applied sciences

MDPI

Article

Blockchain-Based Badge Award with Existence Proof

Min Choi [1], Shinde Rupali Kiran [1], Se-Chang Oh [2] and Oh-Young Kwon [3,*]

[1] Dept. of Information and Communication Engineering, Chungbuk National University, Cheongju 28644, Korea; mchoi@cbnu.ac.kr (M.C.); rupali@cbnu.ac.kr (S.R.K.)
[2] Saltlux, Seoul 06147, Korea; sechang@gmail.com
[3] Dept. of Computer Engineering, Korea University of Technology and Education, Cheonan 31253, Korea
* Correspondence: oykwon@koreatech.ac.kr

Received: 31 March 2019; Accepted: 24 May 2019; Published: 17 June 2019

Abstract: In this paper, we present a badge awarding system for performance assessment in education using blockchain technology. Learners will be awarded badges, which are certified for a predetermined level of progress in terms of learning. All the badges are stored in a backpack, which is an environment for storing and presenting the obtained badges. Badges are immutable and verifiable as well as rigid. The use of badges in the education system makes education more interesting, skill-based, and adaptable to changes. The key contribution of our work is in terms of compatibility with Openbadge specification and integrated cooperating platform between digital badge awarding and blockchaining. Our system implementation is compatible with Open Badges of IMS Global Learning Consortium, which is used to earn, issue, and award badges across various platforms. The badges are trusted by the IMS standard, the criteria to earn a badge is verified through the network, and the overall process is transparent compared to the traditional education system. Moreover, all badge awarding events in our system are recorded in a blockchain. Once stored, the contents cannot be tampered with. Thereafter, anyone can check the validity of the badge through the blockchain. Our platform will be useful for distance learning as well as time and location independent learning. The experimental results are as follows. On a Bitcoin-based digital badge publishing platform, the execution time required to award the badge is 24.53 s, while on the Ethereum-based digital badge publishing platform, the execution time to award the badge is only 3.86 s. It can also be used for career management and personal history. The learners can obtain the current knowledge required for a job. Lifelong learning will be also possible with this platform.

Keywords: blockchain; digital badge; open badge; bitcoin; ethereum

1. Introduction

Blockchain technology is used as the base technology in many fields because it uses a distributed, decentralized database without any central control over the system and is highly secure owing to the use of the SHA 256 algorithm [1]. A survey conducted by the World Economic Forum in 2015 found that those polled believe that there will be a tipping point for government use of blockchain by 2023 [2]. Governments, large banks, software vendors, and companies involved in stock exchanges, especially the Nasdaq stock exchange, are investing heavily in this area. For example, the UK Government recently announced that it is investing £10 million for blockchain research [3] and Santander has identified 20–25 internal use cases for technology that can predict a reduction in banks' infrastructure costs by up to £12.8 billion a year [4]. To understand the relevance of blockchain in the education system, it is important to understand its components and implementation on educational networks. Blockchain is a distributed record of digital events that are linked together to maintain the link and hash values of previous events [5]. In this way, all the events are liked with the chain and stored on each computer in the same network. Everyone can see the events, but no one can change the information,

not even the owner of the event. Public blockchains are accessible to everyone and have the potential to add new blocks to the chain, whereas private blockchains are used by organizations. The best known blockchain is the one at the heart of the Bitcoin system of digital money [6]. "Proof of work" is an important feature of the blockchain technology, where a new block is checked for legitimacy and is added to the chain of blocks. This is done using special notes for the benefit of incentives. This is a verification process, which is also called as mining, and in an education system, the badges are verified using the mining method. It is nearly impossible for any hacker to hack a blockchain, and this makes the Bitcoin blockchain a highly trusted platform [7,8]. Mining requires considerable amount of power and electricity, and even if a hacker has all these things, he/she will still need to spend a considerable amount of time on the network.

A blockchain is formed by linking many blocks together, and each block can hold nearly 1 Mb of data in it. In the Bitcoin network, the blocks contain the timestamp, transactions, and hash of the previous block; however, in our educational network, the blocks contain course credit, assignment, skills, etc. Every student and teacher can see the skills of the student, but they cannot make any changes. The students are able to show their skills by referencing backpack websites containing all the acquired badges. The badges are compatible with most of the internet platforms and can be shared over the internet or social media. IMS Global provides the certification of badges and OpenBadges provides the configuration of the badges. In this research, the issuance of badges and verification is done using the Badgr [9] platform. Originally, a badge in the Badgr platform is only a trust relationship between two parties. This means that so far we have not been able to create chains of trust and networks of trust. However, in this study, we extended and implemented the trust relationship among all participants in the distributed environment of blockchain with regard to the following concerns. (1) Elimination of the inefficiency and social cost problems of various certificate issuing systems: There are some inefficiencies and inconveniences in the certificate issuing systems of educational and public institutions, provided through the existing information system. There are costs related to the issuance of certificates, transcripts, and diplomas for online and offline education and training courses. In order to resolve these problems, we provide a technique for the certification creating/issuing/awarding system by using simple REST (Representational State Transfer) APIs (Application Programming Interfaces) [10]. (2) Difficulties in managing subdivided qualifications: Our system can be easily extended to establish a management system capable of coping with segmentation and short learning contents such as microlearning. We focus on the issuance and management of competency unit certificates as an authentication method for detailed educational and training courses. (3) Establishment of an effective management system for individual education and training history of learners: We established a backpack system to gather and manage the experiences and achievements in official and informal activities obtained from individual and offline education and training. In this way, our system can establish a system to officially certify the collected information, so that the information can be used for future learning and career planning.

In a later section, we describe in detail the implementation of the platform using OpenBadges' specifications. Distance education is possible with this technology, which will lead to the possibility of lifelong learning for all learners. The learner will be able to show his badges online to a recruiter, and the recruiter will able to understand his or her skills in detail. The traditional education system is boring for some students as it mainly focuses on books and exams. On the other hand, by using badges, education becomes skill-based and self-learning-based as well as interesting. By using the Mozilla OpenBadges framework, any organization can issue badges, and the badge receiver can use it to showcase his or her skills and work experience. With our platform, everyone will get the opportunity to share knowledge though the social networking system. The experimental details will be explained in the experiment section.

Today's education is still controlled by educational institutes or administrative bodies, which offer quality, credibility, and knowledge. The current model is not flexible for all learners because of time, money, and distance constraints. To make the learning process easy, flexible, and trustworthy we

established an educational network based on blockchain technology. In this paper, we present the establishment of a testbed for issuing, verifying, and storing badges in the form of blocks of a chain. Blockchain is irreversible and static: once a change is made, it remains forever. It means that all badges saved on the blockchain remains with the issuer forever. In the 21st century, Satoshi Nakamoto's Bitcoin has become the most popular cryptocurrency, and it has received considerable attention [2].

2. Related Works

Blockchain technology has a wide range of applications, such as education, engineering, administration, medicines, elections, construction, and e-government. In this research, we primarily focus on the education field. Therefore, we present some research cases of the using of blockchain technology.

2.1. EDSA

The European Data Science Academy (EDSA) [11] is a good example of the application of blockchain technology for providing data science skills to job seekers. EDSA also helps provide training to a new generation of world leading data scientists.

In the 21st century, data is being produced from all industries at a phenomenal rate, which has introduced numerous challenges regarding the collection, storage, and analysis of this data. However, as the amount of available data continues to increase, so does the demand for professionals who have the necessary skills to manage and manipulate this data.

Owing to this necessity, the EDSA was established to provide a platform to manage the demand and supply of data science experts by providing skill training in real time. Automated tools have been developed to extract dada from job posting portals, such as Indeed [12], Jooble [13], XING [14], and Adzuna [15]. To acquire real-time market need, the data of the last 18 months is considered. EDSA provides detailed recording of accreditations in digital form, for both formal and informal learning contexts.

In order to facilitate accreditation, personalized recommendations are provided to learners studying data science courses. The learners studying various data science subjects earn badges upon reaching certain milestones in their studies, e.g., completing a part of a course or an entire course. The learner will get job recommendations based on full and partial matches with geographical location. Everything is displayed on the dashboard. Partially matching jobs are shown along with course recommendations that fully match that job requirement. Figure 1 shows the details of the EDSA working framework.

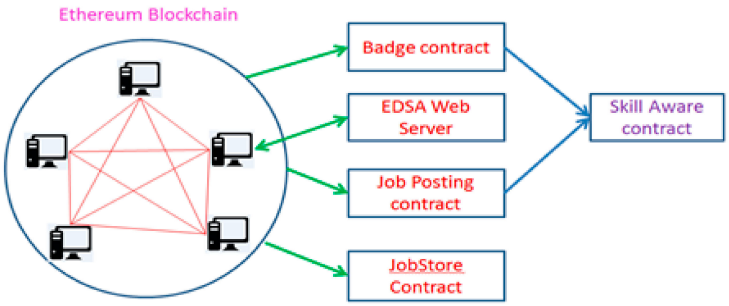

Figure 1. EDSA's approach using blockchain.

