DOI: 10.5748/18CONTECSI/PSE/SEC/6829

AN EVALUATION OF SECURITY FEATURES BASED ON ISO/IEC 25023 FOR A DISTRIBUTED AUTONOMIC SCIENTIFIC PUBLISHER TOOL ON A PERMISSIONED BLOCKCHAIN

Elder Bruno Evaristo Correa - UFPA - Orcid: https://orcid.org/0000-0002-4031-6857

Jeffson Celeiro Sousa - UFPA - Orcid: https://orcid.org/0000-0003-1654-1912

Antônio Jorge Gomes Abelém - UFPA - Orcid: https://orcid.org/0000-0003-4085-6674

Sandro Ronaldo Bezerra Oliveira - UFPA - UNIVERSIDADE FEDERAL DO PARÁ - Orcid: https://orcid.org/0000-0002-8929-5145

The first is associated with the application of ISO/IEC in contexts of blockchain application We have adapted a measurement model, based on the use of metrics contained in ISO/IEC 25023, an international standard called SQuaRE series for comprehensive quality measurement and evaluation, but specifically in the security subcategory in DASP. Definition of safety indicators for the evaluation of software quality based on ISO/IEC 25023 aimed at blockchain-based applications, specifying editorial management scenarios. We use a theoretical methodology in the collection of results, where we define the phases of measurement of the indicators. The calculations are performed according to each subcategory of the security aspect and the metrics that constitute it. Some problems were found, such as the time related to the reviews, the quality of the revision of the works and, in some cases, issues related to copyright, which often focus on the management of a reduced number of large publishers. The focus was on the security aspect because in decentralized networks with distributed mechanisms we see the enormous relevance contained in the security features in the application, and for the proposed evaluation plan in DASP. In other words, the models and quality structures existing in nonstandard organizations cannot be compared to others, since they are often built to different standards and focus only on the quality characteristics of interest to the evaluator.

Keywords: Blockchain, network permissioned, data sharing, Academic Process Management, Distributed Processes, Evaluation Security, ISO/IEC 25023

An Evaluation of Security Features Based On ISO/IEC 25023 for a Distributed Autonomic Scientific Publisher Tool on a Permissioned Blockchain.

ABSTRACT: In the development of projects that aim at management and editorial evaluation methods, mechanisms that foster the product's quality final have great importance. In this scenario, several areas are working together in search of better adequacy and standardization in software development. A basic example is the adequations of evaluation of software engineering and computer networks, which work, so that distributed applications are developed following evaluation criteria and standardized quality standards. In this context, we present the DASP software, an open-source distributed autonomous scientific publisher executed through an allowed blockchain network, automatically organized through intelligent contracts, an alternative in the decentralized management of editorial models. As a form of evaluation, one of the most current standards used by the international organization for standardization (ISO) to perform software quality measurements, ISO/IEC 25023, is adopted. Furthermore, we focused focused on the security aspect, which is one of the categories of ISO/IEC. This aspect was chosen because it was based on the main features that underpin blockchain technology. The quality measurement was carried out following several steps, such as the definition of ISO/IEC 25023, an adaptation of metrics for DASP software evaluation, calculations of the quality value of each functionality, and determination of recommendations for improvements in the software according to the estimates made.

Keywords: Blockchain, Permissioned Network, Data Sharing, Academic Process Management, Distributed Processes, Disintermediation in Management, Evaluation Security, ISO/IEC 25023.

Acknowledgment: The authors would like to thank CNPq (National Council for Scientific and Technological Development) from Brazil for grating a Master's Scholarship and GERCOM / UFPA (Reseasrch Group on Computer Networks and Multimedia Communication / Federal University of Pará) from Brazil for the financial support for this research.

1. INTRODUCTION

There are several forms of software evaluation, including numerous metrics and methods of building environments either for validation or assessment of functionalities of a specific context.

Within this context, a set of international standards called SQUARE (Software Quality and Evaluation Systems and Requirements) was used to assess software quality attributes (SCHÖN et al., 2017). Standards, such as ISO/IEC 25010 summarize high-level features for broader contexts. However, to obtain a quantifiable evaluation, specific and concrete measures are verified according to calculations proposed by ISO/IEC 25023 (ARVANITOU et al., 2017), which constitutes the ISO/IEC 25000 standard (ISO, 2013), which are based on practical criteria involving the treatment and management of information.

Included in the information management characteristics that can be evaluated are criteria such as security, which consists of concepts such as confidentiality, integrity, and availability. Besides these, there are complementary aspects such as authentication, non-repudiation, legality, privacy, and auditing. From these principles, information security is achieved through a set of practices and activities, such as the definition/elaboration of information security processes and policies.

It was based on these software quality measurement standards and security concepts, which we consider specific development scenarios, such as applications running using blockchain networks, which consist of a ledger that stores transaction records. This ledger is maintained in a distributed peer-to-peer (P2P) network composed of a set of nodes. The nodes are blockchain devices responsible for processing and storing all the transactions issued in the ledger, which is structured in blocks linked to each other, thus configuring itself in a blockchain, with the expansion of the use of blockchain technology in several sectors, with its applications, classifications, and characteristics, such as persistence, immutability, auditability, and anonymity. Therefore, it is essential to specify a standardized model of software quality evaluation according to the context and applications proposed (ROA et al., 2015; NAKAMOTO, 2009; BERDIK et al., 2021).

This work aims at two complementary contributions. The first is associated with the application of ISO/IEC in contexts of blockchain application. We have adopted a measurement model based on metrics contained in ISO/IEC 25023, an international standard called SQuaRE series (Software Quality and Evaluation Systems and Requirements) for comprehensive quality measurement and evaluation, but specifically in the security subcategory in DASP.

The second contribution of this work is the definition of safety indicators for evaluating software quality based on ISO/IEC 25023 aimed at blockchain-based applications, specifying editorial management scenarios. The focus was on the security aspect because, in decentralized networks with distributed mechanisms, we see the enormous relevance contained in the security features in the application and for the proposed evaluation plan in DASP.

In other words, the models and quality structures existing in nonstandard organizations cannot be compared to others since they are often built to different standards and focus only on the quality characteristics of interest to the evaluator. When we organize a model based on common elements in other contexts, we make it possible to use an evaluation model in different environments and applications. In this scenario, we divide the mode of creation and development of the metrics' adaptation contained in ISO/IEC 25023 for decentralized and distributed environments.

For this, we apply the measurements in DASP (EVARISTO et al., 2019), an open-source Distributed Autonomous Scientific Publisher, which works on an allowed blockchain network, automatically organized from intelligent contracts, which arrange the whole business logic, enabling auditing, disintermediation in the relationships between the entities evolved in the process, besides immutable registration mechanisms that will allow transparency in all actions performed in the network.

By conducting this research, we propose a measurement model, based on indicators adapted for permissioned blockchain applications aimed at editorial management contexts, in addition to recommendations of good practices for improvements in the system and the security aspect, according to ISO/IEC 25023, which includes confidentiality, integrity, non-repudiation, auditability, and authenticity.

This work is part of the evolution of a previous primary study. We started a survey to verify the validity of an editorial management method executed in a distributed network with a decentralized management mechanism. The last work used a public blockchain network through a whole scenario, where we perform intelligent contracts in the hyper ledger test network. However, evolution's in the discussions related to access and responsibility of the actors involved in the process. We verified that the proposal's correct implementation and development would be over a permissioned blockchain network (EVARISTO et al., 2019).

This work is organized in section 2 related works, which are proposals aimed at editorial process management, followed by section 3, DASP, where the developed application, a scientific publisher, executed using blockchain network mechanisms, is exposed, Included are parameters about the workflow together with the interface of the proposal, session 4 discusses the evaluation methodology, following the measurements adapted to the blockchain context, and finally, session 5 covers the conclusions of the work and talks about future work.

2. RELATED WORKS

For understanding the current scenario and approaches related to the management of editorial processes based on blockchain, we analyzed the literature according to some common characteristics that guide decentralized environments, more specifically blockchain networks, and demonstrate how the technology can establish the origin of the results obtained in the various lines of research, including the tracking of multiple assets that change during the life cycle of the study, in addition to making clear the total absence of means of evaluation that establish a standard of quality in the functions of software or ecosystems in the development of applications in editorial management over blockchain networks, as can be seen in Table 1.

Related to research project funding, DEIP is a decentralized platform to foster and develop the scientific community (Blockchain solutions for scientific workflows, 2018). DEIP is a protocol that aims to be an ecosystem to generate funding for innovative ideas, whose premise is that from the moment the community believes in the proposed project, collaborative funding mechanisms will be used, such as crowdfunding. The DEIP governance model is delegated. Scientists vote for the block generators that keep the platform in their name, signing transaction blocks. To enable this model, DEIP runs its consensus algorithm - Delegate Proof of Expertise (DPoEC).

MaRSChain is a system implemented on a blockchain network composed of two types of the blockchain (EMMADI et al., 2018). In the first block, the blockchain (CBC) conference, which keeps a record of the papers submitted to different channels, and the other block, is made up of the blockchain (PHBC) editor, which contains the records of all

documents published on all media. In addition, to keep a list of descriptions of papers under review. Finally, the double-blind revision model is done by encapsulating the data in the smart contract.

Scienceroot is an initiative developed using blockchain networks that integrates underlying technologies such as distributed file system (IPFS), to create a marketplace together with several shared repositories, which can be seen as a sizeable decentralized database of scientific information (GÜNTHER & ALEXANDRU, 2018), In addition, the platform's aim is to generate a structure for financing scientific projects, based on donations and partnerships with entities willing to collaborate. In short, the Scienceroot project is ambitious, including all the required functionalities in the process of scientific discovery. The three pillars on which the project is based are collaboration platform, funding library, decentralized editorial journal.

