Pharmaceutical Audit Trail Blockchain-Based Microservice

Stefano Loss[1], Lucas Cardoso[2], Nélio Cacho[1] and Frederico Lopes[2]
[1]*Department of Informatics and Applied Mathematics, Federal University of Rio Grande do Norte, Natal-RN, Brazil*
[2]*Metropole Digital Institute, Federal University of Rio Grande do Norte, Natal, Rio Grande do Norte, Brazil*

Keywords: Pharmaceutical Systems, Auditing, Audit Trail, Blockchain, Immutability.

Abstract: Pharmaceutical manufacturing in Brazil requires that its processes are carried out by following rules defined by a supervisory body: the National Health Surveillance Agency (ANVISA, in Portuguese). ANVISA requires that all pharmaceutical systems guarantee all product information's integrity, security, and traceability. These rules ensure that the manufactured products do not pose a risk to their consumers. One of the difficulties for pharmaceutical industries is to provide evidence that production procedures were carried out under internal regulations based on these rules. One way to do this is by using an audit trail. It can store this information automatically using a computer system to record all actions. However, only using audit trails does not guarantee data security; ensuring that all information is immutable is necessary. Therefore, in this paper, we propose an audit trail blockchain-based microservice. This technology stores all transactions in linked and encrypted blocks to avoid illegal modifications. It also guarantees data immutability, security, and traceability. In addition, we present a case study to evaluate the proposed approach using Nuplam's (Nucleus for Research in Food and Medicines) Integrated Management Systems. A stress test was performed in this case study to evaluate the applicability of the proposed solution in pharmaceutical systems.

1 INTRODUCTION

The use of medicinal products made from plants, animals, or minerals has existed since ancient times. According to (Dailey, 2018), there are historical records of civilizations that performed this practice, such as the herbal compendium written by Emperor Shen Nong in China in 100 BC. While the pharmaceutical industry, as it is known today, began to develop in the mid-19th century, according to (Daemmrich and Bowden, 2005). As a result of the emergence of these drugs, it was possible to observe an improvement in birth and mortality rates.

In this evolution, the rigor of regulations and bureaucracies was increased. In this way, bodies responsible for supervising and guaranteeing the quality of the medicines produced were established and strengthened. Among these bodies are the *Food and Drug Administration* (FDA)[1] in the USA founded in 1906 and Brazil's National Health Surveillance Agency (ANVISA) in 1999[2]. ANVISA is also responsible for regulating and inspecting computer systems used by pharmaceutical companies to manage the production of medicines. It defines standards based on normative resolutions and instructions to be complied with by all drug manufacturers.

However, the scenario of advances in systematization and access improvements also takes time and effort. ANVISA also requires all its systems to undergo systematic testing and verification of industry documentation, a complex activity called validating computerized data. One of the requirements of regulatory bodies is to ensure data integrity, and all information must be traceable and immutable. ANVISA must know who took such action, when and for what reason. Through these requirements, the development process becomes more complex and complete.

In this way, it is necessary to record information about every stage in the production process. However, relying only on tools that need manual input of this information to perform the recording is unreliable. An individual may need to remember to write down some data or make mistakes during writing. Therefore, a system capable of automatically storing this data is necessary to guarantee the registry's integrity.

In addition, it is also necessary to ensure that every piece of information is immutable and not to compromise the integrity of the whole record. The data must

[1]https://www.fda.gov/

[2]https://www2.camara.leg.br/legin/fed/lei/1999/lei-9782-26-janeiro-1999-344896-publicacaooriginal-1-pl.html

Loss, S., Cardoso, L., Cacho, N. and Lopes, F.
Pharmaceutical Audit Trail Blockchain-Based Microservice.
DOI: 10.5220/0011685100003414
In *Proceedings of the 16th International Joint Conference on Biomedical Engineering Systems and Technologies (BIOSTEC 2023) - Volume 5: HEALTHINF*, pages 368-375
ISBN: 978-989-758-631-6; ISSN: 2184-4305

remain consistent with the values expected by production. This system must also be able to provide traceable data for external ANVISA audits, for example.

One of the ways to automatically record medicines production information is to use an audit trail in which the system capture and automatically stores the creations, updates, or deletions of information from all records to be audited. It assists in reconstructing events chronologically of the recorded information to facilitate auditing.

