applied sciences

Article

Application of Blockchain in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information

Christian Delgado-von-Eitzen *, Luis Anido-Rifón and Manuel J. Fernández-Iglesias

atlanTTic, Universidade de Vigo, 36310 Vigo, Spain; lanido@det.uvigo.es (L.A.-R.); manolo@uvigo.es (M.J.F.-I.)
* Correspondence: christiandve@uvigo.es

Abstract: Blockchain technologies are awakening in recent years the interest of different actors in various sectors and, among them, the education field, which is studying the application of these technologies to improve information traceability, accountability, and integrity, while guaranteeing its privacy, transparency, robustness, trustworthiness, and authenticity. Different interesting proposals and projects were launched and are currently being developed. Nevertheless, there are still issues not adequately addressed, such as scalability, privacy, and compliance with international regulations such as the General Data Protection Regulation in Europe. This paper analyzes the application of blockchain technologies and related challenges to issue and verify educational data and proposes an innovative solution to tackle them. The proposed model supports the issuance, storage, and verification of different types of academic information, both formal and informal, and complies with applicable regulations, protecting the privacy of users' personal data. This proposal also addresses the scalability challenges and paves the way for a global academic certification system.

Keywords: blockchain; education; GDPR; scalability; lifelong learning; formal learning; informal learning

check for updates

Citation: Delgado-von-Eitzen, C.; Anido-Rifón, L.; Fernández-Iglesias, M.J. Application of Blockchain in Education: GDPR-Compliant and Scalable Certification and Verification of Academic Information. *Appl. Sci.* **2021**, *11*, 4537. https://doi.org/10.3390/app11104537

Academic Editors: Roberto Tonelli, Marco Ortu and Andrea Pinna

Received: 12 April 2021
Accepted: 14 May 2021
Published: 16 May 2021

1. Introduction

The process of issuing and registering academic data is presently a process carried out within each educational institution's proprietary systems and largely isolated from other organizations' record-keeping procedures. This situation impacts directly the verification of students' educational data since, in many cases, the authentication of a transcript or certificate can only be performed manually, which is very costly in resources and time.

With the growing need to demonstrate acquired abilities and skills in an increasingly competitive world, this situation favors the appearance of fake academic certificates, that come from five different sources: (1) "degree mills" that generate fake qualifications that are sold to customers that pay for them [1]; (2) fabricated documents that are generated by inexistent academic institutions [2]; (3) modified documents that alter authentic documents with false dates, courses, specializations, etc.; (4) "in-house"-produced certificates, which are fake academic records created by a real institution and printed and sealed as if they were authentic but made by dishonest employees; and (5) inaccurate translations of authentic documents that are used to accomplish certain requirements in another country with a different language.

Thus, the increasing number of fake accreditations and bogus academic information in a more and more connected society represents a real threat that must be addressed and solved. However, there are neither universally accepted standards to represent academic information nor centralized record-keeping systems for these types of records. Moreover, if a presently active institution discontinues its educational activities and disappears, all its educational data will probably vanish and the traceability between alumni and their original completed studies will be lost, which, in turn, prevents the verification of such studies by a third party. This affects both formal and informal learning, which seems to be increasingly relevant in future professional environments with initiatives such as the one promoted by Google [3], which plans to issue certificates for six-months online courses to students and treat them as the equivalent of a four-year degree if learners pretend to apply for a related job at the company. Amazon (https://aws.amazon.com/certification/?nc1=h_ls accessed on 2 April 2021) and Microsoft (https://docs.microsoft.com/en-us/learn/certifications/ accessed on 2 April 2021) (combining resources from LinkedIn and GitHub) develop similar initiatives.

Furthermore, without a worldwide easily accessible academic information platform, it is not possible to obtain a general perspective of what type of studies, formal or even informal, are the most demanded, or compare how students from different countries acquire their qualifications.

A trustful blockchain-based system can be a solution for these issues since it can tamperproof register academic information to be easily verified by third parties. However, it must be scalable and efficient to record all the related educational data, as well as protect the privacy of every piece of personal information, complying with applicable regulations.

Insofar international regulations are concerned, the General Data Protection Regulation (GDPR [4]) is one of the most relevant and restrictive regulations insofar privacy is concerned for companies and institutions in Europe and in other countries since it provides an overarching coverage of all relevant issues in data protection and was conceived as a robust legal body able to cope with present-day and future challenges. It comprehensibly addresses personal rights in different scenarios, including rights of access to collected data, erasure, restriction of processing, to be notified on any personal data operation, portability of data, objection, or even rights related to automatic decision making and profiling and its limitations. It is important to remark that the regulation is applied to personal information such as name, age, etc. as well as to other data that, in combination with other means, can be used to identify a natural person. Infringements of the GDPR can lead to significant administrative fines.

This research proposes a novel and innovative solution to issue, store, recover, share, and verify heterogeneous and unrestricted types of academic information using blockchain, a technology whose characteristics of resistance to unauthorized modifications and traceability of the operations carried out make it perfect to achieve the pursued objectives. Without changing proprietary information systems, the educational actors can generate and tamperproof register any type of educational data, both formal or informal, and send it to the holder automatically and securely whenever it is requested so the owner can transfer it to a third party who can seamlessly check for its authenticity. In this design, the holder of the academic data has the possibility to share all or only some parts of the issued information with the third party according to their interests. The system also contemplates that if for any reason, the academic institution disappears, under certain conditions, the issued academic accreditations could still be verified and even recovered by the holder.

It is also important to remark that, as it will be later discussed, the existing blockchain-based initiatives to generate and validate academic data utilize diverse approaches to record the information, but they do not take into consideration the strict restrictions imposed by the General Data Protection Regulations (GDPR) in their design, they do not conveniently address the problem of scalability when an increasing number of documents is generated, or both. The proposed solution in this research, which complies with the restrictions imposed by the GDPR, addresses these requirements in an integral way by proposing a solution to face scalability problems when the volume of information is very high, especially strengthening the protection of personal data.

To sum up, the main contributions of this research are as follows:

- It analyzes the application of blockchain technologies to issue and verify educational data;
- It proposes an innovative model that supports the issuance, storage, and verification of different types of academic information under different scenarios that comply with the GDPR and tackles the scalability challenge present in almost every present blockchain initiative;

- It performs a security analysis of the described model;
- It proposes an implementation of the model as a constructive proof of concept with the objective of confirming the feasibility of the designed framework using available state-of-the-art technologies.

The rest of the paper is organized as follows: the main features of blockchain technology and its application in the educational sector and a comparison of related work to the proposed design in this research are introduced and described in Section 2. Then, Section 3 is devoted to introduce some features of the General Data Protection Regulation (GDPR) and to detail the conceptual design of the proposed solution. Section 4 proposes a proof-of-concept implementation with existing technology. Section 5 discusses the results of the proposed model. Finally, conclusions are drawn and future research perspectives are analyzed in Section 6.

2. Preliminaries

Blockchain is an emerging technology introduced in 2008–2009 as the supporting ledger for the Bitcoin cryptocurrency [5], a peer-to-peer electronic cash system aimed to set financial transactions without going through a financial institution or a third party. However, this technology is also used in other platforms such as Ethereum or Hyperledger and applied in more and more sectors with increasing relevance, for the Bitcoin economy and education, as is discussed in this paper, as well as in sectors such as energy [6], agriculture [7], health [8,9], transports or logistics [10], IoT [11,12], in which applications [13], use cases [14] and open issues [15] are identified. In a nutshell, a blockchain consists of a time-ordered set of blocks in which each block is cryptographically linked to the previous one, constructing a chain. As a consequence, a blockchain is almost impossible to alter once created. All the information recorded is tamperproof and distributed across a shared peer-to-peer network.

Each one of these blocks contains transactions of different types (depending on the blockchain) that are created and distributed by the peers of the network. To register new information in the chain, a consensus about its truthfulness has to be reached among the participating peers without the need for a third party. The most extended consensus mechanisms are proof of work (PoW), proof of stake (PoS), and proof of authority (PoA). With the PoW mechanism [5], transactions are validated by solving cryptographic puzzles using brute force, which requires a lot of energy and time for its execution. The active member of the network (called miner) who first solves the puzzle is rewarded.

On the other hand, in systems using PoS [16], the selection of the active member of the network who validates and decides how will the next block be added is performed randomly among all peers, with a probability of being selected proportional to the stake that each member owns in the current blockchain. Therefore, the process of validating and adding new blocks is not as complex as in the PoW consensus mechanism and it is more energy and time efficient.

Finally, some systems utilize a PoA [17] consensus mechanism. With this approach, a small number of active network members are authorized to verify a new block, synchronizing blocks of the chain with the rest of the network peers. A difference with PoW or PoS is that these participants will not always be participating in this process since they will be randomly selected depending on their activity.

Since every piece of information in the blockchain has to be verified before it is included in a block by one or more active members of the network, depending on the consensus mechanism, the amount of data that can be registered is limited, typically some kilobytes. If a larger amount of information needs to be stored, projects such as the InterPlanetary File System (IPFS) [18] can be utilized. IPFS is a hypermedia protocol and a distributed peer-to-peer resilient file system to tamperproof store and share information that can handle bigger file sizes. When a data file is uploaded, a hash digest value of the content is calculated, and this result is used to find the file and recover the data upon request.

Additionally, some blockchains support running smart contracts proposed by Nick Szabo [19]. These are computer programs (Turing-complete in the case of Ethereum [20]) recorded on a block that are executed autonomously by all the active participants in the network. These smart contracts can read, write, modify, and process data according to their programming. Every action is tamperproof registered in the ledger to add confidence.

With respect to the nature of the peers participating in a blockchain, there are three main blockchain types. Public blockchains present no restrictions for joining or leaving, or for accessing the information recorded. In general, all information is public, but in some specific blockchains, some information may be encrypted. On the other hand, in private blockchains, participants may join only if they are invited; hence, they are closed systems operated within institutions. All the information remains private among the authorized members. Finally, consortium blockchains are a combination of the two previous types and are operated by a group of institutions that have a common goal. In this case, authorized partners can join or leave the blockchain upon invitation.

The educational sector addresses blockchain technology and how it could be applied to efficiently protect academic information with relevant initiatives and projects since 2013 [21]. Although there is a growing number of blockchain-based educational applications, most of them are in an early stage of practical development and only a few of them can be actually used by academic institutions and their stakeholders [22].

