Journal of Information Systems and Technology Management – Jistem USP
Vol. 19, 2022, e202219020
ISSN online: 1807-1775
DOI: 10.4301/S1807-1775202219020 Original Article

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[1], https://orcid.org/0000-0002-4031-6857
Jeffson Celeiro Sousa[1], https://orcid.org/0000-0003-1654-1912
Antônio Jorge Gomes Abelém[1], https://orcid.org/0000-0003-4085-6674
Sandro Ronaldo Bezerra Oliveira[1], http://orcid.org/0000-0002-8929-5145

[1]Universidade Federal do Pará, Belém, PA, Brazil

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 to 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 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, academic process management, distributed processes, evaluation security, ISO/IEC 25023.

Manuscript first received: 2022-04-03; Manuscript accepted: 2022-11-10

Address for correspondence:
Elder Bruno Evaristo Correa, Universidade Federal do Pará, Belém, PA, Brazil. E-Mail: ebec2012@gmail.com
Jeffson Celeiro Sousa, Universidade Federal do Pará, Belém, PA, Brazil. E-Mail: jeffson.sousa@icen.ufpa.br
Antônio Jorge Gomes Abelém, Universidade Federal do Pará, Belém, PA, Brazil. E-Mail: abelem@ufpa.br
Sandro Ronaldo Bezerra Oliveira, Universidade Federal do Pará, Belém, PA, Brazil. E-Mail: srbo@ufpa.br

CC BY

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.

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.

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, evolutions 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).

CC BY

This paper is organized section 2 related work, which is proposals aimed at managing the publishing process, followed by section 3, DASP, where the developed application, a scientific publisher, run through blockchain network mechanisms, is exposed, It includes parameters about the workflow along with the interface of the proposal, session 4 discusses the evaluation methodology, following the measures adapted to the blockchain context, and finally, session 5 covers the conclusions of the paper and talks about future work.

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 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 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.

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, increasing 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, and the eminent errors of traditional scenarios can occur. Such as not having control over the intention to circumvent the anonymity scheme proposed by working through the link between the identification of users at a certain level in the application.

CC BY

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.

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, and repositories based on open science concepts with the help of blockchain technology.

Eureka is a platform to assist in the quality analysis of published works (NIYA et al., 2019), in which the application. 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. Responsible for the layer of infrastructure combinations. Stage of sending the revisions through a civil servant configured in the intelligent contract. Responsible for informing the author about the revisions made in stage. In this step, the author will pay the costs of gas transactions (network usability fee).

The collection of proposals that occur and explore blockchain applications is well-known, focusing on platform management of submissions and reviews of scientific papers. Figure 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 of the difference between access of public networks (e.g., Ethereum) and private or permissioned networks (e.g., Hyperledger), is defined in blockchain access identification and control.

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

Figure 1. *Blockchain solutions for managing scientific publications*
Font: Own elaboration (2021).

CC BY

Figure 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;
- Understanding and mastering data management depends directly on the advance in technology and how to access it;
- Distributed data sharing is related to the advancement of the economic sector through 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.

Notably, 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 an exhaustive search of articles, 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.

DISTRIBUTED AUTONOMIC SCIENTIFIC PUBLISHER

Aiming at new management proposals, DASP emerges as an alternative to improve governance in the publication process, promoting disruption by applying distributed and autonomous management among the entities involved in the entire process. For this, the proposal uses the concept of Decentralized Autonomous Organizations (DAOS) as a basis.

The solution features Blockchain properties such as decentralization, transparency, and immutability of records, as well as token economics to improve the scientific process. Since we are presenting a completely open model, we do not perform any token development, however, in the solution development is possible, aiming for some sort of financial reward. Specifically, the DASP proposal embraces the junction of features of decentralized management and distributed communication as shown in Figure 2, with the help of blockchain networks, generating results such as:

CC BY

- Transparency and efficiency: Blockchain technology enables more transparent, instantly accessible, and time-efficient solutions for scientific collaboration;
- Communication: The seamless communication and integration of all stakeholders in the scientific publishing process: researchers, institutions, publishers, and funders - on the Blockchain-based platform, covering all three pillars of academic research - collaboration, funding, and publication;
- Tamper-proof Scientific Process: No possibility of manipulation of scientific results to fulfill the criteria for publications in a particular journal. All results, including, for example, negative results of the experiment, are published and cannot be modified;
- Proof of ownership: by using information associated with the owner of information saved on the blockchain, such as a private key needed to generate a digital signature, the ownership of that information can be guaranteed;
- Confidentiality: a blockchain is agnostic to the category of stored data. Thus, it is possible to store information that guarantees different properties about the data, even without revealing its contents;
- Reward contribution through tokenized inventories: inclusion of economic and reputation incentives in the blockchain protocol; the possibility of the development of reward mechanisms based on (the) cryptocurrency itself to adequately compensate any forms of scholarly activities, including peer reviews;
- Access control: different categories of access control can be employed to the data stored on a blockchain;
- Fair funding processes: since access to research is collaborative, the solution aims to offer any scientist the opportunity to receive adequate funding for a particular research project, regardless of their career status.

