Автономная некоммерческая образовательная организация высшего образования
«Сколковский институт науки и технологий»

На правах рукописи

Мадвал Яш

ИССЛЕДОВАНИЕ ТОКЕНИЗИРОВАННЫХ ЦЕПОЧЕК ПОСТАВОК ПОСРЕДСТВОМ БЛОКЧЕЙНА

Специальность: 1.2.3. Теоретическая информатика, кибернетика

АВТОРЕФЕРАТ

диссертации на соискание учёной степени кандидата технических наук

Москва— 2024

Работа выполнена в центре вычислительной техники, науки о данных и инженерии технологий Автономной некоммерческой образовательной организаций высшего образования «Сколковский институт науки и технологий».

Научный руководитель: **Кабатянский Григорий Анатольевич**, **доктор физико-математических наук**

Научный консультант: **Янович Юрий Александрович**, **кандидат физико-математических наук**

Защита состоится **25 июня 2024 года в 15 часов 00 минут** на заседании диссертационного совета **1.2.3.1.**, созданного на базе Автономной некоммерческой образовательной организации высшего образования «Сколковский институт науки и технологий» (Сколтех)

по адресу: Территория Инновационного Центра «Сколково», Большой бульвар д.30, стр.1, Москва 121205

С диссертацией можно ознакомиться в библиотеке Сколтеха и на сайте организации https://dissovet.skoltech.ru/

Автореферат разослан «____»_____ 2024 года.

Ученый секретарь
диссертационного совета
кандидат физико-математических наук Копелевич Григорий Александрович

Autonomous Non-Profit Organization for Higher Education
"Skolkovo Institute of Science and Technology"

As a manuscript

Madhwal Yash

RESEARCH ON TOKENIZED SUPPLY CHAIN VIA BLOCKCHAIN

Speciality: 1.2.3. Theoretical Informatics, Cybernetics

DISSERTATION ABSTRACT

of the dissertation for the Degree of Doctor of Philosophy in Engineering

Moscow— 2024

The work has been performed at Computational and Data Science and Engineering Department of Skolkovo Institute of Science and Technology.

Scientific supervisor: **Kabatyansky Grigory Anatolyevich**
Doctor of Physical and Mathematical Sciences
Scientific consultant: **Yanovich Yury Aleksandrovich**
Candidate of Physical and Mathematical Sciences

The defense will take place on **June 25, 2024 at 15:00** at the meeting of the Dissertation Council **1.2.3.1**, based at the Autonomous non-profit educational organization of higher education "Skolkovo Institute of Science and Technology" (Skoltech)

address: Skolkovo Institute of Science and Technology, the territory of the Innovation Center "Skolkovo", Bolshoy Boulevard, 30, bld.1, Moscow 121205, Russia

The text of the dissertation is available at the Skoltech library or on the website https://dissovet.skoltech.ru/

Dissertation abstract is sent on «____»_____ 2024.

Academic Secretary of the Dissertation Council
Candidate of Physical and Mathematical Sciences — Kopelevich Grigory Alexandrovich

General characteristics of the work

The primary objective of this dissertation is to determine how the concept of blockchain technology can be implied in supply chain management (SCM). During the research phase, weemphasized how the intermediaries' agreement can provide the transaction details among two segments in an supply chain (SC). Segments of SC lack information flow among all the components. This lack of information sharing leads to a communication gap, and thus, due to this loophole, many corrupt practices can occur, like money laundering, product replacements, etc. This information transformation among the SC components can exist between two elements or across all. We described numerous possibilities, such as a decentralized application (DApp), a possible application to track and trace products, which the following segment of the SC will procure. This procurement process will be recorded in the blockchain chronologically. Although a solution exists for tracking and tracing items in SC, we proposed ways in which two or more things can be tokenized and converted to a new product and record a new token generation on the blockchain.

The **goal** dissertation aims to address key challenges and innovate within the intersection of blockchain technology and supply chain management. The dissertation seeks to develop and implement blockchain protocols to prevent counterfeiting across multi-tier production processes within supply chain projects. Furthermore, it aims to design and deploy robust supply chain protocols with automated dispute resolution mechanisms to enhance transparency and reliability. Additionally, the dissertation endeavors to tackle critical issues in blockchain usage within supply chains, such as improving readability by edge devices, implementing Distributed Denial-of-Service (DDoS) protection mechanisms, and enhancing usability for stakeholders. The dissertation aims to advance supply chain operations' efficiency, security, and trustworthiness through these goals, ultimately contributing to blockchain technology's broader adoption and integration in supply chain management practices.

To achieve this goal, it was necessary to solve the following **tasks**

1. Research and design blockchain protocols to prevent counterfeiting in supply chain projects, from manufacturing to final ownership via multi-tier production.
2. Designing and implementing a robust and auditable supply chain protocol with automated dispute resolution mechanisms.
3. Research and design solutions for blockchain usage problems, namely:
    (a) Readability by edge devices of blockchain's data on products,
    (b) DDoS protection in blockchains without a transaction fee,
    (c) Proof of the correctness of response for templated requests

   in the supply chain and provide solutions.

The **propositions for the defense** are the following:

1. Designed and developed the token-driven protocol for asset tokenization and token conversion in blockchain-based supply chains, leading to auditable, transparent, and reliable communication accessibility.

2. Designed and developed the smart contract protocol for secure data transfer in supply chain management, which supports proof of delivery and performance measurement processes.
3. Designed blockchain integration in relational and graph databases to enable verifiable request responses.
4. Designed fractional reservation-based DDoS protection for blockchains.
5. Optimized format of edge device-readable supply chain transactions.

The following are the **scientific novelty** of the work:

1. Token-driven workflows for the blockchain-based supply chain are provided. Methods to objectify and tokenize things to transform them into new tokens are described. Furthermore, we designed a token-driven workflow for a blockchain-based supply chain. This workflow allows asset tokenization and token conversion, which provides auditable, transparent, reliable communication Accessibility.
2. Secure Data Transfer or supply-driven smart contracts is considered and designed to solve supply chain problems, namely, secure data transfer in distributed energy grids and long-term proof-of-delivery PoD smart contracts for performance measurement for Ponti. We designed applications for applied projects and developed prototypes, e.g., a blockchain system for Russian postage stamps and plastic pipes for the Polyplastic Group. We also designed and implemented several scientific prototypes, like tracking manufacturing items for respirators and medical certificates. The information on the blockchain of prototypes is reliable and verifiable.
3. The Research formulated three problem areas in blockchain usage for supply chains and provided a corresponding solution, namely:
    (a) Auditability: Introduction of blockchain to a traditional database system. We provided two solutions for introducing a blockchain to conventional methods:
        i. Exonum Neo4j graph database
        ii. Data storage on the top of a relational database.
    (b) Availability: Blockchain without transaction fees are prone to DDoS attacks. We provided fractional reservation-based DDoS protection in formulating a method to prevent DDoS attacks in a blockchain environment with high throughput.
    (c) Usability: Interacting with the blockchain via edge devices is difficult. We researched, implemented, and provided ease-of-use interaction via edge devices for the machine-readable label for production that describes the amount of information that can be stored and easily read on curved surfaces with different radii.

The dissertation contributes significant **scientific and practical significance** to the intersection of blockchain technology and supply chain management. By addressing critical challenges in the field, such as counterfeiting prevention and transparency enhancement, the

dissertation provides valuable insights into applying blockchain protocols across multi-tier production processes within supply chains. Moreover, designing and deploying robust supply chain protocols with automated dispute resolution mechanisms offer practical solutions to enhance reliability and transparency in real-world supply chain operations. The dissertation also tackles critical blockchain usage issues, including the readability of edge devices and DDoS protection mechanisms, thereby advancing supply chain practices' efficiency, security, and trustworthiness. Theoretical contributions include the development of novel token-driven workflows and secure data transfer mechanisms, while practical solutions for blockchain usability challenges demonstrate the dissertation's immediate applicability in industrial settings. The comprehensive approach and innovative outcomes underscore its theoretical significance and practical relevance, positioning it as a valuable contribution to academia and industry in blockchain-enabled supply chain management.

