical challenges with very uncertain results and significant compromises. Software development that is compatible with existing technical solutions is also a risk with this method. Whereas existing systems might not be easily compatible, new developments would cost a lot of resources. Therefore, making

[2] Source: https://www.mdpi.com/sustainability/sustainability-11-00384/article_deploy/html/images/sustainability-11-00384-g001.png

software compatible with existing IT solutions in supply chain is described as a large risk.

In the concept of Logistics 4.0 is a great dependency on technology and software. In the event of a software or a system failure, the entire operational value chain could break down. The enterprise or even the entire supply chain becomes highly dependent on the functionality of the technical systems. For this reason, the system must be as resilient and redundant as possible, to ensure operability in the event of a part of the system failing.

In order within Logistics 4.0 technologies to generate value from data and allow data analysis, data needs to be on a level that ensures quality and consistency, calling for unified standards across different functions. It is therefore necessary to develop unified standards that apply throughout the supply chain. The clear definition of interfaces, especially across companies, is of vital importance. Explicit areas of responsibility have to be defined, and the new technologies needs to be integrated into the operational organization.

It is very important to know IT risks when implementing Logistics 4.0. The use of ICT opens the gates to attacks from the virtual world [6]. The larger the network and the more interfaces that exist, the larger the potential attack surface for cyberattacks. Preparations must be made in order to minimize these risks on a technical and organizational level. Technical solutions include firewalls and virtual private network connections.

Critical is the issue of data protection. Competitive advantages can be lost if information falls in the hands of competitors or third parties. This is not only a question of how to protect data from third parties, but also to know which kind of data belongs to whom. In the concept of Logistics 4.0, data ownership remains a central question, because if data is shared along the entire supply chain and on clouds, it becomes hard to control where the data came from and who is allowed to use the data. This is not only a technical point of view, but also a legal question.

Relating to data itself, the amount of data generated and handled must be controlled. Appropriate data quality must be ensured across a multitude of data types. This also relates to theaspects of technical integration and required standards. Data competence must be built up, ensuring that the data that is generated is put to a meaningful purpose and interpreted in a right way. This is the domain of Big Data technology. Big data challenges include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating, information privacy and data source. Following Formula 1, information and communication technologies involved into data/information transfer/processing are one of individual risks.

The core technology of Logistics 4.0 is Cloud computing. Organizations often have concerns about the migration and utilization of cloud computing due to the loss of control over their outsourced resources and cloud computing is vulnerable to risks. Cloud environments experience the same threats as traditional data center environments; the threat picture is the same. That is, cloud computing runs software, software has vulnerabilities, and adversaries try to exploit those vulnerabilities [7]. However, unlike information technology systems in a traditional data center, in cloud computing, responsibility for mitigating the risks that result from these software vulnerabilities is shared between the cloud service providers (CSP) and the cloud consumer. As a result, consumers must understand the division of responsibilities and trust that the cloud service providers meets their responsibilities. The following vulnerabilities are a result of a CSP's implementation of the five cloud computing characteristics:

- Consumers lose some visibility and control over operations when transitioning operations to the cloud. When using external cloud services, the responsibility for some of the policies and infrastructure moves to the CSP.
- On-Demand Self Service Simplifies Unauthorized Use. The on-demand self-service provisioning features of the cloud enable an organization's personnel to provision additional services from the agency's CSP without IT consent. Due to the lower costs and ease of implementing platform as a service (PaaS) and software as a service (SaaS) products, the probability of unauthorized use of cloud services increases. However, services provisioned or used without IT's knowledge present risks to an organization. The use of unauthorized cloud services could result in an increase in malware infections or data exfiltration since the organization is unable to protect resources it does not know about. The use of unauthorized cloud services also decreases an organization's visibility and control of its network and data.
- Internet-Accessible Management APIs can be Compromised. CSPs expose a set of application programming interfaces (APIs) that customers use to manage and interact with cloud services (also known as the management plane). Organizations use these APIs to provision, manage, orchestrate, and monitor their assets and users. These APIs can contain the same software vulnerabilities as an API for an operating system, library, etc. Unlike management APIs for on-

