ORIGINAL ARTICLE
DOI: https://doi.org/10.30932/1992-3252-2024-22-4-4

World of Transport and Transportation, 2024,
Vol. 22, Iss. 4 (113), pp. 153–157

Analysis of the Operation of a Distributed Ledger: An Example of the Airport

Igor N. ROZENBERG

Iakov M. DALINGER

Igor N. Rozenberg [1], Iakov M. Dalinger [2]

[1, 2] Russian University of Transport, Moscow, Russia.
[1] ORCID: https://orcid.org/0000-0001-9589-6783; Web of Science Researcher ID: AAD-7632-2019; Scopus Author ID: 15136568900; Russian Science Citation Index SPIN-code: 2958-4186; Russian Science Citation Index Author ID: 652172.
[2] ORCID: https://orcid.org/0000-0002-7744-7156; Scopus Author ID: 57195278185; Russian Science Citation Index SPIN-code: 8895–3700; Russian Science Citation Index Author ID: 704687.
✉ *[2] iakovdalinger@gmail.com.*

ABSTRACT

Possibilities to use distributed ledger technology are shown referring to storing data in information systems of airports and aviation systems of various levels.

The features of the operation of a distributed ledger are noted regarding information systems. Various options for generating messages for storage using distributed ledger technology are studied along with the parameters of message flows. The features of using blockchain technology when creating distributed ledger are highlighted in case of the need to correct the stored information.

A possibility to use network technologies is shown for forming distributed ledger, the nodes of which are located at significant distances from each other (registries of several airports).

The provided data can be used to create reliable distributed information storage facilities, both within a separate airport and for a group of airports.

Keywords: distributed information system, distributed ledger, blockchain, information security, cryptographic protection, mathematical models, civil aviation, airports.

For citation: Rozenberg, I. N., Dalinger, Ia. M. Analysis of the Operation of a Distributed Ledger: An Example of the Airport. World of Transport and Transportation, 2024, Vol. 22, Iss. 4 (113), pp. 153–157. DOI: https://doi.org/10.30932/1992-3252-2024-22-4-4.

The original text of the article in Russian is published in the first part of the issue.
Текст статьи на русском языке публикуется в первой части данного выпуска.

BACKGROUND

Distributed ledger technology (often blockchain-based technology) is becoming increasingly popular in the creation of distributed information systems due to its features such as [1–6]:

• Distributed storage of copies, allowing simultaneous access to the ledger by many users in different geographic locations.

• Impossibility of making unauthorized changes to the created copies.

• High functional reliability of the ledger.

• Ability to control access to copies in the ledger.

• Coherence (full compliance) of copies in the ledger.

• Ability to unlimitedly expand the ledger's content.

This allows the use of distributed ledger technology to build specialised information systems for enterprises and their pools at the regional and federal levels[1].

The process of creating specialised information systems based on distributed ledgers and their operation differ significantly from the methods of creating and operating systems related to cryptocurrency, which must be considered when carrying out development.

The main differences are as follows:

• The absence of mining associated with the need to compete for the right to enter data into the ledger and for remuneration.

• Territorial localisation of copies of the distributed ledger (e.g., within a region, state, etc.).

• Compliance with legislative, industry and other regulations governing the processing of and access to information.

• The need to ensure the protection of information from specific threats associated with the functioning of the ledger, the properties of the stored information, access control (solving cybersecurity problems).

• The need to ensure access to the ledger for many users (administrators maintaining the ledger; users making requests to the ledger).

• The presence of special means of checking (validating) data entered into the ledger, depending on the purpose of the data.

• The presence of cryptographic means of data protection (encryption, hashing, authentication) [7–11].

Besides, ledger copies contain a large amount of different information structured in blocks, which requires the creation of means for searching and presenting it in a user-friendly form (ledger database).

All this determines the feasibility of creating methods for analysing distributed ledger variants, due to the specifics of its practical application.

Among the tasks of an organisation, an important place belongs to the tasks of forming a flow of data blocks to be recorded in the ledger.

The objective of the study is to analyse a possibility of using distributed ledger technology in creating distributed databases of information systems of airports and airlines of various levels.

The study used *methods* of system analysis, queue theory, probability theory, theory of computer networks and information systems.

RESULTS

Description of the Ledger

It is advisable to create a distributed ledger as a development of integrated distributed databases, when there is a set of information resources with established links, a system of queries and updates [12]. A possible option for organising a distributed ledger is considered for a case of a transport enterprise, for example, an airport, with the following characteristics:

1. A distributed ledger is created based on existing information resources and consists of a group of local data registries of individual airport divisions.

2. All local registries can be created in the form of blockchains – special data chains with the properties listed above [1; 2; 6; 11].

