Blockchain: Research and Applications 5 (2024) 100203

Contents lists available at ScienceDirect

Blockchain: Research and Applications

journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

Research Article

Expedition to the blockchain application potential for higher education institutions

Matthias Gottlieb [a,b,*], Christina Deutsch [b], Felix Hoops [b], Hans Pongratz [c], Helmut Krcmar [b]

[a] Bavarian Ministry of Digital Affairs, 80333 Munich, Germany
[b] Technical University of Munich, 85478 Garching By Munich, Germany
[c] TU Dortmund University, 44139 Dortmund, Germany

ARTICLE INFO

Keywords:
Blockchain
Higher education institution (HEI)
Administration
Protocol level
Application level
Application

ABSTRACT

In the education sector, blockchain is currently at the end of the peak of inflated expectations in Gartner's Hype Cycle. Thus, it is crucial to understand whether this technology meets the expectations of Higher Education Institutions (HEIs). We go on an expedition to identify blockchain application scenarios and its potential for HEI administration—the universities are digitalized to just 23.3%.

Current information systems research addresses classifications of blockchain-based projects (application level) rather than their technical realization (protocol level). Thus, when evaluating blockchain application scenarios in HEI administration, we intensively consider the technical side of blockchain-based projects. We perform a three-step approach: (1) systematic literature review, (2) qualitative exploratory semi-structured interviews to supplement information on market-ready solutions, and (3) an evaluation of the potential of the blockchain-based projects identified, based on HEI administration requirements.

We find that the leading blockchain application scenarios are credential verification and record-sharing. At the protocol level, we obtain equivocal results regarding the technical realization of projects, e.g., their underlying blockchain types and storage models. At the application level, when discussing the potential of different projects, we find that most of them address adaptability, complexity decomposition, and cost reduction requirements between HEIs; interest diversity and stakeholder collaboration between HEIs and business actors; privacy and trust between HEIs and students.

1. Introduction

Now that the Internet has become essential to digitalization, the digital revolution has been transforming almost all areas of life, including the economy, society, science, and education. It has also given rise to innovative technologies, such as blockchain. In education, Higher Education Institutions (HEIs) recognized the potential of digitalization early on [1]. According to Gilch et al. [2], 82.6% of HEIs consider the digital revolution's importance to be high or very high. However, due to the lack of digital transformation in HEI administration [2], this essential area of HEI faces challenges in terms of critical functions, such as record-keeping, authentication, certificate validation, processing of payments, and other management and support tasks.

Simultaneously, the blockchain technology's quick movement along the Gartner's Hype Cycle shows its progressive development and increasing maturity level. With its unique characteristics, blockchain can address the aforementioned problems, and other issues related to immutability, transparency, durability, and accountability can be mitigated by blockchain technology. Thus, blockchain might potentially address the requirements of HEI administrations.

However, blockchain research in information systems remains scarce and mainly focuses on classifications of blockchain-based projects (application level) rather than on their technical realization details (protocol level). To address this gap, when evaluating blockchain application scenarios in HEI administration, we intensively consider the technical side of blockchain-based projects. We go on an expedition and evaluate blockchain-based projects suitable for HEI administration at the application and protocol levels, as introduced by Rossi et al. [3].

We come up with the following research question: *What are the application scenarios of blockchain technology in HEI administration from a technical perspective, and with potential determined in the context of the requirements of individual HEI administrations? (RQ)*. The first part of the

* Corresponding author. Bavarian Ministry of Digital Affairs, 80333 Munich, Germany.
E-mail addresses: matthias.gottlieb@stmd.bayern.de, matthias.gottlieb@tum.de (M. Gottlieb).

https://doi.org/10.1016/j.bcra.2024.100203
Received 27 February 2022; Received in revised form 7 January 2024; Accepted 23 April 2024
Available online 26 April 2024

question refers to the protocol level after Rossi et al. [3], and the second part refers to the application level. We perform a three-step approach: (1) systematic literature review, (2) qualitative exploratory semi-structured interviews to supplement information on market-ready solutions, and (3) an evaluation of the potential of the blockchain-based projects identified, based on HEI administration requirements.

We find that credential verification and record-sharing, followed by credit management, reputation management, and an HEI admission application system, are the leading blockchain application scenarios. At the protocol level, we obtain equivocal results regarding the technical realization of projects, e.g., their underlying blockchain types and storage models. At the application level, we find that most projects, as their potential, address adaptability, complexity decomposition, and cost reduction requirements between HEIs; interest diversity and stakeholder collaboration between HEIs and business actors; privacy and trust between HEIs and students.

The article is structured as follows. First, we provide an insight into the relevant theoretical foundations in Section 2. Building on this, Section 3 takes a deeper look at existing theories in the blockchain area and HEI administration's needs. We describe our approach in Section 4. We then present our findings in Section 5, which serve as a basis for the subsequent critical discussion in Section 6. The article concludes by presenting a summary, relevant limitations, and an outlook on potential future research in Section 7.

2. Theoretical background

No unified definition of blockchain technology exists. The standards based on ISO/TC 307 regarding blockchain and distributed ledger technologies are under development [4]. In the following, we understand blockchain as a distributed ledger technology with an "[…] ordered, back-linked list of transactions" that are grouped into blocks and "[…] take place in a decentralized manner" [5,6]. These blocks share information across multiple data storages (nodes). Hence, each node in the network has identical data records without a central controlling unit [5].

Each block has a block header and a block body (see Fig. 1). The block header contains the block's metadata, including its version, timestamp, previous block hash, nonce, difficulty target, and the Merkle root hash. The block version discloses the validation rules applicable to the block, and the timestamp refers to the block's creation time. In the Merkle tree (with the Merke root hash at the top), each pair of hashes is used to calculate the hash on the higher level in the tree structure. The nonce is essential for calculating the block hash, while miners modify it until it reaches a certain threshold or difficulty target. The transactions (TX in Fig. 1) and the transaction counter form the block body. Multiple blocks form a chain—the blockchain [6].

Regarding access to transactions (authentication), there are two blockchain types: public and private. Combinations of the two types in a hybrid infrastructure are possible. Regarding write permissions and access to transaction validation (authorization), we can distinguish between permissioned and permissionless blockchains.

A *public permissionless blockchain* means that anyone can read and write transactions. Therefore, the system is highly decentralized and needs a way to decide on the block to be added next, which is realized via the consensus mechanism [7]. This blockchain type allows for high scalability due to the absence of restrictions on new nodes joining the system [8].

A *public permissioned blockchain* means that all nodes can read transactions, but a single node can only write and participate in transaction validation after its successful authorization [9].

A *private permissionless blockchain* means that access must be cleared to a certain group or organization, and anyone within this group or organization can read and write transactions. However, this type is rarely discussed in the literature or used in applications [9].

A *private permissioned blockchain* stands for "restricted read and write permissions", meaning that only a limited number of nodes can read transactions, and only the network operator can write transactions and participate in consensus validation [9]. The system is decentralized to a lesser extent than in the case of public blockchains but demonstrates high efficiency. However, as each entering node requires authorization, its scalability is low [8].

A consensus mechanism enables maintenance of the blockchain's consistent state. It enables a decision regarding which block to be added next to the blockchain [8]. In the following, we shed light on some common consensus mechanisms.

One of the consensus mechanisms used most often is Proof of Work (PoW). Since all nodes can potentially participate in transaction validation and PoW requires much power, the main problems are latency and low throughput, which lead to low efficiency [8]. The computing power available to a node determines its ability to add a new block to the ledger. PoW's main shortcomings are its high energy consumption and the time it takes to calculate a single block. The most well-known threat to PoW is the 51% attack. This requires an attacker to control more than 50% of the available computing power, which is nearly impossible to achieve in practice [7].

In Proof of Stake (PoS), validators lock part of their cryptocurrency as a stake, whereby the coin age is decisive for selecting a validator node. After forging a new block, a node may receive a stacking reward. Compared to PoW, PoS is energy efficient [10]. Its main shortcoming is the Nothing-at-Stake problem [11].

Delegated Proof of Stake (DPoS) is based on PoS and is comparable to representative democracy. Stakeholders select witnesses (block producers) by allocating their tokens as votes in their favor. N witnesses who have received the highest number of votes get the suffrage. Compared to PoS, the main advantage is scalability due to participants'

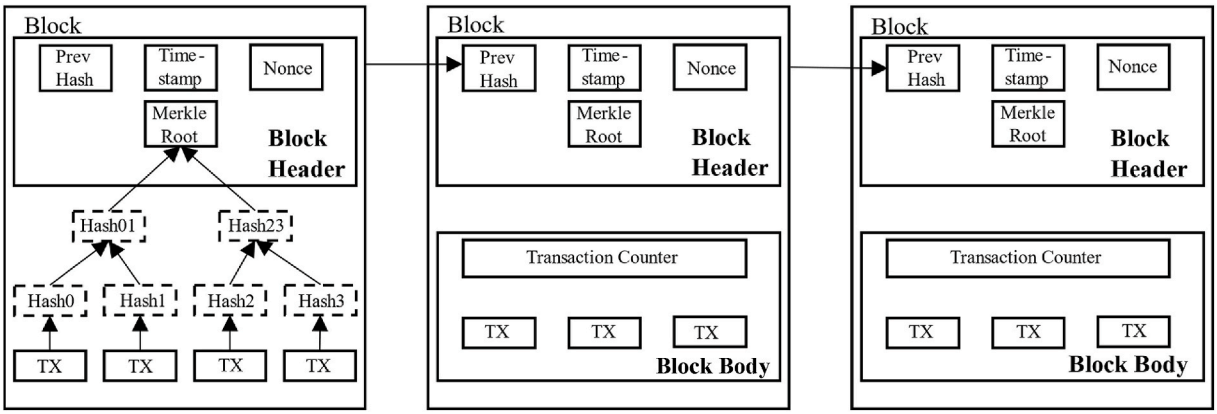

Fig. 1. Blockchain structure.

ability to participate indirectly in the consensus by delegating their voting rights. The main shortcomings encompass trust in a restricted number of nodes and a tendency toward centralization [12].

In Proof of Authority (PoA), by its definition, it is not targeted at permissionless blockchain types, a set of authority nodes responsible for validation is chosen based on their reputation instead of coins. These nodes should confirm their identities as trustworthy. This consensus mechanism allows for high scalability and is less computationally intensive than PoW [13].

3. Related work

The focus of this article is twofold: blockchain technology and its relation to the requirements of HEI administration.

3.1. Blockchain

Cryptocurrencies, especially Bitcoin, as a medium of exchange enabled through blockchain technology, first entered Gartner's Hype Cycle in 2014, while blockchain, as the overarching concept, replaced them only in 2016 [14,15]. Since then, scientists have engaged actively with blockchain-based application scenarios [16]. Casino et al. [16] stated that blockchain-based applications are likely expand to new areas and contexts due to the technology's continuously improving maturity.

According to Rossi et al. [3], existing research on blockchain in information systems is scarce. Regarding the framework for blockchain research in information systems, Rossiet al. [3] differentiated between protocol level, application level, and the interactions between them. Protocol level refers to the blockchain protocol that defines the creation of a blockchain and human actors' interactions with the protocol itself [3]. The identification of blockchain application cases happens at the application level [3]. Rossi et al. [3] mentioned that research into this level is still needed but should be performed instead on the interconnection between the two levels.

