World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

A blockchain-based model to support student activities management

Van-Huy Vu *

Division of Mathematics and Informatics, Faculty of Fundamental Science, Thai Nguyen University of Economics and Business Administration, Thai Nguyen, Vietnam.

World Journal of Advanced Research and Reviews, 2022, 14(02), 515–524

Publication history: Received on 17 April 2022; revised on 19 May 2022; accepted on 22 May 2022

Article DOI: https://doi.org/10.30574/wjarr.2022.14.2.0460

Abstract

The fourth industrial revolution, digital transformation, and blockchain technology are those the terms get most interested in recently. The application of new technology to obtain the accuracy, convenience, and speed in managing work in general always attract much attention from the community. In the field of education, the exploitation of new technologies to promote the development of education and training is not out of the common trend. Current studies in blockchain-based application for education often focuses on exploiting features such as security, immutability, independence, etc., and applying them to verify the correctness and anti-counterfeiting of diplomas/certificates. Researches related to support student management is still very limited. In this paper, we study and propose a blockchain-based application to support the management of students' activities in general, such as managing code of conducts, extracurricular activities or soft skill courses for instance. The aim is to study the application of smart contracts of blockchain technology to support automatic, transparent and unbiased student reward or discipline through conduct point assessment. Along with that, the system will assist in verifying the career skills that students have accumulated to enhance the strength and reliability of the resume or portfolio of students.

Keywords: Education; Blockchain; Smart Contract; Student Managerment

1. Introduction

Blockchain is a topic that has attracted the attention of many researchers recently. It is known as a public ledger in which each transaction is stored in a block. The aim of blockchain is to allow its users to conduct their transactions directly, eliminating the intervention of any third parties. To gain that, blockchain is designed as a decentralized network of peer-to-peer nodes. Each node in the network stores a copy of the transaction ledger. The ledger is only updated whenever there is consensus from the dominant majority of other nodes in the network. After each successful transaction, all participating nodes in the network will be notified. The ledger will always be checked to guarantee the ledger's data is consistent across the network [1].

The basic benefits of blockchain technology are security, decentralization, transparency, and immutability. Along with the development trend of the fourth industrial revolution, blockchain technology has been researched and applied in most fields such as cryptocurrency, financial, commercial, public services, healthcare, risk management. etc. However, the implementation of blockchain technology in the field of education and training seems to be still limited and not commensurate with its potential. Within twelve categories of blockchain applications in education, the majority of applications were focused on certificate management, competencies and learning outcomes management, and evaluating students' professional ability respectively [2]. In another classification with five categories [3], the

[*] Corresponding author: Van-Huy Vu
Division of Mathematics and Informatics, Faculty of Fundamental Science, Thai Nguyen University of Economics and Business Administration, Thai Nguyen, Vietnam.

management of certificates is still the most attractive issue. None of the models has been released to support the management of student activities until now.

The smart contract, which was proposed for the first time by Nick [4], is one of the most important features in blockchain technology, it executes transactions reliably without the intervention of any trusted third parties. Smart contracts have been applied in several aspects such as crowdfunding, voting, securities, and medical research [5]. In the education field, the advantages of smart contracts such as immutability and irreversibility in data, it will help the education industry to deal with the problems of fraud like fake diplomas or certificates for instance.

A small aspect of student management in Vietnam relying on the author's observations is that the management of conduct points or extracurricular activities of students at most universities is still mostly manual. Besides that, the work of rewarding in which assessments were based on activities the student has participated in such as charity or volunteer works; or disciplining students wherever were relied on an assessment of the student's violation of the student code of conduct or internal school regulations needs to ensure accuracy, fairness, openness, no emotional bias, and timeliness. However, student reward and discipline activities in most cases do not fully meet those criteria. The reason is that the entire process of awarding and disciplining schools is done manually. This easily leads to sentimentality in assessing student conduct and a lack of clarity in some aspects.