However, using the audit trail alone does not guarantee that this data is immutable. Since people with direct access to the database can easily modify some records to circumvent some information. The modification usually happens because the data is located in one place (database) in an isolated way where editing one segment of information does not affect the others.

Therefore, blockchain technology can be integrated with audit trail components, allowing secure and reliable auditing through systems. Since the properties provided by the blockchain's nature can improve the system's management and security (Berdik et al., 2021). Therefore, with this integration, it is possible to share data transparently, securely, and reliably without centralizing entities.

Hence, this work presents an innovative solution to register medicines production information using an audit trail blockchain-based microservice. With this microservice, all data is shared to facilitate the auditing process in an immutable, secure, and traceable way. In this context, the contributions of this paper are threefold. First, we present the key concepts to understand this work better (Section 2). Second, a novel pharmaceutical audit trail blockchain-based microservice is introduced in Section 4. Third, related works are described in Section 3.

Afterward, we describe a Case Study involving two pharmaceutical systems controlling the production of Nuplam drugs that would benefit from the proposed solution (Section 5). In addition, we present an architecture to facilitate the audit process involving possible control bodies such as ANVISA and the Ministry of Health. Finally, We evaluate our proposed approaches through a stress test (Section 5).

2 BACKGROUND

2.1 Audit Trail

The audit is "an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes." according to *Institute of Internal Auditors* [3]

The pharmaceutical audit is usually called a "quality audit" falling into the regulatory type. Therefore, the bodies responsible for its execution require the companies inspected to comply with specific regulations. The companies establish these regulations based on standards created by the auditing body, aiming for better final product quality. The body responsible for this regulatory audit in Brazil is ANVISA, which regularly audits pharmaceutical laboratories.

Meanwhile, an audit trail is a process that captures creations, updates, or deletions of information from all records to be audited. This track can be stored either on paper or electronically. It assists in reconstructing events chronologically of the recorded four essential questions (who, what, when, why) to register the main corresponding modification details (Ahmad et al., 2019).

An automated electronic or computerized audit trail eliminates human intervention, reducing the chances of a registration failure and guaranteeing the recording of all information that passes through the system. The FDA, in 2003, recommended its use for companies in the field. This recommendation in which this regulatory body describes the importance of applying some historical information recording tools within a pharmaceutical company, highlighting the audit trail.

However, maintaining an audit trail fulfilling the requirements is complex. In (RANA, 2021), the difficulties encountered in maintaining and managing an audit trail are mentioned. One of these is the increase in storage costs resulting from the eventual large amount of records generated in the life cycle of a track in a computer system. In addition, there is usually no defined period after which this data would no longer need to be kept.

2.2 Blockchain

Appearing in 2008, in the work of an unknown author with the pseudonym Satoshi Nakamoto (Nakamoto, 2008), blockchain technology was initially developed to create a secure and decentralized environment in which it was possible to carry out Bitcoin virtual currency transactions. A blockchain has four main components, which allow its operation and guarantee its transactions' immutability, auditing, and security. According (Puthal et al., 2018), the blockchain's main

[3]https://www.theiia.org/en/about-us/about-internal-audit/

components are the distributed ledger, cryptography, the consensus algorithm, and the transactions.

The **distributed ledger** is the component responsible for recording **transactions** in a chronological and sequentially dependent way and all the information entered in the network. This ledger is structured in a chain of sequential blocks, which store the transactions carried out on the network and are connected through a digital signature generated by **cryptography**. In this chain, the blocks are sequentially inserted, in which the last one represents the most recent transactions. For each new block, this signature is generated based on the immediately previous block, its transactions, and the creation instant (timestamp).

Blockchain transactions are based on exchanging information between network nodes in a Peer-to-Peer (P2P) manner. The P2P concept defines that several nodes form a blockchain network, each storing a copy of the ledger with all the information that has passed through it (Puthal et al., 2018). In this way, all network nodes are responsible for storing and managing network transactions. Regarding its structure, a blockchain transaction is contained within blocks. Each block can contain one or more transactions and use them to generate its signature. Each transaction on a blockchain network corresponds to the state of information on the network, which may represent data creation, update, or deletion.

Lastly, the **consensus algorithm** is responsible for assuring the immutability of blockchain information along with the ledger. This mechanism ensures the security of network data through decision-making techniques used to choose which data is valid in a blockchain. This technique uses P2P characteristics where all network nodes maintain a copy of the ledger. Therefore, it is possible to decide through consensus, involving most network nodes, which data are correct and discard erroneous data.

