

Research article

DOI: <https://doi.org/10.18721/JCSTCS.19302>

UDC 004.8



DESIGN OF AN AUTOMATED FREIGHT TRANSPORTATION MONITORING SYSTEM BASED ON INTERNET OF THINGS NETWORKS USING BLOCKCHAIN TECHNOLOGY

*L.V. Agamirov^{1,2} , V.L. Agamirov^{2,3} ,
P.E. Slyadnikov² , N.V. Toutova² , A. Khaush² *

¹ National Research University “Moscow Power Engineering Institute”,
Moscow, Russian Federation;

² Moscow Technical University of Communications and Informatics,
Moscow, Russian Federation;

³ Moscow Aviation Institute (National Research University),
Moscow, Russian Federation

✉ avhere@yandex.ru

Abstract. The paper proposes an architecture for an automated freight transportation monitoring system based on blockchain technology. When integrating standard blockchain solutions with Internet of Things (IoT) devices into a unified techno-logical system, it is necessary to minimize direct requests to the main registry (root blockchain). This requirement remains essential even when participants of the distributed network are granted permissions to modify smart contract parameters, thereby reducing the load on the root registry while ensuring a high level of security during data transmission: from sensors to the mobile node and from the mobile node to the root system. The paper presents a comparative analysis of distributed ledger platforms, taking into account regional specifics and the possibility of integrating certified domestic cryptographic information protection tools. A prototype of an end-to-end freight transportation monitoring system has been developed and implemented, providing continuous tracking of cargo conditions sensitive to environmental factors. Simulation results confirm the effectiveness of using smart contracts for automating control procedures and ensuring the immutability of logistics operation data. The proposed architecture enables the development of scalable and secure industrial monitoring networks for logistics companies.

Keywords: Internet of Things, blockchain, smart contract, cargo transportation, logistics, mobile node, information security

Citation: Agamirov L.V., Agamirov V.L., Slyadnikov P.E. et al. Design of an automated freight transportation monitoring system based on internet of things networks using blockchain technology. Computing, Telecommunications and Control, 2026, Vol. 19, No. 3, Pp. 18–28. DOI: 10.18721/JCSTCS.19302

Научная статья

DOI: <https://doi.org/10.18721/JCSTCS.19302>

УДК 004.8



ПОСТРОЕНИЕ СИСТЕМЫ АВТОМАТИЧЕСКОГО МОНИТОРИНГА ГРУЗОПЕРЕВОЗОК НА ОСНОВЕ СЕТЕЙ ИНТЕРНЕТА ВЕЩЕЙ С ПРИМЕНЕНИЕМ ТЕХНОЛОГИИ БЛОКЧЕЙН

Л.В. Агамиров^{1,2} , В.Л. Агамиров^{2,3} ,
П.Е. Слядников² , Н.В. Тутובה² , А. Хауш²

¹ Национальный исследовательский университет «МЭИ»,
Москва, Российская Федерация;

² Московский технический университет связи и информатики (МТУСИ),
Москва, Российская Федерация;

³ Московский авиационный институт (МАИ), Москва, Российская Федерация

avhere@yandex.ru

Аннотация. В статье предлагаются концепции построения автоматической системы для передачи чувствительной информации в системах мониторинга на базе блокчейн-сетей с распределенной инфраструктурой. Использование существующих методов построения блокчейн-сетей в сочетании с интеграцией устройств Интернета вещей (IoT) в общий технологический стек предполагает следование концепциям, направленным на минимизацию прямого обращения к корневому реестру. Такой подход сохраняется даже при наличии прав на редактирование параметров, что позволяет снизить нагрузку на сеть, обеспечивая при этом высокий уровень безопасности при передаче данных от датчиков к мобильному узлу и от мобильного узла к корневой системе. В работе представлен сравнительный анализ платформ распределенного реестра с учетом региональной специфики и возможности внедрения сертифицированных отечественных средств криптографической защиты информации. Разработан и реализован прототип системы полного жизненного цикла для грузоперевозок, обеспечивающий непрерывный мониторинг состояния грузов, чувствительных к факторам окружающей среды. Результаты имитационного моделирования подтверждают эффективность использования смарт-контрактов для автоматизации контроля и обеспечения неизменности данных о логистических операциях. Предложенный подход позволяет создавать масштабируемые и защищенные промышленные сети мониторинга для логистических компаний.

