Block-Chain Applied Management System for Student Data: Enhancing Accessibility and Security

Su Min Kim
dept. information system
Hanyang University
Seoul, Korea
smjy9502@naver.com

Chul Woo Park
dept. information system
Hanyang University
Seoul, Korea
tthoutan@gmail.com

Jae Yeon Shin
dept. information system
Hanyang University
Seoul, Korea
jaeyeon.shin.96@gmail.com

Jong Won Oh
dept. information system
Hanyang University
Seoul, Korea
jongwon9978@gmail.com

***Abstract*—Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency. In 2017, Blockchain based cryptocurrency has attracted the world's attention as an investment asset. However in 2018, the industry is active with attempts to differentiate and improve efficiency by combining Blockchains with diverse businesses not only limited to cryptocurrency. Various fields, such as smart keys to control cars, automated payment systems, digital medical certifications, financial transaction history sharing and etc, have already adopted or planning to adopt Blockchain technology. The interest in Blockchain technology keeps increasing. The reason for the interest in Blockchain is its central attributes that provide security, anonymity and data integrity without any third party organization in control of the transactions. We propose Block-Chain Applied Management System for Student Data which can simplify current process of checking student data and assure reliability of data. We write student's informations into ledger as one of transaction information. This transaction information then spread to nodes that are distributed in Blockchain network. By adopting distributed ledger technology, we can minimize time and cost that has been wasted and delete unnecessary procedure.**

***Index Terms*—blockchain, smart contract, solidity, ethereum, software engineering, distributed ledger**

TABLE I
ROLE ASSIGNMENTS

Roles	***Name***	***Task description and etc.***
User	Shin Jae Yeon	look for function that is needed, scheduling, test software
Customer	Kim Su Min	search for libraries, compare with other similar works, test software
Software developer	Park Chul Woo	develop based on requirements, improve software quality
Development Manager	Oh Jong Won	check requirements, specify design and customer's needs

I. INTRODUCTION

A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer-to-peer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world.

The advantages of Blockchain technology outweigh the regulatory issues and technical challenges. One key emerging use case of blockchain technology involves "smart contracts". Smart contracts are basically computer programs that can automatically execute the terms of a contract. When a pre-configured condition in a smart contract among participating entities is met then the parties involved in a contractual agreement can be automatically made payments as per the contract in a transparent manner.

Blockchain technology is finding applications in wide range of both financial and non-financial areas. Financial institutions and banks no longer see blockchain technology as threat to traditional business models. The world's biggest banks are in fact looking for opportunities in this area by doing research on innovative blockchain applications. In a recent interview Rain Lohmus of Estonia's LHV bank told that they found Blockchain to be the most tested and secure for some banking and finance related applications.

Non-Financial applications opportunities are also endless. We can envision putting proof of existence of all legal documents, health records, and loyalty payments in the music industry, notary, private securities and marriage licenses in the blockchain. By storing the fingerprint of the digital asset instead of storing the digital asset itself, the anonymity or privacy objective can be achieved.

In this paper, We propose Blockchain applied management system for student data, new system for inquiring and proving student certificate without complicated process. Our proposal can minimize time and cost that has been wasted.

We focused on two main problems. First, complexity and needlessness of current system's process. Current inquiry and proof system of student data works as follows: the student's information can be checked on the server of the school and downloaded in the form of a document. In the downloaded

document, the date of issuance and the identification number are provided to prove the validity of the document. However, after issuing the document, there is a problem that it is possible to manipulate the grades and the degree by using identification number and etc. Therefore, the scholarship foundations or companies that require the information such as students' grades, degree, enrollment information and etc inquiring information back to school again.

Second, security issue. Thanks to improved server security, it is extremely rare for a student to access a server and manipulate information such as grades, attendance and etc., but we could not say it is absolutely impossible. In addition, data can be lost if the server is attacked. This problem can arise because the server of the school storing the student's data is a single point of failure. In order to eliminate such a single point of failure, it can be solved through a strategy of duplicating or distributing duplicates or triplets. However, in order to take such a strategy, it takes a lot of costs such as security staff, security equipment and so on.