One of the application areas for blockchain is education. Alammary et al. [17], Chen et al. [18], Fernández-Caramés and Fraga-Lamas [19], and Grech and Camilleri [20] have already explored how this area can benefit from blockchain technology. Certificate management, competency and learning outcome management, and the evaluation of students' professional skills are the main application areas in education [17]. Li et al. [21] found academic degree management and the evaluation of learning outcomes to be relevant blockchain application cases. Fernández-Caramés and Fraga-Lamas [19] addressed blockchain for smart campuses. Grech and Camilleri [20] also analyzed blockchain applications for education and found that most of them were in their infancy.

However, the systematic reviews of blockchain for educational purposes mentioned above focus on its application to higher education and to education in general. These reviews only consider the application level in accordance with Rossi et al. [3]. Moreover, as most blockchain-based education-related projects were at the beginning of their development in 2017 [20], up-to-date scientific research is necessary to analyze the available projects and identify mature solutions ready for real-world use. Chen et al. [18] mentioned the need to conduct further research on blockchain opportunities in the context of education.

3.2. HEI administration requirements

As a framework for evaluating blockchain-based projects at the application level, we consider the framework initially introduced in Ref. [22]. The following briefly describes the categories and corresponding requirements behind this framework. To digitally transform an HEI administration or introduce new technologies therein, HEI administrations should consider specific requirements [22]. Four categories distinguish these requirements: (1) HEI to HEI (H2H), (2) HEI to Business (H2B), (3) HEI to Student (H2S), and (4) Services.

(1) H2H refers to the Information and Communication Technology (ICT) usage within an HEI or interactions between HEIs.
(2) H2B deals with the connections between an HEI and its partners.
(3) H2S is about services and applications offered to students.
(4) The Services category is the enabling services representing qualities of the ICTs used in HEIs.

3.2.1. H2H

For the following discussion, we first need to introduce relevant requirements already established by previous work [22]. The H2H category includes *ambidextrous organizations*, *adaptability*, *stability*, *balanced power*, *complexity decomposition*, *flexibility*, *accountability*, *staff education*, *cost reduction*, and *legal regulations*. An *Ambidextrous organization* means that an HEI adopts conflicting values: efficiencies and innovations. An HEI adapting to innovations and technological changes refers to *adaptability*. *Stability* is a phenomenon in which an organization tends to maintain its organizational structure. The HEI usually aims for *balanced power* distribution within the organization. *Complexity decomposition* is about decomposing complex problems, such as software projects, into smaller parts. Having a flexible infrastructure implies *flexibility*. Keeping HEI staff accountable with rules and regulations is covered by *accountability*. The HEI is responsible for providing *staff education* with necessary ICT competencies. The use of technologies yields a *cost reduction*. *Legal regulations* refer to the regulations applicable to digitizing efforts.

3.2.2. H2B

H2B is about *interest diversity* and *stakeholder collaboration*. Since an HEI acts as a managing entity in digital projects, it should know its internal and external stakeholders. Moreover, it should collaborate with them to create joint value propositions.

3.2.3. H2S

Student centricity, *digital identity*, *privacy*, '*no-stop shop'*, *trust*, and *engagement* form the H2S category. *Student centricity* is about an HEI focusing on its students and aiming to satisfy their needs. The ability of a student to identify himself/herself with a digital ID or other means is covered by *digital identity*. The HEI is responsible for guaranteeing students' *privacy*. *'No-stop shop'* refers to an HEI proactively supplying students with services. The HEI should build and maintain a vital level of trust among students. Motivating them to engage with digital services is summed up under *engagement*.

Services include requirements, such as *quality* and *efficiency,* but are not relevant to evaluating blockchain potential at the application level.

In Ref. [22], the authors suggested assessing the proposed requirements matrix in light of more HEIs and technological innovations. Thus, in the following, we focus on blockchain technology as an innovation in educational scenarios (applications) and its potential in HEI administration. Our goal is to identify concrete blockchain-based projects suitable for university administration and to discuss their design at the protocol level. To identify relevant potential, we evaluate these projects in the context of the requirements of HEI administration at the application level.

4. Research design

We conducted a literature review based on Brocke et al. [23] to identify blockchain projects relevant to HEI administration. We focused on the first four steps ((v) in Fig. 2 was out of study focus). Then, we completed our findings by exploring backward citations and qualitative exploratory semi-structured interviews. Fig. 2 depicts our research methodology.

For the literature review, to determine relevant papers, we applied the strategy of Dybå and Dingsøyr [24]. In the first step, we looked for papers available in two databases Scopus and Web of Science Core Collection, which are known for their interdisciplinary coverage. We

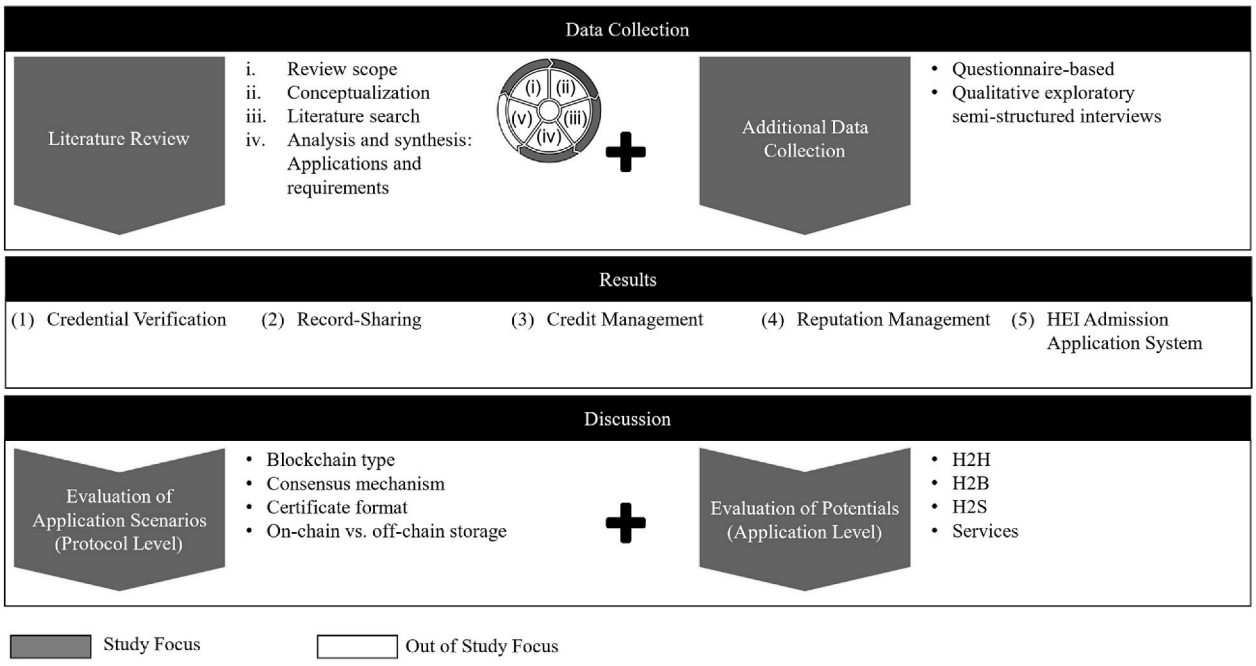

Fig. 2. Research methodology.

used the conjunction of keywords "blockchain" (and its spelling variations) and "education*" (or "universit*" or "HEI" or "HE" or "student*" or "academi*") to search in Title and Abstract fields of each database (June 2020). In Scopus, the search query resulted in 121 articles, and, in Web of Science Core Collection, it resulted in 53 articles. In total, we identified 128 articles. In the second step, we read the papers' titles and only included those focusing on blockchain in education in general or, specifically, in higher education. Some candidates for exclusion consisted of contributions addressing blockchain application in a concrete study program, such as chemistry, as well as those discussing students' education on the topic of blockchain. This step resulted in 107 papers. Next, we read the abstracts of the contributions from the previous step. We included only papers that proposed a concrete blockchain-based project feasible for one of the HEI administration processes. Some excluded papers were about, e.g., a solution focusing on the teaching and learning sector, such as grading a thesis. This step resulted in 55 papers. Compared to Dybå and Dingsøyr [24], we did not conduct a detailed quality appraisal, as we obtained our hits from the Scopus and Web of Science databases. These databases, in most cases, already ensure the high quality of the publications. In the next step, we screened the full texts of the 55 papers. The exclusion criteria were as follows: (1) the paper was not in English, or (2) it did not contain a detailed description of the project's technical details, the intended architecture components, and their interactions. We also excluded papers that did not comply with the inclusion criteria defined in the previous steps. As a result, our search resulted in 17 papers.

In the last step, following Webster and Watson [25], we looked for backward citations. We included a contribution in our search results if one of the 17 papers briefly introduced it as illustrative for a concrete blockchain-based project suitable for HEI administration. We ended up with 29 sources in total.

We contacted their developers to complement the data on market-ready blockchain-based applications. Based on a questionnaire, we conducted qualitative exploratory semi-structured interviews after Myers and Newman [26].

We structured our findings into five categories depending on their primary application objective (see results in Fig. 2 and the next section). We described our results extensively, focusing on their technical realization in terms of blockchain type (permissioned or permissionless, private or public), concrete blockchain type (e.g., Ethereum), consensus mechanism (e.g., PoW), certificate format (e.g., Open Badge), on-chain storage (i.e., data located on the ledger), and off-chain storage (i.e., data located outside of the ledger). We then discussed our results (see discussion in Fig. 2) at the protocol level (see Section 6.1). To do so, we addressed each of the five application categories (results in Fig. 2) separately regarding the solutions assigned. We discussed the categories concerning blockchain type, consensus mechanism, certificate format, and on-chain *vs.* off-chain storage. Afterward, we analyzed blockchain technology's potential in the identified projects at the application level (see Section 6.2). To do so, we applied the requirements for digitally transforming HEI administration from three categories, H2H, H2B, and H2S, introduced in Section 3.2, to the blockchain-based projects.

5. Results

In the following, we provide an overview of blockchain applications by classifying them into five categories and focusing on their technical realization.

We classify blockchain-based projects into five categories: (1) credential verification, (2) record-sharing, (3) credit management, (4) reputation management, and (5) HEI admission application system (see Table 1). If a project is suitable for multiple categories, we assign it to the category corresponding to its primary objective. An exception is EduCTX because its goal changed from credit management to credential verification during the development process (M. Turkanović, personal communication, August 12, 2020). We added this project to the credit management scenario and additionally discussed it under credential verification. Regarding the projects' technical realization at the protocol level [3], we describe them in terms of the high-level blockchain type, including access to transaction validation and read permissions, and the concrete blockchain type. Further characteristics are the consensus mechanism and the data stored on-chain and off-chain.

5.1. Credential verification

The credential verification category includes most projects. We divide the projects into two groups—prototypes and applications—and discuss them separately. The prototype category means that a prototype

Table 1
Categorization of blockchain-based projects.