premises computing, CSP APIs are accessible via the Internet exposing them more broadly to potential exploitation.
- Separation Among Multiple Tenants Fails. Exploitation of system and software vulnerabilities within a CSP's infrastructure, platforms, or applications that support multi-tenancy can lead to a failure to maintain separation among tenants. This failure can be used by an attacker to gain access from one organization's resource to another user's or organization's assets or data [8]. Multi-tenancy increases the attack surface, leading to an increased chance of data leakage if the separation controls fail.
- Data Deletion is Incomplete. Threats associated with data deletion exist because the consumer has reduced visibility into where their data is physically stored in the cloud and a reduced ability to verify the secure deletion of their data. This risk is concerning because the data is spread over a number of different storage devices within the CSP's infrastructure in a multi-tenancy environment. In addition, deletion procedures may differ from provider to provider. Organizations may not be able to verify that their data was securely deleted and that remnants of the data are not available to attackers. This threat increases as an agency uses more CSP services [9].

It follows from the above that the use of CSP services entails a number of risks that can be eliminated or at least reduced by building your own cloud solution, where we are not dependent on a third party in the form of CSP. Such a solution is more advantageous from the security point of view, but entails, among other things, higher investments in the necessary infrastructure. For this reason, many companies choose to use CSP services at least at the beginning of the transformation. Following Formula 1, information and communication technologies involved into data/information transfer/processing are again one of individual risks.

2.3 Social Risks

Of the social risks, job loss is probably the most likely [10]. This applies in particular to those activities that can be automated. The second vulnerable group are employees who are not able to adapt quickly enough and meet the new requirements for activities within the ICT [11]. In particular, IT-related skills will be in demand in the future. Training should ensure that all employees are adequately prepared. Due to the competitive pressure on the labor market and the large number of alternatives for specialists, skilled personnel in particular is associated with high costs. Alternatively, IT-related experts can be accessed via external service providers, which can be contracted, but also are expensive and generate new dependencies. Employees who understand the traditional approach and IT at the same time are highly valued, to mediate between both. New demands on employees and additional tasks at work can lead to overload and strain. The loss of social interaction, as tasks are given increasingly to computers and automated services, is a further social risk.

Among others, additional risks arise from internal resistance and an inadequate corporate culture. It remains a risk that older employees or medium-level managers do not support the necessities of organizational transformation. The risk for an organization to be paralyzed and miss important developments due to a lack of openness and courage to do something new is critical. New systems and processes should be accepted and used. Vital features such as communication and the exchange of information have to be ensured. Relating to several economic and social risks, there is a risk that manufacturing, and services relocation could be a result. Employees' resistance or lack of qualified personnel could drive owners to relocate their business to areas of the world where both aspects do not play such a major role.

2.4 Ecological Risks

One of the areas that needs to be considered from an ecological point of view is consumption. The implementation of Logistics 4.0 in practice and the application of digitization and new technologies involves various ecological risks and impacts. Thoughtful implementation plan can mean the critical difference whether Logistics 4.0 will bring environmental benefits or vice versa environmental risks. An example might be the consumption of raw materials or energy. Implementation of Logistics 4.0 technologies usually requires new machines whose production requires a large amount of raw material. For example, if the generation, transport, and storage of energy for the implementation and use of Logistics 4.0 technologies consumes more energy than the efficiency gains that would be generated, then assuming the complete adoption of all external effects is at least questionable from a macroeconomic point of view [12]. This relates especially to data transmission, decentralized systems such as Blockchain. Each verification transactions within Blockchain requires high computing power and thus high energy consumption. The larger the Blockchain network, the more energy-intensive it is.

Among the ecological risks are increased waste generation and emissions. Many companies making efforts to retrofit the existing machinery and equipment to save costs and resources. However, this will not be possible for the vast majority, due to the great complexity and required new technological capabilities. The majority of parts of the old machines or plants has to be discarded and ends up in landfills. This represents a burden on the global environment, especially since the decomposition and degradation of many waste materials takes a very long time.

An interesting question is Customization - of whether it's an advantage or a risk. On the one hand, customization can mean time, material and energy savings, because the product is produced only on the basis of a specific order. On the other hand, product standardization involves the possibility of product re-use, while individualized products are more difficult to reuse. Therefore, waste might be increased, and recycling might become more difficult with non-standardized products. An inadequate infrastructure poses a major risk to competitiveness in the global market.

