Ocheja *et al. Research and Practice in Technology Enhanced Learning* (2019) 14:4
https://doi.org/10.1186/s41039-019-0097-0

Research and Practice in Technology Enhanced Learning

RESEARCH Open Access

# Managing lifelong learning records through blockchain

Patrick Ocheja[1*], Brendan Flanagan[2], Hiroshi Ueda[2] and Hiroaki Ogata[2]

*Correspondence:
ocheja.ileanwa.65s@st.kyoto-u.ac.jp
[1]Graduate School of Informatics, Kyoto University, 36-1 Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501, Japan
Full list of author information is available at the end of the article

**Abstract**

It is a common practice to issue a summary of a learner's learning achievements in form of a transcript or certificate. However, detailed information on the depth of learning and how learning or teachings were conducted is not present in the transcript of scores. This work presents the first practical implementation of a new platform for keeping track of learning achievements beyond transcripts and certificates. This is achieved by maintaining digital hashes of learning activities and managing access rights through the use of smart contracts on the blockchain. The blockchain of learning logs (BOLL) is a platform that enable learners to move their learning records from one institution to another in a secure and verifiable format. This primarily solves the cold-start problem faced by learning data analytic platforms when trying to offer personalized experience to new learners. BOLL enables existing learning data analytic platforms to access the learning logs from other institutions with the permission of the learners and/or institution who originally have ownership of the logs. The main contribution of this paper is to investigate how learning records could be connected across institutions using BOLL. We present an overview of how the implementation has been carried out, discuss resource requirements, and compare the advantages BOLL has over other similar tools.

**Keywords:** Learning logs, Learning analytics, Blockchain, Privacy, Higher education, k-12, Lifelong learning

## Introduction

Big data has revolutionized many areas of business ranging from search companies to e-commerce, where insights from data have driven personalization, targeted advertising, improved services, and overall business growth. However, similar success has not yet been achieved in the field of education technology, and the use of data-driven education in the field is still lagging behind (Siemens and Long 2011). One of the key challenges in this area is the lack of data continuity. When students change from one institution to another, their learning data remains largely immobile, such as the usual progression from elementary, junior-high, and high school. As institutes maintain separate Learning Record Stores (LRSs) which are not connected to one another, this results in the learning data that was collected at previous institutes not being available for analysis at current or future institutes. The situation causes a typical *cold-start problem*, where the current institution's learning environment does not have sufficient data for effective personalization or adaptation when the learner is first enrolled. In this paper, we propose a solution that enables

the logical movement of learning records using a blockchain as a transport medium and platform for connecting LRSs. In particular, the following problems are addressed by the proposed solution:

- Distributed learning logs across multiple institutions caused by the use of independent disconnected LRSs.
- Inability to transfer or access a learner's data and testimonials across multiple institutions, making it difficult to achieve lifelong learning logging.
- The lack of protection and control of private information by data owners.

Solutions to these problems is integral to the further development of the learning analytics, learning personalization, and learning enhancement. A main motivation of this research is to develop lifelong learning logs for learners. A lifelong learning log typically contain verifiable proves of all the learning activities carried out by a learner (Ogata et al. 2011). As learning is a continuous and an ongoing process, (Ogata et al. 2011) proposed a lifelong learning log as a personal and private journal for documenting learning activities. In this work, we present an implementation where such a journal is recorded as a secure entry on the blockchain. The authenticity of the journal can also be verified easily by consensus using the data stored as blocks within the blockchain and could be used in assessing a person's educational achievement, suitability for employment, and intellectual evaluation. We are particularly interested in using the blockchain to solve this problem because it provides a mechanism for the following:

- Distributed consensus, data consistency, and immutability of processed transactions. These features can make it nearly impossible to alter learning records on the network (Nakamoto 2008).
- Defining clauses or contracts on the blockchain that determine how learning record data transactions are handled and protected.
- Facilitating interaction between multiple stakeholders (institutions, students, third parties) with high transparency and protection of each participant's interest as agreed in defined contracts.

It is also important to protect private information while enabling lifelong learning logs. A key aspect in learning analytics is the control of personal and private information by an individual. This includes the ability to opt out of learning activity tracking and giving parents of underaged learners the right to manage their dependents' learning records (ISO/IEC JTC 1/SC 36 2016; Pardo and Siemens 2014; Rubel and Jones 2016). Usage or access to a learner's learning records should be sought from the learner and/or their institution depending on the terms of agreement between both parties or according to other defined policies. This agreement should contain clauses such as usage policies, access authorization, and storage policies. Our proposed solution is to facilitate these agreements on the blockchain by allowing the learner and their institutions to act as signatories on defined smart contracts and enable the protection of learning records on the blockchain.

Although different institutions utilize different learning platforms, some standards have been proposed for enabling learning records from one institution's learning platform to be correctly interpreted on another institution's platform (Advanced Distributed Learning

2016; IMS Global Learning Consortium 2013). These standards along with those proposed by Ocheja et al. (2018) were used in this paper to implement a system for connecting learning records generated at different institutions on a single public ledger.

In the next section, we will discuss previous research works on connecting academic records and enabling access to educational information beyond a single institution. We will show how such work differs from our proposed system: blockchain of learning logs (BOLL). This will be followed by a detailed explanation of the design of BOLL, how it solves the problem of disconnected learning records, and how privacy and access control policies are enforced. Results obtained from experimenting with this implementation will also be provided. In the final section, we will discuss key discoveries, challenges, and potential directions for future research.

## Related work

There has been previous research into the sharing and verification of academic records, such as digital certificates and transcripts (The Mozilla Foundation 2012; Schmidt 2016). (IMS Global Learning Consortium 2017) developed a Comprehensive Learner Record (IMS CLR) to capture and communicate a learner's achievements in verifiable digital form. In particular, it supports traditional academic programs, co-curricular, and competency-based education. IMS CLR contains data such as courses, competencies, employability skills, degrees, and certificates. While IMS CLR contains more details than the usual transcripts or certificates, it does not provide digital logs of behaviors and activities performed during learning. The granularity of data provided in IMS CLR is still at a high level and does not allow a decentralized implementation for the privacy and access of learning records.

Blockchain technology has been applied to various fields to enable decentralized access and control, such as health (Azaria et al. 2016), finance (Nakamoto 2008), and other sectors as reviewed by Crosby et al. (2016). Educational institutions and learning organizations have also found innovative ways to use the blockchain technology to control access and sharing of various assets and resources as reviewed by (Chen et al. 2018; Bracamonte and Okada 2017; Sharples and Domingue 2016; Grech and Camilleri 2017). While at the time of writing, there were few applications within the field and there are many potential aspects of the education sector in which blockchain can be used, such as *multi-step accreditation, recognition and transfer of credits, rewarding use and re-use of an intellectual property, and students funding and payments on the blockchain* (Grech and Camilleri 2017).

