J Inf Process Syst, Vol.15, No.3, pp.707~716, June 2019
https://doi.org/10.3745/JIPS.03.0121

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Design of Recruitment Management Platform Using Digital Certificate on Blockchain

Won-Yong Jeong* and Min Choi*

Abstract

In this paper, we present a certificate management platform for performance assessment during recruitment using blockchain. Applicants are awarded certificates according to a predetermined level of progress based on their performances. All certificates are stored on a recruitment management platform that serves as an environment for storing and presenting all awarded certificates. The hashed information of all the certificates are stored in the blockchain, and once stored, the contents cannot be tampered with. Therefore, anyone can check the validity of the certificates using this blockchain. Our proposed platform will be useful for recruitment and application management, career management, and personal history maintenance.

Keywords

Applicants Capability Verification, Blockchain, Digital Certificate, Recruitment Platform

1. Introduction

Blockchain technology is used as a base technology because it makes use of distributed and decentralized databases. There is no centralized control over the system. Further, it is highly secured due to the use of SHA-256 cryptographic hash algorithm [1]. During the polls conducted in 2015, the World Economic Forum survey revealed that there will be a tipping point from the government for the use of blockchain by 2023 [2]. Governments, large banks, software vendors, and companies involved in stock exchanges, especially the Nasdaq Stock Market, have been investing heavily in this area. For example, the British Government has recently announced that it will be investing £10 million for blockchain research [3]. On the other hand, Santander has identified 20–25 internal use cases for this technology and predicts a reduction in banks' infrastructure costs by up to £12.8 billion per year [4].

A blockchain is linked by blocks and each block can hold approximately 1 MB data. In the bitcoin network, a block typically contains timestamp, transactions, and hash of previous blocks. However, for the educational network, the block holds course credit, assignment, skills, etc. All students and teachers will be able to see the skills of each student. The students can demonstrate their skills by referencing Mozilla backpack websites that contain all the acquired certificates. These certificates are compatible with most of the Internet platforms and can be shared on the Internet, such as social media. In this research,

Manuscript received May 17, 2019; first revision June 10, 2019; accepted June 12, 2019.

Corresponding Author: Min Choi (cmin1229@gmail.com)

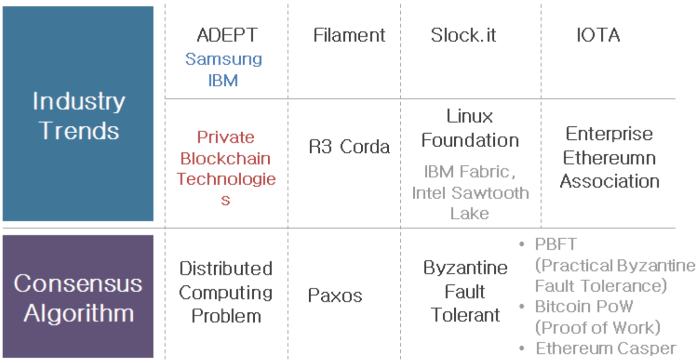
* School of Information and Communication Engineering, Chungbuk National University, Cheongju, Korea (cwell@realcoding.co, cmin1229@gmail.com)

for issuing a certificate and verifying it, we make use of the recruitment management platform. Until now, a certificate in the recruitment platform was considered only to be a trust relationship between two parties. This means that chains of trust and networks of trust have not been created yet. However, in this paper, we extend and implement the trust relationships among all participants in a distributed environment of blockchain with the following criteria.

(1) Elimination of the inefficiency and social cost problems associated with various certificate issuing systems: The existing information system show inefficiency and inconvenience in case of some education and public institutions' certificate issuing system. There are costs involved with issuing certificates, transcripts, and diplomas for online and offline education and training courses. To resolve these problems, we provide a technique for certification creation/issue/award system using simple representational state transfer (REST) APIs.

(2) Difficulties in managing subdivided qualifications: The proposed system can be used to establish a recruitment management platform. We focus on issuance and management of competency unit certificates as an authentication method for detailed education and training courses.