Category	Description	Project	
Credential verification	Projects concerned with verifying credentials, i.e., checking whether the issuer, the verifier, and the holder of the credential can trust each other. A 'credential' is a digital file describing a learning achievement, whereby it should guarantee the authenticity and integrity of its content [27].	**Prototype** * Blockchain Notarization * BTCert * CredenceLedger * Degree Certify * Digital Credentials Consortium (DCC) * Digital Rights Management System (DRMS) * HEI Verify * Project by Sony Global Education * SCVer * TrueRec * UniChain	**Application** * BCDiploma * BlockCerts * Blockchain 4 Education * Diplo-Me * Gradbase * OpenCerts * Proven Open Excellence (PoEx)
Record-sharing	Projects focus on transferring records from an H2H or H2B. A credential verification project always includes record-sharing. However, the verification is not a necessary part of a record-sharing project.	* Blockchain of Learning Logs (BOLL) * Educational Professional Personal Records (EPPR) * Education-Industry Cooperation (EIC) * EduRSS * Grades Chain	
Credit management	Projects refer to the management of the European Credit Transfer and Accumulation System (ECTS) credits that represent academic achievements.	* Credentify * Credits Manager * EduCTX	
Reputation management	Projects concentrate on tokens as a measure of a student, trainer, or institution's reputation.	* Kudos	
HEI admission application system	A project that deals with the student-admission process at an HEI.	* Admission Application System (AAS)	

is already available, implemented with a concrete set of tools, and tested with non-real users, such as threads. An application refers to a project that has already been fully developed, evaluated with real users, and may be in a market-ready state. If a project has been given a name by its author, we mark its first occurrence with '' (e.g., 'CredenceLedger'). For better readability, we assign a name to each of the initially unnamed projects but do not enclose their first occurrences in '' in the text.

5.1.1. Prototypes

There are 11 out of 18 credential verification projects are in the prototype state: '*TrueRec*' [28], '*BTCert*' [29], '*Digital Credentials Consortium*' (*DCC*) [30], '*CredenceLedger*' by Arenas and Fernandez [31], '*UniChain*' by Daraghmi et al. [32], project by *Sony Global Education* [33], Guo et al. [34] (in the following referred to as *Digital Rights Management System* (*DRMS*)), Palma et al. [35] (*Degree Certify*), Badr et al. [36] (*HEI Verify*), Chowdhury et al. [37] (*Blockchain Notarization*), and Curmi and Inguanez [38] (*SCVer*). Most of these solutions involve verifying digital records by third parties. However, *HEI Verify* [36] mainly focuses on verification by other HEIs. Curmi and Inguanez [38] went one step beyond the verification process and started with paper-based documents' digitalization. The *DRMS* [34] allows for educational multimedia data authentication. Unlike other projects, the data sources do not refer to the students' major achievements but to their submissions and the learning materials created by education authorities [34].

The verification process in *TrueRec* [28], *CredenceLedger* [31], and *Sony Global Education* [33] looks as follows. After a credential is issued, its hash is on the blockchain, and the student receives the credential (or access to it). The student can share this document with a third party for verification. The third party then uses a platform (API or mobile application) to compare the locally calculated hash value of the document with the hash value on the blockchain. If both values are the same, the verification process is successful. However, this procedure does not indicate the authenticity of the corresponding document or the validity of the issuing institution.

In *BTCert*'s similar verification process, a certifier first verifies a student's information when he/she applies for a certificate [39]. In *HEI Verify* [36], a student applies for a digital certificate from his/her home HEI and specifies the receiving institution. His/her home university then initiates a transaction with this receiver [36].

Regarding access control, applications rely on Access Control Lists (ACLs) that define parties' permissions [36]. These lists may restrict a participant from accessing a credential and allow the participating parties' identity mapping. Different kinds of permissions are present in *CredenceLedger* [31]. The student defines the sharing policy applicable to data consumers in the system by Chowdhury et al. [37].

SCVer [38] realizes the verification processes with Smart Contracts (SCs). Time-based SCs also regulate *UniChain* [32]. *Degree Certify* [35] issues degree certificates via SCs.

Compared to other projects, the *DCC* [30] does not need an always online issuer or another trusted party. In this system, students are identified by Decentralized Identifiers (DIDs), the most common identifier standard for Self-Sovereign Identities (SSIs), which allow students to be in better control of their private data [40]. Students can decide on using their identity information but cannot change it. The main advantage of DIDs is that centralized Certification Authorities (CAs) are no longer required. Users can create these unique identifiers by themselves, being in control of the information they want to disclose [40].

The *DRMS* consists of two decentralized peer-to-peer networks—Learning User Network (LUN) and Education Certification Network (ECN)—and a local network for each Education Authority (EA), such as a university or school. Therefore, compared to the earlier projects, this solution is the only one that relies on multiple blockchains. However, like the systems discussed before, SCs carry out the verification process.

Regarding the underlying blockchain technology, *BTCert* [29], *SCVer* [38], and *Degree Certify* [35] run on a public permissionless blockchain. *Degree Certify* [35] uses Ethereum, *BTCert* [29] uses Bitcoin, and *SCVer* [38] is blockchain-agnostic. However, *Degree Certify* [35] considers switching to Hyperledger Fabric to enable students to disclose only selected academic data. The authors also considered a hybrid model with a private blockchain for non-profit-making HEIs and a public blockchain for public HEIs [35]. In contrast, the *DCC* aims for a permissioned public blockchain [41]. However, its developers also consider switching to a public permissionless blockchain if a consensus mechanism that does not have as negative an environmental impact as PoW

becomes available [41]. All other projects, except for *DRMS* [34], are based on a permissioned private blockchain: *Sony Global Education* [33] and *HEI Verify* [36] rely on Hyperledger Fabric, *CredenceLedger* [31] rely on Multichain, and the rest rely on Ethereum. *CredenceLedger* by Arenas and Fernandez [31] uses streams instead of cryptocurrency and relies on mining diversity as a consensus mechanism. The authors justified their blockchain choice with higher transaction throughputs, lower costs, and lower resource consumption [31]. The *DRMS* [34] relies on permissioned private and permissionless public blockchains.

When looking at the data stored on the blockchain, we see that the certificates are stored directly on the ledger only in *SCVer* [38], *Degree Certify* [35], and the *DRMS* [34]. The authors explained their decision by the need to put the HEI under "public scrutiny" [35]. Another reason is cost-effectiveness due to the omission of transaction creation for verification and, therefore, payments only for gas consumption [38]. All other projects use the on-chain off-chain model, meaning that the blockchain only stores the document's hash (or the link to the document stored in an external database) and some added non-personal information. The credential itself is in external data storage.

The credentials' format varies among the projects. In *TrueRec*, credentials are in a specific TRU format [28]. In *BTCert*, they are stored as PDFs or JSON files in MongoDB [39]. In the well-advanced *DCC* project, credentials are in JSON-LD and comply with the W3C VC model. In *SCVer* [38], a credential is created based on a paper-based certificate by Tesseract OCR, which extracts data from a certificate's scanned image.

5.1.2. Applications

Applications focusing on credential verification encompass '*Gradbase*' [42], '*Proven Open Excellence*' (*PoEx*) [43], '*BlockCerts*' [44], '*BCDiploma*' [45], '*Diplo-Me*' [46], '*OpenCerts*' [47], and '*Blockchain 4 Education*' [48]. The main difference compared to prototypes is that applications more actively consider GDPR-compliant data storage models and user authentication.

Bitcoin-based *PoEx* is the most straightforward project because it only allows for proving the existence of the document's hash on the blockchain [49]. Therefore, this project is similar to the prototypes *TrueRec* [28], *CredenceLedger* [31], and *Sony Global Education* [33] discussed above. The users can use the interface to upload a file to create its hash. They can then provide the value obtained to a third party, who can then use the same interface to verify the corresponding document's existence at a given time [49].

BlockCerts, in addition to a simple proof of existence, considers further checks. A learner's credential obtained from his/her HEI complies with a certificate template [44]. This certificate can be revoked based on the Open Badges HTTP URI revocation list. For the issuing HEI's check, its public key is extracted from the hosted issuer profile and compared to the public key contained in the transaction. However, *BlockCerts* does not include a mapping between a public key and an organization or a student. Hence, it does not consider the identity management task [44].

In *Gradbase*, the issuing HEI uploads a spreadsheet containing students' degrees to the platform to be stored directly on the blockchain [42]. Afterward, a QR code is generated for each record. Students can include this QR code, or the URL associated with the QR code in their CV or LinkedIn profiles such that an employer can scan it with a QR reader for verification. As the document contains the student's profile picture, an employer can also prove a learner's identity [42].

Like *Gradbase*, which allows the issuer to upload multiple records simultaneously, *OpenCerts* [47] enables batching multiple certificates within a single transaction. SkillsFuture Singapore is responsible for the verification of these institutions. Students of the institutions that are part of the SkillsFuture registry have a Skills Passport, where their certificates are stored [47].

In *Blockchain 4 Education*, two SCs regulate the verification process [48,50]. With the *Blockchain 4 Education* project, its developers address the shortcoming of *BlockCerts* regarding security. Certifiers staying anonymous but being able to prove that they belong to a CA contribute to increased security [48,50].

In *BCDiploma*, an HEI cannot issue a certificate but should get an ID certificate beforehand [51]. The HEI can upload data to *BCDiploma*. These data are encrypted with the Crypto App, based on the idea of Shamir's Secret Sharing, and placed directly on the blockchain. The student receives the certificate's URL. He/she can share this URL with a third party. This third party can use it in the Reader App to see the student's certificate and check the HEI's ID certificate by going to the university's web page or the BCDiploma issuers list containing the HEI's Ethereum address [45,51]. Therefore, compared to *BlockCerts,* which does not focus on identity control, *BCDiploma* allows for authenticity checks of HEIs.

In contrast to *BCDiploma*, several CAs are involved in *Diplo-Me* [52]. Like in *BCDiploma*, the developers of *Diplo-Me* consider the identity checking issue but aim to use an external identification system rather than an integrated identity check. When a CA issues a certificate, it is first encrypted with its private key and then with the user's private key, resulting in a multi-signature [46,52].

Regarding the underlying blockchain technology, five out of seven applications run on permissionless public blockchains, whereby *OpenCerts* [47] and *BCDiploma* [45] currently rely on Ethereum, *Gradbase* [42] and *PoEx* [43] rely on Bitcoin. *BlockCerts* [44] is blockchain-agnostic. *BCDiploma* is a use case of the EvidenZ framework and includes built-in Blockchain Certified Data Tokens (BCDTs) [51]. However, *BCDiploma* developers are considering switching to the Ark platform [53,54]. The blockchain used in *Diplo-Me* [46] and *Blockchain 4 Education* [48] is permissioned Ethereum Quorum.

Regarding data storage, in *BlockCerts* [44], *Blockchain 4 Education* [48], *OpenCerts* [47], and *PoEx* [43], only the document's hash (and some additional non-personal information) is stored on the blockchain. In *Blockchain 4 Education*, the actual documents are stored off-chain in the InterPlanetary File System (IPFS) (W. Prinz, personal communication, August 4, 2020). In *Gradbase*, students' encrypted academic data are stored on the blockchain [42]. In *BCDiploma*, the encrypted data are stored directly on the blockchain, and the erasable persistence keys are in the HEI's external key storage [51]. *Diplo-Me* considers three different data storage options [52]. The first is that only the qualification's signature is stored on the blockchain, and the corresponding credential is saved externally. Second, a double-encrypted anonymized qualification without identity data is placed in the wallet. With the SSI, this qualification is set in the wallet in the last option [52].

