Towards a Blockchain Architecture for Animal Sanitary Control

Glenio Descovi[1], Vinícius Maran[3], Denilson Ebling[2] and Alencar Machado[1,2]
[1]*Technology Center, Federal University of Santa Maria, Santa Maria, Brazil*
[2]*Polytechnic College, Federal University of Santa Maria, Brazil*
[3]*Laboratory of Ubiquitous, Mobile and Applied Computing (LUMAC), Federal University of Santa Maria,*

Keywords: Animal Sanitary Control, Epidemiology, Blockchain, Consensus Algorithms.

Abstract: It is known that Blockchain technology is widely used in cryptocurrency transactions, the technology has become popular with Bitcoin but recently, it has been applied in many areas, including the animal sanitary control. It can be said that Blockchain is an immutable ledger, where systems can store transactions, documents, history, countless data generated in any process. In Brazil, an animal sanitary control platform called Plataforma de Defesa Sanitaria Animal (PDSA-RS) was recently proposed and is widely used in the state of Rio Grande do Sul. Actually, the PDSA-RS uses a centered server with relevant information for the animal sanitary control process. This work presents the process of defining and integrating the PDSA-RS with a private Blockchain managed by a software architecture. The main goal of this integration is to give traceability, immutability and transparency in the existing process and the data generated in the certification of poultry establishments that are part of the animal sanitary control. In the evaluation of the integration process, it was possible to observe that it the blockchain extension offered persistence, anonymity and auditability of the information related to the animal sanitary control.

1 INTRODUCTION

Blockchain recently attracted attention from industry and academia, becoming popular with cryptocurrencies, specifically Bitcoin (Kosba et al., 2016). Blockchain is on the rise, where it is not only being applied to cryptocurrency transactions, but also in other areas, such as document management, as it is versatile and has numerous applications. Its characteristics, such as security, immutability, transparency, make it a great tool for managing and auditing information. Due to this growth in applications involving Blockchain technology, there has been a huge growth in demand for blockchain engineers in recent years.

The technology was developed to solve some problems that have existed for some time, such as, reliability of transactions (banking or not), immutability of information, that is, permanent (the data informed will never change), document management, a single repository of information, among others (Zheng et al., 2018), implemented in a network distributed in public blockchains and in a single network in private blockchain. However, some problems arise as vulnerabilities and scalability according to the amount of information contained in it.

The epidemiological control of diseases has problems that the Blockchain usage fits to solve. There is great importance in the epidemiological control of diseases worldwide, which was even more evident with COVID-19 pandemy. The transmission of diseases often occurs through contact with infected animals and with the increase in meat consumption the risks of spreading diseases increase even more (Arora and Mishra, 2020). This shows the importance of epidemiological control of diseases in animals so that humans are not infected by existing pathogens that put people's lives at risk. To archive this goal, the information related to this control must be secure, immutable and transparent (Arora and Mishra, 2020).

Continuing in this context of epidemiological control, an Plataforma de Defesa Animal do Rio Grande do Sul (PDSA-RS) is being implemented in Brazil, which begins its operation in September/2020. The PDSA-RS acts directly on the traceability of information related to certification of breeding birds in the Brazilian state of Rio Grande do Sul. Is this context, this work proposes the integration of the Blockchain to give immutability to information and crete a unique repository for research or auditability of the data generated in the poultry health of the state of Rio Grande

Descovi, G., Maran, V., Ebling, D. and Machado, A.
Towards a Blockchain Architecture for Animal Sanitary Control.
DOI: 10.5220/0010483303050312
In *Proceedings of the 23rd International Conference on Enterprise Information Systems (ICEIS 2021) - Volume 1*, pages 305-312
ISBN: 978-989-758-509-8

do Sul in the PDSA-RS. First, the work addresses a brief explanation of what it is a Blockchain, its architecture and operation and where it is intended to be used, in this case in the certification of poultry farms (genetics) of breeding birds in the state of Rio Grande do Sul, to guarantee the immutability of the data generated in this process, thus improving the auditability of the information[1].