2.5 Legal and Political Risk

The applicability or diffusion of technologies is also influenced by politicians through laws that either support new technologies and create a favorable environment for their application, or, on the contrary, may create obstacles to the wider deployment of new technologies, either through legislative obstacles or political inactivity - thus, the absence of necessary laws. If digitization and networking are to find their way into the economy, the infrastructure must support and positively influence these efforts. Politicians must ensure that an appropriate infrastructure is provided [13].

One aspect that is often neglected but will have a major impact on the success of I4.0, are legal issues and how they will affect digital transformation. From a legal point of view, open questions need to be clarified with regard to data protection, data possession, data handling, liability (product liability, contractual liability and distribution/assignment of risk), jurisdiction, data protection and IT security, labor law, Intellectual Property. Another risk is the lack of standards, which hampers cross-border cooperation. Some questions of jurisdiction remain unresolved, such as for example when a transaction with a foreign company is carried out via the Internet or the role of online contracts or even "smart contracts" that are made automatically [14].

3 Risk management

We mentioned possible risks associated with the implementation of the Logistics 4.0 concept. At the same time, we must not forget the risks of common logistics processes and of course the risks that individual technologies bring (their weaknesses). But how to work with risks? The answer is Risk management.

Risk management is a systematic mechanism for managing the risks or threats facing an organization in order to enable it to recognize the events that may result in unfortunate or damaging consequences and to establish the best course of action for identifying, assessing, understanding, acting on, and communicating risk issues [15, 16]. The risk management process aims to identify and assess risks in order to enable the risks to be understood clearly and managed effectively. The key step linking identification/assessment of risks with their management is understanding [17]. Risk management also includes taking appropriate measures to minimize threats. However, it is not a one-off process: if risk management is to be effective, it is a continuous process.

In general, risk management steps can be identified:

1. **Establishing the context**: it focuses on the activities of the Company; it identifies what can threaten us with respect to needs, which includes social, economic, legal, technological and ecological factors. In establishing the context, it is also necessary to identify those entities that may influence some of our risk management decisions. A key aim of the 'establish the context' step in the risk management process is to identify the organization's objectives, and those external and internal factors that could be a source of uncertainty, so that risks can be identified more readily.
2. **Identify the Risk**: A company should identify internal and external events that have the potential to effect the company's operations by analyzing the workflows and processes and listing risks and causes, the extent of risk that is faced, and the impact of identified risks on company's operations. It is important that the internal and external events that could affect the achievement of the objectives of the organization are identified, distinguishing between risks and opportunities. For the identification of risks, multiple systems can be used. One of them is to use similar backgrounds, both in our company and in other companies that resemble by their activity or reach. Another possibility is to use specific analyzing tools (Ishikawa diagram, flowchart or other

types of specialized diagram systems) or other standardized analysis systems, such as SWOT analysis (Strengths, Weaknesses, Opportunities, Threats).

3. **Analyze the risk**: After identification, it is important to proceed to risks analysis that have been detected (Technical, external, organizational, management, etc.). Their influence on the project (mild, moderate or severe impact on the project), or the probability of the risk arising (low, intermediate or high probability). The aim of risk analysis is to gain an understanding of the nature of each risk, including the magnitude of its consequences and the likelihood of those consequences, and therefore to derive the level of risk.
4. **Evaluate the risk**: Risk evaluation uses the information generated by risk identification and risk analysis to make decisions about whether each risk falls within an organization's risk criteria and whether it requires treatment. Normally organizations specify the actions required by managers for risks at each level of risk and the time allowed for their completion. They also specify which levels of management will be permitted to accept the continued exposure and tolerance of certain levels of risk.
5. **Treat the Risk**: This is also referred to as Risk Response Planning. During this step you assess your highest ranked risks and set out a plan to treat or modify these risks to achieve acceptable risk levels. How can you minimize the probability of the negative risks as well as enhancing the opportunities? You create risk mitigation strategies, preventive plans and contingency plans in this step.
6. **Monitor and Review the risk**: This is the step where you take your Project Risk Register and use it to monitor, track and review risks. A company should define monitoring Infrastructure by developing control procedures that monitor and review business critical processes, the company should also have audit procedures in place to determine if those risk related control procedures are working effectively and should periodically perform audits on the control procedures to determine or the risk monitoring process are working effectively and as expected, if necessary make adjustments or improvements to improve risk monitoring processes.

