applied sciences

MDPI

Article

Notarization and Anti-Plagiarism: A New Blockchain Approach

Tonino Palmisano [1,*], Vito Nicola Convertini [1], Lucia Sarcinella [1], Luigia Gabriele [2,*] and Mariangela Bonifazi [2]

[1] Department of Informatics, University of Bari Aldo Moro, 70125 Bari, Italy; vitonicola.convertini@uniba.it (V.N.C.); lucia.sarcinella@uniba.it (L.S.)
[2] IZZ2IZZ S.r.l., 70122 Bari, Italy; bonifazi@izz2izz.it
* Correspondence: tonino.palmisano@hotmail.com (T.P.); progetti@izz2izz.it (L.G.)

Abstract: In traditional notarization processes, the correctness of the activities between the parties is guaranteed by a central authority or guaranteeing institution. In this case, the authority is not able to quickly establish the originality of the content to be notarized, or at least to have a large degree of certainty without the use of automated systems. This paper presents a new notarization platform that uses blockchain technology and integrates advanced anti-plagiarism approaches able to effectively detect copyright violations of documents that users want to notarize. In addition, our proposal includes the use of models, methods, and techniques, through which a very high level of privacy and information security can be guaranteed.

Keywords: notarization; anti-plagiarism; blockchain; copyright; privacy; decentralized app; NFT

check for updates

Citation: Palmisano, T.; Convertini, V.N.; Sarcinella, L.; Gabriele, L.; Bonifazi, M. Notarization and Anti-Plagiarism: A New Blockchain Approach. *Appl. Sci.* **2022**, *12*, 243. https://doi.org/10.3390/app12010243

Academic Editor: Gianluca Lax

Received: 24 November 2021
Accepted: 21 December 2021
Published: 27 December 2021

1. Introduction

In today's hyper-connected, data-centric society, there are still areas where some procedures or entire processes are performed in the manner of 100 years ago or so, with little modification over the decades.

One example of many is all the processes that need a central institution to be completed reliably. The issuance of currency, the buying and selling of real estate, the signing of contracts between two or more parties (e.g., by means of signature [1]), and certification processes in general belong to this category.

Currently, we have emerging technologies such as artificial intelligence and blockchain at our disposal, which can come to the aid of overcoming the limitations of these outdated processes.

Blockchain technology in recent years has disrupted finance by supporting the development and creation of self-regulated cryptocurrencies. Leading examples in this regard are Bitcoin [2,3] and Ethereum [4,5], two of the world's most popular cryptocurrencies. To understand the disruptive capacity of blockchain technology, simply consider that Bitcoin has reached a market capitalization of over $1 trillion as of February 2021 [6], outperforming the market capitalization of gold by about 7% as of January 2021 [7].

Thus, having established that blockchain technology can be an operational lever in the previously listed areas (but also in many others), in this paper, we focus our attention on notarization and anti-plagiarism.

One of the main problems in this context consists of the impossibility of objectively verifying the authenticity of documents (or media in general), without the help of a central body such as a public notary. In these cases, blockchain technology is perfectly suited to overcome the limitations of current methods and systems due to its intrinsic characteristics as, for example, the concept of trust, that technology allows not needing a central body to attest to the truthfulness and correctness of any transaction recorded between two or more parties. In fact, as also highlighted by Beck et al. [8], through blockchain technology, it is possible to carry out secure transactions transcending trust, and it is very likely that, overcoming some limitations of scalability and related to the cost of transactions, this technology can completely replace the current processes and systems based on trust.

Blockchain technology is proving to be promising in terms of developing disruptive models, methods, and techniques capable of shaping the economy and life in our society and future societies.

We will focus on the potential of blockchain technology in notarization processes integrated with anti-plagiarism functionalities. In fact, there is currently no block-chain-based notarization tool available that integrates the functionalities of an anti-plagiarism system in order to verify the originality of media that users try to submit for notarization.

Therefore, in the following, some concepts regarding notarization and anti-plagiarism will be introduced. Preferable features of a system in this area will be exposed. In addition, a census of the solutions currently on the market will be made, distinguishing notarization from anti-plagiarism. Finally, a proposed solution that integrates all the identified features either for notarization or anti-plagiarism will be described.

2. Notarization

Traditionally, the process of notarization consists of a set of activities designed to assure the parties involved in a transaction (e.g., formation of a company, patent application, intellectual property protection) that the documents attesting to it are authentic [9].

All these activities involve various stakeholders, ranging from the party's requesting notarization to the central authority that, by way of simplification, ensures the veracity and the legal validity of the necessary documents and the signatures applied to those documents. In essence, the central institution ensures the validity of the transaction by overseeing the process.

Take into consideration three different perspectives: the notary's perspective, the grantor of the power of attorney perspective, and the IT administrator perspective. The analysis from these three different perspectives performed by Arredondo [10] gives us a preliminary view of some of the high-level requirements needed to implement a blockchain-based notarization service.

As also pointed out by Maesa and Mori [11], it emerges that one of the main aspects to be taken care of is the timing of data registration on blockchain. Depending on the congestion of the blockchain network used, there can be even a few hours difference between the time when the data registration on blockchain is requested and the time when it actually happens. In addition, the need emerges to save the submitted documents in some way in a repository [10], to be available when there is a need to verify their legitimacy.

There are several blockchain-based notarization apps on the market today, both decentralized and centralized. In order to compare them, we identified the features and the functionalities that a notarization app should have. For notarization apps, these are:

- Supported blockchains;
- File custody service;
- Hash custody service;
- P2P file custody service;
- Free space size;
- Type of archive server (centralized or decentralized);
- Notarization Report (PDF);
- Custom notarized file template;
- Multiple digital signatures;
- File sharing; and
- Massive file upload.