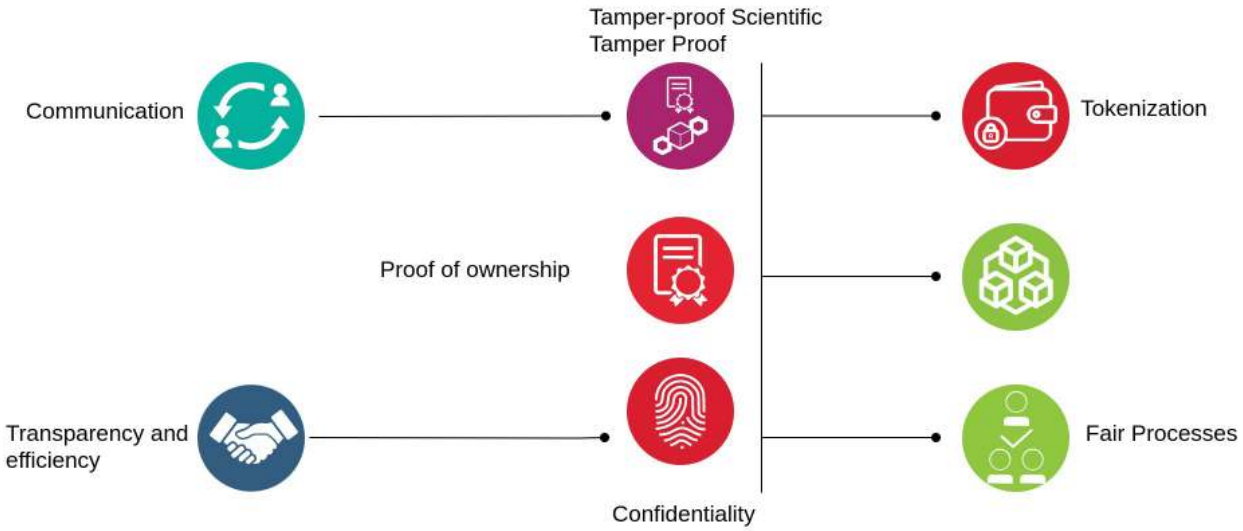


Figure 2 *Characteristics of decentralized management*
Fonte: Own elaboration (2021).

CC BY

Besides the technical discussion, related to the tools and applications available in the editorial process and all its particularities, whether direct or indirect, mentioned throughout the work, the model of relationships that we are proposing in this work also involves debates about how scientific production can be improved, based on mechanisms that encourage creativity, cooperation, and evaluation of scientific work. There are also social discussions, there are often numerous technological proposals that try to assist in the evolution of more coherent and fairer forms of evaluation, however, we need to be aware that technology, represented here, is just a tool and if we do not build human and ethical values, if these technologies are not used with analysis and social commitment, the results can be very bad.

It is based on these principles and characteristics that the proposal, we developed the DASP software, aiming at the flexibility and humanization of the process, more direct relations without any controlled entity between the parties, intermediation of decisions, and distribution of responsibility among all those involved in the evaluation processes, causing the integralization of groups and fomenting lines of research that are more and more collaborative. These are the main gains of the proposal, when visualizing the forms of interactions in DASP it is clear the reduction of bureaucratic criteria that naturally influences the reduction of economic criteria.

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

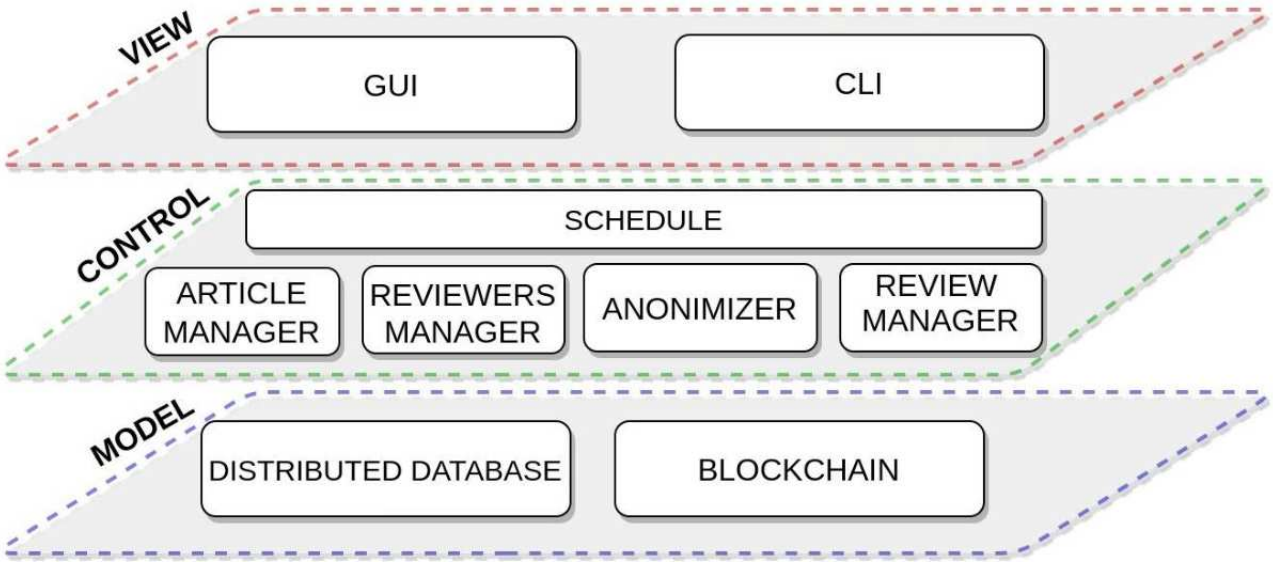


Figure 3. *DASP Architecture*
Font: Evaristo et al., 2019.

CC BY

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 3 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. Thus, where we define a set of classes, interfaces, and collaborations and their relationships through the class diagram in Figure 4, we represent structural aspects of the tool, its attributes and methods, and the relationships between these various classes.