2.2. Learner-Centered Blockchain of Open University In U.K.

The Open University of United Kingdom [16] has published a learner-centered approach for learning using blockchain technology. In that paper, they presented a learner-centered ecosystem using blockchain. This ecosystem includes the learner, teachers, courses, learning material, and validation system with learner's connection as shown in Figure 2. The learners are enrolled on a number of

courses and they can utilize the additional learning resources. The tutors and other teaching staff provide both informal and formal feedback as the complete summative and formative assessment of the learner. Central administrative bodies issue formal certificates according to their institutional processes. Each learner has a badges and achievement visualization space called passport; it can be used instead of a traditional resume to present his or her skills to the employer. This system provides transparency, trust, privacy, and security.

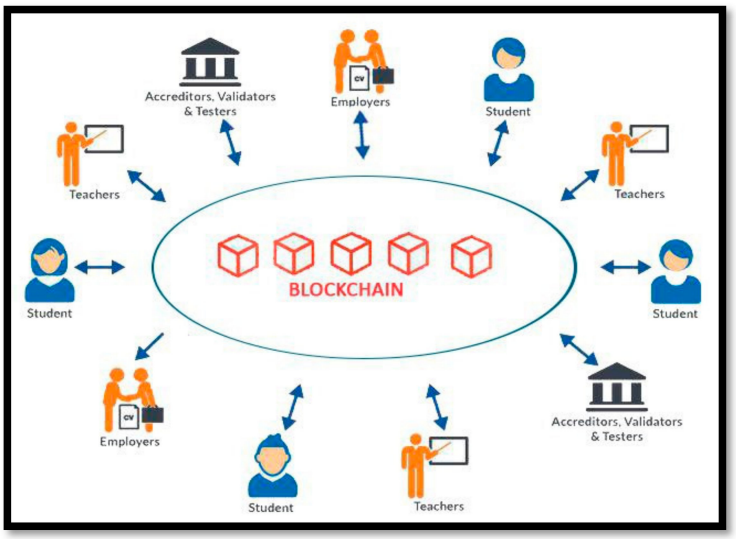

Figure 2. Learner centered blockchain approach.

2.3. U.C Davis' Digital Badge

In the 21st century, we need new talents with various practical skills. For example, the establishment of a life sciences, economics, and humanities course, which enables students to experience on-site learning by combining eight different departments, can create talent required to develop a sustainable agriculture and food system. The new curriculum should be run mainly on the basis internships or field practice outside the classroom. One of the methods designed to allow students to express themselves differently is the 'digital badge' system. The core competencies required for college graduates are 'systematic thinking', 'experiment and questionability', 'value comprehension', 'human communication ability', 'strategic management ability', 'citizen participation ability', and 'development ability'. These core competencies are expressed as a 'digital badge' in U.C. Davis's Digital Badge [17,18], and each competency is divided into five stages: skill, knowledge, honor, experience, and competence. As shown in Figure 3, the 'digital badge' system is an evaluation criterion for human capital that verifies widely and accurately the adequacy of the necessary capabilities in the mobile connected society.

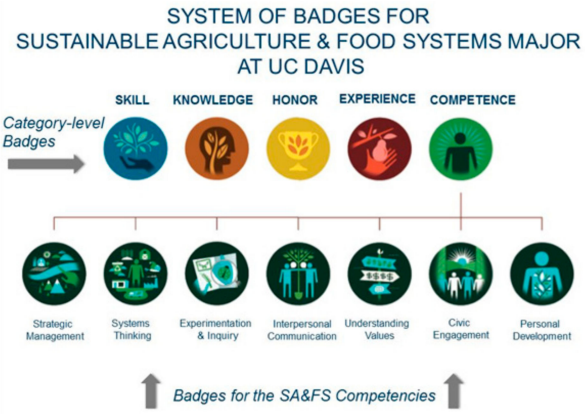

Figure 3. Digital badge system for sustainable agriculture & food systems major at U.C. Davis.

2.4. Cisco's Digital Badge System

Cisco [19] is a partner of Acclaim—Pearson View's badge platform—and provides the following services through Acclaim; web version of credentials that can be shared online labor market insight to understand the individual's technical ability and connection with the profession, and credible checking of credentials in real time. The individual's credentials are displayed in a digital image with proven metadata describing the credentials and the process required to achieve the qualification. Marking the credentials with a badge is a simple, easy, and reliable way to share a person's achievements online in real time. This is concrete evidence of what the individual has done for the company and its colleagues, and it provides employment information based on this to the individuals.

2.5. Swarm and IBM's Open Badge

The badges are suitable for team building games and attendee motivation, as well as for recruitment decisions and other important staff considerations. Receiving the badge demonstrates that the attendees are representing their skills and knowledge to others outside their traditional working environment and participating in a broader expert community in the field. David Leaser, chief program manager at IBM, said in an essay on the Open Badge [20] program, "Whether your employer is hiring new employees or planning on-site promotion, badges are a way to verify employee skills." Badges are a great way to encourage attendees to motivate themselves to learn new things and develop new skills.

2.6. Microsoft Exam and Certification Badge

Microsoft partnered with Pearson VUE's Acclaim platform to provide a badge for certification acquisition [21]. The badge is a Microsoft certification mark that is available on the web and consists of images and unique metadata associated with the certificate holder. The badge provides the owner detailed information about the technology and demonstrates possession of the technology. The benefits of Microsoft badges are as follows; ① easily share certification and test results with an expert network, ② identify who employs the technology holder, ③ identify the expected salary of the workplace that requires the Microsoft skills possessed by the badge holder, and ④ search for job-related announcements related to certification details and complete support with just a few clicks.

The blockchain technology has been implemented in education by Oxford academics by launching the 'Blockchain University' in 2018. A blockchain-powered government means that all its services including visa applications, bill payments, and license renewals are digitized [17] A paperless government equates to enhanced productivity, less time wasted, and less money spent per year [22]. In the next section, we present our approach using a testbed and the regtest mode.

3. Digital Badge System with Blockchain Support

In this section, we explain the detailed architecture and implementation of the digital badge platform based on blockchain. As shown in Figure 4, it consists of the following major components or steps; badge award, badges repository such as backpack, distributed storages in the form of blockchain, and verification.

3.1. System Architecture

In this research, the Badgr platform, which is compatible with Openbadge [8,9] specification, is used as an underlying platform for our digital badge management system. The most important information to be described when creating a badge are badge class, badge award criteria, issuer, name, description, etc. Badge creation should be preceded by badge awarding for digital badge issue.

The process of issuing a digital badge is as follows. ① Initially, a badge should be created (digital badge creation) unless the badge already exists. ② The digital badge issuer generates badge assertion and digital signature through a public key-based cryptosystem. ③ The digital badge issuer delivers the image of the badge to the recipient (or pushes it to the recipient's backpack account). ④ The recipient

decides whether to receive and disclose the corresponding digital badge in his/her backpack. ⑤ The digital badge recipients can view/manage the digital badges they have acquired (backwards compatible according to the IMS Global standard) using the backpack web page or Mozilla backpack that will be developed in this project, and the badges can be shared with the outside world. Figure 5 shows the behavior of each system component used in this study and the resulting change in data.

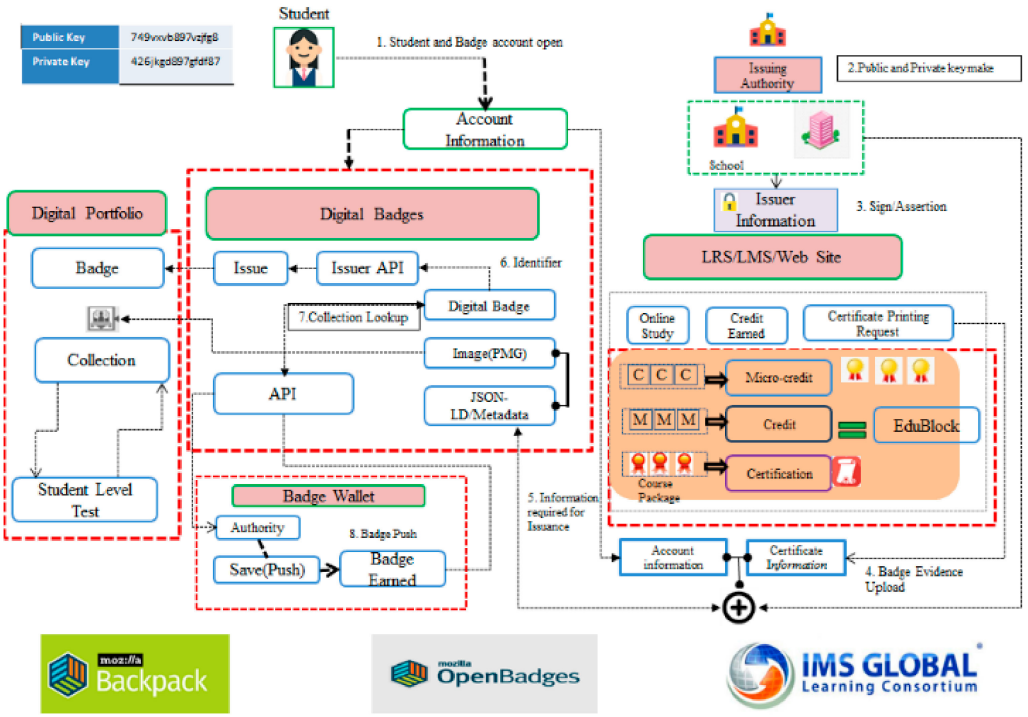

Figure 4. Control flows on digital badge of our system implementation.