Referring to the credential format, we found that, in *BCDiploma* [45], *Blockchain 4 Education* [48], and *BlockCerts* [44], the certificates comply with the Open Badges format. In *BlockCerts*, the information in the certificate encompasses the data about the certificate itself, the issuer's information, the URL of the issuer's website, e-mail, name, revocation list, the public key and signature lines, and the recipient's information [44]. Embedding the Diploma Supplement in the certificate is also possible [44]. The certificates in *OpenCerts* are currently in general-purpose JSON, but the developers aim to represent them in the special-purpose Open Badges format expressed in JSON-LD [47]. Diplo-Me certificates are also in JSON format, and the data model is compatible with existing Bologna and EU models, such as Europass and Diploma Supplement [46,52].

5.2. Record-sharing

In record-sharing projects, records can be transferred either as H2H or H2B. The first project, the '*EduRSS*' [55], stores and shares records among HEIs. In contrast, *Education-Industry Cooperation* (*EIC*) system [56] enables certificate transfer between HEIs and companies. The next project deals with Educational Professional Personal Records (*EPPRs*) [57] shared between HEIs and third parties. The fourth, Blockchain of Learning Logs ('*BOLL*') by Ocheja et al. [58], enables the transfer of lifelong learning educational logs across institutions. Learning tools

generate these records—the Learning Management System (LMS) Moodle and a digital book reader BookRoll. Han et al. [59], the last solution's authors (in the following addressed as *Grades Chain*) thought that student certificates should contain academic achievements such as grades and any concrete steps the student has taken to complete a course.

Regarding the underlying blockchain technology, the *EduRSS* system runs on permissioned private Ethereum with PoS [55]. In this project, to prevent collusion tamper attacks, the data are periodically replicated to the public Ethereum [55]. *BOLL* [58], *EPPR* [57], and *Grades Chain* [59] rely on permissioned public Ethereum blockchains. The *EIC* prototype [42] is the only project based on Hyperledger Fabric.

In *EduRSS* [55], only the Merkle tree root hashes are on the blockchain. The corresponding files are encrypted and placed on the HEI's storage server. However, the authors mentioned that centralized storage usage is not desirable and planned to replace it with a decentralized solution, such as the IPFS [55]. In *BOLL*, the hashes are also on the blockchain, and the corresponding records that comply with the xAPI or IMS Caliper standards are stored off-chain in MongoDB [58]. However, as only the hashes are on the blockchain, the learning logs can no longer be retrieved if an institution and the corresponding LMS no longer exist. In *Grades Chain* [59], only the documents' URLs are written on the blockchain, and records are stored in external databases. The same applies to *EPPR* [57], but a Resource Description Framework (RDF) database acts as data storage.

5.3. Credit management

The '*EduCTX*' platform [60], the prototype of Srivastava et al. [61] (in the following referred to as *Credits Manager*), and the '*Credentify*' application [62] form the next category—credit management. All these projects refer to rewarding students with tokens that correspond to unspecified or ECTS credits. An ECTS credit is a whole number and corresponds to 25–30 h of work a student should accomplish to achieve a defined learning outcome [63].

Turkanović et al. [60] proposed a system called *EduCTX*. It is a credit platform where ECTS credits are equal to the ECTX tokens, whereby each student has a wallet to collect ECTX tokens. Currently, the developers of *EduCTX* are transforming their solution into a credential verification platform that aims to follow the SSI and Verifiable Credential (VC) concepts (M. Turkanović, personal communication, August 12, 2020). In the prototype *Credits Manager* [61], tokens representing credits are also transferred to the student's wallet upon completing a course. *Credentify* allows an HEI to issue micro-credentials mapped to ECTS credits [62]. HEIs also have wallets to store credentials issued, which these institutions can use to prove their accreditation [62]. Non-fungible Tokens (NFTs) that are part of the *Credentify* system [62] may prevent duplicate assignments of credits and control an asset's ownership. *EduCTX* [60] and *Credits Manager* [61] aim to overcome these issues with a multi-signature.

Regarding the underlying blockchain technology, the *EduCTX* project initially ran on Ark [60], while Srivastava et al. [61] also realized *Credits Manager* using this platform. However, *EduCTX* developers switched to Ethereum, as Ark does not support SCs. The main issue with SCs is that the creator of an SC is automatically its owner (M. Turkanović, personal communication, August 12, 2020). Hence, such creators can easily manipulate the network. The developers solved this problem by introducing a list of SC owners. The next issue was that the University of Maribor, the HEI where the *EduCTX* platform was developed, would still decide on the membership of new HEIs. To account for this centralization issue, SCs were adjusted, allowing other members to vote. However, as Ethereum is a permissionless public blockchain, developers started considering working with Hyperledger Fabric. The main reasons for choosing this blockchain were its facility for permissioned enterprises and the possibility of creating a consortium network composed of HEIs as nodes. (M. Turkanović, personal communication, August 12, 2020).

In contrast to the previous two projects, the 0xcert framework serves as the basis of *Credentify* and manages NFTs that comply with Ethereum's ERC-721 and ERC-2477 standards [64]. This framework simplifies the issuance of NFTs on the Ethereum blockchain.

Regarding the data stored on the blockchain, in the *Credentify* system, the ledger does not contain personal information [62]. This is also true for the *EduCTX* system [60]. At the beginning of development, corresponding files were stored on a single server at the University of Maribor (M. Turkanović, personal communication, August 12, 2020). To remove this centralized off-chain storage, its developers started storing documents in encrypted form in the IPFS and aimed at a W3C standardization for the credentials (M. Turkanović, personal communication, August 12, 2020). In *Credentify*, the credentials follow the JSON format [62].

5.4. Reputation management

The reputation management category is like the credit management projects discussed above, as getting rewarded with cryptocurrency for acquiring competency is comparable to a student's effort to receive an ECTS credit. This category only includes two projects. In both contributions, by Sharples and Domingue [65] and Lizcano et al. [66], an 'educational reputation currency' [65], referred to as '*Kudos*', measures the reputation of students, trainers, and organizations. Both prototypes run on a permissioned public Ethereum blockchain, and SCs automate micropayments. In Ref. [65], students and organizations use wallets to store their Kudos. Certificates or other authorship records, such as scientific works, are stored on the blockchain, and each item is associated with reputational tokens [65].

Lizcano et al. [66] extended and concretized the framework introduced in Ref. [65]. They proposed a system where Kudos are transferred to a student when he/she proves to have a particular competency by solving a "standard problem" [66]. The currency is transferred to a trainer if he/she trains a student according to the market's current needs [66].

5.5. HEI admission application system

We finish the presentation of our findings with a unique blockchain-based project, a "[…] digital university admission application system with study documents and e-portfolio […]" by Mori and Miwa [67] (in the following referred to as *AAS* for *Admission Application System*). A study document contains the student's data, such as subject grades, curricular, and extracurricular activities. In the e-portfolio, the student describes the learning processes for these activities.

The authors proposed using a permissioned private Ethereum for the system's implementation [67]. They extended the ERC-721 standard such that an NFT contains the owner's and the issuer's addresses [67]. In contrast to fungible values and cryptocurrencies, such as Bitcoin, NFTs are limited in number and not interchangeable [68]. In *AAS*, NFTs contain the actual data on-chain. In contrast, *Credentify*, a credit platform, also uses NFTs, but only the URIs are in the tokens [62].

6. Discussion

In the following, we discuss our results at both the protocol and application levels [3]. The first section is dedicated to discussing blockchain-based projects at the protocol level. The second section deals with the potential these projects offer at the application level when evaluated in the context of HEI administration requirements divided into three categories: H2H, H2B, and H2S.

6.1. Application scenarios (protocol level)

Before diving into the discussion of the five project groups we

identified, we first provide the categories for classifying blockchain-based projects at the protocol level. Fig. 3 depicts this classification and shows an exemplary placement of the *DCC* project in the classification of blockchain-based projects.

Regarding its *state*, a project can be a prototype, i.e., a solution implemented with a selected set of tools and tested with non-real users. A project that is fully developed and has already been tested with real users is an application. An application may be market-ready if it has accounted for the business model, potential distribution channels, and customers. *The number of blockchains* refers to the number of blockchains used to implement a project. The number varies between a single blockchain and multiple chains. *Infrastructure* refers to access to transactions and can be private, public, or hybrid, whereby hybrid is a combination of private and public. We differentiate between permissioned and permissionless options regarding *access* to transaction validation. For the selection of *concrete blockchain types*, we only include Bitcoin, Ethereum, Hyperledger, and agnosticism which are the state-of-the-art options we encountered in the projects during our analysis.

Regarding the *storage* mechanisms, we distinguish between on-chain and off-chain possibilities. The on-chain way covers projects in which data are stored directly on the blockchain. In off-chain projects, data are stored externally. Lastly, we distinguish between Open Badge, JSON-based, W3C VC Data Model, TRU, and PDF as *formats* of the credentials in the projects.

We start our discussion with the two most prominent project groups—credential verification and record-sharing—and continue with less significant application categories, as introduced in Section 5.

6.1.1. Credential verification

The credential verification projects' main idea is to provide a student with a credential and give him/her the possibility to share this credential with a third party that can verify it. A student can request a credential from his/her HEI, or it can automatically be issued when he/she completes a course or a degree. The solutions *BlockCerts* [44], *Credentify* [62], and *Diplo-Me* [46] offer a wallet where a student can collect, manage, and store his/her credentials. Hence, they support student-centricity and lifelong learning. Credential verification is beneficial for HEI's administrative student support process due to the simplified certificate issuance and verification. Moreover, it may improve the HEI's accreditation by preventing credential falsification.

The checks performed in the projects may include proofs of existence, ownership, and user identity. In this context, proof of exists refers to whether a certification existed at a specific time. The document's hash is calculated and compared to the hash previously put on the blockchain, whereby a timestamp can also be obtained. Proof of ownership stands for the verification of whether a particular actor is the record owner. A multi-signature is widespread, meaning an issuer and a student sign a certificate. The signature decryption allows for the document's validity check. However, the public key associated with the signature may not be linked to any legal, physical entity. To enable proof of identity, i.e., the user's authentication, a CA can perform the initial check and record it in an identity registry for future identity checks. DIDs help realize a decentralized approach.

Some projects offer simple notarization services, considering the first two proofs. *SCVer* [38], *CredenceLedger* [31], *UniChain* [32], *TrueRec* [28], *PoEx* [43], *BlockCerts* [44], and *Sony Global Education* [33] are such solutions. The main shortcoming of *BlockCerts* [44] and other notarization systems based on a public blockchain is that the issuer ID does not guarantee that the URL of the underlying institution is legitimate [69]. In the system, no control mechanism or restriction prevents illegitimate institutions from signing and creating certificates [69]. Thus, the organization (or person) that puts records on the blockchain is responsible for their correctness and integrity. However, the main advantage of a public blockchain is that proof of existence can be executed by consulting the public ledger at any time. Even if the corresponding issuing institution no longer exists, such proof is possible, which is not the case for permissioned private blockchains.

Nevertheless, this permissioned blockchain type, used in *Sony Global Education* [33], *UniChain* [32], and *CredenceLedger* [31], ensures that validators with confirmed identities can check the reliability of participants. Hence, the probability of the documents being authentic increases. Moreover, permissioned blockchains support energy and cost-saving consensus mechanisms, such as PoA, due to the network participants' identifiability.