With the goal of understand the operation and applicability of the Blockchain for animal health, in which the objective is to obtain a high confidence traceability of the information generated in the process, confidence based on the characteristics of the Blockchain, thus maintaining the information immutable, facilitating the auditability and traceability of the data generated in the process. Immutable, in this context immutability is one of the main characteristics of Blockchain technology, it is about maintaining the data once entered in the ledger without changes, ensuring that the information never undergoes changes (Zheng et al., 2018). With this objective, a software architecture was defined and prototyped. The prototype was applied in a scenario based on the real data, generated by the PDSA-RS.

The paper is organized as follows: in Section 2, we present the main related concepts necessary for the article. In Section 3, we present the context of the research itself. In Section 4 we present the case study carried out by the research and the discussion of the lessons learned in the integration process. In Section 5 we present the conclusions of this work and future research possibilities.

2 CONCEPTUAL FOUNDATION

This section contextualizes the basic concepts used in the research and implementation of the prototype integrated to the PDSA-RS.

2.1 Blockchain

Blockchain is a technology on the rise in which it was first proposed in mid-2008 and implemented in 2009 (Nakamoto and Bitcoin, 2008). It can be considered as a ledger, where each transaction is registered in a block chain, a chain in which it grows gradually when inserting new blocks to it (Zheng et al., 2018). The Blockchain technology has some characteristics that make it popular: Decentralization, Persistence, Anonymity and Auditability of the information contained in the block chain. Technology can work in an decentralized environment since it uses security techniques (cryptographic hash, digital signature based on asymmetric cryptography) and the distributed consensus mechanism (Zheng et al., 2018), thus reducing costs and improving the efficiency of transactions, without the need for a mediator, such as a registry office.

2.1.1 Blockchain Architecture

It is a chain of blocks or sequence of blocks, which contains the record of transactions carried out and added to the blockchain (Wang et al., 2019a). Each block has a reference to the previous block, the reference is a hash value for the entire block (Zheng et al., 2018), so if there is a change in the block, the change will be noticed. According to (Zheng et al., 2018), the block has the following elements: header and body. The Header element has the following information: (i) Block version, (ii) Hash of the parent block, (iii) Hash value of all transactions in the block, (iiii) Timestamp of block creation, (iiiii) Nonce[2], value added to the block to give variability to the hash value (Miers et al., 2019);

The body of the block is composed of a transaction counter, the blockchain uses an asymmetric encryption mechanism to validate the authentication of transactions (Omohundro, 2014). Within the architecture, it is necessary to talk about the digital signature, where each user has a pair of keys, one public and one private, in which the private key is used to sign the transactions. The most widely used block chain algorithms like the digital signature blockchain include the elliptic curve algorithm (ECDSA) (Johnson et al., 2001).

2.1.2 Blockchain Main Pillars

Blockchain technology has some fundamental pillars (Wang et al., 2019b):

- Has a **Ledger**, which is a base of data that stores information and is configured in a distributed manner. Therefore, this Ledger also guarantees the transparency and immutability of the information;
- **Cryptography**, each participant within the network, as well as each transaction is encrypted by

[1] https://www.gov.br/agricultura/pt-br/assuntos/sanidade-animal-e-vegetal/saude-animal/programas-de-saude-animal/pnsa (portuguese)

[2] Nonce: Unique random number that in Bitcoin is used in the validation of blocks. It is used to find a valid hash value, the greater the difficulty of the nonce, that is, the greater the number of zeros to the left of the nonce number, the number of possible valid hashes decreases. (Miers et al., 2019)

the participant himself, he has a digital certificate with which he will sign these transactions. Therefore, the entire transaction within a blockchain is privately and encrypted;

- **Smart Contracts**, are the business rules that are applied to this data;
- **Consensus**, guarantees stability and validates the transactions to guarantee a transactional order within the blockchain network, for that there are consensus algorithms.