Ключевые слова: Интернет вещей, блокчейн, смарт-контракт, грузоперевозки, логистика, мобильный узел, защита информации

Для цитирования: Agamirov L.V., Agamirov V.L., Slyadnikov P.E. et al. Design of an automated freight transportation monitoring system based on internet of things networks using blockchain technology // Computing, Telecommunications and Control. 2026. Т. 19, № 3. С. 18–28. DOI: 10.18721/JCSTCS.19302

Introduction

The transformation of modern logistics toward cost reduction and the implementation of transportation quality control systems has increased the relevance of Internet of Things (IoT) technologies. According to Future Market Insights, spending on IoT solutions in logistics amounted to 50.26 million USD in 2024. It is projected to grow to 189.62 million USD by 2034, with a compound annual growth rate (CAGR) of 14.2% [1].

A similar trend is observed in the market for blockchain-based solutions. According to Global Market Insights, the global blockchain logistics market is demonstrating steady growth driven by increasing requirements for supply chain transparency, the reduction of disputes among supply chain

participants, and the need to ensure the immutability of logistics data¹. The highest demand is concentrated in the areas of product provenance tracking, document workflow automation, and transportation condition monitoring [2].

On the one hand, the scaling of networks integrating various sensors, controllers, and actuating devices opens up new opportunities for improving the quality of freight transportation monitoring. On the other hand, it creates a number of challenges and increases the requirements for the hardware employed and the quality of communication channels [3].

Among the key challenges are the need for real-time transmission of cargo-related data, including geolocation information, and the continuous monitoring of transportation parameters such as temperature, humidity level, vibration loads, and other indicators. The use of sensors optimizes operational processes by replacing manual inspection of cargo and vehicle conditions with automated monitoring at terminals and warehouses. Another significant challenge is the scalability of such systems, where information security in traffic transmission becomes a critical concern, particularly with respect to data immutability and the redistribution of information flows within core storage systems.

Addressing these challenges requires a technological foundation capable of providing an environment for recording key events in logistics processes. One potential solution is the application of blockchain technology in combination with smart contracts, where data collection from IoT devices is performed automatically in accordance with predefined algorithms.

The aim of this study is to assess the applicability and potential approaches to integrating blockchain platforms into the architecture of logistics-oriented IoT networks while taking into account the specifics of the Russian environment. Particular attention is paid to the development of a lightweight service intended for interaction with IoT devices and blockchain infrastructure.

Materials and methods

System monitoring architecture

One of the key problems of traditional logistics chains is the issue of trust among participants, including the sender, carrier, and recipient. In the event of cargo damage (for example, due to a violation of temperature conditions), data obtained from monitoring devices may be falsified by an interested party or lost. The proposed solution involves the creation of an autonomous trusted auditor based on IoT technologies and a distributed ledger implemented through a blockchain network. The core element of the system is a “smart” IoT container capable of independently recording specific environmental parameters (such as temperature, pressure, etc.), signing them with a cryptographic key directly on the end device, and transmitting them to a blockchain ledger that is immutable for unauthorized parties. Such an approach transforms IoT devices into independent observers, eliminating the human factor and preventing data falsification.

A similar approach is discussed in a number of recent studies devoted to the digitalization of supply chains [4, 5]. These works also emphasize that the combination of IoT and blockchain technologies enables the creation of a mechanism for continuous tracking of goods during transportation, in which every event is automatically recorded in a distributed ledger and becomes verifiable by all participants in the supply chain [6].

The conceptual interaction model within the supply chain is based on the separation of areas of responsibility. Regardless of the specific platform implementation, three key logical roles can be identified within the system:

1) **The transportation initiator or a dedicated coordinating entity** acts as the contract administrator with full access privileges. This participant defines the transportation conditions, including permissible

¹ Blockchain in Logistics Market Size, Share, and Industry Analysis, By Technology (Public Blockchain, Private Blockchain, and Others), By Use Cases (Track and Trace, Transparency and Compliance, Smart Contracts, Inventory Management, and Counterfeit Prevention), By Industry (FMCG, Pharmaceutical, Manufacturing, Automotive, and Others), and Regional Forecast, 2026-2034. [online] Available at: <https://www.fortunebusinessinsights.com/thankyou/request-sample-pdf-s-bar-report/111635> [Accessed 16.07.2026].

ranges of temperature, humidity, illumination, and geolocation parameters. In addition, the administrator creates a digital representation of the agreement in the form of a smart contract – an algorithm containing the logic for condition verification – and deploys this contract to the network, thereby initiating the monitoring process.