Moreover, due to the lack of reliable verification mechanisms, it is very difficult for third parties such as employers, institutes, or other organizations in case they want to verify the accuracy of the extracurricular activities or soft skills that were listed on the student's curriculum vitae.

All the above issues are expected to be completely overcome by applying smart contracts in blockchain technology. In the next section, we will present a simple model of smart contract application in supporting the management of student activities while studying at the university.

2. Background

2.1. Blockchain

Blockchain is a mechanism of database technology that records transactions in blocks, which are linked and secured using cryptography. These blocks have been hosted on decentralized networks and cannot be modified or changed [6]. Each block contains information about its index, its transactions, its previous block, a nonce, a timestamp, etc, [5]. The first block is known as the genesis block. Figure 1 shows the visualization of blockchain. These blocks are considered immutable, shared ledger. Identical copies of the ledger are kept on many computers spread across the network. These individual computers are called nodes. In case one of the blocks is changed, then no subsequent block will be accepted. The consensus mechanism as proof-of-stake (POS) [7] or proof-of-work (POW) [8] is designed to update data for blockchain. The consensus is usually done by the node which first solves the puzzle. The benefits of the consensus mechanism can be mentioned as the near-instant speed of transactions when executed without the need for third-party intervention. In addition, users are also protected by using virtual addresses in transactions without having to use their identities. Some features of blockchain technology make it more attractive to the scholar for the education system [3].

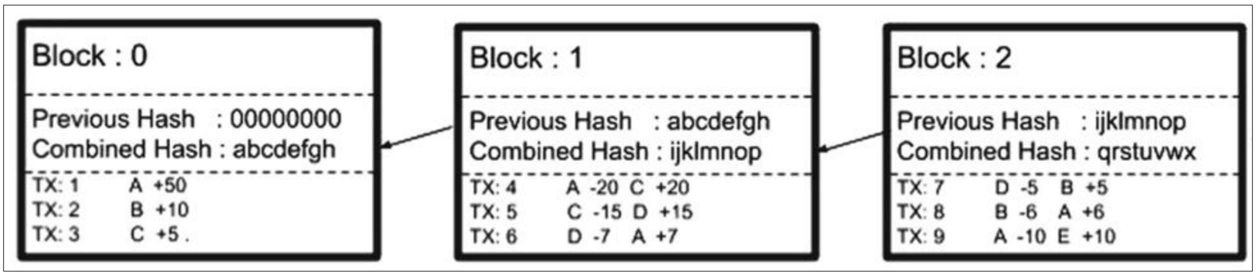

Figure 1 Blockchain visualization

- Decentralization: By spreading the data information across a network, instead of storing it in a central database, the blockchain becomes harder to tamper with.
- Immutability: No entity can manipulate, replace, or falsify data stored on the blockchain network.
- Transparency: Anyone who joins the network can check information about the existence of data stored on the blockchain at a specific time.

- Trust: Blockchain provides trust through technology instead of trust in centralized authority.

2.2. Smart Contract

A smart contract is a set of protocols that regulate the rules between the untrustworthy involved in a transaction [9]. It is a set of computer code that is executed whenever predefined conditions are met. usually written in programming languages such as Python, Solidity, or JavaScript. The key features of a smart contract that make it widely used include legality, productiveness, consistency, customizability, observability, verifiability, self-enforceability, and access-controlling [10].

- Legality: The same as lectronic records or electronic signatures, smart contracts secured through blockchain technology are considered to be in an electronic form and legally recognised.
- Like electronic records or electronic signatures, smart contracts secured through blockchain technology are considered legally recognized.
- Probativeness: Process scenarios and data must be securely stored and they can be used as legal evidence.
- Consistency: Smart contracts are not in conflict with existing laws.
- Customizability: Smart contracts are customizable, for example, combining basic contracts into a complex one.
- Observability: Smart contracts and the information related to their execution are clearly accessible.
- Verifiability: This is a necessary capability to check the correctness and security of smart contracts.
- Self-enforceability: It is enforceable as long as the basic rules of contractual agreements are observed.
- Access-controlling: Access control through ownership or only accessible for contract-related persons