3. It is advisable to use blockchain technology in case where there are increased requirements for data security, but this creates significant difficulties with making changes to the stored data.

4. Each local registry is created for one or more airport divisions; information from local registries may overlap.

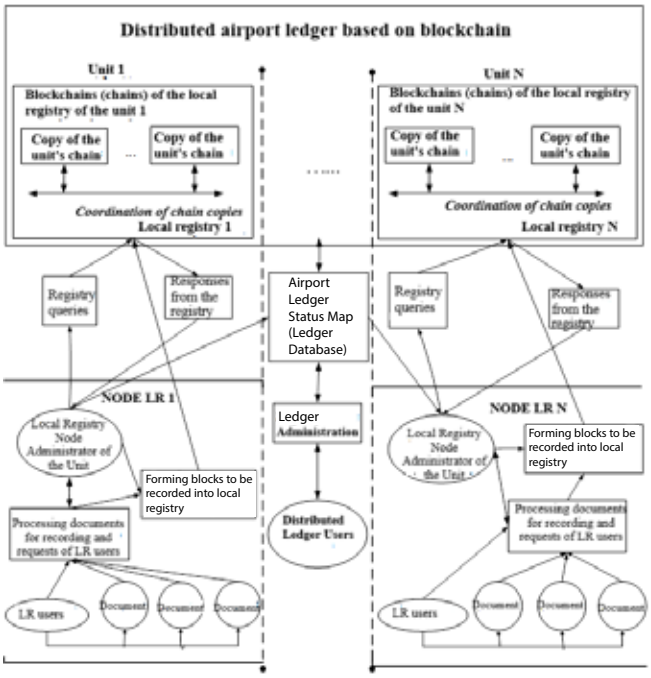
5. To enter records (blocks) into local registries, special workstations with the appropriate software are allocated, allowing for validation and reconciliation of data.

6. Copies of local registries are available to employees, registries' administrators of the relevant departments, who ensure their filling and registries' operation upon requests of airport employees and external organisations (registries' users).

7. The distributed ledger contains a map of local registries (ledger's database), where data for access to local registries upon requests is generated.

Working with the ledger consists of generating blocks of documents for recording, recording blocks and copies in local registries, processing requests to

[1] Spirkina, A. V. Development of a model for the application of distributed ledger systems and assessment of their impact on network characteristics. Ph.D. (Eng) thesis. St.Petersburg, SPbSUT publ., 2022, 186 p.



Pic. 1. Generalised structure of the airport distributed ledger [compiled by the authors].

the registry (searching for the required information, presenting the found information in the required form). The blocks generated for recording are checked (validated) for the absence of copies, the correctness of the recording and, after successful verification, are recorded according to the established rules in the local registry (blockchain) of the relevant department.

An example of a variant of the generalised structure of an airport's distributed ledger is shown in Pic. 1. In this case, local registries are created using blockchain technology.

It is possible to scale the structure for an air transport system that includes several aviation and auxiliary (servicing) enterprises.

Employees – administrators of local registries have the right to form blocks of documents to be recorded into their registries, process queries to registries.

Blocks consist of a finite number of documents that are processed in a given department (unit).

Each administrator forms blocks from a given set of documents available to him, so that the blocks of different administrators do not contain identical documents.

Documents can be formed during a unit's work, or come from external departments or organisations.

Before recording the created block into the local registry, it is validated, which consists of checking the correctness of the documents, checking the absence of identical documents in different blocks, checking the correctness of the data entry regarding the owner (creator) of the block.

For validation, the created block is sent to all employees – administrators of the local registry. The administrator who received the block checks it and sends a response with the results of the check to the address of the administrator who created the block.

If all the responses are collected and they are all positive, the administrator who created the block records it into his copy of the local registry.

If several administrators work with one and the same copy, then the recording occurs in the order established for them without drawing the recording right.

At specified times, the local registry copies are reconciliated.

It is possible to clarify the operations related to the specifics of an enterprise, for example, the use of document encryption, distribution of keys for processing blocks and documents, establishment of special rules for maintaining and agreeing on copies of the local registry.

To ensure the search for documents within the entire distributed ledger, a map of local registries of an institution is compiled. The map is a specialised database that stores information on the location of documents, data on block owners, data for generating queries to local registries.

To create and ensure the operation of local registries of the distributed ledger, hardware and software tools are created – nodes of local registries,

which can be considered as workstations of local registries' administrators [2; 3]. Data blocks for recording in the ledger are created on the nodes.

All nodes operate as part of the local network of the institution or a regional or local network.

The network must provide the ability to implement established access rights to nodes for employees of the institution, provide protection from unauthorised access to registries and ledger, protect communication channels, and ensure the localisation of the distributed ledger within the institution. There are various solutions to these problems, which have been thoroughly studied in the literature [8; 14; 15].