After a thorough analysis of the scientific literature reporting on blockchain applications in education [22–27], the most frequent category of blockchain use cases in this field is the issuance and verification of academic certificates, although there are many other applications [28,29]. Among the most illustrative examples of the introduction of blockchain for certificate management, the University of Nicosia was the first higher education institution to use Bitcoin to register such certificates [21]. As an additional example, the MIT Media Lab designed, prototyped, and developed an open source platform called Blockcerts on the top of the Bitcoin and the Ethereum blockchains, to issue academic diplomas and let them be verified easily by third parties [21]. Both projects basically register the hash digest of academic certificates (not the full data) in the corresponding blockchain to safeguard the information.

Since these projects do not record the complete information on the chain, if the educational organization disappears and the learner loses their certificate, it cannot be recovered. To solve this, initiatives such as [30] save the whole information of the academic credential on the private Hyperledger Fabric blockchain what, as it will be later discussed, is not always a valid solution from the GDPR's point of view.

Other relevant initiatives such as EduCTX [31] are focused on different aspects of the educational process since they propose issuing tokens as credits for learning units similar to the European Credit Transfer System (ECTS), which academic institutions transfer to the students for the courses that they complete.

From Tables 1 and 2, where different related proposals are described and compared with the proposed design in this work, it can be concluded that almost all the initiatives analyzed, except [32] and this proposal, utilize one single blockchain. This simplifies design and implementation but limits performance and compromises scalability. Wahab et al. [33] suggest the use of Tangle, a special rapid blockchain. However, at this time, it does not fully support smart contracts.

Compliance with the GDPR and its requirements (e.g., data portability, accountability of accesses and operations, data modification support, right to be forgotten, etc.) is not fully addressed by any of the initiatives investigated, except for the design presented in this research. Only Daraghmi et al. [17] and Lam and Dongol [34] take partially into account some related aspects, but none addresses them specifically.

Academic information is stored in a combination of off-chain and blockchain systems in 20 out of the 32 initiatives collected, according to different approaches. This storage strategy is also utilized in this proposal. The rest of the works store data directly on-chain in various types of blockchain. Only in a few cases [1,17,35–37], data are encrypted to protect them. The solution proposed in this paper also implements encryption for data protection.

The proposal discussed in this paper also includes provisions for data regeneration to prevent information loss [31,34,35,38–44]. Moreover, all initiatives analyzed support educational information to be directly verified except for Nicosia's development [21], which relies on a Portable Document Format (PDF) file to list the hash digests of issued certificates. This contribution also supports a rich variety of academic data types [32,34–36,43–50], including flexible record formats [34,46,47].

Another relevant feature provided by this conceptual framework is the possibility of sharing only specific parts of the educational information of a given holder [32,45].

To facilitate access and verification of academic information, our solution supports the generation of QR codes or websites [17,30,41,48,51].

Only two initiatives [38,52] in addition to this proposal support learning analytics or statistics from the registered information. This feature may provide in the future still unknown information on worldwide educational trends, the most demanded studies, the profile of alumni from the characteristics of diplomas issued, etc.

Finally, some initiatives were identified that provide persistent storage even if the issuing academic institution disappears [31,35,38,39,43–45]. To address this situation, several approaches are utilized and, in the case of the contribution discussed in this paper, it is addressed in a way that is compatible with the GDPR.

After a thorough analysis of the scientific literature about blockchain applications in the field of education including relevant surveys [22–27], relevant challenges were identified. They are enumerated below, together with the approaches followed in this research to address them.

1. Education is a discipline with a global dimension that encompasses many stakeholders who must exchange information despite the fact that their organizations are independent. Blockchain brings many applications to this field that require a new interconnection model [49] that is difficult to integrate into the proprietary systems of each entity. The system proposed in this research is adaptable and does not require different organizations to modify their information systems.
2. Achieving privacy in blockchain applications is a real challenge when personal information, protected by many regulations in different countries, is processed. Public blockchains should not be chosen to tamperproof store personal information, even encrypted [35], and consequently, private or consortium blockchains should be preferred [1]. However, from a privacy and regulatory point of view, in some countries (e.g., European Union countries under the scope of the GDPR), it may not be a valid solution [4]. Conscious of this issue, some proposals [1,17,38,46] store information offline but register the corresponding hash digests on the blockchain to ensure the integrity and traceability of information. Nonetheless, in some countries with more permissive regulations (e.g., Brazil [39]) personal information can be openly stored if related to public education. On the contrary, as pointed out above, the European GDPR forbids registering any personal data in unmodifiable permanent storage such as a blockchain [53], which must be anonymized. This is a relevant design constraint, and it is important to emphasize that hashing personal data, from the GDPR's point of view, cannot be considered a completely valid anonymization technique [4]. Finally, the immutability feature of blockchain also makes it impossible to modify or delete data, even for legitimate reasons, which, in turn, collides with GDPR's right to be forgotten. The model proposed in this research solves this challenge with a design that preserves the privacy of users and complies with the GDPR.
3. Storage, scalability, and performance of blockchain-based systems to issue, store, and verify academic information are also key challenges to be addressed in order to achieve its general adoption when the number of transactions containing academic information increases. Present-day blockchain frameworks (Bitcoin, Ethereum, . . .) have a very limited storage capacity, compared to other systems [35]. For example,

the Bitcoin core protocol limits blocks to 1 MB in size [57], although there are specialized blockchain-based decentralized storage networks to store higher amounts of data (IPFS, Storj, Sia, Filecoin, Swarm, etc.) [58]. The current blockchain-based proposals present some issues related to their scalability, that is, the ability to handle large volumes of transactions at high speeds. In general, state-of-the-art blockchain implementations exhibit relatively low transaction efficiency and high confirmation delays. As an example, seven transactions per second (tps) are achieved in Bitcoin and 15 tps in Ethereum. In the case of Hyperledger, hundreds or even thousands of tps can be obtained depending on the actual configuration utilized. In contrast, centralized systems such as VISA can process a maximum of 24,000 tps [33,59].

Nowadays, millions of academic certificates are issued annually around the world. As an example, according to the European Tertiary Education Register (ETER) [60], there are 2465 higher education institutions hosting more than 17 million students at Bachelor, Master, and PhD levels and 225 million students around the world in 2018 [61]. To address the challenges of increased storage requirements, scalability and performance, the proposed model combines on-chain and off-chain storage and distributes the blockchain system into interconnected blockchains, respectively. Note that the aforementioned situation, with many independent educational document issuers, facilitates a distributed approach.

Section 5 below discussed the model proposed in Section 3 to solve these issues, together with related specific proposals with similar objectives summarized in Section 2.

Table 1. Comparison of other related initiatives to the proposed model related to scalability and GDPR.

Initiative	Scalability Number of Blockchains	Right to Erasure	Data Modification	Grant/Remove Permissions	Data Portability	Data Access Accountability
Arenas and Fernández [40]	1 bc Multichain	-	-	-	-	✗
Arndt and Guercio [53]	1 bc	-	-	✗	✗	✗
Badyal and Chowdhary [30]	1 bc	-	-	✗	✗	✗
Bandar et al. [52]	1 bc	-	-	-	-	-
Blockcerts [47]	1 blockchain Bitcoin/Eth	-	✗	✗	-	✗
Bore, et al. [36]	1 bc HL Fabric	-	-	-	-	-
Cheng et al. [41]	1 blockchain Ethereum	-	-	-	-	-
Cheng, et al. [48]	1 bc (HLF)	-	-	-	-	-
Daraghmi et al. [17]	1 bc Eth	-	-	✓	-	✓
Ghazali and Saleh [54]	1 bc	-	-	-	-	✗
Gresch et al. [55]	1 bc Eth	-	-	-	-	-
Han et al. [42]	1 bc Eth	-	-	-	-	-
Jeong and Choi [51]	1 bc Bitcoin/Eth	-	-	-	-	-
KARATAŞ [43]	1 bc Eth	✗	✗	✗	✗	✗
Kuvshinov, et al. [32]	Several private bcs and 1 public	-	-	-	-	✗
Lam and Dongol [34]	1 bc HL	-	✓	-	-	✗
Li and Han [35]	1 bc Eth	-	-	-	-	✗
Li et al. [45]	1 bc	-	-	-	-	✗
Lizcano et al. [38]	1 bc Eth	-	-	-	-	✗
Nicosia [21]	1 bc Bitcoin	-	-	-	-	-
Ocheja et al. [46]	1 bc Eth	-	-	-	-	✗
Palma et al. [39]	1 bc Eth	✗	-	-	-	✗
Prinz et al. [56]	1 bc Eth	-	-	-	-	✗
Rooksby and Dimitrov [49]	1 bc Eth	-	-	-	-	-
Saleh et al. [1]	1 bc HL	-	-	-	-	-
Srivastava et al. [44]	1 bc ARK	-	-	-	-	-
Sun et al. [50]	1 bc	-	-	-	-	-
Turkanović et al. [31]	1 bc ARK	-	-	-	-	✗
Wahab et al. [33]	1 bc Tangle	-	-	-	-	✗
Xu et al. [37]	1 bc	-	-	-	-	✗
This design	1 consortium and n private bcs	✓	✓	✓	✓	✓

Table 2. Comparison of other related initiatives to the proposed model related to scalability and GDPR.