To increase anonymity (AIMEUR et al., 2012) among the members involved in the conferences and of the reviewers and authors, the P3ERS Privacy Peer Review System was introduced. This distributed system adds a layer of anonymity to the verification process in the double-blind model. This is achieved with the group's consensual signature. The third blind feature also ensures that the program does not know the author's list of members and the exact assignment of articles to reviewers. Thus, increases objectivity during evaluation in the system. However, even if they work with distributed servers, they still exist at the point of being a centralized architecture, the eminent errors of traditional scenarios can occur. Such as not having control over the intention to circumvent the anonymity scheme proposed by work through the link between the identification of users at a certain level in the application.

Aiming to integrate blockchain networks with the entire publication cycle, the Orvium proposal (ORVIUM, 2019) offers incentive principles of open science, aiming to improve the dissemination of research. The proposal provides a reward system in its reviews through the Orvium token asset. Furthermore, the platform offers the ability of individuals and institutions to create decentralized autonomous journals. Still, the proposal does not clarify whether there is the possibility of integration with existing publishers or journals. In addition, a public blockchain network is used, as the Ethereum in its development, which in turn generates essential issues of how to identify who is joining the network, identification that is compromised in public or non-permissioned networks, even if there is a validation system to insert new blocks in the network, it is not known how malicious a new entity in the network can be, a question that is solved by doing a deeper analysis, such as hash verification, transparent information in the whole chain of blocks, like those that happen in permissioned networks.

Blockchain for Science (BFS, 2017) is an organization that aims to be a colossal ecosystem integrator, besides connecting applications that work with decentralized mechanisms of information anonymously. Furthermore, it is a large community that provides an aid platform for developing projects, promoting events to encourage research, reviewing documents, data sharing, repositories based on open science concepts with the help of blockchain technology.

Eureka is a platform to assist in quality analysis of published works (NIYA et al., 2019), in which the application consists of six steps:

1. Relate to the submission of the article and the link in the intelligent contract, linked to the payment that will be used as a reward to all parties in the process,
2. Responsible for the layer of infrastructure combinations (the MongoDB, a Node server. JavaScript, and a remote Ethereum node),

3. Stage of sending the revisions through a civil servant configured in the intelligent contract,
4. Responsible for informing the author about the revisions made in stage 3. In this step, the author will pay the costs of gas transactions (network usability fee),
5. Before the publication in which the editor approves the work.

After the magazine, a reward with an EKA token is generated from the referenced authors. However, Eureka is a project maintained by ScienceMatter, a platform that, in principle, is open access, but an initial access fee causes inconsistencies in the established policies.

Table 1 - Blockchain solutions for managing scientific publications

Common features among the works	DEIP	MaRSChain	ScienceRoot	P3ERS	Orvium	Blockchain for Science	ScienceMatters and EUREKA	DASP
Use of Token	X	-	X	-	X	-	X	-
Transparency in Work flow	X	X	-	X	X	X	X	X
Property management intellectual	-	-	X	-	X	X	-	X
Identification of the members	X	X	X	X	X	-	X	X
Transparency in data process	X	-	X	-	X	-	X	X
Disintermediation management	X	-	-	-	X	-	-	X
Editor's responsibility	-	-	-	-	-	-	X	X
Call for Papers Edition	-	-	-	-	-	-	-	X
Configuration Revision Models	-	-	-	-	-	-	-	X
Identification and control blockchain access	X	-	-	-	-	-	-	X
						X = Contains	- = Does not contain	

Font: Own Ellaboration (2021).

The collection of proposals that occur and explore blockchain applications is well-known, focusing on platform management of submissions and reviews of scientific papers. Table 1 presents features that make up the scenario using proposals based on blockchain networks, focusing on usage, data sharing, privacy, crypto, and token-related issues (In the bid, no token was developed. At this time, the application is based on a cooperative model, but it is possible through the APIs in the hyper ledger platform to configure the environment to accept tokens in transactions), technical issues (e.g., consensus mechanisms and permission structures). The definition in the difference between access of public networks (e.g., Ethereum) and private or permissioned networks (e.g., Hyperledger), defined in blockchain access identification and control.

In which the importance of editorial scenarios and the identification of everyone who accesses or integrates the network is of total relevance, managing the business plan established by the application, alternatives for generating replicable models, either in the traditional focus or aiming at the decentralized scenario that blockchain offers (creation of instances) and the development of means for distributed data storage and security.

Table 1 demonstrates means of sharing, and the discussion of new models of relations can directly influence how data are treated, increasing numerous points of discussion, such as:

- Models that enable the availability of data can strengthen the access to democracy of the entities and general,
- Technological advances and support for access to distributed data may influence new relationship models in the means of scientific production,
- To understand and master data management depends directly on the advance of technology and how to access it,

- Distributed data sharing is related to the advancement of the economic sector about the reduction of costs inserted in academic and editorial management tools.

The questions specified above demonstrate the various lines and branches of research related to the production and dissemination of knowledge. Since the concept of distributed systems of expertise enables a rearrangement in the quality of data dissemination, we propose a framework that works on a blockchain network, which uses the Hyperledger fabric as a framework for collaboration between users from data sharing and management. This solution shares trust among authors, reviewers, and editors. In addition, due to the immutability of the blockchain network, changes in metrics performed to reviews will be noticed by all users in the system, reducing bias among reviewers.

In Table 2 a survey is made of papers covering the evaluation means that use ISO 25023 and documents that evaluate the blockchain application. The idea is to explore how it evaluates applications in various contexts. Therefore, the survey was based on some characteristics that can be implemented as a starting point. Such as the specification of the security assessment, the standardization of an evaluation model, the application of this model in various contexts (used in multiple applications), evaluation in different access modes (applications, data, etc.), specific assessment of the functions embodying the application. And finally, whether the appraisal generates a discussion of the results obtained.

The work (AZIZ et al., 2018) defines the proposition to measure the software quality with ISO 25023, regarding limitations, focused on the safety aspect. In the proposal, we developed software of internal management of the research laboratory to which the author is linked, where this application is divided into five functions of the user consisting of the system administrator, a record of tests, record of rent and equipment, manager of the laboratory and head of the laboratory. This work specifies a framework used in the implementation, divisions, and measurement phases of access to the system by members of the evaluated laboratory. The objective of the evaluation is to propose improvements in scenarios that focus on the management of access to academic research laboratories.

In (JUNG, 2016), the idea of the work is to create a model for classification, analysis, and testing of data according to ISO/IEC 25023 categories. The results show a regression model in aspects such as usability related to the test date, which proved the difference in the test date and the number of errors of the tester. This difference implies a proven inconsistency in the difference in the number of errors in the type of software being evaluated from ISO/IEC 25023.

The work (NAKAI et al., 2016) approaches a standardized structure that embraces numerous contexts from the international standard called SQuaRE (System Quality Requirements and Evaluation Software). The idea is to validate some measures, especially those of technical nature, or that were not easy to compute in the integration of the automation system or did not provide enough guidance to identify a practice to be used. To validate the work, a commercial framework was developed to perform the evaluation using 30 metrics and 6 of quality using metrics that were defined as standard by the result.

The work (DINH et al., 2017) is an evaluation and a classification that describes the use of private blockchain. The work intends to use this classification to understand the different platforms that are permissioned or not permissioned where was developed a benchmarking panel, called Blockbench. Furthermore, it can evaluate some metrics with latency, throughput, scalability, and performance of the platforms considered (ethereum, hyper ledger, and Parity).

In work (KUZLU et al., 2019), within the hyper ledger project, several platforms or sub-projects compose it. One of them is hyper ledger fabric, which is one of the best-known structures in the scenario that guide blockchain. So, this work addresses a specific evaluation, where it is the closed scope for the assessment of throughput, latency, and scalability of applications running on the network, where it analyzes the successful transactions per second, response time per transaction in seconds, and the number of participants that the platform can serve. Still, a detail of this evaluation is the use of participants in an AWEC2 resort, i.e., being used a private cloud structure.

The work (BALIGA et al., 2018) performs a more detailed evaluation used in the Quorum platform, a permissioned blockchain network, analyzing the performance related to the functions implemented in the smart contract and consensus algorithms. The assessment is performed by inserting different workloads, and graphs are generated with parameters verified on the evaluation, such as Latency and Throughput, where the workloads are scaled linearly for the entire range of the network, indicating that Quorum has good scaling characteristics.

Table 2 - Evaluation methods and models

Evaluated characteristics	Aziz (2018)	Jung (2016)	Nakai (2016)	Dinh (2017)	Kuzlu(2019)	Baliga (2018)	DASP Evaluation
Specific safety assessment	X	-	-	X	-	-	X
Standardized definition of valuation	-	X	X	-	X	-	X
Application of the evaluation in different contexts	-	-	X	X	-	-	X
Evaluation of the different means of access	-	-	-	X	-	-	X
Feature Evaluation	X	X	X	-	X	X	X
Discussion of results	-	-	X	X	X	X	X
						X = Contains	- = Does not contain

Font: Own elaboration (2021).

According to the above works, it is possible to observe that software evaluation methods, such as ISO and all the characteristics that compose them, occur in theoretical scenarios or implementations of use cases in web models, centralized and traditional. In contrast, works evaluating applications that run over blockchain networks. However, it is notable that the evaluation is guided on the same metrics (latency, scalability, etc.) of evaluation. There is no standardized evaluation model that can be adapted to different scenarios and applications.

It is in this scenario that this work differs since, based on a thorough search of papers, we found no results that evaluate applications developed in decentralized environments and distributed architectures, such as blockchain networks, where typically their applications are implemented and considered without a specific standard of defined metrics, data collection mechanisms, and without standardized analysis criteria.