Ignoring risks associated with business or other activities might not pay off. Risks may negatively affect the following areas: financial situation; reputation, credibility and status; customer and public confidence in a particular organization; health and safety of employees, customers; facilities, equipment and environment. All possible risks must be taken into account in each part of the business. Each area of activity is unique and the risks it entails are also specific. Effective risk management does not mean that all risks are avoided: however, we can significantly mitigate the risks and their consequences.

4 Blockchain

A blockchain is a decentralized, distributed database that is used to maintain a continuously growing list of records, called blocks. Each block contains a timestamp and a link to a previous block. By design and by purpose blockchains are inherently resistant to modification of the data. Functionally, a blockchain can serve as "an open, distributed ledger that can record transactions between two parties efficiently and in a variable and permanent way." [18, 19]. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made.

Blocks are made public to all the network after being linked to one another using "hashes" which take an input string of any length and convert it into a fixed-length string. Hashing is generating a value or values from a string of text using a mathematical function and is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering.

4.1 Mathematical Foundations of Blockchain

The fundamental part of Blockchain are cryptographic algorithms. In particular, the ECDSA algorithm is an Elliptic Curve Digital Signature Algorithm, which uses elliptic curves and finite fields to sign data so that a third party can confirm the authenticity of the signature by eliminating the possibility of falsification. ECDSA uses different procedures for signing and verification, consisting of several arithmetic operations. The signing algorithm makes use of the private key, and the verification process makes use of the public key.

Elliptic Curve Cryptography (ECC) is a method of public-key encryption based on the algebraic function and structure of a curve over a finite graph. It uses a trapdoor function predicated on the infeasibility of determining the discrete logarithm of a random elliptic curve element that has a publicly known base point.

Basic principle: you have a mathematical equation which draws a curve on a graph, and you choose a random point on that curve and consider that your point of origin. Then you generate a random number, this is your private key, you do some magical mathematical equation using that random number and that “point of origin” and you get a second point on the curve, that’s your public key. When you want to sign a file, you will use this private key (the random number) with a hash of the file (a unique number to represent the file) into a magical equation and that will give you your signature. The signature itself is divided into two parts, called **R** and **S**. In order to verify that the signature is correct, you only need the public key (that point on the curve that was generated using the private key) and you put that into another magical equation with one part of the signature (**S**), and if it was signed correctly using the the private key, it will give you the other part of the signature (**R**). So to make it short, a signature consists of two numbers, **R** and **S**, and you use a private key to generate **R** and **S**, and if a mathematical equation using the public key and S gives you R, then the signature is valid. There is no way to know the private key or to create a signature using only the public key.

ECDSA uses only integer mathematics, there are no floating points (this means possible values are 1, 2, 3, etc. but not 1.5.), also, the range of the numbers is bound by how many bits are used in the signature (more bits means higher numbers, means more security as it becomes harder to ‘guess’ the critical numbers used in the equation), as you should know, computers use ‘bits’ to represent data, a bit is a ‘digit’ in binary notation (0 and 1) and 8 bits represent one byte. Every time you add one bit, the maximum number that can be represented doubles, with 4 bits you can represent values 0 to 15 (for a total of 16 possible values), with 5 bits, you can represent 32 values, with 6 bits, you can represent 64 values, etc. one byte (8 bits) can represent 256 values, and 32 bits can represent 4294967296 values (4 Giga). Usually ECDSA will use 160 bits total, so that makes well, a very huge number with 49 digits in it. ECDSA is used with a SHA1 cryptographic hash of the message to sign (the file). A hash is simply another mathematical equation that you apply on every byte of data which will give you a number that is unique to your data. Like for example, the sum of the values of all bytes may be considered a very dumb hash function. So if anything changes in the message (the file) then the hash will be completely different. In the case of the SHA1 hash algorithm, it will always be 20 bytes (160 bits). It’s very useful to validate that a file has not been modified or corrupted, you get the 20 bytes hash for a file of any size, and you can easily recalculate that hash to make sure it matches. What ECDSA signs is actually that hash, so if the data changes, the hash changes, and the signature isn’t valid anymore.

The elliptic curve needs to consist of points that satisfy the equation:

$$y^2 = ax^3 + b$$

(x,y) on the curve represent a point, while both a and b are constants.