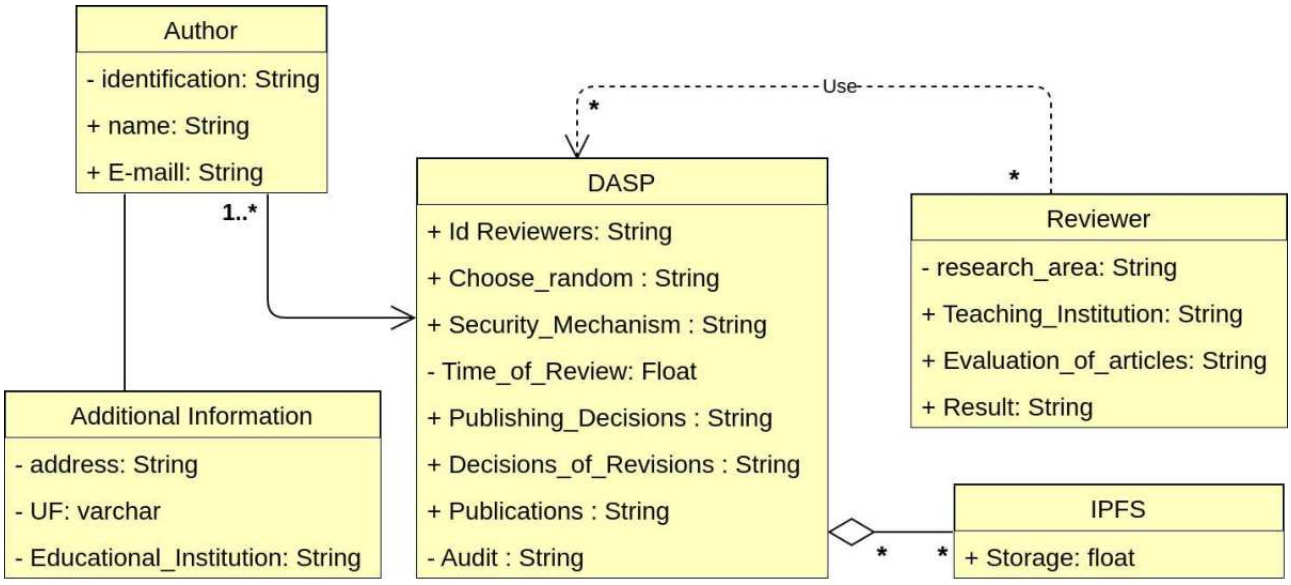


Figure 4. *Tool ClassDiagram*
Font: Own elaboration (2021).

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

- **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.

CC BY

- **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.
- **Review Manager:** Responsible for verifying the quality of the review, which the community itself will determine.

DASP WORKING

Figure 5 shows how the editorial process in the proposed tool is established.

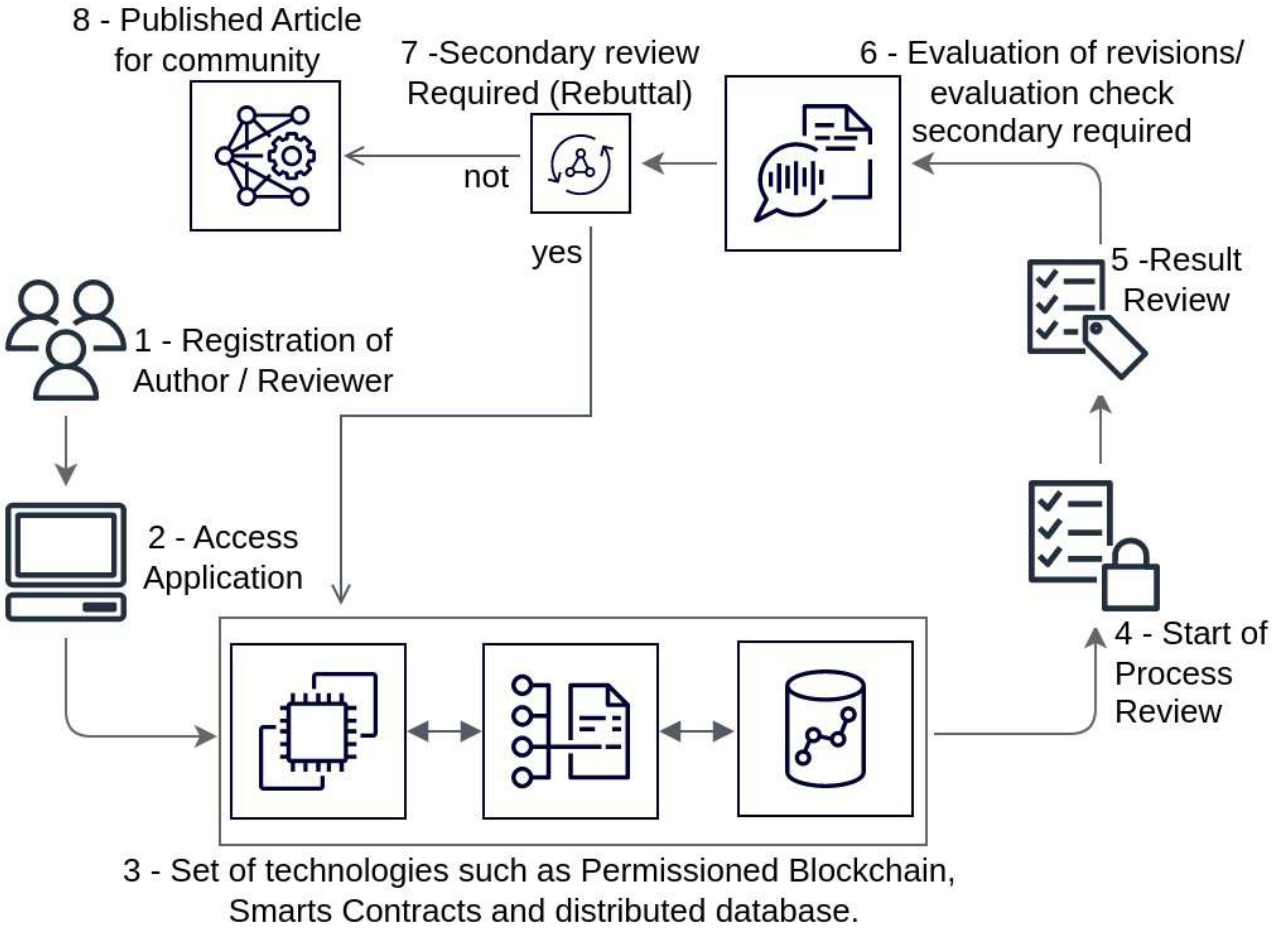


Figure 5 *DASP Workflow*
Font: Own elaboration (2021).

CC BY

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 (Rebuttal) (7). Otherwise, the result is sent to the author (8), But the process is best detailed through the activity diagram, as defined in Figure 6.

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 7, where business rules, defined in the CTO. transactions, are followed, which are the allowed transactions between assets and network participants.

