BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
MINISTRY OF INFORMATION AND COMMUNICATIONS
POSTS AND TELECOMMUNICATIONS INSTITUTE OF TECHNOLOGY

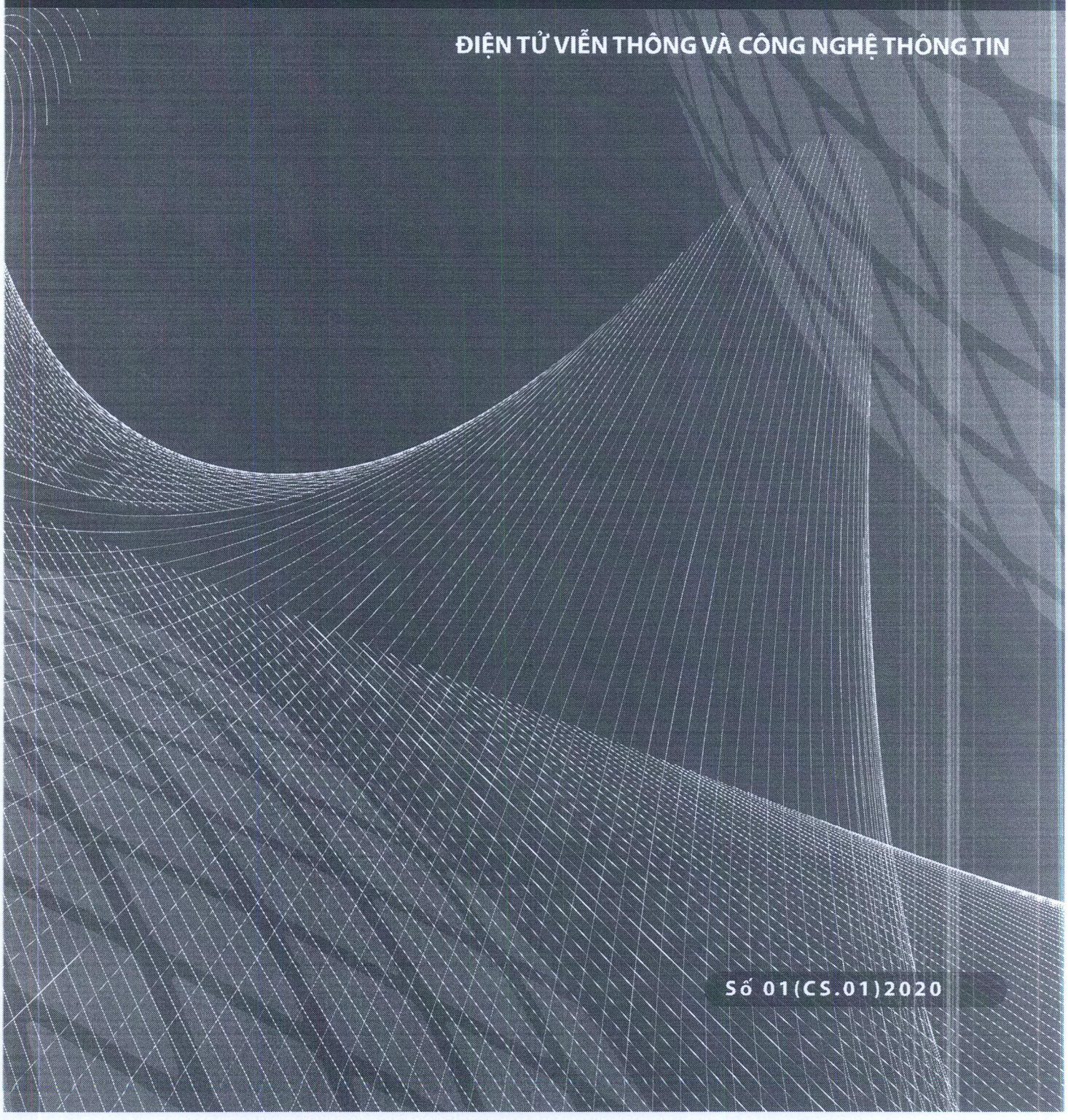
ISSN 2525 - 2224

TẠP CHÍ KHOA HỌC CÔNG NGHỆ

THÔNG TIN VÀ TRUYỀN THÔNG

JOURNAL OF SCIENCE & TECHNOLOGY ON INFORMATION AND COMMUNICATIONS

ĐIỆN TỬ VIỄN THÔNG VÀ CÔNG NGHỆ THÔNG TIN



Số 01(CS.01)2020

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
MINISTRY OF INFORMATION AND COMMUNICATIONS
POSTS AND TELECOMMUNICATIONS INSTITUTE OF TECHNOLOGY