More details about mathematical description of Elliptic curve cryptography is given, for example, by Hans Knutson [20] or Eric Rykwalder [21].

4.2 Cryptographic hash functions

A cryptographic hash function is a special class of hash functions that has various properties making it ideal for cryptography. There are certain properties that a cryptographic hash function needs to have in order to be considered secure:

- Deterministic – meaning that the same message always results in the same hash.
- Quick Computation - The hash function should be capable of returning the hash of an input quickly. If the process isn’t fast enough then the system, simply won’t be efficient. Computationally hash functions are much faster than a symmetric encryption.
- Pre-Image Resistance - Given a hash value h it should be difficult to find any message m such that h = hash(m). This property means that it should be computationally hard to reverse a hash function. This property protects against an attacker who only has a hash value and is trying to find the input.
- Second pre-image resistance - Given an input m_1, it should be difficult to find a different input m_2 such that hash(m_1) = hash(m_2). This property is sometimes referred to as weak collision resistance. Functions that lack this property are vulnerable to second-preimage attacks.
- The Avalanche Effect - Even if you make a small change in your input, the changes that will be reflected in the hash will be huge.
- Collision resistance - It should be difficult to find two different messages m_1 and m_2 such that hash(m_1) = hash(m_2). Such a pair is called a cryptographic hash collision. This property is sometimes referred to as strong collision resistance. It requires a hash value at least twice as long as that required for pre-image

resistance; otherwise collisions may be found by a birthday attack [22].

Informally, these properties mean that a malicious adversary cannot replace or modify the input data without changing its digest. Thus, if two strings have the same digest, one can be very confident that they are identical. Second pre-image resistance prevents an attacker from crafting a document with the same hash as a document the attacker cannot control. Collision resistance prevents an attacker from creating two distinct documents with the same hash.

4.3 Consensus Algorithms in Blockchain

Consensus algorithms are of the highest relevance to blockchain technology since the purpose of Bitcoin was to transfer value in an unregulated, distrusting environment, where a sure way of validating transactions was needed. The goal of the consensus algorithm is to ensure a single history of transactions exists and that that history does not contain invalid or contradictory transactions. For example, that no account is attempting to spend more than the account contains, or to spend the same token twice, so-called double-spending.

We know that Blockchain is a distributed decentralized network that provides immutability, privacy, security, and transparency. There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely secured and verified. This is possible only because of the presence of the consensus protocol which is a core part of any Blockchain network.

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment. Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

Bitcoin solved the consensus problem by, for each new block announcing a target, which the hash of the previous block, the current block and a variable nonce has to equal less than. Since the output of the hashing function is evenly distributed, it's impossible to create a block such that it with certainty will be easy to reach the target. Therefore, there is a race between the mining computers in the network to find the right nonce. Once a target is reached, the mining computer broadcasts that block to the network and other participants validate the transactions. If enough validating nodes find the transactions to add up, they agree upon that block being added to the chain. This procedure is called proof-of-work (PoW). Since the goal is, not to give too much power to a single person or organization, a limited resource has to be chosen which will be spent upon voting for the validity of a block. In PoW, that resource is computing power.

Proof of Stake (PoS) is the most common alternative to PoW. In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, validators invest in the coins of the system by locking up some of their coins as stake. After that, all the validators will start validating the blocks. Validators will validate blocks by placing a bet on it if they discover a block which they think can be added to the chain. Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets and their stake increase accordingly. In the end, a validator is chosen to generate a new block based on their economic stake in the network. Thus, PoS encourages validators through an incentive mechanism to reach to an agreement.

There are a number of other algorithms such as: Proof of Burn (PoB), Proof of Capacity, Proof of Elapsed Time (PoET), Proof of Activity, Proof of Weight, Proof of Importance, Leased Proof of Stake, etc.

Implementation into logistic model of AutoID processing

Many information systems (ERP and other categories) are nowadays extended for providing better/extended data security as a prevention for information risks. For the purposes of presentation and modelling AutoID processes College of Logistics uses its laboratory model of data gathering information with basic information system. Basic structure of the physical model is presented at Figure 2a, example of data structures used is at Figure 2b.