2.3. Merkle Tree

Merkle Tree [11] is a cryptographic data structure also known as binary hash trees. The Merkle tree allows users to verify a specific transaction without downloading the entire blockchain. The Merkle root of a given block is stored in the header. The leaf nodes are the data hash of the Tree. The two leaf nodes are paired to become the parent node at the upper level. This pairing process is repeated recursively until there is only one node which is the tree root. A Merkle path for a leaf is the shortest list of nodes required to calculate the root hash.

3. Related work

Blockchain technology with its outstanding features is one of the most popular and interesting technologies today. These features include increased reliability, decentralized structure, improved security and privacy, reduced cost, speed, visibility and traceability, immutability, tokenization, etc. With such features, blockchain is applied in many areas such as cryptocurrency, financial and public services, healthcare domain, risk management, etc. [12].

In education, blockchain applications have been investigated in several aspects such as certificate/degree verification and revocation, user-centric educational record management, students' professional ability evaluation, blockchain-based educational institute systems, and online learning environment [3]. Among them and related to our work, certificate/degree verification and revocation have the most attractive. Blockcerts [13] is known as the first open platform for creating, issuing, viewing, and verifying digital certificates. The digital diploma is registered on a blockchain, cryptographically signed, tamper-proof, and shareable. A famous platform that uses blockchain applications is called EduCTX [14]. This platform has implemented a decentralized, trusted system of higher education credit conversion and transfer for students and higher education institutions. To date, only the Massachusetts Institute of Technology (MIT), the University of Nicosia, and the University of Birmingham research center based on the Blockcert [13] to develop their own systems. Whenever students have completed the course, a digital certificate is issued and recorded on the blockchain. In order to deal with counterfeiting certificates, Cheng [15] proposed a digital certificate system based on blockchain technology. The system firstly generates the electronic file of a paper certificate, then create a related QR-code and inquire string code sticking on the paper certificate. Verifier can check the authenticity of the certificate via mobile phone scanning or website inquiries. Another blockchain-based system is called UZHBC [16] which includes the issuance and verification of diplomas were proposed. This system uses Etherium blockchain to deploy. The author defined two functions in the smart contract are called *issueCertificate* and *verifyCertificate* for issuing and verifying the diploma purpose. Focusing on validating issued certificates, Curmi et al. [17] proposed a blockchain application solution to verifying the authenticity of issued certificates. TUDocChain [18] is also another method for issuing, securing, and verification of transcripts in an immutable and secure ledger. A smart contract written in solidity is used to manage the profile of the issuer, certifier, and student. Another smart contract is used to manage the information of certificates.

4. Proposed Model

4.1. Objects of management

Rewarding or disciplining students is an annual school activity. It plays an important role because it helps to improve the personal development of students while also maintaining the discipline of the school. It is necessary to build up a code of conduct and a regulation to participate in the common activities of the university to personal development orientation as well as standardize behavior for students. In the reality, this depends on the particular conditions of each school. In order to create favorable conditions for students to develop themselves comprehensively, beside academic skills, students need to participate in a number of activities such as: Self-help, soft skill courses (presentation skills, Q&A skills), extracurricular activities (kids helping kids, blood donation, youth volunteers), physical development (athletics club, table tennis, badminton clubs), etc. Each of which is assigned a certain point. If an activity belongs to the conduct category for instance, it is the group in which the student compromises not to violate. And of course, if a student violates any regulation in this category, then the corresponding points related to this regulation will be deducted. Example: public intoxication (0 to 4 points). In this case, if students violate this regulation, they will have 0 to 4 points deducted from their Total Activity Score; Another example, blood donation (8-10 points). This "activity" does not belong to the conduct category. If students participate in blood donation, they will get 8 to 10 points on their Total Activity Score.