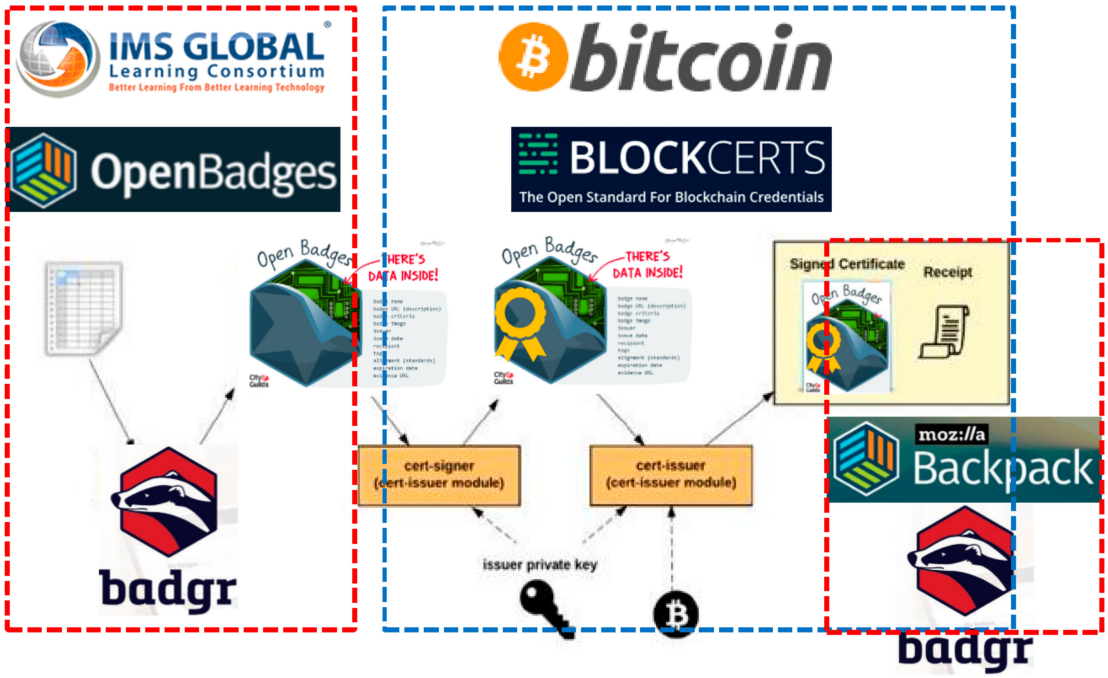

Figure 5. Digital badge issuing process on our system implementation.

For issuing a badge, information about the recipient should be provided as follows. ① The web server that provides the JSON-LD file, including the profile of the badge issuer, badge class, and assertion for stable URL, should work. ② The badge is issued to the email address of the digital badge recipient. ③ In the case of a signed assertion in the above process, a public/private key pair must be created to host the public key [23].

3.2. Blockchain Implementation Support with Badge Issuance

Now, we describe the details of the digital badge platform based on blockchain. Originally, the Badgr platform itself did not support blockchain. Therefore, in this study, we have implemented an upgraded digital badge platform to operate in conjunction with the blockchain. The issuing and backpack management system can create, issue, and manage badges conforming to the OpenBadge specification. Therefore, in this study, a block badge-based digital badge issuance and backpack management system was implemented in conjunction with block chain support [24], and the block badge-based digital badge issuance and backpack management system, which was originally aimed at, was constructed. The digital badge assertion information, which is issued by the digital badge management system, is displayed through the JSON viewer as shown in Figure 6. The information within the assertion are as follows.

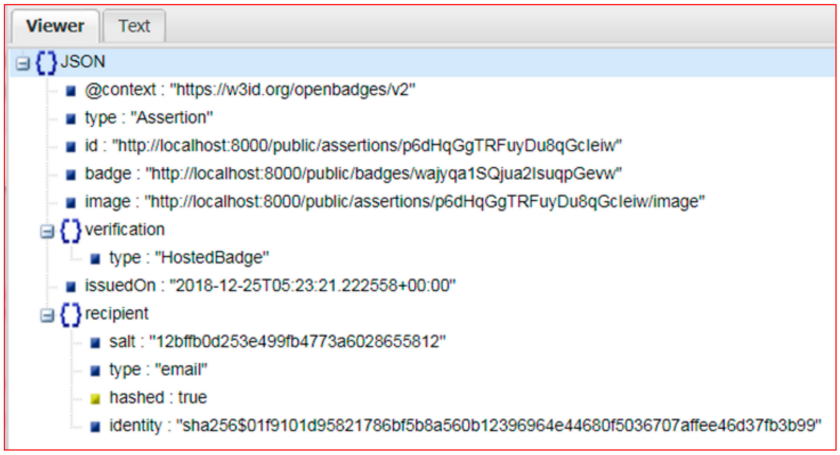

Figure 6. Digital badge assertion information.

The digital badge is a combination of an image and the metadata associate with it. The image of the badge is a pictorial format of the achievement, and the metadata includes details of the achievement, such as issues, skills, credits, or microcredits gained by the student. The badges in an education network works like traditional university certificates, but the badges are more trustworthy and fairly compared to university certificates. A detailed view of a badge is shown in Figure 7; it is also called as split view of the badge.

- ✓ id: a unique identifier for the badge; this is expected to be locally unique, not globally unique.
- ✓ recipient: the recipient of the achievement
- ✓ badge: URL that describes the type of badge being awarded. The endpoint should be a Badge Class.
- ✓ verify: data to help a third party verify this assertion
- ✓ issuedOn: date on which the achievement was awarded
- ✓ image: URL of an image representing the user's achievement. This must be a PNG image, and if possible, the image should be prepared via the baking specification.
- ✓ evidence: URL of the work that the recipient did to earn the achievement. This can be a page that links out to other pages if linking directly to the work is infeasible.

✓ expire: if an achievement has some notion of expiry, this indicates when a badge should no longer be considered valid.

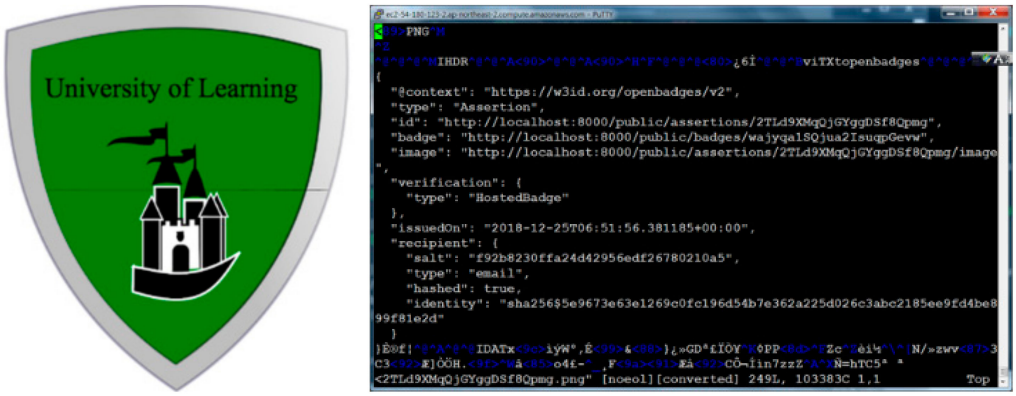

Figure 7. A digital badge example and baked information within the badge instance.

Published digital badges are available in two types (JSON or PNG): The first is the previous assertion/JSON format, in which the information of the badge is expressed in the form of text and URL. The second format is in the form of a PNG image file containing the information of the badge [25]. The image file is a normal PNG file, as shown in the figure above. The badge assertion information is baked inside the PNG file by the iTxt format of the png file. In this work, we utilize both types of badges at the same time. The badge baking is the process of embedding the assertion into the badge image. We can simply say "attaching information with the image", but the difference is that the associated information is always attached with the image and is compatible on many platforms. Our platform bakes the information of "id", "image", and "recipient" to the digital badges. The iTxt chunk provides support for international text, and is represented using the UTF-8 encoding of UCS. The badge image is in PNG (Portable Network Graphics) format; therefore, the information associated with it must be compatible to the image file format. The iTxt format is compatible with the PNG encoder, and therefore baking is only possible with the iTxt format.