The first basic feature for the notarization apps considered in this paper is the supported blockchain(s). The most basic notarization apps should use only one blockchain, while more advanced ones should use more than one.

The goal of using multiple blockchains is to have backup and redundancy services available. When—even if it is a remote possibility—all nodes in a network are turned off, using a single blockchain the user would not be able to access the notarized files. Instead, using a redundancy mechanism, the files requested by the user at the time of a network of nodes going down would still be available.

The file custody service consists of storing the notarized file in a dedicated user space. This will ensure that the file will always be available to the users when they need to prove the trustworthiness of the file recorded within the blockchain.

Similar to the file custody service, the hash custody service allows users to have access to the hash of each and every previously notarized file.

The P2P file custody service would allow the notarized file to be split in many small fragments within the blockchain being used. This makes it impossible to reconstruct a file unless you are the owner of the file. In this context, any latency and speed issues in retrieving files from the blockchain network can be solved through the application of edge computing and edge caching principles. The effect is twofold. In addition to increased performance in file retrieval, there are added benefits in terms of privacy preservation and in terms of security [12].

Reliability is also guaranteed, because in the event that several nodes on the network fall at the same time, the edge caching file retrieval system will repair them and make them available to the user at the same time as a file is retrieved from the network. There are also very substantial advantages in reducing costs. In fact, by distributing the nodes around the world, the use of additional HW is not required. This will lead to a significant reduction in equipment investment costs.

Regarding the amount of memory space made available to the user, having a memory space available in the cloud, accessible directly from the notarization app, would allow the user to save a number of previously notarized files, hashes, and notarization reports in the cloud (dependent on the amount of memory space available). Within this memory space in the cloud, the user can call up files, hashes, and reports.

The type of archive server indicates whether the app uses a centralized or decentralized archive. A decentralized type of server is preferable, because it overcomes the limitations of centralized servers, both from the point of view of reliability and cyber security, and from the privacy protection perspective.

For example, as shown in several papers, in healthcare, patients' privacy is of critical importance. In [13], the importance of patient data is emphasized; here, we talk about patient-generated health data and their possible exploitation in applications that draw on data generated by wearable devices. In [14], the security for healthcare systems based on pervasive social networks is discussed and again privacy preservation plays a key role. To counteract the problems related to privacy preservation, Yue et al. [15] propose an architecture called HDG (healthcare data gateways), which uses a private blockchain cloud to store highly sensitive encrypted patient data. Al Omar et al. [16,17] propose a new blockchain completely oriented towards privacy protection of health data. Kuo and Hono-Machada [18] propose blockchain technology (along with machine learning techniques) for predictive health modeling and to protect privacy in operations that require interoperability between different institutions. Houtan and Makrakis [19] focus on the concepts of electronic health record and patient health record as the core of blockchain-based applications in healthcare. They perform a literature study highlighting the various approaches used and analyze the proposed solutions considering the advantages and disadvantages of using blockchain technology in different forms, including from a privacy protection perspective. Kasyap and Tripathy [20] highlight the criticalities of some systems currently used in healthcare proposing a framework based on the adoption of blockchain technology to overcome the limitations of such solutions, preserving privacy and ensuring a higher level of security.

In IoT, privacy protection and security are equally important as in healthcare. For Dorri et al. [21], an approach based on the use of blockchain technology can provide a decentralized privacy and security solution that respects the principles of confidentiality, integrity, and availability, more commonly known as CIA. Panarello et al. [22] also agree that blockchain technology is very effective in addressing security threats and protecting privacy. They also show how much the concept of privacy is related to that of security, and how the key features of blockchain technology can help. Another study on how blockchain technology can be used to improve security and protect privacy is reported in the paper by Zhu and Badr [23], in which the possible architectural solutions available in the literature for a blockchain-based identity management system are explored, also focusing on the security that this type of solution is able to provide in the IoT context. Dwivedi et al. [24] propose a model framework that involves the use of wearable IoT devices to capture patient data that will then be manipulated and used in medical systems. They, too, put blockchain technology at the center for solving issues related precisely to privacy and security. Mohanta et al. Mohanta et al. wrote a paper [25] in 2020 focused on the security and privacy challenges in IoT. They identified blockchain as an enabling technology for solving the analyzed problems. Additionally, in the recent paper by Alfandi et al. [26], it is highlighted how blockchain technology can be a pillar to overcome the limitations of other existing technologies and methodologies to protect privacy and to make systems more secure; in this case, decentralized IoT systems.

All these works, with their solutions and proposals, are just a few of the countless examples that can be found in the literature. They have as a common denominator the use of blockchain technology as a possible solution to the privacy and security issues that may exist in the use and manipulation of highly sensitive data.

Having focused on these fundamentally important aspects, such as security and privacy, let us move on to the other features that a notarization app should offer.

A notarization app should provide a notarization report (e.g., in PDF) to be able to easily show the immutability of a file recorded in a sure date on blockchain.

It would also be helpful for users to have a set of custom templates available for drafting files to be authenticated. For example, in drafting certificates for completion of training courses, each school or training institution can thus draft its own custom template from the one provided, with logos, custom graphics, and specific wording. In this way, users would have a tool similar to Microsoft Word templates to be used to speed up the drafting of the most commonly used documents (e.g., course certificates, contracts from standard templates such as OSCON [27], etc.), to be notarized later.