(3) Establishment of effective management system for individual education and career history of applicants: We establish a backpack system to acquire and manage the experiences and achievements of official and informal activities of individuals, apart from offline education and training. In this way, our proposed method establishes a system that officially certifies the collected information, such that the information can be used for future learning and career planning.



Industry Trends	ADEPT Samsung IBM	Filament	Slock.it	IOTA
	Private Blockchain Technologies	R3 Corda	Linux Foundation IBM Fabric, Intel Sawtooth Lake	Enterprise Ethereumn Association
Consensus Algorithm	Distributed Computing Problem	Paxos	Byzantine Fault Tolerant	• PBFT (Practical Byzantine Fault Tolerance) • Bitcoin PoW (Proof of Work) • Ethereum Casper

Fig. 1. Industry trends and consensus algorithms in field of blockchain.

In Fig. 1, we have categorized the existing researches on blockchain field and have discussed the advantages and disadvantages of them. We will try to simplify the blockchain platforms by examining the cases that have been studied by various industries. First, we consider a platform called Africa-Europe Diaspora Development (ADEPT) [5] that is developed by IBM and Samsung. There is also a platform called Filament. ADEPT and Filament in Fig. 1 are applicable for Internet of Things (IoT) environment with a blockchain. The R3 Corda platform introduces a novel concept when it comes to a consensus algorithm. This allows a large number of people to jointly validate a certification or a document. In R3 Corda [6], one does not necessarily have to share all the ledgers with others. However, it is a concept that is present in our proposed idea. Therefore, R3 Corda places a part of the ledger on the chain and also places a part of the ledger off-chain as well. Further, in terms of consensus algorithms, this is one of the key things a blockchain platform must have. Therefore, any blockchain platform must adopt one of the several existing consensus algorithms. We usually use a lot of algorithms such as proof-of-stake (POS) [7] and proof-of-work (POW) [8]. Practical Byzantine Fault Tolerance (pBFT) [9] provides a way to improve the existing POW or POS limitations. Also, various approaches such as Paxos can solve the existing performance limitations. When we look at the process of establishing transactions among these individuals on a blockchain platform, we will always have to compare them with the existing ones. In the past, I used to use the blockchain, which made me feel better. In the past, we used a lot when we were doing transactions called transactions.

In the past, we would need to digitally sign using an X.509 certificate when performing transactions, such as card payment. The reason behind this was to prevent the denial of the payment and to ensure legal protection of non-repudiation. This way the person would not be able to deny that he or she signed once it has been signed using the certificate. This has allowed many individuals to perform transactions committed onto blockchain. However, as we use the blockchain platform, the participants in the multiple blockchains, which are composed of multiple participants, in our case, peers, jointly examine the individual transactions and determine the transaction behavior in a distributed environment.

Using the blockchain based digital certification, we can facilitate and offer accreditation or personalized recommendations for learners who study data science courses. Learners who study various data science subjects earn digital certifications upon reaching certain milestones during their studies, e.g., completion of a part of a course or the entire course. Learners get job recommendations based on full or partial matches with the geographical location. For example, companies wish to find applicants that matched with the companies in terms of geographical location, capabilities, and digital certifications. With the use of the proposed method, everything is displayed on the dashboard. Partial matching jobs are displayed with the corresponding course recommendations. Taking up these recommended courses can help one completely match for a particular job. Fig. 1 shows in detail popular blockchain frameworks.

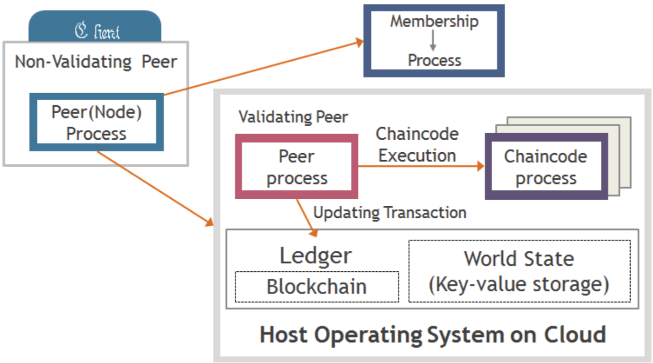


Fig. 2. Hyperledger blockchain architecture and smart contracts.