### Brief introduction to blockchain

A blockchain is a decentralized and distributed peer-to-peer network which has a single immutable public ledger containing all transactions performed by participants on the network. Each participant is uniquely identified by a pair of public-private key. A public key can be used for public identification while the private key is required for authorizing transactions sent by the owner. The owner of a private key can also use it to claim an asset that has been encrypted with their public key. A transaction typically includes the sender's public key, a data field, and the hash of the preceding transaction. The data field makes it possible for the blockchain to store various digital assets in a transaction, such as certificates, property rights, licenses, etc.

To ensure the integrity of the entire network in a public blockchain, all participants engage in solving a cryptographic puzzle before a transaction is processed. A solution to a puzzle is the first correct solution submitted and only when the solution is accepted by more than 50% of the participants on the network. This effectively replaces the need for a third party mediation as each participant also has a copy of all transactions on the network and can query the validity of any transaction. Consequently, it becomes possible to ensure decentralization, offer transparency, and engender trust.

It is important to note that apart from the public blockchain where anyone can join the network and all parties have equal voting rights, we can also have a private blockchain or a consortium blockchain. In a private blockchain, access is restricted within the group and the rules of the network are often determined by the convener. Whereas in a consortium blockchain, access is restricted within the group but everyone in the group has equal voting rights and decisions are made by consensus.

While previous research works (Back 2002; Szabo 1997) play a fundamental role in the current implementation of the blockchain, the first concrete implementation was proposed by Satoshi Nakamoto (Nakamoto 2008) as Bitcoin, a peer-to-peer electronic cash system. The emergence of other blockchain implementations, such as Ethereum (Buterin and et al. 2013) and Hyperledger (Cachin 2016) have led to further development of decentralized applications (DApps) in various non-financial sectors including healthcare (Azaria et al. 2016), and more recently, education (University of Nicosia 2014; Ocheja et al. 2018; Sony Global Education 2017; Schmidt 2016).

The Ethereum blockchain supports DApps by allowing the definition, deployment, and execution of smart contracts. A smart contract is a cryptographic "box" which is only unlocked when the conditions defined within the box are met (Buterin and et al. 2013). (Szabo 1997) noted that the basic idea behind smart contracts is to make it possible to embed into hardware or software different kinds of contractual clauses, including collateral, bonding, delineation of property rights, etc. It is implemented in such a way that it will make a malicious breach of contract expensive. In this work, we use the Ethereum blockchain and learning logs smart contracts to realize and ensure privacy and security of lifelong learning logs by implementing the BOLL system.

### Blockchain in education

In Table 1, a list of some applications of blockchain technology in the education sector are shown. Schmidt (2016) proposed Blockcerts, originally from Open Badge (The

**Table 1** Features of current applications of blockchain in education

| Application | Blockchain type | Record type | Actual data stored | Verification | Access to records |
|---|---|---|---|---|---|
| Blockcerts | Bitcoin | Certificates | Hash of certificates | Open | Off-blockchain authorization |
| UNIC | Bitcoin | Certificates on MOOC | Grouped hash of certificates | Open | Off-blockchain authorization |
| SGE | Hyperledger | Academic records | N/A | N/A | N/A |
| Proposed system | Any Turing-complete blockchain | Academic records and permissions | Hash of academic records | Open | On-blockchain authorization |

Mozilla Foundation 2012), as an open standard for creating, issuing, viewing, and verifying blockchain-based certificates. Cryptographic hashes of these certificates are stored on the blockchain where they are protected from malicious alteration and unauthorized access. However, the granularity of learning process is important for learning analytics and achieving data-driven education. As certificates are mainly a representation of accomplishments and do not express the process of learning, our proposed system considers not only certificates, but also fine grain learning log data.

Another project by the University of Nicosia (UNIC) (University of Nicosia 2014) looks at also placing academic certificates of its students on the blockchain. While this is similar to Blockcerts, UNIC operates from a more specific angle of single institution use case, and the certificates are for courses taken on its massive open online course (MOOC) platform. Another difference between Blockcerts and UNIC's implementation is that the former stores hashes of certificates distinctly, while the latter groups reference to certificates for students in a particular course term and store the hash of the grouped references on the blockchain. Although the approach of grouping certificates together may be advantageous for storage optimization, it might become a limitation for access and privacy where a single cryptographic hash points to multiple students' certificates. Our proposed system solves this particular limitation of UNIC by completely storing learning records distinctly and allowing third party tools to determine the relationships between learning logs.

Blockcerts and UNIC's MOOC platform provide open mechanisms for verifying educational records stored on the blockchain. However, these applications are yet to provide a way to manage permissions to these records on the blockchain. On Blockcerts and UNIC's MOOC platform, permissions that define access to educational records are being managed outside the blockchain. This method of managing permissions to data is referred to as "off-blockchain authorization." In contrast, BOLL provides an on-blockchain authorization where permissions to educational records can also be managed on the blockchain by the definition and use of smart contracts.

Other reviews on the applications of blockchain technology in academic institutions (Bracamonte and Okada 2017; Sharples and Domingue 2016; Chen et al. 2018) have reported on the proposed use of blockchain to give incentives in the form of tokens for peer-review ("ReviewCoin"), an "educational reputation currency" for academic achievements ("Kudos"), and a cryptocurrency for good academic performance. These systems focus on managing learning achievements on the blockchain, whereas our proposed system lays emphasis on using the blockchain to achieve lifelong learning records by connecting granular learning activities and not just learning achievements.

Sony Corporation and Sony Global Education (Sony Global Education 2017) published a press statement about a system already developed to apply blockchain technology - IBM Blockchain powered by Hyperledger Fabric 1.0, to the field of education. This system is said to have two core functions; authenticate and control usage rights of educational data and an application programming interface for handling these rights aimed at educational institutions. While the goals of the ideas expressed in the press release are similar to ours, Sony Global Education is yet to publish any technical document on the implementation or usage specification of this system. To the best of our knowledge, Ocheja et al. (2018) are the first to provide a technical specification on the application of blockchain technology to educational records different from certificates.

In this work, our key contribution is to provide a concrete implementation of a blockchain-based platform for learning logs based on previous research by (Ocheja et al. 2018). We show that it is possible to achieve a privacy-preserving lifelong learning log using the blockchain with defined smart contracts, discuss resource requirements, and the benefits of our proposed system. We also discuss potential challenges that may be faced and provide solutions on how such issues could be tackled.

## Methodology

In carrying out this research, we adopted the design-based research (DBR) methodology (Wang and Hannafin 2005). Wang and Hannafin (2005) defined DBR as a research method which focuses on exploring systematic but flexible techniques targeted at improving educational practices through iterative analysis, design, development, and implementation requiring collaboration between researchers and practitioners and leading to new useful principles. The idea of iterative analysis as applied in DBR helps to validate design decisions. In the event that a design approach fails in the validation phase with real-world practitioners, another cycle of iteration can consider alternative techniques. Such a repetitive task makes it possible to arrive at a more feasible implementation that meet the needs of the end-users.