Initiative	Storage	Regenerate Data	Verification	Share Data Partially	Different Data Types	Data Encrypted	Flexible Format	QR/Web to Verify Data	Support for Learning Analytics	Data Available after Closure
Arenas and Fernández [40]	Off. + hash	✓	✓	✗	✗	-	-	✗	✗	✗
Arndt and Guercio [53]	Off./Bc	✗	✓	✗	-	-	-	✗	-	✗
Badyal and Chowdhary [30]	Bc	✗	✓	✗	-	✗	-	✓	-	✗
Bandar et al. [52]	Off. + hash + digital id	-	✓	✗	✗	-	-	-	✓	✗
Blockcerts [47]	Off.	✗	✓	✗	✓	-	✓	✗	✗	✗
Bore, et al. [36]	Off. + hash + pointer	-	✓	✗	✓	✓	-	-	-	✗
Cheng et al. [41]	Off. + hash + cert. id	✓	✓	✗	-	-	-	✓	-	✗
Cheng, et al. [48]	Off.	✗	✓	✗	✓	-	-	✓	-	✗
Daraghmi et al. [17]	Off./hash	-	✓	✗	-	✓	-	✓	-	✗
Ghazali and Saleh [54]	Off./hash	-	✓	✗	-	-	-	✗	-	✗
Gresch et al. [55]	File + hash	✗	✓	✗	✗	✗	✗	✗	✗	✗
Han et al. [42]	Off. + pointer to data +hash	✓	✓	✗	-	-	-	-	-	✗
Jeong and Choi [51]	Off.	✗	✓	✗	✗	-	-	✓	✗	✗
KARATAŞ [43]	Eth	✓	✓	✗	✓	✗	✗	✗	-	✓
Kuvshinov, et al. [32]	On. in a private bc + hash	✗	✓	✓	✓	✗	-	✗	-	✗
Lam and Dongol [34]	HL + Access control	✓	✓	-	✓	✗	✓	✗	-	✗
Li and Han [35]	Off.	✓	✓	✗	✓	✓	-	-	-	✓
Li et al. [45]	Off. + OBE codes	✗	✓	✓	✓	✗	✗	✗	✗	✓
Lizcano et al. [38]	Off. + some data on	✓	✓	✗	✗	-	✗	✗	✓	✓
Nicosia [21]	Off. + hash	✗	✗	✗	✗	✗	✗	✗	✗	✗
Ocheja et al. [46]	Off. + hash +pointer	-	✓	✗	✓	-	✓	-	-	✗
Palma et al. [39]	Bc	✓	✓	✗	✗	✗	✗	-	✗	✓
Prinz et al. [56]	Off.	-	✓	✗	-	-	-	-	-	✗
Rooksby and Dimitrov [49]	Bc	-	✓	-	✓	-	-	✗	✗	✗
Saleh et al. [1]	Off.+hash	-	✓	-	-	✓	-	-	-	✗
Srivastava et al. [44]	On. (token)	✓	✓	✗	✓	-	-	-	-	✓
Sun et al. [50]	Bc + hash	-	✓	-	✓	-	-	-	-	-
Turkanović et al. [31]	On. (token)	✓	✓	✗	✗	✗	✗	✗	-	✓
Wahab et al. [33]	Off. + hash	✗	✓	✗	✗	-	-	-	-	-
Xu et al. [37]	On.	-	✓	✗	-	✓	-	-	-	✗
This design	Off. + hash + pointer to data	✓	✓	✓	✓	✓	✓	✓	✓	✓

Legend: BC = Blockchain; Eth = Ethereum; HLF = Hyperledger Fabric; Off = Off-chain; On = On-chain.

3. Proposed Model

The study of the state of the art of blockchain in education, the requirements of the academic organizations in the framework of the GDPR, and previous initiatives, their limitations, and drawbacks, discussed in the previous section, shed some light on the desired properties of novel solutions addressing the challenges identified.

Motivated by the findings obtained in the process described above, a novel conceptual design of a system is proposed to issue, store, and verify different types of academic information, both for formal and informal learning, that can be applied to different usage scenarios. We can find in the literature [22–27], several relevant use cases in the following:

- Certificate issuance and management of academic information. This application is further discussed below to illustrate the solution proposed. For this use case, an academic institution issues a certificate, transcript, or diploma and records information on the blockchain so it can be verified for authenticity or recovered, even by authorized third parties;
- Registration of learning paths. In this use case, student's achievements are registered by the educational institutions on the blockchain for both formal and informal studies so they can also be verified. Academic data managed in this case extend the certificates and diplomas mentioned in the previous point.
- Tracking of competence values. Diplomas and certificates are not the only alternatives to provide evidence about the competences acquired by a student since their grades can be converted into competence values that can be issued by the academic institution to be verified by authorized third parties.
- Recording of academic credits. Another application of this solution is to record learners' credits achieved for successfully completed courses. This type of academic information would be generated by the educational organization according to the proposed model.
- An indirect use case of the proposed model in this section, as it will be discussed later, corresponds to the enrichment of the academic information managed in the previous use cases with additional public nonsensitive personal data, such as the type of academic information, degree, or category of a certificate. This could be used to anonymously generate statistics, learning analytics data, or trends relevant to the education domain.

It is important to remark that the proposed model also protects and keeps data private, complying with the GDPR even in the case that the educational institution disappears. The proposal is scalable and efficiently implementable using currently available technologies, which, in turn, guarantees its potential application and sustainability. According to these characteristics, the solution discussed below is intended to serve as a conceptual framework for the development of final systems addressing the issues identified.

To protect personal academic information in this proposal, the provisions in Art. 6 Section 1 of the GDPR and related articles are considered whenever there are no other applicable regulations or laws. Therefore, the designed solution should allow data subjects to control the access to their information, share only a part of it according to their interests, be notified when data are processed, and reclaim and carry away their personal records (Article 20 of the GDPR). It should also support allowing and removing permissions to a specific party (Art. 7 Section 3 of the GDPR). The right to erasure (i.e., the "right to be forgotten" in Article 17 of the GDPR) will also be technically considered in the proposed system.

In general, the designed solution that will be described in the following sections complies with the Privacy by Design principle (Art. 25 of the GDPR) and would allow educational institutions to tamperproof store heterogeneous types of academic information that can be verified by third parties if holders grant them the necessary authorization.

To tackle the issue of scalability and performance, the proposed design will be modeled as a main consortium and an indeterminate number of private blockchains connected to the core blockchain. Each blockchain, both the main one and the private ones, will be formed by recognized and properly authorized educational entities or subjects. The difference between them is that members of the main blockchain will be organizations related to the education domain on a national and international scale, while members of the different private blockchains will be regional or local academic institutions., although national or international organizations can also be part of the private blockchain with a different role.

Each one of these private networks will be independent of the others and they will be self-organized according to geographic, economic, or other criteria. All of them will periodically send specific transactions to the main blockchain. With this approach, the most intense process of issuing all the academic information is accomplished by distributing it into different private blockchains following the latest scalability models in blockchain-related initiatives (cf. Polkadot [62], Ethereum 2.0 [63], or Hyperledger Fabric [64]).

Presently, each academic entity uses its own information system to manage its educational data, and it would be idealistic to assume that this would change. Consequently, and in order to comply with the GDPR as explained above, academic data issued will be stored within the organization's databases and not in the blockchain.

Nevertheless, the model includes a solution for those cases in which the academic institution closes, and the information cannot be recovered from their servers since the data are no longer available. To face this situation, a new private blockchain formed by selected recognized educational organizations connected to a private IPFS is proposed to store orphan records (cf. Section 3.5).

The process of issuing and verifying any academic record in this model by a third party is described in the following paragraphs using the example of an academic certificate, but the approach would be perfectly applicable with any other type of information or a combination of them. However, for efficient use of resources, it is not recommended to keep records with limited long-term relevance (e.g., to record each individual student's exam grade).

Figure 1 depicts an overview of the proposed design, describing its key elements as well as their relationships.

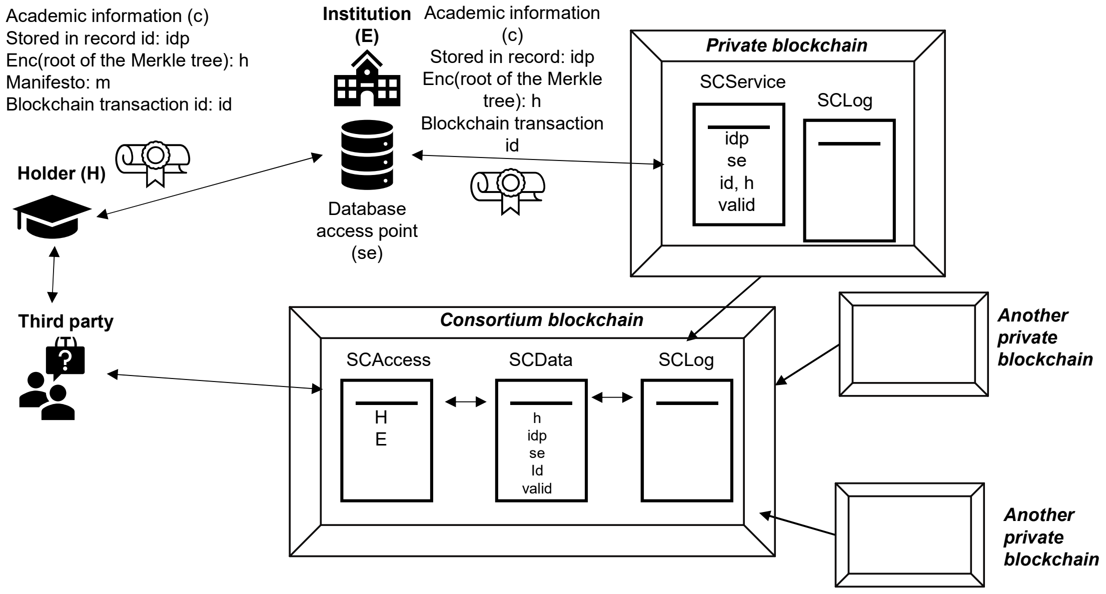

Figure 1. Proposed design (overview).

3.1. Issuance of Academic Information

The process, illustrated in Figure 2, starts when the academic institution (E) issues the diploma containing some sensitive (name, surname, degree, date, etc.) and nonsensitive information (type of academic information, educational institution, course name, number of credits, etc.) to the holder (H) with a certain custom structure in the form of a Merkle tree

(A Merkle tree is a structure of data that allows efficient and secure storage and verification of content with a large amount of information) [21] and generates also the corresponding manifesto. Both organization *E* and holder *H* are represented by their blockchain accounts. It is highly recommended (as described in [5]) for the holder to generate a new account for each academic certificate issued to avoid linkability and to store them all securely in a mobile app or a computer.