2.1.3 Consensus Algorithms

In this section, we will focus on four consensus algorithms. Private Blockchains are best advised to manage an organization's internal information. All nodes in a blockchain have an exact copy of the blocks that make it up (Miers et al., 2019). For a new block to be inserted, the blockchain uses consensus algorithms. The three algorithms presented in this paper are:

- **Proof-of-Work (PoW):** This algorithm is currently used in Bitcoin, it has a huge energy expenditure. All nodes in the network need at all times to calculate a specific Hash using different nonces, when finding this Hash the node informs the other nodes, they must confirm this Hash and then validate the transaction. Because of this behavior, this algorithm is called mining (Miers et al., 2019).
- **Proof-of-Stake (PoS):** Compared to PoW, PoS saves more energy and is more effective, because instead of requiring nodes to mine, in this algorithm the highest possibility of mining the next block is from those who have a larger amount of coins. Some blockchain networks in order not to favor the wealthier use randomization mechanisms to choose the next node that will validate the block (Zheng et al., 2018).
- **Proof-of-Authority (PoA):** This algorithm is used in private blockchain networks. It is a consensus where a set of authorities are responsible for validating transactions, and to submit or create a valid block, the person responsible for creating the block requires the approval of all authorities involved in this blockchain network (Miers et al., 2019).

2.2 Animal Sanitary Control in Reproduction Birds

Poultry health is a major concern and a high strategic priority for poultry companies. Diseases are a potential risk to livestock production in any country. The lack of sanitary control on farms can have consequences such as (i) reduced productivity of lots, (ii) total slaughter of birds, (iii) interdiction of farms thus increasing the cost of production, loss of market, among others. In Brazil, the Brazilian National Poultry Health Program (Brazil, 2021) highlights that the main objectives of the program are: (i) Prevent and control diseases of interest in poultry and public health, (ii) Define actions that enable the health certification of the national poultry stock, (iii) Encourage the development of healthy poultry products for the internal and external market;

Thus establishing the prevention, control and surveillance measures of the main poultry diseases that impact public and animal health, which are: (i) Avian influenza, exotic in Brazil (never identified), (ii) Newcastle disease, latest occurrences in 2006, (iii) Salmonelosis (Gallinarum, Pullorum, Enteritidis and Typhimurium), (iiii) Mycoplasmosis (Galliseptcum, Synoviae and Meleagridis (turkeys)).

2.3 Plataforma de Defesa Sanitária Animal do Rio Grande do Sul (PDSA-RS)

The PDSA-RS platform aims to provide better information and process management and automation for the existing animal health control process. It integrates agents from different areas, the integration between the existing sectors characterizes a public-private management model that brings improvements to epidemiological surveillance. The PDSA-RS is presented to users in five main portals: (i) Rio Grande do Sul State Veterinary Service Portal (SVE), (ii) Technical Responsible Portal (RTs), (iii) Agricultural Laboratory Portal (Laboratory), (iv) Brazilian Ministry of Agriculture Portal (MAPA) and (v) Administration Portal (Admin);

The PDSA-RS follows the Brazilian epidemiological surveillance standards and the National Poultry Sanitation Program (Brazil, 2021).

2.4 Related Work

The section is dedicated to present related work with this proposal. (Tripoli and Schmidhuber, 2018) presented a general idea in which the applicability of the blockchain covers the process of the food and supply chain as a whole, that is, from production on the farm to sale to the final consumer through the retailer. In contrast, the research of this work covers only part of the process, that of animal sanitary control, where at the end of it, the establishment responsible for the animals receives a sanitary certificate.

The research (Makkar et al., 2020) states that the attributes of blockchain technology make it ideal for a number of applications in the animal production and animal health sectors, sectors in which this work is included in. Another work that is related is the research (Feng et al., 2020). It proposes a sustainability flowchart for traceability systems based on blockchains. Therefore being related to this research because it is also about traceability of animal sanitary control. The work (Vingerhouts et al., 2020) presents a case study of software modeling for the 'traceability' of animals from birth to the arrival at the final consumer's plate, identifying and keeping all the stages in which the animal went through its life.

All the works identified are related to at least one part in which this research has joined, but none has a case study implemented in a real environment.