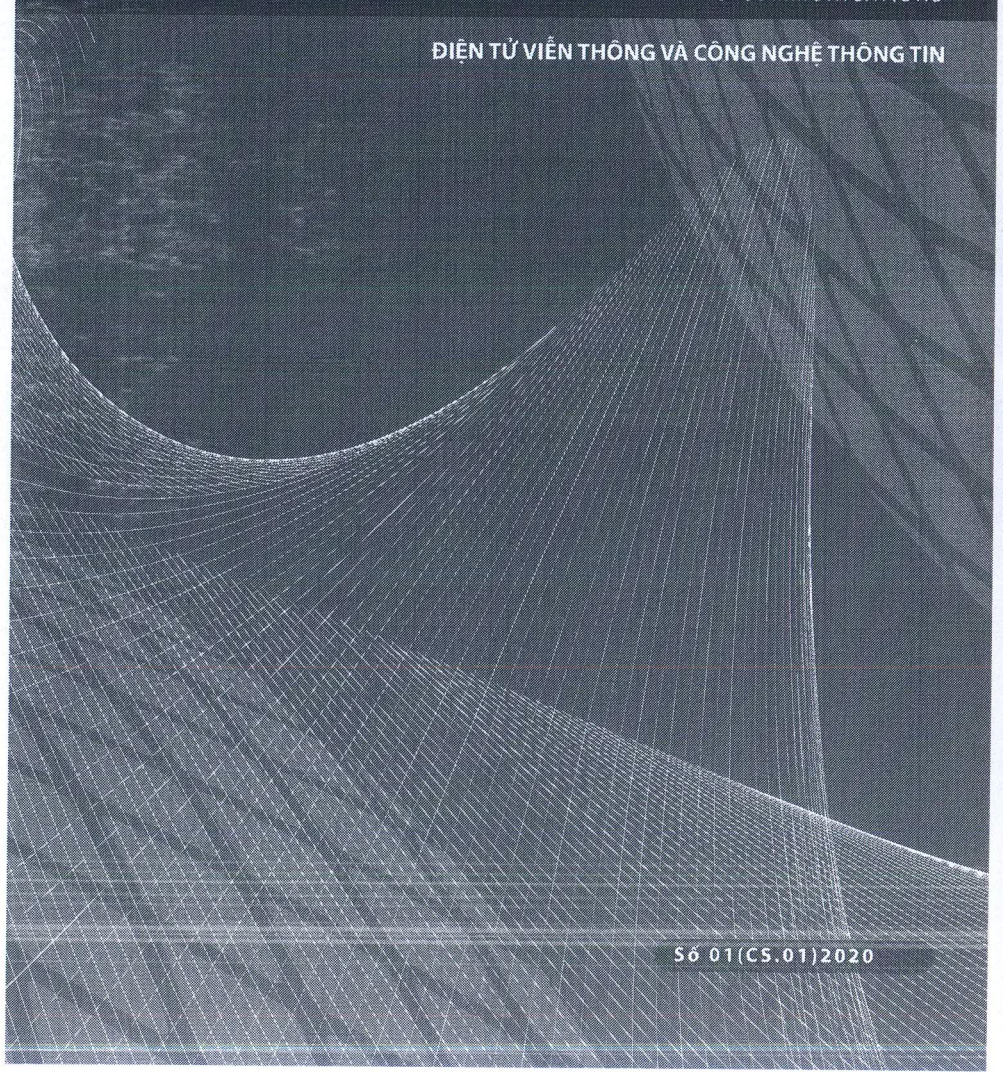
ISSN 2525 - 2224

TẠP CHÍ KHOA HỌC CÔNG NGHỆ

THÔNG TIN VÀ TRUYỀN THÔNG

JOURNAL OF SCIENCE & TECHNOLOGY ON INFORMATION AND COMMUNICATIONS

ĐIỆN TỬ VIỄN THÔNG VÀ CÔNG NGHỆ THÔNG TIN



Số 01(CS.01)2020

TẠP CHÍ KHOA HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG Số 01(CS.01)2020

TẠP CHÍ KHOA HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Journal of Science and Technology on Information and Communications

Tạp chí Khoa học công nghệ Thông tin và Truyền thông" là tạp chí chuyên ngành có phản biện độc lập, được xuất bản thường kỳ nhằm công bố các kết quả nghiên cứu khoa học và công nghệ trong các lĩnh vực đào tạo và nghiên cứu khoa học của Học viện, phục vụ công tác đào tạo, nghiên cứu khoa học của cán bộ, giảng viên, nghiên cứu viên, nghiên cứu sinh, học viên cao học và sinh viên ở trong và ngoài Học viện.

Giấy phép xuất bản số 697/GP-BTTTT ngày 21/12/2015

Tòa soạn: Tầng 1, Nhà A1, Học Viện Công nghệ Bưu chính Viễn thông, Km10, Nguyễn Trãi, Hà Đông, Hà Nội
Trang web: http://jstic.ptit.edu.vn/index.php/jstic
Email: jst@ptit.edu.vn

Journal of Science and Technology on Information and Communications (JSTIC) is a scientific journal periodically published by Posts and Telecommunications Institute of Technology (PTIT). The goal of the JSTIC is to publish peer reviewed practical and theoretical research papers in the various fields of Information and Communications. We welcome diverse innovative participation of local and international researchers to build a sustainable and high quality scientific journal.

Publication permit No. 697/GP-BTTTT issued Dec. 21, 2015

Editorial office: Floor 1, Posts and Telecommunications Institute of Technology, Km 10, Nguyen Trai Street, Ha Dong, Ha Noi
Website: http://jstic.ptit.edu.vn/index.php/jstic
Email: jst@ptit.edu.vn

TẠP CHÍ KHOA HỌC CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Journal of Science and Technology on Information and Communications

MỤC LỤC/CONTENTS

BLOCKCHAIN APPLICATION IN AUTHENTICATING HIGH-SCHOOL STUDENTS' TRANSCRIPT

Cong Hung Tran[1], Dien Tam Le[2], Hieu Le Ngoc[3], Thi Xuan Dinh Ho[4]
[1] Posts and Telecommunications Institute of Technology
[2] Thu Duc Technology College
[3] Ho Chi Minh City Open University
[4] Saigon University

Abstract: After completing the High School program, students are received school reports issued by the school where they completed their high school program, and the students get the hard copies of study reports (i.e. certificates, degree, paper of academic transcripts). Therefore, making fake transcripts for illegal purposes can be done easily, quickly and at low cost. In this paper, we propose a model of authenticating student-transcript system based on Blockchain network. This proposal system uses smart contracts to build a Private Blockchain network based on Ethereum platform, to build decentralized applications - Decentralized Application (dApp), distributed file systems IPFS (Interplanetary File System) .... with these will generate the hash value for each transcript/scoreboard. The hash value of the scoreboard file (file hash) will be stored on the Blockchain network and used in the process of validating the student's scoreboard/transcript quickly and accurately, avoiding the fake scoreboard. With the testing results of hundreds of transcript, that we can easily check the transcript whether true or fake with 100% correction. We can make sure of the accuracy of verification using Blockchain and its application. The testing is still limited but we can extend more, open a very potential perspective of verifying students' study result.

Keywords: Blockchain, IPFS, dApp, Ethereum, Smart contract, high-school transcript.