3. DISTRIBUTED AUTONOMIC SCIENTIFIC PUBLISHER (DASP)

DASP architecture presents itself as an integrating tool composed of modules specialized in managing several functions that cover the editorial process. It had requirements defined the following functional standards (login, job submission, job evaluation, rebuttal, access to reviews) and not available (time, space, programming languages, compiler versions, database, operating system, development method, etc.). Thus, where we define a set of classes, interfaces, and collaborations and their relationships through the class diagram in

Figure 1, we represent structural aspects of the tool, its attributes and methods, and the relationships between these various classes.

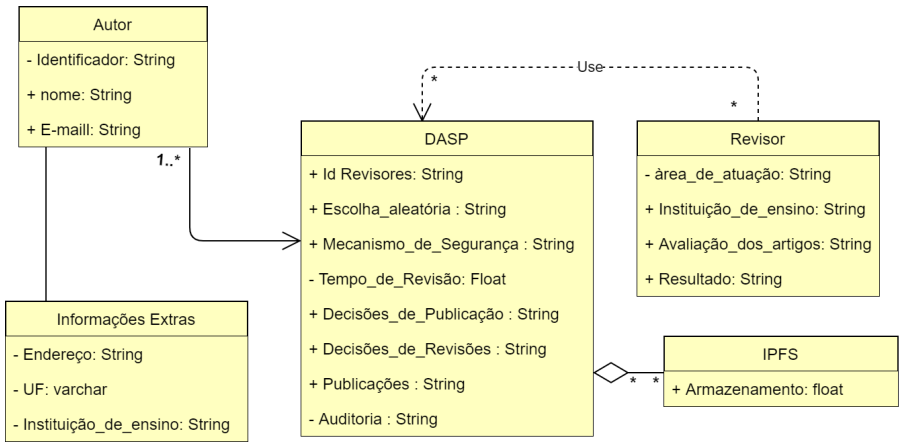


Figure 1 - Class Diagram of the Tool
Font: Own elaboration (2021).

As a mechanism to isolate the business rules from the presentation layer of the tool, based on the requirements mentioned above, we use the Model-View-Controller (MVC) design standard that allows the project to be divided into very well-defined layers. First, the controller interprets the mouse or keyboard inputs sent by the user and maps these user actions to commands sent to the model and the view window to make the appropriate change. This way, the model manages data elements, answers questions about their state, and answers instructions to change shape.

Figure 2 shows the component architecture of DASP using the MVC design standard. The model layer is divided into the blockchain allowed network, more specifically the Hyperledger Composer platform management in intelligent contracts and configuration of the business rules that will be used in the application and records of interactions conducted on the network. The model layer belongs to the article storage engine, in which we use the InterPlanetary File System (IPFS), a distributed database. The control layer consists of modules responsible for the entire process management. The logic is based on smart contracts, making clear the communication and responsibility of each module. Finally, in the vision layer, there is some interaction with the user, by graphical interface or command lines, where that the playground platform allows access via a command-line interface (CLI).

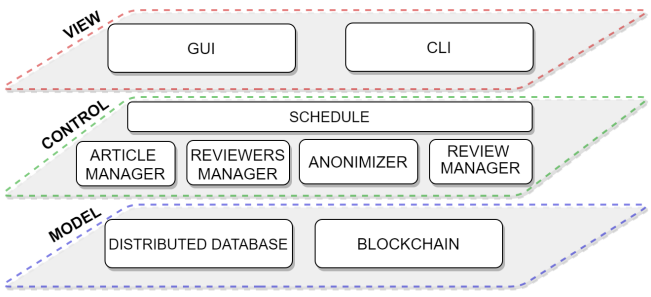


Figure 2 - DASP Architecture
Font: EVARISTO *et al.* (2019).

As far as application control is concerned, it is divided into process managers and time organizers (scheduler):

- **Scheduler:** Responsible for the deadline (Call jobs) and the communication between the other modules,
- **Article Manager:** Responsible for organizing file submission and verifying the document being sent to the correct entity,
- **Reviewer Manager:** Responsible for verifying the random choice of reviewers, following the concept of process security, where they prove the conditions of the reviewer's favorite, the number of points or tokens the reviewer has, and the number of reviews performed,
- **Anonymizer:** When a submission is made, assets are added to the blockchain. A new transaction is made, and this record is called AssetRegistry within the hyper ledger Composer network, linked to an identifier. Through this identifier, every transaction (submission or review) is verified, even allowing the audit of the process if requested,
- **Review Manager:** Responsible for verifying the quality of the review, which the community itself will determine. In it is found the logical evaluation function together between the author, the study itself, and the community. The evaluation method is observed through discussions about the level coherence of the evaluations, which can be provided tokens or points, which will be a form of payment for the assessment having been judged by the whole fairly and impartially.

3.1. DASP Working

Figure 3 shows how the editorial process in the proposed tool is established. From the moment the author or reviewer registers (1), it is clear that both entities have different roles at this point. While the author will submit, the reviewer will wait for some evaluation invitation through the application access interface (2). At this moment, DASP receives the file and picks a random reviewer based on who is registered with the publisher. Then, after the article has been accepted, it is linked to the reviewer's identifier to generate a record of the beginning of the review process (4).

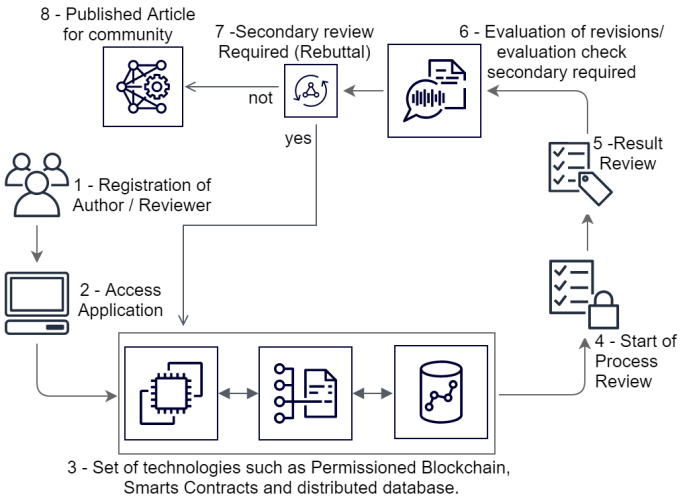


Figure 3 - DASP Workflow
Font: Own elaboration (2021).

After finalizing the review, the author forwards it to DASP, along with the result (5). For this revised work, a new hash is generated, containing all the information inserted by the author. From this moment, DASP checks if the revision is coherent with the policies of impartiality and clarity previously established by the event's organization (6). Besides this step, a new modification may be necessary, and the work is sent back to the edit (Rebutall) (7). Otherwise, the result is sent to the author (8), But the process is best detailed through the activity diagram, as defined in Figure 4.

Specifically, DASP was implemented using different servers(considering the 1.2 release of hyperledger fabric) through the use of Docker, with the help of the angular platform and the Node-RED tool for developing the device as shown in Figure 5, where business rules, defined in the CTO.transactions, are followed, which are the allowed transactions between assets and network participants.

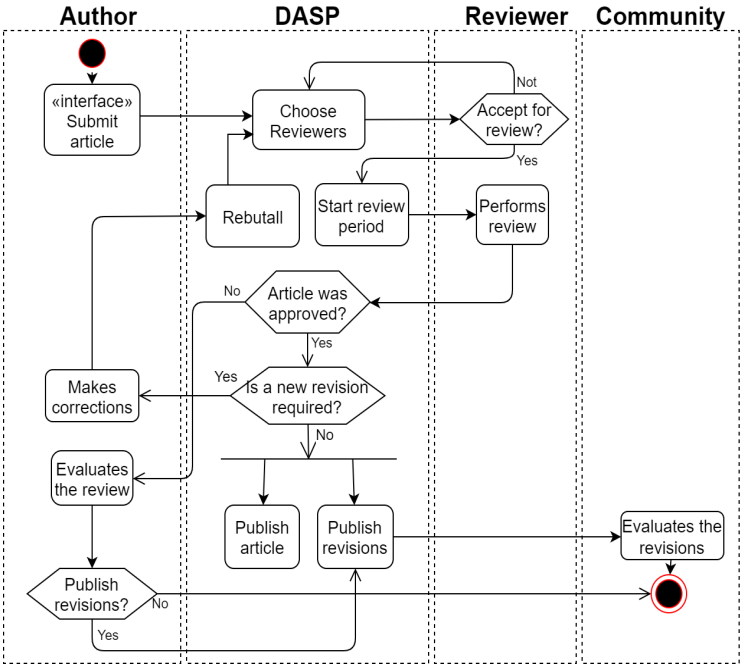


Figure 4 - Activity Diagram of the Tool
Font: Own elaboration (2021).

3.2.1. Database

To create a Business Network Definition (BND), we need to create a project structure with the Yeoman generator with a Hyperledger Composer parameter to create a skeleton of a business network containing all the components of a business network.

A business network comprises assets, participants, transactions, access control rules, and, optionally, events and queries. In the skeleton of the commercial web, there is a template file (extension.cto) that contains the class definitions for all assets, participants, and transactions in the retail network. In addition, the business network structure includes an access control document (permissions.acl) with basic access control rules, a script file (logic.js) containing transaction processor functions, and a package.json file containing corporate network metadata. The main document to be developed is the template file (extension.cto). This file must be written in the Hyperledger Composerlanguage template. The template file contains the definitions of each asset class, transaction, participant, and event.

In the definitions of the participant author, we indicate that he is identified by e-mail, and he has the attribute of personal profile as first name, last name, and an optional identifier, all the String type. A Boolean field has also been implemented to indicate whether the author is a reviewer or not. The author has a score and a reputation, both of the Double type to measure, respectively, the quality of his published articles and the quality of this user according to the community itself. In addition, the author has a relationship with an asset of the Details type that has complementary information to this author that we will detail below along with other assets.