2.3 Orthus

Orthus is a blockchain platform to provide interoperability between systems by securely sharing information in the Smart Cities context (Loss et al., 2019). It enables the creation of solutions in distributed networks to share data and services in a transparent, secure, and reliable way without centralizing entities. The Orthus architecture comprises Java Actor classes implemented using the Akka toolkit[4] focused ins scalability and uses a Broker for indirect communication between all nodes.

Each system must implement the Orthus component to be part of the network. Orthus components are instantiated once for each system, and this association (System + Orthus components) is called a node. Communication between a system and the Orthus Gateway component occurs through REST requests. The Orthus network is comprised of distributed nodes and a network of brokers that enables data exchange, in the form of contextual elements, by sharing transactions and blocks that were created by one of the nodes and validated by all.

[4]https://akka.io/

3 RELATED WORKS

Many other solutions in different contexts have used audit trails to store data. In the health area, the article written by (Rostad and Edsberg, 2006), in which an analysis of the audit trail generated by an electronic patient record system is performed. Based on this analysis, this article tries to improve this system's role-based access control model by reducing exceptional situations in which it is necessary to access the system with administrator permission.

Another article in this area is (Cruz-Correia et al., 2013), in which the authors gather information from audit trails implemented in four Portuguese hospitals to analyze them. They performed records evaluations based on the audit trail's completeness, comprehensibility, and traceability standards. In addition, they interviewed the members of these hospitals to find out if they were adequately consulting the audit trail.

The legal area paper (Allinson, 2001) researches the use of audit trails by Australian security forces as evidence for legal cases. It explains that these forces have a legal obligation to keep all information an information system generates in an audit log.

After analysis, it is essential for an audit trail that its information is readable and secure. The authors highlight the importance of having a well-implemented path for reconstructing the processes carried out within the system. Furthermore, in the works of (Cruz-Correia et al., 2013) and (Allinson, 2001), it is possible to observe how neglected the audit trail is in the hospitals and security forces.

Still, in the research on audit trails, blockchain technology has much to offer in this area. In particular, in the paper written by (Abreu et al., 2018), the possibilities brought by the usage of blockchain in audit trails are explored. Some companies that developed products trying to integrate both concepts are in it. Beyond that, this paper introduces other computer-based assisting tools for auditing and exposes some of the authors' thoughts on how to make blockchain technology more accepted by the populace.

Another related work in which an audit trail ap-

plication based on private blockchain was developed, called by the authors *BlockTrail*, (Ahmad et al., 2019). This article focused on implementing a blockchain in which it was structured hierarchically to reduce the retrieval time of its information. This work proposed the blockchain implemented to be of the private type. It is necessary to know all network users, as they may need to be held legally responsible for any errors recorded in the audit trail.

Apart from the previous ones, another blockchain-based solution found while searching the literature was an article in which a private blockchain network was designed and implemented to ensure the security and reliability of an audit trail for configuring technical manufacturing components (Regueiro et al., 2021).

This literature review concluded that a blockchain-based audit trail is also suitable for laboratory situations, as it allows the control of writing data. This control is relevant because organizations that may have access to the track for viewing should not be able to enter data into the blockchain network. In addition, if the amount of information recorded eventually becomes too large, it will be possible to limit the access of users who do not perform actions relevant to ANVISA's audit, such as purchasing office supplies.

4 AUDIT TRAIL MICROSERVICE

The auditing microservice studied in this article has an architecture, as depicted in Figure 1, with a structure composed of six core components: a controller, a service, a model, a repository, a consumer, and a supplier. Besides them, there are three other auxiliary ones: a blockchain adapter, a report template, and a report builder.

These core components work as their names indicate: the controller works as the REST API; the service handles the business logic; the model defines data structure; the repository connects to the database; the consumer and supplier both control the data flow to a broker.

Within this architecture, the controller and the consumer/supplier handle two different kinds of data flows. On the one hand, the controller is used to communicate with an external application; for example, one reads the information from the microservice. In this case, this application would use the available API GET routes to access the auditing information recorded in the microservice and display it to a user.

On the other hand, the consumers and suppliers handle the communication with the integrated systems. These brokers handle this communication by organizing the flow of information between the integrated members. This architecture's service and the repository have no special functions besides what they would usually have. The service helps connect all components while maintaining an appropriate business logic, and the repository serves as an internal database representation.