I. INTRODUCTION

Currently, student wants to enroll in vocational schools, intermediate schools, colleges, ... or they want to apply for a job in companies, enterprises they need to back up the paper of transcript and related documents together from the authentication of the local education department of the government or School (where the student's original transcript is issued) or a notary office certifying the copy is valid. The process of backing up and validating transcripts in traditional way as mentioned above is a manual, complicated and time-wasting process. In the process of authenticating the transcript in the traditional way as mentioned above, the agencies and organizations tasked with authentication may miss cases of fake transcripts. At that time, those cases may have the opportunity to use for illegal purposes. [1]

The use of Blockchain technology for the purpose of storing transcripts will contribute to eliminating the possibility of counterfeiting transcripts. Blockchain technology helps to store distributed data and data stored on the Blockchain network is almost impossible to modify.

In this paper, we try to solve two main problems: firstly, to build a Private Blockchain network based on

Contact author: Tran Cong Hung,
Email: conghung@ptithcm.edu.vn
Arrival: 04/2020, Revised: 04/2020, Accepted: 04/2020

Ethereum, using the POA - Proof of Authority consensus protocol. The second is building a Decentralized Application (dApp) that provides services and interfaces for users to interact with the Blockchain network. The content of the paper is divided into 6 sections: Part I – introduction; Part II - the basic theoretical basis; Part III - the related research works; Part IV - the proposed model and Algorithms; Part V - experiments and results assessment; Part VI - conclusions and recommendations.

II. BACKGROUND

A. Authentication - authenticate user data.

Authentication [2] is the act of authenticating an object, incident, or someone to be trusted. Authentication usually depends on one or more authentication factors to prove it. Data validation is the process of determining the origin and integrity of data. Data validation has two elements: the authentication that you are receiving data from the exact entity and the integrity of that data.

B. Blockchain

Blockchain concept

According to the "Mastering Bitcoin" edition of author Antonopoulos, Blockchain is defined as a technology that stores and transmits information by blocks linked together by coding and extending over time. Each block contains initialization information, transaction information, and is linked to previous blocks via hash information.

Classification

Based on several criteria, the Blockchain system is divided into 3 main categories: [3]

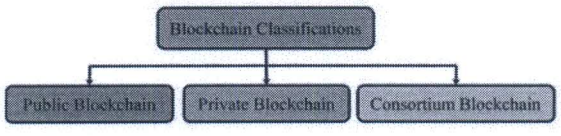


Figure 1: Classification of Blockchain system [3]

- *Public Blockchain:* A public Blockchain provides an open platform for everyone and all organizations. All participants are empowered to read, write data, transact, perform checks or review any part of the Blockchain system. The typical type of this Blockchain system are cryptocurrencies. For example: Bitcoin, Ethereum…
- *Private Blockchain:* This is a Blockchain system established to facilitate the sharing and exchange of private data of a group of individuals (within an organization) or between multiple organizations. It is also known as the Permissioned Blockchain because users cannot arbitrarily access the system unless they receive an invitation. For example, Ripple is a form of Private Blockchain.
- *Consortium Blockchain:* Nodes in the system are predefined and responsible for consensus and authentication of newly created blocks. To authenticate blocks, a multi-signature system is used, a block is considered valid when it is verified by the signatures of the nodes in the system. For example, banks or joint venture financial institutions will use their own Blockchain.

Blockchain characteristics

- *Decentralization - distributed data:* Consensus algorithms in Blockchain are used to maintain the consistency of data in a distributed network.
- *Persistency - immutability:* It is almost impossible to delete or restore transactions once they are included in the Blockchain.
- *Anonymity - Privacy:* Each user can interact with the Blockchain with an address, without revealing the user's identity. The information and data in Blockchain chains are dispersed and absolutely safe, only the holder of the Private Key can access that data.
- *Auditability - Transparency:* Transactions can easily be verified and monitored. Anyone can follow the path of data in Blockchain from address to address and can statistics the entire history on that address.

C. Consensus Algorithm Proof of Authority – POA [4]

This algorithm selects nodes to verify transactions based on the reputation of nodes in the network, so it is suitable for Private Blockchain. Nodes with high reputation (authority) will be chosen as Miner nodes to verify transactions. This will encourage network users to maintain their reputation and limit illegal activities. PoA can be considered as a variant of PoS in which reputation plays a role as a deposit asset. However, because this

model has the disadvantage of a decentralized model and the validation rights belong to several selected nodes. Therefore, the ability to entice reputable users to perform illegal actions is possible.

D. Ethereum - smart contract [5]

In 2015, the Ethereum Blockchain was born, allowing decentralized applications and smart contracts to operate on Blockchain. Ethereum can perform peer-to-peer transactions (p2p) through a virtual currency unit called Ether and is based on a PoW consensus mechanism. To put it simply, Ethereum provides the foundation for creating smart contracts and building distributed applications.

Smart contracts were first proposed by Nick Szabo in 1994. Smart contracts are self-executing contracts with terms agreed upon by the parties involved. The contract is written in the form of program code that exists on a decentralized blockchain network. Smart contracts allow transactions to be conducted anonymously and allow transactions between untrusted parties without the need for a third party.

Currently, Ethereum is one of the most popular platforms for developing smart contracts. In Ethereum, smart contracts are written in high-level languages such as Solidity, Serpent, LLL ... then compiled into bytecode for implementation on EVM. A Turing-complete virtual machine called the Ethereum Virtual Machine (EVM) is used to execute bytecode.

Solidity: is a procedural programming language with syntax like JavaScript, C ++ or java. The most common and commonly used language for writing smart contracts is created by Gavin Wood.

III. RELATED WORKS

In 2018, based on the concept of European Credit Transfer and Accumulation System (ECTS) - European credit accumulation and conversion system - and Blockchain technology, the article *"EduCTX: A blockchain-based higher education credit platform"* [6] proposed to develop a credit system for higher education and named it EduCTX. The ECTX platform is initially towards a more transparent and technologically advanced form of higher education systems. However, the installation and implementation are not extensive and only at the level of storing student credits by lecturers. This is an article with a good idea and opens a lot of prospects, especially showing the superiority of Blockchain.