Fig. 2 outlines the structure of the IBM's Hyperledger Fabric platform. It is a platform developed by IBM and distributed in an open source form. For the Hyperledger platform, a distributed P2P (peer-to-peer) environment is adopted allowing several peers to participate. The system consists of a non-validating peer, a validating peer, and a membership process. A non-validating peer does not participate in the validation and verification process for the block in which the transaction is generated, instead the validating peer is responsible for this verification. Therefore, the validation of the ledger for the distributed ledger is performed by a number of validating peers. It also consists of an application execution program called Chaincode that can perform a smart contract. For the implementation of the Chaincode, we can use either Go language or Java language. When the transaction occurs, the data is stored in the distributed ledger. This Hyperledger platform is also classified as a consortium blockchain. It is possible to operate this blockchain platform in a kind of closed structure. So, there is a membership process for member management as well.

Next, let us take a look at the ethereum virtual machine (EVM) platform structure and ethernet platform. The EVM platform basically adopts a distributed P2P-based environment. In terms of the language used for implementing smart contracts, we offer a separate program language called Solidity. This is called the EVM. It is a kind of virtual machine that can compile and deploy smart contract codes developed using Solidity to run smart contracts. So, it acts as a smart contract on the EVM, and also gets the smart contract executed. The EVM platform will be a form of stacking machine among the existing traditional computer architectures. In other words, we have a stack structure in memory that can be used for data operations. We place the operands for computation into the stack structure using the push operation. The stacked architecture operates by taking out the topmost two operands on the pushed stack, performing the operations, and putting the results on the stack again. The machine executes the computation using these operands and puts the calculated results into the stack. There is a code area, where the program is placed, and a storage area. There is also a stack area, which is a parameter area used for data sharing with the outside world. Further, there are additional extras that contain information such as call data.

In the later section, we provide implementation of the platform in detail using the Open Badges specification [10]. This technology makes application management possible leading to lifelong learning possibility for applicants. Applicants will be able to show their certificates virtually to the recruiters. The recruiters will be able to understand the candidate's skills in detail. In this research, we focus on designing a framework where any organization can issue certificates such that the certificate recipients can reveal it to highlight their skills. In the proposed platform, everyone will get an opportunity to share their knowledge though a social networking system. In this paper, the experimental details will be explained under the experiment section. Nowadays, recruitment is still controlled by companies, institutes, or administrative authorities that offer quality, credibility, and knowledge. This current model is not flexible for all applicants because of constraints related to time, money, and distance. To make recruitment and application process easy and flexible along with increased trustworthiness, we will establish an educational network based on blockchain technology.

2. Blockchain Based Digital Certification for Recruitment

In this section, we will describe the detailed architecture and implementation of the digital badge platform based on blockchain technology. It consists of the following major components or steps: certificate issue, certificate repository, distributed storages in the form of blockchain, and verification. In this research, a recruitment management platform, which is compatible with the Open Badges specification [10], is used as an underlying platform for our digital badge system. The most important information to be described are the dates of certificate creation, certificate-type(class), criteria, issuer, name, description, and so on. Certificate creation should be preceded by certificate awarding for digital certificate issuing.

Each student has a wallet application that can hold a digital certificate. An institution issues a digital certificate if the student meets certain conditions for receiving the certificate. At this time, public key cryptography is used to sign the certificate of the personalization agent. Therefore, in the future, it remains possible to verify whether the certificate issued by the corresponding personalization agent was correct or not. Initially, to issue a digital certificate, a certificate should be created. The institutions generate certificate assertion and digital signature through public key cryptography. The digital certificate issuer delivers an image to the recipient (or pushes it to the recipient's backpack account). The recipient decides whether to receive and disclose the corresponding digital certificate present in his or her backpack. Digital certificate recipients can view or manage the digital certificate they have bought (backward compatibility according to IMS Global Learning Consortium).