The model is rail yard in H0 scale. It represents very simple configuration with two parallel rail ovals. There are two simple stations for simulation of loading and unloading. Data read from the train model are processed in a connected information system (EPCIS). RFID readers with antennas are placed in specified locations of the rail yard model together with magnetic readers, together they monitor the movement of the trainset. Models of wagons are made of plastic. This is difference from real metal wagons. This is limitation for modelling of radiofrequency readings.

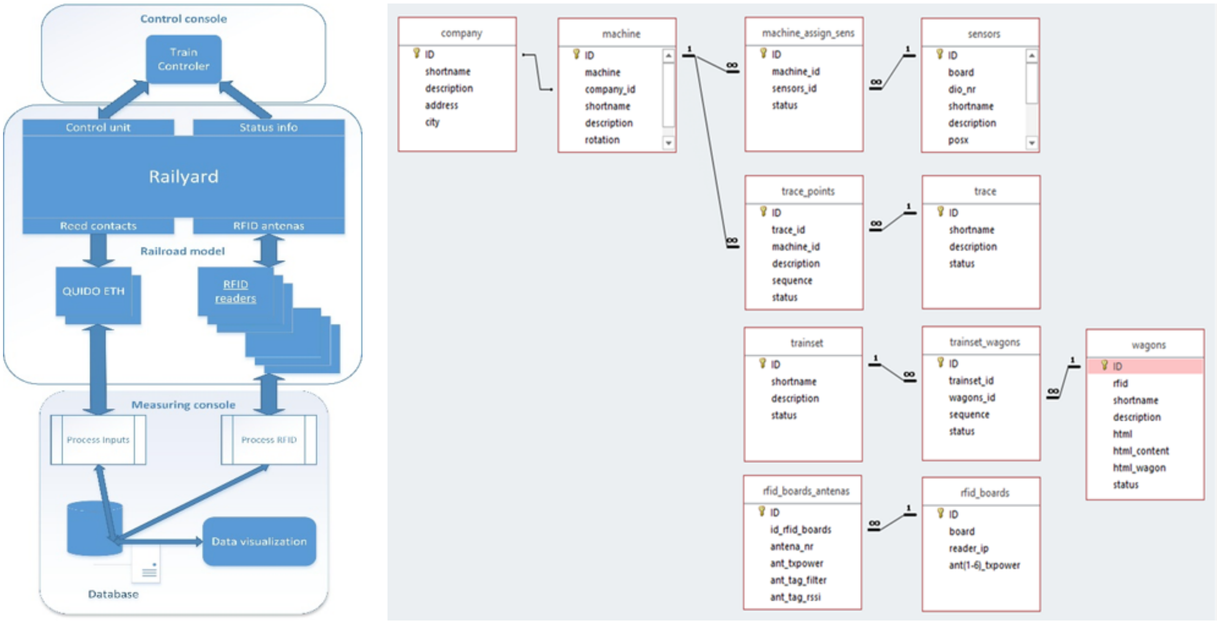

Figure 2: a: block structure of physical model; b: part of data structures (tables with relations)

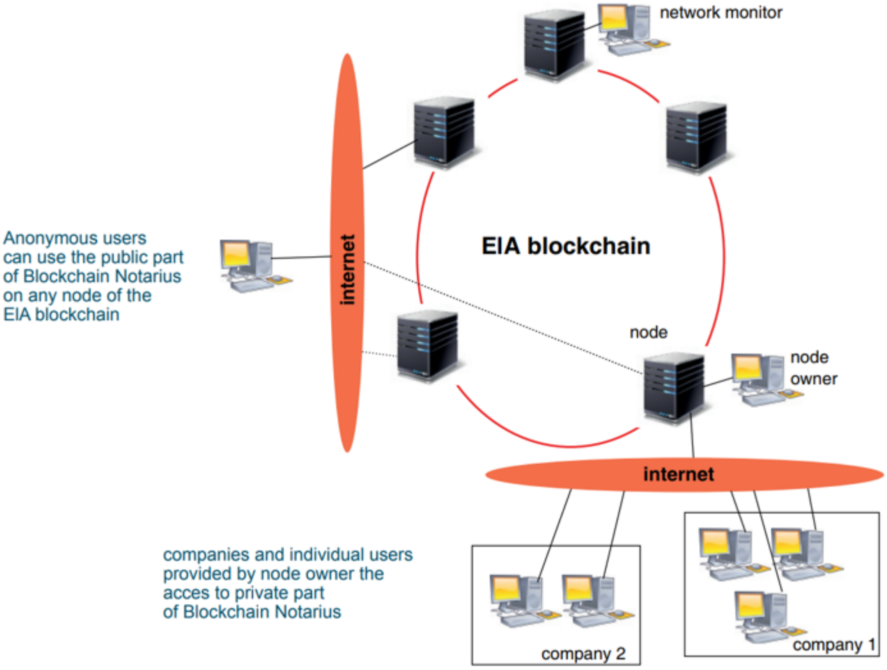
network monitor
EIA blockchain
internet
Anonymous users can use the public part of Blockchain Notarius on any node of the EIA blockchain
node
node owner
internet
companies and individual users provided by node owner the acces to private part of Blockchain Notarius
company 2
company 1