3.2.2. Definition of Assets

There are three types of assets in the definition of the assets: details, article, and review. The details save the Author/Reviewer password, ensuring that it is part of an asset it belongs to and has access to. It is important to remember that there is no encryption implementation for password storage, although all transactions and information are encrypted in the blockchain network.

The active article is identified by an ID, automatically generated by the network when transacting, which has fields like title, tags, IPFS hash, and concept in string format. In the definition of the article itself, we store in Boolean form parameters that indicate if the article needs revision and if it was published, and its Date-Time format. Finally, there is an attribute to count the corrections made, Integer type, the Double article score, and an array of relations with revision type assets. The latter serves to store, along with the article, the revisions that were created from it.

An ID also identifies the active review, automatically generated by the network when transacting, has fields like article title, article tags, hash article, all in string format. In the definition of the article itself, we store in Boolean format parameters that indicate if the Reviewer accepted the review, was completed by the Reviewer, and if it was published and its date in Date-Time format. Finally, we have an attribute to count the evaluation of the review by the Integer community, the points of the reviewed Double article, and two relations with assets of the article type and author. These last ones are used to store together with the review, the article that is being reviewed, and the Reviewer that owns the study.

Each participant operates the assets in the blockchain network through transactions. These transactions are also modeled in this template file (.cto).

There are several transactions for various purposes, but they all work basically in the same way. They have attributes that work as parameters later used by this transaction in its logical sequence. Some transactions may also contain a field for Asset or Participant relationships.

3.2.3. DASP API

Hyperledger Composer has a command to generate a custom REST API based on the implemented commercial network. By default, the Hyperledger Composer REST server includes a feature that produces a set of RESTfull APIs for all assets, participants, and transactions in an implemented blockchain. The Hyperledger Composer REST server also contains the following features:

- EventsusingWebSockets,
- Authentication using Passport's authentication middleware,
- Multi-user mode, so that authenticated users can provide their credentials in the blockchain,
- HTTPS and TLS for secure client-server communications.

These features are all designed to be general-purpose and ready to use. The Hyperledger Composer REST server is distributed as an application called composer-rest-server, which can be installed using Node Package Manager (NPM) or Docker and includes all these features. The REST API provided a functional, neutral language abstraction layer to develop the proposed system in this work.

3.2.4. Client Application

Hyperledger Composer fabric 1.2 also has a Yeoman module, NodeJS package that facilitates projects, used to create projects for use with Hyperledger Composer. This generator also allows you to develop angular applications but only supports simple and basic definitions of business network models. The generated application (including the web forms it produces) will not invest in more complex types of networks, so the system proposed in this work has undergone severe modifications to suit what is expected of the application and its use cases. Being a NodeJS application, some packets have been added to support the features, the IPFS-HTTP-client package, for example, server to communicate with the implemented IPFS network.

3.2.5. Techical Interaction

Within the technical context of DASP's operating flow, the permissioned network (release hyperledger composer fabric 1.2) is divided into the nodes authorizers, storage, collectors, coordinators, and customers. In addition, the components in the architecture communicate using channels. Structures were created specifically to perform transactions privately and confidentially, isolating different entities. Thus, the track is how the components can communicate safely and reliably in the blockchain (AZIZ et al., 2018).

The authorizing nodes (fabric certificate authorities) are responsible for two tasks: the first, in certifying that any component, be it a user or a smart contract, that wants to use the system is who it says it is (in other words, recognizing the authenticity of the component); the second, in authenticating the part and authorizing it to use certain functionalities (e.g., to perform transactions) or to access other factors, after its certification.

The committing peer nodes are responsible for the persistence of one or more transaction chains, which were transmitted through the channels created in the system. Thus, they are the nodes that store the various blockchain. So, it will allow two benefits: privacy and scalability. Finally, the collector nodes (endorsing peer) are responsible for two tasks: the first, to collect the transactions coming from the clients; the second, to analyze, using smart contracts, if the transaction has any associated policy or rule.

The coordinating nodes (ordering peer) are responsible for two tasks: first, to receive the transactions from the clients; second, to perform an ordering on those transactions so that the blockchain is consistent (i.e., to stay the same on all the nodes that will store those transactions). In this sense, all the coordinating nodes acting on a particular blockchain must reach a consensus on the order in which the transactions will be added to the blockchain by the storage nodes. Finally, the customer nodes (application) perform transactions in the system, send them to the collecting nodes, and pass them on to the sending nodes.

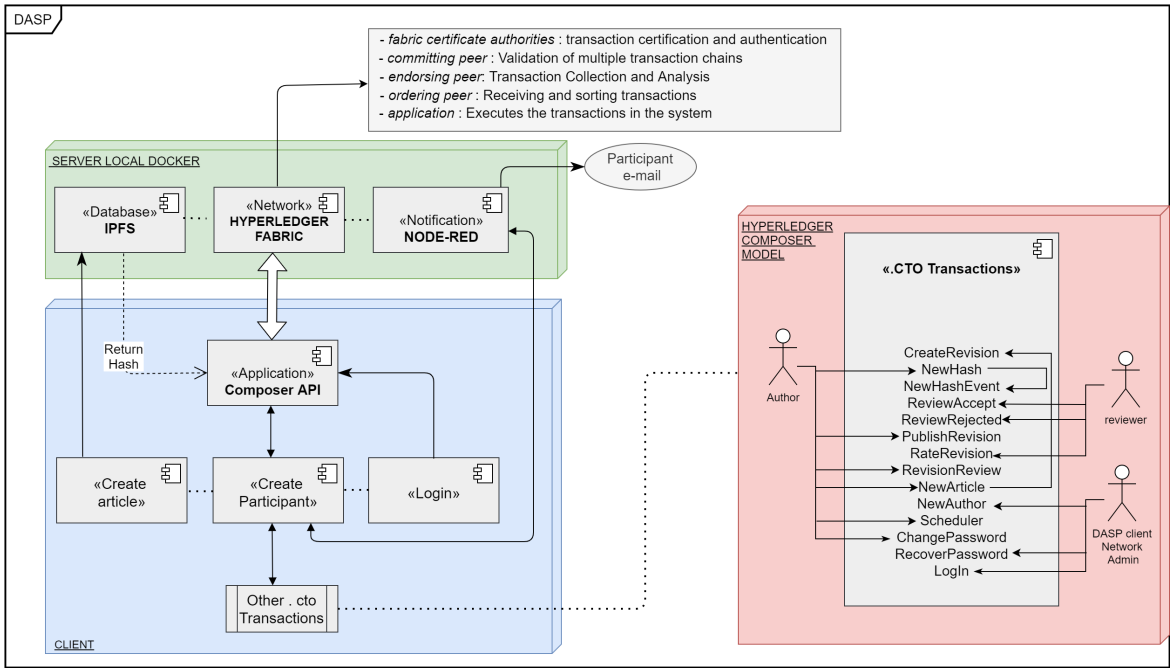


Figure 5 - DASP Overview
Font: Own elaboration (2021).

3.2.6. Definition of Instances

One of the significant gains of distributed applications is configuring environments and creating networks that can communicate or even define unique nodes of decentralized applications. In this relationship, DASP offers a standard node, as shown in Figure 6, which can be adaptable and reconfigured to expand scientific data sharing and evaluation projects from a permissioned blockchain network. Furthermore, it can be noted that there are numerous possibilities for new schemes of editorial systems, following traditional methods or innovative methods, which aim for a more collaborative relationship as according to Figure 6

The goal is to offer a kind of pre-configured ecosystem where the changes would be made from the business logic inserted in the smart contract. In which the developer of the project will insert all the permissions of the entities that will compose the application and identify each one with the whole hierarchical process that that project will have, besides specifying its characteristics of access and evaluation methods among the existing pairs, for example:

- We hold responsibility for business rules, controls, and standards in a shared manner that is fair to everyone on the network,
- Choice of an operator in the network must follow the procedures and policies previously determined,
- Direct or indirect inclusion in the developed instance has to follow the criteria of analysis and network interests.

It works as an association, identity verification, authorization, and identity management service provider in a blockchain network with permission. By authorizing specific network operations, access control lists can be used to provide other levels of authority. It can be developed from a primary example too. Another feature is the ability to create channels that allow participants to create separate transaction books. It is an essential choice for networks where some participants may be competitors and do not want

everyone to know all the transactions they make. The channel ledger is only available to channel participants.

The transaction sequence is delegated to a modular component separate from the pairs that execute the transactions and keep the ledger to reach a consensus. Since the agreement is modular, implementation can be adapted to reliable assumptions in a deployment or solution. In addition, this modular architecture allows the platform to have a complete set of tools that can be used for signature or ordering fault tolerance.