In the design of our proposed system, we first conducted a literature review on previous works that have attempted to enable lifelong learning logs. Specifically, we used the framework proposed by Ocheja et al. (2018) as a guide in deciding how functionalities on our proposed system are different from other systems. We also considered the different stakeholders that are involved in managing and accessing learning records, such as learners, teachers, administrators, researchers, and other third parties so as to ensure that our system caters for their needs. This was carried out by observing current processes and concerns in academic institutions involving these stakeholders, such as privacy, security, accessibility, availability, and consistency of learning records.

Consequently, we developed smart contracts that reflect how learning records are generated and how access to them is controlled and managed. As learning records are categorized by action words or verbs from which they resulted from (IMS Global Learning Consortium 2013; Advanced Distributed Learning 2016), we adopted an action verb-based method of storing and managing privacy of learning records on our proposed system. In this case, learning records of the same action verb for a particular learner, are written to the same smart contract on our proposed system alongside their permissions.

We validated our design by using data from learning tools in our institute's production environment. These data contain information about learners' activities on the learning tools including quiz, read, assignments, view, and other events. To validate our design using this data, we developed scripts that simulate the creation of these learning events. The output of each simulated event is then written to our proposed system. This simulation approach of validating our design is useful in this work as most features of our proposed system can be programmatically triggered.

## System design

We propose a blockchain of learning logs (BOLL): a blockchain platform that connects the learning logs of students across the different institutions they have attended on a single,

public, and immutable ledger. We present BOLL as a solution to the problem of transferring educational data between different institutions as students move from one institution to another. It also solves the cold-start problem in learning analytics systems where a new students' learning environment is created without being informed by previous learning activities, even though their current learning activity is based on experiences at their previous school. Previous learning data could serve as a robust foundation upon which new learning environments are created when a learner enrolls in a new institute. (Ocheja et al. 2018) identified key features of the blockchain that makes this implementation possible. These include decentralization, single public ledger, privacy, immutability, and the deployment of smart contracts. We build on these key features to enable connected learning logs across different institutions, defined smart contracts to regulate access, and implement mechanisms to classify learning logs to also enable easy indexing and quick look-up times.

In the following subsections, we will discuss the components of the BOLL system. These components form the major requirements for realizing a design that facilitates connected learning logs on the blockchain. They include at least one fully functional blockchain node, an LRS, and a set of smart contracts installed on the blockchain node. A fully functional blockchain node is a node that is able to mine transactions. In addition, an institution can setup multiple miner nodes or miner threads in their production environment in a distributed way to facilitate mining speed.

### BOLL system

Currently, various institutions and learning platforms store and manage their learning records separately with no standard method to move learning records from one platform to another without duplicating user information as shown in Fig. 1. In Fig. 2, we propose a change from current implementations of learning management systems and platforms to a blockchain of learning logs where all learning institutions can co-exist on a single public ledger. This can be facilitated by using the proposed BOLL system and policies defined by smart contracts. Institutions that take part in the BOLL system can agree to

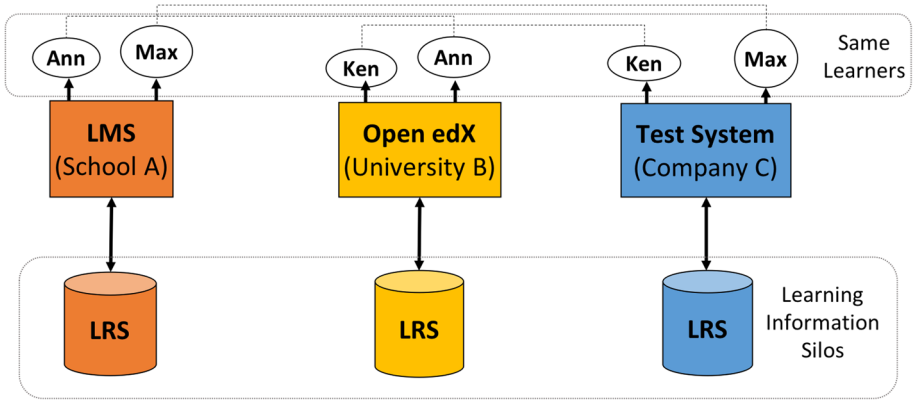


**Fig. 1** Current learning systems design. This shows an example of the current design of most learning systems where learning management systems are separately managed. Consequently, user data are largely non-transferable across these learning systems even when the users want to

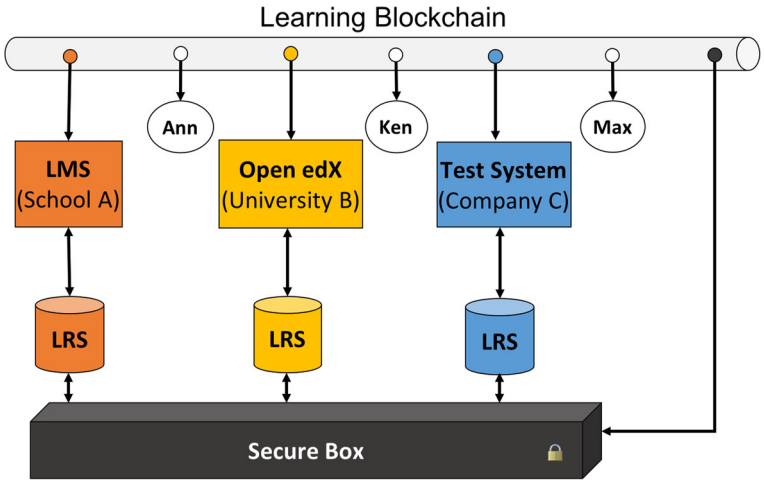


**Fig. 2** Proposed design of blockchain of learning logs (BOLL). Our proposed idea of how learning systems should be designed to enable the ability for learners to conveniently and efficiently manage their lifelong learning logs. With one identifier across multiple learning systems, the BOLL system can be used to connect learning records across different institutions

allow students access to their learning records while at other institutions, and can state the conditions for such access on the blockchain. The proposed system also solves the problem of different user accounts at multiple institutions by linking a single BOLL user identity to all LRSs within the network.

We also use the nested transactions feature of the blockchain where the contents of blocks represent pointers to learning data with ownership and access policies. Nodes on the peer-to-peer network represent learning providers. Learning activities performed by learners on the learning platforms of learning providers on the network are logged on the blockchain as string representations of queries that can be executed on the LRSs of learning providers to retrieve such activities. To ensure data consistency and immutability, at transaction initiation time, we execute accompanying queries on the LRS and include a cryptographic hash of the obtained result as part of the block information. Future response from the execution of this query can be compared to the stored hash and if different, the response is invalid and rejected. We propose a secure box for executing these queries against a providers' LRSs with reference to the blockchain network to maintain established permissions.