The **validity and reliability of the results and conclusions** are ensured using diverse blockchain and tokenization analyses, along with their alignment with existing literature. Different methods were conducted to ascertain the replicability of tokenization procedures in blockchain systems, thus preventing counterfeiting, improving transparency, and resolving disputes automatically in multi-tier production processes. Addressing practical challenges like readability by edge devices and DDoS protection, the dissertation aims to increase efficiency, security, and trust in supply chain operations. Developing reliable blockchain protocols and solutions contributes to blockchain technology's broader adoption and integration in real-world supply chain practices. Furthermore, the formulations and insights articulated within the research have been evaluated rigorously at international conferences dedicated to blockchain and applications. Moreover, the validation of the findings is reinforced through their publication in peer-reviewed journals within the blockchain and distributed ledger technology domain, further supporting their credibility and significance within the academic and professional communities.

Approbation of the work and publications

The main results on the dissertation topic are presented in 12 printed publications, all indexed in Scopus or Web of Science, including two papers in Q1 Journals and one in the Rank A conference proceedings. The materials of the works were presented at the following conferences in the form of oral and poster presentations: IEEE International Conference on Blockchain and Cryptocurrency 2019 (Seoul, Korea), 2nd International Conference on Blockchain Technology and Applications (Xian, China), 2020 IEEE International Conference on Blockchain and Cryptocurrency (virtual), 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (virtual), 4th International Conference on Computers in Management and Business (virtual), 2021 3rd Blockchain and Internet of Things Conference (virtual), 2021 4th International Conference on Blockchain Technology and Applications (virtual).

The **author's contribution** includes setting goals, planning experimental activities, and systematically analyzing literature data. The author's programming expertise has significantly advanced blockchain applications in supply chain management. The author has

addressed critical challenges such as counterfeiting prevention and transparency enhancement through innovative solutions, designed and developed blockchain-based applications for supply chain protocols, and tackled usability issues, such as readability and DDoS protection; the author's contributions have improved efficiency and security within supply chains. The author participated in preparing and presenting oral and poster presentations at scientific conferences and writing articles for international peer-reviewed scientific journals. The work was done at the Computational and Data Science and Engineering Department of the Skolkovo Institute of Science and Technology.

The content of the work

The **abstract** provides a brief description of the whole dissertation.

The chapter **"Introduction"** covers the relevance of the work, the goal, and objectives, presents the objects of research, scientific novelty, the practical significance of the work, key results, approbation of the results, and personal contribution of the author.

In the 1st chapter **"Background blockchain bases supply chain"**, we describe what blockchain technology is, how it works, its architecture, and its types. Additionally, we discuss the challenges in the supply chain and how it can be integrated with blockchain.

Protecting legitimate supply chains from counterfeiting has become a significant challenge. In 1998, the OECD's report on the Economic Impact of Counterfeiting [1] showed that the same manufacturer often made counterfeit products contracted to produce authentic products. The counterfeiting strategies are increasingly sophisticated as, in many cases, counterfeiters apply the same technologies and use the same suppliers as legitimate brands [2]. Thus, a variety of counterfeiting strategies has emerged and affected the legitimate supply chain, such as genuine parts or products being stolen from the honest supply chain (e.g., disposed-of genuine products are recovered), factory overruns, or near copies being illegally produced by sub-contractors, counterfeit products, and genuine products are bundled and distributed together.

Over the past years, many industrial sectors have reported infiltrating counterfeit products into their supply chains. For instance, the aviation sector has expressed strong concerns about detecting counterfeit aircraft parts in the legitimate supply chain. Such detections have been reported in the US and Europe's civil and military aircraft supply chains.

Several factors contribute to this phenomenon. Global supply chains constitute a complex and extensive network of actors involved in production and distribution processes. In such circumstances, many companies find it challenging to map and monitor their suppliers and sub-suppliers beyond the second tier of their supply chains. This limited visibility results in lower control over the supply chain and increased exposure to risks such as counterfeiting. In some cases, these vulnerabilities allow illicit networks to penetrate legitimate supply chains and exploit the services provided by supply chain intermediaries.

Therefore, it becomes urgent to take the necessary measures, such as smart supply chain management (SCM) techniques, to protect better legitimate supply chains from counterfeiting threats, including enhancing cooperation between supply chain actors, improving information exchange and security, and actively promoting transparency and best practices in SCM.

Figure 1 below shows a small representation of how the full development of blockchain technology can be implemented across the different components of the chain—this overview of how the technology can work in a real-time scenario. We have taken a simple case of an automobile manufacturing assembly line.

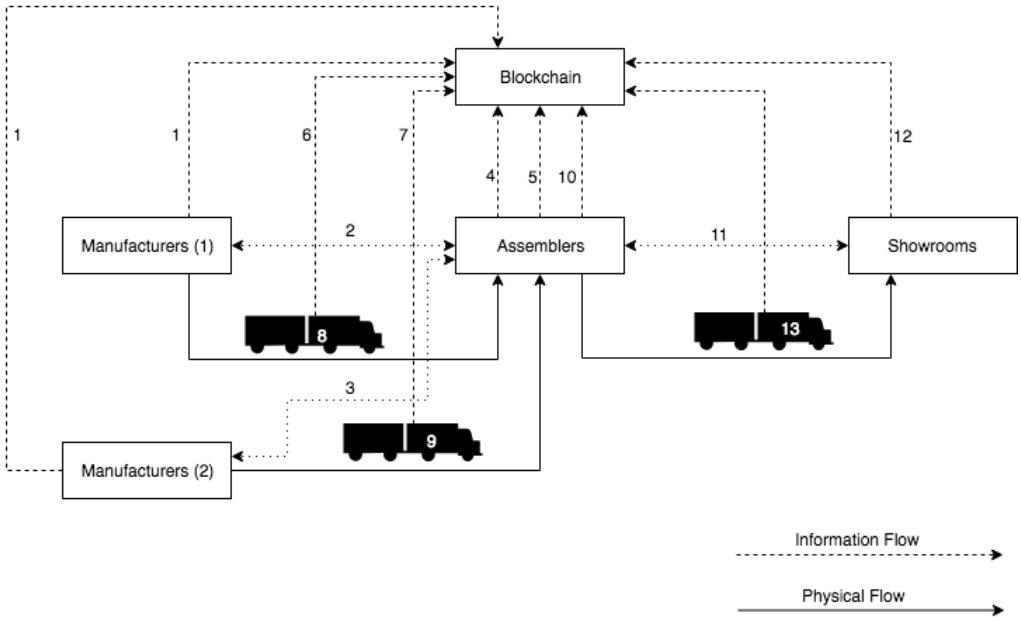


Figure 1 — Blockchain Development on Supply Chain

Manufacturers (1) produce an engine of the car, put it on sale, and notify the chain members. The product information comprises details like buyer, seller, and description that will consist of details. In Parallel, another *Manufacturers (2)* produces the car's structure and notifies its sale to the entities in the chain. Note that leveraging blockchain's potentiality allows us to control the access to who can purchase. The assembler will communicate with the manufacturers to procure the products from the *Manufacturers (1)* and *Manufacturers (2)* respectively, and purchase them. This purchasing transaction is recorded and committed to the blockchain (4 and 5). The shipment starts from *Manufacturers (1)*. It will be notified on the chain with all details of package number, truck number, etc. This will ensure that the end product received at the assembly hub is the same as that from the manufacturing hub.

Once the product is assembled and ready, it is notified to the next buyers, in this case, the showroom. The showroom's product buying follows the same process as the preceding entities. Every step in this process records all the movements and activities in the blockchain.

In the wider and huger aspects, the basic complexity of the supply chain can be seen as shown above. In this complex scenario, many complications occur when dealing with the product. In this chain, it isn't easy to monitor the quality and track the individuality of the

components in the whole supply chain. If in a wider aspect, i.e., in the scenario of the web of the supply chain, instead of monitoring segment-wise, it will be more useful if we implement individual smart contracts among the individual components of the chain instead of individual layers, as we see that with each component among the individual layer, it will have separate conditions and requirements that it should be met when a product from predecessor layer moves to next layer.