In Fig. 3, the blockchain is a platform where a particular person implements a transaction by telling a second party how much he or she wants to transfer to a third party. At this point, if he or she does any specific action, the transaction chain is observed to see what kind of state changes occur in the blockchain. First, he or she assumes that the transaction is made to a friend. To do that, he or she must know the address of the friend. The friend must possess a wallet to receive the initiated payment. To obtain this, we would need to check the friend's wallet address. The address is obtained through QR code or email address. Next, the sender can write down his or her address when the transfer is done. So, one's the friend's address is obtained, the sender needs to write something that he or she would like to transfer. Then, when the sender presses the transfer button on the computer screen or smartphone, he or she will be transferred from the blockchain platform. In this process, the blockchain platform first writes down the initiated transfer. Next, it signs with the private key of the sender. Signing with a private key means encrypting it with a private key in the public key cryptosystem. When signed with the private key, the transaction is propagated on the blockchain network. Subsequent transactions must be approved by the blockchain miners for the transactions to be committed in real.

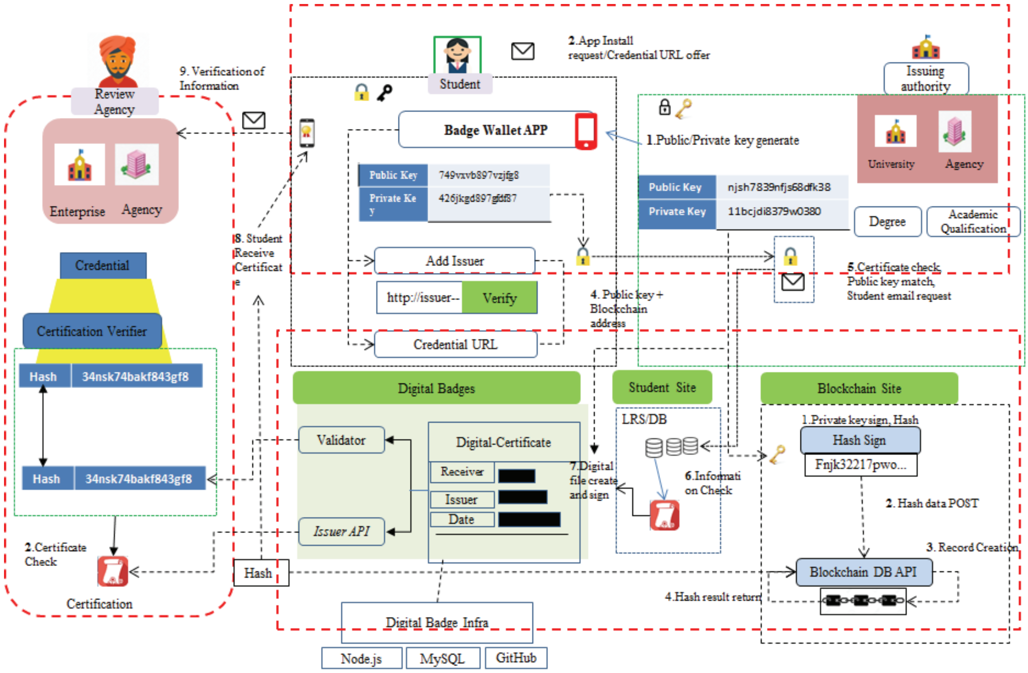


Fig. 3. System architecture.

In this research, we use two basic platforms, as shown in Fig. 4. The first is the blockchain servers including Bitcoin and Ethereum platforms, and the second is the Blockcerts platform for managing the digital certificate generated through the blockchain. The generated digital certificate is managed via a distributed repository. These digital certificates 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. We can make use of one of these two methods to distinguish assertion information: host type and signed type. The consensus algorithm deals with determining and confirming the block. For this, POW is the most familiar and widely used method. When one proves that he or she has done a particular amount of work through several hash operations, it means that he or she has found a value that otherwise cannot be found without running the hash multiple times. The result proves that one did a reasonably good job of finding the right value.

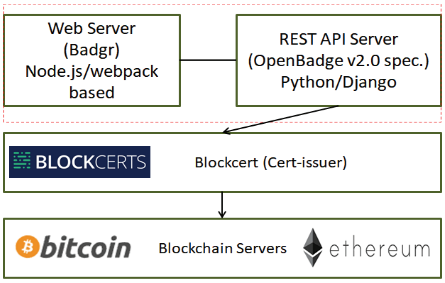


Fig. 4. JSON for digital badge based on OpenBadge specification and JSON for digital badge based on OpenBadge specification with blockchain.