3 SOFTWARE ARCHITECTURE DEFINITION FOR ANIMAL SANITARY CONTROL

Blockchain technology has great potential to change the existing workflow and processes (Košťál et al., 2019). The animal health process can be part of this change identified using Blockchain. Adding the information generated in the animal health process to a Blockchain apparently becomes appropriate, as its main characteristics support speed, accuracy, reliability and immutability, requirements necessary to audit information and generate reports.

3.1 Process of Blockchain Integration

The use of Blockchain technology for the animal sanitary control process will not replace, for now, the current process, but in the near future there are great possibilities for this replacement, with the idea that each process carried out to generate a certificate will be recorded in the Blockchain, thus, available to official agents and international authorities.

By making the process more transparent, easier and safer, bringing benefits as in the case of an outbreak of animal or plant disease, contaminated animals can be tracked more quickly (Tripoli and Schmidhuber, 2018). Figure 1 represents a simplified blockchain system for animal sanitary control of breeding birds, illustrates the process in the physical, digital flow and how the data produced in this process is stored in the Blockchain. The data is stored block by block, generating a network of interconnected blocks, thus producing the benefits mentioned above, such as traceability, immutability, transparency and a history of the process.

Implementing Blockchain in the traceability of records generated in animal sanitary control has great potential, but it can be a challenge. Blockchain can become slow according to the amount of data inserted in it (Košťál et al., 2019), in the same way it will require a complete reflection of the agents involved in animal health, of how they approach the processes and activities involved in the process.

3.2 Software Architecture Definition

The architecture definition of this research was based on the existing software structure used for the PDSA-RS process. Figure 2 illustrates the current PDSA-RS architecture and the blockchain architecture incorporated in the platform. The architecture extension components (presented in Figure 2) are described below: **Service (1)** has certain rules and definitions so that the information and access permissions are correct, so it **requests access (2)** to the **Blockchain management API (3)**. Upon obtaining access, the service sends the generated data to API (3), the data is then verified and encrypted with the authority's private key (4). After this process, the **authority (4)** is asked to create a new block to insert the information. For this creation request to occur, the **Proof-of-Authority algorithm (5)** is executed, thus ending the flow by inserting the data into the **Blockchain (6)**.

In Figure 2, the item (5) is marked with a red circle, representing that the algorithm is not currently being implemented. In place of this algorithm for carrying out implementation tests, we used Proof-of-Work alghoritm. The following section will present the case study of the scenario of the first tests of the proposed architecture, where some points were identified in the process in which the blockchain architecture could act.

4 CASE STUDY

To evaluate the prototype that implements the theory of this work, the sanitary control certification process of poultry establishments in the state of Rio Grande do Sul was mapped, an animal health process for breeding birds.

4.1 Case Study Definition

The process was mapped using the Business Process Model and Notation (BPMN), thus obtaining the central points where the architecture proposed by the

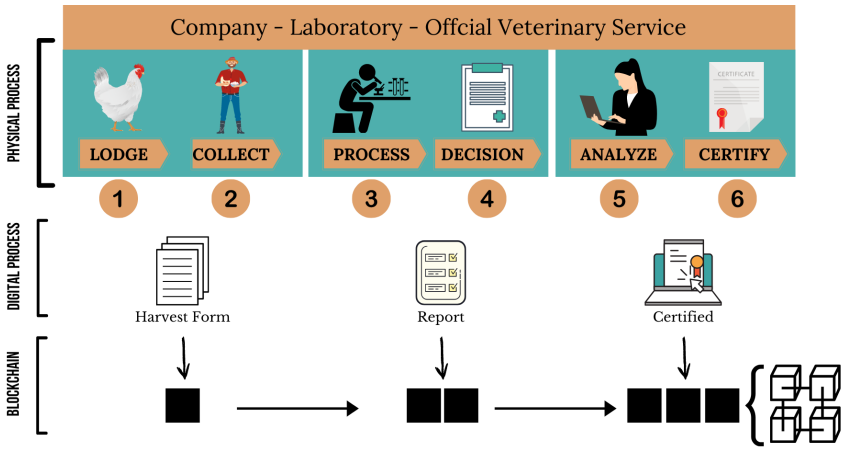

Figure 1: Simplified view of Blockchain application in animal health for breeding birds.