The multiple digital signature service, on the other hand, would allow multiple users to digitally sign the same file to be notarized (e.g., a private deed between two or more people).

The file sharing service would serve as a way for a user to demonstrate to another person, or legal entity, that they are the owner of the notarized information. Coupled with the generation of an applicable QR code on a document, it would make that document inviolable from a copyright perspective.

Finally, massive loading of files would allow notarization of an entire set of files, notarizing every file in the set in a single operation. The massive upload can also be useful for notarizing many files that contains other files, such as archive files that contain other files. In this specific case, the notarization would be for the archive file.

3. Anti-Plagiarism

When we think of anti-plagiarism systems, we usually refer to systems that protect intellectual property, especially in music or art. Blockchain technology is able, even in this area, to provide a particularly useful support.

Currently, there is no single system universally recognized as a standard in the field of anti-plagiarism, although, in recent years, in the international literature, and therefore in the scientific community, the direction that is perceived is that of the use of blockchain technology as an enabler. This technology, in fact, could potentially succeed in ensuring adequate protection of copyright. For example, Jing et al. [28] propose a specific solution for source code copyright protection through blockchain. Andi et al. [29] focus on plagiarism in the scientific community and propose a possible use of blockchain technology to curb plagiarism in scientific publications. Seo et al. [30] propose a platform for anti-plagiarism control of web content by exploiting the features of blockchain technology.

These are just a few of the countless examples found in the literature from which the industry takes its cues. All these solutions, however, struggle to achieve widespread global adoption and market acceptance.

From the implementation point of view, regarding anti-plagiarism systems, the features that an app should have include:

- Supported antiplagiarism system;
- P2P file custody service;
- Free space size;
- Languages supported;
- Anti-plagiarism report (PDF); and
- File sharing.

A supported antiplagiarism system refers to the set of technologies used as an ecosystem to support the platform for antiplagiarism audits. This can be web only, web plus database, or web plus database plus repository. In terms of the databases used, it can be public, private, or both public and private. The repository, on the other hand, is used to collect information for the creation of a knowledge base from which to draw for antiplagiarism audits.

Regarding the characteristics of the P2P file storage service, the size of the free space available, and the file sharing service, the same applies as mentioned above about the desired characteristics of notarization apps.

As previously mentioned for notarization apps, regarding the free space size available to the user, this is a very useful feature, because it allows the user to save a number of previously verified files and anti-plagiarism reports in the cloud (dependent on the amount of space available). As for notarization apps, within this space, the user can recall files and anti-plagiarism reports.

In the case of antiplagiarism verification on text files, an antiplagiarism app should cover as many languages as possible, because, in this way, a higher level of accuracy in discovering possible plagiarism in other languages than the original text can be achieved.

Finally, an anti-plagiarism app should return a report to the user, preferably in PDF format for interoperability, summarizing the information detected about possible plagiarism.

4. Comparative Analysis

Taking into consideration the previously desired features for a notarization app, we can evaluate the adherence of the identified notarization solutions to these features.

4.1. Notarization Blockchain-Based Apps

All the apps analyzed in this paper use the SHA-256 algorithm [31] for generating the hash of the file(s) to be notarized.

The Noberasco app “Opentimestamps” [32] is a web-app based on the Bitcoin (BTC) blockchain [2,3]. It is an app that allows you to put a “time stamp” on a file by selecting it and without uploading the file to the Noberasco servers. This is to preserve the privacy of users. The system returns a file to the user with ”.ots” extension that contains the proof of notarization. Noberasco also allows you to verify the date of existence of a file by uploading the previously returned file with ”.ots” extension and by selecting the original file that will not be uploaded to the server. It does not offer any other functionality.

The “BCH Notary” app [33] allows you to attest to the ownership of a file, using the Bitcoin cash (BCH) blockchain [34] at a cost of 0.0002 BCH. In this app, you can only notarize and verify the ownership of a document by selecting it on local machine. The file will not be uploaded to their servers. It does not support any additional functionality.

The “Chainsign” app [35] is based on the EOS blockchain [36,37]. This app notarizes files for free. Chainsign locally calculates the hash of the file being notarized without uploading to a server. It is also possible to enter the web address of a file to be notarized.

The hash algorithm used is SHA256. Chainsign does not offer further functionalities beyond those described above.

The app called CERTO [38,39] performs notarization of files using the NXT blockchain [40,41] and the multichain platform "Ardor" [42,43]. CERTO allows for notarization of individual files, and it is possible to also have the function of chain of custody. Finally, it is possible to obtain a notarization report in PDF format. No other functionality is supported.

Quadrans Foundation [44] offers a free tool for notarizing files [45,46], a centralized app based on the Quadrans blockchain [47]. The notarization process is entirely managed via email. Among the available features, there is the notarization of several files at the same time, but the user is asked to insert all the files to be notarized in a single archive. So, the entire archive is notarized and not the single file it contains. Furthermore, the notarization system offered by Quadrans Foundation uses a centralized archive server.

Dedit [48,49] propose a centralized app that uses the user browser to run the SHA256 algorithm to notarize files. Only the hash of the file, plus some metadata, are transmitted to Dedit's centralized server. The hash is recorded on the Algorand blockchain [50–52] with a timestamp. At the end of Dedit's notarization process, a PDF report is made available to the user. In addition, Dedit offers a file custody service (not P2P) with a free space available of 10 MB, a multiple digital signature service, and a file sharing service.

In the table below, we made a check of the desirable features for each notarization app considered.