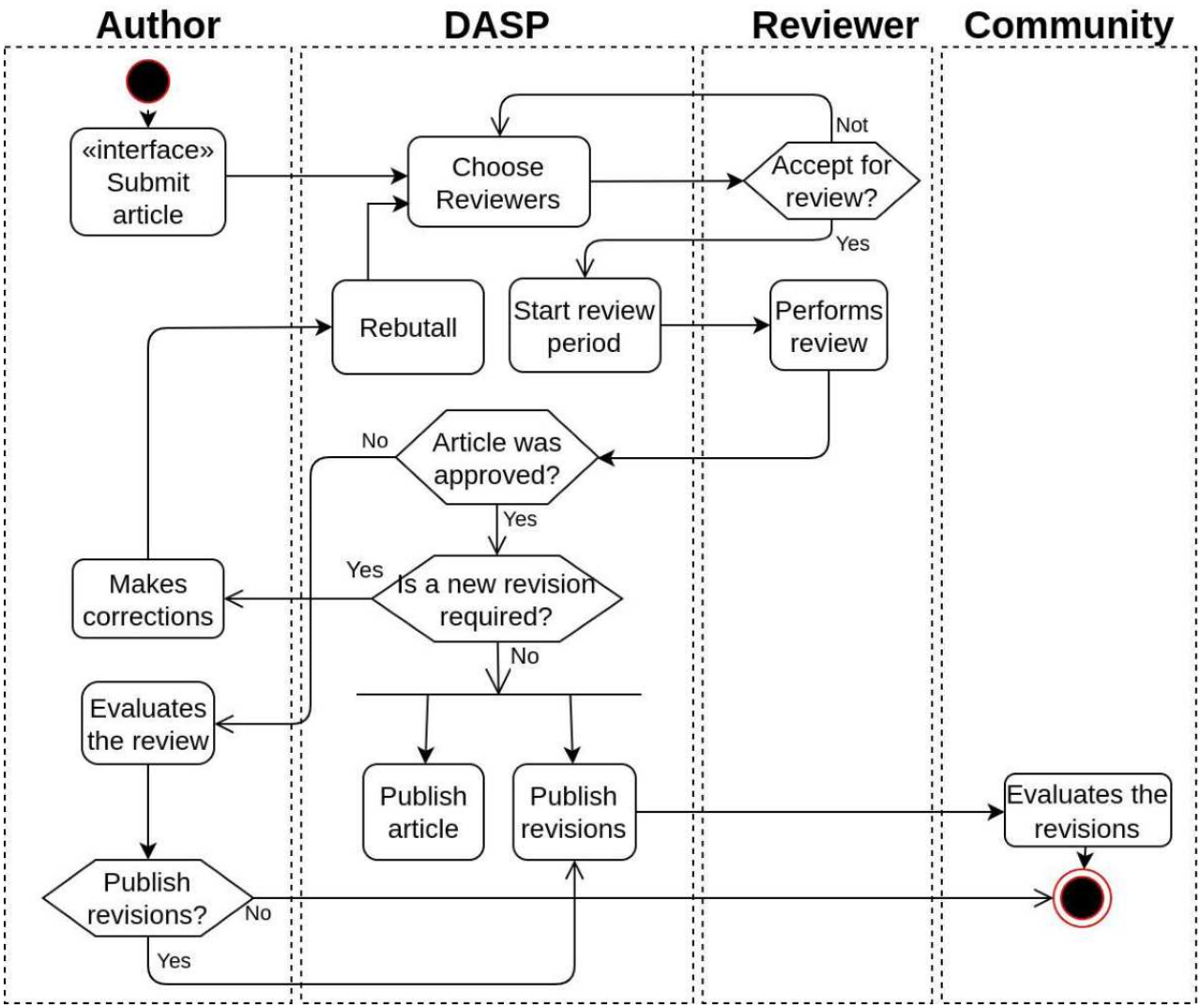


Figure 6. *Activity Diagram*
Font: CORREA et al., 2021.

CC BY

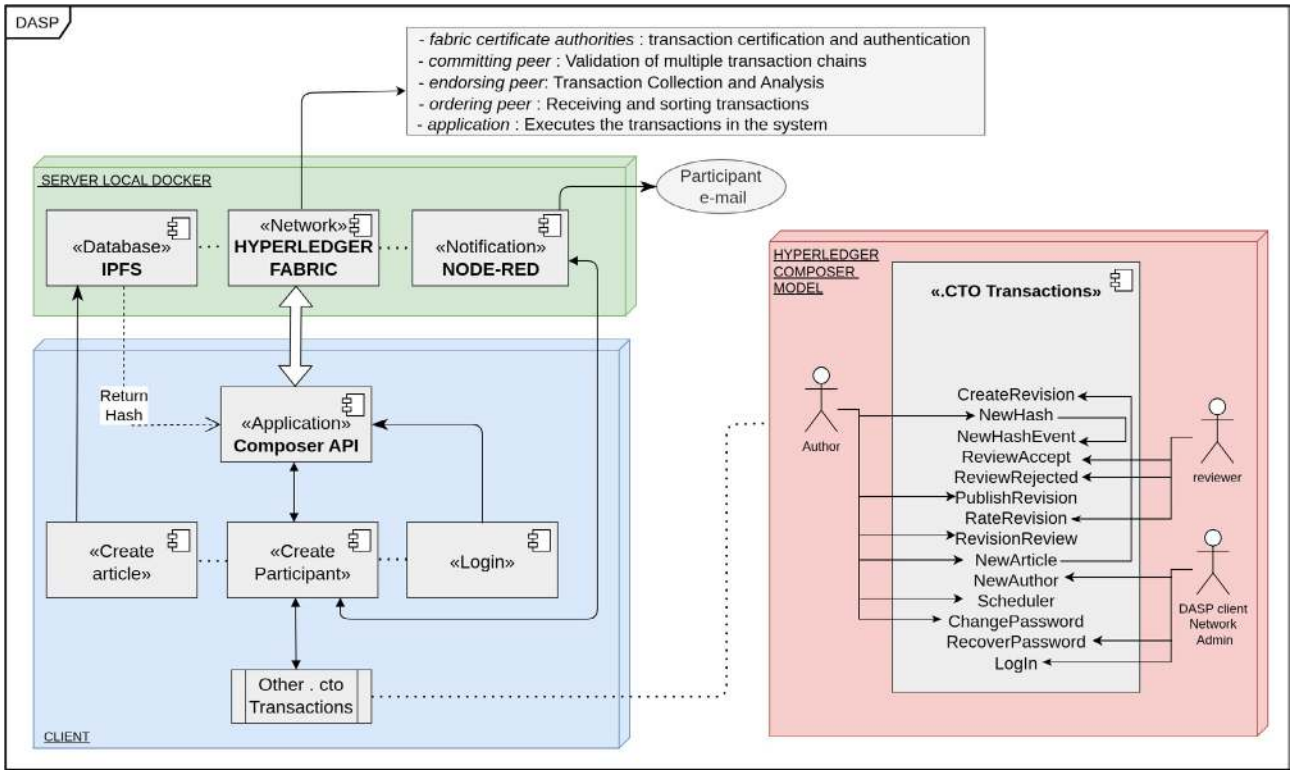


Figure 7. DASP Overview

Font: Own elaboration (2021).