Mathematical Models of Local Registry Nodes

The creation of a distributed ledger requires solving series of problems and analysis, allowing to obtain numerical values of the characteristics of the distributed ledger operation depending on the parameters (intensity of the flow of queries to the ledger, intensity of the flow of documents to be entered into the ledger, duration of query processing in the ledger, structure and composition of ledger blocks):

• Analysis of the processes of forming document blocks on recording nodes in local registries.

• Analysis of the processes of recording blocks in blockchains of local registries and creating copies.

• Analysis of the processes of processing ledger users' queries.

To carry out the analysis, mathematical models with message absorption have been developed, presented in works [13; 16–18]. Several models allowing to study network structures are presented in work [14].

In this case, the absorption of elementary messages (documents) implies their formation into the blocks to be recorded in the ledger.

In the models, each document corresponds to an elementary message, and the process of forming a block of documents corresponds to the creation of a complex message (block) in systems with the absorption of elementary messages.

As a rule, the number of documents received for processing and storage is finite, therefore, as a node model, a system with a fixed composition of a complex message (block of documents) and a limited number of places for elementary messages (documents) waiting in queue was considered.

When creating the models, it was assumed that N document streams, elementary messages ($\infty > N \geq 1$) arrive at the node, and M blocks (complex messages) are formed from these messages. The rules for forming blocks on nodes are specified by the matrix $\mathbf{M} = \|m_{ij}\|$, where $m_{ij} \geq 0$ is the number of documents of a stream number j that are part of a block of type i ($i = 1, 2,\ldots, M$; $j = 1, 2,\ldots, N$) [19].

When forming the elements of the matrix **M**, it was assumed that the following conditions were met:

a) Documents of each stream can participate in the creation of blocks of only one type (sets of available documents are established for each employee and each department (unit) creates its own blocks and documents).

b) Each block includes at least one document.

There are possible options that are considered in mathematical models:

– The duration of a block formation is unlimited, and the formation ends when the required number of documents are received.

– The duration of block formation is limited.

– The number of documents in a block is a random value.

The loss of documents in the ledger is excluded by setting a sufficiently large number of places on the nodes for documents to wait for the formation of blocks in which they will be included.

Models for analysing options are presented in [13; 16–18; 20]. The models make it possible to additionally study the following options for the composition of the generated document blocks: a block is formed from documents of only one type (stream), the number of which is specified; a block is formed from documents of different streams, the number of documents of each stream is specified.

The use of mathematical models allows us to calculate the values of the ledger's characteristics that particularly include:

• Average duration of forming a block of documents to be recorded in the ledger.

• Average waiting time for a document to be recorded in the ledger.

• Average length of the documents' queue.

• Average time of recording a block in the ledger (when calculating this characteristic, the absence of competition for recording in the ledger (blockchain) is considered and the recording occurs according to the order established for the administrators' nodes).

The models allow us to vary parameters of the ledger (of the models, respectively) to find optimal or acceptable solutions in terms of the characteristic values. These parameters include:

• Block composition.

• Average duration of block formation.

• Acceptable length of the documents' queue.

• Number of administration nodes for the local registry.

Mathematical models of system analysis can be used to analyse the processes of creation and operation of a distributed ledger that operates without drawing the right to record the generated blocks (complex messages).

CONCLUSIONS

Distributed ledger technology and blockchain technology today occupy an important place in solving information security problems: ensuring integrity, protecting against data modification, access control, and data reconciliation.

A wide variety of practical applications where data is used requires the development and preliminary analysis of methods for creating data blocks for storage in the ledger, the structure and algorithms for the operation of distributed ledger nodes. To solve these problems, it is advisable to use mathematical modelling.

Data on the possible development and study of a distributed ledger based on blockchain for an airport can be scaled for the case of an air transport system, for regional air transportation management systems.

REFERENCES

1. Bashir, I. [Original title] Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained. Edition in Russian, transl. from English by Raitman, M. A. Moscow, DMK Press publ., 2019, 538 p. ISBN 978-5-97060-624-7.

2. Gorbunova M. V., Ometov A. Y., Komarov M. M., Bezzateev S. V. Survey of distributed ledger technology integration challenges. *Informatsionno-upravliaiushchie sistemy* [*Information and Control Systems*], 2020, No. 2, pp. 10–19 (In Russian). DOI: 10.31799/1684-8853-2020-2-10-19.

3. Nosirov, Z. A., Fomichev, V. M. Analysis of Blockchain Technology: Architectural Basics, Application Examples, Future Trends, Problems and Disadvantages. *Systems of Control, Communication and Security*, 2021, Iss. 2, pp. 37–75 (in Russian). DOI: 10.24412/2410-9916-2021-2-37-75.