The audit object model, in this microservice, defines the structure with which the transaction information has to conform to be accepted. According to the structure defined in this case, the model needs to have: an object identifier (ID) to track the transaction; a *revision*, to maintain the timeline information through versioning; the user responsible for a transaction; the name of the integrated service that sent the transaction; the operation type (create, update or delete); the name of the entity modified by the operation; the current state of the object, with the modifications; a timestamp of the transaction to know when it happened. All this structure is depicted in Figure 1.

Regarding the auxiliary components, the blockchain adapter converts the transaction data handled by the microservice to a format readable by the integrated blockchain. The report template is composed of a set of fixed phrase molds to be filled with the transaction information to convert it into a readable form. At the same time, the report builder is responsible for correctly filling these template phrases with the information.

Figure 2 depicts, in a superficial manner, the path a transaction goes through in this architecture. The transaction path starts from the integrated system and into the microservice via a broker until it reaches the blockchain and returns a status result message regarding its completion.

.

5 CASE STUDY - NUPLAM

The Nucleus for Research in Food and Medicines (Nuplam, in Portuguese)[5] is a chemical and pharmaceutical laboratory within the Federal University of Rio Grande do Norte (UFRN). Nuplam has, among its competencies, to research, develop and produce medicines for the Brazilian Ministry of Health (MS), supplying medicines throughout Brazil.

One of the most challenging factors for Nuplam is to record all events throughout the medicine's life cycle using SigNuplam and OPDigital. This cycle begins with the arrival of raw materials, goes through production, and ends with the delivery to the Ministry

[5]https://Nuplam.ufrn.br/pagina.php?a=historia

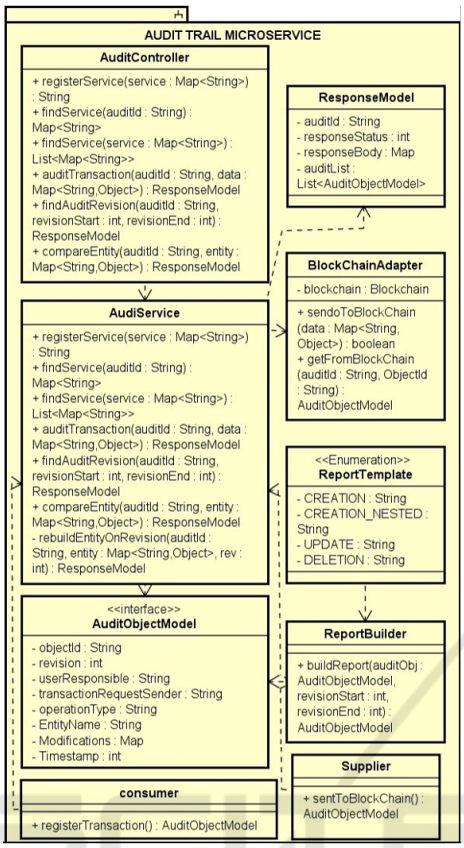

Figure 1: Class Diagram of Audit Trail Microservice.

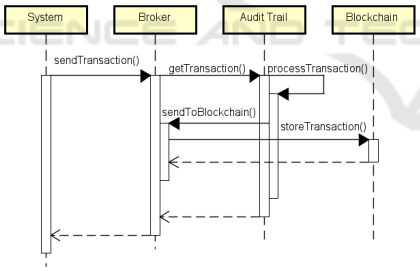

Figure 2: Sequence Diagram of Audit Trail Microservice.

of Health. This process involves different entities, and at each step, all historical data must be recorded in immutable, secure, and audit ways complying with the regulations established by ANVISA.

To better fulfill the ANVISA requirements, Nuplam developed its computerized systems to manage its internal procedures. This decision was influenced by advances in the Information Technology (IT) sector at UFRN that resulted in the development of an Integrated Management System for the Nuplam (SigNuplam) and a system for controlling Nuplam medicines production (OPDigital).

All information systems developed within the pharmaceutical context are regulated by the National Health Surveillance Agency (Anvisa). The systems must undergo systematic testing processes and verification of industry documentation, a complex activity called Computerized Data Validation, which requires the creation of a specific sector to carry out these checkings.

The ANVISA requirements for this system are diverse and must guarantee the data's integrity, security, and traceability. In other words, in addition to people who cannot access them improperly, we must also know who took which action and for what reason. Through these requirements, the development process becomes even more complete and complex.