Figure 3: Blockchain Notarius structure[3]

Real metal environment requires special tags to eliminate lower readability [23].

Blockchain technology is used to secure data describing particular steps of defined logistics processes. Selected event records are used for hashes generation and theses hashes are sent to one of blockchain nodes in EAI Notarius structure. The Blockchain Notarius application provides service of registration of data files on the blockchain, and the service of verification of whether a submitted copy of a file is identical to the registered original. See Figure 3.

[3] Source: http://www.electroindustry.cz/fs/97be04be-ee93-11e9-aac5-00155d092b8f-blockchain-brochure-eng.pdf

5 Conclusion

The Logistics 4.0 concept brings a number of advanced technologies (IoT, Big Data, cloud computing, 3D printing or Blockchain) and with them several key benefits for the future of the supply chain, such as E2E visibility - producing and making available the sort of high-quality, mission critical data upon which efficient transport operations depend, real-time and integrated planning a monitoring. Regarding the supply chain, the digital transformation and the use of intelligent and cooperative systems will make the supply chain smarter, more transparent and more efficient in every stage. There will be a particular focus in new models which will be more closely to individual customer needs, promoting a significantly increase of the decision-making quality and become more and more flexible and efficient in the near future.

Unfortunately, implementation of new technology brings not only benefits but also potential risks. Poor implementation means for companies' large economic risk, especially with regard to high initial investment. It is necessary to think carefully what technologies are suitable for the company and determine the right time to implementation them. It is also necessary to identify any technical, social, ecological or legal risks. All these risks do not act separately but are closely related and overlapping. To avoid risks due to poor implementation and the related threats to the company, it is necessary to use risk management.

Participation in EAI blockchain allow College of Logistics to present up to date attempt do data security. Our students can get familiar with processes for safe information processing and academic staff has very good resource for modelling, experimenting and simulation in processing and securing of logistic data in information systems.

References

[1] Kagermann H, Walster W, Helbig J. Recommendations for Implementing the Strategic Initiative Industrie 4.0 [Internet]. Communication Promoters Group of the Industry - Science Research; 2013 Apr [cited 2019Sep7]. Available from: https://www.din.de/blob/76902/e8cac883f42bf28536e7e8165993f1fd/recommendations-for-implementing-industry-4-0-data.pdf

[2] Jazdi N. Cyber physical systems in the context of Industry 4.0. In: 2014 IEEE International Conference on Automation, Quality and Testing, Robotics. Cluj-Napoca: IEEE / Institute of Electrical and Electronics Engineers Incorporated; 2014.

[3] Lee I, Lee K. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons. 2015;58(4):431–440.

[4] Risk management — Vocabulary [Internet]. ISO/Guide 73:2009. ISO/Guide 73:2009; [cited 2019Aug6]. Available from: https://www.iso.org/obp/ui/

[5] Heckmann I, Comes T, Nickel S. A critical review on supply chain risk — Definition, measure and modeling. Omega. 2015Apr; 52:119–32.