4.2. Proposed System

The system we propose uses a point system to evaluate and manage student activities. A point value is assigned to each activity. We consider each student activity in general as a skill. For simplicity, we classify them into two types of skills. Extracurricular activities are career skills (CS). The behaviors in the code of conduct are life skills (LS). The overview of our proposed model can be summarized in Figure 2 below.

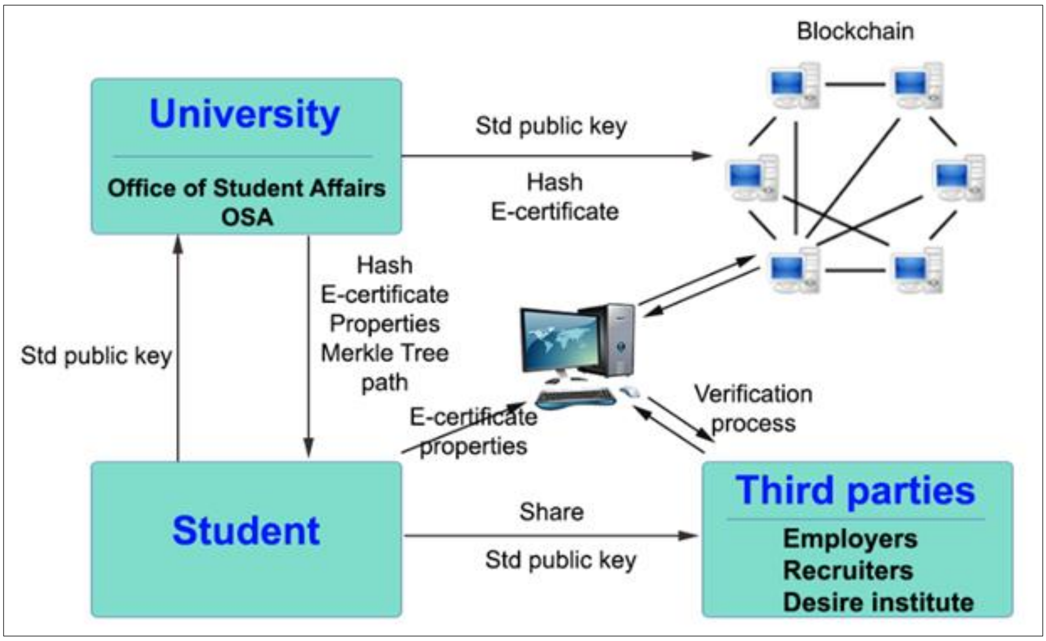

Figure 2 Overview the component of a blockchain in proposed model

- The Office of Student Affairs (OSA) of the University list “the skills”
- Students select “the skills” to perform.
- OSA generates the smart contract for each selected skill of student.
- An E-certificate of “the skill” is issued to the student when a skill is comple
- The third-party can verify the E-certificate of the student when he or she shares it

4.2.1. Career skills

The activities in this category are the activities that the school encourages students to participate in. These activities aim to develop non-academic skills that are considered useful skills for students' future careers. For example, these are the most preferred extracurricular activities: leadership work and positions, part-time jobs, sports, and athletic participation, academic clubs and teams, artistic and creative pursuits, volunteering and community service, and internships. OSA manages and lists those skills so that students can choose to participate, or the skills that student desires to perform or attend can also be suggested by students themself. Students can choose one or more of these skills to participate in. For each skill a student has taken or completed in this section, an electronic certificate (E-certificate) will be issued. Along with that, a point value is the corresponding amount of cryptocurrency that will be added to the student's wallet. Smart contracts are applied to these skills. E-certificate in this case is verifiable. Students instead of having to provide a hard copy of certificates (if any) or just list them in their CVs without reliable endorsement, or just share their smart contract address to third parties for verification. This is not only very fast, saves time and money but is also reliable.