In the 2nd chapter **"Blockchain solution for Tokenized SCM"**, we described Blockchain for Tokenised Supply Chain Management and how a physical product could be digitally tokenized and represented on the blockchain. This chapter focuses on the following features: **Asset Volume Tokenization** and **Token Conversion**.

The blockchain-based supply chain management system for their market is proposed in the section. we highlighted how multiple items to be tokenized on the blockchain can be scalable. An example of postage stamps is because stamp circulation can be transparent and guarantee invariability of the volume produced and used stamps. Counterfeit and unaccounted postage stamps used on mailings cost postal administrations significantly each year. Corporate and individual clients become victims of stamp fraud and incur losses when security teams investigate such mailings. Blockchain technology is supposed to be a solution to make the postage stamps market transparent and to guarantee the invariability of stamp volume produced and used.

The blockchain-based supply chain for postage stamps can be considered similar to tokenizing multiple identical postage stamps with the same value. It was shown that postal stamp circulation could be considered SCM [3], and illegal changes in it cause considerable financial damage to the states and companies [4–6]. The solution considers the Russian Post as a reference organization, but it must be mentioned that the proposed solution can be generalized to other indicia. The post company accepts mailings with the following indicia: meter stamps, postage stamps, and printed postage impressions for envelopes and postcards. Franking machines are primarily used by corporate clients processing mail in bulk. Franking machines with different capacities of imprint indicium (meter stamp) significantly speed up the process of mail processing. Even though an official franking machine is not designed to print indicia with a face value exceeding the advance paid to the company for future delivery services, many fraudulent schemes with postage meters have been revealed. In fraudulent schemes, a franking machine owner can send mail for free by imprinting false and not cash-backed meter stamps.

It is important to note that the company is not the only party losing from counterfeit postage. A sender is also at risk: purchasing counterfeit stamps incurs a loss when mailings are detained and investigated by a postal security team. The drawbacks of stamp circulation mentioned above are typical for many postal administrations. The proposed solution might become a worldwide practice.

Blockchains could be categorized by the level of access to the blockchain data [7; 8], and the proposed solution is organized as a private permissioned blockchain with

linked timestamping. The blockchain for stamp circulation should be private to keep the company's monopoly on the primary market, and it could be permissioned to increase the user's privacy. Timestamping in a private blockchain is the most common way to guarantee history invariableness and protect clients' rights. We implemented the system on an extensible open-source framework for creating blockchain applications called Exonum [9].

To perform experiments, we created an Exonum-based digital cryptocurrency that circulates in the same manner as the real physical stamp in the investigated supply chain model. In more detail, we associate the cryptocurrency entity or crypto token with each physical stamp. As in typical cryptocurrency, each token can be emitted, sold, and retailed. In addition to these operations, each token corresponding to the case can be canceled, and an appropriate physical stamp is used to send mail. The proposed blockchain system keeps a reliable record of the whole circulation of tokens to guarantee that each physical stamp was used only once. Secondary users can trust that the physical stamp is valid. It is a private blockchain system where only validators and auditors have read access to the whole blockchain.

Another aspect of tokenization is an application-based blockchain solution for registering vaccinating authorities and providing relevant vaccine certificates that anyone can verify in no time. Additionally, analysis of data retrieved from the blockchain is provided because the data reading will be happening by thousands of authorities.

A smart contract was deployed on the testnet on a local computer with the Ganache framework that helped our prototype run. After migrating the contract on the blockchain, we called the function *registerHospital()* from that smart contract. We registered four hospitals with the names *Hospital_1*, *Hospital_2*, *Hospital_3*, and *Hospital_4*, respectively, by passing the required parameters and broadcasting to the blockchain network. After registering hospitals, the function *vaccinatePeople()* was called and broadcasted to the network on the registered hospital at random. The parameter Name was generated with the help of the Python library. The time of vaccination was passed as UNIX from provided by the EVM. The system registered vaccination of 1000 people with random names generated by a random registered hospital.

Once the blockchain records the vaccine certificate, by calling the function to view *PublicBook*, we can publicly verify the certificate by passing a valid certificate. Otherwise, an error will be thrown. For verification, 1000 random certificate numbers were generated and verified. *Note: For simplicity, the certificates were generated from 1 to 1000, i.e., for 1000 certificate registration, the certificate number was incremented and registered.*

Figure 2 shows the cumulative distribution function of a single certificate verification time. The request time has mean value $m = 0.024$ seconds and standard deviation $\sigma = 0.005$ seconds. Requests do not need to be written in the blockchain, and they can be executed in parallel on different processes of a single machine and different read-only blockchain copies (nodes). We designed and deployed a decentralized application (DApp) based on the above result.

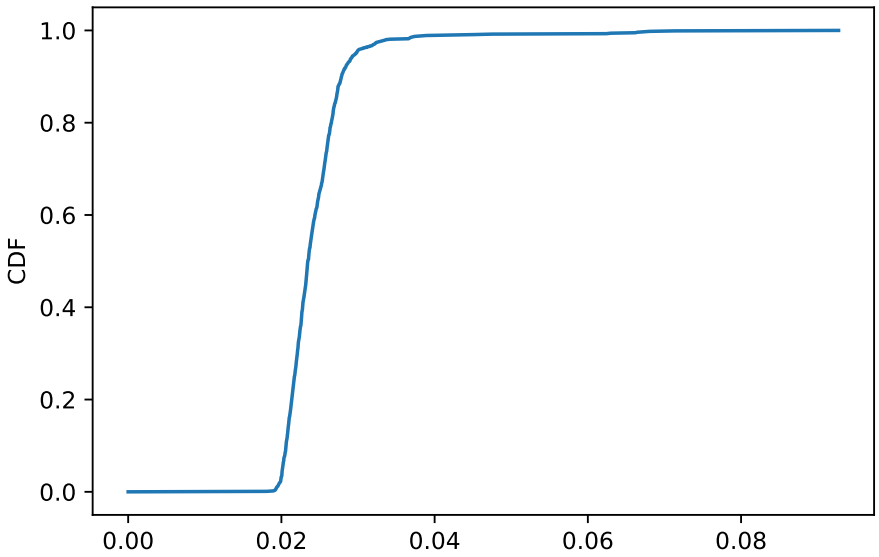
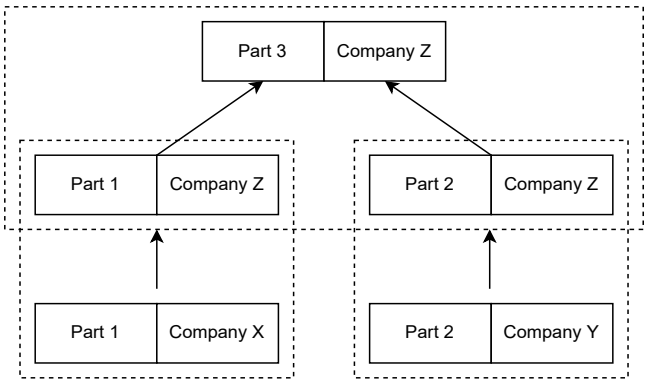


Figure 2 — The cumulative distribution function (CDF) of a single certificate verification time expressed in seconds

A fundamental property of the blockchain is the verification of ownership. Regarding cryptocurrency or digital assets, blockchain technology's ownership verification can verify the authenticity of digital assets, like currency, digital twins, etc. Apart from the data transfer that is stored, the record of the ownership can be stored along with it. Digital certificates, specifically for health cards, should be non-transferable, and fortunately, there exist blockchain frameworks that provide non-transferable functionalities.