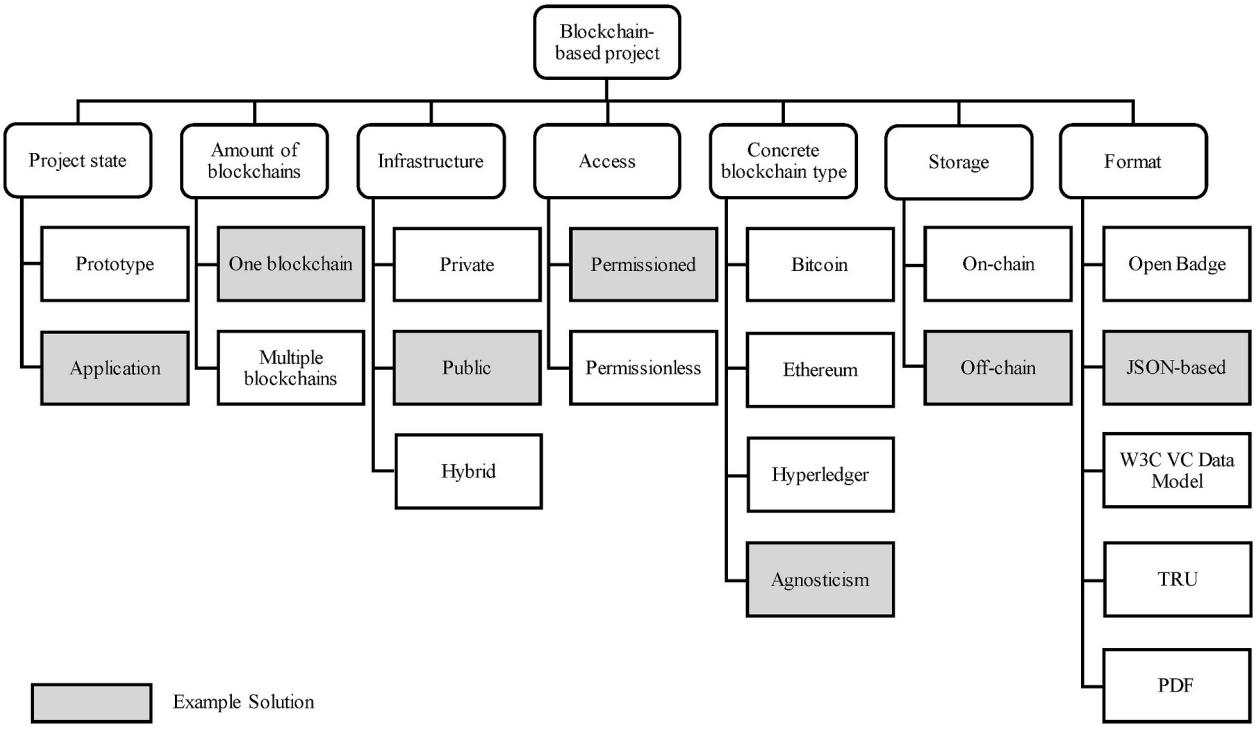

Fig. 3. Classification of blockchain-based projects and exemplary placement of DCC

Permissionless public *BCDiploma* [45], *Gradbase* [42], *OpenCerts* [47], *BTCert* [29], and *Degree Certify* [35] allow for openness and go one step beyond the projects discussed above by including some additional checks. In *Gradbase* [42] and *BTCert* [39], an entity checks student data. A list containing all authenticated issuers is available in *BCDiploma* (their blockchain addresses are on the *BCDiploma* website) [45] and *OpenCerts* (Identity Registry) [47]. In *Degree Certify* [35], a Registration Authority (RA) registers HEIs, and in *OpenCerts* [47], a CA-like organization, SkillsFuture Singapore, does so. However, the main problem with CAs is that all participants should trust them. In contrast to the voting mechanism in which multiple nodes are engaged in the HEI's admission process, as in *EduCTX* [60], a CA may introduce the centralization issue into a decentralized system. Moreover, a CA may represent a single point of failure.

In *Diplo-Me* [46], different CAs are involved, whereby their DIDs can be obtained [52]. The addresses of user wallets are also associated with DIDs [52]. Baldi et al. [70] mentioned a similar solution as potential proof of identity for the *BlockCerts* [44] project. They proposed replacing the Hosted Issuer Profile from the issuer ID with a digital certificate in X.509 format. Such a certificate is generated with the Elliptic Curves compliant with the eIDAS Regulation. It contains the issuer's public key and is issued by a CA. To reduce the centralization caused by the CA, they mentioned the usage of DIDs [70]. Three systems, *DCC* [30], *EduCTX* [60], and *Blockchain 4 Education* [48], consider legally binding user authentication. The *DCC's* developers plan an identity registry to be part of the system to enable student verification by an ID obtained via eIDAS or Shibboleth and issuer verification by DNS names and SSL certificates [41].

Among the credential verification projects, there are outstanding solutions regarding their technical realization: *DRMS* [34] and *BCDiploma* [45]. The system by Guo et al. [34] is the only project that relies on a private and public blockchain combination. Such a combination is different from simple data replication from a private to a public ledger for security purposes present in *EduRSS* [55]. In their system, the private blockchain serves as certificate storage, while the public blockchain makes these certificates (double-signed) accessible to third parties [34]. What is unique about *BCDiploma* is that this application relies on a multi-key algorithm for data encryption, whereby some keys are owned by the HEI and some are owned by the student [51]. This approach supports deleting one of these keys, particularly the persistence key located in the HEI's key storage, to stop further data access [51].

Considering the blockchain types previously described, blockchain-agnosticism, meaning that a wide range of blockchain types is supported, maybe the best choice. When developing a system that is blockchain-agnostic from the beginning, developers can quickly switch between different blockchain types and choose the one that suits their requirements best [71]. Although the initial development process may be complicated, further adoption is significantly simplified, making rapid reactions to changes possible. *BlockCerts* [44] and *DCC* [30] are examples of blockchain-agnostic applications.

When looking at the consensus mechanisms used in the projects, half of the projects still rely on PoW, which is the default for Bitcoin. Regarding data storage, in most projects focusing on credential verification, some information (non-personal or encrypted) is on-chain. Some additional data to enable access to this information or the digital certificate itself are stored off-chain. Therefore, in *BCDiploma*, encrypted information is on the blockchain and the persistence key that enables access to it is in the HEI's "Keystore" [51]. However, in the future, due to advanced quantum machines, encrypted personal data stored on the blockchain may become a vulnerability [72]. In *UniChain*, in contrast, only the document's hash is placed on the blockchain, while the corresponding record is in a local database [32]. In four projects, the databases are local, which introduces a single point of failure. Only three projects rely on decentralized storage, either the IPFS or the cloud. These storage types support the decentralized nature of blockchain technology. The remaining six projects follow the on-chain-only model, meaning that the data are located only on the blockchain. In one prototype, the certificate is on the private blockchain, and its encrypted version is on a public blockchain [34]. Some prototypes consider storing personal information on the blockchain, which can be problematic from the perspective of EU General Data Protection Regulation (GDPR). In contrast, projects in the application state implementing the on-chain-only model place strictly non-personal information on the ledger.

6.1.2. Record-sharing

Record-sharing focuses on the transfer of educational records H2H or H2B. Hence, it may play a role in an HEI administration's internationalization process because it allows for global record exchange with other HEIs.

All projects in this category consider proofs of existence and ownership: most rely on the typical public-private key infrastructure for proof of ownership. An SC or a CA carries out the users' identity verification without being legally binding. In *BOLL*, an SC is responsible for the authentication of students and learning providers [58]. A CA executes university registration in *EduRSS* [55].

Two projects run on a permissioned private blockchain and three on a permissioned public blockchain. As record-sharing projects aim to disclose records to other parties, it may be preferable to implement them with a permissioned public blockchain instead of a permissioned private blockchain to make the records publicly verifiable.

Most projects rely on Ethereum and use SCs for authorization management, automated credentials sharing, and receiver notifications. The main reasons for using this type of blockchain, like the credential verification scenario, are SC deployment and authorization rights management. Hyperledger Fabric, which is used in the project by Liu et al. [56], focusing on credential transfer H2B, also allows for permissions management. Additionally, it enables secured transactions whose protection, compared to the pure H2H exchange, tends to be more critical when transferring data to industry partners. Only two Ethereum-based projects use the default PoW, whereas the remaining two rely on PoS. Ethereum 2.0 plans to switch to PoS due to its efficiency and energy reduction [73].

The data are distributed across off-chain and on-chain storage locations in all Ethereum-based projects, whereby no personal data but only the hash or the URL is on the blockchain, which follows the GDPR. However, all projects still rely on a centralized external database, which is a single point of failure. Nevertheless, the authors of *EduRSS* have already recognized their centralized solution's shortcomings and considered switching to the IPFS [55].

6.1.3. Credit management

Next, we discuss projects targeted at credit management. In contrast to the previous two application scenarios, this scenario does not focus on credentials but credits. This project category may be especially beneficial for HEI internationalization and student support processes. The projects support the Erasmus agreements by simplifying the credits' recognition and improving the students' mobility and portability of their achievements among European HEIs.

All projects in this category address proofs of existence and ownership. In these solutions, there is an association between the tokens and credits. Interestingly, *Credentify*, based on 0xcert, relies on NFTs that can be used in Know Your Customer (KYC) checks [74] that allow for identity verification.

All three projects rely on permissioned public blockchains. However, only one project runs on Ethereum. The two others are being (or were) developed with the platform Ark. Compared to Ethereum; its main advantages include side chains and the default DPoS consensus mechanism. However, the *EduCTX* platform developers decided to switch from Ark to Ethereum, as Ark does not allow the deployment of SCs (M. Turkanović, personal communication, August 12, 2020).

The storage model is known only for the *EduCTX* platform. Like

EduRSS [55], the developers first used an on-chain off-chain model with a local database, realized its shortcomings, and switched to the IPFS (M. Turkanović, personal communication, August 12, 2020).

6.1.4. Reputation management

The reputation management scenario is comparable to the credit management scenario. However, now the focus is on reputation measured in *Kudos* rather than on academic achievements measured in credits. The project by Sharples and Domingue [65] is one of the first blockchain-based projects applicable to education. The second project in this category is a logical continuation of this solution [66]. Both systems may benefit internationalization and student support processes. Moreover, they may support accreditation as they deal with HEI reputation, which may be an additional assessment of an organization.

Although the system by Sharples and Domingue [65] is one of the first blockchain-based education-related projects, it already relies on a permissioned public blockchain. This blockchain type allows third parties to read data on the blockchain but still enables permission control. Both solutions run on Ethereum and, thus, are based on the idea of public verification, an innovative approach compared to other projects developed at that time, such as *BTCert* [29]. The projects use PoS as a consensus mechanism. However, the community''s willingness to participate in the mining activities may be low, as the "only" reward the participants get is the cryptocurrency *Kudos* that may not be externally valuable [66].

In both prototypes, all the data are placed directly on the blockchain, meaning that both projects represent on-chain-only models. Sharples and Domingue [65] saw the blockchain as a system of unified record storage across multiple institutions. Lizcano et al. [66] highlighted that students have their competence history stored on the blockchain, whereby third parties can influence their future employees' training by formulating "standard problems". Although an external database stores these problems, we cannot consider this project an on-chain off-chain model, as the results and *Kudos* are on the ledger.

6.1.5. HEI admission application system

The admission application process by Mori and Miwa [67] is the only project that does not focus on the management of credentials, credits, or reputation. It supports automating student admissions, hence being advantageous for student support processes.

The prototype runs on a permissioned private blockchain, and the authors used Ethereum to deploy SCs [67]. Such a blockchain prevents information leakages, which is essential for storing the data on-chain. Similar to *Credentify* [62], NFTs are used in the system [67]. Since the information is on-chain, it cannot be tampered with without making a block invalid. In *Credentify* [62], modifications of data stored off-chain (behind the URL) are possible without affecting the blockchain.