5.1 SigNuplam

SigNuplam[6] is an Enterprise Resource Planning (ERP) developed and implemented following ANVISA regulations. This web system must ensure that all access points are via the Local Area Network (LAN) within NUPLAM, including wi-fi. It guarantees that all laboratory employees with internal access to a computer can access and use the system only if they are registered.

SigNuplam was initially developed in modules that sought to replicate Nuplam's physical organization in departments, each with specific needs. In this way, the laboratory departments corresponding modules were developed into seven modules: 1) Documents of Quality; 2) Quality Assurance; 3) Maintenance Management; 4) Logistics; 5) Purchases and Contracts; 6) Human Resources Management; 7) Support.

In this way, SigNuplam also needs all module information to be recorded securely and audited. The audit trail can store this information automatically using a computer system to record all actions taken while manufacturing medicines, helping to provide evidence.

5.2 OPDigital

OPDigital is a mobile app that aims to monitor all stages of drug production lines. While executing the steps, this system automates filing a production order document. This document contains the rules and steps of the drug production line that operators must confirm during production. These operators fill in real time using tablets running OPDigital to add photos and a description of the fulfillment of the steps of these activities.

In addition to facilitating the filling of production orders, this system also facilitates real-time monitor-

[6]https://pluni.imd.ufrn.br/pluni/30/visualizarProduto

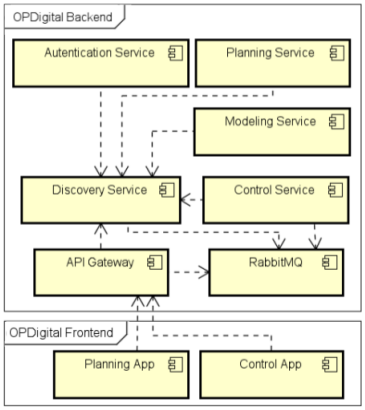

Figure 3: OPDigital Architecture.

ing of the execution of these orders by those responsible for this department. OPDigital is also responsible for generating reports from other Nuplam departments (e.g., Logistics, Quality Control) and for inspection by ANVISA.

OPDigital was implemented following the microservice architecture style. As shown in Figure 3, OPDgital architecture is divided into two packages: *back-end* and *front-end*. The *front-end* contains the *Planning App* and *Control App*. These apps use an API Gateway to integrate to *back-end*.

Discovery Service works as a microservice orchestrator to organize the execution of the requests that use a broker to interact with other microservices. At the same time, as detailed above, *Control* and *Planning* Services are responsible for the Nuplam production line.

Like SigNuplam, OPDigital also requires that all drug production line information be securely recorded and audited. The audit trail can automatically store this information helping to provide evidence and facilitate the audit.

5.3 Case Study Architecture

Aiming to implement this blockchain in the SigNuplam and OPDigital audit trail, it was necessary to define how its main components will be used in this case. Starting with the encryption implemented using the asymmetric public and private keys method. Every user registered in SigNuplam or OPDigital will receive a private key that will be used to sign transactions while keeping its content transparent. This key will be managed on the SigNuplam server using the user's existing credentials to access different machines.

Regarding the ledger, all transactions carried out through SigNuplam or OPDigital will be stored after verification of the user's signature. These transactions

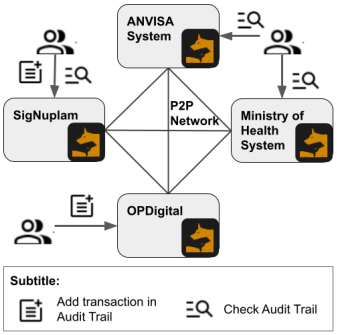

Figure 4: Case Study Blockchain Integration.

will be replicated to all nodes on the network. After applying a consensus mechanism, such transactions are grouped, forming a block inserted into the ledger and sent to all network nodes.

There are several consensus mechanisms, and the choice depends on the blockchain implementation used. The blockchain used in this case study is Orthus, described in Section 1. The rationale of this choice is that Orthus uses a Broker to receive the requests and is focused on scalability with high throughput (transaction per second). Regarding the chosen broker, RabbitMQ[7] was chosen since it was already used in implementing OPDigital and supported by Orthus. The only integration difficulty would be with SigNuplam since this system did not use this broker.