4.2.2. Life skills

Like the code of conduct, the activities in this category include commitments that students must not violate. Similar to CS, however, this is mandatory for all students and is evaluated yearly. At the beginning of each semester, students will be provided a list of code of conduct, smart contracts will be established for these activities. This can be an integrated smart contract instead of a single contract. Any student found in violation of the stated in the LS, he or she will get zero points for that. Otherwise, the student will receive the corresponding number of points in his or her wallet. LS is not for the purpose of applying for jobs or scholarships, but just for assessing student conduct yearly. Since this is the internal way to assess student behaviors of the university, then these smart contracts will not need to be verified by third parties in the future even though are entirely doable. Instead of the traditional process of assessing student conduct points, it is resolved by smart contracts automatically, clearly, and transparently. Students can self-check their conduct points through their personal e-wallets. Along with that, the university also relies on the point value in each student's wallet to make a decision to reward and discipline students.

4.3. Workflow model

The workflow of the proposed model can be seen as Figure 3. Figure 3a is the process to register a student into the blockchain network of the University. This is performed only once after the student is admitted to the University. Each student will be assigned a key pair including a private key and a public key. The RSA algorithm will be used in this case. A crypto wallet will also be created for the student as well. Students will use this wallet to collect conduct points as well as other e-certificates after each task they completed. Conduct points are calculated automatically and they will be used for rewarding or disciplining students after each semester or each school year. Besides that, a wallet is also a place for data stored on the blockchain such as e-certificates of extracurricular activities, which will be validated by third parties in the future.

Figure 3b is the workflow of our proposed model.

- OSA lists the set of {CSs, LSs} – those are the list of activities or tasks (extracurricular and code of conducts) for the student to choose. Students can also suggest other activities or skills that are off the list they would like to participate in. Of course, for these skills to be valid, they need to be approved by the OSA.
- Check the eligibility of current students in the system.
- Students select the task in {CSs} to perform and select all tasks in {LSs} to commit not to violate. The number of tasks that the student chooses must ensure that the total points accumulated in a semester or an academic year must reach the minimum requirement by the University.
- OSA creates a smart contract using the student public key for each selected task. There are two types of smart contracts, one corresponding is Publishing Data and another is a Verification e-certificate.
- OSA update student wallet: Whenever a task is completed, the student will receive the corresponding points for that specific task.

Figure 4 [19] is the process to create a new blockchain in the system for an admitted student.