Figure 8 shows the results of the digital badge award in accordance with the Merkle Proof 2017 protocol [17], Merkle Tree, and storing Merkle path information. The above type is BTCOpReturn [18], because the underlying platform indicates that Bitcoin is used among Bitcoin and Ethereum. In particular, it can be seen that the OPReturn field performs Merkle Proof-based existence verification on the document through the OPReturn field, while the OPReturn field conventionally stores money transaction information in the existing Bitcoin blockchain.

In this research, we use two basic platforms: The first is the Badgr platform for creating the OpenBadge standard-based digital badge, and the second is the Blockcert platform [24], for managing the digital badge generated through the blockchain. The generated digital badge is managed via backpack repository (compatible with Mozilla OpenBadge backpack). These digital badges can be shared via e-mail, cell phone, etc. In addition, these digital media can be promoted to a third party through a social networking service (SNS).

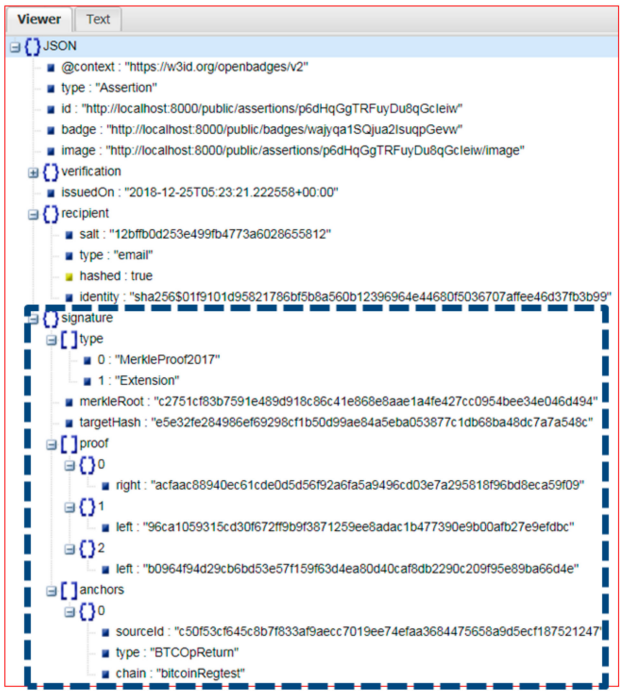

Figure 8. Digital badge assertion information with extension of blockchain in this research.

3.3. Digital Badge Instance

Originally, there is two types of methods to distinguish assertion information: hosted type and signed type. Also, conventional Badgr does not natively support the ability to store data in the blockchain. That is, conventional Badgr manages the information of the badge itself and stores the information according to the specification defined by OpenBadges. (1) If an assertion uses "hosted" verification and there is no cryptographic signature to verify that the full document here is the exact one published by the issuer, the verifier and displayer platforms will likely discard the embedded Badge Class and issuer Profile here and replace them with the values discovered at their id URIs, because only those hosted documents can be trusted to be created by the issuer. (2) If an assertion uses "signed" verification, the validator may accept the embedded values as the intended Badge Class and issuer Profile, and if they have multiple records for those entities that use the declared id, the validator may choose how to index and present that information. The issuers should change the ids of their Badge Classes when they make edits if they wish the edits to be essentially understood as a different achievement than the one published under the original id.

Figure 9 shows the flow chart of the platform operation developed in this study. As shown in the figure, the digital badges and certifications are issued by the issuing authority to the student, and they are also recorded by the issuing authority to generate blockchain transactions. Backpack is a badge repository, the original concept of which was proposed by Mozilla. Digital badges and certifications are verified by the certification verifier on the Bitcoin blockchain in regression test mode or the Ropsten Ethereum network [26]. The regression test mode of Bitcoin is used to establish a new blockchain with private control but has the same rules as the public Bitcoin network. This mode is specially used for research and development purposes, where the rules are predefined. Any individual or organization can create an Issuer profile and begin defining and issuing digital badges. Any entity that can be described with a name, description, URL, image, and email address is a possible candidate to become an Issuer. To issue a digital badge, we need a technology platform that is compatible with the Open Badges specification [12].

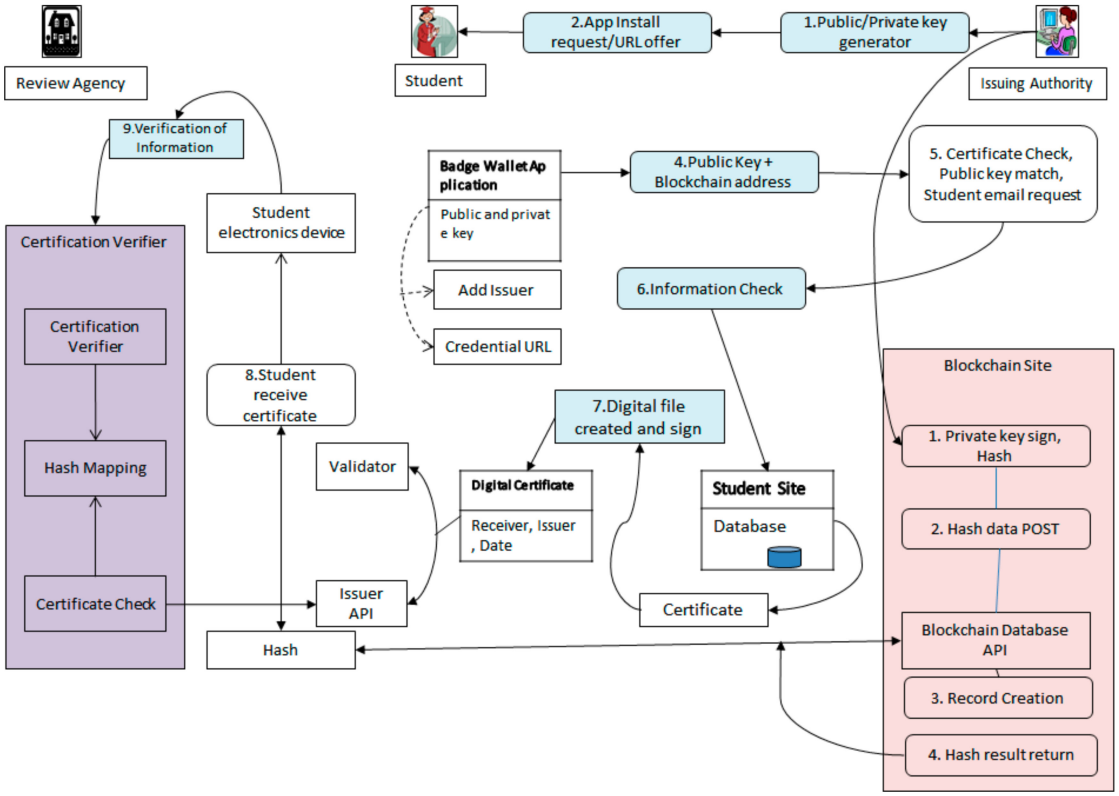

Figure 9. Flowchart of digital badge award and verification on our system implementation.

We used a total of four servers to develop the proposed system. The first is a web server for providing the user UI. The second is a REST API server for performing operations conforming to the Open Badge standard. The third is a blockcert server for recording transactions in the blockchain. The fourth is a blockchain network. In this study, the Bitcoin server in the regression test mode is used for Bitcoin and the Ropsten test network [26] is used for Ethereum. In this study, all the servers were implemented in the AWS EC2 cloud platform as shown in Figure 10.

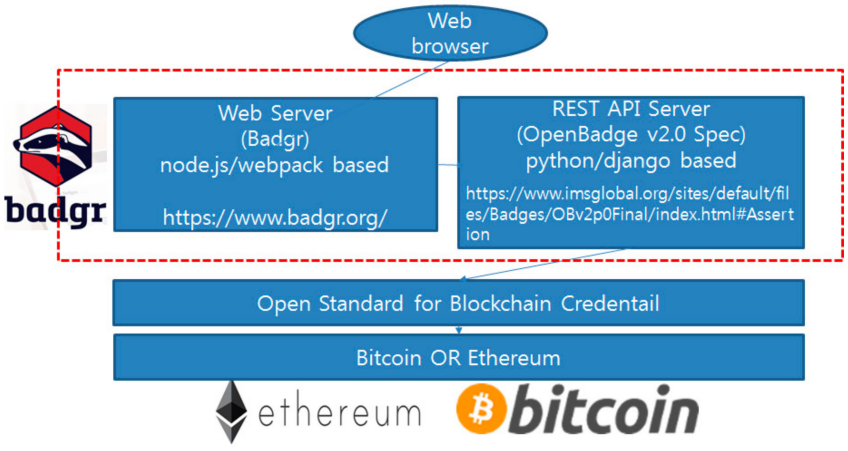

Figure 10. System components and interfaces for blockchain based digital badge award.