4. Khan, N. FAST: A MapReduce Consensus for High Performance Blockchains. Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems. New York, NY, USA: Association for Computing Machinery, 2018, pp. 1–6. DOI: 10.1145/3282278.3282279.

5. Sadeghi, M., Mahmoudi, A., Deng, X. Adopting distributed ledger technology for the sustainable construction industry: evaluating the barriers using Ordinal Priority Approach. *Environmental Science and Pollution Research*, 2022, Vol. 29 (7), pp. 10495–10520. DOI: 10.1007/s11356-021-16376-y.

6. Sherman, A. T., Javani, F., Zhang, H., Golaszewski, E. On the Origins and Variations of Blockchain Technologies. *IEEE Security Privacy*, 2019, 17(1), pp.72–77. DOI: 10.1109/MSEC.2019.2893730.

7. Ryabko, B. Ya., Fionov, A. N. Cryptography in the information world [*Kriptografiya v informatsionnom mire*]. Moscow, Goryachaya liniya-Telekom publ., 2018, 300 p. ISBN: 978–5–9912–0729–4.

8. Stallings, W. Cryptography and Network Security. Principles and Practice. Edition in Russian, transl. from English. 2nd ed. Moscow, Williams publ., 2001, 672 p. ISBN: 5–8459–0185–5.

9. Tchmora, A. Modern applied cryptography [*Sovremennaya prikladnaya kriptografiya*]. Moscow, Gelios ARV publ., 2001, 256 p. ISBN: 5–85438–037–4.

10. Haber, S., Stornetta, W. S. How To Time-Stamp a Digital Document. *Journal of Criptology*, 1991, Vol. 3, Iss. 2, pp. 99–111. DOI: 10.1007/bf00196791.

11. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016. 336 p. ISBN: 978–0–691–17169–2.

12. Arsenyev, B. P., Yakovlev, S. A. Integration of distributed databases [*Integratsiya raspredelennykh baz dannykh*]. St. Petersburg, Lan publ., 2001, 464 p. ISBN: 5–8114–0300–3.

13. Pankov, K. N., Saksonov, E. A. Using Probabilistic Methods in the Analysis of Information Security of Distributed Ledger Systems. In: 2021 Systems of Signals Generating and Processing in the Field of on Board Communications, Moscow, Russia. Institute of Electrical and Electronics Engineers Inc., 2021. DOI: 10.1109/IEEECONF51389.2021.9416006.

14. Vishnevsky, V. M. Theoretical foundations of designing computer networks [*Teoreticheskie osnovy proektirovaniya kompyuternykh setei*]. Moscow, Tekhnosfera publ., 2003, 512 p. ISBN: 5–94836–011–3.

15. Tanenbaum, A. S., Van Steen, M. Distributed Systems: Principles and Paradigms. Edition in Russian. St. Petersburg, Piter publ., 2003, 877 p. ISBN: 5–272–00053–6.

16. Dalinger, Ia. M. Analysis of Complex Messages Flows in Information Processing Systems. *Vestnik TOGU*, 2015, Iss. 1 (36), pp. 59–64. EDN: TPTDKD.

17. Dalinger, Ya. M., Leokhin, Yu. L., Saksonov E. A. The Model of the Processing Node with the Data Absorption. Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, Belarus, 2018, pp. 193–197. DOI: 10.1109/SYNCHROINFO.2018.8457008.

18. Saksonov, E. A., Leokhin, Yu. L., Dalinger, Ya. M. The Model of the Processing Node with the Data Replication. Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Minsk, Belarus, 2018, pp. 564–568. DOI: 10.1109/SYNCHROINFO.2018.8457025.

19. Dalinger, I. M. Analysis of data streams in systems with message absorption [*Analiz potokov dannykh v systemakh s pogloscheniem soobscheniy*] Informatics and Control Systems, 2012, No. 3, pp. 26–34. [Electronic version of the journal]: https://ics.togudv.ru/media/2012/ N33_03_1.pdf. Last accessed 23.08.2024.

20. Maull, R., Godsiff, Ph., Mulligan, C., Brown, A., Kewell, B. Distributed ledger technology: Applications and implications. FINRA, 2017, Vol. 26, Iss. 5, pp. 481–489. DOI: 10.1002/jsc.2148 [access for subscribers]. ●

Information about the authors:

Rozenberg, Igor N., *D.Sc. (Eng), Professor, Corresponding Member of the Russian Academy of Sciences, Chief Scientific Officer of Russian University of Transport, Moscow, Russia, tu@miit.ru.*

Dalinger, Iakov M., *Ph.D. (Eng), Vice-Rector of the Scientific and Educational Center for Air Transport of Russian University of Transport, Moscow, Russia, iakovdalinger@gmail.com.*

Article received 16.08.2024, approved after reviewing 16.09.2024, accepted 25.09.2024.