2) **The mobile agent (carrier)** operates an IoT node located within the cargo compartment. This hardware-software system is installed on the vehicle and functions as a lightweight client of the blockchain network. It continuously collects telemetry data from sensors, performs preliminary onboard data processing in order to reduce network load, and transmits only critical events or periodic reports to the blockchain, authenticated by the device's digital signature [7].

3) **The auditor** is an entity with read-only or validation access to the distributed ledger. At any time, the auditor can verify the cargo status and the integrity of the transportation history, as well as record the completion of the contract upon cargo delivery.

The proposed system is based on the principle of architectural immutability after deployment. Violation detection is performed outside centralized servers, within a decentralized infrastructure built on smart contracts. The lifecycle of the monitoring process can be represented as follows² [8]:

1) **Recording conditions in the smart contract.** Transportation conditions and data related to carriers, recipients, and senders are specified within the smart contract. For example, one of the parameters may define the permissible temperature range for goods during transportation. The smart contract contains a comprehensive set of conditions, which may only be modified by the administrator acting as the responsible entity.

2) **The cryptographic binding of IoT devices** enables the local registration of contract conditions during the initialization of procedures and their subsequent processing within the system. This makes it possible to define multiple operational constraints and develop a mathematical framework for assessing actual parameter variations during transportation.

3) **Incident detection.** If the sensors detect a deviation from the predefined norm, or if aggregated indicators over a certain period reveal a violation of transportation conditions, the IoT device generates a transaction containing information about the violation and records it in the smart contract.

4) **Immutability.** The transaction is included in a block, linked to previous records through cryptographic hashing, and propagated across all nodes in the network. Data deletion or modification is impossible without compromising the integrity of the blockchain; therefore, the proposed structure can be characterized as highly resistant to tampering.

It should be noted that such an architecture corresponds to the concept of “traceability by design,” in which the system is developed with the objective of ensuring subsequent verification of the origin and condition of cargo at every stage of the transportation route [9–11].

Comparative analysis of blockchain networks

Selecting an appropriate blockchain platform for logistics applications and substantiating this choice constitutes one of the primary objectives of the proposed project. For consortium and enterprise-grade solutions, which include the system under development, platforms supporting a permissioned access model while ensuring high transaction throughput and confidentiality are considered. The following platforms satisfy these requirements [12]:

1) **Hyperledger Fabric** is a platform developed by the Linux Foundation and positioned as a framework for enterprise blockchain networks. Its key advantage is a modular architecture and a flexible channel system that enables transaction isolation between specific consortium participants. This feature is critical for logistics scenarios, where the shipper and carrier should not disclose commercial details to the entire network. However, the performance of the platform strongly depends on hardware configuration. Deploying a full peer node on low-power devices (e.g., Raspberry Pi-based units inside cargo containers) is challenging due to high computational requirements. In addition, the use

² MEXC. Chto takoe smart-kontrakty? [What are smart contracts?] [online] Available at: <https://www.mexc.com/ru-RU/learn/article/what-are-smart-contracts-1> [Accessed 16.07.2026].

of non-domestic cryptographic algorithms requires additional layers of adaptation for certification within the Russian jurisdiction³ [13].

2) **Corda**, developed by the R3 consortium, was originally designed for the financial sector but has also found applications in logistics. Its main feature is the absence of a global transaction ledger. Information is stored only between participants of a specific transaction, which ensures a high level of privacy and reduces network overhead. However, since Corda shares data only among parties involved in a given deal, it complicates the creation of a unified dataset. As a result, regulatory authorities face difficulties in verifying the full lifecycle of goods across all stages. Additionally, the issue of certification compliance within the Russian jurisdiction remains unresolved⁴ [14].

3) **Ethereum (Private, Quorum)** enables the use of the Solidity ecosystem and development tools while eliminating the high fees and low throughput of the public network. Quorum provides mechanisms for private transactions and various consensus protocols. However, for the purposes of this study, a critical drawback is the use of cryptographic standards that do not comply with Russian regulatory requirements. Data signed using such cryptography cannot be directly accepted as legal evidence in Russian arbitration proceedings without costly and complex forensic examination⁵ [15].

4) The **“Confident” platform** is a specialized enterprise-grade blockchain solution developed by the Russian company Web3 Tech for building governmental and corporate distributed trusted systems. Unlike foreign counterparts, this platform is designed from the outset to comply with Russian legislation and to integrate with existing IT infrastructure within the Russian market⁶ [16].