4. Experimental Results

In order to implement a functionality that works with the blockchain platform, the most rational thing to do would be to use the dedicated REST API. It allows users to save time and the financial expenditure needed for the development of systems from scratch and focus on aspects that are more

significant and essential for the core services or tasks. With this approach, the users will not be obliged to stick to a single programming language or SDK. That, in turn, will take off some of the limits from the team of developers. For this purpose, our blockchain-based digital badge publishing system proposed in this study also provides the REST API for linking with external systems. We can look up the transaction ID based on blockchain (Ethereum).

In this research, we implemented a digital badge issuance and backpack management platform with blockchain (Ethereum and Bitcoin) support. It enables digital badge issuance in conjunction with blockchain by using a badge issue API. After badge award, our system provides a transaction ID value (within a field named as txid) in the response of the badge issuing API (JSON—extensions field) as extensions field. Figures 11–18 show the REST APIs in detail.

API-NAME	CreateBadge				
DESC	새로운 배지 생성				
Request					
	URL	http://54.180.6.77:8000/v1/issuer/issuers/yJ4IGh8JS5Gt-3I6irYe_A/badges			
	Method	POST			
	Headers	**Name**	**Type**	**Required**	**Desc**
		Authorization	User ID별 상이	REQUIRED	예: dr.choimin@gmail.com 계정의 경우 "Bearer Ubhfns38SnSqpNqTXsquV894NuZRto"
		Content-Type	application/json	OPTIONAL	
	Parameters	**Name**	**Type**	**Required**	**Desc**
		BODY	raw - JSON(application/json)	REQUIRED	{"name":"test","description":"test badge","image":" CByJOsAAAgAElEQVR4Xuy9aZcc53UmeN8tltxqX1EACgtJkCBFUhSpXeKRZct93G532wbd9pnj0x 7Llqw+4w/zB4T5A/ML5ttMzxwPrW6PJG+SKHGnalkUN+xLYQcKteYW27vNuZEZhUAyq1AgkRQ ARR4WM5EZ8UbEjYj3iefe595LoHgVFrjzFiA9Q9qPs4nDhw/TI0celUtLR8nS0hFar19iUZly72pFKEO Z8gx3DWXtIGaOC9xECXPsCNXQ5MYm3AqHM0mYtIRZkISDoZZTCmCJBXyn1FpDWfoZ3xkAA2 LBdo+j8840Jfi9ZgzwN547KAUAGojloNNvmWYAkFgC1MSgOt9q/N1YBdoSHB6IIdwY0NTgcgqo ISQ2AqgBUBAppW0yhFMSxlrAlYR4Jq4zJBYawaeIj43hEjDqNYua8pA1JTnzaqhIdATEwfNxMQjF uB5OHiwoP3ud79rCcHtfqRX7znNBvmo432knShW+s22wGYX4W+2VYqi72eB7Vwrt5v8rD1Mn3/
		issuers	GET URL	REQUIRED	예 : MinOffice의 경우 "yJ4IGh8JS5Gt-3I6irYe_A"
Response					
	Entities	**Name**	**Type**	**Desc**	
			application/json	{ "created_at": "2019-01-24T03:02:11.027409Z", "created_by": "dr.choimin@gmail.com", "id": 7, "name": "test", "image": "http://54.180.6.77:8000/media/uploads/badges/issuer_badgeclass_25453089-d124-4515-a843-d8fb4a38064c.png", "slug": "7iEOsSm4QxatKpu8y-Xrww",	

Figure 11. REST API for creating badge.

API-NAME	EarnerCollections				
DESC	현재 Authorization field에 의해 특정되는 배지 수여자가 구성한 컬렉션 분류 리스트				
Request					
	URL	http://54.180.6.77:8000/v1/earner/collections?json_format=plain			
	Method	GET			
	Headers	**Name**	**Type**	**Required**	**Desc**
		Authorization	User ID별 상이	REQUIRED	예: dr.choimin@gmail.com 계정의 경우 "Bearer Ubhfns38SnSqpNqTXsquV894NuZRto"
		Content-Type	application/json	OPTIONAL	
			...		
	Parameters	**Name**	**Type**	**Required**	**Desc**
Response					
	Entities	**Name**	**Type**	**Desc**	
			application/json	[{ "name": "MyCollection", "slug": "HUM1P0c2RJ-G8-_DWiNskQ", "description": "1", "share_hash": "", "share_url": "", "badges": [{ "id": "t_jgcbC3TvGURV9pg7z1hw", "description": "" }, { "id": "HQqj935ZQ7e51IWCc2L0gw",	

Figure 12. REST API for listing earner collections.

API-NAME	BadgeList			
DESC	현재 Authorization 정보에 의해서 특정되는 사용자에 대한 수여된 배지 리스트를 제공			
Request				
URL	http://54.180.6.77:8000/v1/earner/badges?json_format=plain			
Method	GET			
Headers	**Name**	**Type**	**Required**	**Desc**
	Authorization	User ID별 상이	REQUIRED	예: dr.choimin@gmail.com 계정의 경우 "Bearer Ubhfns38SnSqpNqTXsquV894NuZRto"
	Content-Type	application/json	OPTIONAL	
				...
Parameters	**Name**	**Type**	**Required**	**Desc**
Response				
Entities	**Name**	**Type**	**Desc**	

		application/json	[
			{
			"recipient_identifier": "dr.choimin@gmail.com",
			"acceptance": "Accepted",
			"narrative": "asdfasdf",
			"evidence_items": [],
			"extensions": {},
			"id": "j4Fb_7DrS462CoU1eNSRXQ",
			"json": {
			"id": "http://54.180.6.77:8000/public/assertions/j4Fb_7DrS462CoU1eNSRXQ",
			"type": "Assertion",
			"uid": "j4Fb_7DrS462CoU1eNSRXQ",
			"recipient": {
			"recipient": "dr.choimin@gmail.com",
			"type": "email"
			},
			"badge": {
			"id": "http://54.180.6.77:8000/public/badges/wajyqa1SQjua2IsuqpGevw",
			"type": "BadgeClass",
			"name": "testbadge1",
			"description": "",
			"image": "http://54.180.6.77:8000/public/badges/wajyqa1SQjua2IsuqpGevw/image",
			"criteria": "http://testbadge1.criteria.com",
			"criteria_text": "test1",	

Figure 13. REST API for listing badges.

API-NAME	BadgeFromIssuer			
DESC	특정 발급자로부터 발행된 특정 배지 조회			
Request				
URL	http://54.180.6.77:8000/v1/issuer/issuers/U2bhfn5tRcudD6Nj-z7p2Q/badges/o1nCMDjURFSA1U0LNQmRpg			
Method	GET			
Headers	**Name**	**Type**	**Required**	**Desc**
	Authorization	User ID별 상이	REQUIRED	(아래 access token REST API로 받은 값)
	Content-Type	application/json	OPTIONAL	
				...
Parameters	**Name**	**Type**	**Required**	**Desc**
	issuers	GET URL	REQUIRED	예 : BCLab1 의 경우 "U2bhfn5tRcudD6Nj-z7p2Q"
	badges	GET URL	REQUIRED	예 : Test 배지의 경우 "o1nCMDjURFSA1U0LNQmRpg"
Response				
Entities	**Name**	**Type**	**Desc**	
		application/json	{ "created_at": "2018-12-26T05:38:56.301594Z", "created_by": "dr.choimin@gmail.com", "id": 4, "name": "BCLab badge", "image": "http://54.180.6.77:8000/media/uploads/badges/issuer_badgeclass_b1c44873-61df-43c6-97d1-ae3f95f1a45e.png", "slug": "o1nCMDjURFSA1U0LNQmRpg", "criteria_text": "123", "criteria_url": null, "recipient_count": 5, "pathway_element_count": 0,	

Figure 14. REST API for listing badges from a certain Issuers.

API-NAME	UserProfile			
DESC	현재 Authorization field에 의해 특정되는 사용자의 프로파일 정보 가져오기			
Request				
URL	http://54.180.6.77:8000/v1/user/profile			
Method	GET			
Headers	**Name**	**Type**	**Required**	**Desc**
	Authorization	User ID별 상이	REQUIRED	(아래 access token REST API로 받은 값)
	Content-Type	application/json	OPTIONAL	
Parameters	**Name**	**Type**	**Required**	**Desc**
Response				
Entities	**Name**	**Type**	**Desc**	
		application/json	{ "first_name": "", "last_name": "", "email": "dr.choimin@gmail.com", "slug": "LEO6fDfwT_SOvOMZtD0XTg", "agreed_terms_version": 0,	

Figure 15. REST API for User Profile.