As Orthus is a private blockchain type, a less expensive algorithm can be used as there is confident trust in the network participants. In this way, Byzantine algorithms can be used, in which consensus is achieved through the election of a reliable leader who generates the block. This block is checked by all other nodes and accepted if considered valid by more than two-thirds (Lamport et al., 2019).

Participants in the proposed blockchain network for this case study, besides SigNuplam and OPDigital, must include at least two or more organizations, such as ANVISA and the Ministry of Health. These two other network members will be allowed to view the audit trail, thus being able to audit the transactions. This network structure is exemplified in Figure 4.

Figure 5 describes the flow followed by a transaction performed by a network user. When using SigNuplam, all modification actions a user performs through the system will be sent to all network nodes and gathered in blocks. Then, a node will be chosen to close the block and send it to the others to be validated by the consensus mechanism. After validation, the block is inserted into the chain of all system nodes and becomes immutable.

[7]https://www.rabbitmq.com/

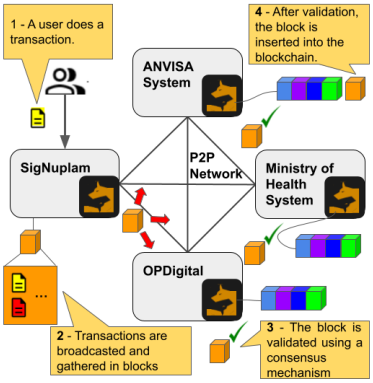

Figure 5: Flow of insertion of transactions in blockchain from the SigNuplam trail.

Although blockchain brings advantages in security and auditing to the audit trail, there are also some disadvantages. The cryptography and the consensus mechanism increase the processing time needed to record new information. In addition, another disadvantage, querying an ancient track record can take a long time due to the use of the blockchain structure.

However, comparing the disadvantages with the blockchain's benefits, the increased data immutability, transaction transparency, and the security of block information can overcome the disadvantage of direct access to a database. It ensures that the audit trail serves for a regulatory audit, such as ANVISA.

5.4 Systems Integration

Integrating the audit trail microservice with the existing SigNuplam was done using the concept of Aspect Oriented Programming (AOP) inside Spring's library [8]. An Aspect class was implemented to intercept the system's transactions and send them to the RabbitMQ and the microservice.

This class watches over all methods responsible for sending data to the database. Upon noticing any save, update or delete operation, it would first send the data to the RabbitMQ before continuing with the normal flow asynchronously. Using an Aspect class was a choice because it would not warrant refactoring the existing code in SigNuplam. While using an asynchronous flow was chosen to not generate unnecessary bottlenecks from the microservice or blockchain response time.

As OPDigital uses an orchestrated microservice architecture, every request information has to go through a conductor, which is the *DiscoveryService*. The integration between this system and the audit microservice is done by the conductor using the information coming back from other microservices concerning saving, updating, or deleting operations. This information is then sent by it to RabbitMQ on the topic listened to by the audit microservice.

6 CASE STUDY EVALUATION

In order to assess the proposed microservice, a stress test against the implemented case study was performed. The proposed solution aims to simulate these systems' usage daily, where all operations should be registered. Therefore, this test will determine the maximum request number of simultaneous users this solution supports.

6.1 Test Environment

The 2vCPU, 4GB RAM, and Ubuntu 18.04.2 LTS virtual machines in the cloud were used to deploy and simulate the proposed solution in a distributed way. Four Audit Trail Microservice were deployed according to the case study using Docker Compose[9] to configure and create containers of the components of the microservice and besides Orthus.

After that, Apache JMeter[10] was used as a load testing tool for measuring and analyzing the solution's performance for this test running outside the cloud. The requisitions simulate a high number of simultaneous requests.

6.2 Test Results

For these tests, it has been configured to reach up to 500 instances. After this test, the average time of each requisition for the different scenarios (10, 50, 100, and 500 users) was analyzed.

Table 1: JMeter Summary Report Table (in milliseconds).

Users	Samples	Avg.	Min	Max	Deviation	Throughput
10	300	26	8	295	28.56	113.2/sec
50	1,500	77	6	681	97.75	208.1/sec
100	3,000	107	4	645	96.26	230.7/sec
500	15,000	246	4	1446	217.99	497.7/sec

Table 1 shows the number of simultaneous users, number of samples, average time (in milliseconds), minimum time, maximum time, standard deviation, and throughput (transaction per second) of each test. It is essential to highlight the average response time for each request to create a transaction; for 10, 50, 100, and 500 concurrent users. In this table, it is

[8]https://docs.spring.io/spring-framework/docs/4.3.15.RELEASE/spring-framework-reference/html/aop.html

[9]https://docs.docker.com/compose/

[10]https://jmeter.apache.org/

possible to notice that the throughput gets proportionally smaller with increased users. It starts at about 11 times bigger than the number of users, counting down to a little below one time.