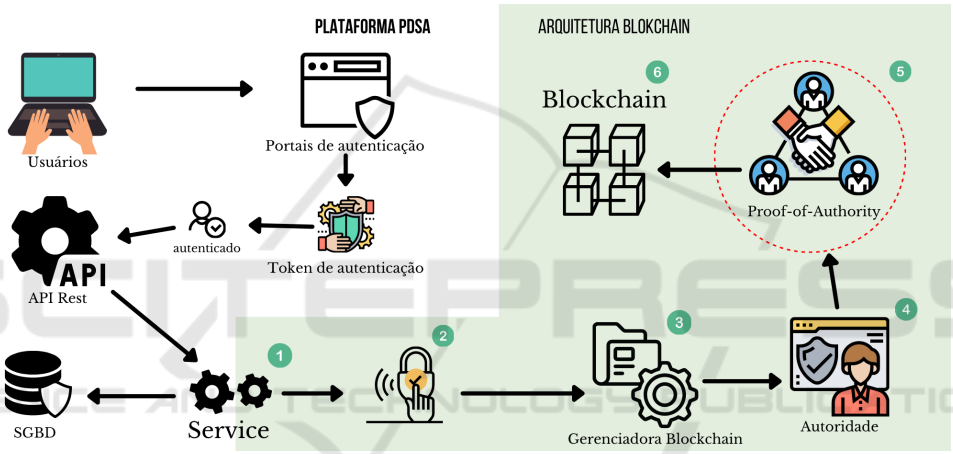

Figure 2: Existing / preliminary architectural overview.

work would act. With the mapping it was defined which data to store and at what time to store, as the mapped process was very large, it was divided in two, represented in Figures 3 and 4. Therefore, the points identified to store the generated data were, respectively: (i) Data filled in the harvest form, (ii) Data contained in the report issued by the agricultural laboratory, (iii) Certificate (information processed from raw data from previous steps);

With this data set collected, a health certificate is issued. And each step is contained in a block of the Blockchain. The next section will describe the prototype implemented to perform the insertion of steps 1,2 and 3.

4.2 Application and Discussion

After the mapping process, we prototyped the software architecture to integrate blockchain in PDSA-RS. In the prototype, the information generated in the steps mentioned above 1, 2 and 3 were inserted in the Blockchain of the same. With the use of this prototype, it was identified that the data recovery started to become increasingly slower as the block chain increased. For this reason a log schema was implemented in a relational database, this strategy is to supply the need for information consumption by the end user, where all information stored in this schema is inserted into the blockchain. Therefore, ensuring security, immutability and auditability of the blockchain and the speed and scalability of the relational database.

Another strategy adopted was to reduce the number of blocks generated, where each step of the process was transformed into a block, generating a quantity of 3 blocks for each certificate issued. To reduce this amount, it was adopted that each step of the process is a transaction, where at the end we have 3 transactions: (i) data from the harvest forms, (ii) data from the reports and (iii) data processed from the pre-