Figure 3 shows a typical setup of our implementation for one institution. We use an open-source learning management system (LMS), Moodle (Moodle 2001) and a digital book reader, BookRoll (Flanagan and Ogata 2017), as the learning tools. All learning records emitted from these tools through learning activities of learners are stored in a central database, MongoDB: a document-oriented database, through Open Learning Record Warehouse (OpenLRW) which is an open-source LRS (Apereo 2016). These learning records are either in conformance with the xAPI standard (Advanced Distributed Learning 2016) or IMS Caliper standard (IMS Global Learning Consortium 2013). We also provide an implementation of a subroutine for retrieving records from the MongoDB through a wrapper method on OpenLRW and writing them to the blockchain. For this implementation, we used the open-source Ethereum blockchain written in Go programming language (Ethereum 2013a).

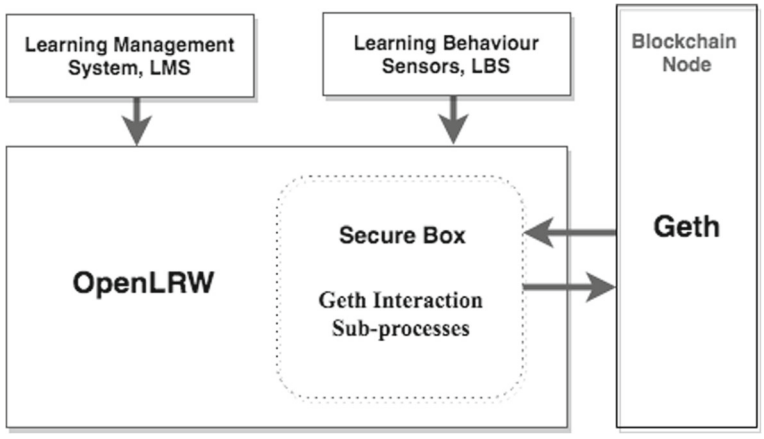


**Fig. 3** BOLL architecture—one institution. To enable the use of BOLL at an institution, it is required to have a learning management system or learning behaviour sensors, a learning record store, a secure box, and a blockchain node. This figure shows these key requirements and how they are interfaced

### System access and privacy control

The BOLL system enforces smart contracts that contain learning data access permissions, ownership, and a mapping between the permissions and ownership. The state transition functions of these smart contracts can be modified to reflect the conditions that should be met before data read or write access is granted. Figure 4 shows a hypothetical hierarchical design of these smart contracts. We define three main smart contracts, namely, registrar-learning provider contract (RLPC), learner-learning provider contract (LLPC), and index contract (IC) for both providers and learners.

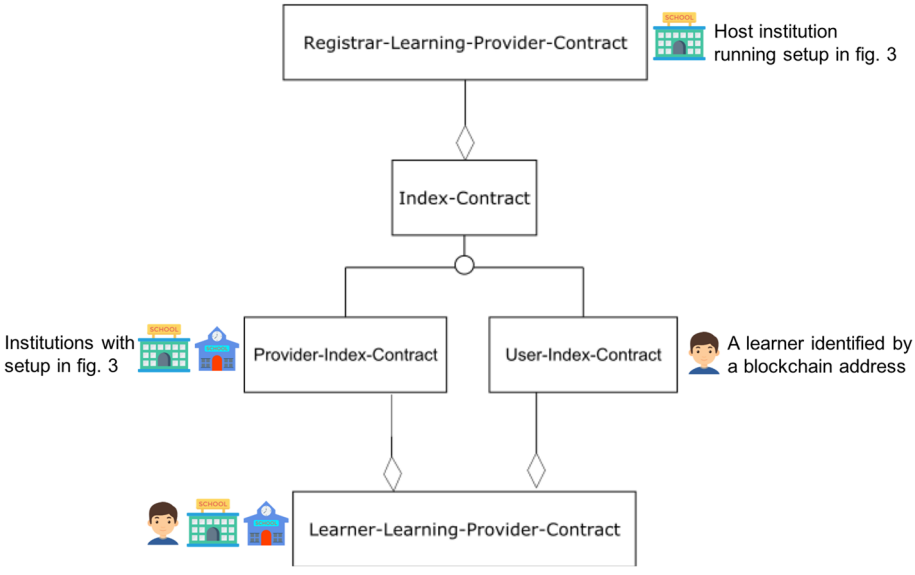


**Fig. 4** Hierarchical view of BOLL system smart contracts. This figure shows the top-level design of the BOLL system's smart contracts. The smart contracts control how institutions join the blockchain, how learning records are written, indexed, or accessed. The smart contracts also contain information on how permissions can be granted at various levels

The RLPC controls how students, teachers, organizations, and institutions become authorized learners or learning providers on the learning blockchain. For institutions and organizations, these requirements are often administratively decided. Hence, we propose that typical implementations should consider existing structures for establishing communication and accessing information in institutions and organizations. In our implementation, we maintain a registry of institutions that are allowed to join the BOLL system's network using the institution's domain name and an encrypted message signed with their private key and then verified with their public key. In Table 2, we describe some of the attributes/functions defined in the RLPC.

An index contract is also installed to provide a mechanism for fast look-up of entries and access permissions on BOLL. This unique design solves the current limitation of Solidity (Ethereum 2013b), which is a smart contract programming language that does not provide a look-up interface for data types. Although, arrays and hash table-like data types are provided, the cost of looking up an entry in an array computationally grows with the size of the array. On the other hand, the hash table-like implementation does not provide an interface for accessing the keys to the values in the hash table. This means that, to look up any entry in the hash table, we should have the key stored elsewhere. In our case, to look up a learning event, we should have a pointer to that learning event. Thus, it is necessary to develop a mechanism for storing the pointers or keys to the learning events, otherwise we risk losing information written on the blockchain. In Tables 3 and 4, we define the internal contents of the provider index contract (PIC) and the user index contract (UIC) respectively. The PIC is for learning providers while the UIC is peculiar to learners. We use a hash table-like implementation for keeping a list that maps learners to their LLPCs, and another list that maps learning providers to LLPCs they have with learners and with other learning providers that learners have granted access.

The LLPC represents a proof of existence of a learner's learning data on a learning provider's platform. This smart contract is dedicated specifically to handling a learner's learning record and how it is accessed. We decided to use a specific smart contract for this purpose so as to make it easy to transfer learning records from one institution to another. With our design, a transfer can easily be done by invoking the *grantAccess* function (with permission from the owner or their institution) on the LLPC without erasing or physically dislodging the learning record. The LLPC contains information such as the blockchain address of the owner, the URL of the originating learning provider's LRS with a hashed id parameter for retrieving the original record, a hash of expected learning data for ensuring data has not been tampered with, and a key-value pair of institution's address and their access permissions (read, write, grant-read, grant-write, none).