A comparison of the main characteristics of the presented platforms is provided in Table 1.

Table 1

Comparative analysis of the presented platforms

Criterion	Hyperledger Fabric	Corda	Ethereum (Private, Quorum)	Confident
Platform type	Permissioned	Permissioned	Permissioned, Private	Permissioned
Consensus	Raft, Kafka, PBFT	Notary-based platform	IBFT, Raft	Asynchronous, based on Russian algorithms
Confidentiality	Channels, private data	“Need-to-know” model	Private transactions	Cryptographic isolation, GOST
Regulatory requirements (RF)	Not compliant	Not compliant	Not compliant	Compliant
Node resource requirements	High	Medium	Medium	Medium

Considering the requirements for product certification, data protection, and ease of integration with heterogeneous IoT devices, as well as the ability to operate under conditions of unstable connectivity, the “Confident” platform represents the most balanced technological solution for developing a domestic fault-tolerant logistics management system under the given constraints.

³ Nefedov N. Hyperledger Fabric dlia Chainikov [Hyperledger Fabric for Dummies]. [online] Available at: <https://habr.com/ru/companies/ibm/articles/444874/> [Accessed 16.07.2026].

⁴ Shunko A. Corda – open source blokchein dlia biznesa [Corda – open-source blockchain for business] [online] Available at: <https://habr.com/ru/articles/452258/> [Accessed 16.07.2026].

⁵ Alexx. Vypolnenie publichnykh i privatnykh tranzaktsii v blokcheine JPMorgan Quorum s ispol'zovaniem Web3 [Executing public and private transactions on the JPMorgan Quorum blockchain using Web3]. [online] Available at: <https://habr.com/ru/articles/456368/> [Accessed 16.07.2026].

⁶ Konfident – blokchein-platforma dlia biznesa i gosudarstva [Confidant – a blockchain platform for business and government]. [online] Available at: <https://web3tech.ru/platform/architecture> [Accessed 16.07.2026].

System design

Currently, there is an issue related to compliance with cargo transportation conditions, particularly with respect to regulations governing the handling of goods. This problem is further exacerbated by the lack of a simple and accessible evidentiary basis for suppliers and their customers. In disputed situations (for example, in cases of cargo damage), it is practically impossible to objectively determine the responsible party – whether the incident is a result of the carrier’s actions or improper packaging by the sender. The existing practice allows one of the contracting parties to manipulate data in its own favor.

To address this problem, an automated cargo monitoring system based IoT and blockchain technologies has been developed. The system is built on Raspberry Pi 4B/5 single-board computers acting as mobile gateways that collect data from a set of IoT sensors. These sensors continuously record critical parameters specific to each type of cargo (such as temperature, humidity, vibration, geolocation, and others), compliance with which is stipulated by contractual conditions. The use of blockchain ensures the immutability of the collected data, fully eliminating the possibility of record falsification by any party. In addition, smart contracts are protected from post-deployment modification after being agreed upon and uploaded to the network, while on-gateway telemetry processing allows hardware noise to be filtered out, thereby minimizing technical errors [17, 18].

This approach enables the system to be used not only for technical monitoring but also as an evidentiary framework in dispute resolution, for example with insurance companies and regulatory authorities, ensuring full compliance with information security legislation requirements.

A key non-functional requirement of the system is to ensure high availability and fault tolerance of the mobile equipment throughout the entire transportation route. This requirement is implemented through the integration of automated IoT-based solutions. Edge sensors are responsible for continuous telemetry data acquisition, while a dedicated service performs initial processing, aggregation, and cryptographic protection of the data prior to its transmission to the platform’s distributed network [19, 20]. This ensures stable system operation under conditions of unstable connectivity and guarantees the integrity of the transmitted information.

Transactions and smart contract execution

A transaction is an atomic operation in a blockchain executed on behalf of a network participant that modifies the global state of the distributed ledger. It represents a fundamental system element: when a transaction is submitted, a node initiates a request containing a set of data for modifying information, access rights, or the state of smart contracts.

Before a transaction is included in a block, it undergoes a strict sequence of validation checks on the node side. If a transaction fails at least one stage of validation, it is rejected and is not added to the pool of confirmed transactions.

Critical validation stages:

1) **Timestamp.** The transaction creation time must not deviate from the time of inclusion of the current block in the blockchain by more than 2 hours backward or 1.5 hours forward. This protects the network against replay attacks.