As shown in Table 1, none of the notarization apps considered encapsulate all the desired features. In detail, even though all notarization apps analyzed allow you to notarize a file, none of the analyzed solutions offer P2P file custody services or a decentralized type of archive server, not adequately ensuring the privacy and security of the information contained in the notarized files. In addition, none of the solutions provide a custom template for notarized files and a massive file upload feature to help users with tasks in the notarization process. Finally, the free storage space provided by only one of these solutions is only 10 MB, which is too small to store large files (such as dissertations, project documents, AutoCAD files, etc.).

Table 1. Notarization apps features.

	Noberasco	BCH Notary	ChainSign	Certo	Quadrans	Dedit
Web site	[32]	[33]	[35]	[39]	[46]	[48]
Supported Blockchains	BTC	BCH	EOS	Ardor NXT	Quadrans	Algorand
File Custody Service	NO	NO	NO	NO	NO	YES
Hash Custody service	YES	YES	YES	YES	YES	YES
P2P File Custody Service	NO	NO	NO	NO	NO	NO
Free Space Size	NO	NO	NO	NO	NO	10 MB
Type of Archive Server [1]	NO	NO	NO	NO	C	C
Notarization Report (PDF)	NO	NO	NO	YES	YES	YES
Custom Notarized File Template	NO	NO	NO	NO	NO	NO
Multiple Digital Signatures	NO	NO	NO	NO	NO	YES
File Sharing	NO	NO	NO	NO	NO	YES
Massive File Upload	NO	NO	NO	NO	NO	NO

[1] C = Centralized, D = Decentralized.

4.2. Anti-Plagiarism Blockchain-Based Apps

PlagioScanner [53] offers an anti-plagiarism service mainly aimed at university students for thesis verification. By uploading a file, it performs verifications anonymously using both web and database system support and costs EUR 0.33per page to analyze. PlagioScanner service is able to analyze up to 40 pages in 6 min and offers users a complete and downloadable report in which are indicated the parts of text liable to plagiarism. It also supports up to 129 different languages. PlagioScanner does not offer any additional features or services compared to those identified as desirable.

ZeroPlagio [54] also aims to be a university-focused anti-plagiarism app. The supported anti-plagiarism system works both via web and via database. The anti-plagiarism service offered is anonymous and costs EUR 0.33 for each uploaded page. It also supports up to four different languages and provides a detailed report in PDF format. ZeroPlagio does not support any other features or services.

Among the different services offered by Grammarly writing assistant [55], there is also a plagiarism checker service [56] that works on uploaded files by the users. The antiplagiarism service offered by Grammarly is only supported by a web verification system. It does not use a database. It also supports three languages for antiplagiarism checks and provides a PDF report for the user. Grammarly Plagiarism Checker does not have costs based on the amount of text to be translated but has subscription plans that start at USD 12 per month. It does not offer other services.

Dupli Checker [57] allows one to perform antiplagiarism checks either by uploading documents in various formats or by using a URL of a web page. The verification system supports web mode only. Checks are performed in seven languages and return a PDF report to the user. In terms of costs, Dupli Checker provides subscription plans with limitations on the number of search queries and the number of total words. No additional functionality is provided.

Plagiarism Checker [58] uses only a web-based verification system (no database). Plagiarism checking is performed in several ways. You can upload a document in one of the supported formats, or you can paste plain text directly on the web page, or you can connect to a Dropbox account. The system provides support for anti-plagiarism checks in 21 different languages and provides an anti-plagiarism report in PDF format. From the cost point of view, Plagiarism Checker offers several subscriptions and customizable plans, starting from 10 USD/month, with limitations on search queries, immediacy of PDF reports, batch searches, and use of additional side features (e.g., citation assistant, text comparator, and URL text comparator). It does not offer additional features and/or services.

In the following table, we made a checklist of the desirable features for each anti-plagiarism app considered.

Table 2 shows that all the systems analyzed support the use of the web system for anti-plagiarism analysis. Only PlagioScanner and ZeroPlagio also use a database for more effective plagiarism analysis. Almost all anti-plagiarism systems return a detailed report to the user, except PlagioScanner. Regarding the supported languages, instead, the anti-plagiarism systems considered support at least three languages as in the case of Grammarly, up to a maximum of 129 for PlagioScanner.

Table 2. Anti-Plagiarism Apps Features and Services.

Feature or Service	PlagioScanner	ZeroPlagio	Grammarly	Dupli Checker	Plagiarism Checker
Web Site	[53]	[54]	[56]	[57]	[58]
Anti-Plagiarism system supported	Web + DB	Web + DB	Web	Web	Web
P2P file storage service	NO	NO	NO	NO	NO
Free Space Size	NO	NO	NO	NO	NO
Supported languages	129	4	3	7	21
Antiplagiarism report (pdf)	NO	YES	YES	YES	YES
File sharing	NO	NO	NO	NO	NO

None of the anti-plagiarism systems considered support P2P file storage service, nor do they provide free space to the user, nor do they support file sharing.

In conclusion, none of the analyzed anti-plagiarism systems are compliant with all the features and the services identified as desirable.

5. Proposed Solution

Solutions have been found that implement only the notarization process or only the anti-plagiarism process. The proposed solution solves both problems of integrating in a single process all the activities necessary for notarization and antiplagiarism, and the problems concerning security and privacy protection through the proposed technological methodologies.

The proposed solution consists of a decentralized app that embraces all the previous mentioned functionalities and services, both for notarization and anti-plagiarism. In fact, the ideal solution must perform the notarization process by verifying, which is imperative, that the content submitted for notarization by users is free of plagiarism. As mentioned above, moreover, the anti-plagiarism system must cover as many languages as possible and use both web and database support in order to guarantee with a high degree of reliability that the anti-plagiarism check is carried out correctly. In the following Figure 1 there's the proposed solution schema.