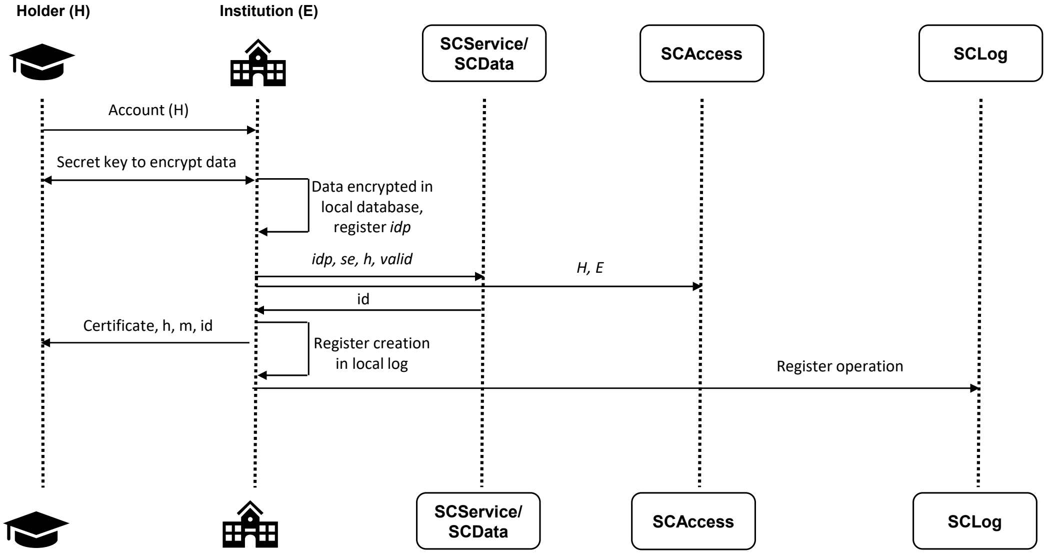

Figure 2. Issuance of academic information.

All the information included in the certificate is recorded by the institution in its private and isolated database in the register *idp* and encrypted with a secret key only known by *E* and *H*.

The academic institution is also connected to a private blockchain and sends a transaction containing: a pointer to its internal database register (*idp*), the location (hostname and port) of the database server access point (*se*), the root of the Merkle Tree (*mt*) of the academic information encrypted with its private key (*h*), that information is valid and a list of accounts that can access this information (*aa*). These data are recorded in a transaction (*id*).

Some nonsensitive information *public data* (*pd*) such as the type of certificate may also be added to the transaction in the blockchain to support global data analytics by the issuer, but it is not mandatory.

The issuer transmits using a secure channel to the holder the complete certificate (*c*), its encrypted Merkle tree (*h*), the manifest (*m*), and the transaction id (*id*). The institution must register every operation in a local log, which must be also hashed and sent to the blockchain to provide accountability of any modifications (smart contract *SCLog*).

The private smart contract *SCService* is the only authorized external access point to the records stored in the local database of the institution, which verifies that the requesting account is allowed to access the data.

Periodically, each private blockchain transmits to the main consortium the registered information, which is divided into the *SCData* smart contract that contains the encrypted root of the Merkle tree -*h*-, *idp*, *se* and information that the data are valid and *SCAccess* with the list of authorized accounts (*aa*).

3.2. *Verification of Academic Information*

In case a third-party *T* (represented by its blockchain account) needs to check the authenticity of a diploma, three different cases are considered.

3.2.1. Case 1: The Holder Sends a Third Party the Certificate and Allows Its Verification

In this scenario, the holder *H* sends to the third-party *T* using a secure channel all the information contained in the certificate (*c*), the blockchain transaction *id,* and grants access to the data by adding *T's* account in the *SCAccess* (*aa*), indicating use case number one. When *T* asks for *id* in *SCData* to obtain the encrypted root of the Merkle tree *h*, it checks *aa* to validate that is authorized and, regardless of the result, logs in *SCLog* that holder's data tried to be accessed by *T*. If access is granted (*T*'s address was included in *aa*), and the requested information is the same indicated by *H* in *aa*, *T* receives the validity of the data and *h*, decrypts *h* with the institution's public key, and compares the result with the root of the Merkle tree (*mt*) of the certificate (*c*) to verify and check if it has not been revoked.

The data exchanged between the holder and a third party, together with the interactions with the different smart contracts in this scenario, are depicted in Figure 3.

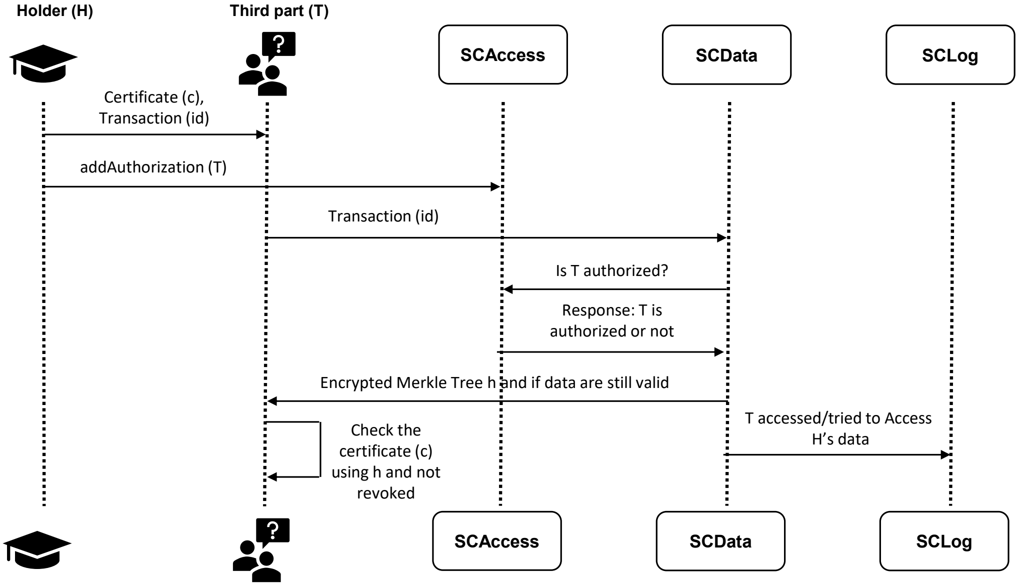
Holder (H)
Third part (T)
SCAccess
SCData
SCLog
Certificate (c), Transaction (id)
addAuthorization (T)
Transaction (id)
Is T authorized?
Response: T is authorized or not
Encrypted Merkle Tree h and if data are still valid
T accessed/tried to Access H's data
Check the certificate (c) using h and not revoked
SCAccess
SCData
SCLog

Figure 3. Overview of the process in case 1.

3.2.2. Case 2: The Holder Only Wants to Share Parts of the Academic Information

This is a different case in which the holder *H* wants to share with a third-party *T* only some academic information from the whole certificate (*c*), unveiling some data to preserve their privacy. To achieve, *H* sends to *T* using a secure channel only some data contained in the certificate (*c*), the calculated Merkle paths of the shared information, the manifest (*m*), the blockchain transaction *id,* and adds *T*'s account in the *SCAccess* (*aa*) to grant access indicating use case number two. When *T* requests the encrypted root of the Merkle tree *h* from *SCData*, it queries *SCAccess* to check that is allowed and logs in *SCLog* that the data of the holder will be accessed by *T* (or not, if access is not granted). *T* recuperates if data are valid and *h*, decrypts *h* with the organization's public key and compares the result with the calculated root of the Merkle tree and paths from the received information to confirm that it is valid and not revoked.

The sequence diagram that represents the flow of information and interactions among actors and related smart contracts is graphically represented in Figure 4.

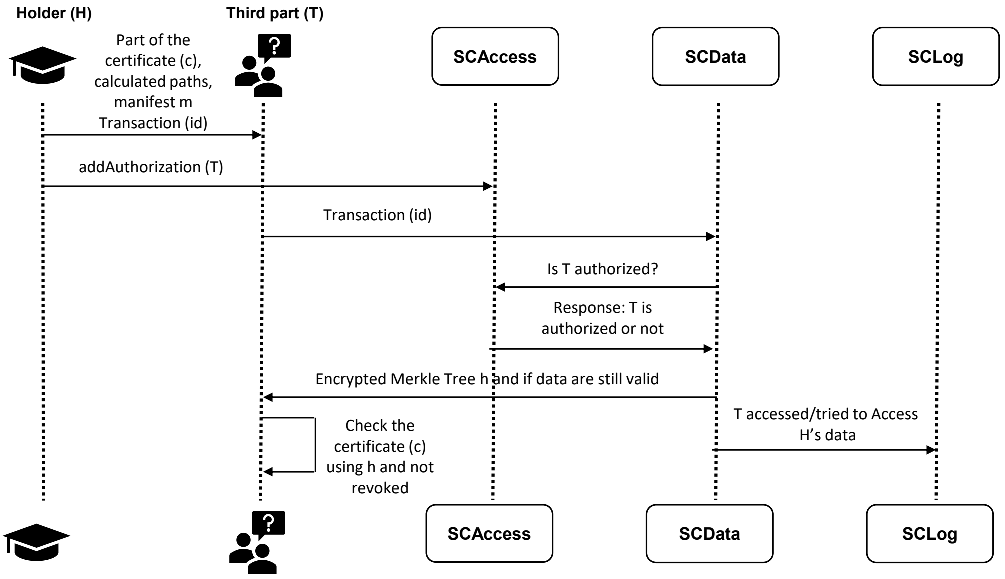
Holder (H)
Third part (T)
SCAccess
SCData
SCLog
Part of the certificate (c), calculated paths, manifest m Transaction (id)
addAuthorization (T)
Transaction (id)
Is T authorized?
Response: T is authorized or not
Encrypted Merkle Tree h and if data are still valid
T accessed/tried to Access H's data
Check the certificate (c) using h and not revoked
SCAccess
SCData
SCLog

Figure 4. Overview of the process in case 2.

3.2.3. Case 3: The Holder Allows a Third Party to Receive the Certificate Directly from the Academic Institution

In this use case, the holder *H* needs a third-party *T* to obtain the whole certificate (*c*) directly from the issuing entity *E* instead of sending it directly (to give more confidence because the holder no longer has the academic information, etc.). To achieve this, the holder *H* transmits to *T* the blockchain transaction *id* and adds *T*'s address in *SCAccess* (*aa*) indicating use case number three. *T* requests the record id of the academic information in the database (*idp*) and the database server access point (*se*) from SCData, which after checking *T*'s permissions in *SCAccess*, sends it to *T*. When *T* obtains these data and asks *SCService* for the certificate (*c*), which, after verifying *T*'s authorization (in *SCAccess*), queries the information in the local database and sends to *T* the data using a secure channel. Both *SCData* and *SCService* log in *SCLog* that *T* has tried to access or actually accessed the record. If necessary, *T* could confirm the authenticity and validity of (*c*) following the first procedure (case 1). The whole sequence diagram for this case is depicted in Figure 5, which depicts the interactions among holder, third party, and institution through the different smart contracts.