The transaction hash is stored in the block of the blockchain. We implement tokenization, where each part is represented as a token. Any intermediary level comprising a multiple tokenized component supplied by the previous levels of the supply chain is generated from a new token value of a specific type. At this level, a newly produced token will have a particular conversion rule and will consist of all details of its producers and origins. Figure 3 (b) represents the tabular representation of Figure 3 (a) Table 3 Produces new token $P3$ in company Z's wallet, which is the input of $Transaction1$ (Tx1) and $Transaction2$ (Tx2).



Tx 1 (Transaction 1)	Company Y - P1 Token	Company Z + P1 Token
Transfer	**Input**	**Output**

Tx 2 (Transaction 2)	Company Y - P2 Token	Company Z + P2 Token
Transfer	**Input**	**Output**

Tx 3 (Transaction 3)	P1 from Company Z's Wallet	P3 Token for Company Z's Wallet
	P2 from Company Z's Wallet	
Transfer	**Input (Addition)**	**Output**

Figure 3 — (a) SCM structure, (b) Log Book

A transparent supply chain network in the aviation industry using a private permissioned blockchain will create trust among all the levels of this supply chain. It will counter the corrupt practices involved and reduce the possibility of replacement of counterfeited products/parts in this chain of supplies. Despite the chance that the purchases are made from the certified seller, introducing Blockchain technology will authenticate that components or subcomponents of aircraft originate from accredited sellers, too, and are not replaced, and the information is not tampered with. This implementation can scope beyond the aviation industry and could be implemented in other automotive or manufacturing industries. Since the supply chain process creates lots of transaction data, the proposed framework can be combined with fractional reservation to prioritize the pending transactions to include in the block and meet real-world demands.

In the 3rd chapter **"Data Processing for Supply Chain Management"**, we described how data could be processed on the blockchain. This chapter focuses on **Secure Data Transfer** and **Supply Chain Driven Smart Contracts**.

We considered the application of renewable energy sources in the power grid, which increases the necessity of tracking the system's state, especially in smart grids with a bidirectional data transfer of power. The section proposes an integration of distributed state estimation with a blockchain-designed communication platform. A detailed analysis of the blockchain-based application in distributed state estimation is described. The numerical analysis shows that the proposed method meets real-world performance requirements and brings high security and reliability to the distributed state estimation process.

Building DSE's data transmission architecture based on BC provides a security feature of the technology to transfer data among system areas. BC integration can ensure honesty in the system as the sender can only sign each transaction. Thus, increasing trust and security to resolve any dispute can arise for an incorrect transaction, which is less likely.

We proposed an algorithm that listens to all the transaction calls of the first deployed smart contract and updates the state of the connections of this smart contract. This algorithm takes four parameters, i.e., sender, receiver, iteration, and payload. Each area in our case study has a different data payload size (i.e., state variables that need to be transferred). With each iteration, data are passed as arrays of float integers as string type because it is impossible to pass a negative number in a smart contract. With each transaction of the iteration, the transaction event is emitted and notified to the receiving area, which can process the data off-chain as per use.

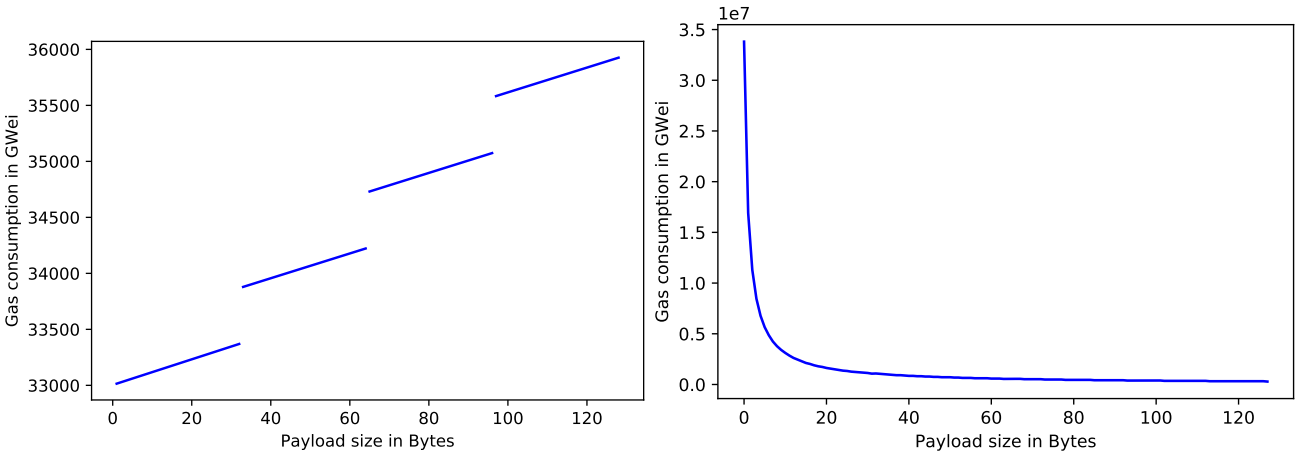


Figure 4 — (a) Gas consumption in Gwei to transfer bytes with payload size, (b) Gas consumption to transfer 1024 bytes per payload size in Bytes

Figure 4 (a) shows the result of the experiment to check the gas consumption, the amount of gas used to execute a transaction, with respect to the transaction payload size in bytes of different values in a transaction, i.e., in a hexadecimal value and used to check how it will influence the processing time. Different value precision results in different payload sizes. We executed 128 transactions of payload size one and bytes of size k from 1 to 128. In EVM, a one-word is a maximum of 32 bytes. Zero bytes pad each payload up to the closest factor of 32 and processed as a sequence of 32 bytes words. Most of the operation consumption goes to cryptographic signature checks by the nodes. Gas consumption varies with different byte sizes, and we can see a significant shift for each consecutive 32 byte, but within each set, the gas fees increased linearly with an increment of a byte.

Figure 4 (b) indicates the optimization of the transfer procedure where several transactions can be concatenated as one string, i.e., bulk data transfer. This would result in fewer transactions to transfer the same amount of data without spending extra gas for each execution. For the experiment, we measured the gas consumption to transfer 1024 bytes per 2^{k-1} bytes where $k \in \{1, \ldots, 8\}$, with an increase in payload size, the gas consumption reduces for computation at nodes.

A contribution to learning about performance measurement and the transaction cost implications while developing and applying smart contracts: an experimental design science approach is applied to develop an open-source blockchain to explore ways to make the delivery processes more efficient, the Proof-of-Delivery (PoD) more reliable, and the performance measurements more accurate. The theory of Transaction Costs is applied to evaluate the cost implications of adopting smart contracts in the management of the PoD. The findings show that smart contracts make the delivery processes more efficient and PoD more reliable. Yet, the methods and metrics are too complex and qualitative, limiting the smart contract's capability to measure performance. The findings indicate potential transaction cost reduction by implementing a blockchain-based performance measurement.

A Buyer submits a pre-contractual agreement to the Seller and confirms the contract upon verification by the Seller of available stock, production capacity, fleet, and delivery capacity. The contract has starting at time T_s and end time T_e. The Seller must deliver order quantities in the range $[Q_m, Q_M]$ during a time interval $[T_s, T_e]$ to the specified warehouse location, with a minimum success rate r. During the term of the contract, the Buyer creates order delivery tasks containing order parameters, estimated time of arrival (ETA), i.e., $t_{eta} > \tau + T_p$, where is the task creation time, T_p is the contract parameter for the minimal allowed gap between task creation and emission of an ETA t_{eta}.

Following Fotouhi et al.'s [10] operational model, the Seller can accept or reject order delivery tasks submitted by the Buyer within a specific time. If accepted, the Seller organizes the order delivery task, and on delivery, the Seller and Buyer create a transaction with the order delivery parameters, the actual delivery time, and whether the goods comply with the quality. If the delivery time is within the range of the eta $[t_{eta} - \Delta t_{eta}, t_{eta} + \Delta t_{eta}]$ and if the order quantity and quality are ok, the delivery is successful. The delivery is successful if both the Seller's and the Buyer's signals are successful. If both signals are unsuccessful, the delivery has failed. However, if they have different views on the quality of the delivery, a dispute is opened.