In 2017, the article *"ECBC: A High Performance Educational Certificate Blockchain with Efficient Query"* [7] published in Springer magazine, author Yuqin Xu et al. Proposed a digital education certificate (Educational Certificate) based on Blockchain platform, called ECBC, can be used as an infrastructure for educational certificates, providing management and query services for educational certificates. With the ECBC proposal in this article, the experimental results do not include many practical cases, but open a great potential in Blockchain application to authenticate the user data, especially the data. whether the degree, certification number.

In the article *"Implementation of Fingerprint-Based Authentication System Using Blockchain"* [8] published in Springer Nature Singapore, in 2019, Dipti Pawade and the authors built a fingerprint-based biometric authentication system. Blockchain technology. The article has opened many methods and solutions to improve performance as well as accuracy and high security.

The article *"Blockchain Architecture to Higher Education Systems"* [9] proposed a Blockchain architecture for e-Learning solutions in education systems at a higher level. The proposed architecture called the Proof of Educational Transcript System (PETS) is evidence of the education transcript system. The paper has not developed an experiment for the system, but the application of Blockchain is potential and opens many prospects in the education system.

In the article *"An Efficient Traceable and Anonymous Authentication Scheme for Permissioned Blockchain"* [10], the author has designed an authentication scheme that can look up the operation history and anonymize authentication (without logging in) with the Highly secure and efficient using the

Permissioned Blockchain network. The experimental results show that the article has come up with a more efficient authentication scheme than previous studies and can be easily deployed in the Permissioned Blockchain network. The article asserts that Blockchain technology enhances the security and ability to authenticate users, validating user data accurately and effectively.

IV. PROPOSED MODEL

A. Model description

- ***Input:*** student's transcript file.
- ***Output:*** the status of the transcript querying from Blockchain network:
  - Transcript does not exist on the system.
  - Transcript already exists but not yet confirmed.
  - Transcript already exists and has been verified.

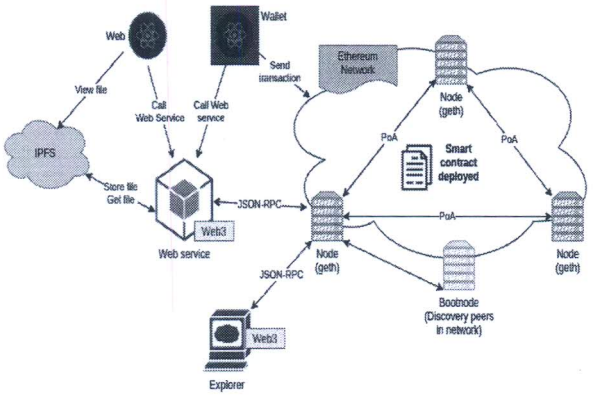


Figure 2: Overview model of the system

- ***Building Blockchain network:*** to build a Private Blockchain network using the Ethereum platform with a minimum of 3 Node nodes. The consensus protocol proposed for use in this blockchain network is the Proof of Authority (POA for short).
  - *Server 1 (Node1):* Acting as the Ethereum Sealer Node. In this model, we use the POA consensus rule, so that all blocks are mined (sealed) by the specified servers. Servers collect transactions, execute them, update their status and sign blocks using their private keys and use the public key to identify themselves on the system. network.
  - *Server 2 (Node 2):* functions like Server 1. Both of these servers are involved in signing transactions and contain a complete copy of the Blockchain network.
  - *Server 3 (Node 3):* Contributing to backup data of the Blockchain network without participating in the generation of the new block. Its backup process verifies (verifies) whether the newly received block is valid or not and updates the newly received block into its own ledger data. It will then broadcast the new block to the nodes adjacent to it.
  - *Boot-Node (Discovery peers in the network):* Through this boot-node, nodes can join the Private Blockchain network quickly. Boot-node has the function of helping nodes in the peer network to discover (search) each other. Nodes can have dynamic IPs but the boot-node is usually run on a static IP and thus acts like a public address where the node will find the node connecting to itself.
- ***Decentralized Application (dApp):*** These dApps are applications built and operated outside the Blockchain network. These dApps, including Web, Web service, Wallet, Explore, will provide services and interfaces for users to interact with the Blockchain network.
- ***Building of the Interplanetary File System (IPFS):*** Student transcripts in file format are managed and stored on a distributed IPFS – a distributed file system.

B. Functions of the system

- ***Upload record function:*** allows updating, storing information and status of transcripts on Blockchain network.
- ***Check record status function:*** allows checking the status of the transcript on the Blockchain network.
- ***View record function:*** allows you to view information about the student's transcript.
- ***Signup function:*** allows students to register student information (e.g. Using student code) and add teachers' Ethereum address to the Blockchain network.

C. User roles in the system

The construction system has 4 roles of users, including:

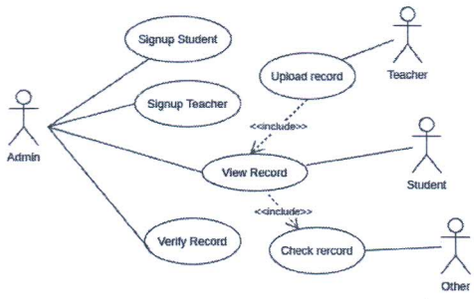


Figure 3: Users and roles in the system.

- ***Admin***: Admin has the highest role in the system, managing and affecting all data of the Blockchain network by using wallets to send transactions. Admin has the right:
  - Register to save new student code (Signup student).
  - Sign up to save the teacher's Ethereum address (Signup Teacher).
  - Verify student transcripts that exist in the Blockchain network (Verify record).
  - View the grades of any student (View record).
- ***Teacher***: The teacher has the right to add a new student transcript to the Blockchain.
- ***Student***: Students have the right to see their own points (View record).
- ***Other:*** are third parties outside the school system such as employers, intermediate schools, vocational training institutions…. The limited authority of Other users is only to check the status of students' transcripts on the Blockchain network (Check record).