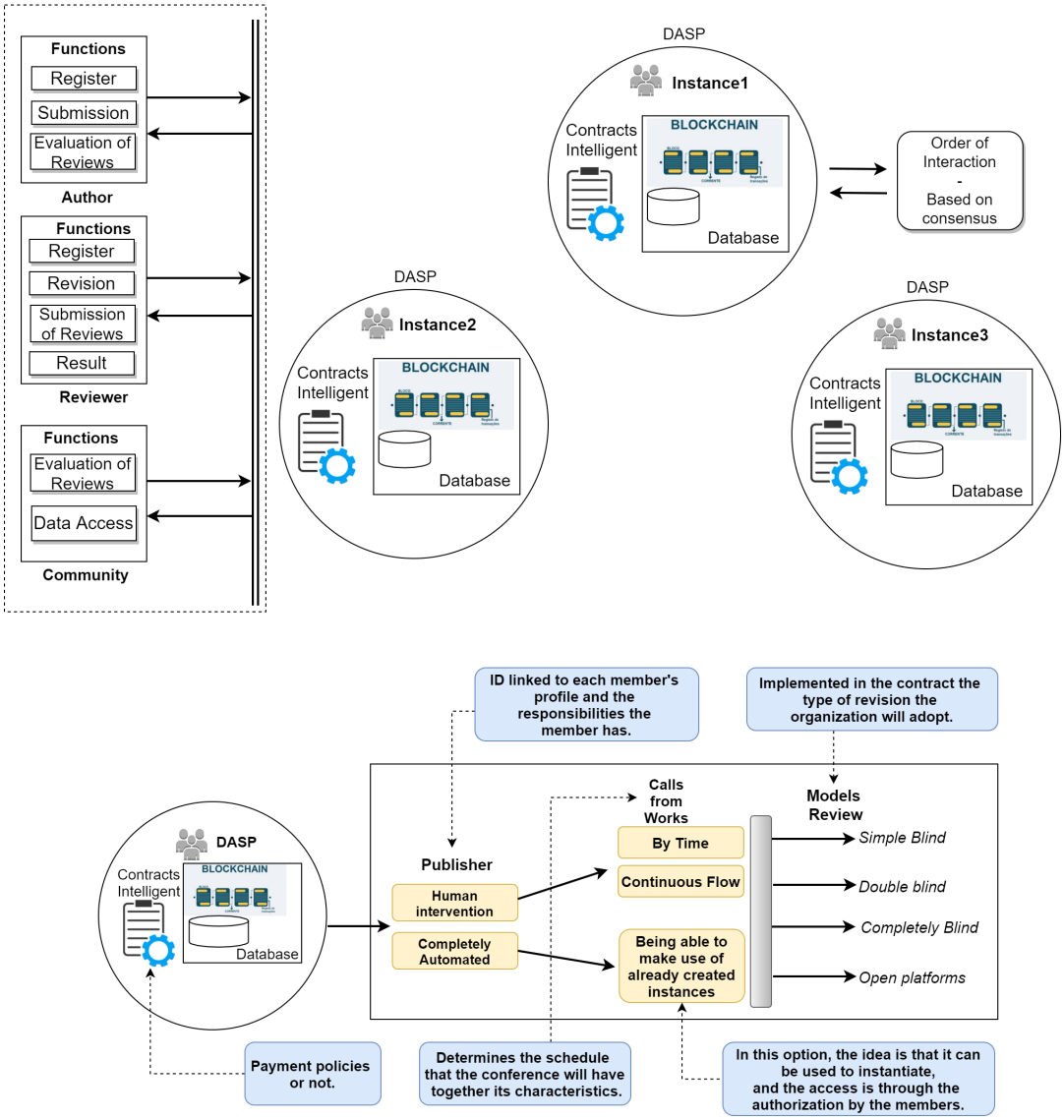


Figure 6 - Instance Models
Font: Own elaboration (2021).

3.2.7. DASP User Interface

Figure 7 shows the initial entries of users, such as Login and the registration of their accounts. Being authors and reviewers, an important detail is that one of the rules contained in the intelligent contracts, for the author to become a reviewer, it is enough for him to make some submission, regardless if the result of the work is accepted or rejected.

After the registration process, the user is directed to the upload area of the article, where he must insert the subject of the work along with the description.

After submitting the article, DASP performs the random selection by the registered reviewers, where a notification is sent to the reviewer by the e-mail address selected by DASP to review the article. The chosen reviewer will have the option of accepting or rejecting to be the reviewer of the article. The review status flows. This process is shown only to the reviewer, where he can download the work for reading. Later, he should generate the evaluation, along with the recommendations based on the task of the article and the status of reviews of the author's papers. At this stage, the author can have a record of his revised works and their expected results.

It is possible to check during the whole process, in the transactions' region, all the records of the process, from the login until the reception of the final result, that is, any action in the network is registered, making possible the auditability of the whole process, besides generating transparency in all management of a specific conference.

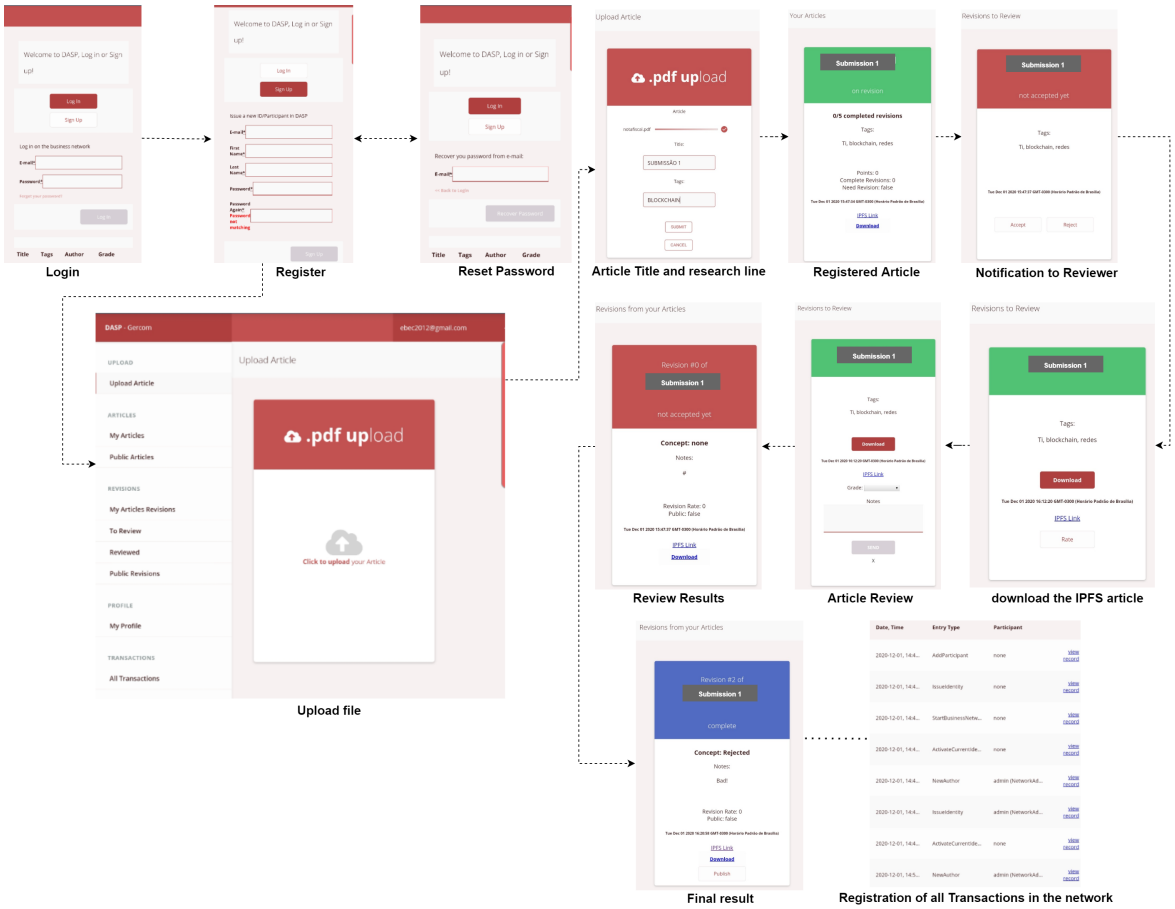


Figure 7 - DASP User Interface
Font: Own elaboration (2021).

4. EVALUATION METHODOLOGY

This section determines the collection phases, specifying the defined indicators and their use and discussions about the results obtained, considering the metrics proposed by ISO 25023 and the characteristics that can be measured in a blockchain scenario, pointing out recommendations for improvements in decentralized and distributed applications.

We use a theoretical methodology to collect results, where we define the phases of measurement of the indicators. The calculations are performed according to each subcategory of the security aspect and the metrics that constitute it. We base the collection on functionalities already implemented in the software and following quality standards about how the interactions of the developed modules communicate, besides calculations based on specific parameters of the blockchain technology, where we determine an expected value of (X). This standard varies in the intervals [0,1] evaluation according to the number of functions running in the developed software. Another evaluation model focuses on measuring each analyzed scope, i.e., a specific collection of software functions, in addition to determining collection criteria based on the implemented functionalities.

4.1 Security Measures

This section is intended to evaluate the security of the DASP software based on ISO 25023. Specifically, the security measures are used to assess the degree to which a product or system designs information and data so that people or other products or systems have access to the data appropriate to their authorization types and levels.

This International Standard does not assign ranges of values of the measures to-rated levels or to grade compliance because these values are defined based on the system, product, or a part of the product, and depending on factors such as the category of the software, integrity level, and users' needs. On the other hand, some attributes have a desirable range of values, which does not depend on specific user needs but depends on generic factors; for example, human cognitive primarily factors, in other words, evaluation takes place through the use of empirical observation of the functions that make up the software.

The method used to apply the ISO to DASP is divided into two phases. The first is the adaptation of the variables that make up the ISO formulas for DASP. The second is to realize the relationship between these variables and the DASP code. Thus, we base the collection of functionalities implemented in the software and the following quality standards on how the interactions of the developed modules are communicating. Besides calculations based on specific blockchain technology parameters, we determine an expected value of (X), a standard that varies in the unit range from 0 to 1 in the evaluation according to the number of functions running in the developed software and how well the execution behavior is.

The process of collecting and developing analysis to obtain the results, using tables, occurred through the subjective analysis of the intelligent contract and the observation and analysis of the functions inserted via the interface. The contract is analyzed line by line, taking as context the developed functions, the interactions between members, access mechanisms, properties of responsibilities given to each network entity. That is, it is analyzed all the logic of business. ISO/IEC 25023 provides the basis for calculations through formulas and metrics to be entered using the division of subcategories. In these subcategories, there are characteristics proper to each parameter that should undergo quantitative evaluation.

In the context of DASP measurement and the criteria that permeate the security aspect of blockchain networks, we have developed a quality verification model related to the evaluation. Those are the parameters that need to be analyzed according to the functionalities implemented. We also build collection criteria, which are associated to what each executable functionality in the software. And finally, we determine analysis criteria, where we specify improvements according to their behavior during use and following the metrics.