6.2. Evaluation of potentials (application level)

We now evaluate the potential of blockchain-based projects at the application level based on the HEI administration's requirements. We use the requirements initially introduced in Ref. [22]. We only include representative applications, i.e., projects in the application state (see Section 5.1).

6.2.1. H2H

An *ambidextrous organization* implies that blockchain-based projects can be both—efficient and innovative [75]. We use the combined on-chain off-chain storage constellation to explain when an HEI can be perceived as an ambidextrous organization. An HEI does so by not completely switching to a blockchain-based storage approach but maintaining its data storage with students' credentials.

Suppose that only the document's hash is on the blockchain and that a student is responsible for storing the corresponding file, as in *BlockCerts* [44], and that student deletes the file. In that case, there is no way to obtain it from the hash. When relying on the on-chain off-chain data model in connection with the decentralized IPFS, as in *EduCTX* [76] and *Blockchain 4 Education* [48], the file is usually not just uploaded to the IPFS but previously encrypted with the receiver's public key [77]. However, if the user loses his private key, access to the document may become problematic. Therefore, in the abovementioned cases, the HEI should maintain its certificate storage. With it, the HEI benefits from a project but reduces its adverse effects, although such storage is centralized and may be a single point of failure. In *BCDiploma*, where the records are written directly on the blockchain, the responsibility for the keys is distributed between the HEI and the user [51]. The HEI can perform an intended data erasure by deleting the persistence key [51].

Adaptability—the next requirement—is easy to achieve, as an application has a low entry barrier for universities and offers various adjustment possibilities. HEIs can adapt open-source projects to their needs optimally. An institution can directly adjust the underlying code, as in *DCC* [30] and *BlockCerts* [44]. Other projects, e.g., *EduCTX*, provide detailed, easy-to-follow node setup instructions (M. Turkanović, personal communication, August 12, 2020).

To maintain *stability*, a university administration should consider introducing time-tested solutions that many clients already use or that, at least, have been actively tested. However, it should still seek innovations to stay up with the competition.

Simultaneously, to prevent the 'failure trap', i.e., taking too many risk-intensive actions, the HEI should not start using a blockchain-based application that is very new and whose shortcomings are still unknown. We assume that the only projects in active utilization are *BCDiploma,* with 80 client institutions across Europe [51], and *OpenCerts,* with 16 Singaporean HEIs as clients.

Although identified blockchain-based projects cannot directly address the *balanced power* requirement, solutions that rely on SCs, such as *EduRSS* [55], *BOLL* [58], and *UniChain* [32], allow for effective management of stakeholders' permissions. In *EduRSS*, e.g., an SC is responsible for checking whether the receiving party can access a particular item of data [55]. Moreover, blockchain-based projects are not fully artifactual because real users participate in consensus determination. CAs are also involved in most systems, such as *OpenCerts* [47] and *Blockchain 4 Education* [48].

Regarding *complexity decomposition*, each blockchain-based project consists of smaller parts. Therefore, when looking at the most straightforward proof of existence service—*PoEx* [49], we see that, first, a client uploads a document to the platform; then, its hash is calculated; and, in the last step, it is compared to the hash located on the blockchain. In a more complex application—*BCDiploma*—the cryptographic algorithm is divided into several steps, beginning with consolidating the diploma's URL with its persistence key [51]. An HEI can directly work on these minor problems in code form in open-source projects.

The Flexibility to be offered by a blockchain-based project is strongly connected to an HEI owning a flexible infrastructure. Blockchain-agnostic projects, such as *BlockCerts* [44] and *DCC,* can fulfill this requirement. Their infrastructure is easily adjustable if new blockchain technologies appear.

The only project that considers *accountability* is the reputation management system by Lizcano et al. [66]. In this prototype, a trainer is awarded the reputation cryptocurrency Kudos after successfully training a student. Therefore, Kudos can be considered an accountability measure.

Regarding *staff education*, in most projects, such as *Blockchain 4 Education* [48] and *EduCTX* [60], the staff do not need any blockchain-specific knowledge to upload student certificates to the platform. However, these people may still need an information session on using these systems effectively.

Cost reduction can be achieved by most projects, as they allow for automating credential verification, credential sharing, and credit management. Credit management projects may reduce costs because credits assigned to a student should be checked and recognized manually only

once (W. Prinz, personal communication, August 4, 2020). Thus, if a student goes to another HEI, these credits can be evaluated automatically. The HEI effort and expenditure are lower in credential verification projects, as a third party can rely on an application to automatically verify student credentials.

The project's underlying blockchain technology costs usually depend on the blockchain type, the consensus mechanism, the number of transactions, and the size of each transaction. In most solutions based on Ethereum, there is a fee for each transaction, whereby Ethereum appears in combination with the default PoW, which has many shortcomings [78]. Gas consumption is lower in the case of only SC-based transactions and no inbuilt tokens, as in *OpenCerts* [47]. In Quorum, an enterprise-specific solution like Ethereum, the gas concept still exists, but its price is almost zero. However, only two projects, *Diplo-Me* [52] and *Blockchain 4 Education* [48], are based on this blockchain type. In credential verification projects, the speed of writing data on the blockchain matters less than that of the verification process (W. Prinz, personal communication, August 4, 2020). The transaction size is not an issue, as in many projects, such as *OpenCerts* [47] and *BlockCerts* [44], only documents' hashes are on the blockchain.

In business models related to credential verification applications, preferably the verifier rather than the issuing HEI oversees payment. Therefore, in *BTCert* (D. Galindo, personal communication, August 5, 2020), *EduCTX* (M. Turkanović, personal communication, August 12, 2020), and *Gradbase* [42], the HEI does not pay for issuing credentials, but a third party is charged for verification. Some projects, such as *Diplo-Me* [52], are free to use. Although most business models proposed are beneficial for HEIs, they should still execute a detailed cost-benefit analysis before using a blockchain-based project. They should especially consider the relevant onboarding costs.

Legal regulations are the next requirement. Even though an HEI cannot change the legal basis applicable to a blockchain-based project, it can still use a legally compliant solution. According to M. Turkanović (personal communication, August 12, 2020), compliance with legal requirements is no longer a problem because most blockchain-based projects have already recognized that no personal data should be on the blockchain. This statement refers to the EU GDPR, which a Europe-based HEI should always consider.

Referring to the approaches after Rieger et al. [79], how to create a GDPR-compliant blockchain-based project, four projects follow the pseudo anonymization approach. *Blockchain 4 Education* [48] and (the planned version of) *EduCTX* (M. Turkanović, personal communication, August 12, 2020) store the document's link on the blockchain and the corresponding file in the decentralized IPFS. In projects such as *BlockCerts* [44], the certificate is not stored in a database but is kept directly by the student, whereby its hash is on the blockchain. Such an approach complies with the GDPR. Regulations for the NFTs used in *Credentify* do not yet exist [62,80].

In compliance with the recommendations by Rieger et al. [79], none of the projects, except for *Gradbase* [42], *BCDiploma* [45], and *Diplo-Me* [46], place any personal data on the blockchain. *Gradbase* writes encrypted personal data on the blockchain, which may be problematic in the future due to the increasing potential of quantum computing [42]. *BCDiploma* relies on multilevel encryption based on Shamir's Secret Sharing [51], and *Diplo-Me* offers multiple data protection profiles [52]. In *BCDiploma*, encrypting a file several times with "[…] multiple hashes and multiple encryption methods" allows for overcoming the GDPR problem but tends to be complicated and user-unfriendly (M. Turkanović, personal communication, August 12, 2020). Referring to the *Diplo-Me* data protection profiles [52], the first two correspond with the EU GDPR, as no personal data are on the blockchain. In the third case, compliance is possible if the identity data in the wallet, such as SSI, are GDPR-compliant. Hence, most projects do not place any personal data on the blockchain, and those that do, include additional protection and encryption mechanisms.

The term 'erasure' is still unclear in the context of the "right to be forgotten" [81]. In most projects, such as *BlockCerts* [44] and *OpenCerts* [47], private key destruction is an erasure alternative because the public data encrypted with this key are no longer accessible. Therefore, if a student wants to use the "right to be forgotten" in *BCDiploma*, then, after checking his/her ID, his/her HEI deletes the persistence key from its 'Keystore' [51]. Without this key, the record's decryption is no longer possible [51]. In *Diplo-Me*, the SCs realize this right [52]. The student can deny access to his/her data by activating the function 'Deactivate'. 'Reactivate' is also available. For irreversible denial, there is the function 'Destroy'. The last possibility is to delete the keys required for data access [52].

The permissioned private blockchain recommended by Rieger et al. [79] that projects, such as *Diplo-Me* [46] and *Sony Global Education* [33], run on is beneficial for rectification. In permissionless public enterprise solutions, rectification is realized by setting the corresponding transaction invalid [79]. The transaction itself remains on the ledger. Data rectification in a private blockchain happens by modifying the relevant block and rehashing all of the following [81]. In a public ledger, this process is challenging, as all participants would be considered data controllers. Moreover, it is easier for data controllers to fulfill their communication duties in a private network than in a public network, as only parties with certain permissions can access it.

6.2.2. H2B

Interest diversity is central to the H2B category. Multiple parties with diverse interests engage in all blockchain-based projects. The actors participating in most credential verification and record-sharing solutions are the issuers of the credentials, students, and verifying third parties. Some systems, such as *OpenCerts* [47], may involve an entity responsible for user authentication.

Regarding *stakeholder collaboration*, the interactions of HEIs with external parties are simplified by the credential verification solutions that allow these parties to verify students' achievements without contacting the university. Most record-sharing projects focus on record exchange between HEIs. The collaboration between the universities is also supported if they are part of one blockchain network, as in *EduCTX* [60] and *Blockchain 4 Education* [48]. Credit management projects allow for HEIs' partnerships, as these institutions can easily exchange information about curricula. Moreover, university comparability may increase. The *Blockchain 4 Education* platform [48] can be considered as a result of stakeholder collaboration.

6.2.3. H2S

In the H2S category, *student centricity* is not addressed. Credential verification projects are not unambiguously student-centric, HEI-centric, or third-party-centric, as all parties' needs are satisfied similarly. Students obtain their documents in digital form and can easily share them for verification purposes with third parties. They also benefit from improved mobility. Third parties can quickly verify students' achievements. However, if in a project, a lifelong learning wallet is available to a student, as in *Diplo-Me* [52] and *DCC* [41], this solution is more student-centric. Credential verification should be user-centric, with the user being the owner of the credentials. The record-sharing projects focus on the data exchange between HEIs, so they are HEI-centric. Credit management projects may be HEI-centric or student-centric. These projects simplify the credit recognition process for HEIs and improve the portability and acceptance of academic achievements for students.

The *digital identity* requirement is also part of the H2S category. Identity management is one of blockchain technology's potentials. However, associating a public key with a user's identity in a blockchain system can be ambiguous. To prevent this ambiguity, the user needs an account in addition to his/her blockchain address. The X.509 certificates try to overcome this problem by mapping a public key to a qualified name and are either self-signed or signed by a CA responsible for the identifier uniqueness, whereby CAs can be a single point of failure [82,

83]. In contrast, in combination with DIDs, the SSI is decentralized and allows the data owner to control his/her data [82]. Moreover, the student can disclose a minimum amount of information, and his/her consent is required to use the DID.