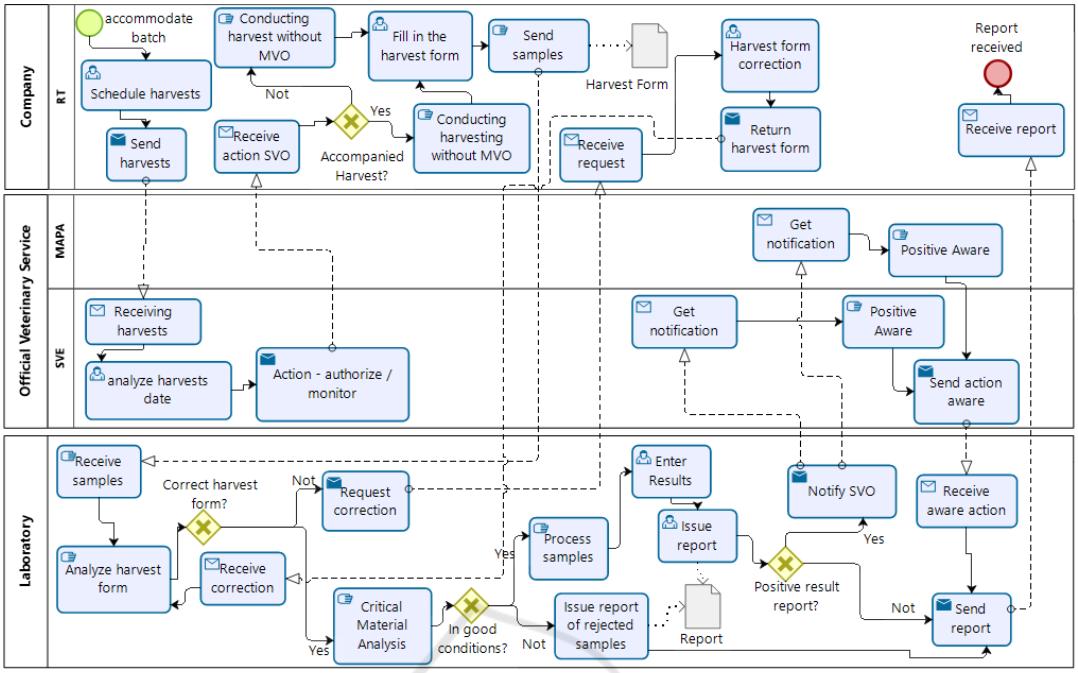

Figure 3: Process to obtain a sanitary report on the moment of life of a poultry batch.

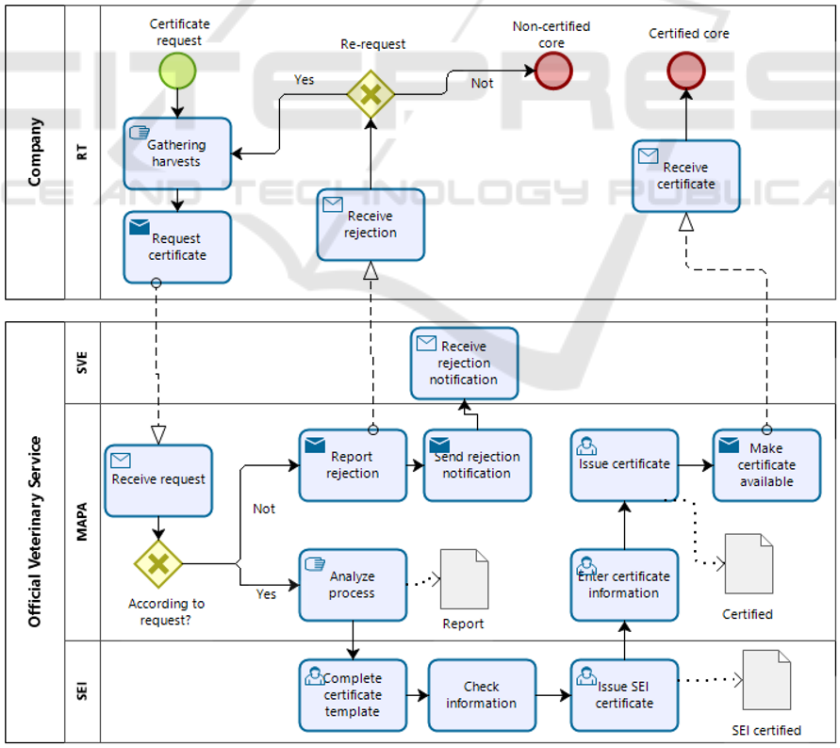

Figure 4: Process to obtain a health certificate from the nucleus of a poultry establishment.

vious steps, contained in a single block, facilitating auditability, forming a certificate and reducing from 3 blocks to 1, a significant 66.66% reduction in the block size. The block is created using the Proof-of-Authority algorithm. Finally, a smart contract was developed to ensure that transactions actually meet the necessary specifications, in other words, if you really have all the information (data) needed to issue a cer-