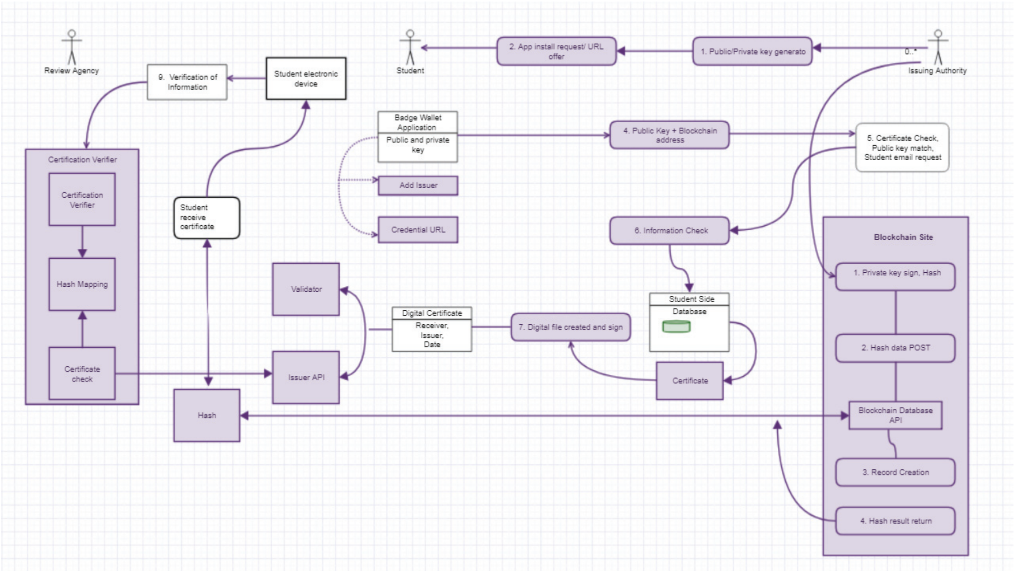


Fig. 5. Flow chart of digital badge award on our system implementation.

Fig. 5 shows the flow chart of the platform operation developed in this study. In the figure, digital certifications are issued to the student by an issuing authority and the issuing authority also records the generation of blockchain transactions. Backpack is a certificate repository, the original concept of which was proposed by Mozilla.