2) **Versioning and types.** The system verifies whether support for the specified transaction type and version has been activated in the blockchain through the voting mechanism.

3) **Integrity.** A cryptographic signature check is performed. If the transaction data has been modified after signing, the signature becomes invalid, and the node rejects the transaction.

It should be noted that the process of constructing the blockchain ensures that data included in it cannot be removed. If an attacker attempts to delete or modify a transaction in an already created block, the block hash will change, breaking the cryptographic linkage with subsequent blocks, which will cause the entire branch to be rejected by honest nodes [21–23].

The lifecycle of a transaction on the “Confident” platform is illustrated in Fig. 1.

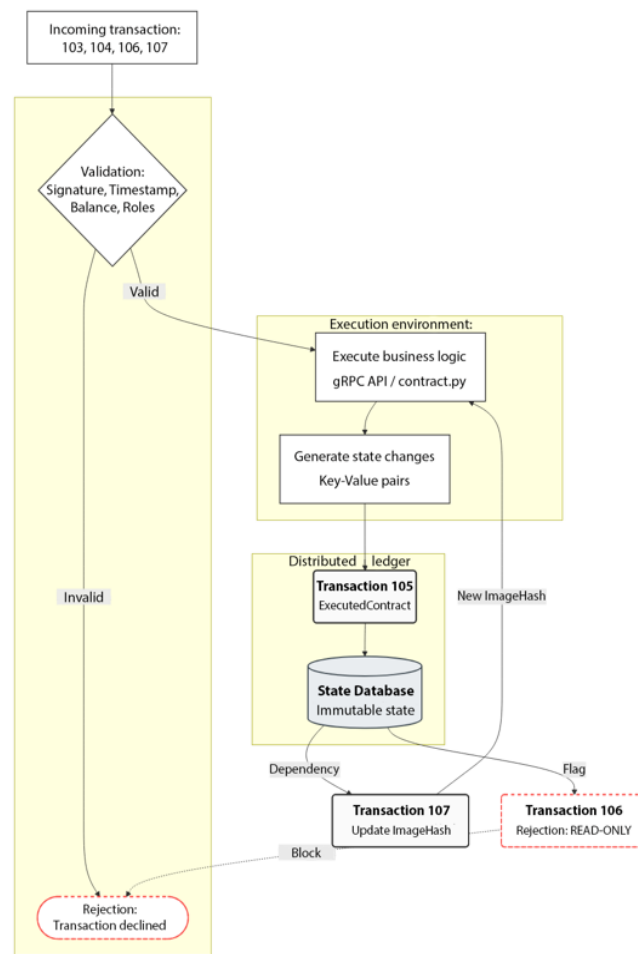


Fig. 1. Smart contract verification process on the “Confident” blockchain platform

On the presented platform, smart contracts are executed in isolated Docker containers. This approach ensures the security of the entire system in the event of a failure of an individual contract and enables the implementation of contract logic in any programming language. The smart contract code is stored off-chain.

The contract initialization process within the system proceeds as follows:

- 1) **Build.** A developer builds a Docker image containing the contract code and uploads it to an external repository, such as Docker Registry.
- 2) **Commitment.** A contract creation transaction is submitted to the blockchain, containing a reference to the image and its cryptographic hash.
- 3) **Execution.** Upon receiving the transaction, network nodes automatically download the specified image from the repository, verify its hash to ensure container integrity, and each participant executes the contract locally.

Thus, the image hash is recorded across all nodes, guaranteeing that all participants execute the same immutable code.

Results and discussion

Hardware-software implementation

To implement the approach described above, a distributed network consisting of three clusters was deployed, simulating a real supply chain, schematically illustrated in Fig. 2.

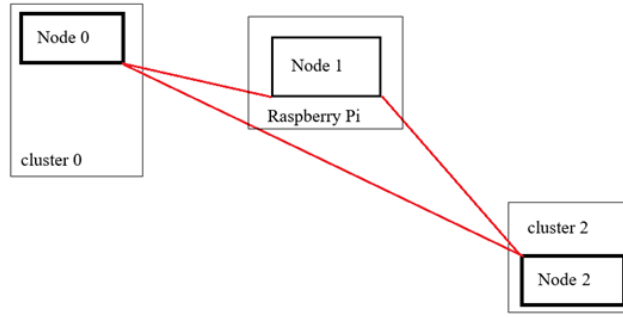


Fig. 2. Network architecture based on the “Confident” blockchain platform

Description of Fig. 2 structure:

1) **Cluster 0 (Sender/Node 0)** is a full-featured validator node acting as a “Control Center.” Through a web interface, the administrator defines smart contract parameters (temperature range, geofencing zones, time constraints, and other conditions associated with the contract waybill) and initiates its deployment across the network. Node 0 compiles the contract logic and signs the contract creation transaction.