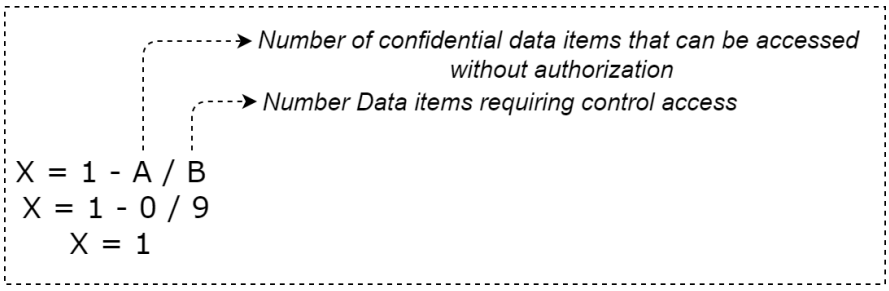
In the following sections, you will find details on how safety features were used in DASP.

4.1.1 Confidentiality

In the aspect of confidentiality, we analyzed three points:

1. Access Control

In the access control, we calculate the data in the software and how they can be accessed, considering the access login (username and password). The username and password are the starting points for the authorization, where the access permissions in DASP constitute nine fields (B). These fields are associated with the CTO. Configuration, being that of these fields 0 are initial permissions that do not need verification (A). A specific measurement formula is defined in ISO 25023 itself, as described below:



The fields that make up the CTO are:

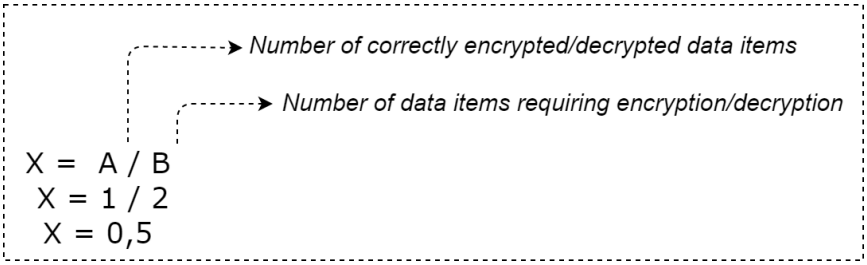
- Upload Article
- My Articles
- Public Articles
- My Articles Revisions
- To Review
- Reviewed
- Public Revisions
- My Profile
- All Transactions

In this context, we calculate that the value in the access control metric in DASP is $X = 1$, fitting the developed verification model, following the analysis criteria determined in ISO.

2. Encrypted Data

The encryption of data is related to the amount of data encrypted by DASP. The blockchain network generates a public signature key corresponding to a private key known only by its owner. For every user interested in publishing work, a pair of signature keys is generated in the transaction performed on the network. It is a file system for creating and updating mutable links to the contents of IPFS. Objects in IPFS are addressed to the content, and the address changes every time the content changes. A name in IPNS is the hash of a public key. In DASP, the article is submitted, and the hash generated is linked to the user and a possible reviewer through an article submission channel via IPFS.

In this case, correctly encrypted and decrypted data (A) add one field that is of access to the authentication data in the internal application in the distributed database (IPFS) and 2 data fields that require encryption and decryption (B). The measurement formula is:

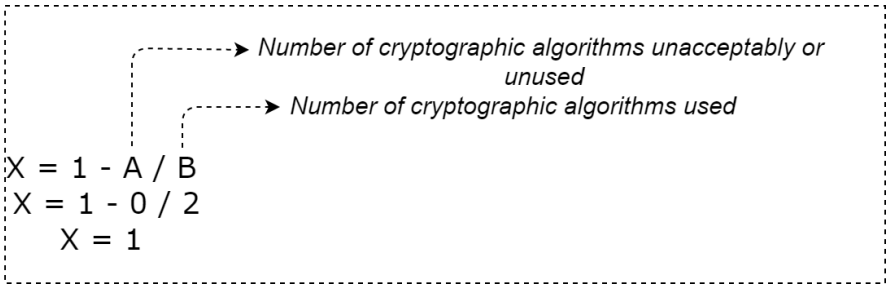


The observed value fits in *0,5* since the cryptography patterns of symmetric keys in DASP are configured in the blockchain access network itself.

3. Strength of Cryptography the Algorithm

In this metric, the proportion of cryptographic analysis of the algorithm used in the application is analyzed. DASP works with two base algorithms since external modules execute their algorithm verification and encryption of the stored data. Such as, for example, the IPFS file system encrypts the data through SHA-256, which generates a hash sent to DASP, which executes its base, the BFT-Smart algorithm, through the hyperledger fabric 1.2.

At this point, we analyze the number of cryptographic algorithms unacceptable or unused (A), compared to the number of cryptographic algorithms used (B), applying the formula:

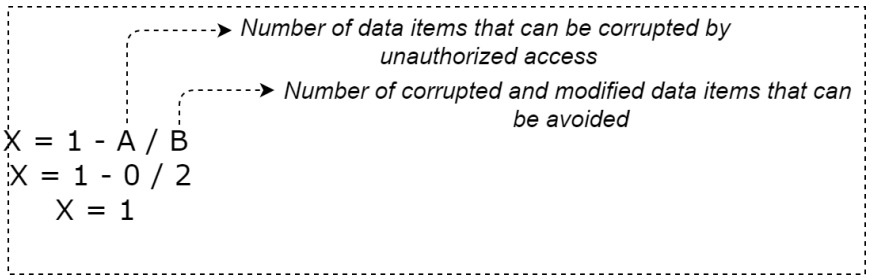


4.1.2 Integrity

In the aspect of integrity, we have three measuring factors:

4. Data Integrity

Data integrity focuses on potential threats that cause data damage, such as transaction verification control. In this context, the measurement metrics concentrate on data that can be corrupted by unauthorized access (A) acting on 0 fields and data for which corrupted and modified data can be avoided (B), which are associated with two fields, which are submitted articles, User ID and password. The measurement formula is:

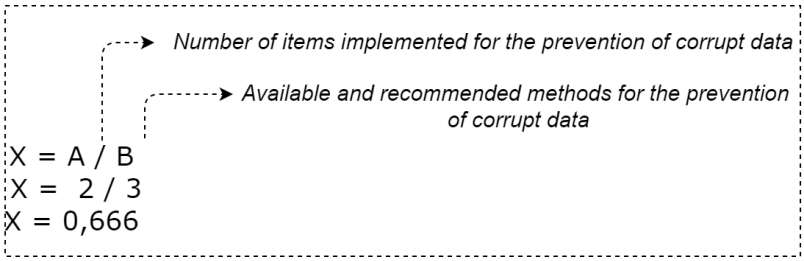


Based on the calculations about the DASP functionalities according to the metric, we arrive at the value of $X = 1$.

5. Prevention of Corrupted Internal Data

Another measurement factor is related to the prevention of corrupt internal data, which focuses on verifying and developing functions for preventing corrupt data at various application levels. In the blockchain environment, there are native verification mechanisms in the network. When any alteration or attempt of unauthorized manipulation in one of the blocks of this chain, the hash number (identifier in the network) is altered. Therefore, it loses its relation with other blocks of the data.

Hash, in technical terms, is known as Content Identifier (CID) in IPFS. CID is a label used to point to material in IPFS. It does not indicate where the content is stored. The cryptography hash of the content is used to generate the CID. A different CID is generated based on the encoding or version used. CID version identifier that indicates which version of the CID is developed. A multi-code identifier format suggests the target of the content. The hash corresponds to a multi-hash of 46 characters starting with "Qm," defining the algorithm (SHA-256) and the length (32 bytes) used by IPFS. The measurement formula is:



The data prevention metric analyzes the extent to which the available prevention methods for corrupted data are implemented. According to DASP, there are fields such as the insertion in the IPFS of a data, alteration via hash, and finally, intrinsic in the application, the immutability of records on the blockchain network. In this scope, we obtained the value of 2 fields linked to the methods implemented in DASP for prevention and three areas related to available. We recommended procedures for prevention, where we reached the value X = 0,666.

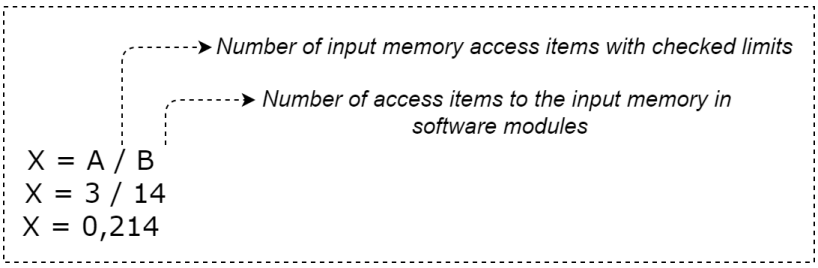
6. Validity of Accesses

The validity of the accesses, which measures the valid entries of the user, scalability of the system, and the modules implemented outside the application, contained within the interface:

- Login
- Register
- Reset Password
- Upload File
- Article Title and Research Line
- Registered Article
- Notification to Reviewer
- Review Results
- Article Review
- Download the IPFS article

- Final Result
- Registration of all Transactions in the network
- IPFS
- NodeJS

We calculate three valid (tagged with "*") input fields with verified user limits and 14(Value of general areas) access fields to DASP modules, where we arrive at the value of $X = 0.214$. The formula was used for this calculation:

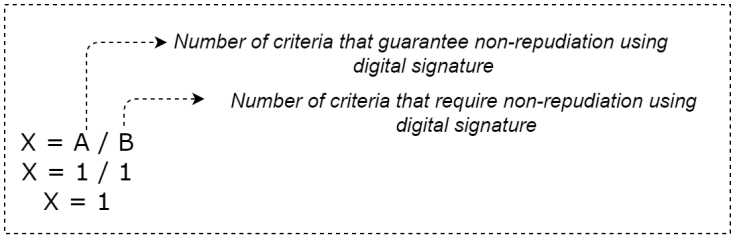


4.1.3 Non-Repudiation

In the aspect of non-repudiation, we have one measuring factor:

7. Use of Digital Signature

In this aspect, Non-Repudiation is the measurement category related to the register of the number of actions and events that can be checked in the software. There is only one quality subcategory in this feature, which is the use of digital signature. When registering in blockchain networks, one obtains one's identification from an algorithm, which scans the content and calculates its identity. Another characteristic that should be mentioned is that once registered in the blockchain, the information becomes immutable, besides having the date and time of insertion traceable in the system (the so-called timestamp). In this context, we identify that the maximum value of measurement in DASP fits the value $X = 1$, where the verification fields that guarantee and require non-repudiation have been filled according to the ISO formula:



In this subcategory, the network access parameters available in the software in an automated way are registered.