The empirical success rate $\hat{r}$ is in the interval $[s/Q \cdot 100\%, (s+d)/Q \cdot 100\%]$. $Q = s+f+d$, where s, f, d, and Q correspondingly, the number of successful, failed, disputable, and total deliveries. Only disputable deliveries can change their status over time. Furthermore, the change can be a successful or failed type. So, the interval can only shrink. The Seller can get a bounty payout once $s/(s+f+d) \cdot 100\% \geq r$; Buyer can claim charge penalties if $(s+d)/(s+f+d) \cdot 100\% < r$.

The workflows for the performance contract and single-order delivery tasks are as follows. Single-order quantities are constrained in size by production capacity, availability of supplies for production, and capacity of LSPs performing the physical distribution. Thus, an economic order quantity described by Utama et al. [11] and Combe [12] is negotiated during the pre-contractual agreement. The algorithm of the delivery performance contract is shown in Figure 5.

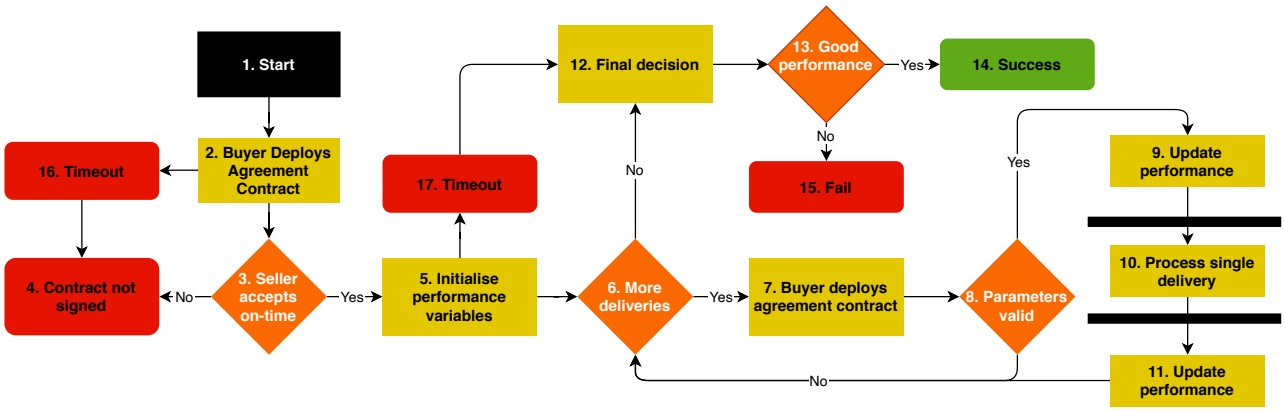


Figure 5 — Proof of delivery flowcharts: Performance contract algorithm

Building upon Sarac et al. [13] and Chen et al. [14], the following algorithm to process a single order delivery controls two main criteria: the deviation from the maximum waiting time for the delivery truck (i.e., Estimated Time of Arrival or delivery time), and the deviations from the quality of the cargo (i.e., order quantity, the origin of the cargo, the destination of the cargo, and condition of the goods and packaging) (Figure 6)

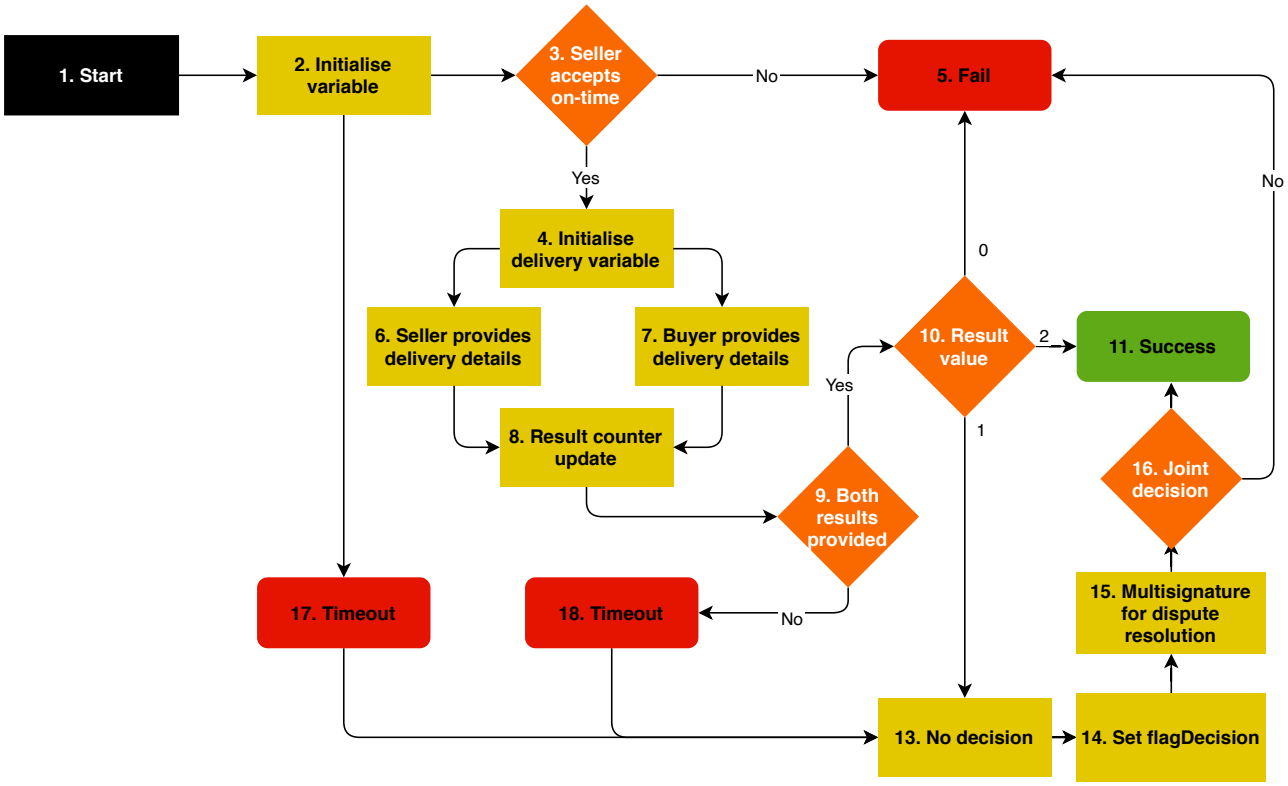


Figure 6 — Proof of delivery flowcharts: Single delivery processing algorithm

In the 4th chapter **"Blockchain extension for Supply Chain"**, we described an environment for blockchain. This chapter focuses on **Auditability**, **Availability**, and **Usability**.

We describe how to combine an Exonum blockchain and a Neo4j graph database into a system that can provide a verifiable audit trail of data integrity and its modifications for information stored in a graph database.

One of the attractive features of blockchain technology is its ability to enable multiple parties with varying levels of trust in one another to collaborate on a shared version of the truth. In this instance, the parties contribute to a single, shared database. By using blockchain, they have assurance against censorship attempts and a tried-and-true consensus mechanism that enables every stakeholder to participate and audit the blockchain. This is especially useful in a professional setting where multiple parties need access and permission to edit information in a database.

A peer-to-peer network with each participant running their copy of a Neo4j graph database has been built. Peers collectively review proposed medications of information stored in the Neo4j, decide on the order of the changes, and then record actual changes in the graph

database–while keeping the history of the modifications in an Exonum blockchain for subsequent auditing in case of a dispute over data quality arises.

In the proof of concept, every modification to data stored in the graph database must be performed via the blockchain. The entire blockchain network must validate the change and reach a consensus on the modification for it to be permanently recorded on the blockchain. The Exonum blockchain itself is never altered before this consensus is reached. Instead, the parties modify their forks to the blockchain and, as consensus is reached, execute them onto the actual Exonum blockchain.