2) **Carrier/Node 1** is a mobile node based on a Raspberry Pi device, integrated directly into the transport vehicle. It operates in a “light client” mode optimized for limited computational resources.

3) **Cluster 2 (Customer/Node 2)** is the receiving party, acting as a monitoring and auditing node that synchronizes the ledger to verify cargo status upon arrival.

The primary workload is handled by Node 1 (mobile node), as it collects all data and, in the event of a violation, propagates it to the network. The data processing pipeline consists of the following stages:

1) **Initialization and caching.** At the start of the shipment, Node 1 connects to the network and, using a unique Contract ID, loads the contract conditions (e.g., $t \in [20.0; 35.0]$) into a local cache. This ensures system operability even in the absence of Internet connectivity (GSM/LTE) during transit.

2) **Data acquisition and validation.** A Python-based microservice periodically polls a microcontroller connected to the sensor suite (temperature, light intensity, pressure). The obtained values are immediately compared against the reference contract parameters: if a sensor value falls outside the admissible range $t_{\text{sensor}} \in [t_{\text{min}}; t_{\text{max}}]$, a violation is registered.

3) **Cryptographic commitment.** In the event of a detected violation (e.g., temperature exceeding the permissible range or light sensor activation indicating tampering), the system generates a transaction containing a violation marker. Sensor readings and associated metadata may be stored in full within the Raspberry Pi memory for subsequent analysis and additional evidentiary support.

4) **Finalization.** Upon arrival at the destination, Node 1 submits a smart contract invocation transaction that updates the cargo status in the global ledger.

Experimental evaluation

As an experiment, an arbitrary cargo transportation scenario with predefined storage condition requirements was simulated. During the contract creation stage, the smart contract was configured with a set of permissible parameter ranges, which were subsequently transmitted to the Raspberry Pi device, as shown in Fig. 3.

As shown in Fig. 3, the following permissible ranges were defined: temperature from 20 to 35 °C, illumination from 700 to 1100 lux, and pressure from 900 to 1100 pascals.

During the monitoring process, the microservice detected a deviation in the illumination parameter (light), where the value dropped to 539 at a minimum allowable threshold of 700, as well as a temperature spike up to 40 °C.

```

root@ubuntu:/home/vboxuser/Desktop/Raspberry# ./script_download.sh
Rasb_serv.py script_download.sh test_script_serv.sh
root@ubuntu:/home/vboxuser/Desktop/Raspberry# ./script_download.sh
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total  Spent  Left  Speed
100  754  100  754    0    0   29000    0 --:--:-- --:--:-- --:--:-- 29000
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload  Total  Spent  Left  Speed
100  932  100  861  100    71  37434   3086 --:--:-- --:--:-- --:--:-- 42363
Sensor ranges from config:
temperature: 20.0 - 35.0
press: 900.0 - 1100.0
light: 700.0 - 1100.0

Server listening on port 55555
Waiting for sensor data...
-----
Received temperature: 32.0
Received light: 539.0
Received press: 1064.0
Received temperature: 40.0
Received light: 130.0
Received press: 1070.0

```

Fig. 3. Smart contract deployment and transmission of retrieved data to the Python service

```

    },
    {
      "type": "string",
      "value": "crash",
      "key": "integrity"
    }
  ]
}

```

Fig. 4. Updated cargo state in the blockchain ledger

The validation system automatically classified these events as a violation. The processing result was recorded on the blockchain via a smart contract invocation transaction. As shown in the ledger state dump presented in Fig. 4, the cargo integrity variable (*integrity*) was irreversibly set to “crash”.

Conclusion

The presented work proposes an architecture for an automated cargo transportation monitoring system based on blockchain technologies.