D. Proposed algorithm

To approach the purpose of this paper, the proposed algorithm contains 3 componential algorithms: algorithm of updating record, algorithm of viewing record and algorithm of checking status of record.

Algorithm 1: Update record

- ***Input***: Student transcript of the file.
- ***Output:*** The Transaction Hash code indicates that the transcript was successfully updated.

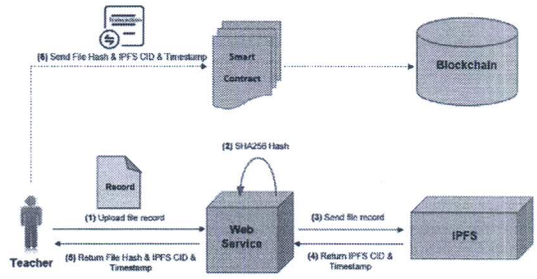


Figure 4: The process of updating the transcripts.

Steps of the algorithm:

- ***Step 1:*** The teacher uses a wallet to upload the student's transcript as a file to Web Service.
- ***Step 2:*** At the Web Service, the transcript will be encrypted using the SHA256 encryption algorithm. The result we get 1 hash value of that transcript file (File Hash). At the same time, the transcript file is also uploaded to the IPFS system. After successfully uploading the IPFS system, the Web Server will receive an Object which contains the IPFS code (IPFS CID) and information about when the transcript file was updated on the system (Timestamp). Web Services will return to users including File Hash, IPFS CID and Timestamp.
- ***Step 3:*** The user will save the information including File Hash, IPFS CID and Timestamp in the smart contract (Blockchain system) through the use of a wallet to create transactions and send it to the smart contract address with the method specified as *addGrade()*.
- ***Step 4:*** After sending the transaction successfully, the Blockchain system notices a hash segment called Transaction Hash. With this hash we can check the transaction information through Explorer.

Algorithm 2: View record

- ***Input***: The hash value of the transcript (file hash) and student code (StudentCode).
- ***Output:*** Include:
  - The IPFS path contains the URL record file.
  - Information on student transcript (imformation record) including date of updating the transcript on the system, student code.
  - Transcript status on Blockchain network.

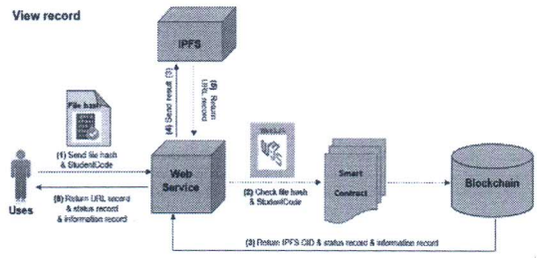


Figure 5: Diagram showing the process of viewing transcripts.

Steps of the algorithm:

- ***Step 1:*** User sends the hash value of the transcript (file hash) and student code (StudentCode) to the Web Service.
- ***Step 2:*** After receiving the file hash and StudentCode, Web Service via Web3.js to call get () function in the smart contract. The smart contract will match the StudentCode provided by the user with the StudentCode stored on the system, and check if the hash file of the transcript is corresponding to the StudentCode. If the conditions are met, the smart contract will return to the Web Service information including the IPFS CID, the hash file, the information of the transcript (Timestamp, StudentCode) and the status of the transcript (status record).
- ***Step 3:*** With the results returned from the smart contract, the Web Service will send to the IPFS system and the system will return the URL containing the transcript file (URL record), information of the transcript (Timestamp, StudentCode) and status record (status record).

Algorithm 3: Check the status of transcript

- ***Input***: Student transcript in file format.
- ***Output:*** The transcript status on the Blockchain network system (does not exist, already exists but has not been confirmed, already exists and has been confirmed).

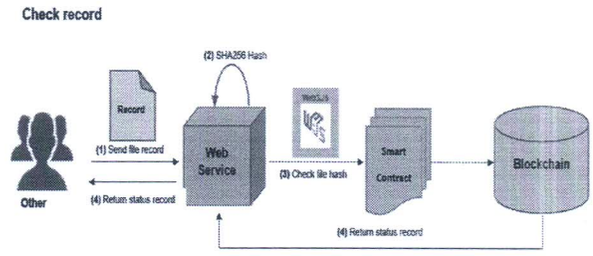


Figure 6: Diagram showing the process of checking transcripts status.

Steps of the algorithm:

- ***Step 1:*** Other users send the score file as a file to a Web Server.
- ***Step 2:*** At the Web Service, the transcript will be encrypted with 1 using SHA256 algorithm. The result we get 1 hash value of that transcript (file hash). With that hash file, Web Service via Web3.js to call the *checkGrade()* function in the smart contract to check the status of the transcript.
- ***Step 3:*** Return one of the following 3 states of the transcript:
  - Transcript does not exist if this hash file does not match any hash file already stored in the Blockchain system.
  - A transcript already exists but has not been authenticated if this hash file matches a hash file stored in the Blockchain system, but the corresponding scorecard has not been authenticated by the Admin.
  - The transcript already exists and has been verified if the hash file if the hash file matches a file that has been stored in the Blockchain system and the corresponding scorecard file that has been authenticated by the Admin.

V. EXPERIMENTS AND EVALUATION OF RESULTS

A. Experimental simulation environment

- OS Ubuntu 18.04, Intel® Core ™ i7-8550U CPU @ 1.80GHz, 8GB RAM.
- Use the Docker tool (version 19.3.8) and Docker-compose (version 1.21.2).

- Smart contract is written in Solidity language on framework as Truffle.
- NodeJS (version V10.19.0) and npm (version 6.14.3) are used to build the Web Service.
- Use RPC (Remote Procedure Call) protocol and format data in JSON format.
- Use the Web3.js library to interact with the Private Blockchain network.
- For the Private Blockchain system, we use the Ethereum Blockchain platform, PoA consensus protocol.

Evaluation criteria:

- Time of authentication.
- Accuracy.
- Convenience.