4.1.4 Authentication

In the aspect of authentication, there are two standards of measurement:

8. Efficient Authentication Mechanism

The efficient authentication mechanism, which refers to how well the application authenticates the identities, specifies the login identification with user ID and password, which applies Password Authentication Protocol (PAP). PAP is authentication initiated by

the user by sending a package with credentials (username and password) at the beginning of the connection. The system only identifies the login with username and password. In DASP, we evaluated two fields that refer to the number of authentication mechanisms provided (A) and three fields that are related to the number of authentication mechanisms specified (B), in which was found the value X = 0,666.

Validity of Access	Available in Software
1 - Validates if the value of the attribute is a date, time or date time	YES
2 - Validates if the value of the attribute is a valid e-mail address	YES
3 - Validates if the value of the attribute exists in a table, or in the blockchain network	YES
4 - Checks if an attribute is receiving a valid upload File.	YES
5 - Validates if the value of the attribute has a certain size	NOT
6 - Checks if the attribute is of the type specified by type. (integer, floating, string, date, time)	YES
7 - Validates if the value of the attribute is unique in the corresponding database table executed in IPFS	NOT
8 - Validates if the value of the attribute is a "http" or URL "https".	NOT

Number of authentication mechanisms (user ID/password or IC card)

Number of specific authentication mechanisms

X = A / B
X = 2 / 3
X = 0,666

9. Authentication Compliance Rules

The Rules of Compliance in Authentication are based on the necessary proportion of rules in authentication when established in DASP, for example:

- Defining identity class,
- Login and logout,
- Access control filter,
- Result of the authorization of manipulation,
- Function-based access control,
- Configuring the authorization manager,
- Defining the authorization hierarchy,
- Using rules of business.

Within these rules' context, we calculated the five implemented authentication rules number fields (A) and eight specific authentication rules number fields (B), where we reached the value of $X = 0,625$ according to the ISO formula:

Number of authentication rules implemented

Number of authentication rules specified

X = A / B
X = 5 / 8
X = 0,625

4.1.5 Auditing

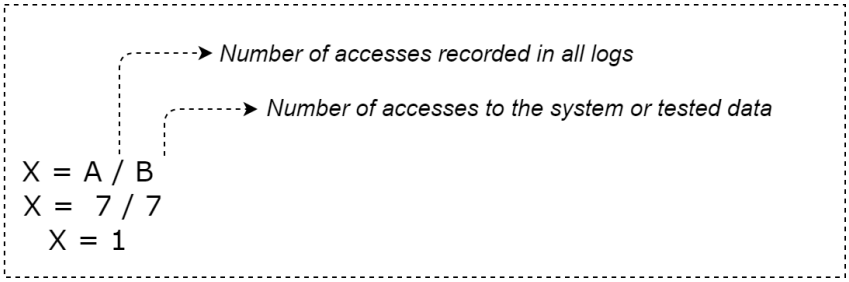
The aspect of auditing is associated with two fundamental points, such as:

10. User Access Auditing

User access audit, in which we verify the measurement of the entire record of transactions made internally since the user access to the access to data. Using blockchain technology, it is possible in the application itself to generate reports of all interactions performed:

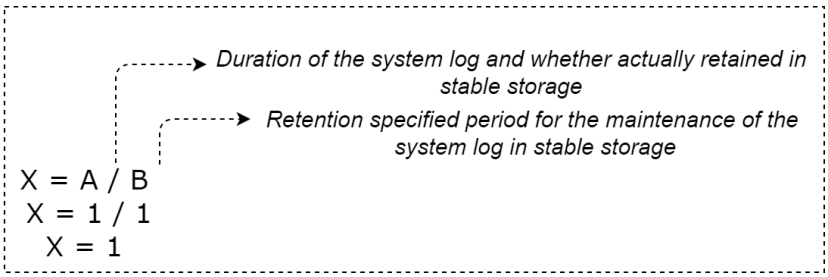
- Login
- Create Participant
- Create Article
- Composer API
- IPFS DEAMON
- Hyperledger fabric 1.2
- NodeJS

In DASP, we have verified seven fields responsible for registered access based on logs (A) and seven areas that express ticket to the system or to the data that have been tested. Applying the formula below, we had the value of $X = 1$:



11. System Log Retention

Finally, System Log Retention is directly associated with the user access, and the time the application can remain stable, performing data storage. In DASP, the entire log in the system is stored in the blockchain network, besides the storage being done in the distributed database, which registers the hash storage. In other words, the calculation is made directly using the records of the application itself. The value was measured using the user's access and permanence logs stably in the application. Applying the formula below, we had the value of $X = 1$:



4.1.6 Consideration

Table 3 was created considering aspects of ISO and specific characteristics of blockchain applications, DASP. Values were specified about each metric, determining measurement actions, indices, and problem solving levels, about the application's behavior. These values

were developed according to the level of implementation of the application and maturation of functionalities. Another point that we notice is the possibility of being an evaluation model used in different scenarios when we talk about Distributed Ledger Technology (DLT) environments.

Table 3 - DASP Security category measuring and indicators

Subcategories/Metrics	Measuring Indicators	Indicator Collection
Confidential		
- Access Control	Ok - X >= 1 Alert - 1 > X > 0,9 Critical - X <= 0,9	* Measure Access Functions * Measure Access Rules * Measure Authorization Control
- Encrypted Data	Ok - X >= 0,5 Alert - 0,5 > X > 0,1 Critical - X <= 0,1	* Measure Encrypted Requirements * Measure Correct Cryptography
- Encryption Strength of the Algorithm	Ok - X >= 1 Alert - 1 > X > 0,9 Critical - X <= 0,9	* Measure safety criteria in system actions * Calculate registration and non-repudiation in the functionalities of the blockchain network in DASP
Integrity		
- Integrity of data	Ok - X >= 0,9 Alert - 0,9 > X > 0,7 Critical - X <= 0,7	* Measure data integration functions * Measure data modification functions
- Internal data prevention corrupted	Ok - X >= 0,6 Alert - 0,6 > X > 0,4 Critical - X <= 0,4	* Measure the level of data access prevention
- Validity of Accesses	Ok - X >= 0,4 Alert - 0,4 > X > 0,2 Critical - X <= 0,2	* Measure level of data damage related to external module functions
Non-Repudiation		
- Use of Digital Signature	Ok - X >= 1 Alert - 1 > X > 0,9 Critical - X <= 0,9	* Measure safety criteria in system actions * Calculate registration and non-repudiation in the functionalities of the blockchain network in DASP
Authenticity		
- Authentication Mechanism efficient	Ok - X >= 0,6 Alert - 0,6 > x > 0,2 Critical - X <= 0,2	* Measure authentication rules in the tool
- Compliance Rules in authentication	Ok - X >= 0,6 Alert - 0,6 > x > 0,3 Critical - X <= 0,3	* Measuring software configuration (functionality) * Measure the quality of transaction rules (implemented contract rules) * Calculate Registration and authenticity of the functionalities of the blockchain network in DASP
Auditability		
- User Auditing	Ok - X >= 0,8 Alert - 0,8 > X > 0,7 Critical - X <= 0,7	* Measure software configuration (features) * Measure the quality of transaction rules (based on blockchain record searches).
- System Log Retention	Ok - X >= 1 Alert - 1 > X > 0,9 Critical - X <= 0,9	* Measuring stability criteria in user use

Ok - nothing Alert - Verification of errors or instabilities Critical - Plan, analyze and apply solutions

Font: Own elaboration (2021).

4.1.7 Recommendations for improvements according to the measurement according to ISO standard

In this subsection, we address some recommendations for improvements that ISO 25023 itself provides, based on the measurement results in Figure 8, where we summarize in

Table 3, we determine mechanisms for measuring indicators, variations according to each subcategory, such as, for example, "Ok," which occurs when the functionalities are in perfect synchrony in the application, "Alert" fits when something in the application is not executing correctly and "Critical" is when it is necessary, drastic modification in the application, it is from this parameter that we calculate the value of *X*. Figure 8 generally exposes the results obtained in the DASP measurement.

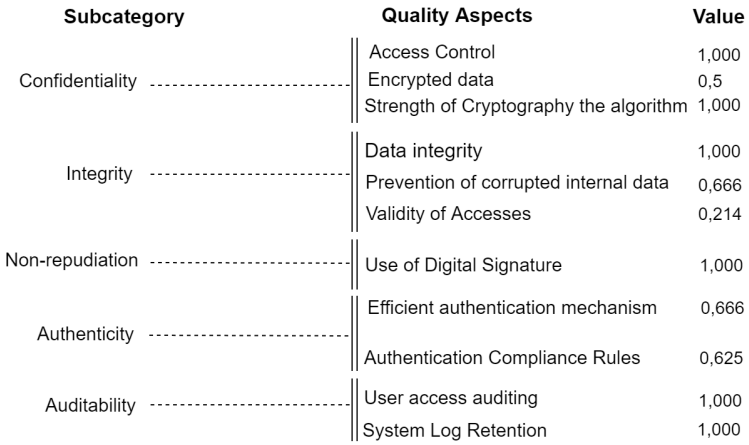


Figure 8 - DASP Security Category Measuring Results
Font: Own elaboration (2021).