Main results:

1. The selection of the “Confident” platform is justified based on a comparative analysis (Hyperledger Fabric, Corda, Ethereum), taking into account technical characteristics and compliance with Russian cryptographic standards (GOST).
2. A three-layer architecture (initiator – mobile agent – auditor) is developed, featuring a clear separation of responsibilities and reduced network load through edge device data processing.
3. A prototype based on a Raspberry Pi single-board computer, simulating an onboard node, and the “Confident” platform was implemented and tested. The prototype confirmed the feasibility of scenarios including initialization, monitoring, violation detection, and the immutability of event recording.
4. Data immutability and transparency were achieved, providing an objective evidentiary basis for dispute resolution between supply chain participants.

Future research is aimed at developing a scalable solution for cargo monitoring, logistics automation, and integration with insurance companies and regulatory authorities.

REFERENCES

1. **Mukhamedova Z.G., Osadchuk V.D., Tulaev A.U.** Prospects for the use of blockchain technology in the organization of the transportation process and supply chain. *Journal of Transsib Railway Studies*, 2022, Vol. 50, No. 2, Pp. 142–156.
2. **Jun Chen, Shiyan Xu, Kaikai Liu, Shuqi Yao, Xiao Luo, Huan Wu.** Intelligent Transportation Logistics Optimal Warehouse Location Method Based on Internet of Things and Blockchain Technology. *Sensors*, 2022, Vol. 22, No. 4, Art. no. 1544. DOI: 10.3390/s22041544
3. **Slyadnikov P.E., Toutova N.V., Erokhin A.G.** Analysis of the problems and prospects of integrating blockchain in Internet of Things systems. *Online scientific journal "Age of Quality"*, 2025, Vol. 2, Pp. 1–16.
4. **Pavlikhin A.** The use of blockchain technology to track supply chains: from theory to practice. *Current Research*, 2023, Vol. 145, No. 15. DOI: 10.5281/zenodo.15648628
5. **Ergashov B., Turdieva G.** A study of digitalization and its impact on food safety and supply chain with modern technologies. *Universum*, 2024, Vol. 127, No. 10. [online] Available at: <https://7universum.com/ru/tech/archive/item/18408> [Accessed 17.09.2026]
6. **Kargopolov A.S., Kripak M.N., Kiyashko L.A.** Prospects and Possibilities Blockchain Technology Application in Logistics. *International Journal of Advanced Studies*, 2023, Vol. 13, No. 4, Pp. 205–217. DOI: 10.12731/2227-930X-2023-13-4-205-217
7. **Dlimi Z., Ezzati A., Ben Alla S.** A Lightweight Blockchain for IoT in Smart City (IoT-SmartChain). *Computers, Materials and Continua*, 2021, Vol. 69, No. 2. Pp. 2687–2703. DOI: 10.32604/cmc.2021.018942
8. Жизненный цикл смарт-контракта [Электронный ресурс] // bsmarted.com. URL: <https://bsmart-ed.com/ru/topics/soliditi/zhiznennyy-tsikl-smart-kontrakta> (дата обращения: 20.04.2026).
9. **Tregubov V.N.** Implementation of the Internet of Things and Blockchain Technologies in Autonomous Logistics. *Modern Information Technologies and IT-Education*, 2019, Vol. 15, No. 3, Pp. 782–790. DOI: 10.25559/SITITO.15.201903.782-790
10. **Fu Yongguang.** Coordination mechanisms for regional supply chains under the framework of eaeu and belt and road initiative coupling: the role of digital technologies. *Flagman nauki [Flagship of science]*, 2025, Vol. 33, No. 10, Pp. 1–5.
11. **Alzharni F., Saeedi K., Zhao L.** Architectural Patterns for Blockchain Systems and Application Design. *Applied Sciences*, 2023, Vol. 13, No. 20, Art. no. 11533. DOI: 10.3390/app132011533
12. **Jim Zhang.** Enterprise Blockchain Protocols: A Technical Analysis of Ethereum vs Fabric vs Corda. *Kaleido*, 2023. [online] Available at: <https://www.kaleido.io/blockchain-blog/enterprise-blockchain-protocols-a-technical-analysis-of-ethereum-vs-fabric-vs-corda> [Accessed 17.09.2026].
13. **Yi Li, Jinsong Wang, Hongwei Zhang.** A survey of state-of-the-art sharding blockchains: Models, components, and attack surfaces. *Journal of Network and Computer Applications*, 2023, Vol. 217, Art. no. 103686. DOI: 10.1016/j.jnca.2023.103686
14. **Bin Cao, Xuesong Wang, Weizheng Zhang, Houbing Song, Zhihan Lv.** A Many-Objective Optimization Model of Industrial Internet of Things Based on Private Blockchain. *IEEE Network*, 2020, Vol. 34, No. 5, Pp. 78–83. DOI: 10.1109/MNET.011.1900536
15. **Kim M., Kim K., Kim J.-H.** Cost Modeling for Analyzing Network Performance of IoT Protocols in Blockchain-Based IoT. *Human-centric Computing and Information Sciences*, 2021, Vol. 07, No. 11, Pp. 1–14. DOI: 10.22967/H CIS.2021.11.007
16. **Pomogalova A.V.** The Efficiency Assessment of the Blockchain Networks Adaptive Algorithm as Part of a Multi-Consensus System on Communication Networks. *Proceedings of Telecommunication Universities*, 2024, Vol. 10, No. 5, Pp. 34–42. DOI: 10.31854/1813-324X-2024-10-5-34-42
17. **Hang L., Kim D.-H.** Optimal blockchain network construction methodology based on analysis of configurable components for enhancing Hyperledger Fabric performance. *Blockchain: Research and Applications*, 2021, Vol. 2, No. 1, Art. no. 100009. DOI: 10.1016/j.bcra.2021.100009