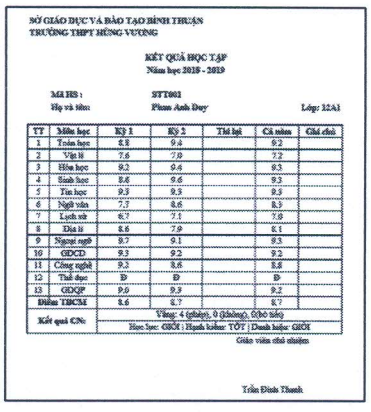
B. Experiments and results

Experimental data

Table 1: Experimental dataset.

No.	Number of File Record	File Size	Format file
1	300 ~ 400	100 ~ 300 Kb	.pdf

Transcript illustrates


SỞ GIÁO DỤC VÀ ĐÀO TẠO BÌNH THUẬN
TRƯỜNG THPT HÙNG VƯƠNG

KẾT QUẢ HỌC TẬP
Năm học 2018 - 2019

Mã HS : 5TT001
Họ và tên: Phan Anh Duy Lớp: 12A1

TT	Môn học	Kỳ 1	Kỳ 2	Thi lại	Cả năm	Ghi chú
1	Toán học	8.8	9.6		9.2	
2	Vật lí	7.6	7.9		7.7	
3	Hóa học	9.0	9.4		9.3	
4	Sinh học	8.6	9.6		9.3	
5	Tin học	9.3	9.3		9.3	
6	Ngữ văn	7.7	8.6		8.3	
7	Lịch sử	6.7	7.1		7.0	
8	Địa lí	8.6	7.9		8.1	
9	Ngoại ngữ	9.7	9.1		9.3	
10	GDCD	9.3	9.2		9.2	
11	Công nghệ	9.3	8.6		8.8	
12	Thể dục	Đ	Đ		Đ	
13	GDQP	9.0	9.3		9.2	
Điểm TBCM		8.6	8.7		8.7	
Kết quả CN:		Vắng: 4 (phép), 0 (không), 0 (Đi trễ)				
		Học lực: GIỎI | Hạnh kiểm: TỐT | Danh hiệu: GIỎI				

Giáo viên chủ nhiệm

Trần Đình Thanh

Figure 7: Transcript illustrating.

Result

Case 1: The transcript's status does not exist on the system (the transcript has not been stored by the teacher on the system). At that time, the test result of the transcript is **"Grade Record does not exist."**.

Table 2: Experimental results with *Case 1*.

No.	Student ID	Transcript	File hash	Result
1	ms001	File1.pdf	31c7b132359e35a52c5fe0796598fc34f410c7484cef79854ca97c51bf	True
2	ms002	File2.pdf	245f5e9adf42dac4a4c4d6f6r6a6v656bxd9814vaf24756f2fv22c2576d	True
3	ms003	File3.pdf	91hj7b132359e35a52c5fe0796598fc34f410c7484cef79854ca97c32q	True
4	ms004	File4.pdf	9ca72c5fe079b132359e35a52c5fe0796598fc34f410c7484cef79854c	True
5	ms005	File5.pdf	52c5fe071359e35a52c5fe0796598fc34f410c7484cef79854c8fc34f41	True
6	ms006	File6.pdf	8fc34f41059e35a52c5fe0796598fc34f410c7484cef79854ca9 fe07kl	True
7	ms007	File7.pdf	54ca97c51bf31c7b132359e35a52c5fe0796598fc34f410c7484cef798	True
8	ms008	File8.pdf	9e35a52c5fe079854ca97c51bf96598fc34f410c7484cef731c7b13235	True
9	ms009	File9.pdf	410c7484cef79854ca97c51bf31c7b132359e35a52c5fe0796598fc34f	True
10	ms010	File10.pdf	359e35a52c5fe0731c7b13296598fc34f41054ca97c51bf c7484cef798	True

Result with case 1: The system is 100% accurate.

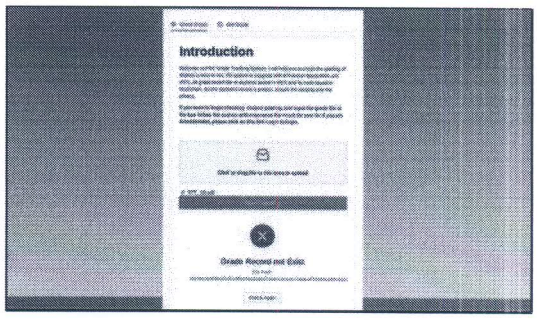


Figure 8: The transcript test interface with *Case 1*.

Case 2: The transcript's status is correct but not yet authenticated by the Admin. (The transcript has been stored by the teacher on the system, but the Admin has not yet verified the transcript). At that time, the test outcome is **"Grade Record is true but not verified."**.

Table 3: Experimental results with *Case 2*.

No.	Student ID	Transcript	File hash	Result
1	ms011	File11.pdf	fe0796598fc32359e35a52c50c7484cef79854ca97c51bf34f4131c7b1	True
2	ms012	File12.pdf	24 f2fv22c2576d 5f5e9a4d6f6r6a6v656bxd9814vaf24756df42dsc4s4c	True
3	ms013	File13.pdf	c5fe0796598fc34f410c 91hj7b132359e35a527484cef79854ca97c32q	True
4	ms014	File14.pdf	410c7484cef79854c 9ca72c5f2c5fe0796598fc34f e079b132359e35a5	True
5	ms015	File15.pdf	e071359e35a52c5fe052c5f796598fc34f410c7484cef79854c8fc34f41	True
6	ms016	File16.pdf	484cef79854ca9 fe07kl 8fc34f41059e35a52c5fe0796598fc34f410c7	True
7	ms017	File17.pdf	31c7cef79854ca97c51bf b132359e35a52c5fe0796598fc34f410c7484	True
8	ms018	File18.pdf	c5fe0796598fc34f410c7484cef79854ca97c51bf31c7b132359e35a52	True
9	ms019	File19.pdf	ef79854ca97c51bf31c7b132359e35a52c5fe0796598fc34f410c7484c	True
10	ms020	File20.pdf	34cef79854ca97c51bf 1c7b132359e35a52c5fe0796598fc34f410c748	True

Result with case 2: The system is 100% accurate.