The address refers to a hexadecimal string uniquely generated and having corresponding private and public keys. A learner can have as many LLPCs as the number of distinct

**Table 2** Registrar-learning provider contract (RLPC)

| Attribute | Description |
|---|---|
| Owner | Address of starting institution |
| Registered participants | Addresses of participants mapped to their index contract |
| Register | A function for registering new users |
| Unregister | Deactivates a user |
| Assign index contract | Assigns an index contract to a user |

**Table 3** Provider index contract (PIC)

| Attribute | Description |
|---|---|
| Owner | Address of institution |
| Learners to learning records | A mapping of learners' address to their LLPCs |
| Learners | A list of all learners at this institution |
| Insert learning records | Inserts a new LLPC |
| Get learning records | Retrieves a learner's learning records |

types of learning events carried out. These events could be any of the xAPI or IMS Caliper action verbs (IMS Global Learning Consortium 2017; Advanced Distributed Learning 2016). Also, an institution may request access to read a student's learning logs contained in an LLPC contract by invoking the *requestAccess* function in the LLPC smart contract. Other invocable functions on the LLPC smart contract as shown in Table 5 include *insertLearningEvent*, *grantAccess*, and *revokeAccess* which respectively insert learning event and grant or revoke access to a learning record.

#### BOLL processes

A BOLL system setup consists of at least one institution as shown in Fig. 3 to serve as host. BOLL has two main user groups: institutions and teachers/learners/students. We will now discuss the required steps in setting up a BOLL. In Fig. 5, we make a list of processes, actors, and the necessary smart contracts with the required operations to be performed. The RLPC is first installed on the blockchain node serving as the host. One institution should volunteer to serve as the host node. With this, all institutions that wish to join the blockchain will have to request to be registered by having a similar setup as in Fig. 3, and then sending a registration request to the RLPC which was initially installed on the hosting institution's blockchain node. Upon approval, the RLPC is updated with their information and a PIC is created. Learners that opt to have their learning records on the blockchain will have to go through the account setup process. This process handles the generation of blockchain address for the learner, creation of an index contract (UIC), and the final phase of registering the generated blockchain address and UIC address in the RLPC.

On the blockchain, learning records are uniquely grouped using the action verb field and the user's blockchain address. Writing learning histories involves performing at least one transaction on the blockchain. The process begins with retrieving the action verb of the learning record and converting it to a corresponding hexadecimal number. This is required as we want to optimize gas usage on the blockchain. Gas as used here refers to the computational cost for processing transactions on the blockchain. The amount of gas

**Table 4** User index contract (UIC)

| Attribute | Description |
|---|---|
| Owner | Address of learner |
| Providers to learning records | A mapping of providers' address to learner's LLPCs |
| Providers | A list of a learner's learning providers |
| Insert learning records | Inserts a new LLPC |
| Get learning records by providers | Retrieves LLPC written by a learning provider |
| Get learning records by record type | Retrieves LLPC for a given action verb |

**Table 5** Learner-learning provider contract (LLPC)

| Attribute | Description |
|---|---|
| Owner | Address of learner |
| Record type | The action verb for this series of learning events |
| Permissions | Mapping of providers to their allowed permissions; *read, write, grant* |
| Learning events | List of learning events of the same record type |
| Insert learning event | Adds a new learning event |
| Request/grant/revoke access | *Ask/give/deny* access to this LLPC |
| Pending requests | A collection of pending access requests |

required to process a transaction increases with the size of the data in the transaction to be processed. Hence, writing strings of variable length require more computational resources in solving the Proof-of-Work especially when the string is lengthy. After converting the action verb to a hexadecimal equivalent, we then query the blockchain to know if a smart contract based on this action verb exists for this user. If it does, we retrieve the smart contract and simply update it with the current learning record's query string and query result hash. If no such smart contract exists for this action verb, we create the smart contract and update the index contracts of both the provider and the learner. The latter case will require four transactions which need to be mined on the blockchain.

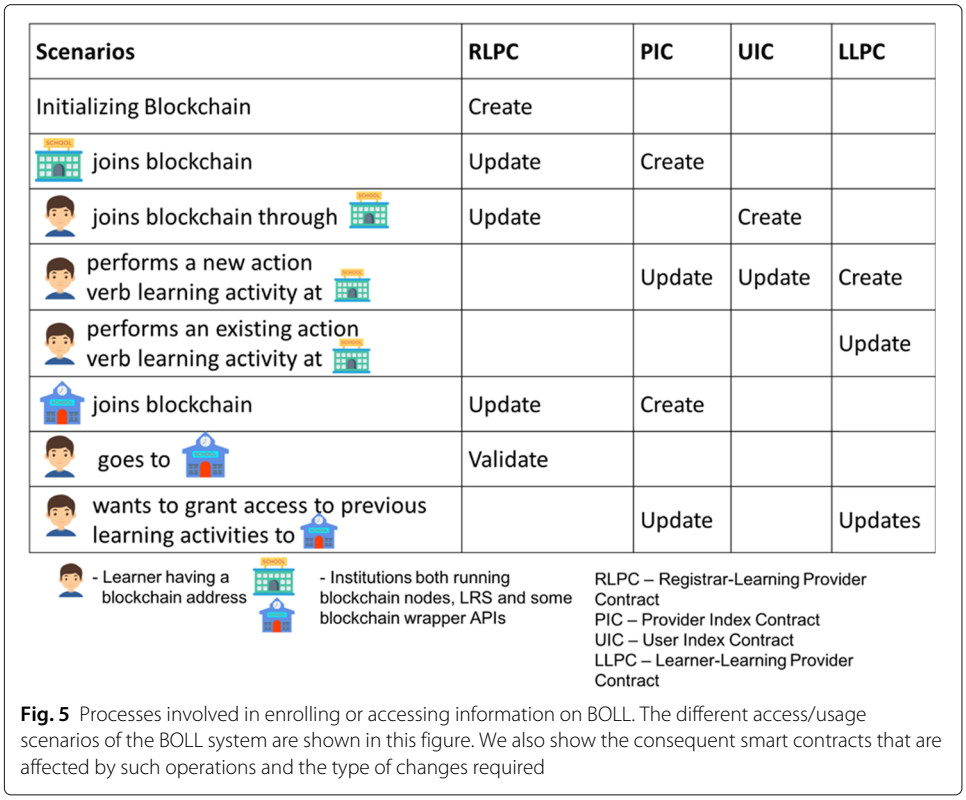


**Fig. 5** Processes involved in enrolling or accessing information on BOLL. The different access/usage scenarios of the BOLL system are shown in this figure. We also show the consequent smart contracts that are affected by such operations and the type of changes required

### Experiment setup

In this experiment, we measure the performance of the BOLL system. To carry out this experiment, it is required to have at least a setup as shown in Fig. 3. We ran this setup on a Dell EMC PowerEdge R530 Hardware (16GB RAM, 512 SSD) with Ubuntu 16.04 Server installed. Also, we setup two other similar instances of Geth in Fig. 3 on the same server so as to ensure distributed mining of transactions.