Still, in Table 1, it is not shown that the error percentage is 0% in the first three entries. While in the fourth, it reaches 12.39%. This fact shows that between 100 and 500 simultaneous users, there is a moment (probably close to the 250) when the server cannot keep up with the requests. It is also perceptible that the throughput has reached a threshold.

On the upside, that auditing system was developed in a factory with few employees. Besides that, the PCs would not all be used simultaneously through most of the expedient. From these circumstances, it is possible to conclude that this microservice will be able to show its best performance most of the time.

7 CONCLUSIONS

This paper presented a pharmaceutical audit trail blockchain-based microservice intending to store all pharmaceutical system operations with integrity, security, and traceability besides facilitating the audit process. Using this proposed microservice, any pharmaceutical system can automatically register and share its operations within a blockchain. This information sharing can facilitate the audit process by the competent bodies and prevent possible fraud by ensuring the immutability of data stored on the blockchain.

Moreover, we presented a case study involving two systems related to medicine production (SigNuplam and OPDigital) and two supervision systems (ANVISA and the Ministry of Health). This scenario was used to evaluate the proposed solution through load testing. In this test, an increasing number of simultaneous users was simulated, making requests in the system that should be registered in the blockchain through the proposed solution.

From the results, it is perceptible that the audit trail microservice can handle at least 100 to 200 simultaneous users without any data loss and with good throughput. Therefore, it can be used in small or medium-sized companies with around that amount of simultaneous users.

In future works, the search for specific information within the blockchain must be analyzed, considering the performance (time required), since the information is stored in a chained and chronological way and tends to increase over time. Another factor to consider is the readability of the audit trail during the audit process.

ACKNOWLEDGEMENTS

This work is supported by the Nuplam[11] and Smart Metropolis Lab[12].

REFERENCES

Abreu, P. W., Aparicio, M., and Costa, C. J. (2018). Blockchain technology in the auditing environment. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6. IEEE.

Ahmad, A., Saad, M., Njilla, L., Kamhoua, C., Bassiouni, M., and Mohaisen, A. (2019). Blocktrail: A scalable multichain solution for blockchain-based audit trails. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE.

Allinson, C. (2001). Information systems audit trails in legal proceedings as evidence. *Computers & Security*, 20(5):409–421.

Berdik, D., Otoum, S., Schmidt, N., Porter, D., and Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, 58(1):102397.

Cruz-Correia, R., Boldt, I., Lapão, L., Santos-Pereira, C., Rodrigues, P. P., Ferreira, A. M., and Freitas, A. (2013). Analysis of the quality of hospital information systems audit trails. *BMC medical informatics and decision making*, 13(1):1–10.

Daemmrich, A. and Bowden, M. E. (2005). Emergence of pharmaceutical science and industry: 1870–1930. *Chem Eng News*, 83.

Dailey, J. W. (2018). Pharmaceutical industry. *Encyclopedia Britannica*.

Lamport, L., Shostak, R., and Pease, M. (2019). The byzantine generals problem. In *Concurrency: the works of leslie lamport*, pages 203–226.

Loss, S., Cacho, N., Lopes, F., and Valle, J. M. (2019). Orthus: A blockchain platform for smart cities. In *Proceedings of IEEE International Smart Cities Conference ISC2 2019*. IEEE.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260.

Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., and Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine*, 7(4):6–14.

RANA, K. (2021). How audit trail can lead to increased compliance and transparency. *The Economic Times*.

Regueiro, C., Seco, I., Gutiérrez-Agüero, I., Urquizu, B., and Mansell, J. (2021). A blockchain-based audit trail mechanism: Design and implementation. *Algorithms*, 14(12):341.

Rostad, L. and Edsberg, O. (2006). A study of access control requirements for healthcare systems based on audit trails from access logs. In *2006 22nd Annual Computer Security Applications Conference (ACSAC'06)*, pages 175–186. IEEE.

[11] https://nuplam.ufrn.br/

[12] https://smartmetropolis.imd.ufrn.br