If academic records published in the consortium blockchain contain other public nonsensitive personal data, such as the type of academic information, degree, or category of the certificate, this could be used to anonymously generate statistics, learning analytics data, or trends relevant to the education domain.

3.3. Modification of Academic Information

If the institution *E* or the holder *H* would like to modify some concrete academic information due to different reasons (such as a typographical error, incorrect data, etc.), the institution must correct the information in its internal database, generate a new certificate (c'), and send a new h, h' to the blockchain (*SCService*), which will generate a new transaction id'. This information must be sent along with the new certificate (c') to the holder (and, if necessary, a new manifest m') so that any verification of the previous data (case 1 or case 2) will indicate that there is an error since these have been altered. All the necessary data exchanges and operations are illustrated in Figure 6.

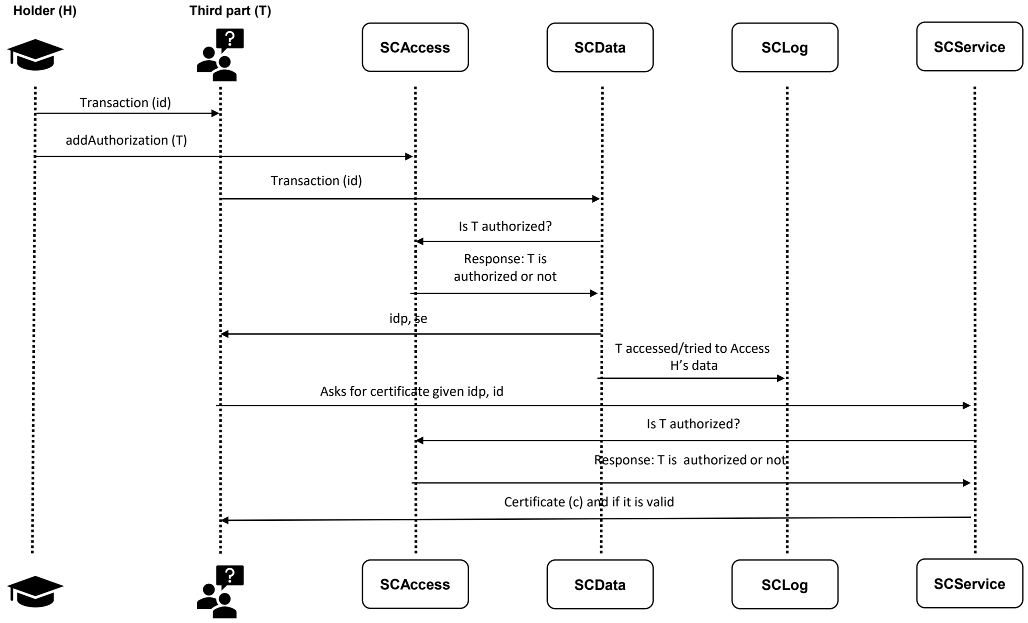

Figure 5. Overview of the process in case 3.

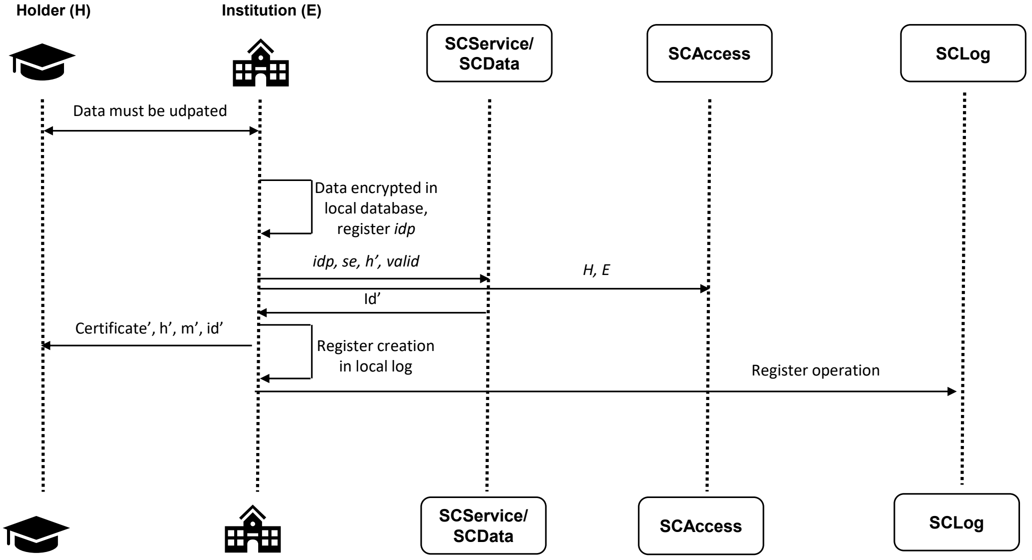

Figure 6. Modification of academic information.

Any modification of the information in the private database must be logged and registered in *SCLog*.

From this point on, the procedure to verify, modify, or delete would be the same as if the academic information were new.

3.4. Revocation/Deletion of Academic Information

If the organization *E* or holder *H* wishes to eliminate the academic information, and it is possible from a legal point of view, the institution must proceed to delete the academic information and modify the blockchain (*SCService* and later *SCData*), setting to cero the information (*idp, se, h*), tagging the data as invalid and eliminating all the accounts in *SCAccess* for that record, as depicted in the sequence diagram presented in Figure 7.

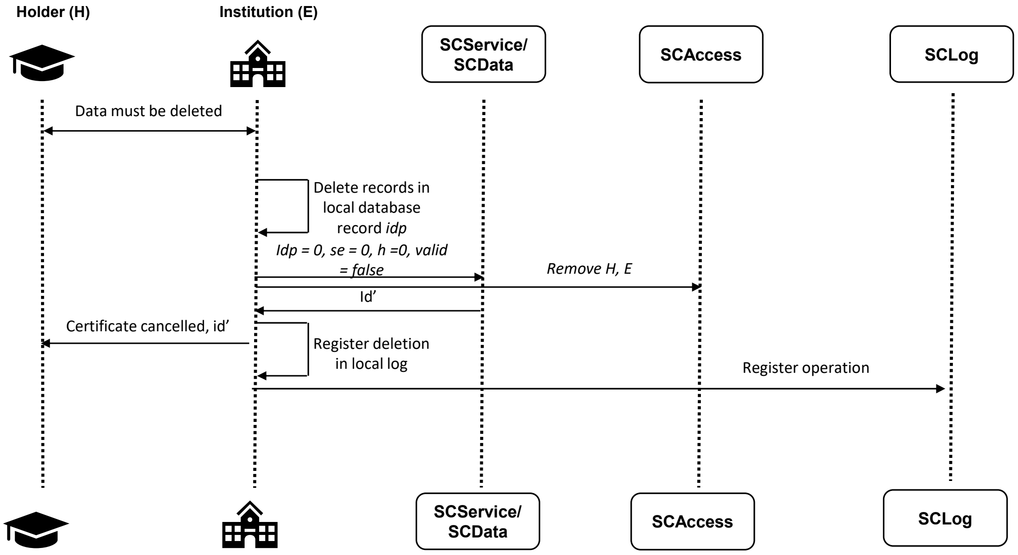
Holder (H)
Institution (E)
SCService/ SCData
SCAccess
SCLog
Data must be deleted
Delete records in local database record idp
Idp = 0, se = 0, h =0, valid = false
Remove H, E
Id'
Certificate cancelled, id'
Register deletion in local log
Register operation

Figure 7. Revocation/deletion of academic information.

Only nonpersonal information would remain in the blockchain in past transactions (*idp*, *se*, *h*, *valid*) and any further verifications of the academic data would return an error.

3.5. How to Verify or Recover Any Academic Information in Cases Where the Issuing Institution Disappears

An unsolved common issue in all the initiatives that do not store the academic information in the blockchain to comply with the GDPR is that if the institution disappears, educational data cannot be recovered.

In the framework proposed, if the holder has the certificate and related information, as described in the design and the system, is still operational except for the academic institution (*E*) being out of business, cases 1 and 2 can be initiated, and the verification of the authenticity of the information can be checked without further difficulties. Nevertheless, if *E* is no longer available (necessary in case 3) and all its servers and databases are not operational, the complete academic information cannot be recovered (case 3).

To cope with this scenario and only in the case that the educational organization *E* is expected to disappear, it should proceed as follows:

- The institution *E*, before discontinuing its educational activities, should publish the affected educational data in their final form as stored in its databases (encrypted with a key shared with each holder as described in this model) in a distributed file system such as a private IPFS connected to a private blockchain that can only be used and accessed by some trustful, prestigious selected organizations. Although these entities have direct access to the records, their contents cannot be read since they are originally encrypted. Associated with each protected academic information in IPFS, a private blockchain will exist in which the pointer to the information in the distributed file system and the same information it was recorded on the private and consortium blockchain will be stored.
- If a holder *H* would like to recover their certificate (case 3), the system should relocate the database access point to a new location, where a smart contract should check if *H* is allowed in *SCAccess* to access the Information. If it has the proper permissions, it should make it encrypted, but since *H* has the secret shared key with the discontinued institution *E*, it could recover the original information.
- Under this scenario, if the holder *H* deletes their secret key, as the encrypted information is only stored on a private distributed storage with limited access, the "right to be forgotten" should be achieved since the GDPR considers deleting the decrypting keys to be a valid option.

The distributed storage system should have sufficient capacity and scalability, although it should not store all the certificates and academic information in the world but only that corresponding to educational institutions that disappeared.

3.6. Compliance with Security Requirements

The proposed model is designed to fulfill the most demanding security requirements: integrity, confidentiality, authentication, access control, availability, nonrepudiation, and ultimately, full compliance with the GDPR.

Data stored in the blockchains cannot be modified once registered due to its immutability. As a consequence, integrity is achieved while at the same time only nonpersonal information is saved on the chain. Academic information is stored off-chain encrypted with a secret key only known by the issuer and the holder. Even if the issuer's or the holder's systems are compromised, private information cannot be recovered unless the decryption keys are also exposed. For the case in which the institution disappears and its information is stored in a restricted access blockchain, being encrypted with a key only known by the holder and the discontinued organization, it can be considered that it remains confidential.

Apart from data security, the designed model achieves privacy preservation by anonymity if the holder uses different accounts to avoid linkability among the diverse issued data on the chain to him/her.