Our key performance indicators for the BOLL system specifically considers the amount of computational resources required to mine: intermediate transactions, write, update, and access learning records. To measure these, we used the gas usage and timestamp parameter of each transaction to understand both computational and time resource requirements. Using learning records generated by students' activities on Moodle LMS and BookRoll, we simulated some of the processes outlined in Fig. 5. Learning records are generated and logged on the OpenLRW whenever students use BookRoll. Table 6 shows the numerical description of the population and sample space. Six hundred fifty-one students generated 498,842 records of which 291 students' learning records reflected in the randomly sampled 500 learning records to be written on the blockchain.

Writing these learning records on the blockchain requires creating, updating, and validating different smart contracts as shown in the process outlined in Fig. 5. The distribution of transactions generated as a result of the various operations required to write 500 learning records of 291 students is shown in Fig. 6. A total of 3104 transactions were generated with 1000 of them coming from permissions and indexing operations (UIC and PIC) on the learning records.

## Result

From our test, we observed that processing various smart contracts on the BOLL system requires different computational cost. In Table 7, we show a list of these transactions. As stated earlier, gas usage is a representation of the complexity of an operation. Currently, there are no standards on how to determine the equivalent conversion from gas to physical currency. Some factors could guide the determination of such including the cost of electricity, servers, and maybe cost of labor. In our implementation, we note that while create operations (1, 3, and 5 in Table 7) require more gas usage, update operations are less expensive (2, 4, and 6 in Table 7). Creating an LLPC is computationally complex and requires 1,814,374 gas to process. This is because the permissions and learning records indexing strategy are defined in this smart contract and installed upon creation. Similarly, PIC and UIC require 1,030,138 gas to process because of the indexing strategy defined in the index smart contracts.

In our test case, we obtained a waiting time, $W_t$ of 14 min per transaction. Importantly, $W_t$ is different from the time it takes to mine a transaction. On the Ethereum blockchain, this is a function of the current complexity of the Proof-of-Work otherwise referred to as the difficulty. The Proof-of-Work (PoW) is a cryptographic puzzle that involves finding

**Table 6** Test data description

| | Number of learning records | Number of users | Number of action verbs |
|---|---|---|---|
| Total | 498,842 | 651 | 8 |
| Sampled | 500 | 291 | 7 |

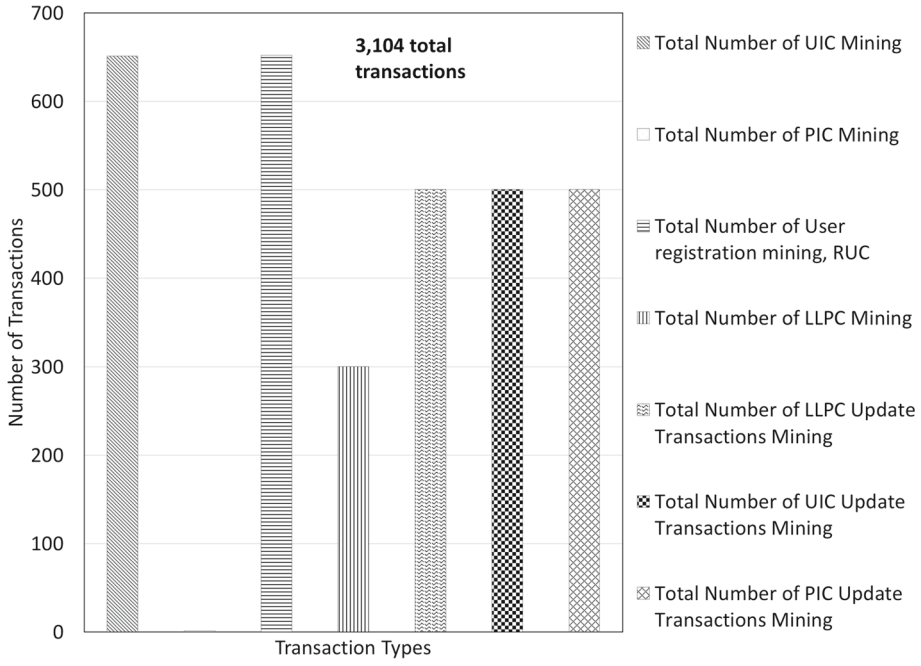


**Fig. 6** Smart contract mining operations. This figure shows the statistical representation of various smart contract update operations resulting from different processes including user registration, learning records insertion, granting permissions, and record indexing

a value whose SHA-256 hash begins with a given number of zero bits. This is enforced to ensure that mining nodes on the blockchain have done some amount of work and the resulting write operations were done in consensus with other participants on the network agreeing to the result of the PoW. It also makes revocation of write operations difficult.

In Fig. 7, we show a plot of difficulty in mining the different blocks representing our learning log transactions over time. The difficulty increases or decreases depending on the amount of computational resources available and the computational power spent on computing the preceding puzzle across the system. In Fig. 8, we also show a plot of the time elapsed between transaction creation and its effective mining over the different blocks' timestamp. The graph shows a near linear increase in time difference because transactions are mined in turns hence our earlier calculation of a 14-min waiting time.

**Table 7** Computational cost of smart contract operations

| S/no. | Smart contract | Action | Frequency of operations | Average cost (gas $10^3$) |
|---|---|---|---|---|
| 1. | PIC | Create | One time | 1030 |
| 2. | PIC | Update | Every time | 115 |
| 3. | UIC | Create | Onetime | 1030 |
| 4. | UIC | Update | Every time | 27 |
| 5. | LLPC | Create | On new action verb | 1814 |
| 6. | LLPC | Update | Every time | 298 |
| 7. | RUC | Update | On user registration | 55 |

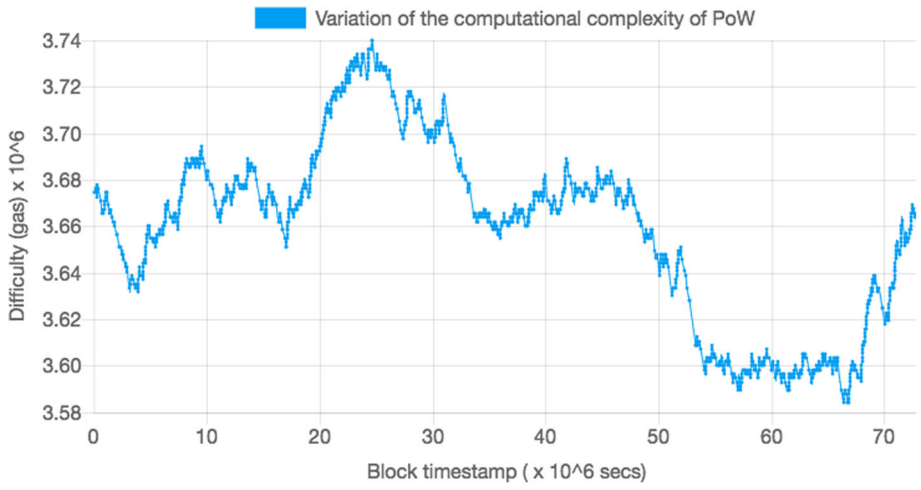


**Fig. 7** PoW computational complexity over time on BOLL. This figure shows the growth of the Proof-of-Work (PoW) over time as more blocks get added to the blockchain. We note that the PoW time complexity does not usually grow, but in some cases reduces depending on the availability of computational resources

In Table 8, we compare the features and performance of our BOLL system to other learning infrastructure. While most learning infrastructure provide support for single-sign-on (SSO), only IMS CLR and BOLL provide support for connecting learning logs. Consequently, systems that do not provide support for connecting learning logs often face the cold-start problem. However, only BOLL system offers a high degree of privacy through smart contracts-based access authorization where learners can actively determine who can collect their learning logs and access them at a later time.