The proposed decentralized app prototype includes a frontend that uses a service to manage notarization operations, a service for operations involving anti-plagiarism and a service for generating NFTs (non-fungible tokens) [59] that can be accessed internally using advanced API.

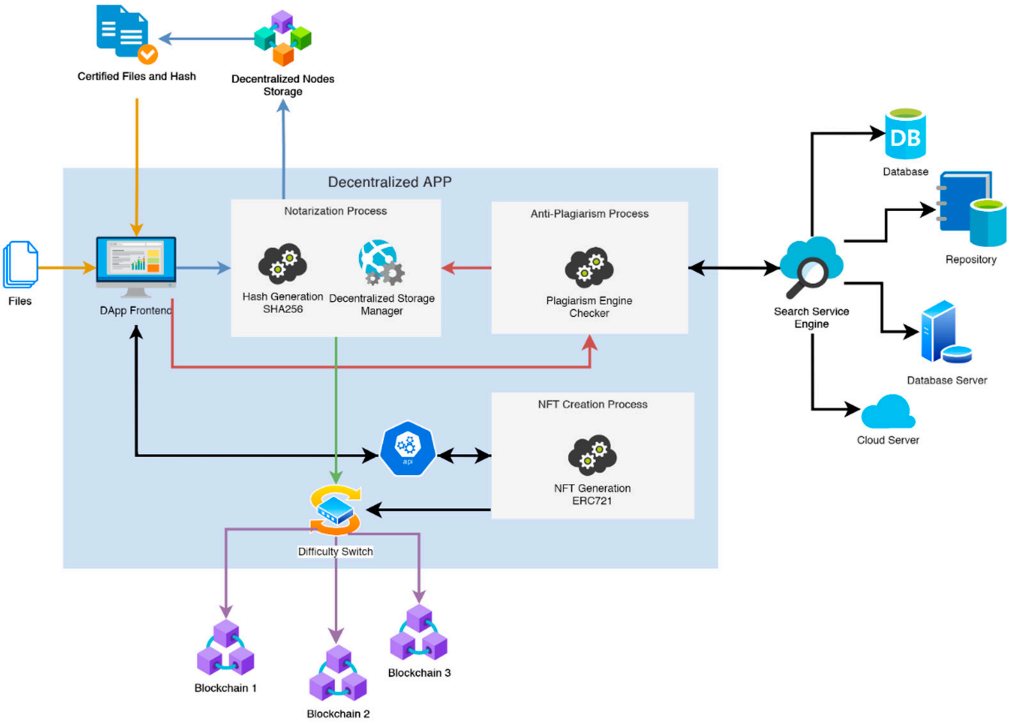

Figure 1. Proposed solution schema.

The set of public databases, private databases, and repositories required for antiplagiarism checks are external to the proposed solution. Some examples of third-party solutions that can be used in this context are Unicheck [60] and Oxico [61].

Another important element of the prototype is the difficulty switch for selecting the cheapest blockchain to store notarization information and NFTs created with ERC721. The decentralized app also allows for the creation of an NFT from the notarized files, according to ERC-721 (Ethereum request for comments 721) standard [62].

One more key characteristic is the use of a P2P file storage system. In the proposed solution, we implemented this by the use of a decentralized node storage. This is in order to raise the level of privacy assurance, especially for all those files that contain sensitive user data. The use of blockchain technology is able to guarantee data integrity [63]. Experimental tests, in fact, show that audit mechanisms [63,64] can also increase resistance to data integrity threats such as binding attacks [64], at least as long as quantum computers will not be used to crack cryptographic keys [63]. There are several solutions to implement P2P file storage system, such as Internxt [65] and Sia [66].

Regarding the exploitation of blockchain technology within such a system, first of all, by supporting more than one blockchain, a high degree of reliability can be achieved in case of a significant drop in a network of nodes. This will reduce costs and eliminate potential data loss. From a transaction affordability perspective, selecting the network with the lowest transaction cost and scheduling the use of the other two with a low priority result in a low, scheduled cost. Obviously, the cost is greatly reduced compared to the immediate storage operation on all used blockchains. Moreover, it is possible to change the notarization process according to the type of blockchains when the mining difficulty increases, with a heavy saving in transaction costs. If one of the blockchains becomes saturated, a switching mechanism of the primary network to be used is applied. For example, in 2017, when BTC reached USD 21,000, average transaction fees exceeded USD 62 [67] due to the massive number of purchase requests; in this case, the difficulty of the network was very high due to the high number of transactions required, so the transaction costs rose exponentially.

In this context, such rates would be impractical for the goal of lowering, by several orders of magnitude, notarization costs, so the switching mechanism will use the blockchain network with the highest rates as last, queuing up the transaction with the lowest possible priority to pay the lowest rates on that network. Even though it will take longer for the transaction to register on the latter network, it does not matter, because the transaction will already be registered on the faster and cheaper network.

In order to understand how the existing internal components and processes within the proposed solution work, we describe two of the possible usage scenarios below.

5.1. Notarization of One or More File

In the first example scenario, the proposed solution acquires one or more files to be authenticated from the user. Before the actual notarization, an antiplagiarism check of the submitted files is performed, using the Plagiarism Engine Checker that interfaces with the Search Service Engine component. The latter is composed of third-party APIs that are used to perform all the plagiarism checks using both public and private databases and repositories. Possible plagiarism is searched on heterogeneous sources and on all available media. To pass the check, it is necessary to obtain a reliability of 80% or more, i.e., the content of the files can contain a maximum of 20% of non-original content (deriving from quotations and similar) in order not to plagiarize other works. At this point, the decentralized app initiates two separate processes that use the ecosystem. One process is used to create the fingerprint (hash), and a separate process is used to perform the fragmentation of the files and store them in the decentralized node storage.