API-NAME	IssuerProfile			
DESC	배지 발행자에 대한 프로파일 정보 받기			
Request				
URL	http://54.180.6.77:8000/public/issuers/U2bhfn5tRcudD6Nj-z7p2Q			
Method	GET			
Headers	**Name**	**Type**	**Required**	**Desc**
	Authorization	User ID별 상이	REQUIRED	(아래 access token REST API로 받은 값)
	Content-Type	application/json	OPTIONAL	
Parameters	**Name**	**Type**	**Required**	**Desc**
	issuers	GET URL	REQUIRED	예 : BCLab1 의 경우 "U2bhfn5tRcudD6Nj-z7p2Q"
Response				
Entities	**Name**	**Type**	**Desc**	
		application/json	{ "@context": "https://w3id.org/openbadges/v2", "description": "123", "url": "http://www.bclab.com", "email": "cuteconference@gmail.com", "type": "Issuer", "id": "http://54.180.6.77:8000/public/issuers/U2bhfn5tRcudD6Nj-z7p2Q", "name": "BCLab1" }	

Figure 16. REST API for Issuer Profile.

API-NAME	Awarding Badge			
DESC	배지 이슈어가 특정 수신자에게 배지 수여하기			
Request				
	http://54.180.6.77:8000/v1/issuer/issuers/da6FtP03Qlaq1KBtHfxP0w/badges/31_cK9F9RHKt9LxyUEgSzA/assertions			
Method	POST			
Headers	**Name**	**Type**	**Required**	**Desc**
	Authorization	User ID별 상이	REQUIRED	(아래 access token REST API로 받은 값)
	Content-Type	application/json	OPTIONAL	
Parameters	**Name**	**Type**	**Required**	**Desc**
	issuers	GET URL	REQUIRED	예 : BCLab1 의 경우 "U2bhfn5tRcudD6Nj-z7p2Q"
	badges	GET URL	REQUIRED	예 : BCLab1 의 경우 "U2bhfn5tRcudD6Nj-z7p2Q"
Response				
Entities	**Name**	**Type**	**Desc**	
	blockchain 등록 후 extensions 필드에 transaction ID를 기록하여 리턴함	application/json	{ "created_at": "2019-02-06T17:54:32.877864Z", "created_by": "cuteconference@gmail.com", "slug": "STrAyLMDQuilNd4eoi2C5w", "image": "http://54.180.6.77:8000/media/uploads/badges/assertion-STrAyLMDQuilNd4eoi2C5w.png", "recipient_identifier": "cuteconference@gmail.com", "recipient_type": "email", "narrative": null, "evidence_items": [], "revoked": false, "revocation_reason": null, "expires": null, "hashed": true, "extensions": { "txidod": { "txid": "43da75618f02e59623e8c1a47ec1ee27abb12c17744f74a81993176ec92c3799" } }, "json": { "@context": "https://w3id.org/openbadges/v1", "type": "Assertion",	

Figure 17. REST API for awarding badges.

API-NAME	Get Access Token		
DESC	Access Token 받아오기		
Request			
Method	http://54.180.6.77:8000/o/token		
	POST		
Headers	**Name**	**Type**	**Required**	**Desc**
	Content-Type	application/x-www-form-urlencoded	OPTIONAL	
	...			
Parameters	**Name**	**Type**	**Required**	**Desc**
	grant_type	password	REQUIRED	
	client_id	public	REQUIRED	
	scope	rw:profile rw:issuer rw:backpack	REQUIRED	
	username	cuteconference@gmail.com	REQUIRED	
	password	koreatech1	REQUIRED	
Response			
Entities	**Name**	**Type**	**Desc**
		application/json	{ "access_token": "VcVwgYPxprymLXykJPNbOohyGMz5NC", "token_type": "Bearer", "expires_in": 86400, "refresh_token": "8pRhjftz4hFIARBDIKqbtH5uWOzm9I", "scope": "rw:profile rw:issuer rw:backpack" } 각 API 접속시 token-type+" "+access_token의 형태로 사용

Figure 18. REST API for access token requirement.

Ethereum blockchain provides EtherScan (http://etherscan.io) to search block information. In particular, Ropsten is a test network widely used by developers, and it also provides a home page for the Ropsten network (http://ropsten.etherscan.io). Therefore, it is possible to access the transaction information and inquire the corresponding transaction information.

As shown in Figure 19, we call the badge by issuing the REST API with POSTMAN, and the blockchain transaction ID in the extensions field is 0x98c400... txid. When calling the REST API, we need to list some arguments as headers. The first is the authorization key required for OAuth2 authentication. The second is the setting of the content type. The authorization key is issued through OAuth2 and is a valid key value only for a certain period of time. It is compatible with OAuth2; therefore, the user can log in using the login account and password of another system that uses Oauth2 (Twitter, Facebook, etc.) [27].

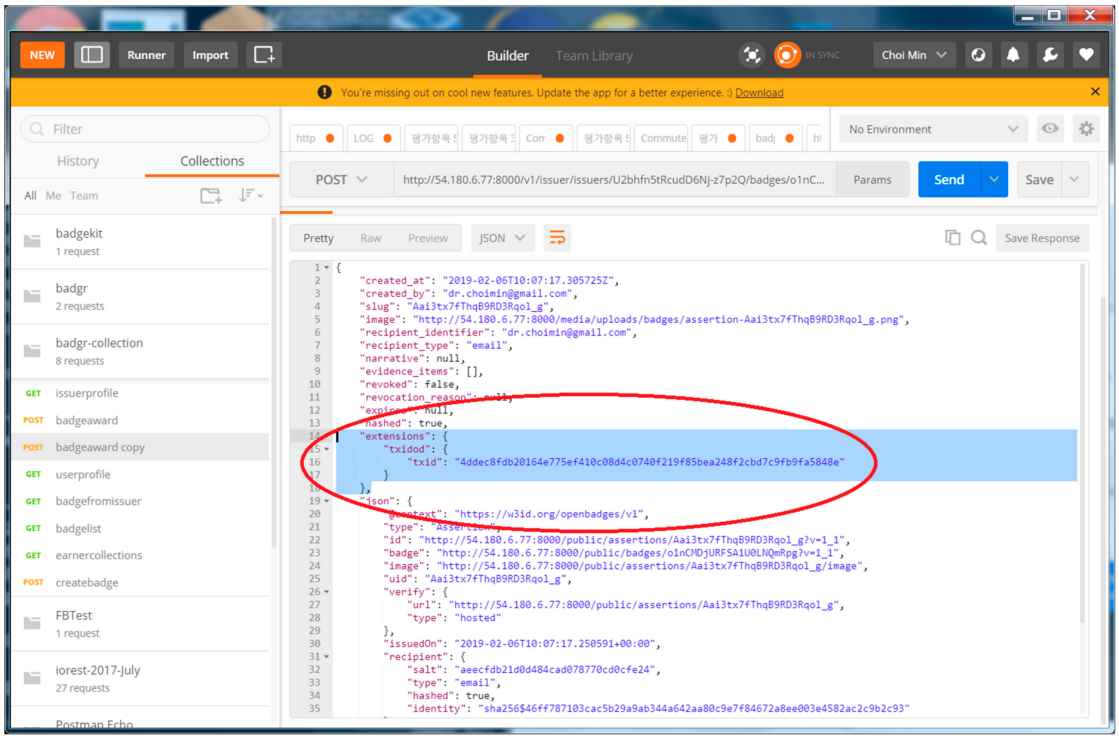

Figure 19. Extension field in result returned as JSON to digital badge award by REST API.

Figure 20 shows the transaction recorded in the Ethereum blockchain at the same time as the badge was issued. We provide the transaction id as the return value of the REST API for issuing the badge in this study. The id value is provided as an extension field of the return value of the bad issuing REST API. The following Figure 21 demonstrates badge issuance and verification on our developed platform. The first screen is the screen for badge award. Enter the information, such as the name, e-mail address, badge award condition, etc., of the badge recipient and press the Badge issue button. Then, as shown in the second screen, information on the issued badge is displayed. The third screen is used to share the badge with a third party after the badge is issued. It can be shared through social networking services such as Facebook, LinkedIn, and Twitter so on, through this menu [28].

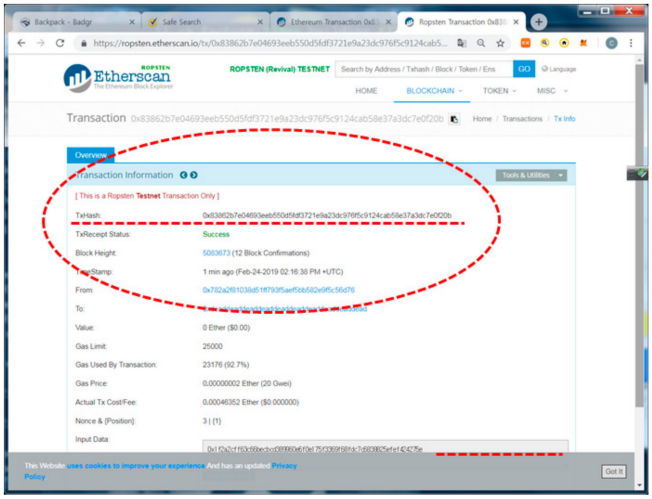

Figure 20. A Transaction example on Ethereum after blockchain based digital badge award.