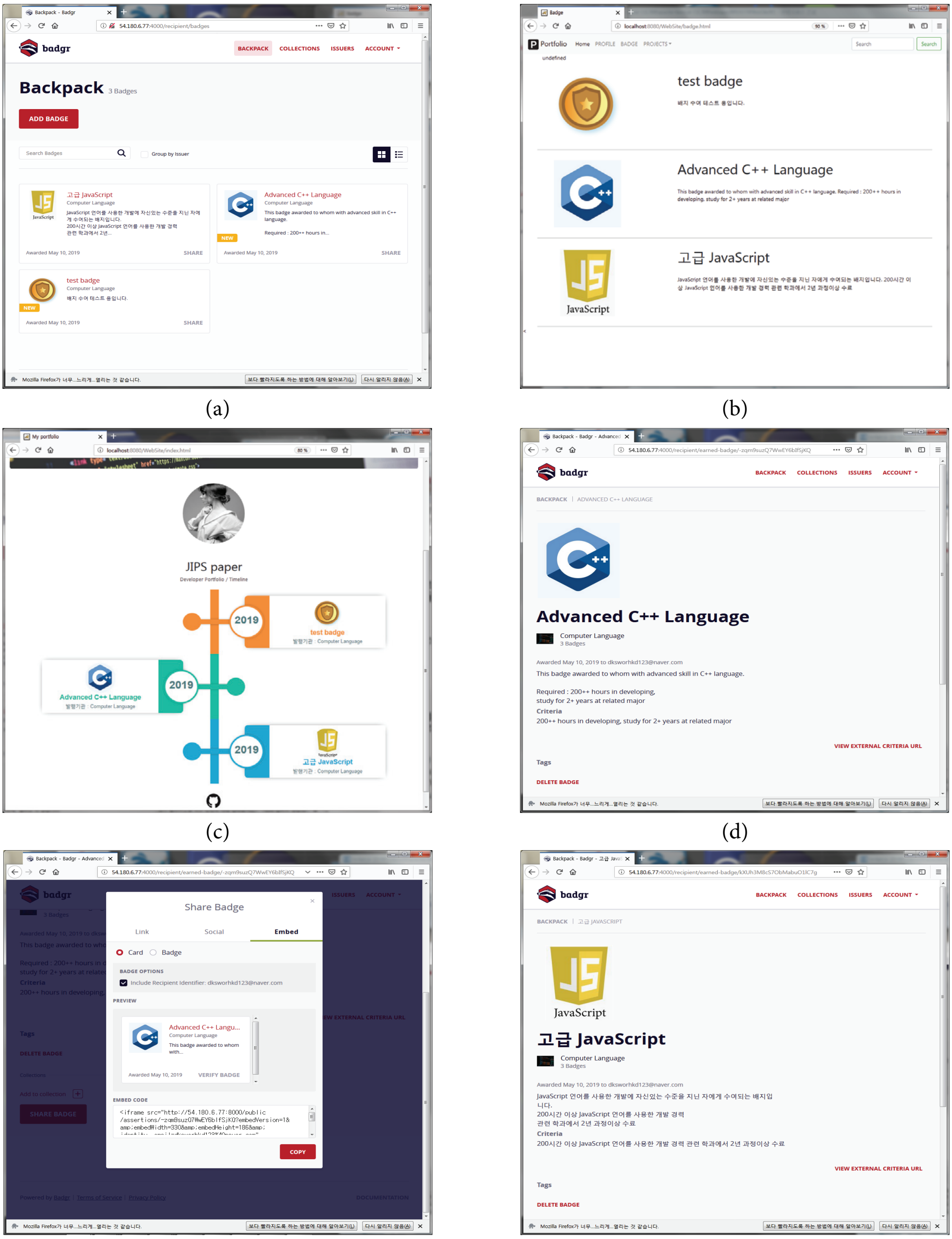
Digital certifications are verified by the verifier on blockchain in regression test mode for Bitcoin and in Ropsten test network for Ethereum networks. The regression test mode for bitcoin is used to establish a new blockchain with private control but has the same rules as a public bitcoin network. This mode is especially used for research and development purpose, where the set of 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 for becoming an issuer. To issue a digital badge we just need a technology platform that is compatible with Open Badges specification.

3. Experimental Results

In this research, we implemented a digital certification issuance and backpack management platform with blockchain Ethereum and Bitcoin support. It provides a digital badge issuance in conjunction with blockchain during badge issue API. After certificate issue, our system provides a transaction ID, txid, in the response of the certificate issuing API as extensions field. Ethereum blockchain provides the EtherScan (http://etherscan.io) to search block information. In particular, Ropsten is a test network widely used by developers, and also provides a homepage for the Ropsten network (http://ropsten.etherscan.io). Therefore, it is possible to access the transaction information and inquire the corresponding transaction information.

In this research, we call the certificate by issuing REST API with POSTMAN and that the blockchain transaction ID in the extensions field is 0x0204400... 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 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, so you can log in using the login account and password of another system using OAuth2 such as Twitter or Facebook. The transaction can be recorded in the Ethereum blockchain at the same time as the certificate was issued. We provide the transaction id as the return value of the REST API for issuing the certificate in this study. The id value is provided as an extension field of the return value of the bad issuing REST API. Fig. 6 demonstrates certificate issuance and verification on our developed platform. The first screen is the screen for certificate award. After entering the information such as the name, e-mail address, certificate award condition, certificate recipients, users press the certificate issue button. Then, as shown in the second screen, information on the issued certificate is displayed. The third screen is used to share the certificate with a third party after the certificate is issued. It can be shared through social networking services such as Facebook, LinkedIn, Twitter, and so on. Fig. 6(d) shows the screen when the "VERIFY" button is pressed in the third figure. In order to validate the digital certificate issued by our platform, we enter information about the path (URL) or image (PNG) of the certificate, and the recipient of the certificate. Then, we get as the following information about the certificate.