The creation of the hash from the submitted files, is performed through the use of the SHA256 encryption algorithm [31], which, in addition to ensuring very high standards of cryptographic security, allows quick identification of any transaction on the blockchain network. The hash of the files is recorded on three different blockchains to ensure, as previously mentioned, high reliability in case of saturation and/or collapse of a blockchain network. So that the difficulty level of the algorithm does not interfere with the network speed and transaction costs, the difficulty switch is used to decide where it is most convenient to store the file hash first in terms of cost/speed ratio.

After storing the hash on at least one of the blockchain networks, the process of fragmenting and storing the files by the component called "Decentralized Storage Manager" can start. This process consists of encrypting the files and splitting them into n different segments. Each segment is then encrypted with n different randomized encryption keys. Finally, each encrypted segment is deployed on the decentralized nodes storage (on a large number of nodes, depending on the characteristics of the edge-cloud infrastructure). The proposed solution then generates the certificate of authenticity of the submitted files, containing the previously generated hash and the transaction on the used blockchain.

A total of three certificates of authenticity will be generated, one for each of the three blockchains used.

At this point, the proposed solution will allow the user, starting from the hash in his possession, to recover the notarized files, reconstructing the structure present within the decentralized nodes.

5.2. NFT from Notarized Files

After the notarization and anti-plagiarism operations described earlier, the user will have available in his memory space the list of files submitted to the decentralized app. These files can be transformed, upon explicit request of the user, into an NFT to facilitate and guarantee the process of transferring the ownership of the files in question.

Moreover, the proposed solution, if connected through APIs, can allow the sale of notarized files on third party marketplaces, always guaranteeing their originality and content.

6. Conclusions and Future Works

Currently, no solution has been found that integrates all the processes and functionalities explained above. In this way, the potential of using an integrated environment in which to perform all the functions described above with all the advantages that derive from it is overshadowed. Therefore, the proposed solution may represent a disruptive revolution in this ambit as the only candidate to innovate the notarization process with the exploitation of new enabling technologies and methodologies (e.g., blockchain, P2P storage service, difficulty switch, etc.), and that integrating an anti-plagiarism system allows users to have the almost absolute certainty that the content submitted to notarization is original. Moreover, the prototype brings a further innovation by introducing the possibility to create NFTs of the notarized files. This gives users an additional way to prove ownership of the files, further strengthening the notarization concept, while also having a tool to easily transfer the ownership of these files.

Our prototype also appears interesting because it allows several advantages to be obtained from different points of view. From an economic point of view, there are numerous advantages, both in terms of the total cost of notarization operations compared to a traditional notarization process and in the use of the switching mechanism across multiple blockchains that further optimizes and lowers platform costs.

From the point of view of the integrated process, it is not necessary to draw on several different services, but it is possible to obtain notarization, antiplagiarism, and NFT generation, starting from one or more files, through the use of a single decentralized app.

From a security perspective, instead, as we have already seen previously, in case of a blockchain network crash, we can use backup networks. In addition, notarized files are stored in a fragmented manner, so no one but the owners of the files has the ability to reconstruct them. According to digital preservation regulations, a file must meet the requirements of "accessibility, usability, authenticity, and retrievability of documents," or a "process" whose purpose is to ensure that certain documents not only can be found over time but also remain intact. With our decentralized servers, we can solve this problem. In addition, we can achieve high resistance to attacks, because decentralized architectures offer enormous advantages for data integrity. In fact, wide distribution across geographies makes it impossible to reconstruct files, which also makes them resistant to the much-feared ransomware attacks.

Future developments come through obtaining resources for industrialization of the prototype, first of all to implement an API system to make the process highly versatile, scalable, interoperable, and usable externally from other ecosystems. In the future, the utilization of the decentralized storage system will be improved in terms of versatility by implementing additional services based on advanced encryption and file-sharing systems. The decentralized file storage will be also enhanced through the use of the latest technological innovations in decentralization. Moreover, the experimentation of the prototype will be carried out to be industrialized with strategic partners, testing both the stability and the security of the system by penetration test, stress test, and everything necessary to ensure security against attacks to the decentralized app.