However, as these forks are created, they are communicated to the Neo4j database, and the changes are executed immediately. These changes can only be rolled back before the forks are verified and added to the permanent record of the blockchain. This could lead to a mismatch between what was agreed via consensus on the blockchain and what was recorded in the database. We had to find a better way to synchronize the blockchain records with the Neo4j database information. We investigated two possible solutions: an **apply and rollback** approach and a **two-step** approach.

We describe and evaluate a database extension with blockchain-related structures, leaving consensus beyond the scope. An account-based prototype of cryptocurrency is a model example. The proposed extension allows for checking transaction content and user balance without a full database lookup. Numerical experiments to study the overhead of the proposed extension are provided.

Massive traffic events that impact all the nodes in the distributed system may cause a Denial of Service (DoS). Managing DoS attacks is even harder in peer-to-peer projects because multiple equal rights nodes (miners or maintainers) communicate globally to secure the network.

In most blockchains, users can send transactions. Moreover, as a system's throughput is limited, the ability to send transactions should be limited in some honest and transparent way. Otherwise, the pool of unconfirmed (pending) transactions–mempool–could be overloaded, and it may cause DoS. In Bitcoin, users pay a fee for each transaction to address this issue. Steem.io introduced an alternative approach based on the fractional reservation of the blockchain block space. This approach adapts similar ones from the network routing and banking systems.

The block space fractional reservation for blockchains in terms of a score function is introduced in this section. The authors made a private blockchain project demo on the Exonum framework. The score function influences only mempool processing; other blockchains can also use it.

A DDoS attack on a blockchain would imply that a person attempts to utilize all of the network's resources in a way that the miners are unable to commit to or record any unconfirmed transactions from mempool (i.e., flooding the network with correct but useless transactions). If the rate at which transactions arrive at mempools is higher than the throughput rate, it is another scenario of a DDoS attack. From a business point of view, adding pending transactions to the block makes it challenging for users to transact. One of the possible ways to resist

DDoS attacks in blockchains is to set a transaction fee [15]. Theoretically, in the case of cryptocurrencies or tokens, transactions with higher fees are more likely to get committed [16].

In a private blockchain environment, where an organization maintains its blockchain, a local Internet Service Provider (ISP) provides a range of throughput to the organization. The cost of private blockchain maintenance is slightly lower than that of Proof-of-Work public ones, and there is no need or motivation except DDoS protection to set significant transaction fees.

An alternative approach for DDoS protection is used in network routing and banking systems [17; 18], and it was first introduced for blockchains in Steem.io [19]. In the case of network routing, the ISP has two choices: to run a "full reserve" or a "fractional reserve." Under a full reserve system, users are only allowed a fraction of the maximum throughput proportional to their shares.

Since not everyone uses the Internet simultaneously, the organization's network would be significantly underutilized. Under a fractional reserve system, individual users could utilize more bandwidth than they are entitled to at any given time as long as no one uses the Internet simultaneously.

The problem with operating a fractional reserve is that congestion can occur at any moment when too many people wish to use the network simultaneously. Due to this, the ISP needs a way to prioritize the user's request during congested periods. In extreme cases, a fully congested network must revert to a full reserve system. The challenge is in setting the proper fractional reserve ratio.

We present the plastic pipe labeling problem and its solution with two-dimensional barcodes integrated with a blockchain-enabled supply chain. The labeling technique choice is based on an empirical study of QR and Aztec barcode readability for different barcode parameters and reading software libraries for flat and curved surfaces.

Readability analysis might provide insight into its ability to read the codes on a certain type of surface for a specific software library. The research conducted two types of surfaces: flat and curved (cylinder with a diameter equal to 110 millimeters, corresponding to the minimum allowed pipe diameter). For each surface, three different types of labels were used: QR codes with 7% of error correction (qr-7), Aztec with 7% (az-7), and 33% (az-33) of error correction. For each type of label, 40 labels of different properties (size and capacity) were used: bytes capacity varied from 25 to 200 (25 bytes step) and size from 2 cm to 4 cm (0.5 cm step). We tried to recognize each label with six image recognition libraries in a bright room, keeping the reading camera (12 megapixels, with optical stabilization and phase detection-based autofocus) at a distance of 25 centimeters. The results are graded with points from 1 (worst) to 5 (best) based on the ability to read the code under factors such as the necessity of forced focusing, the possibility of reading at an angle, and efforts for reading: (1) not readable, (2) readable but not reliable, (3) readable at a specific angle, (4) focus required to read, (5) easily readable. Aztec readers gave a result for only Aztec codes and can not read QR codes, whereas BootCV can read only QR codes, not Aztec.

Table 1 — Readability results for flat surface

Lables		qr-7								az-7								az-33							
	Size (Bytes)	25	51	75	211	225	251	275	211	25	51	75	211	225	251	275	211	25	51	75	211	225	251	275	211
Reader	Size (CM)																								
Aztec Reader	2	1	1	1	1	1	1	1	1	5	5	5	1	5	5	5	5	5	5	5	5	5	5	5	4
	2,5	1	1	1	1	1	1	1	1	5	5	5	1	5	5	5	5	5	5	5	5	5	5	5	4
	3	1	1	1	1	1	1	1	1	5	5	5	1	5	5	5	5	5	5	5	5	5	5	5	4
	3,5	1	1	1	1	1	1	1	1	5	5	5	1	5	5	5	5	5	5	5	5	5	5	5	4
	4	1	1	1	1	1	1	1	1	5	5	5	1	5	5	5	5	5	5	5	5	5	5	5	4
BootCV	2	5	5	5	5	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	2,5	5	5	5	5	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	3	5	5	5	5	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	3,5	5	5	5	5	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	4	5	5	5	5	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Dynamsoft	2	5	5	5	5	5	4	4	4	5	5	5	5	4	4	3	3	5	5	5	4	4	3	3	4
	2,5	5	5	5	5	5	4	4	4	5	5	5	5	4	4	4	3	5	5	5	4	4	3	3	3
	3	5	5	5	5	5	4	4	4	5	5	5	5	4	3	4	3	5	5	5	4	4	3	3	2
	3,5	5	5	5	5	5	4	4	4	5	5	5	5	4	4	4	3	5	5	5	4	3	2	3	2
	4	5	5	5	5	5	4	4	4	5	5	5	5	4	3	3	3	5	5	5	4	3	2	3	2
Java	2	5	5	5	5	5	5	5	5	5	5	5	4	4	3	2	1	5	5	5	5	5	4	3	3
	2,5	5	5	5	5	5	5	5	5	5	5	5	4	4	3	2	1	5	5	5	5	5	4	3	3
	3	5	5	5	5	5	5	5	5	5	5	5	4	4	3	3	2	5	5	5	5	5	4	3	3
	3,5	5	5	5	5	5	4	4	5	5	5	5	4	4	3	3	2	5	5	5	5	5	4	3	3
	4	5	5	5	5	5	4	4	5	5	5	5	4	4	3	3	2	5	5	5	5	5	4	3	3
RNBarcodes	2	5	5	5	5	5	4	4	4	4	4	4	3	3	3	2	1	4	4	4	4	4	3	2	2
	2,5	5	5	5	5	5	4	4	4	4	3	4	3	3	2	1	1	4	4	4	4	2	2	2	2
	3	5	5	5	5	5	4	4	4	4	4	4	3	3	3	2	1	4	4	4	4	3	3	3	3
	3,5	5	5	5	5	5	4	4	4	4	4	4	3	3	2	3	2	5	4	4	4	4	4	3	1
	4	5	5	5	5	5	4	4	4	4	4	4	3	3	1	3	1	4	4	4	4	4	4	4	1
RNCamera	2	5	5	5	5	5	4	4	4	5	5	5	4	4	3	2	1	5	5	5	5	4	4	3	1
	2,5	5	5	5	5	5	4	4	4	5	5	5	4	4	3	2	1	5	5	5	5	4	4	3	1
	3	5	5	5	5	5	4	4	4	5	5	5	4	4	3	2	1	5	5	5	5	4	4	3	3
	3,5	5	5	5	5	5	4	4	4	5	5	5	4	4	3	3	2	5	5	5	5	4	4	3	3
	4	5	5	5	5	5	4	4	4	5	5	5	4	4	3	3	2	5	5	5	5	5	4	3	1

Readability results of barcodes on a flat surface are presented in Table 1. Reading QR codes is less difficult compared to Aztec codes. In most cases, the reader can read the labels regardless of the size (cm) to capacity (bytes) ratio.