Our Blockchain applied management system for student data uses distributed ledger technology which is also a core concept of Blockchain. We intend to list the student's information (grades, proof of attendance, degrees, etc.) in the ledger as a single transaction information. The transaction information described above is propagated to a large number of nodes distributed in a Blockchain network through the characteristics of a Blockchain called a large distributed public ledger. Through this process, students' information on the Blockchain ledger is intended to be reliable enough information without any special evidence process.

The process by which the information recorded on the Blockchain records is obtained is as follows. The hash value of the transaction information is used as an input value in the calculation of the merklehash of the block containing the transaction, and the merklehash is used as the input value in the calculation of the block hash. The calculated block hash value is stored as the value of previousblockhash of the next block. Therefore, if any transaction information is changed, the merklehash of the merge tree containing the transaction information is changed and the block hash is changed as the value is changed. In this case, the value of previousblockhash of the block having the previous block as the block needs to be updated. In other words, to maintain the chain, the value of previousblockhash must be updated, the nonce value must be obtained again, and a new block hash must be obtained, and the value of the connected block hash must be newly calculated. In this way, all subsequent blocks must be remined from the block where the transaction information was changed. It takes an average of 10 minutes to mine a block, so if a malicious node changes the transaction information of the immediately preceding block, the good nodes continue to block the original block chain in which the transaction information has not been changed, so that after 10 minutes, the length of the bad chain of the malicious node becomes shorter than the length of the block chain held by the other good nodes And the shortest length (the block chain generated by the malicious node) is discarded at the moment when two block chains are encountered.(Due to the fact that, if a branching chain chain collides, more work proofs are performed to select blocks of longer length) By using structural characteristic of Blockchain, it can guarantee credibility just because it is written in distributed ledger in Blockchain.

As our final goal is to make students and the place where needs certificate comfortable. Just clicking our service can simplify lots of steps than before.

The paper is organized as follows. Section 2 lists all the requirements. Section 3 discusses the related works.

II. Requirements

A. Blockchain Network environment

- implement in cloud based environment by using 'Amazon Web Service'

B. Private Blockchain Network

- implement private Blockchain network which can decide participation of node through central administrator
- use Java based Solidity
- smart contract based on ethereum

C. Web based application

- place web based application on top of private blockchain platform where smart contract is built in
- user(student, school, enterprise HR department) can easily utilize service without knowing blockchain or certain language
- simply designed GUI
- reason for developing web based application is because most of authenticating student information works are done in web environment.
- after web service is made, change to hybrid web to provide application service

D. Sign up function

- send request to become a node
- can be signed up when central administrator give access to Blockchain network
- after get permission to join blockchain network, make ID and password

E. Log-in function

- log-in to system with ID and password that was made at sign up stage
- has function to find forgotten ID and password
- if log-in is successful, we can access to blockchain network and main page of our program
- if log-in fails for 5 times, we cannot get into network and also we need to get reauthentication.

F. Main Page

- section for grade certificate
- section for proof of enrollment
- section for certificate of degree
- have mypage section where we can change our personal data such as ID, password and etc.

G. Section for grade certificate

- inquire into grade information
- has print button to make copy of certificate
- has save button to download in document format file

H. Section for proof of enrollment

- inquire into enrollment information
- has print button to make copy of certificate
- has save button to download in document format file

I. Section for certificate of degree

- inquire into degree information
- has print button to make copy of certificate
- has save button to download in document format file

J. My page

- function to change password
- shown only when user is log-in

K. Composition of Blockchain network

- central administrator: student service center in University
- node that store decentralized ledger that contains student informations: College of Engineering, College of Liberal Arts, College of Social Science, College of Business and etc.
- participants: students, enterprises HR manager (who wants to verify applicant's information), scholarship foundation (request student's grade information for state scholarship)
- as network is private, it doesn't need mining process which can have possibility to provide much faster speed

L. Front-end

- make it work well to get along with back-end server
- follow current portal system's design factor, but differentiate in GUI based on user's environment and experience
- use HTML, CSS, JAVASCRIPT to design web page and get input and send it to server

M. Back-end

- use JAVASCRIPT to implement
- use web.js,api to make data connection between smart contract and web application
- web application server is built in cloud or in local by installing Node.js

III. Related Works

As Blockchain technology has potential power, There are lots of attempts to adapt Blockchain technology in various fields. Especially, it can be applied as a replacement of current authentication method. There are several examples that are similar to our works.