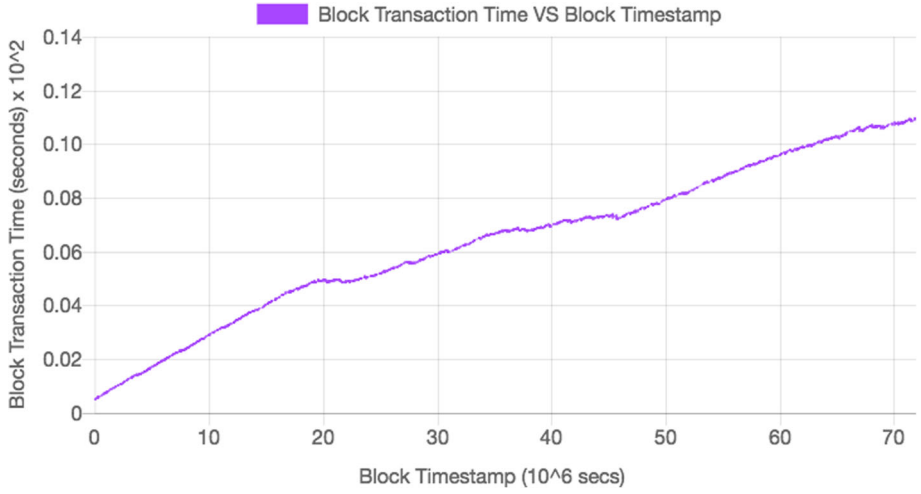


**Fig. 8** Time elapsed between transaction submission and mining completion vs mining completion time. In this figure, we show the plot of the time difference between mining transaction submission and mining completion against mining completion time. This shows that as more blocks get added to the blockchain, the time taken to mine a block increases with the last added block potentially having the highest mining-wait time

**Table 8** Comparison of BOLL system to other learning infrastructure

| Learning infrastructure | Single sign-on (SSO) | Connected learning logs | Fast write of bulk records | Decentralized (privacy, security, etc.) |
|---|---|---|---|---|
| LMS and LRS with xAPI and caliper integration | ✓ | X | ✓ | X |
| IMS CLR | ✓ | ✓ | ✓ | X |
| BOLL system | ✓ | ✓ | △ | ✓ |

## Discussion

Here, we discuss some discoveries, questions, and problems that arose during the implementation and testing of the proposed BOLL system.

### Privacy

On BOLL, the identity of learners from their institution's learning tools is not shared between different institutions. Instead, we generate a sequence of bytes called address for each learner upon registration. For subsequent record look-ups, we use this address as a way of tracking their records on BOLL. This design ensures that only authorized parties can link records on BOLL to the right learner.

From our implementation, we confirmed that unless one has access to the learner's private key, it is impossible to access their learning records without their permission. This is made possible by the inherent security of the blockchain, installed smart contracts and given that all access to such learning records are made through BOLL. We make the assumption that learners would guard their private key from unauthorized access. A third party can have read, write, or grant privileges to the LLPC smart contract containing a learner's learning records. By default, only the learner and their institution where such learning records were generated can grant access to third parties. If a third party requires access to these learning records, they can send an access request to the learner. The learner or their institution can then choose whether to grant any or all of the three access privileges to the requesting third party.

However, we observed a limitation in using action verb-based smart contracts. In grouping learning records according to action verbs, if a learner gives an institution access to read one action verb, such institution is authorized to read all their learning records having that action verb regardless of the learning material from which the learning event emanated. This problem can be solved by extracting identifiers for different learning materials and use a pair of these identifiers and action verbs as a way of keeping access to learning records limited to learning materials.

Also, a learner may choose to deauthorize a third party from having access to their learning records. This is possible by removing the third party's address from the list of authorized accessors in the LLPC. However, we do not currently allow the deauthorization of the learner's current institution especially when no other institution has access to their learning records. This is because if all institutions are deauthorized from accessing a learner's records, it will be impossible to locate their records on the institution's platform. We address this issue while discussing *demise of an institution*, and we suggest that prior to such deauthorization, a learner should enable backup of their data to an authorized data storage site on BOLL.

#### Performance

Our BOLL system currently has an average waiting time of 14 min. This means that for a new learning log to be written on the BOLL network (writing operation may include learner registration, LLPC contract creation, and/or updating and indexing), one would have to wait for an average of 14 min. This time might be acceptable for some use case where learning logs are not required to be read from the blockchain in real-time as soon as they are generated on the learning platforms. In fact, $W_t$ can be much less than 14 min, an isolated case where LLPC is only being updated, it would take between 30 s and 2 min. We are also currently considering integrating new patch-set from the Ethereum lightning network; an off-chain scalable solution that in some sense allows for distributed and faster mining.

#### Installable smart contracts

We have defined a number of installable smart contracts for decentralized control and access of learning logs: RLPC, UIC, PIC, and LLPC. While permissions may differ for different types of learning logs and users, our implementation considers a generic permission structure for all learning logs. We also treat access authorization in a similar manner but empower the users with the ability to grant or revoke access at any time using pre-installed smart contracts. We consider it interesting to look at the various scenarios that might occur when learning logs are of different types and governed by different data policies. One possible solution would be the presentation of smart contracts in a form where learners can understand the concept of the smart contract and be able to select an appropriate smart contract that may suit their needs from an open pool of personal learning logs smart contracts.

#### Demise of an institution

As only a hash of the learning log and its location is recorded on the blockchain, there is a possibility of a learning log outliving its host institution. For example, a student might graduate from an institution and 10 years later, that institution ceases to exist. In a case where all computing facilities such as the LRS of that institution is also shutdown, then the learning logs whose references are held on the blockchain cannot be retrieved anymore. To solve this problem, we envisage a learning blockchain where not only just institutions exist on the network but also third parties who can offer data backup services. These third parties do not act as mediators in anyway but rather serve as storage centers for learners on the blockchain. Another alternative will be to specify smart contract policies where learning records are held on file for a certain duration of time. Currently, we do not recommend that the blockchain should replace traditional databases except for simple-size data.

#### Cost

Cost of computation and infrastructure are the key factors in determining the budget for a learning blockchain. In our implementation of the BOLL system, we incurred some cost in procuring and setting up the servers on which the blockchain node was hosted, electricity bills, internet, etc. In deciding how miners on the learning blockchain get rewarded, these costs need to be factored in. Whether such cost is transferred to the learners or institutions is an open question for stakeholders. Whichever

might be decided, the blockchain provides a way to measure such cost through gas usage.