As in any other interconnected system, information exchanges must be carried out using secure connections. The security of the nodes that are part of the blockchain and their interconnection with the access points to educational institutions must be properly secured and every private key should be carefully handled and protected.

With this model, only authorized third parties by the holder can access nonpersonal information to validate or recover the educational information, and every operation is tamperproof logged in the system to provide accountability.

To maintain trust in the system, it is important that only recognized entities and organizations are allowed to be part of the private blockchains and the main one, but that is outside the limits of the designed model since it is a matter of adding or not certain academic organizations. In any case, if any inappropriate behavior is detected, the institution could always be annulled and, with it, the related academic data.

Availability is a key feature of blockchain since, by its own design, it replicates the information; therefore, this security service, as long as any node of the network remains operational, will be fulfilled.

Nonrepudiation can be verified since to carry out any operation, as described in the model, it is necessary by the different actors to use their private keys and the information, and the result will be permanently registered in the blockchain, and hence, it cannot be repudiated.

4. Proof-of-Concept Implementation

An implementation of the model introduced in Section 3 is discussed below. This implementation was devised as a constructive proof of concept with the objective of confirming the feasibility of the proposed conceptual framework. Only available state-of-the-art technologies are involved in this implementation, and no assumptions are made about future technologies or upcoming existing ones.

Blockchain is a relatively recent set of technologies that is in a process of maturing and continuous improvement in general, and, in particular, in the aspect of interconnecting blockchains such as designed in this proposal. Some initiatives related to Ethereum, Polkadot, or Hyperledger, for example, work in this line [62,63]. All potential implementations of the design proposed in Section 3 must consider the security of the chosen blockchain platform (e.g., Bitcoin [65], Ethereum [66], Hyperledger [67], etc.), its protocols and features, especially when exposed in a production environment [68–71] and in the educational field [72].

To demonstrate and exemplify the feasibility of the proposed model with current technology, the system was designed using Hyperledger Fabric as a framework. Hyperledger Fabric [73] is a permission platform for distributed ledger solutions built upon a modular architecture that provides high degrees of confidentiality, flexibility, resiliency, and scalability, besides supporting pluggable implementations of several components such as consensus mechanisms or membership services for identity management.

The reasons to select Hyperledger Fabric for this initial implementation are as follows:

- It is a private, efficient processing blockchain, enabling parallel processing with thousands of transactions per second depending on the topology and configuration [74];
- It provides a membership identity service that manages user ID and authenticates all participants in the network, allowing the creation of access control lists to provide different levels of permission depending on the role;
- It enables the creation of private channels to assure privacy and confidentiality; hence, information cannot be accessed without proper permissions to the network participant;
- It allows the creation of smart contracts called "chaincode" in the Hyperledger Fabric network required by the proposed design;
- It implements a modular architecture with pluggable components for different types of identity, consensus mechanisms, or encryption algorithms.

To model the implementation of this proposal, a five-element system was devised.

4.1. Holder and Third-Party Users

Both the holder and third-party users have an account, which will be stored in the mobile app or web account of the stakeholders and can consume the provided services in the system using the Hyperledger Fabric SDK for Node.js using one or more dedicated servers in the cloud managed by the consortium, who also developed and maintains the mobile app and the web service, as represented graphically in Figure 8.

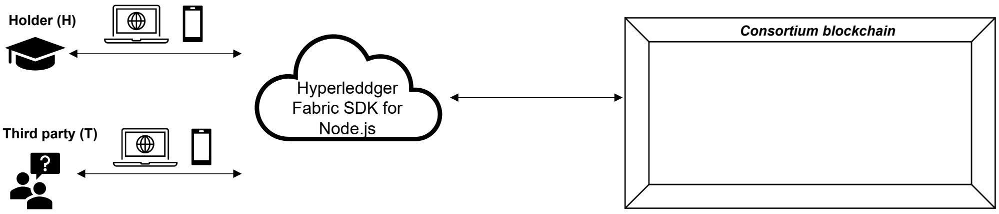

Figure 8. Holder and third-party access to the consortium blockchain.

It is considered that both the holder and any third-party user have an account in the main consortium blockchain, and how they obtain it is out of the scope of this implementation since it is a basic generation of an account in Hyperledger.

4.2. Educational Institution

The institution is connected to one of the private blockchains based on Hyperledger Fabric, as shown in Figure 9, and has at least one account to issue the different academic data with the proper permissions.

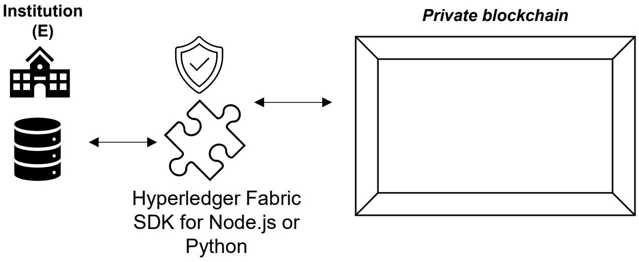

Figure 9. Interaction between the institution and the private blockchain.

The process of retrieving the holder's account, generating a shared key, issuing, encrypting, and storing the information in the database, and securely transferring the academic data issued as described in the model is out of the scope of this concrete implementation since it depends on each particular case and consists of an exchange of data, and this initial proof-of-concept implementation focuses on specific aspects related to blockchain.

Since, as already stated, the institution uses its own proprietary information systems, it is considered that they have an API that can be securely consumed to interact with the associated private chain using the Hyperledger Fabric SDK for Node.js or Python, depending on the technology applied, it is not mandatory for the organization to change their databases to join the initiative, although some adaptations can be required to connect the internal servers to the blockchain using the API, which must be properly protected and hardened using a firewall, an intrusion detection system (IDS) and/or an intrusion detection and prevention system (IDPS).

4.3. Private Blockchains

Each private blockchain is based on Hyperledger Fabric in this initial implementation, although any other blockchain framework that supports the proposed model can be used whenever it can be connected to the main consortium blockchain to transfer the information and has a mechanism to exchange information with the institutions, as previously described.

The different smart contracts described in the proposed model are programmed using chaincode.

The members of the private blockchain and their roles are agreed offline, and the infrastructure is dimensioned with resources enough to be able to process all the generated data by the connected institutions, which are organized into private chains by geographical, economical, or other criteria (for example, the public national universities may be within the same private blockchain, the universities belonging to a federation, etc.). The management of each private chain falls on the set of institutions that are part of it.

4.4. Consortium Blockchain

The consortium blockchain is based on the Hyperledger Fabric framework and its members are recognized academic institutions, each one with at least one account and the permissions properly configured with the associated roles.

In this proof-of-concept implementation, at least one node of the main blockchain is connected to each of the private blockchains and, with the Fabric SDK for Node.js or Python depending on the technology installed in the internal servers which, periodically retrieves the confirmed transactions and operations from the diverse private blockchains to the consortium, where new chaincode is deployed according to the proposed model to fulfill the specifications.

The block diagram of the consortium blockchain and how it interconnects with the other private ones are represented in Figure 10.

4.5. Private Blockchain Connected to IPFS to Store Academic Information from Disappeared Institutions

As proposed in Section 3.5, if an institution disappears, all the academic information could be stored in a private blockchain controlled by the consortium. The practical implementation of this scenario is using another blockchain based on the Hyperledger Fabric framework connected to the main consortium blockchain through the Hyperledger Fabric SDK for Node.JS, as depicted in Figure 11.

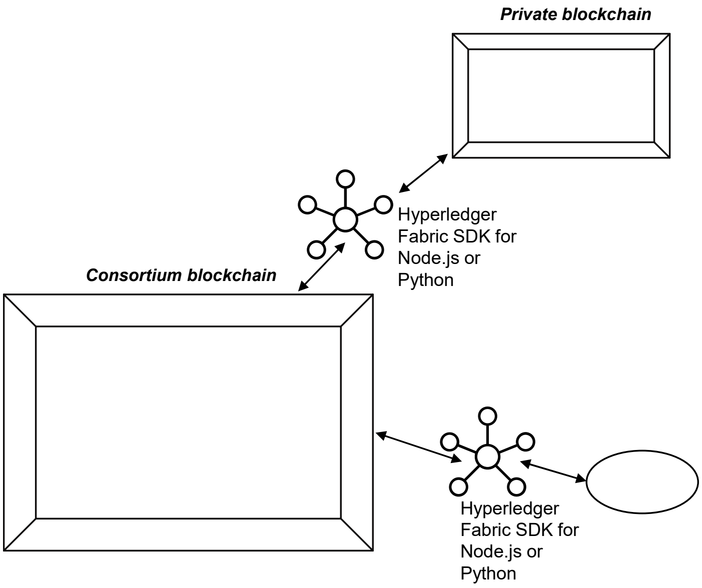
Private blockchain
Hyperledger Fabric SDK for Node.js or Python
Consortium blockchain
Hyperledger Fabric SDK for Node.js or Python

Figure 10. Consortium blockchain and its interconnection with the private ones.

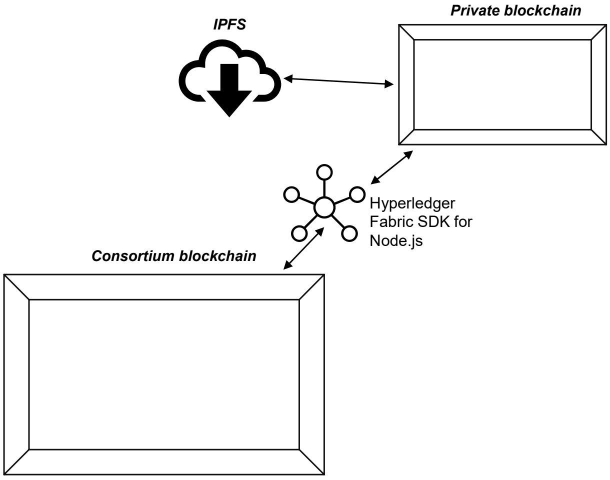

Figure 11. The consortium blockchain and the private one to store academic information using IPFS.

The process of transferring the encrypted academic data from the institution to the IPFS (InterPlanetary File System) distributed storage cannot be generalized since it depends on the specific technology of the issuing organization, but the idea is that uploading and fetching files is performed through InterPlanetary File System. An authorized system operator, in case of closure of the entity, can add the records of the institution to IPFS. A hash is generated for the uploaded information, which is then included in the private blockchain network associated with the issued record; therefore, it can be retrieved if requested by the authorized holder, as explained in the model.