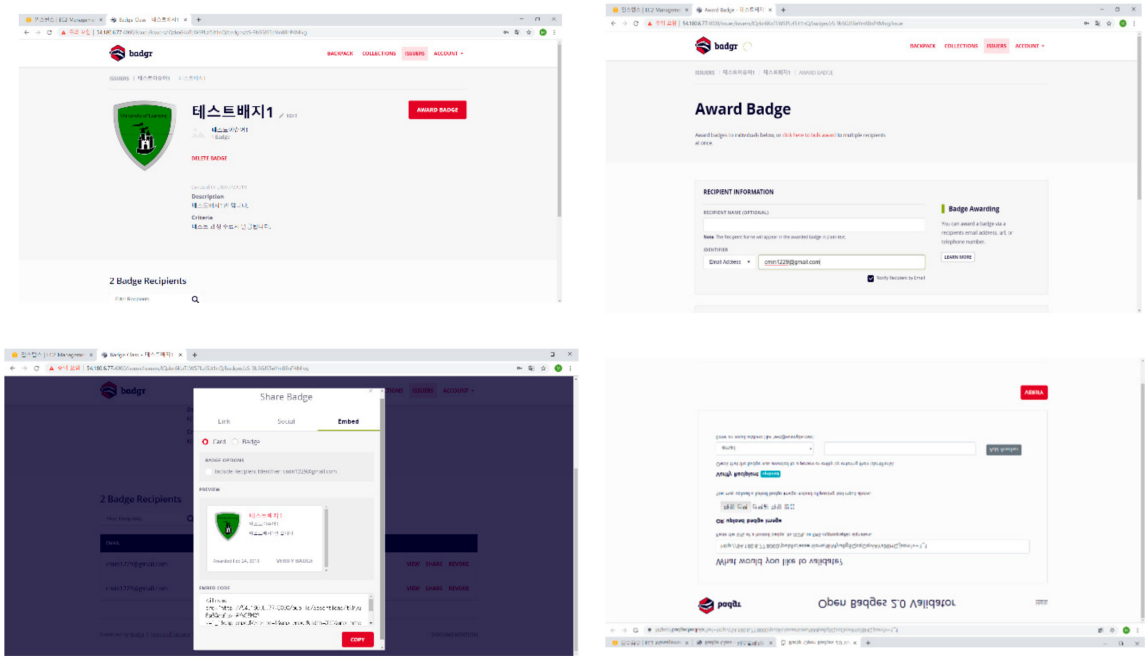

Figure 21. Badge award & validation (step 1).

The fourth figure shows the screen when the "VERIFY BADGE" button is pressed in the third figure. In order to validate the digital badge issued by our platform, we enter information about the path (URL) or image (PNG) of the badge, and the recipient of the badge. Actually, we input the badge path (URL) as http://websiteURL:8000/public/assertions/JuhSiPp6QzevLW9xCsaRYg.json?v=2_0. Then, we get as the following information about the badge.

{“@context”:”https://w3id.org/openbadges/v2”,”type”:”Assertion”,”id”:”http://websiteURL:8000/public/assertions/JuhSiPp6QzevLW9xCsaRYg”,”badge”:”http://websiteURL:8000/public/badges/zS-9bSGJS5eYm88nP4Mivg”,”image”:”http://websiteURL:8000/public/assertions/JuhSiPp6QzevLW9xCsaRYg/image”,”verification”:{“type”:”HostedBadge”},”issuedOn”:”2019-04-25T15:30:23.011305+00:00”,”recipient”:{“salt”:”adcb295ba30f46efaff73260df8cdb78”,”type”:”email”,”hashed”:true,”identity”:”sha256$beb816a75e389c1ed263943e605493665dd31314820dde7d8769b8ab409af611”},”txid”:{“txid”:”375656367231ce4cc9471dfe9cd322eb65fbf5163ee31a8ebe3b32598f1a56bd”}}

Figure 22. Badge assertion information.

This badge verification and validation is based on principles of easy testing of modular components and consistent patterns of interaction between those components. It relies on the Redux pattern from the ReactJS community. There are several important characteristics that together make for predictable operation and division of responsibilities: ① Single source of truth: There is one object tree that represents the entire state of the application. It is managed in a “store” and expressed in simple data types. ② This state is read-only and can only be modified by submitting “actions” that are handled by the store one at a time, always producing a new copy of the state. Because python variables are pointers to memory space, this makes for efficient storage and comparison. Actions are simple dicts with a “type” property. ③ The mechanism for changing state occurs through “reducers”, which inspect incoming actions and return a new copy of the portion of the state they oversee.

In order to verify the integrity of digital badges, Figure 23 shows that the validator must take input from the user, analyze that input, access the relevant badge resources, and ensure that each of them are well-formed and that they are linked together appropriately before packaging up the results and returning them to the user. This entails the ability to handle a wide variety of different inputs and configurations of badge resources. The validator keeps track of not only the badge data but also the processing tasks. All application state for a request is in a state object dict managed by a store created upon user input.

We implemented a blockchain platform to record the history of digital badges. Therefore, we can query the blockchain transaction history by using etherscan.io after issuing the badge. We can see the image shown in Figure 22 when we search a transaction with txhash value after a block time. The block time is ~12.6 s: it is the mean time required to propagate a new block across a vast majority of nodes in a P2P network. An Ethereum transaction is recorded into Ethereum’s blockchain faster than a Bitcoin transaction would be recorded into Bitcoin’s blockchain. (Bitcoin’s block time is roughly 10 min)

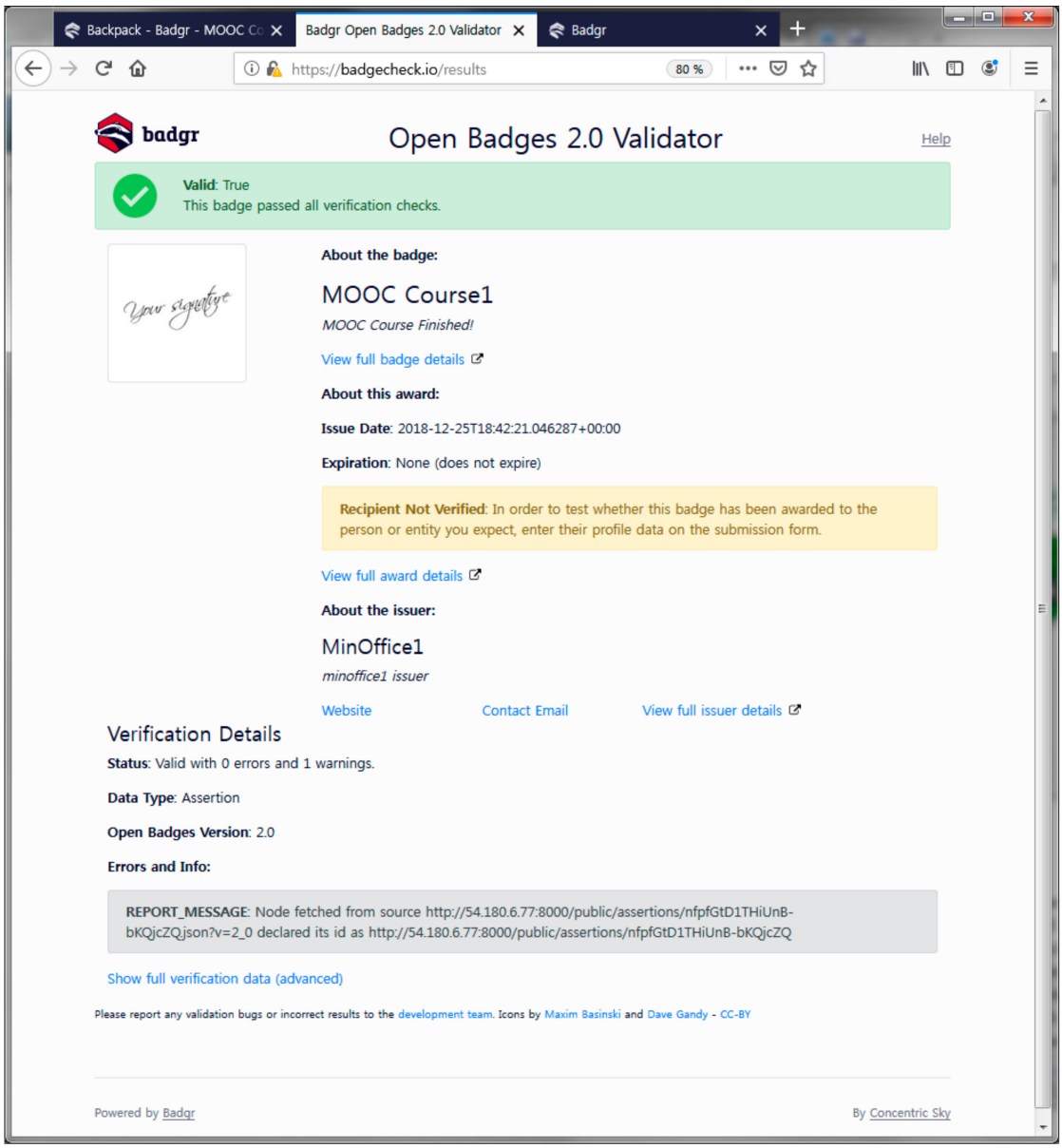

Figure 23. Badge award & validation (step 2).