Author Contributions: Conceptualization, L.G.; Formal analysis, M.B.; Investigation, M.B.; Project administration, L.G.; Supervision, T.P.; Writing—original draft, T.P.; Writing—review & editing, T.P., V.N.C. and L.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by IZZ2IZZ S.r.l.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Impedovo, D.; Pirlo, G. Automatic Signature Verification in the Mobile Cloud Scenario: Survey and Way Ahead. *IEEE Trans. Emerg. Top. Comput.* **2021**, *9*, 554–568. [CrossRef]
2. Bitcoin.org. Bitcoin—Open source P2P Money. 2021. Available online: https://bitcoin.org (accessed on 27 July 2021).
3. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 21 July 2021).
4. Ethereum.org. Home | ethereum.org. 2021. Available online: https://ethereum.org/en/ (accessed on 20 July 2021).
5. Buterin, V. A Next Generation Smart Contract & Decentralized Application Platform. 2013. Available online: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 21 July 2021).
6. ANSA. Bitcoin Supera 1.000 Miliardi di Capitalizzazione—Economia—ANSA. 2021. Available online: https://www.ansa.it/sito/notizie/economia/2021/02/19/bitcoin-sale-ancora-e-supera-i-53.000-dollari-nuovo-record_c896efd9-ab4f-4175-8ea6-97a59e1b34e4.html (accessed on 21 July 2021).
7. criptovalute24.com. Bitcoin Alle Stelle: Bitcoin BTC Supera l'oro nel 2021. 2021. Available online: https://www.criptovalute24.com/bitcoin-btc-supera-l-oro/ (accessed on 21 July 2021).
8. Beck, R.; Czepluch, J.S.; Lollike, N.; Malone, S. Blockchain—The Gateway to Trust-Free Cryptographic Transactions. In Proceedings of the Twenty-Fourth European Conference on Information Systems (ECIS), Istanbul, Turkey, 12–15 June 2016.
9. NNA (National Notary Association). What Is Notarization—National Notary Association. 2021. Available online: https://www.nationalnotary.org/knowledge-center/about-notaries/what-is-notarization (accessed on 21 July 2021).
10. Arredondo, A. *Blockchain and Certificate Authority Cryptography for an Asynchronous On-Line Public Notary System*; The University of Texas: Austin, TX, USA, 2017.
11. Di Francesco Maesa, D.; Mori, P. Blockchain 3.0 applications survey. *J. Parallel Distrib. Comput.* **2020**, *138*, 99–114. [CrossRef]
12. Weisong, S.; Xingzhou, Z.Y.W.; Qingyang, Z. Edge Computing: State-of-the-Art and Future Directions. *J. Comput. Res. Dev.* **2019**, *56*, 69–89.
13. Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016.
14. Zhang, J.; Xue, N.; Huang, X. A Secure System for Pervasive Social Network-Based Healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [CrossRef]
15. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef] [PubMed]
16. Al Omar, A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. *Future Gener. Comput. Syst.* **2019**, *95*, 511–521. [CrossRef]
17. Al Omar, A.; Rahman, M.S.; Basu, A.; Kiyomoto, S. MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. *Lect. Notes Comput. Sci.* **2017**, *10658*, 534–543. [CrossRef]
18. Kuo, T.-T.; Ohno-Machado, L. ModelChain: Decentralized Privacy-Preserving Healthcare Predictive Modeling Framework on Private Blockchain Networks. *arXiv* **2018**, arXiv:1802.01746.
19. Houtan, B.; Hafid, A.S.; Makrakis, D. A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare. *IEEE Access* **2020**, *8*, 90478–90494. [CrossRef]
20. Kasyap, H.; Tripathy, S. Privacy-preserving Decentralized Learning Framework for Healthcare System. *ACM Trans. Multimed. Comput. Commun. Appl.* **2021**, *17*, 1–24. [CrossRef]
21. Dorri, A.; Kanhere, S.S.; Jurdak, R. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 13–17 March 2017; pp. 618–623. [CrossRef]
22. Panarello, A.; Tapas, N.; Merlino, G.; Longo, F.; Puliafito, A. Blockchain and IoT Integration: A Systematic Survey. *Sensors* **2018**, *18*, 2575. [CrossRef] [PubMed]