Technical 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).

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 7, 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 8.

CC BY

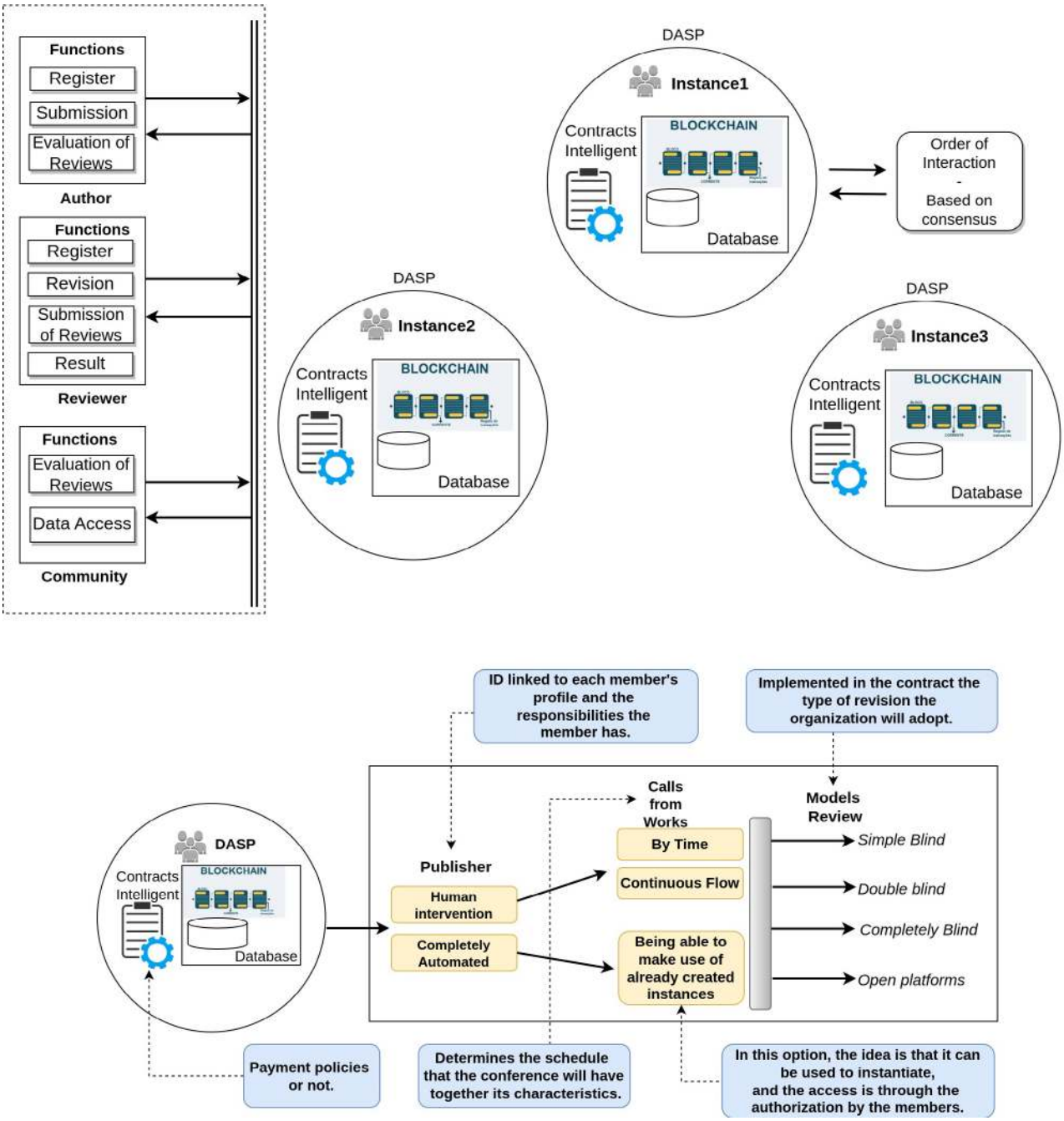


Figure 8. Instance Models
Font: Own elaboration (2021).

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. It works as an association, identity verification, authorization, and identity management service provider in a blockchain network with permission.

CC BY

EVALUATION METHODOLOGY

This section determines the collection phases, specifying the defined indicators and their use, and discussions 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 follow 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.

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 communicated. 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, and 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.

CC BY

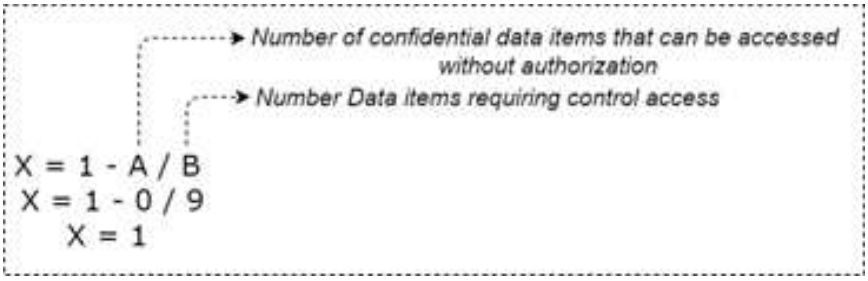
In the context of DASP measurement and the criteria that permeate the security aspect of blockchain networks, we have developed a quality verification model related to the evaluation. Those are the parameters that need to be analyzed according to the functionalities implemented. We also build collection criteria, which are associated with 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.