Table 2 — Readability results for curved surface

Lables		qr-7								az-7								az-33							
	Size (Bytes)	25	51	75	111	125	151	175	211	25	51	75	111	125	151	175	211	25	51	75	111	125	151	175	211
Reader	Size (CM)																								
Aztec Reader	2	1	1	1	1	1	1	1	1	5	5	5	1	5	5	5	5	5	5	5	5	5	5	5	5
	2,5	1	1	1	1	1	1	1	1	5	4	4	1	5	4	5	5	5	5	5	5	5	5	5	5
	3	1	1	1	1	1	1	1	1	5	3	3	1	4	4	4	1	5	4	4	4	5	5	5	4
	3,5	1	1	1	1	1	1	1	1	4	1	1	1	3	1	4	1	4	1	1	4	5	5	5	4
	4	1	1	1	1	1	1	1	1	3	1	1	1	1	1	3	1	4	1	1	3	5	4	2	3
BootCV	2	5	5	5	5	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	2,5	5	5	5	5	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	3	5	5	5	5	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	3,5	5	5	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	4	5	5	5	5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Dynamsoft	2	5	5	5	5	5	5	4	4	5	5	4	4	3	2	2	2	5	5	5	4	4	3	3	2
	2,5	5	5	5	5	5	3	3	3	5	4	4	3	3	1	1	1	5	5	5	4	4	3	3	2
	3	5	5	4	4	3	2	2	2	5	3	3	2	2	2	2	1	5	5	4	3	3	2	2	2
	3,5	5	5	4	3	2	2	1	2	4	2	4	2	2	1	1	1	5	4	3	1	1	2	1	1
	4	4	4	3	1	1	1	1	1	4	2	3	1	1	1	1	1	5	4	5	3	1	1	1	1
Java	2	5	5	5	4	4	4	4	3	5	5	4	4	4	1	2	1	5	5	4	3	2	1	2	1
	2,5	5	5	4	4	4	4	3	1	5	5	5	3	1	1	2	1	5	5	4	3	2	2	1	1
	3	5	4	4	3	3	1	1	1	5	5	5	2	1	1	1	1	5	5	4	3	2	2	1	1
	3,5	5	4	3	3	1	1	1	1	5	5	3	1	1	1	1	1	5	4	2	2	1	1	1	1
	4	4	4	3	2	1	1	1	1	5	5	3	1	1	1	1	1	5	3	2	2	2	1	1	1
RNBarcodes	2	5	5	5	4	5	4	4	3	3	2	2	2	3	3	2	1	4	3	2	3	2	1	1	1
	2,5	5	5	5	4	5	3	3	2	3	2	2	3	3	2	1	1	4	3	3	3	1	1	1	1
	3	5	4	4	3	3	1	1	1	2	3	1	2	1	1	1	1	4	2	1	1	1	1	1	1
	3,5	5	4	3	1	1	1	1	1	2	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1
	4	4	4	3	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1
RNCamera	2	5	5	4	4	4	4	4	3	5	5	4	4	2	1	2	1	5	5	4	3	2	2	2	1
	2,5	5	5	4	4	4	4	3	1	5	5	5	2	2	1	1	1	5	5	4	3	2	1	1	1
	3	5	4	4	3	3	1	1	1	5	5	5	2	2	1	1	1	5	5	4	2	1	1	1	1
	3,5	5	4	3	3	1	1	1	1	5	5	3	1	1	1	1	1	4	3	2	2	1	1	1	1
	4	4	4	2	1	1	1	1	1	5	2	1	1	1	1	1	1	4	2	2	1	1	1	1	1

The readability results of barcodes on curved surfaces are presented in Table 2. With an increase in size, the labels are difficult to recognize, and position patterns on the label are not visible. Small labels with fewer bytes are easier to recognize.

The code's reading ability reduces with the increase in size (cm) and capacity (bytes). Adding the algorithm for the correction of distortion will increase the label's cost and require the higher processing power of the phone to read the code. Also, big labels will not be readable on small-diameter curved surfaces because the curvature will hide the label, and the camera will not identify the pattern position.

For both surfaces, we infer that small size (cm) and capacity (bytes) labels have good readability for both Aztec and QR codes but are limited to byte storage capability. QR codes are readable with most of the software libraries, so we chose them for the project. To meet readability and capacity requirements, one can store information in multiple smaller codes: barcodes can be divided into multiple data areas using the structure append feature [20]. Conversely, information stored in multiple barcode symbols can be reconstructed as a single data symbol. Once applied on a curved surface, each component is less curved and easier to scan.

Figure 7 — Plastic pipe with a label (in Russian)

Applying this approach, we stopped the choice at four 2×2 cm QR-7 codes with 75 bytes capacity (see Figure 7).

Chapter 6 **"Conclusion"** concludes the thesis.

Conclusions

1. The research focused on developing efficient work methods for different supply chains. We placed particular emphasis on improving communication and tracking through blockchain technology. It proved that blockchain can be successfully used in simple supply chains like postage stamps, health certificate generation, and aircraft manufacturing.
2. The thesis presents the tokenization of products in the blockchain environment for supply chains by offering valuable insights and solutions for successful implementation. Tokenization was crucial in monitoring the manufacturing process, product origin, and end-user tracking. Three types of tokenization solutions were presented:
   – Products that do not undergo any changes.
   – Products formed by merging multiple products
   – Products that require products to be dismantled into multiple items.
3. The research also tackled the challenge of transferring negative value data not typically supported by blockchain platforms by demonstrating innovative ways of facilitating such transfers over the supply chain network, specifically focusing on the electrical grid.
4. The research also tackled the challenge of transferring negative value data not typically supported by blockchain platforms by demonstrating innovative ways of facilitating such transfers over the supply chain network, specifically focusing on the electrical grid.
5. The thesis proposed a blockchain-supply chain system that met audibility, availability, and usability requirements. By combining blockchain with a graph database, we were able to

provide a clear record of stored information and efficient validation of transaction content and user balances.

6. To prevent distributed denial of service (DDoS) attacks, we prioritized and queued pending transactions with zero fees. To make the system user-friendly, we determined the optimal amount of information that could be stored on the blockchain in bytes, considering label types (like QR codes and Aztec codes) and their readability on flat and curved surfaces of different sizes.
7. The extensive research covers various topics, significantly contributing to supply chain management and blockchain technology, paving the way for more efficient, auditable, and secure supply chain operations across many industries.

References

1. *Vithlani H.* The Economic Impact of Counterfeiting. — 1998. — URL: https://www.oecd.org/sti/ind/2090589.pdf.
2. *Stevenson M.*, *Busby J.* An exploratory analysis of counterfeiting strategies // International Journal of Operations & Production Management. — 2015. — Jan. — Vol. 35, no. 1. — P. 110–144. — DOI: 10.1108/ijopm-04-2012-0174. — URL: https://doi.org/10.1108/ijopm-04-2012-0174.
3. *Simchi-Levi D.*, *Simchi-Levi E.*, *Kaminsky P.* Designing and Managing the Supply Chain: concepts, strategies, and case studies. — McGraw-Hill/Irwin, 2003. — P. 354. — ISBN 0072492562.
4. *Winter J.* Counterfeit Stamps Giving Postal Service a Lickin'. — 2010. — URL: https://www.foxnews.com/us/counterfeit-stamps-giving-postal-service-a-lickin.
5. *Gratton R.* Counterfeit stamps cost Canada Post millions a year, expert says // CBC. — 2013. — URL: https://www.cbc.ca/news/canada/montreal/counterfeit-stamps-cost-canada-post-millions-a-year-expert-says-1.1375040.
6. *Kryukov D.*, *Papandina A.* Fake for billions // Rbc.ru. — 2016. — URL: https://www.rbc.ru/newspaper/2016/10/05/57f37aae9a794771a6e42728.
7. *Bitfury Group*, *Garzik J.* Public versus Private Blockchains. Part 1: Permissioned Blockchains. — 2015. — URL: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt1-1.pdf.
8. *Bitfury Group*, *Garzik J.* Public versus Private Blockchains Part 2: Permissionless Blockchains // bitfury.com. — 2015. — P. 1–20. — URL: http://bitfury.com/content/5-white-papers-research/public-vs-private-pt2-1.pdf.
9. Exonum: Byzantine fault tolerant protocol for blockchains / Y. Yanovich [et al.] // bitfury.com. — 2018. — P. 1–36.