23. Zhu, X.; Badr, Y. Identity Management Systems for the Internet of Things: A Survey towards Blockchain Solutions. *Sensors* **2018**, *18*, 4215. [CrossRef] [PubMed]
24. Dwivedi, A.; Srivastava, G.; Dhar, S.; Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* **2019**, *19*, 326. [CrossRef] [PubMed]
25. Mohanta, B.K.; Jena, D.; Ramasubbareddy, S.; Daneshmand, M.; Gandomi, A.H. Addressing Security and Privacy Issues of IoT using Blockchain Technology. *IEEE Internet Things J.* **2020**, *8*, 881–888. [CrossRef]
26. Alfandi, O.; Khanji, S.; Ahmad, L.; Khattak, A. A survey on boosting IoT security and privacy through blockchain. *Clust. Comput.* **2021**, *24*, 37–55. [CrossRef]
27. Oscon. Fac Simile di Contratto—Oscon. 2021. Available online: https://oscon.it/ (accessed on 18 August 2021).
28. Jing, N.; Liu, Q.; Sugumaran, V. A blockchain-based code copyright management system. *Inf. Process. Manag.* **2021**, *58*, 102518. [CrossRef]
29. Andi; Purba, R.; Yunis, R. Application of Blockchain Technology to Prevent the Potential of Plagiarism in Scientific Publication. In Proceedings of the 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, 16–17 October 2019; pp. 1–5. [CrossRef]
30. Seo, T.-H.; Byun, M.; Lee, H.-S. Development of Web Content Similarity Search Platform using Blockchain. *J. Digit. Contents Soc.* **2020**, *21*, 165–172. [CrossRef]
31. NIST (National Institute of Standards and Technology). *Secure Hash Standard*; FIPS Pubs (Federal Information Processing Standards Publications); NIST: Gaithersburg, MD, USA, 2002.
32. Noberasco—Opentimestamps. 2021. Available online: https://noberasco.theblockchains.it/opentimestamps (accessed on 16 July 2021).
33. Bitcoin.com. BCH Notary | Bitcoin.com. 2021. Available online: https://notary.bitcoin.com/ (accessed on 16 July 2021).
34. Bitcoincash.org. 2021. Available online: https://bitcoincash.org/ (accessed on 27 July 2021).
35. ChainSign. Proof of Existence and Ownership by Blockchain, a Blockchain Timestamp Service. 2021. Available online: https://chainsign.app/ (accessed on 19 July 2021).
36. Eos.io. Home—EOSIO Blockchain Software & Services. 2021. Available online: https://eos.io (accessed on 19 July 2021).
37. Eos.io. Documentation/TechnicalWhitePaper.md at Master EOSIO/Documentation GitHub. 2018. Available online: https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md (accessed on 19 July 2021).
38. CERTO. Blockchain: Certifica l'autenticità della tua opera con un click | CERTO. 2021. Available online: https://certo.legal (accessed on 19 July 2021).
39. CERTO. ART Certo | Home. 2021. Available online: https://app.certo.legal (accessed on 19 July 2021).
40. Jelurida. What is Nxt? | Jelurida. 2021. Available online: https://www.jelurida.com/nxt/what-is-nxt (accessed on 19 July 2021).
41. Nxt Community. Nxt Whitepaper. 2014. Available online: https://www.jelurida.com/sites/default/files/NxtWhitepaper.pdf (accessed on 21 July 2021).
42. Jelurida. What is Ardor? | Jelurida. 2021. Available online: https://www.jelurida.com/ardor/what-is-ardor (accessed on 19 July 2021).
43. Jelurida. Jelurida Whitepaper. 2017. Available online: https://www.reddit.com/r/NXT/comments/75vufs/jelurida_white_paper/ (accessed on 21 July 2021).
44. Quadrans Foundation. 2021. Available online: https://quadrans.io/ (accessed on 20 July 2021).
45. Quadrans Foundation. Quadrans Foundation—Tools. 2021. Available online: https://quadrans.io/tools.php (accessed on 20 July 2021).
46. Quadrans Foundation. Quadrans Foundation—Notarisation Tool. 2021. Available online: https://notarize.quadrans.io/ (accessed on 20 July 2021).
47. Costa, D.; Fiori, F.; Milan, P.; Sala, M.; Vitale, A.; Vitale, M. *QUADRANS WHITEPAPER. REV.01*; Quadrans Foundation: Mendrisio, Switzerland, 2019.
48. Dedit.io. Dedit. 2021. Available online: https://dedit.io/ (accessed on 20 July 2021).
49. Dedit.io. Dedit. 2021. Available online: https://app.dedit.io/faq (accessed on 20 July 2021).
50. Algorand. The Blockchain for FutureFi | Algorand. 2021. Available online: https://www.algorand.com/ (accessed on 20 July 2021).
51. Algorand. White Papers | Algorand. 2021. Available online: https://www.algorand.com/technology/white-papers (accessed on 20 July 2021).
52. Chen, J.; Micali, S. ALGORAND: The Efficient and Democratic Ledger. *arXiv* **2016**, arXiv:1607.01341.
53. PlagioScanner. Antiplagio by Plagio Scanner: La qualità per tutti. 2021. Available online: https://www.plagioscanner.com/ (accessed on 21 July 2021).
54. ZeroPlagio. Zero Plagio/Software Antiplagio Online (Sicuro & Anonimo). 2021. Available online: https://www.zeroplagio.com/ (accessed on 21 July 2021).
55. Grammarly Inc. Grammarly: Free Online Writing Assistant. 2021. Available online: https://www.grammarly.com/ (accessed on 22 July 2021).
56. Grammarly Inc. Plagiarism Checker | Grammarly. 2021. Available online: https://www.grammarly.com/plagiarism-checker (accessed on 22 July 2021).

57. Dupli Checker. Plagiarism Checker | 100% Free and Accurate—Duplichecker.com. 2021. Available online: https://www.duplichecker.com/ (accessed on 22 July 2021).
58. Plagiarism Checker. No 1 Free Plagiarism Detector. 2021. Available online: https://www.plagiarismchecker.co (accessed on 22 July 2021).
59. Regner, F.; Schweizer, A.; Urbach, N. NFTs in Practice—Non-Fungible Tokens as Core Component of a Blockchain-based Event Ticketing Applicatio. In Proceedings of the Fortieth International Conference on Information Systems, Munich, Germany, 15–18 December 2019.
60. Unicheck. Plagiarism Checker for Educators and Students | Unicheck. 2020. Available online: https://unicheck.com/ (accessed on 15 December 2021).
61. OXSICO. Oxsico Similarity Checker for Universities and Schools Plagiarism. 2021. Available online: https://www.oxsico.com/ (accessed on 15 December 2021).
62. ethereum.org. Standard Token Non Fungibile ERC-721. 2021. Available online: https://ethereum.org/en/developers/docs/standards/tokens/erc-721/ (accessed on 14 October 2021).
63. Zikratov, I.; Kuzmin, A.; Akimenko, V.; Niculichev, V.; Yalansky, L. Ensuring data integrity using blockchain technology. In Proceedings of the 2017 20th Conference of Open Innovations Association (FRUCT), St. Petersburg, Russia, 3–8 April 2017; pp. 534–539. [CrossRef]
64. Xu, Y.; Zhang, C.; Wang, G.; Qin, Z.; Zeng, Q. A Blockchain-Enabled Deduplicatable Data Auditing Mechanism for Network Storage Services. *IEEE Trans. Emerg. Top. Comput.* **2020**, *9*, 1421–1432. [CrossRef]
65. Internxt. Be Limitless. 2021. Available online: https://internxt.com/ (accessed on 15 December 2021).
66. Sia. 2021. Available online: https://sia.tech/ (accessed on 15 December 2021).
67. Partz, H. Bitcoin Transactions Fees in US Dollars Near All-Time High Levels. Cointelegraph.com. 2021. Available online: https://cointelegraph.com/news/bitcoin-transactions-fees-in-us-dollars-near-all-time-high-levels (accessed on 30 September 2021).