In the aspect of confidentiality, we analyzed three points:

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
- PublicArticles
- MyArticlesRevisions
- To Review
- Reviewed
- PublicRevisions
- My Profile
- All Transactions

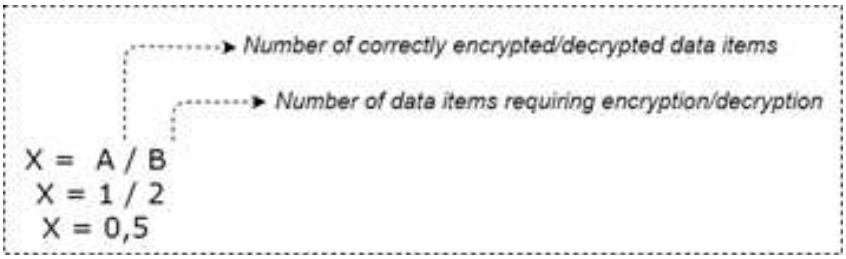
In this context, we calculate that the value in the access control metric in DASP is $X = 1$, fitting the developed verification model, following the analysis criteria determined in ISO.

CC BY

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 are 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:

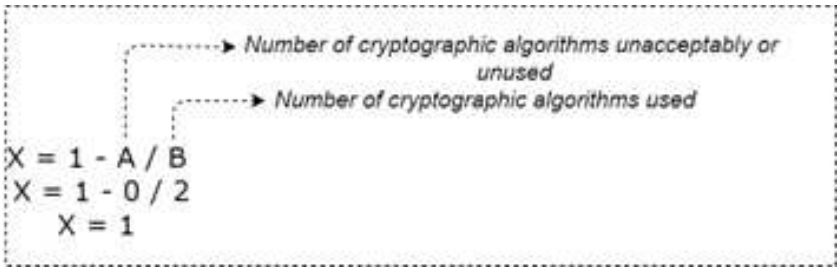


The observed value fits in *0,5* since the cryptography patterns of symmetric keys in DASP are configured in the blockchain access network itself.

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:



Integrity

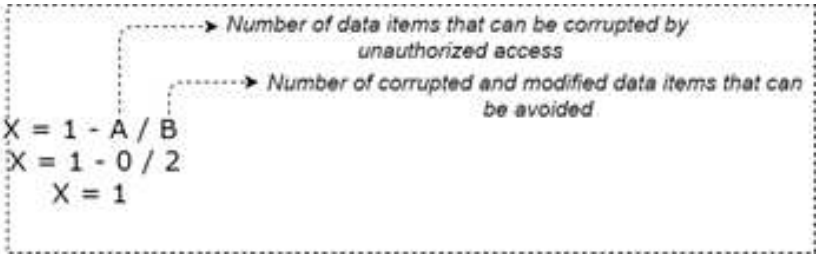
In the aspect of integrity, we have three measuring factors:

CC BY

Data Integrity

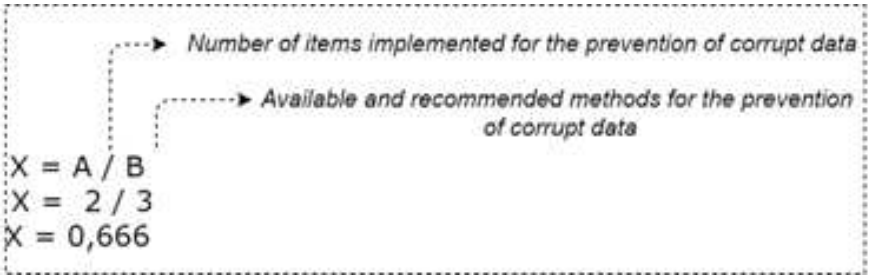
Data integrity focuses on potential threats that cause data damage, such as transaction verification control. In this context, the measurement metrics concentrate on data that can be corrupted by unauthorized access (A) acting on 0 fields and data for which corrupted and modified data can be avoided (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 $X = 1$.



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 availability. We recommended procedures for prevention, where we reached the value X = 0,666.

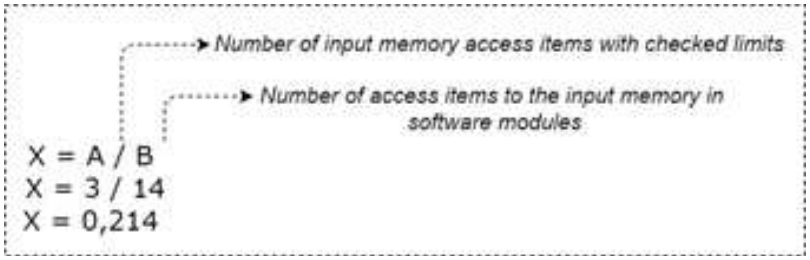
CC BY

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
- ArticleTitleandResearchLine
- RegisteredArticle
- NotificationtoReviewer
- 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:



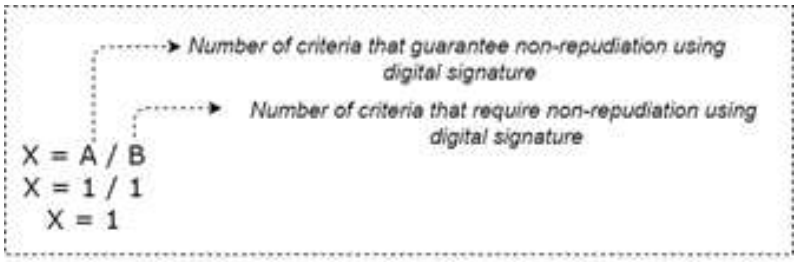
Non-Repudiation

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

CC BY

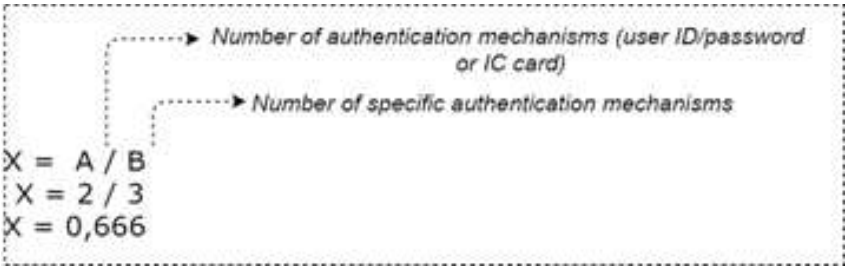
becomes immutable, besides having the date and time of insertion traceable in the system (the so-called timestamp). In this context, we identify that the maximum value of measurement in DASP fits the value $X = 1$, where the verification fields that guarantee and require non-repudiation have been filled according to the ISO formula:



EfficientAuthenticationMechanism

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



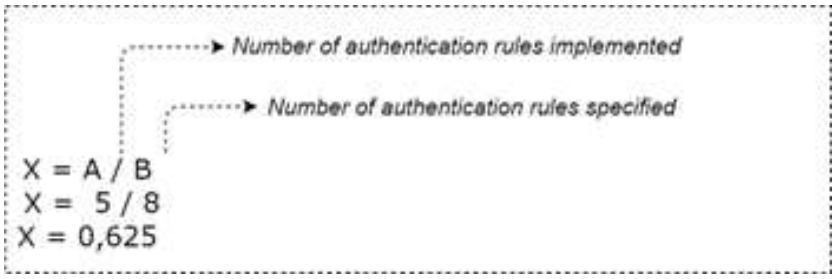
CC BY

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:

- Definingidentityclass;
- Login and logout;
- Access control filter;
- Result of the authorization of manipulation;
- Function-based access control;
- Configuringtheauthorization manager;
- Definingtheauthorizationhierarchy;
- Usingrulesof 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:



Auditing

In this aspect auditing, is associated with two fundamental points, such as:

User Access Auditing

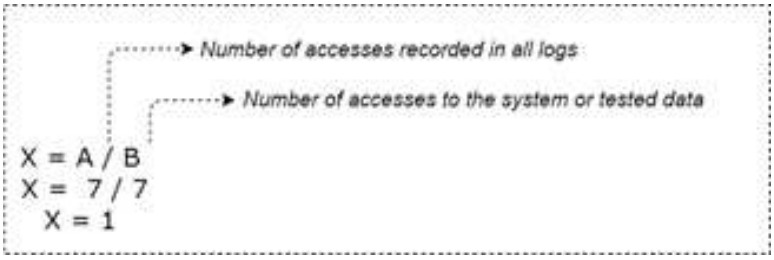
User access audit, in which we verify the measurement of the entire record of transactions made internally since the user accesses the access data. Using blockchain technology, it is possible in the application itself to generate reports of all interactions performed.

- Login
- CreateParticipant
- CreateArticle
- Composer API

CC BY

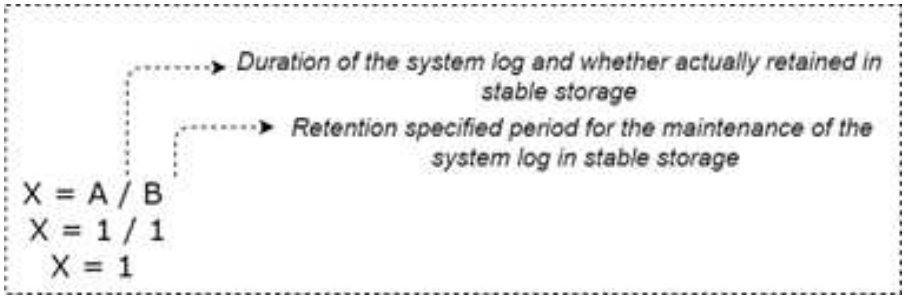
- IPFS DAEMON
- Hyperledgerfabric 1.2
- NodeJS

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



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, all the 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 $X = 1$:



Consideration

Figure 9 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 the 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.