5. Discussion

The proposed framework is designed with the *privacy by design* principle in mind to protect personal data and to comply with the European GDPR, one of the most restrictive regulations insofar privacy is concerned. By using this system, data subject's consent must be explicitly granted and registered as the holder transmits to the institution *E* their blockchain account to be associated with the issued academic information.

After the educational data were issued by the institution, the holder of the data has the possibility to allow and later withdraw access to all or only certain data items to any third party just by adding or removing their account (*T*'s) in a smart contract. Everything is trustfully and tamperproof recorded.

The design allows extending how the information can be accessed. For example, if the holder *H* would like to share their academic records (or parts of them) using a nonpredictable URL in a web page (or using a QR code), and hence, anyone can check for the authenticity of the data without accessing directly to the blockchain, it could be easily performed. In this use case, only a web service (provided by any public or private company free or at cost) is necessary, whose blockchain associated account should be authorized by *H* in *SCAccess*, and therefore, access to the verification could be granted. In this scenario, there would not be an exact record of who accessed that URL since it would be publicly accessible. The only information accounted for would be that the web service requested access to the data.

If the holder *H* or the institution *E* decides to cancel access to a third party by removing its account in *SCAccess*, it will receive a notification and should delete all the related information both online and offline. While institution *E* exists, a holder has the possibility to request all the information about them by just submitting all their associated blockchain accounts (different *H*s of the same holder) to comply with the portability requirement of the GDPR.

The holder can find out who (and when) tried to access or even accessed their data just by querying the logs, as required by the GDPR. The right to be forgotten can be implemented by requesting the institution to erase all the recorded data about the holder. If this is legally feasible, the organization would delete the records from its local databases, tag the data as invalid in the blockchain and eliminate all the accounts in *SCAccess* for that holder so the information cannot be accessed by anyone. Only nonpersonal information would remain in the blockchain since no academic data are ever stored in the blockchain.

In case academic institution *E* disappears, all the associated academic information should be published in a private blockchain connected to an IPFS distributed file system so the holder of the educational data could have them verified and even recover them using the secret key. Under this scenario, if the holder *H* deletes their secret key, as the encrypted information is only stored on a private distributed storage with limited access, the "right to be forgotten" is preserved since the GDPR considers deleting the decrypting keys to be a valid option.

The proposed model utilizes several blockchains to tackle scalability and performance issues since in the educational sector, there are data generation peaks in specific moments of the year (e.g., at the end of the term). With this solution, every private blockchain should be independently dimensioned to safely record all the transactions in a reasonable time and, later, transfer the data to the main consortium blockchain where transactions would be incorporated, but they do not need to be intensely analyzed since they come from a theoretically reliable source (a private blockchain). For this reason, a proof of stake or even a proof of authority can be used as the consensus mechanism by the main blockchain.

The technical implementation of these models faces three main challenges. The first one is the interconnection and authorization of the different blockchains to exchange data in an efficient and secure way. This is an active field of research with initiatives such as Polkadot [62] and Ethereum 2.0 [63] currently under development.

Moreover, the log system must be extremely fast to tamperproof store all the accesses to the information and operations. To achieve this, blockchains such as Hyperledger Fabric or Tangle [75] should be used.

Finally, the private blockchain with access to the IPFS distributed file system should have enough capacity and performance to store all the records of defunct academic institutions.

6. Conclusions and Future Work

None of the initiatives analyzed in which blockchain is presently applied in the world of education complies with the GDPR, registers any type of academic information, or conveniently addresses the scalability problem in case the system is massively adopted and the volume of transactions increases exponentially, which, in turn, limits their global applicability.

These challenges are individually addressed by this innovative contribution. The proposed solution allows, on the one hand, to reliably store and make verified by a third party any type of academic record without compromising the privacy of personal data and complying with the requirements of the GDPR. On the other hand, the system layout, based on a set of blockchains, enhances the performance and scalability of the system.

Future work already under development is focused on (i) technically prototyping an operational scheme based on this model utilizing currently existing technology, (ii) developing a proof-of-concept implementation system, (iii) validating it with real users, and (iv) measuring and evaluating the outcomes (i.e., among others, average response time and throughput of the system even changing the number of academic information to be recorded, distribution of the submitted queries and transactions).

Author Contributions: Conceptualization, C.D.-v.-E., L.A.-R. and M.J.F.-I.; methodology, C.D.-v.-E.; software, C.D.-v.-E.; validation, C.D.-v.-E., L.A.-R. and M.J.F.-I.; formal analysis, C.D.-v.-E., L.A.-R. and M.J.F.-I.; investigation, C.D.-v.-E.; data curation, C.D.-v.-E., L.A.-R. and M.J.F.-I.; writing—original draft preparation, C.D.-v.-E. and M.J.F.-I.; writing—review and editing, C.D.-v.-E., L.A.-R. and M.J.F.-I.; supervision, C.D.-v.-E., L.A.-R. and M.J.F.-I. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

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

References

1. Saleh, O.S.; Ghazali, O.; Rana, M.E. Blockchain based framework for educational certificates verification. *J. Crit. Rev.* **2020**, *7*, 79–84. [CrossRef]
2. Muzammil, M. Corrupt schools, corrupt universities: What can be done? *Comp. A J. Comp. Int. Educ.* **2010**, *40*, 385–387. [CrossRef]
3. Creating Pathways to Careers in IT. Available online: https://services.google.com/fh/files/misc/it_cert_impactreport_booklet_rgb_digital_version.pdf. (accessed on 16 March 2021).
4. Lyons, T.; Courcelas, L.; Timsit, K. *Blockchain and the GDPR*; The European Union Blockchain Observatory and Forum, European Commission: Brussels, Belgium, 2018.
5. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://www.bitcoin.org/bitcoin.pdf. (accessed on 17 January 2021).
6. Andoni, M.; Robu, V.; Flynn, D.; Abram, S.; Geach, D.; Jenkins, D.; McCallum, P.; Peacock, A. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
7. Mirabelli, G.; Solina, V. Blockchain and agricultural supply chains traceability: Research trends and future challenges. *Procedia Manuf.* **2020**, *42*, 414–421. [CrossRef]
8. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Appl. Sci.* **2019**, *9*, 1736. [CrossRef]
9. Jiang, S.; Cao, J.; Wu, H.; Yang, Y.; Ma, M.; He, J. BlocHIE: A BLOCkchain-Based Platform for Healthcare Information Exchange. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP), Taormina, Sicily, Italy, 18–20 June 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2018; pp. 49–56. [CrossRef]
10. Pournader, M.; Shi, Y.; Seuring, S.; Koh, S.L. Blockchain applications in supply chains, transport and logistics: A systematic review of the literature. *Int. J. Prod. Res.* **2019**, *58*, 2063–2081. [CrossRef]
11. Conoscenti, M.; Vetro, A.; de Martin, J.C. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2016; pp. 1–6. [CrossRef]
12. Jiang, S.; Cao, J.; Wu, H.; Yang, Y. Fairness-based Packing of Industrial IoT Data in Permissioned Blockchains. *IEEE Trans. Ind. Inform.* **2020**, 1. [CrossRef]
13. Konstantinidis, I.; Siaminos, G.; Timplalexis, C.; Zervas, P.; Peristeras, V.; Decker, S. *Blockchain for Business Applications: A Systematic Literature Review*; Abramowicz, W., Paschke, A., Eds.; Springer International Publishing: Cham, Switzerland, 2018; Volume 320, pp. 384–399.
14. Butijn, B.-J.; Tamburri, D.A.; Heuvel, W.-J.V.D. Blockchains. *ACM Comput. Surv.* **2020**, *53*, 1–37. [CrossRef]
15. Casino, F.; Dasaklis, T.K.; Patsakis, C.F. A systematic literature review of blockchain-based applications: Current status, classification and open issues. In *Telematics and Informatics*; Elsevier Ltd: Amsterdam, The Netherlands, 2019; Volume 36, pp. 55–81. [CrossRef]

16. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol*; Katz, J., Shacham, H., Eds.; Springer International Publishing: Cham, Switzerland, 2017; Volume 10401, pp. 357–388.
17. Daraghmi, Y.-A.; Yuan, S.-M. UniChain: A Design of Blockchain-Based System for Electronic Academic Records Access and Permissions Management. *Appl. Sci.* **2019**, *9*, 4966. [CrossRef]
18. Marjit, U.; Kumar, P. Towards a Decentralized and Distributed Framework for Open Educational Resources based on IPFS and Blockchain. In Proceedings of the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 13–14 March 2020; pp. 1–6. [CrossRef]
19. Szabo, N. Formalizing and Securing Relationships on Public Networks. *First Monday* **1997**, *2*. [CrossRef]
20. Swan, M. *Blockchain: Blueprint for a New Economy*, 1st ed.; O'Reilly Media, Inc.: Sebastopol, CA, USA, 2015.
21. Grech, A.; Camilleri, A.F. *Blockchain in Education*; Publications Office of the European Union: Luxembourg City, Luxembourg, 2017.
22. AlAmmary, A.; Alhazmi, S.; Almasri, M.; Gillani, S. Blockchain-Based Applications in Education: A Systematic Review. *Appl. Sci.* **2019**, *9*, 2400. [CrossRef]
23. Yumna, H.; Khan, M.M.; Ikram, M.; Ilyas, S. *Use of Blockchain in Education: A Systematic Literature Review*; Nguyen, N.T., Gaol, F.L., Hong, T.-P., Trawiński, B., Eds.; Springer: Cham, Switzerland, 2019; Volume 11432, pp. 191–202.
24. Malibari, N.A. A Survey on Blockchain-based Applications in Education. In Proceedings of the 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 12–14 March 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 266–270. [CrossRef]
25. Bhaskar, P.; Tiwari, C.K.; Joshi, A. Blockchain in education management: Present and future applications. *Interact. Technol. Smart Educ.* **2020**. ahead of print. [CrossRef]
26. Caldarelli, G.; Ellul, J. Trusted Academic Transcripts on the Blockchain: A Systematic Literature Review. *Appl. Sci.* **2021**, *11*, 1842. [CrossRef]
27. Raimundo, R.; Rosário, A. Blockchain System in the Higher Education. *Eur. J. Investig. Heal. Psychol. Educ.* **2021**, *11*, 21. [CrossRef]
28. Fernández-Caramés, T.M.; Fraga-Lamas, P. Towards Next Generation Teaching, Learning, and Context-Aware Applications for Higher Education: A Review on Blockchain, IoT, Fog and Edge Computing Enabled Smart Campuses and Universities. *Appl. Sci.* **2019**, *9*, 4479. [CrossRef]
29. Hameed, B.; Murad, M.; Noman, A.; Javed, M.; Ramzan, M.; Ashfaq, F.; Usman, H.; Yousaf, M. A Review of Blockchain based Educational Projects. *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*. [CrossRef]
30. Badyal, S.; Chowdhary, A. Alumnichain: Blockchain based records verification service. *Int. J. Innov. Technol. Explor. Eng.* **2019**, *8*, 4296–4299. [CrossRef]
31. Turkanovic, M.; Holbl, M.; Kosic, K.; Hericko, M.; Kamisalic, A. EduCTX: A Blockchain-Based Higher Education Credit Platform. *IEEE Access* **2018**, *6*, 5112–5127. [CrossRef]
32. Kuvshinov, K.; Nikiforov, I.; Mostovoy, J.; Mukhutdinov, D. Disciplina: Blockchain for Education. 2018. Available online: https://www.disciplina.io/yellowpaper.pdf (accessed on 21 February 2021).
33. Wahab, A.; Barlas, M.; Mahmood, W. Zenith Certifier: A Framework to Authenticate Academic Verifications Using Tangle. *J. Softw. Syst. Dev.* **2018**, *2018*. [CrossRef]
34. Lam, T.Y.; Dongol, B. A blockchain-enabled e-learning platform. *Interact. Learn. Environ.* **2020**, 1–23. [CrossRef]
35. Li, H.; Han, D. EduRSS: A Blockchain-Based Educational Records Secure Storage and Sharing Scheme. *IEEE Access* **2019**, *7*, 179273–179289. [CrossRef]
36. Bore, N.; Karumba, S.; Mutahi, J.; Darnell, S.S.; Wayua, C.; Weldemariam, K. Towards Blockchain-enabled School Information Hub. In Proceedings of the Ninth International Conference on Information and Communication Technologies and Development—ICTD, Lahore, Pakistan, 16–19 November 2017; ACM: New York, NY, USA, 2017; pp. 1–36. [CrossRef]
37. Xu, Y.; Zhao, S.; Kong, L.; Zheng, Y.; Zhang, S.; Li, Q. ECBC: A High Performance Educational Certificate Blockchain with Efficient Query, in Theoretical Aspects of Computing—ICTAC 2017. *Lect. Notes Comput. Sci.* **2017**, *10580*, 288–304. [CrossRef]
38. Lizcano, D.; Lara, J.A.; White, B.; Aljawarneh, S. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. *J. Comput. High. Educ.* **2020**, *32*, 109–134. [CrossRef]
39. Palma, L.M.; Vigil, M.A.G.; Pereira, F.L.; Martina, J.E. Blockchain and smart contracts for higher education registry in Brazil. *Int. J. Netw. Manag.* **2019**, *29*, e2061. [CrossRef]
40. Arenas, R.; Fernandez, P. CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. In Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Stuttgart, Germany, 17–20 June 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2018; pp. 1–6.
41. Cheng, J.-C.; Lee, N.-Y.; Chi, C.; Chen, Y.-H. Blockchain and smart contract for digital certificate. In Proceedings of the 2018 IEEE International Conference on Applied System Invention (ICASI), Taiwan, China, 13–17 April 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2018; pp. 1046–1051.
42. Han, M.; Li, Z.; He, J.; Wu, D.; Xie, Y.; Baba, A. A Novel Blockchain-based Education Records Verification Solution. In Proceedings of the 19th Annual SIG Conference on Information Technology Education, Fort Lauderdale, FL, USA, 3–6 October 2018; Association for Computing Machinery (ACM): New York, NY, USA, 2018; pp. 178–183.
43. Karataş, E. Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System. *Int. J. Inform. Technol.* **2018**, *11*, 399–406. [CrossRef]

44. Srivastava, A.; Bhattacharya, P.; Singh, A.; Mathur, A.; Prakash, O.; Pradhan, R. A Distributed Credit Transfer Educational Framework based on Blockchain. In Proceedings of the 2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T), Allahabad, India, 21–23 September 2018; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2018; pp. 54–59.
45. Li, T. Design of Outcome-based Education Blockchain. *IJPE* **2018**, *14*, 2403. [CrossRef]
46. Ocheja, P.; Flanagan, B.; Ueda, H.; Ogata, H. Managing lifelong learning records through blockchain. *Res. Pr. Technol. Enhanc. Learn.* **2019**, *14*, 4. [CrossRef]
47. Baldi, M.; Chiaraluce, F.; Kodra, M.; Spalazzi, L. Security analysis of a blockchain-based protocol for the certification of academic credentials. *arXiv* **2019**, arXiv:1910.04622.
48. Cheng, H.; Lu, J.; Xiang, Z.; Song, B. A Permissioned Blockchain-Based Platform for Education Certificate Verification. *Commun. Comput. Inf. Sci.* **2020**, *3*, 456–471.
49. Rooksby, J.; Dimitrov, K. Trustless education? A blockchain system for university grades1. *Ubiquity J. Pervasive Media* **2020**, *6*, 83–88. [CrossRef]
50. Sun, H.; Wang, X.; Wang, X. Application of Blockchain Technology in Online Education. *Int. J. Emerg. Technol. Learn.* **2018**, *13*, 252–259. [CrossRef]
51. Jeong, W.-Y.; Choi, M. Design of recruitment management platform using digital certificate on blockchain. *J. Inf. Process. Syst.* **2019**, *15*, 707–716. [CrossRef]
52. Bandara, I.; Ioraş, F.; Arraiza, M.P. The Emerging Trend of Blockchain for Validating Degree Apprenticeship Certification in Cybersecurity Education. *INTED2018 Proc.* **2018**, *1*, 7677–7683. [CrossRef]
53. Arndt, T.; Guercio, A. Blockchain-Based Transcripts for Mobile Higher-Education. *Int. J. Inf. Educ. Technol.* **2020**, *10*, 84–89. [CrossRef]
54. Ghazal, O.; Saleh, O.S. A graduation certificate verification model via utilization of the blockchain technology. *J. Telecommun. Electron. Comput. Eng.* **2018**, *10*, 29–34.
55. Gresch, J.; Rodrigues, B.; Scheid, E.; Kanhere, S.S.; Stiller, B. The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling. In *Business Information Systems*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2019; Volume 339, pp. 185–196.
56. Prinz, W.; Kolvenbach, S.; Ruland, R. Blockchain for Education: Lifelong Learning Passport. *ERCIM News* **2020**, *120*, 15–16.
57. Göbel, J.; Krzesinski, A. Increased block size and Bitcoin blockchain dynamics. In Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC), Melbourne, Australia, 22–24 November 2017; Institute of Electrical and Electronics Engineers (IEEE): Piscataway, NJ, USA, 2017; pp. 1–6.
58. Benisi, N.Z.; Aminian, M.; Javadi, B. Blockchain-based decentralized storage networks: A survey. *J. Netw. Comput. Appl.* **2020**, *162*, 102656. [CrossRef]
59. Lyons, T.; Courcelas, L.; Timsit, K. *Scalability, Interoperability and Sustainability of Blockchains*; The European Union Block-chain Observatory and Forum, European Commission: Brussels, Belgium, 2019.
60. Eter Project. European Tertiary Education Register 2021. Available online: https://ec.europa.eu/education/european-tertiary-education-register_en (accessed on 11 February 2021).
61. UNESCO Institute for Statistics. Enrolment by Level of Education (Both Sexes) 2018. Available online: http://data.uis.unesco.org/ (accessed on 14 February 2021).
62. Wood, G. Polkadot: Vision for a Heterogeneous Multi-Chain Framework. 2016. Available online: https://polkadot.network/PolkaDotPaper.pdf (accessed on 17 January 2021).
63. Ethereum. Ethereum 2.0 (Eth2) 2021. Available online: https://ethereum.org/en/eth2/ (accessed on 21 February 2021).
64. Cachin, C. Architecture of the Hyperledger Blockchain Fabric. *Work. Distrib. Cryptocurrencies Consens. Ledgers* **2016**, *310*, 4.
65. Longo, R.; Podda, A.S.; Saia, R. Analysis of a Consensus Protocol for Extending Consistent Subchains on the Bitcoin Blockchain. *Computation* **2020**, *8*, 67. [CrossRef]
66. Sun, T.; Yu, W. A Formal Verification Framework for Security Issues of Blockchain Smart Contracts. *Electronics* **2020**, *9*, 255. [CrossRef]
67. Andola, N.; Gogoi, M.; Venkatesan, S.; Verma, S. Vulnerabilities on Hyperledger Fabric. *Pervasive Mob. Comput.* **2019**, *59*, 101050. [CrossRef]
68. Lin, I.-C.; Liao, T.-C. A Survey of Blockchain Security Issues and Challenges. *Int. J. Netw. Secur.* **2017**, *19*, 653–659. [CrossRef]
69. Lyons, T.; Courcelas, L. *Blockchain and cyber security*; The European Union Blockchain Observatory and Forum, European Commission: Brussels, Belgium, 2020.
70. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Futur. Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
71. Iqbal, M.; Matulevičius, R. *Blockchain-Based Application Security Risks: A Systematic Literature Review*; Proper, H.A., Stirna, J., Eds.; Springer International Publishing: Cham, Switzerland, 2019; Volume 349, pp. 176–188.
72. Nabil, A.; Nafil, K.; Mounir, F. Blockchain Security and Privacy in Education: A Systematic Mapping Study. In *Advances in Intelligent Systems and Computing*; Springer Science and Business Media LLC: Berlin/Heidelberg, Germany, 2020; pp. 253–262.

73. Androulaki, E.; Bortnikov, V.; Cachin, C.; de Caro, A.; Enyeart, D.; Muralidharan, S.; Murthy, C.; Smith, K.; Sorniotti, A.; Cocco, S.W.; et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *arXiv* **2018**, arXiv:1801.10228. [CrossRef]
74. Nasir, Q.; Qasse, I.A.; Abu Talib, M.; Nassif, A.B. Performance Analysis of Hyperledger Fabric Platforms. *Secur. Commun. Netw.* **2018**, *2018*, 1–14. [CrossRef]
75. Popov, S. The Tangle. Available online: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf (accessed on 2 April 2021).