[6] Whitmore A, Agarwai A, Xu LD. Information Systems Frontiers. Information Systems Frontiers [Internet]. 2014Apr [cited 2019Aug6];17(2):261–74. Available from: https://www.researchgate.net/publication/271921561_The_Internet_of_Things-A_survey_of_topics_and_trends

[7] Whitmore AD, Agarwai AD, Xu LD. The Internet of Things — A survey of topics and trends. Information Systems Frontiers [Internet]. 2014Apr [cited 2019Aug6];17(2):261–74. Available from: https://www.researchgate.net/publication/271921561_The_Internet_of_Things-A_survey_of_topics_and_trends

[8] Hölbl M. Cloud Computing Security and Privacy Issues [Internet]. Council of European Professional Informatics Societies. Council of European Professional Informatics Societies; 2011 [cited 2019Sep6]. Available from: https://www.cepis.org/media/CEPIS_Cloud_Computing_Security_v17.11.pdf

[9] Heuser LC, Nochta ZC, Trunk NC. ICT shaping the world: A scientific view. Chichester: John Wiley & Sons; 2009.

[10] Beier G, Niehoff S, Ziems T, Xue B. Sustainability aspects of a digitalized industry – A comparative study from China and Germany. International Journal of Precision Engineering and Manufacturing-Green Technology [Internet]. [cited 2019Aug8];4(2):227–34. Available from: https://link.springer.com/article/10.1007/s40684-017-0028-8

[11] Gajbhiye A, Shrivastava KMPD. Cloud computing: Need, enabling technology, architecture, advantages and challenges. In: 2014 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence) [Internet]. Noida: IEEE; 2014 [cited 2019Aug9]. Available from: https://ieeexplore.ieee.org/document/6949224 DOI 10.1109/CONFLUENCE.2014.6949224

[12] Sarkis J, Zhu Q. Environmental sustainability and production: taking the road less travelled. International Journal of Production Research [Internet]. 2017Aug21 [cited 2019Aug11];56(1-2):743–59. Available from: https://www.tandfonline.com/doi/full/10.1080/00207543.2017.1365182

[13] Yin, R.K. Case Study Research: Design and Methods; Sage: Thousand Oaks, CA, USA, 2009

[14] Franco M, Almeida J. Organisational learning and leadership styles in healthcare organisations: An exploratory case study. Leadership & Organization Development Journal [Internet]. 2011Nov [cited 2019Sep12];32(8):782–806. Available from: https://www.researchgate.net/publication/235320808_Organisational_learning_and_leadership_styles_in_healthcare_organisations_An_exploratory_case_study

[15] Berg HP. Risk management: Procedures, methods and experiences. Reliability and Risk Analysis: Theory and Applications [Internet]. 2010Jul [cited 2019Aug17];1. Available from: https://www.researchgate.net/publication/228393958_Risk_management_Procedures_methods_and_experiences

[16] Dickson G. Principles of Risk Management. Glasgow Caledonian University; 1995.

[17] Wiengarten F, Humphreys P, Gimenez C, McIvor R. Risk, risk management practices, and the success of supply chain integration. International Journal of Production Economics [Internet].

2016Jan [cited 2019Aug17];171(3):361–70. Available from: https://www.sciencedirect.com/journal/international-journal-of-production-economics

[18] Narayanan A, Bonneau J, Felten E, Miller A, Goldfeder S. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press; 2016.

[19] Lakhani MIKR. The Truth About Blockchain [Internet]. Harvard Business Review. 2019 [cited 2019Sep6]. Available from: https://hbr.org/2017/01/the-truth-about-blockchain

[20] Knutson H. What is the math behind elliptic curve cryptography? [Internet]. Hackernoon; 2018 [cited 2019Aug16]. Available from: https://hackernoon.com/what-is-the-math-behind-elliptic-curve-cryptography-f61b25253da3

[21] Rykwalder E. The Math Behind Bitcoin [Internet]. CoinDesk. CoinDesk; 2014 [cited 2019Sep9]. Available from: https://www.coindesk.com/math-behind-bitcoin

[22] Katz J, Lindell Y. Introduction to modern cryptography. Boca Raton: CRC Press Taylor & Francis; 2015.

[23] Kodym O, Kavka L, Sedláček M. Logistic Chain Data Processing. Albena: STEP92; 2015 [cited 2019Aug11]. Available from: https://www.sgem.org/sgemlib/spip.php?article5610&lang=en

[24] EIA blockchain is the blockchain for your business [Internet]. EIA Blockchain Services; 2019 [cited 2019Oct1]. Available from: http://www.electroindustry.cz/fs/97be04be-ee93-11e9-aac5-00155d092b8f-blockchain-brochure-eng.pdf