This certificate verification 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. (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.



고급 JavaScript
Computer Language
JavaScript 언어를 사용한 개발에 자신있는 수준을 지닌 자에게 수여되는 배지입니다.
200시간 이상 JavaScript 언어를 사용한 개발 경력 관련 학과에서 2년...
Awarded May 10, 2019

Advanced C++ Language
Computer Language
This badge awarded to whom with advanced skill in C++ language.
Required : 200++ hours in...
Awarded May 10, 2019

test badge
Computer Language
배지 수여 테스트 용입니다.
Awarded May 10, 2019

(a)

test badge
배지 수여 테스트 용입니다.

Advanced C++ Language
This badge awarded to whom with advanced skill in C++ language. Required : 200++ hours in developing, study for 2+ years at related major

고급 JavaScript
JavaScript 언어를 사용한 개발에 자신있는 수준을 지닌 자에게 수여되는 배지입니다. 200시간 이상 JavaScript 언어를 사용한 개발 경력 관련 학과에서 2년 과정이상 수료

(b)

My portfolio
localhost:8080/WebSite/index.html
JIPS paper
Developer Portfolio / Timeline
2019
test badge
발행기관 : Computer Language
2019
Advanced C++ Language
발행기관 : Computer Language
2019
고급 JavaScript
발행기관 : Computer Language

(c)

Backpack - Badgr - Advanced
54.180.6.77:4000/recipient/earned-badge/-zqm9suzQ7WwEY6bIfSjKQ
badgr
BACKPACK
COLLECTIONS
ISSUERS
ACCOUNT
BACKPACK | ADVANCED C++ LANGUAGE
VIEW EXTERNAL CRITERIA URL
Tags
DELETE BADGE

Advanced C++ Language
Computer Language
3 Badges
Awarded May 10, 2019 to dksworhkd123@naver.com
This badge awarded to whom with advanced skill in C++ language.

Required : 200++ hours in developing,
study for 2+ years at related major
Criteria
200++ hours in developing, study for 2+ years at related major

(d)

Backpack - Badgr - Advanced
54.180.6.77:4000/recipient/earned-badge/-zqm9suzQ7WwEY6bIfSjKQ
Share Badge
Link
Social
Embed
PREVIEW
EMBED CODE
COPY
VERIFY BADGE
SHARE BADGE
Add to collection
Collections
Powered by Badgr | Terms of Service | Privacy Policy
DOCUMENTATION

● Card ○ Badge

BADGE OPTIONS
☑ Include Recipient Identifier: dksworhkd123@naver.com

Advanced C++ Langu...
Computer Language
This badge awarded to whom with...
Awarded May 10, 2019

```
<iframe src="http://54.180.6.77:8000/public
/assertions/-zqm9suzQ7WwEY6bIfSjKQ?embedVersion=1&
amp;embedWidth=330&amp;embedHeight=186&amp;
```

(e)

Backpack - Badgr - 고급 Java
54.180.6.77:4000/recipient/earned-badge/kXUh3M8cS7ObMabuO1lC7g
badgr
BACKPACK
COLLECTIONS
ISSUERS
ACCOUNT
BACKPACK | 고급 JAVASCRIPT
JavaScript
VIEW EXTERNAL CRITERIA URL
Tags
DELETE BADGE

고급 JavaScript
Computer Language
3 Badges
Awarded May 10, 2019 to dksworhkd123@naver.com
JavaScript 언어를 사용한 개발에 자신있는 수준을 지닌 자에게 수여되는 배지입니다.
200시간 이상 JavaScript 언어를 사용한 개발 경력
관련 학과에서 2년 과정이상 수료
Criteria
200시간 이상 JavaScript 언어를 사용한 개발 경력 관련 학과에서 2년 과정이상 수료

(f)

Fig. 6. Screenshots of our system implementation: (a) description and list about issued/awarded digital certifications on API server, (b) awarded digital certifications listed on our recruitment management server, (c) time-lined view of awarded digital certifications for an applicant on our recruitment management server, (d) detailed description for a digital certification on our recruitment management server, (e) digital certification verification functionality on API server, and (f) detailed description for another digital certification on our recruitment management server.