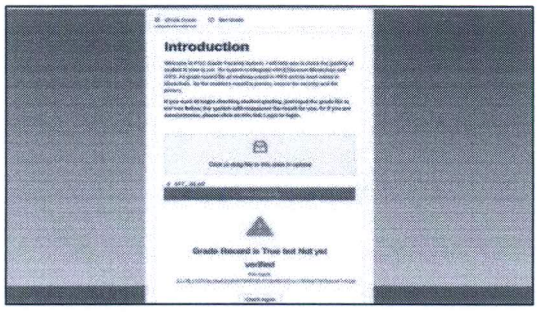


Figure 9: Interface for checking transcript with ***Case 2***.

Case 3: The status of the transcript is correct and verified. (The transcript has been stored by the teacher on the system and the Admin has confirmed the transcript). At that time, the test result of the transcript was **"Grade Record is true and verified"**.

Table 4: Experimental results with ***Case 3***.

No.	Student ID	Transcript	File hash	Result
1	ms021	File21.pdf	598fc32359fe0796e35a52c50c7484cef7c7b19854ca97c51bf34f4131	True
2	ms022	File22.pdf	fe9a4d6f6r6a6v656bxd924f2fv22c2576d5814vnf24756df42dac4a4cd	True
3	ms023	File23.pdf	359e35a527484cef79854ca97c32q5fe0796598fc34f410c 91hj7b132	True
4	ms024	File24.pdf	410c7484cef79854c9ca72c5f2c5fe0796598fc34f e079b132359e35a5	True
5	ms025	File25.pdf	4f410c7484cef79854c8fc34f41e071359e35a52c5fe052c5f796598fc3	True
6	ms026	File26.pdf	96598fc34f410c7484cef79854ca9 fe07kl 8fc34f41059e35a52c5fe07	True
7	ms027	File27.pdf	796598fc34f410c748431c7cef79854ca97c51bf b132359e35a52c5fe0	True
8	ms028	File28.pdf	c31c7b132359e35a525fe0796598fc34f410c7484cef79854ca97c51bf	True
9	ms029	File29.pdf	fe0796598fc34f410c7484c ef79854ca97c51bf31c7b132359e35a52c5	True
10	ms030	File30.pdf	bf 1c7b132359e35a52c5fe0796598fc34f410c74834cef79854ca97c51	True

Result with case 3: The system is 100% accurate

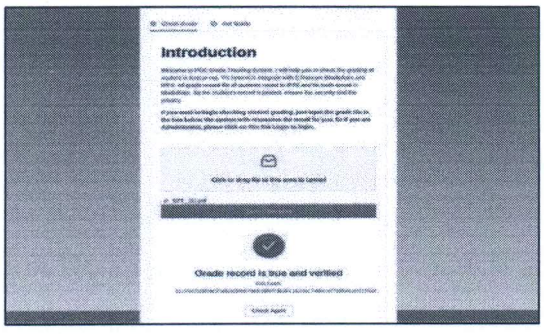


Figure 10: Interface for checking transcript with ***Case 3***.

With 300 data sets of transcripts, the system produces the following results:

Table 5: Experimental results with 300 transcript files.

No.	Number of File Record	Accuracy		
		Case 1	Case 2	Case 3
1	50~100	100%	100%	100%
2	100~150	100%	100%	100%
3	150~200	100%	100%	100%
4	200~250	100%	100%	100%
5	250~300	100%	100%	100%

C. Assessment of the results

The proposed model provides an authentication system for user data - student transcripts - based on the Blockchain Network (using Ethereum platform). The system after the experiment was evaluated as follows:

- Fast authentication time.
- Simple authentication process, easy to follow.
- Verify the student's transcript on the system for most accurate results, the transcript is difficult to be fake.
- Manage and store students' transcripts safer, more transparently and invariably.
- The system helps reduce the need for manpower during the validation of transcripts.

Table 6: Comparation and evaluation of the proposed system and traditional method.

No.	Evaluation criteria	Authentication transcripts by the proposed system	Authentication transcripts by the traditional way
1	***Time***	Less time-consuming: just a few seconds for a verification.	Take a lot of time: Copy, notarized verification or input data into the school system to check, then compare it manually, check it true or not. This process may take 02 ~ 03 minutes for a verification.
2	***Procedure***	Perform authentication on computers connected to the Internet anytime, anywhere.	The authentication process is complicated and must go through many agencies and organizations.
3	***Trust level***	High, hard to fake thanks to the immutability and transparency of Blockchain.	Depends on many factors. May be tampered with during authentication.
4	***Storage location***	Blockchain network system. (safe, Decentralized)	Schools.
5	***Convenience***	More	Less
6	***Popularity***	Not popular	Popular

No.	Evaluation criteria	Authentication transcripts by the proposed system	Authentication transcripts by the traditional way
7	*Human Resources*	Less	More than

With authentication transcripts by the traditional method, an organization or company wants to verify a student's transcript, they must rely on a certified copy of the school (where the student is attending) or a copy certified by the competent authority (notary office or local government). This makes it difficult as students spend a lot of time and effort in copying and verifying the transcript; Transcripts must be kept for long term at the school; The verification has to go through many stages and use a lot of manpower. Even so, transcripts can still be faked easily.

Currently, an organization or company wants to verify a student's transcript, they can also visit the website / portal of the school that provided the student transcript. This is also a common way that many people are doing. This will take at least 02 minutes or more to perform. The comparison of the proposed model with the traditional way of verifying the transcript is often different. It shows the effectiveness of the proposed model..

VI. CONCLUSIONS AND RECOMMENDATIONS

In this paper, we have built and tested a student transcript system based on the Blockchain network using the PoA consensus algorithm. The proposed a system which can adapt quickly, accurately and reliably in verifying a student's transcript, avoiding forging a student's fake score sheet. With the result outcomes can prove the efficiency and power of Blockchain, it can apply in many aspects of our life, it is also very potential to develop and improve this approach further and deeper.