The *privacy* requirement is already part of the discussion in H2H, as it is embedded in EU GDPR *legal regulations*.

'No-stop shop', in the context of blockchain-based projects, means that not the student should request a service or a record from a system, but the system should proactively serve them with these items. In the prototype by Badr et al. [36], the student issues a request and defines the receiving institution. In contrast, in *Degree Certify* [35], the credential is issued automatically upon course completion. The issuing institution acts proactively in the enterprise solution *Gradbase* by uploading a spreadsheet with users' degrees [42]. In contrast, in *BTCert*, students apply for certificates [39]. Therefore, there is no clear tendency toward a 'no-stop shop'. However, the applicability of this requirement is also unclear [22].

The *trust* requirement refers to the trust of clients, including students, institutions, and third parties. Compared to systems not relying on blockchain technology, blockchain-based solutions may increase customers trust through the immutable nature of the records stored on the blockchain and data verification by multiple nodes. However, to be fully trusted by the users, a blockchain-based solution should also comply with the EU GDPR to ensure users privacy and data protection. Moreover, it should be easy to be used by all parties. HEIs should receive detailed setup instructions, as in *EduCTX* [60], or projects should offer a high degree of transparency by being open source, as aimed by *DCC* [30]. Students should be able to use the platform or interface without having any blockchain knowledge or creating a blockchain account, which is fulfilled by *Diplo-Me* [46] but not by *PoEx* [43]. Moreover, a short description of the underlying technology provided on the website, as in *Credentify* [62], can be advantageous.

The projects do not address *engagement*. However, the HEI administration can fulfill this by informing employees and students about the blockchain-based application it takes into usage. The information provision can happen via multiple channels, such as a newsletter.

Table 2 concludes the findings and depicts the mapping between the blockchain-based projects and the HEI administration requirements they address.

7. Conclusions, limitations, and future work

We found that projects focusing on credential verification and record-sharing prevailed regarding the application level [3]. These project categories are especially useful for HEI administration's student support and internationalization processes. We obtained equivocal results regarding the projects' technical realization at the protocol level [3]. Permissioned private and permissionless public were the most common blockchain types for credential verification solutions and permissioned private and permissioned public were the most common blockchain types for record-sharing. Ethereum (and Quorum) and agnosticism, combined with PoW, were the prevailing concrete blockchain types in credential verification solutions. The record-sharing projects were based on Ethereum. Most projects relied on the on-chain off-chain storage model, placing the credential's hash (and other non-personal information) on the blockchain and storing the digital certificate off-chain, preferably in a decentralized database, such as the IPFS.

To minimize limitations, we tried to identify as many relevant sources as possible by relying on the backward citation method used by Webster and Watson [25]. However, the search terms used represent one of the shortcomings. Although we were able to cover a wide range of blockchain-based solutions, we did not show any contributions discussing European initiatives. One of them is the European Blockchain Services Infrastructure (EBSI), a blockchain infrastructure that offers cross-border public services. Next, the projects' allocation to the distinct categories was highly subjective. We decided not to assign a project to multiple categories to achieve better readability and a more generic overview.

As blockchain is a rapidly evolving technology, future researchers can extend the overview of blockchain-based projects to be used by higher education administrations with newly developed solutions. They can focus on contributions proposed in scientific databases and governmental documents, e.g., working papers by the Organization for Economic Cooperation and Development, to account for country-specific initiatives, such as EBSI. Future studies may not focus on the education domain in general but on its concrete areas: research, teaching, and administration. Future researchers are encouraged to develop different and more precise classifications of the projects' application scenarios. Moreover, future work can rely on the classification for

Table 2
Mapping of blockchain-based applications to HEI administration requirements.

	BCDiploma	BlockCerts	Blockchain 4 Education	Credentify	Digital Credentials Consortium	Diplo-Me	EduCTX	Gradbase	OpenCerts	PoEx
H2H										
Ambidextrous organization	×	×	×				×			
Adaptability		×			×		×		×	
Stability	×								×	
Balanced power			×			×			×	
Complexity decomposition	×	×	×	×	×	×	×	×	×	×
Flexibility		×			×					
Accountability	Not addressed									
Staff education	Not addressed									
Cost reduction	×	×	×	×	×	×	×	×	×	×
Legal regulations	×	×	×		×	×	×		×	
H2B										
Interest diversity	×	×	×	×	×	×	×	×	×	×
Stakeholder collaboration	×	×	×	×	×	×	×	×	×	×
H2S										
Student centrality		×		×	×	×	×			
Digital identity	×		×	×	×	×				
Privacy	×	×	×		×	×	×		×	
"No-Stop Shop"								×		
Trust				×	×	×	×			
Engagement	Not addressed									

blockchain-based projects we introduced at the protocol level to evaluate a project from a technical perspective.

For practitioners, we recommend relying on the evaluation of projects' potential to identify a project that is highly likely to fulfill their requirements at the application level. In general, we propose to pay more attention to student centricity to support HEIs as a process-oriented organizations. Practitioners are encouraged to allow students to manage their credentials actively and provide them with a legally binding decentralized SSI such that they can be in control of their identities. Blockchain-agnostic open-source projects should be preferred to enable adaptability and flexibility. For a project to be highly likely to be EU GDPR compliant and cost reducing, the type of blockchain used would be the permissioned private blockchain. Additionally, practitioners should aim for consensus mechanisms other than PoW to increase projects' efficiency and sustainability. They should also target the standardization of credentials.

CRediT authorship contribution statement

Matthias Gottlieb: Conceptualization, Methodology, Visualization, Formal analysis, Investigation, Writing – review & editing, Project administration. **Christina Deutsch:** Writing – original draft, preparation, Methodology, Data curation, Formal analysis, Visualization, Investigation, Writing – review & editing. **Felix Hoops:** Investigation, Validation, Writing – review & editing. **Hans Pongratz:** Conceptualization, Writing – review & editing, Funding acquisition. **Helmut Krcmar:** Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

The intention on which this report is based was funded by the German Federal Ministry of Education and Research under the funding code 534800. The responsibility for the content of this publication lies with the authors.

References

[1] T. Barton, C. Müller, C. Seel, Hochschulen in Zeiten der Digitalisierung: Lehre, Forschung und Organisation, Springer, Vieweg Wiesbaden, 2019, https://doi.org/10.1007/978-3-658-26618-9 (In Germany).
[2] H. Gilch, A.S. Beise, R. Krempkow, et al., Digitalisierung der Hochschulen: Ergebnisse einer Schwerpunktstudie für die Expertenkommission Forschung und Innovation. https://www.econstor.eu/handle/10419/194284, 2019 (In Germany).
[3] M. Rossi, C. Mueller-Bloch, J.B. Thatcher, et al., Blockchain research in information systems: current trends and an inclusive future research agenda, J. Assoc. Inf. Syst. Online (2019) 1388–1403, https://doi.org/10.17705/1jais.00571.
[4] ISO, Standards by ISO/TC 307, Blockchain and distributed ledger technologies. https://www.iso.org/committee/6266604/x/catalogue/p/1/u/1/w/0/d/0. (Accessed 15 February 2022).
[5] A.M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, O'Reilly Media Inc., Sebastopol, CA, 2014.
[6] Z. Zheng, S. Xie, H. Dai, et al., An overview of blockchain technology: architecture, consensus, and future trends, in: Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, 2017, pp. 557–564, https://doi.org/10.1109/BigDataCongress.2017.85.
[7] S. Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf, 2008 (Accessed 15 February 2022).
[8] V. Buterin, On public and private blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/, 2015. (Accessed 10 February 2022).
[9] R. Beck, C. Müller-Bloch, J.L. King, Governance in the blockchain economy: a framework and research agenda, J. Assoc. Inf. Syst. Online 19 (10) (2018) 1020–1034, https://doi.org/10.17705/1jais.00518.
[10] S. King, S. Nadal, PPCoin: peer-to-peer crypto-currency with proof-of-stake. https://decred.org/research/king2012.pdf, 2012.
[11] J. Roberto, Understanding proof of stake: the nothing at stake theory. https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027, 2018. (Accessed 16 February 2022).
[12] S. Walters, Delegated proof of stake (DPoS) - total beginners guide. https://www.coinbureau.com/education/delegated-proof-stake-dpos/, 2018. (Accessed 3 February 2022).
[13] A. Vorotnikov, Proof-of-Authority chains. https://github.com/openethereum/wiki/blob/master/Proof-of-Authority-Chains.md. (Accessed 16 December 2021).
[14] Gartner Inc., Hype Cycle for emerging technologies. https://www.gartner.com/en/documents/2809728/hype-cycle-for-emerging-technologies, 2014. (Accessed 13 February 2022).
[15] S. Hulsbomer, Hype Cycles der letzten zehn Jahre: Gartner-Trends im Reality Check. https://www.computerwoche.de/article/2783404/gartner-trends-im-reality-check.html, 2015. (Accessed 13 February 2022).
[16] F. Casino, T.K. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: current status, classification and open issues, Telematics Inf. 36 (2019) 55–81, https://doi.org/10.1016/j.tele.2018.11.006.
[17] A. Alammary, S. Alhazmi, M. Almasri, et al., Blockchain-based applications in education: a systematic review, Appl. Sci. 9 (12) (2019) 2400, https://doi.org/10.3390/app9122400.
[18] G. Chen, B. Xu, M. Lu, et al., Exploring blockchain technology and its potential applications for education, Smart Learn, Environ. Times 5 (1) (2018) 1, https://doi.org/10.1186/s40561-017-0050-x.
[19] T.M. Fernández-Caramés, P. Fraga-Lamas, 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. 9 (21) (2019) 4479, https://doi.org/10.3390/app9214479.
[20] A. Grech, A.F. Camilleri, Blockchain in Education, Publications Office of the European Union, Luxembourg, 2017, https://doi.org/10.2760/60649.
[21] X. Li, P. Jiang, T. Chen, et al., A survey on the security of blockchain systems, Future Generat. Comput. Syst. 107 (2020) 841–853, https://doi.org/10.1016/j.future.2017.08.020.
[22] C. Deutsch, M. Gottlieb, H. Pongratz, Adoption of E-government requirements to higher education institutions regarding the digital transformation, in: N. Edelmann, C. Csáki, S. Hofmann, et al. (Eds.), Electronic Participation, 2021, pp. 90–104, https://doi.org/10.1007/978-3-030-82824-0_8.
[23] J. vom Brocke, A. Simons, B. Niehaves, et al., Reconstructing the giant: on the importance of rigour in documenting the literature search process. Proceedings of the 17th European Conference on Information Systems, ECIS, 2009.
[24] T. Dybå, T. Dingsøyr, Empirical studies of agile software development: a systematic review, Inf. Software Technol. 50 (9–10) (2008) 833–859, https://doi.org/10.1016/j.infsof.2008.01.006.
[25] J. Webster, R.T. Watson, Analyzing the past to prepare for the future: writing a literature review, MIS Q. 26 (2) (2002) (xiii–xxiii).
[26] M.D. Myers, M. Newman, The qualitative interview in IS research: examining the craft, Inf. Organ. 17 (1) (2007) 2–26, https://doi.org/10.1016/j.infoandorg.2006.11.001.
[27] europass, What are digital credentials?. https://europa.eu/europass/en/what-are-digital-credentials. (Accessed 2 February 2022).
[28] B. Boeser, Meet TrueRec by SAP: trusted digital credentials powered by blockchain. https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain/, 2017. (Accessed 10 January 2022).
[29] University of birmingham block chain laboratory, BTCert Web Page (2017). http://www.btcert.org. (Accessed 12 February 2022).
[30] Digital credentials consortium. https://digitalcredentials.mit.edu/. (Accessed 4 January 2022).
[31] R. Arenas, P. Fernandez, CredenceLedger: a permissioned blockchain for verifiable academic credentials, in: Proceedings of the 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), IEEE, 2018, pp. 1–6, https://doi.org/10.1109/ICE.2018.8436324.
[32] E.Y. Daraghmi, Y.A. Daraghmi, S.M. Yuan, UniChain: a design of blockchain-based system for electronic academic records access and permissions management, Appl. Sci. 9 (22) (2019) 4966, https://doi.org/10.3390/app9224966.
[33] Sony Global Education, Creating a trusted experience with blockchain. https://blockchain.sonyged.com/. (Accessed 13 February 2022).
[34] J. Guo, C. Li, G. Zhang, et al., Blockchain-enabled digital rights management for multimedia resources of online education, Multimed. Tool. Appl. 79 (15) (2020) 9735–9755, https://doi.org/10.1007/s11042-019-08059-1.
[35] L.M. Palma, M.A.G. Vigil, F.L. Pereira, et al., Blockchain and smart contracts for higher education registry in Brazil, Int. J. Netw. Manag. 29 (3) (2019) e2061, https://doi.org/10.1002/nem.2061.
[36] A. Badr, L. Rafferty, Q.H. Mahmoud, et al., A permissioned blockchain-based system for verification of academic records, in: Proceedings of the 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), IEEE, 2019, pp. 1–5, https://doi.org/10.1109/NTMS.2019.8763831.
[37] M.J.M. Chowdhury, A. Colman, M.A. Kabir, et al., Blockchain as a notarization service for data sharing with personal data store, in: Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 1330–1335, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00183.
[38] A. Curmi, F. Inguanez, Academic achievement recognition and verification using blockchain, in: U. Schwardmann, C. Boehme, D.B. Heras, et al. (Eds.), Euro-Par 2019: Parallel Processing Workshops, Springer, Cham, 2020, pp. 153–165, https://doi.org/10.1007/978-3-030-48340-1_12.
[39] BlockTechCert/BTCert. https://github.com/BlockTechCert/BTCert, 2017. (Accessed 17 December 2021).