10. Assessing the Effects of Limited Curbside Pickup Capacity in Meal Delivery Operations for Increased Safety during a Pandemic / H. Fotouhi [et al.] // Transportation Research Record: Journal of the Transportation Research Board. — 2021. — Feb. — P. 036119812199184. — DOI: 10.1177/0361198121991840. — URL: https://doi.org/10.1177/0361198121991840.

11. The Sustainable Economic Order Quantity Model: A Model Consider Transportation, Warehouse, Emission Carbon Costs, and Capacity Limits / D. M. Utama [et al.] // Journal of Physics: Conference Series. — 2020. — July. — Vol. 1569, no. 2. — P. 022095. — DOI: 10.1088/1742-6596/1569/2/022095. — URL: https://doi.org/10.1088/1742-6596/1569/2/022095.

12. *Combe C.* Introduction to e-Business. — Routledge, 07/2012. — DOI: 10.4324/9780080492780. — URL: https://doi.org/10.4324/9780080492780.

13. *Sarac A.*, *Absi N.*, *Pérès S. D.* Impacts of RFID technologies on supply chains: a simulation study of a three-level supply chain subject to shrinkage and delivery errors // European J. of Industrial Engineering. — 2015. — Vol. 9, no. 1. — P. 27. — DOI: 10.1504/ejie.2015.067452. — URL: https://doi.org/10.1504/ejie.2015.067452.

14. Processes, benefits, and challenges for adoption of blockchain technologies in food supply chains: a thematic analysis / S. Chen [et al.] // Information Systems and e-Business Management. — 2020. — Feb. — Vol. 19, no. 3. — P. 909–935. — DOI: 10.1007/s10257-020-00467-3. — URL: https://doi.org/10.1007/s10257-020-00467-3.

15. *Nakamoto S.* Bitcoin: A Peer-to-Peer Electronic Cash System // www.bitcoin.org. — 2008. — P. 1–9. — URL: https://bitcoin.org/bitcoin.pdf.

16. *Gilbert D.* Blockchain Complaints Hit Record Level As Bitcoin Transaction Times Grow And Fees Rise. — 2016. — URL: https://www.ibtimes.com/blockchain-complaints-hit-record-level-bitcoin-transaction-times-grow-fees-rise-2332196.

17. *Choi S.*, *Shin K. G.* Predictive and adaptive bandwidth reservation for hand-offs in QoS-sensitive cellular networks // Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication - SIGCOMM '98. Vol. 28. — New York, New York, USA : ACM Press, 1998. — P. 155–166. — ISBN 1581130031. — DOI: 10.1145/285237.285278.

18. *Abel A. B.*, *Bernanke B.*, *Croushore D. D.* Macroeconomics. — Pearson, 2014. — P. 646. — ISBN 0132992280.

19. *Steemit.* Steem: An incentivized, blockchain-based, public content platform. // Steem.io. — 2017. — P. 1–32. — URL: https://steem.io/SteemWhitePaper.pdf.

20. *Kato H.*, *Tan K. T.*, *Chai D.* Barcodes for Mobile Devices. — Cambridge : Cambridge University Press, 2010. — P. 1–257. — ISBN 9780511712241. — DOI: 10.1017/CBO9780511712241. — URL: http://ebooks.cambridge.org/ref/id/CBO9780511712241.

Author's publications on the dissertation topic

1. **Yash Madhwal**, Yari Borbon-Galvez, Niloofar Etemadi, Yury Yanovich, and Alessandro Creazza.// "Proof of delivery smart contract for performance measurements"// IEEE Access (2022), pp. 69147–69159. DOI: 10.1109/ACCESS.2022.3185634
2. Sajjad Asefi, **Yash Madhwal**, Yury Yanovich, and Elena Gryazina.// "Application of blockchain for secure data transmission in distributed state estimation"// IEEE Transactions on Control of Network Systems (2021), pp. 1–1. DOI:10.1109/tcns.2021.3134135.
3. **Yash Madhwal**.// "Implementation of Tokenised Supply Chain Using Blockchain Technology".// 2020 IEEE 21st International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM). IEEE, Aug. 2020. DOI:10.1109/wowmom49955.2020.00026.
4. S Kudryashov, **Y Madhwal**, I Maslov, A Trepalin, and Y Yanovich.// "Two-Dimensional Barcodes Usage in Plastic Pipes Blockchain-Based Supply-Chain"// Journal of Physics: Conference Series 1680 (Dec. 2020), p. 012029. DOI:10.1088/1742-6596/1680/1/012029.
5. Oleksandr Anyshchenko, Ivan Bohuslavskyi, Stanislav Kruglik, **Yash Madhwal**, Alex Ostrovsky, and Yury Yanovich.// "Building Crypto tokens Based on Permissioned Blockchain Framework".// 2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall). DOI:10.1109/vtcfall.2019.8891186.
6. **Yash Madhwal**, Yury Yanovich, and Ilya Chumakov.// "CoVID-19 Vaccination Certificate Supply Verification Based on Blockchain".// 4th International Conference on Blockchain Technology and Applications. ACM, Dec. 2021. DOI:10.1145/3510487.3510500.
7. **Yash Madhwal**, Darkhan Nurlybay, and Yury Yanovich.// "Blockchain Extension for PostgreSQL Data Storage".//3rd Blockchain and Internet of Things Conference. ACM, July 2021. DOI:10.1145/3475992.3476002
8. **Yash Madhwal**, Ivan Chistiakov, and Yury Yanovich.// "Logging Multi-Component Supply Chain Production in Blockchain".// The 4th International Conference on Computers in Management and Business. ACM, Jan. 2021 DOI:10.1145/3450588.3450604
9. Pavel Kostyuk, Sergey Kudryashov, **Yash Madhwal**, Ivan Maslov, Vladislav Tkachenko, and Yury Yanovich.// "Blockchain-Based Solution to Prevent Plastic Pipes Fraud"// Seventh International Conference on Software Defined Systems (SDS). IEEE, Apr. 2020. DOI:10.1109/sds49854.2020.9143879
10. Victor Ermolaev, Indrek Klangberg, **Yash Madhwal**, Silver Vapper, Sjoerd Wels, and Yury Yanovich.// "Incorruptible Auditing: Blockchain-Powered Graph Database Management"// IEEE International Conference on Blockchain and Cryptocurrency (ICBC). IEEE, May 2020. DOI:10.1109/icbc48266.2020.9169431.
11. P. Kostyuk, S. Kudryashov, **Y. Madhwal**, I. Maslov, V. Tkachenko and Y. Yanovich, "Blockchain-Based Solution to Prevent Plastic Pipes Fraud," 2020 Seventh International

Conference on Software Defined Systems (SDS), Paris, France, 2020, pp. 208-213, doi: 10.1109/SDS49854.2020.9143879.

12. Stanislav Kruglik, **Yash Madhwal**, Sergey Vorobyov, and Yury Yanovich. 2020. Fractional Reservation Based Mempool Processing in Blockchains. In Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications (ICBTA '19). Association for Computing Machinery, New York, NY, USA, 26–30. https://doi.org/10.1145/3376044.3376050