A. Chain SIGN

Chain SIGN is a first blockchain based contract platform made by blockchain platform specialized company 'TheRoof' and document management specialized company 'Cyberdime'. This is a new contract platform that assure trust by adding blockchain technology into original electronic contract system. It can have same effect with notarization in current electronic contract.

B. EduCTX

This platform is based on the concept of the EuropeanCredit Transfer and Accumulation System (ECTS). It constitutes a globally trusted, decentralized higher education credit, and grading system that can offer a globally unified viewpoint for students and higher education institutions (HEIs), as well as for other potential stakeholders, such as companies, institutions, and organizations. As a proof of concept, they present a prototype implementation of the environment, based on the open-source Ark Blockchain Platform. Based on a globally distributed peer-to-peer network, EduCTX will process, manage, and control ECTX tokens, which represent credits that students gain for completed courses, such as ECTS. HEIs are the peers of the blockchain network. The platform is a first step toward amore transparent and technologically advanced form of higher education systems. The EduCTX platform represents the basis of the EduCTX initiative, which anticipates that various HEIs would join forces in order to create a globally efficient, simplified, and ubiquitous environment in order to avoid language and administrative barriers

C. New Blockchain Management System for Student Learning Data Developed by Sony

Sony Corporation and Sony Global Education, a Sony subsidiary focused on global educational services, has developed a new platform for student education records based on Blockchain technology. The new solution will allow school administrators to consolidate and manage educational data for students in several schools, as well as record and refer to their learning history and digital transcripts with greater certainty. It will be developed with IBM Blockchain, and will use blockchain technology running on the IBM Cloud to track students' learning progress, as well as to establish transparency and accountability of school achievement among students and schools. The platform will provide students with a digital and reliable record of their achievements that can be easily and quickly verified by any future employer or educational institutions. The data recorded on the platform is verified using IBM Blockchain and can be shared with stakeholders, including school administrators and prospective employers.

D. MEDIBLOC

MEDIBLOC is a project to solve current medical information system by using blockchain technology. It returns medical information that has been spread through each medical center. MEDIBLOC's goal is to create a world where individuals, medical providers, and medical researchers all enjoy a new

medical experience by ensuring that medical information is securely distributed around individuals.

E. CHAIN ID

CHAIN ID issues a joint certificate through the consensus of the nodes (participants) in the network. The joint certificate is already authenticated through the consensus of the nodes and can be used freely throughout the network without any additional authentication. The smart contracts will guarantee the integrity of the data, ensuring that the certificate is trustworthy and without the risk of being altered. The information and status of the certificate is shared among the nodes in real-time so that all the participants will have the same information. By all the nodes having the same data, CHAIN ID can prevent single points of failure, such as hacking attempts that may happen in centralized network environments. Using CHAIN ID, users can experience a more convenient and reliable environment for making financial transactions.

F. BankSign

Customers who use Bank Sign can obtain a joint certificate from one bank, and they can easily use the mobile banking service of the other bank with simple authentication. The customer renewed the certificate every year when using the bank service and had to go through the registration and authentication process for each bank. However, Bank Sign makes it easy to access banking services from multiple banks at once. The authentication method has also been improved with convenience passwords, fingerprints, and patterns. The Bank Sign prevents the forgery of the certificate through the distributed agreement, which is a characteristic of the blockchain, and the synchronization of real-time authentication information between the banks. In addition to security, the block hain has increased security by encrypting communication segments and double-encrypting data and networks. This enhanced security has increased the validity period of the joint certificate from one year to three years.