[40] Decentralized identifiers: the easy guide. https://medium.com/metadium/decentralized-identifiers-the-easy-guide-fb96429e8b24, 2019. (Accessed 2 February 2022).
[41] Digital Credentials Consortium, Building the digital credential infrastructure for the future. https://digitalcredentials.mit.edu/docs/white-paper-building-digital-credential-infrastructure-future.pdf. (Accessed 2 February 2022).
[42] Gradbase. https://gradba.se/en/. (Accessed 3 January 2022).
[43] PoEx.io. https://poex.io/. (Accessed 10 February 2022).
[44] BlockCerts. https://www.blockcerts.org/guide/. (Accessed 10 February 2022).
[45] BCdiploma. https://www.bcdiploma.com/. (Accessed 3 January 2022).
[46] Diplo-me. https://www.diplo-me.eu/index.html. (Accessed 3 January 2022).
[47] OpenCerts. https://docs.opencerts.io/v1/. (Accessed 10 January 2022).
[48] W. Gräther, S. Kolvenbach, R. Ruland, et al., Blockchain for education: lifelong learning password, in: Proceedings of 1st ERCIM Blockchain Workshop 2018, European Society for Socially Embedded Technologies (EUSSET), 2018, https://doi.org/10.18420/blockchain2018_07.
[49] Proof of existence. http://docs.proofofexistence.com/#/. (Accessed 10 February 2022).
[50] S. Kolvenbach, R. Ruland, W. Gräther, et al., Blockchain 4 education, in: Proceedings of 16th European Conference on Computer-Supported Cooperative Work - Panels, Posters and Demos, European Society for Socially Embedded Technologies (EUSSET), 2018, https://doi.org/10.18420/ecscw2018_p7.
[51] BCD, BCDiploma. https://github.com/VinceBCD/BCDiploma/blob/master/Whitepapers/BCD-WhitePaper_v2.2.pdf, 2018. (Accessed 10 February 2022).
[52] L. Lantero, P. Marchionni, Diplo-Me (2019). https://www.cimea.it/Upload/Documenti/4083_DIPLOME_WhitePaper_1.5.pdf. (Accessed 10 February 2022).
[53] V. Langard, BCD report #12-May 30th 2020. https://medium.com/bcdiploma/bcd-report-12-may-30th-2020-44959f789025, 2020. (Accessed 13 February 2022).
[54] R. Alva, ARK & BCdiploma—showcasting ARK technology at the university of lille's technical day. https://medium.com/ark-io/ark-bcdiploma-showcasing-ark-technology-at-the-university-of-lilles-technical-day-854d90a537f4, 2020. (Accessed 13 February 2022).
[55] H. Li, D. Han, EduRSS: a blockchain-based educational records secure storage and sharing scheme, IEEE Access 7 (2019) 179273–179289, https://doi.org/10.1109/ACCESS.2019.2956157.
[56] Q. Liu, Q. Guan, X. Yang, et al., Education-industry cooperative system based on blockchain. Proceedings of the 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), IEEE, 2018, pp. 207–211, https://doi.org/10.1109/HOTICN.2018.8606036.
[57] A. Alkouz, A. HaiYasien, A. Alarabeyyat, et al., EPPR: using blockchain for sharing educational records. Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT), IEEE, 2019, pp. 234–239, https://doi.org/10.1109/ITT48889.2019.9075126.
[58] P. Ocheja, B. Flanagan, H. Ueda, et al., Managing lifelong learning records through blockchain, Res. Pract. Technol. Enhanc. Learn. (RPTEL) 14 (1) (2019) 4, https://doi.org/10.1186/s41039-019-0097-0.
[59] M. Han, Z. Li, J.S. He, et al., A novel blockchain-based education records verification solution. Proceedings of the 19th Annual SIG Conference on Information Technology Education, ACM, 2018, pp. 178–183, https://doi.org/10.1145/3241815.3241870.
[60] M. Turkanović, M. Hölbl, K. Košič, et al., EduCTX: a blockchain-based higher education credit platform, IEEE Access 6 (2018) 5112–5127, https://doi.org/10.1109/ACCESS.2018.2789929.
[61] A. Srivastava, P. Bhattacharya, A. Singh, et al., A distributed credit transfer educational framework based on blockchain. Proceedings of the 2018 Second International Conference on Advances in Computing, Control and Communication Technology (IAC3T), IEEE, 2018, pp. 54–59, https://doi.org/10.1109/IAC3T.2018.8674023.
[62] Credentify, Introducing flexible equity in European education. https://credentify.eu/. (Accessed 4 January 2022).
[63] European Commission, European credit transfer and accumulation system (ECTS). https://ec.europa.eu/education/resources-and-tools/european-credit-transfer-and-accumulation-system-ects_en. (Accessed 3 February 2022).
[64] 0xcert. https://docs.0xcert.org/. (Accessed 3 February 2022).
[65] M. Sharples, J. Domingue, The blockchain and kudos: a distributed system for educational record, reputation and reward, in: K. Verbert, M. Sharples, T. Klobučar (Eds.), Adaptive and Adaptable Learning, Springer, Cham, 2016, pp. 490–496, https://doi.org/10.1007/978-3-319-45153-4_48.
[66] D. Lizcano, J.A. Lara, B. White, et al., Blockchain-based approach to create a model of trust in open and ubiquitous higher education, J. Comput. High Educ. 32 (1) (2020) 109–134, https://doi.org/10.1007/s12528-019-09209-y.
[67] K. Mori, H. Miwa, Digital university admission application system with study documents using smart contracts on blockchain, in: L. Barolli, H. Nishino, H. Miwa (Eds.), Advances in Intelligent Networking and Collaborative Systems, Springer, Cham, 2019, pp. 172–180, https://doi.org/10.1007/978-3-030-29035-1_17.
[68] Reasons why you should invest in non-fungible tokens (NFTs). https://medium.com/ovrthereality/reasons-why-you-should-invest-in-non-fungibletokens-nfts-594cec7f4ff2, 2020. (Accessed 13 February 2022).
[69] N. Smolenski, Top 10 reasons to use blockcerts. https://medium.com/learningmachine-blog/top-10-reasons-to-use-blockcerts-ec7d29f2712c, 2018. (Accessed 16 February 2022).
[70] M. Baldi, F. Chiaraluce, M. Kodra, et al., Security Analysis of a Blockchain-Based Protocol for the Certification of Academic Credentials, arXiv, 2019 preprint. arXiv:1910.04622.
[71] K. Pfluger, Why choose a single blockchain when you can be blockchain agnostic?. https://medium.com/crowd-machine/why-choose-a-single-blockchain-when-you-can-be-blockchain-agnostic-98f524b58945, 2018. (Accessed 13 February 2022).
[72] A.K. Fedorov, E.O. Kiktenko, A.I. Lvovsky, Quantum computers put blockchain security at risk, Nature 563 (7732) (2018) 465–467, https://doi.org/10.1038/d41586-018-07449-z.
[73] Ethereum 2.0 (Eth2). https://ethereum.org/en/eth2/, 2020. (Accessed 7 January 2022).
[74] 0xcert, Highlights of 0xcert public pre-sale. https://0xcert.org/news/public-pre sale-highlights/, 2018. (Accessed 10 December 2021).
[75] J. Magnusson, D. Koutsikouri, T. Päivärinta, Efficiency creep and shadow innovation: enacting ambidextrous IT Governance in the public sector, Eur. J. Inf. Syst. 29 (4) (2020) 329–349, https://doi.org/10.1080/0960085x.2020.1740617.
[76] EduCTX. http://www.eductx.org/. (Accessed 15 December 2021).
[77] Coral health, Learn to securely share files on the blockchain with IPFS. https://medium.com/@mycoralhealth/learn-to-securely-share-files-on-the-blockchainwith-ipfs-219ee47df54c. (Accessed 10 February 2022).
[78] M. Zochowski, Why proof-of-work is not viable in the long-term. https://medium.com/logos-network/why-proof-of-work-is-not-viable-in-the-long-term-dd96d2775e99, 2019. (Accessed 16 January 2022).
[79] A. Rieger, F. Guggenmos, J. Lockl, et al., Building a blockchain application that complies with the EU general data protection regulation, MIS Q. Exec. 18 (4) (2019) 263–279, https://doi.org/10.17705/2msqe.00020.
[80] IURICORN, Non-fungible tokens from a legal perspective. https://www.iuricorn.com/non-fungible-tokens-from-a-legal-perspective/, 2019. (Accessed 13 February 2022).
[81] European Commission, Rules for business and organisations. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en. (Accessed 2 February 2022).
[82] G. Fedrecheski, J.M. Rabaey, L.C.P. Costa, et al., Self-sovereign identity for IoT environments: a perspective. Proceedings of the 2020 Global Internet of Things Summit (GIoTS), IEEE, 2020, pp. 1–6, https://doi.org/10.1109/GIOTS49054.2020.9119664.
[83] Oracle. X.509 certificates and certificate revocation lists (CRLs). https://docs.oracle.com/javase/8/docs/technotes/guides/security/cert3.html. (Accessed 2 February 2022).