CC BY

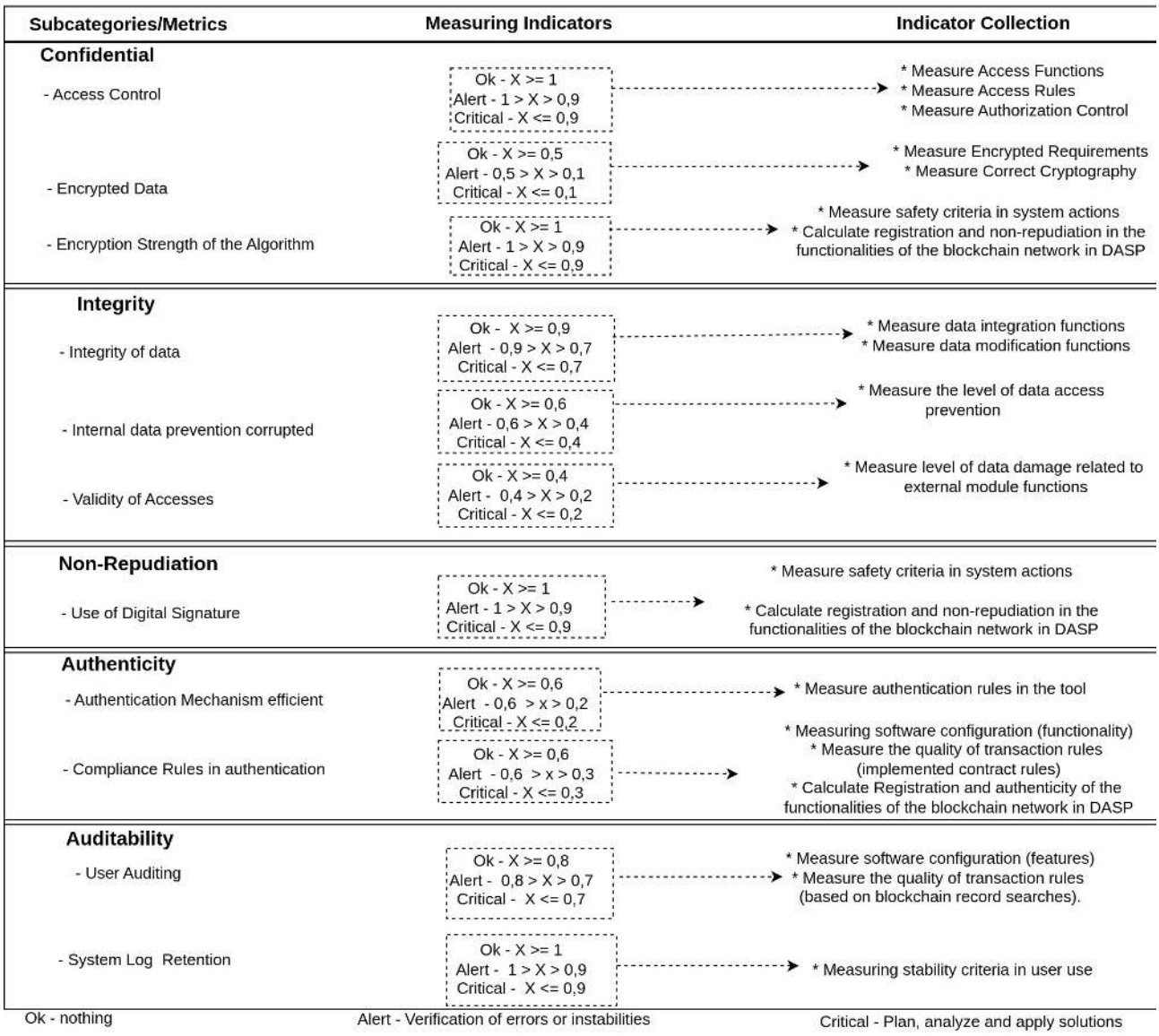


Figure 9. *DASP Security category measuring and indicators*
Font: Own elaboration (2021)

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 10, which we summarize in figure9, 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 10, generally exposes the results obtained in the DASP measurement.

CC BY

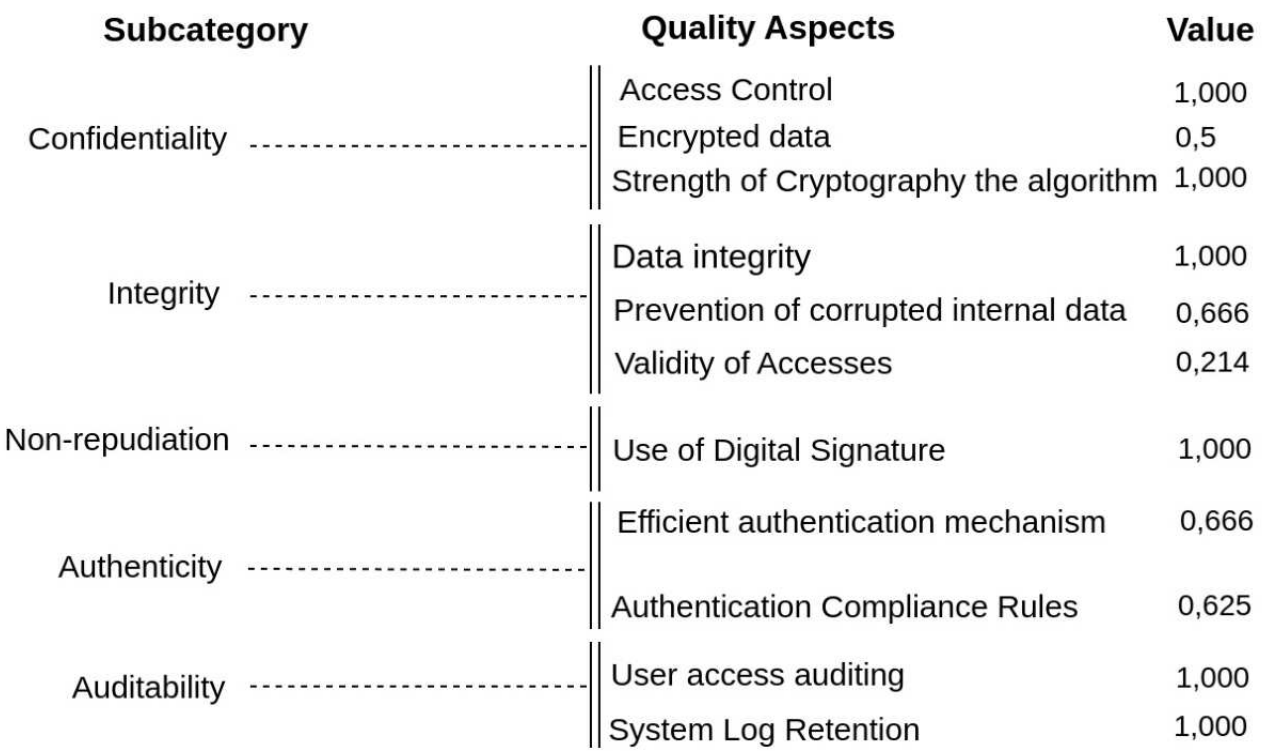


Figure 10 *Results obtained*
Font: Own elaboration (2021)

Still based on the measurement of indicators according to figure 9, 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 figure 11 to specify the criteria that need to be improved at the first moment of the measurement in the publisher.

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.

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.

CC BY

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.

Figure 11. *Recommendations for DASP Improvements according to the use of ISO 25023*
Font: Own elaboration (2021).

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.

CC BY

CONCLUSION

In this work, we presented DASP, a tool that seeks to distribute the management and 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 to 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.

In 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.

ACKNOWLEDGMENTS

This research was partially supported by National Council for Scientific and Technological Development (CNPq) and by Ministry of Science, Technology, Innovation and Communications.

REFERENCES

AIMEUR, E., BRASSARD, G., GAMBS, S., SCHONFELD, 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.

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

Blockchain solutions for scientific workflows (2018) "*Deip: Decentralized research platform".* Available online at: https://deip.world. Accessed 1n 08/19/2021.

CORREA, Elder Bruno Evaristo; NASCIMENTO, Vagner De B.; ABELÉM, Antonio JG. DASP: Distributed and Autonomic Scientific Publisher Proposal for Editorial Process Management on Permissioned Blockchain. In: *2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*. IEEE, 2021. p. 25-26.

CC BY

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 on 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.

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 onlineat: https://docs.orvium.io/Orvium-WP.pdf. Accessed on 08/19/2021.

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

CC BY