4. Conclusion

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 certificate 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 website developed through this study provides the following functions. Applicants can maintain evidence of their personal competence through a digital backpack. Applicants will upload evidence documents such as TOEIC, certificates, coursework certificates, and short-term lecture attendance certificates to the blockchain-based platform built through this study. The interviewer of the company can verify on the basis of the block chain by accessing the website constructed through this research on the supporting documents and supporting documents attached to the application form. In this way, applicants are convenient to manage and submit application documents. Interviewers can conveniently verify the supporting documents submitted by applicants on a blockchain basis.

Acknowledgement

This work is supported by the Basic Science Research Program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (No. NRF-2017R1E1A1A01075128).

References

[1] A. Shanti Bruyn, “Blockchain: an introduction,” 2017; https://beta.vu.nl/nl/Images/werkstuk-bruyn_tcm235-862258.pdf.

[2] A. Mikroyannidis, J. Domingue, M. Bachler, and K. Quick, “A learner-centred approach for lifelong learning powered by the blockchain,” in *EdMedia+ Innovate Learning*. Waynesville, NC: Association for the Advancement of Computing in Education, 2018, pp. 1388-1393.

[3] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, “Blockchains everywhere: a use-case of blockchains in the pharma supply-chain,” in *Proceedings of 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, Lisbon, Portugal, 2017, pp. 772-777.

[4] A. Mikroyannidis, J. Domingue, M. Bachler, and K. Quick, “Smart blockchain badges for data science education,” in *Proceedings of 2018 IEEE Frontiers in Education Conference (FIE)*, San Jose, CA, 2018, pp. 1-5.

[5] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, “A blockchain-based supply chain quality management framework,” in *Proceedings of 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE)*, Shanghai, China, 2017, pp. 172-176.

[6] H. Halpin and M. Piekarska, “Introduction to security and privacy on the blockchain,” in *Proceedings of 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Paris, France, 2017, pp. 1-3.

[7] M. Aloqaily, B. Kantarci, and H. T. Mouftah, "A generalized framework for quality of experience (QoE)-based provisioning in a vehicular cloud," in *Proceedings of 2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, Montreal, Canada, 2015, pp. 1-5.

[8] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," in *Proceedings of 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*, Jounieh, Lebanon, 2018, pp. 1-6.

[9] M. Aloqaily, B. Kantarci, and H. T. Mouftah, "On the impact of quality of experience (QoE) in a vehicular cloud with various providers," in *Proceedings of 2014 11th Annual High Capacity Optical Networks and Emerging/Enabling Technologies (Photonics for Energy)*, Charlotte, NC, 2014, pp. 94-98.

[10] "Issuing Open Badges: why issue Open Badge," 2016; https://openbadges.org/get-started/issuing-badges/.

Won-Yong Jeong https://orcid.org/0000-0002-8131-1593

He received the B.S. degree in Computer Science from Kwangwoon University, Korea, in 2009. From 2005 to 2014, he worked at Entaz where the mobile game developer and publisher as a CTO. At 2015 he had been a faculty member of Department of Entrepreneurship Education Center of Wonkwang University. Since 2016 he set up a company that name is Realcoding that has made coding education software. His current research interests include coding education software, blockchain, and machine learning.

Min Choi https://orcid.org/0000-0002-8031-1022

He received the B.S. degree in Computer Science from Kwangwoon University, Korea, in 2001, and the M.S. and Ph.D. degrees in Computer Science from Korea Advanced Institute of Science and Technology (KAIST) in 2003 and 2009, respectively. From 2008 to 2010, he worked for Samsung Electronics as a Senior Engineer. Since 2011 he has been a faculty member of Department of Information and Communication of Chungbuk National University. His current research interests include blockchain, high performance computing, cloud computing, interconnection network, and embedded computing.