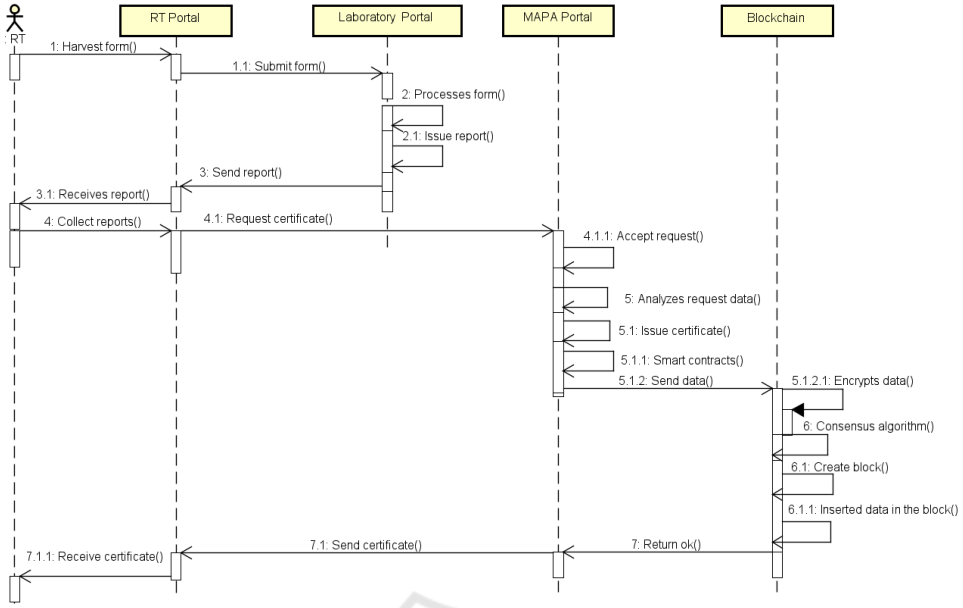

Figure 5: Sequence diagram of certification process in PDSA-RS with the Blockchain extension.

tificate. However the recovery of the data contained in the blockchain has been recovered consistently, ensuring a reliable history of the data of the health certification process of poultry establishments.

Figure 5 represents a simplified sequence diagram that wraps Figure 4, 5 and adds blockchain functionality. From activity 5.1.1 of the sequence diagram, blockchain functionality begins to emerge: 5.1.1 Smart Contracts, when analyzing the data and issuing the certificate via the platform, the smart contracts are triggered verifying that all the data necessary for the certificate to be sent to the blockchain were provided by the PDSA-RS platform. Once verified, they are sent to the blockchain (5.1.2).

The following code is a small example of a code snippet from a smart contract for Ethereum, using the Solidity, high-level object-oriented programming language designed to implement Smart Contracts (Dannen, 2017), used to validate the data mentioned in step 5.1.1, in which it is triggered when a certificate is issued via the platform. After the end of the contract execution, the data are sent to the blockchain.

```
pragma solidity >=0.4.0 <0.6.0;

contract ValidadeData {
   // Simplified structure of a Certificate
   struct Certificate {
      string harvest_term;
      string age_birds;
      string protocol;
      uint   lot_number;
      string responsible_harvest;
   }

   Certificate c;

   function validade() public {
      // business rules
   }
}
```

5.1.2.1 Encrypts the data, the data when sent is encrypted to be inserted into the blockchain block. 6 Consensus algorithm, while the data is encrypted, the consensus algorithm is called, creating a new block (6.1). Then the data is written to the block (6.1.1) and thus remains available and immutable forever. After this action, the blockchain returns a successful transaction response and the platform provides the certificate to the requester (7, 7.1, 7.1.1).