## Conclusion

In this work, we proposed a solution to the current challenge of connecting learning records across different institutions. One of the main contributions of this work is providing a concrete implementation of a blockchain platform that enable these features. This paper also presents an overview of the resource requirements for running such a system, and the potential benefits when compared to other alternative tools. We also discussed potential challenges and possible approaches to guide future work. While we acknowledge that the time taken to write learning records to the blockchain currently is not suitable for real-time access-based systems, we recommend its usage in scenarios where transition from one institution to another occurs over a given period of time that is within the waiting time as earlier presented. We also discussed about defining and enforcing existing user data privacy policies on the learning logs using smart contracts. While our implementation considers top-level approach of representing these permissions, it will be necessary to understand the implications of having action verb-based privacy definitions.

In future work, greater focus on detailed components of learning logs and corresponding privacy measures is required to develop standardized formats for representing permissions on the blockchain. The scalability of the current BOLL system should also be investigated to ensure that it can handle being implemented as a wide-reaching system.

**Acknowledgements**
Not applicable.

**Funding**
This research was supported by JSPS KAKENHI Grant-in-Aid for Scientific Research (S) Grant Number 16H06304.

**Availability of data and materials**
The research data is stored in the university. Due to the university data policy, the data cannot be shared.

**Authors' contributions**
PO designed and carried out the research studies. BF and HU participated in discussions related to system design and implementation. PO drafted the manuscript. HO supervised this research and contributed to the review and discussion of the manuscript. All authors read and approved the final manuscript.

**Competing interests**
The authors declare that they have no competing interests.

## Publisher's Note



**Author details**
[1]Graduate School of Informatics, Kyoto University, 36-1 Yoshida-Honmachi, Sakyo-ku, Kyoto 606-8501, Japan. [2]Academic Center for Computing and Media Studies, Kyoto University, Yoshida-Nihonmatsu, Sakyo-ku, Kyoto 606-8501, Japan.

Received: 15 October 2018 Accepted: 23 January 2019
Published online: 01 March 2019

**References**

Advanced Distributed Learning (2016). Experience API (xAPI) Specification. http://github.com/adlnet/xAPI-Spec/. Accessed 18 May 2018.

Apereo (2016). OpenLRW: open learning record warehouse. https://github.com/Apereo-Learning-Analytics-Initiative/OpenLRW. Accessed 08 Apr 2018.

Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). Medrec: using blockchain for medical data access and permission management, In *Open and Big Data (OBD), International Conference On* (pp. 25–30): IEEE.

Back, A. (2002). Hashcash-a denial of service counter-measure.

Bracamonte, V., & Okada, H. (2017). A review of blockchain technology applications for academic institutions. *IEICE Tech. Rep. Tech. Comm. Soc. Implications Tech. Inf. Ethics (SITE)*, *117*(340), 11–14.

Buterin, V., & et al (2013). Ethereum white paper. Accessed 12 Apr 2018.
Cachin, C. (2016). Architecture of the hyperledger blockchain fabric, In *Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310*.
Chen, G., Xu, B., Lu, M., Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learn. Environ.*, *5*(1), 1.
Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Appl. Innov.*, *2*, 6–10.
Ethereum (2013a). Ethereum in Go language. https://github.com/ethereum/go-ethereum. Accessed 04 Apr 2018.
2013b
Ethereum (2013b). The Solidity contract-oriented programming language. https://github.com/ethereum/solidity. Accessed 27 July 2018.
Flanagan, B., & Ogata, H. (2017). Integration of learning analytics research and production systems while protecting privacy. In W. Chen (Ed.), *Proceedings of the 25th International Conference on Computers in Education. New Zealand: Asia Pacific Society for Computers in Education* (pp. 333–338).
Grech, A., & Camilleri, A.F. (2017). *Blockchain in education*. Luxembourg: Publications Office of the European Union.
IMS Global Learning Consortium (2017). Comprehensive learner record. https://www.imsglobal.org/activity/comprehensive-learner-record. Accessed 28 May 2018.
IMS Global Learning Consortium (2013). Learning measurement for analytics whitepaper. Retrieved 2018-04-07, from https://www.imsglobal.org/sites/default/files/caliper/IMSLearningAnalyticsWP.pdf.
ISO/IEC JTC 1/SC 36 (2016). *Information technology for learning, education and training – learning analytics interoperability – Part 1: Reference model*. Geneva, CH: Standard, International Organization for Standardization.
Moodle, H.Q. (2001). Moodle learning management system. https://moodle.org/. Accessed 28 May 2018.
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved 2018-03-18, from https://bitcoin.org/bitcoin.pdf.
Ocheja, P., Flanagan, B., Ogata, H. (2018). Connecting decentralized learning records: A blockchain based learning analytics platform, In *Proceedings of the 8th international conference on learning analytics and knowledge* (pp. 265–269). New York: ACM.
Ogata, H., Li, M., Hou, B., Uosaki, N., El-Bishouty, M.M., Yano, Y. (2011). Scroll: Supporting to share and reuse ubiquitous learning log in the context of language learning. *Res Pract. Technol. Enhanc. Learn.*, *6*(2), 69–82.
Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *Br. J. Educ. Technol.*, *45*(3), 438–450.
Rubel, A., & Jones, K.M. (2016). Student privacy in learning analytics: an information ethics perspective. *Inf. Soc.*, *32*(2), 143–159.
Schmidt, P. (2016). Blockcerts–an open infrastructure for academic credentials on the blockchain. MLLearning (24/10/2016). Retrieved 2018-05-22, from https://medium.com/mit-media-lab/blockcerts-an-open-infrastructure-for-academic-credentials-on-the-blockchain-899a6b880b2f.
Sharples, M., & Domingue, J. (2016). 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* (pp. 490–496). Cham: Springer International Publishing.
Siemens, G., & Long, P. (2011). Penetrating the fog: analytics in learning and education. *EDUCAUSE Rev.*, *46*(5), 30.
Sony Global Education (2017). Sony develops system for authentication, sharing, and rights management blockchain technology. https://www.sony.net/SonyInfo/News/Press/201708/17-071E/index.html. Accessed 28 Sept 2017.
Szabo, N. (1997). Formalizing and securing relationships on public networks. *First Monday*, *2*(9).
The Mozilla Foundation (2012). Peer 2 Peer University in collaboration with The MacArthur Foundation: Open badges working paper. Accessed 05 May 2018.
University of Nicosia (2014). University of Nicosia: Academic Certificates on the Blockchain. http://digitalcurrency.unic.ac.cy/certificates. Accessed 07 May 2018.
Wang, F., & Hannafin, M.J. (2005). Design-based research and technology-enhanced learning environments. *Educ. Technol. Res. Dev.*, *53*(4), 5–23.