The development direction of the proposed model is to build a Private Blockchain network with more nodes to ensure data is backed up on multiple nodes. In addition to authenticating transcripts, the proposed system can be deployed to validate other user data such as medical records, certificates of marriage registration, etc.

REFERENCES

[1] Nitin Kumavat, Swapnil Mengade, Dishant Desai, Jesal Varolia, (2019), "Certificate Verification System using Blockchain", *International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com*

[2] "WIKIPEDIA" (Updated 06/12/2019) [Online] https://en.wikipedia.org/wiki/Authentication.

[3] Deepak Puthal, Nisha Saroha Malik, Saraju P.Mohanty, Elisa Kougianos, (2018), "Everything You Wanted to Know About the Blockchain: Its Promise, Components, Processes, and Problems". https://www.researchgate.net/publication/326102908

[4] Tran Cong An, Pham Thi Xuan Diem, Tran Van Toi, Le Thi Thu Lan, Lam Duong Quoc, (2019), "Building a Product Origins Tracking System based on Blockchain and PoA Consensus Protocol", *2019 International Conference on Advanced Computing and Applications (ACOMP).*

[5] Shuai Wang, Yong Yuan, Xiao Wang, Juanjuan Li, Rui Qin, Fei-Yue Wang, (2018),"An Overview of Smart Contract: Architecture, Applications, and Future Trends", *2018 IEEE Intelligent Vehicles Symposium (IV) Changshu, Suzhou, China, June 26-30, 2018.*

[6] Muhamed Turkanovic, Marko Holbl, Kristjan Kosic, Marjan Hericko, Aida Kamisalic, (2018), "EduCTX: A blockchain-based higher education credit platform", *Citation information: DOI 10.1109/ACCESS.2018.2789929, IEEE Access.*

[7] Yuqin Xu, Shangli Zhao, Lanju Kong, Yongqing Zheng, Shidong Zhang, Qingzhong Li, (2017), "ECBC: A High Performance Educational Certificate Blockchain with Efficient Query". *Springer International Publishing AG 2017, pp. 288–304.*

[8] Dipti Pawade, Avani Sakhapara, Melvita Andrade, Aishwarya Bdgujar, Divya Adep. (2019), "Implementation of Fingerprint-Based Authentication System Using Blockchain", *Springer Nature Singapore Pte Ltd.*

[9] K. Palanivel, (2019), "Blockchain Architecture to Higher Education Systems", *International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS) Volume VIII, Issue II, February 2019 | ISSN 2278-2540.*

[10] Qianqian Su, Rui Zhang, Rui Xue, You Sun , (2019), "An Efficient Traceable and Anonymous Authentication Scheme for Permissioned Blockchain", *Springer Nature Switzerland AG.*

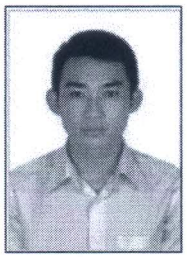
HỆ THỐNG XÁC THỰC BẢNG ĐIỂM HỌC SINH TRUNG HỌC PHỔ THÔNG DỰA TRÊN HỆ THỐNG MẠNG BLOCKCHAIN

Tóm tắt: Học sinh sau khi hoàn thành chương trình học của bậc Trung học phổ thông (THPT) sẽ được Nhà trường – nơi học sinh đó hoàn thành chương trình năm học cuối của bậc THPT – cấp học bạ, trong đó có các bảng điểm dưới dạng văn bản cứng – bảng điểm giấy. Chính vì vậy, việc làm giả bảng điểm nhằm mục đích phi pháp được thực hiện dễ dàng, nhanh chóng và chi phí thấp. Trong bài báo này, chúng tôi đề xuất một mô hình hệ thống xác thực bảng điểm học sinh dựa trên hệ thống mạng Blockchain. Hệ thống sử dụng hợp đồng thông minh (smart contract), xây dựng hệ thống mạng Private Blockchain trên nền tảng Ethereum, xây dựng các ứng dụng phi tập trung - Decentralized Application (dApp), hệ thống tập tin phân tán IPFS (Interplanetary File System)…. Giá trị băm của tập tin bảng điểm (file hash) sẽ được lưu trữ trên hệ thống mạng Blockchain và được sử dụng trong quá trình xác thực bảng điểm học sinh nhanh chóng, chính xác, tránh được việc là giả bảng điểm.

Từ khoá: *Blockchain, IPFS, dApp, Ethereum, Smart contract, bảng điểm.*

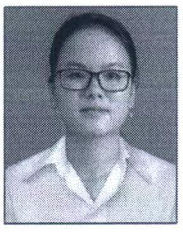
AUTHORS

Tran Cong Hung was born in Vietnam in 1961. He received the B.E in electronic and Telecommunication engineering with first class honors from HOCHIMINH University of technology in Vietnam, 1987. He eceived the B.E in informatics and computer engineering from HOCHIMINH University of technology in Vietnam, 1995. He received the Master of Engineering degree in telecommunications engineering course from postgraduate department Hanoi University of technology in Vietnam, 1998. He received PhD. at Hanoi.



Le Dien Tam was born in Vietnam in 1987. He received Master Computer science in Universite Pierre et Marie CURIE, France, 2014. He is currently a PhD. Candidate in Computer science and engineering from Kyung Hee University, Korea in 2020.

Le Ngoc Hieu has been working in IT industry as a IT System Architect since 2010. In 2018, He completed Master Degree at Post & Telecommunication Institute of Technology. As now, he is working as an IT lecturer for HCMC Open University. His major study is about cloud computing and cloud efficiency for better service; his minor study is about education, especially education in IT line.



Ho Thi Xuan Dinh was born in 1988. She received a bachelor's degree in 2011, majoring in computer science at Ho Chi Minh City University of Education, Vietnam. Currently, she is a Master's candidate in Computer Science from Saigon University, Vietnam. She is a Computer teacher at Hung Vuong High School, Binh Thuan