5 CONCLUSIONS

We know that blockchain technology is on the rise, not just in the financial or cryptocurrency area, where it has become popular, but in other areas. This work described the main characteristics of a blockchain, explaining its architecture and functioning and its consensus algorithms. Demonstrated how it can be applied to the traceability of animal sanitary records because of its characteristics, an immutable ledger, where you have the entire process in a safe way and

complete like this improving the management and auditability of the records, making it transparent to the official bodies involved. A case study mapped with BPMN of the health certification of poultry establishments in the state of Rio Grande do Sul for breeding birds was presented. Mapping that made it possible to apply the knowledge acquired for the implementation of a blockchain integration prototype with the already existing PDSA-RS platform, with the objective of storing the data generated in the certification to obtain traceability and auditability of high confidence and of added value.

Therefore, the prototype fulfilled its objective by bringing to the certification process the benefits that a blockchain provides us, such as transparency, agility, immutability, security and reliability, but at the same time, it brought us a problem of poor performance when recovering data according to blockchain size increase. The problem was solved with a change in how to insert the data in the blockchain and with a log schema implemented in a relational database, witch gives better data recover performance and query capabilities, uniting the benefits of both (blockchain and database).

Future works envisaged so far are: (i) Compare performance and benefits of different blockchains implementations, like Ethereum and Hyperldger, in the context of private blockchains, (ii) Develop more Smart Contracts, to automate more parts of the process and make it more and more intelligent, (iii) Improve Smart Contract performance and correctness and (iiii) Identify and map similar processes with the potential for implementing blockchains.

ACKNOWLEDGEMENTS

This work is part of "Research and Development of Innovative Technologies Focused on Agribusiness" (n. 051568) and is financed by FUNDESA.

REFERENCES

Arora, N. K. and Mishra, J. (2020). Covid-19 and importance of environmental sustainability. *Environmental Sustainability*, page 1.

Brazil, M. (2021). Ministério da agricultura, pecuária e abastecimento; programa nacional de sanidade avícola (pnsa). https://www.gov.br/agricultura/pt-br/assuntos/sanidade-animal-e-vegetal/saude-animal/programas-de-saude-animal/sanidade-avicola. Accessed: 2021-01-04.

Dannen, C. (2017). *Introducing Ethereum and solidity*, volume 318. Springer.

Feng, H., Wang, X., Duan, Y., Zhang, J., and Zhang, X. (2020). Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges. *Journal of Cleaner Production*, page 121031.

Johnson, D., Menezes, A., and Vanstone, S. (2001). The elliptic curve digital signature algorithm (ecdsa). *International journal of information security*, 1(1):36–63.

Kosba, A., Miller, A., Shi, E., Wen, Z., and Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *2016 IEEE symposium on security and privacy (SP)*, pages 839–858. IEEE.

Košťál, K., Helebrandt, P., Belluš, M., Ries, M., and Kotuliak, I. (2019). Management and monitoring of iot devices using blockchain. *Sensors*, 19(4):856.

Makkar, H. P., Costa, C., et al. (2020). Potential blockchain applications in animal production and health sector. *CAB Reviews*, 15(035):1–8.

Miers, C., Koslovski, G., Pillon, M., Simplício Jr, M. A., UZH, B. B. R., and Battisti, J. H. (2019). Análise de mecanismos para consenso distribuído aplicados a blockchain.

Nakamoto, S. and Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, 4.

Omohundro, S. (2014). Cryptocurrencies, smart contracts, and artificial intelligence. *AI matters*, 1(2):19–21.

Tripoli, M. and Schmidhuber, J. (2018). Emerging opportunities for the application of blockchain in the agri-food industry. *FAO and ICTSD: Rome and Geneva. Licence: CC BY-NC-SA*, 3.

Vingerhouts, A. S., Heng, S., and Wautelet, Y. (2020). Organizational modeling for blockchain oriented software engineering with extended-i* and uml. In *CEUR Workshop Proceedings*, volume 2749, pages 23–34. CEUR Workshop Proceedings.

Wang, S., Ouyang, L., Yuan, Y., Ni, X., Han, X., and Wang, F.-Y. (2019a). Blockchain-enabled smart contracts: architecture, applications, and future trends. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(11):2266–2277.

Wang, Y., Han, J. H., and Beynon-Davies, P. (2019b). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management: An International Journal*.

Zheng, Z., Xie, S., Dai, H.-N., Chen, X., and Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4):352–375.