5. Conclusions

Our system implementation is compatible with Open Badges of IMS Global Learning Consortium, which is used to earn, issue, and award badges across various platforms. The badges are trusted by the IMS standard, the criteria to earn a badge is verified through the network, and the overall process is transparent compared to traditional education systems. Moreover, all badge awarding events in our system are recorded into a blockchain. This is one of the most distinguishing features of our system with other systems. Once the badge award information stored in blockchain, the contents cannot be tampered with. Thereafter, anyone can check the validity of the badge through the blockchain.

The results of the test evaluation are as follows. On a Bitcoin-based digital badge publishing platform, the execution time required to award the badge is 24.53 s, while on the Ethereum-based digital badge publishing platform, the execution time it takes to award the badge is only 3.86 s.

This research can be utilized for certificate issuance and management of educational and training courses. It is applicable to online and offline educational and training courses conducted by the Ministry of Labor. The education and training courses are divided into microlearning units, and students who

have completed them can receive digital badges. The certificate issuance requirements for large units of education and training courses, such as courses or degrees, are made up of digital badges of appropriate microlearning units for each certificate and can be issued when these requirements are met. The issued digital badge can be registered in the blockchain. This research can also be used for career management using e-portfolio. The digital badge acquired by individual students is collected and managed by the e-portfolio. Each collected history can be viewed by other organizations or individuals who need it, but with the student's permission. By analyzing the collected information, future plans can be developed for each student, which can be utilized for employment and career guidance. Point-based royalty rewards program can also be realized using tokens. The royalty rewards system can be operated according to the instructor's discretion in order to improve educational effectiveness. In this way, we can use a token issued by a blockchain as a point. Royalty points can be rewarded to encourage student participation in learning activities during education and training programs. Thus, the students can substitute a part of the tuition fee with the royalty points.

Author Contributions: M.C., R.S., S.-C.O., and O.-Y.K. conducted a comprehensive research of Blockchain-based Badge Award with Existence Proof. All authors read and approved the final manuscript.

Funding: This research was supported by project for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Ministry of SMEs and Startups, grant number S2599713, in 2018 and supported by the National Research Foundation, grant number NRF-2017R1E1A1A01075128.

Acknowledgments: This work was jointly supported by project for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Ministry of SMEs and Startups, grant number S2599713, in 2018 and was supported by the strategic research project of the National Research Foundation (NRF) by grant number NRF-2017R1E1A1A01075128.

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

References

1. Shanti Bruyn, A. Blockchain an Introduction. 26 August 2017. Available online: https://beta.vu.nl/nl/Images/werkstuk-bruyn_tcm235-862258.pdf (accessed on 8 June 2019).
2. Rizzo, P. World Economic Survey 2015. 24 September 2015. Available online: https://www.coindesk.com/world-economic-forum-governments-blockchain (accessed on 8 June 2019).
3. Das, S. The UK Treasury Is Embracing Block Chain, Digital Currencies and Big Data Research. Available online: https://www.ccn.com/the-uk-treasury-is-embracing-block-chain-digital-currencies-and-big-data-research (accessed on 8 June 2019).
4. Oscar Williams-Grut, Santander is experimenting with bitcoin and close to investing in a blockchain startup. Available online: https://www.businessinsider.com/santander-has-20-25-use-cases-for-bitcoins-blockchain-technology-everyday-banking-2015-6?r=UK (accessed on 8 June 2019).
5. Mikroyannidis, A.; Domingue, J.; Bachler, M.; Quick, K. Smart Blockchain Badges for Data Science Education. In Proceedings of the IEEE Frontiers in Education Conference (FIE), San Jose, CA, USA, 3–6 October 2018.
6. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. October 2000. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 8 June 2019).
7. Mikroyannidis, A.; Domingue, J.; Bachler, M.; Quick, K. A Learner-Centred Approach for Lifelong Learning Powered by the Blockchain. In Proceedings of the World Conference on Educational Media and Technology, Amsterdam, The Netherlands, 25 June 2018; pp. 1403–1408.
8. Issuing Open Badges. Available online: https://openbadges.org/get-started/issuing-badges/ (accessed on 8 June 2019).
9. Surf.net, Whitepaper on Open Badges and Micro-Credentials. Available online: https://www.surf.nl/files/2019-06/Whitepaper-on-open-badges-en-micro-credentials.pdf (accessed on 8 June 2019).
10. Chen, S.; Shi, R.; Ren, Z.; Yan, J.; Shi, Y.; Zhang, J. A Blockchain-Based Supply Chain Quality Management Framework. In Proceedings of the 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), Shanghai, China, 4–6 November 2017; pp. 172–176.

11. Mikroyannidis, A.; Domingue, J.; Bachler, M.; Quick, K. Smart Blockchain Badges for Data Science Education. In Proceedings of the 2018 IEEE Frontiers in Education Conference (FIE), San Jose, CA, USA, 3–6 October 2018. [CrossRef]
12. #1 Job Site in the World. Available online: https://www.indeed.com/ (accessed on 8 June 2019).
13. Searching Jobs Around the World. Available online: https://jooble.org/ (accessed on 8 June 2019).
14. For a Better World. Available online: https://www.xing.com (accessed on 8 June 2019).
15. The Best Place to Start Your Job Search. Available online: https://www.adzuna.com/ (accessed on 8 June 2019).
16. Mikroyannidis, A.; Domingue, J.; Bachler, M.; Quick, K. Learner-Centred Approach for Lifelong Learning Powered by the Blockchain. In Proceedings of the EdMedia: World Conference on Educational Mediaand Technology, Amsterdam, The Netherlands, 25–29 Jun 2018; Association for the Advancement of Computing in Education (AACE): Waynesville, NC, USA, 2018; pp. 1403–1408.
17. Mewburn, I.; Blackmore, K.; Freund, K.; Rutherford, E.; Jenks, H. *INSIGNIA—Digital Badges for Research Education*; Final report; The Australian National University: Canberra, ACT, Australia, 2016.
18. UC Davis's Digital Badge. Available online: http://www.econovill.com/news/articleView.html?idxno=267288 (accessed on 8 June 2019).
19. Cisco's Digital Badge System. Available online: https://learningnetwork.cisco.com/docs/DOC-32253 (accessed on 8 June 2019).
20. Swarm and IBM's Open Badge. Available online: https://www.swarmapp.com; https://www-304.ibm.com/services/learning/ites.wss/zz-en?pageType=page&c=M425350C34234U21 (accessed on 8 June 2019).
21. Microsoft Exam and Certification Badge. Available online: https://www.microsoft.com/en-us/learning/badges.aspx (accessed on 8 June 2019).
22. Moubarak, J.; Filiol, E.; Chamoun, M. On blockchain security and relevant attacks. In Proceedings of the 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM), Jounieh, Lebanon, 18–20 April 2018; pp. 1–6. [CrossRef]
23. Aloqaily, M.; Kantarci, B.; Mouftah, H.T. On the impact of quality of experience (QoE) in a vehicular cloud with various providers. In Proceedings of the 2014 11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies (Photonics for Energy), Charlotte, NC, USA, 15–17 December 2014; pp. 94–98. [CrossRef]
24. BLOCKCERTS The Open Standard For Blockchain Credentials. Available online: https://www.blockcerts.org/guide/ (accessed on 8 June 2019).
25. Baking. Available online: https://www.w3.org/TR/PNG/#11iTXt (accessed on 8 June 2019).
26. Bitcoin Developer Documentation. Available online: https://bitcoin.org/en/developer-examples#testnet (accessed on 8 June 2019).
27. Halpin H.; Piekarska, M. Introduction to Security and Privacy on the Blockchain. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, 26–28 April 2017; pp. 1–3.
28. Aloqaily, M.; Kantarci, B.; Mouftah, H.T. Introduction to Security and Privacy on the Blockchain. In Proceedings of the 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB), Montreal, QC, Canada, 4–7 October 2015; pp. 1–5.