18. **Poleshkina I.O., Vasilyeva N.V.** Use of blockchain technology as supply chain management system involving air transport. *Civil Aviation High Technologies*, 2020, Vol. 23, No. 2, Pp. 72–86. DOI: 10.26467/2079-0619-2020-23-2-72-86
19. **Osokina E.B., Zabolotskaya D.V.** Microcontroller system for monitoring the state of the cargo transportation environment. *Ekspluatatsiia morskogo transporta [Operation of marine transport]*, 2021, Vol. 99, No. 2, Pp. 156–161. DOI: 10.34046/aumsuomt99/23
20. **Pennino D., Pizzonia M., Vitaletti A., Zecchini M.** Blockchain as IoT Economy Enabler: A Review of Architectural Aspects. *Journal of Sensor and Actuator Networks*, 2022, Vol. 11, No. 2, Art. no. 20. DOI: 10.3390/jsan11020020
21. **Zabludn G.Iu., Tutova N.V., Sliadnikov P.E.** Dostizhenie otkazoustoichivosti v korporativnykh informatsionnykh sistemakh s pomoshch'iu algoritmov raspredelennoogo konsensusa [Achieving fault tolerance in enterprise information systems using distributed consensus algorithms.]. *REDS: Telekommunikatsionnye ustroystva i sistemy [REDS: Telecommunication Devices and Systems]*, 2025, Vol. 15, No. 2, Pp. 32–37.
22. **Toutova N.V., Gaeva A.P., Agamirov V.L., Agamirov L.V., Andreev I.A.** Blockchain in Education: A New Approach to Storing and Verification of Academic Works. *2024 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED)*, 2024, Pp. 1–4. DOI: 10.1109/TIRVED63561.2024.10769792
23. **Slyadnikov P., Toutova N., Erokhin A., Frolova E., Vanina M.** Modeling of Blockchain Systems in Internet of Things Networks. *2025 Systems of Signals Generating and Processing in the Field of On-Board Communications*, 2025, Pp. 1–4. DOI: 10.1109/IEEECONF64229.2025.10948109

INFORMATION ABOUT AUTHORS / СВЕДЕНИЯ ОБ АВТОРАХ

Levon V. Agamirov

Агамиров Левон Владимирович

E-mail: itno_agamirov@mail.ru

ORCID: <https://orcid.org/0009-0009-6909-9399>

Vladimir L. Agamirov

Агамиров Владимир Леонович

E-mail: avhere@yandex.ru

ORCID: <https://orcid.org/0000-0001-9181-7726>

Pavel E. Slyadnikov

Слядников Павел Евгеньевич

E-mail: p.e.slyadnikov@mtuci.ru

ORCID: <https://orcid.org/0009-0009-6284-515X>

Natalia V. Toutova

Тутова Наталья Владимировна

E-mail: e-natasha@mail.ru

ORCID: <https://orcid.org/0000-0002-2851-8472>

Anton Khaush

Хауш Антон

E-mail: anton.khaush@gmail.com

ORCID: <https://orcid.org/0009-0008-7929-5492>

Submitted: 20.05.2026; Approved: 16.07.2026; Accepted: 17.08.2026.

Поступила: 20.05.2026; Одобрена: 16.07.2026; Принята: 17.08.2026.