Still based on the measurement of indicators according to Table 3, we observe that some points need improvement in either the implementation or even editing of contract rules that organize the business logic, access filters, rules of hierarchy between author, reviewer, and community inserted internally in DASP and scalability of access to the application are functions that need adjustments, following the standards developed. Therefore, we defined Table 4 to specify the criteria that need to be improved at that first moment of the measurement in the publisher.

This evaluation sounds like something incoherent when we evaluate a born technology not to be standardized. However, we organize an evaluation model in this work, considering all the concepts and characteristics that guide blockchain technology, where the evaluation makes a mix of standards that understand architecture, terminologies to harmonize images, elements, and essential foundations for building technological solutions using blockchain, to demystify some issues and guide users and developers, especially regarding good practices.

4.1.8 Discussion of the evaluation method used

Measurement issues generate ambiguity in understanding and limit evaluation methods. In particular, software quality managers struggle to define the quality of software products due to misconceptions in evaluation methods. According to this (KUZLU et al., 2019), 28% of institutions (companies, etc.) apply the ISO/IEC standard in their software products. However, the ISO/IEC standard has general and ambiguous metrics, measurements, inputs, and outputs applied practically to projects and products of software development or evaluation of projects developed.

Table 4 - Recommendations for DASP Improvements according to the use of ISO 25023

Improvement Recommendations	details
Access Manager	Check new way to organize the access, filter the access to the Application,in addition to entering the name and password that already exists, we intend to add Authorization notifications via SMS or e-mail.
Hierarchization of access	Definition of authorization in the access hierarchy that includes all the Entes inserted in the publisher, in addition to applying quality history in Reviews held during the conferences held.
Rules of business	When we define authorization between entities, it is necessary to edit the tasks, papers and operations that each one is allowed to perform in DASP. In addition to specify functions that the user can operate.
System access scalability	This point is important so we can check and confirm how the Software will behave with a large number of access to DASP.
Modules implemented outside the application	We verified that it is relevant the behavior of interconnected modules Externally, in DASP IPFS plays the role of distributed database, where we verify the importance of categorizing its functions in a more clear, such as encryption of stored data, modification of hashs, quality of the protocol of information delivery between members in DASP.

Font: Own elaboration (2021).

This work proposes a model adapted for software scenarios that run on a decentralized communication model and distributed architecture, specifically blockchain networks—the study started by defining each ISO 25023, then mapping the system and calculating the *X*-value. In the next step, we proposed some recommendations for improving the system to meet the quality of ISO 25023. The Threshold used in the measurements is from *0 to 1* to categorize the rating point described in the assessment.

As an explanation of the results obtained, they were given from the observation that there are several means of evaluation, whether practical or theoretical, in this scenario using a subjective theoretical model, because, when it comes to the ISO standard, means of calculating the degree of execution of any functionality contained in software is provided. Still, each context has different organizations and development.

We noticed from this criterion that blockchain network environments (whether permissioned or not) do not have an evaluation standard. No measures focus on the quality of the functions developed. That is, there is no standard model for a decentralized editorial context. Blockchain networks have common execution characteristics among the various types of existing networks. What differs are the forms of access to the network. It was noted that in ISO, there is a security category. And there are subcategories such as confidentiality, integrity, non-repudiation, audit, and authenticity. These are characteristics that guide blockchain networks.

It was then that we used several formulas and metrics that ISO provides, following the descriptions contained in each one of them, considering each characteristic that composes them, since blockchain applications have specific functions and means of communication, besides the transactions being all recorded on the network itself, the database used, also part of a particular execution, through a distributed file system.

5. CONCLUSION

In this work, we presented DASP, a tool that seeks to distribute the management, reduce the intermediation in the submission, review, and publication of articles, based on a set of entities and characteristics that occur in the peer review. In this context, some problems were found, such as the time related to the reviews, the quality of the revision of the works,

and, in some cases, issues related to copyright, which often focus on managing a reduced number of large publishers.

Beyond that, it is an alternative looking for permissioned networks (private), compared to the related work that all offer permissionless networks (public). One of the main gains of using permissioned networks is the possibility of identifying entities in the network, providing a greater degree of trust between members. Validation is much easier, and the group decides what the application rules are permissioned blockchain can be much more efficient and flexible than public ones in two crucial points: they register more transactions per second. Moreover, they do not generate an excessive expenditure of energy in their records.

As future works, we intend to perform an evaluation, applying the evaluation model used in DASP in the other applications that constitute the related works. Through this, we obtain a result that is adequate to the quality of software development in applications that run on blockchain networks. In addition, but specifically in editorial tools aimed at sharing and evaluating scientific data using quality standards and software development, the International Organization for Standardization (ISO) seeks to provide a set of requirements. When well implemented, ensure greater confidence that the organization can regularly provide products and services that meet its customers' needs and expectations and comply with applicable laws and regulations.

REFERENCES

AIMEUR, E., BRASSARD, G., GAMBS, S., SCHÖNFELD, D. (2012) "P3ERS: Privacy-preserving peer review system". Transactions on Data Privacy, 5, 553-578.

ARVANITOU, E., AMPATZOGLOU, A., CHATZIGEORGIOU, A., GALSTER, M., AVGERIOU, P. (2017) "A mapping study on design-time quality attributes and metrics". Journal of Systems and Software, 127, 52-77.

AZIZ, M., SAPTA, I., ROCHIMAH, S. (2018) "Security Characteristic Evaluation Based on ISO/IEC 25023 Quality Model, Case Study: Laboratory Management Information System". In 2018 Electrical Power, Electronics, Communications, Controls and Informatics Seminar (EECCIS) (pp. 332-336).

BALIGA, A., SUBHOD, I., KAMAT, P., CHATTERJEE, S. (2018) "Performance evaluation of the quorum blockchain platform". arXiv.org. Available online at: https://arxiv.org/abs/1809.03421v1. Accessed in 08/19/2021.

BERDIK, D., OTOUM, S., SCHMIDT, N., PORTER, D., JARARWEH, Y. (2021) "A survey on blockchain for information systems management and security". Information Processing & Management, 58(1), 102397.

BFS - Blockchain for Science (2017) "Blockchain for Science: Reproducible Results Through Openness to Scientific Self Correction". Available online at: https://www.blockchainforscience.com. Accessed in 08/19/2021.

Blockchain solutions for scientific workflows (2018) "Deip: Decentralized research platform". Available online at: https://deip.world. Accessed in 08/19/2021.

DINH, T. T., WANG, J., CHEN, G., LIU, R., OOI, B., TAN, K. (2017) “BLOCKBENCH: A Framework for Analyzing Private Blockchains”. Proceedings of the 2017 ACM International Conference on Management of Data.

EMMADI, N., MADDALI, L., SARKAR, S. (2018) “MaRSChain: Framework for a Fair Manuscript Review System Based on Permissioned Blockchain”. In Euro-Par 2018: Parallel Processing Workshops - Euro-Par 2018 International Workshops, Turin, Italy, August 27-28, 2018, Revised Selected Papers (pp. 355-366). Springer.

EVARISTO, B., NASCIMENTO, V., DEFRÉMONT, A., PINHEIRO, B., ABELÉM, A. (2019) “Editora Científica Autônoma e Distribuída sobre Blockchain Privada”. In Anais do II Workshop em Blockchain: Teoria, Tecnologia e Aplicações. Porto Alegre: SBC.

GÜNTHER, V. & ALEXANDRU, C. (2018) “Scienceroot Whitepaper”. Available online at: https://www.scienceroot.com/resources/whitepaper.pdf. Accessed in 08/19/2021.

ISO (2013) “ISO / IEC 25010: 2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models”. Geneve.

JUNG, H. J. (2016) “The Software Quality Testing on the basis of the International Standard ISO/IEC 25023”. Journal of the Korea Convergence Society, 7, 35-41.

KUZLU, M., PIPATTANASOMPORN, M., GURSES, L., RAHMAN, S. (2019) “Performance Analysis of a Hyperledger Fabric Blockchain Framework: Throughput, Latency and Scalability”. In 2019 IEEE International Conference on Blockchain (Blockchain) (pp. 536-540).

NAKAI, H., TSUDA, N., HONDA, K., WASHIZAKI, H., FUKAZAWA, Y. (2016) “Initial Framework for Software Quality Evaluation Based on ISO/IEC 25022 and ISO/IEC 25023”. In 2016 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 410-411).

NAKAMOTO, S. (2009) “Bitcoin: A Peer-to-Peer Electronic Cash System”. Cryptography Mailing list at https://metzdowd.com. Accessed in 08/19/2021.

NIYA, S., PELLONI, L., WULLSCHLEGER, S., SCHAUFELBÜHL, A., BOCEK, T., RAJENDRAN, L., STILLER, B. (2019) “A Blockchain-based Scientific Publishing Platform”. In 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) (pp. 329-336).

ORVIUM (2019) “Whitepaper: Accelerated Scientific Publishing (v1.7)”. Available online at: https://docs.orvium.io/Orvium-WP.pdf. Accessed in 08/19/2021.

ROA, P. A., MORALES, C., GUTIÉRREZ, P. (2015) “Norma ISO/IEC 25000”. Tecnología Investigación y Academia, 3(2), 27–33.

SCHÖN, E. M., THOMASCHEWSKI, J., ESCALONA, M. J. (2017) “Agile Requirements Engineering: A systematic literature review”. Computer Standards & Interfaces, 49, 79-91.