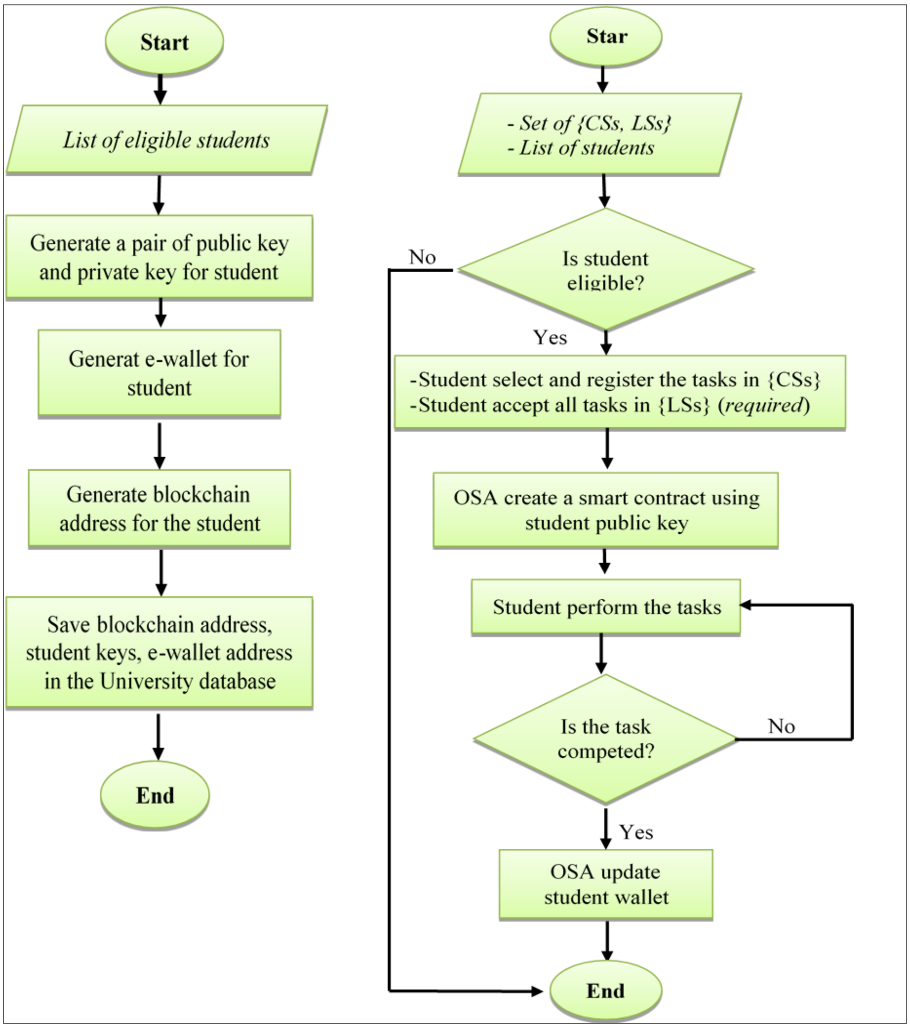
Start
List of eligible students
Generate a pair of public key and private key for student
Generat e-wallet for student
Generate blockchain address for the student
Save blockchain address, student keys, e-wallet address in the University database
End
Star
- Set of {CSs, LSs}
- List of students
Is student eligible?
No
Yes
-Student select and register the tasks in {CSs}
-Student accept all tasks in {LSs} (required)
OSA create a smart contract using student public key
Student perform the tasks
Is the task competed?
No
Yes
OSA update student wallet
End

Figure 3 a) Add a student to the blockchain network; b) Workflow proposed model

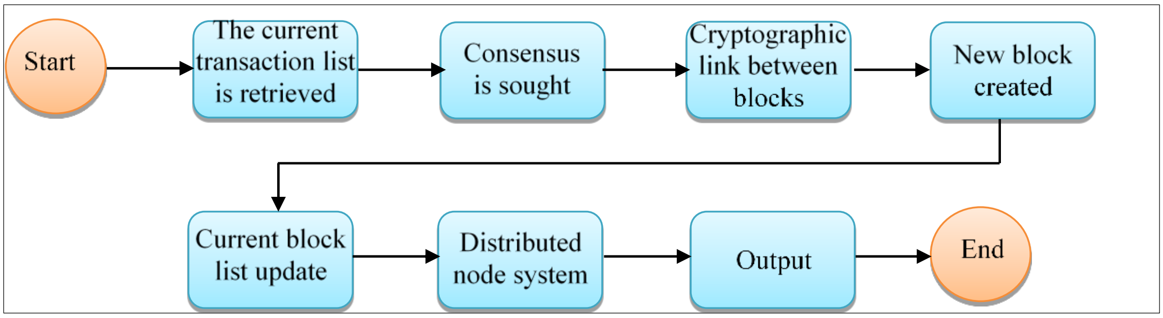
Start
The current transaction list is retrieved
Consensus is sought
Cryptographic link between blocks
New block created
Current block list update
Distributed node system
Output
End

Figure 4 Create a new blockchain

4.4. Smart Contract

Following the study of smart contracts applying for the transcript as in [20], we present the pseudocode for two types of smart contracts: publishing data and verification e-certificate.

Algorithm 1: Pseudocode for Publish data smart contract

- Input: OSA_ID, Task_ID, Year, MerkleRoot, std_ public_key.
- Output: Data is writen on Blockchain netwok.

```
if checkPermission(OSA_ID) == OSA_public_key then
    if checkPermission(std_ID) == std_public_key then
        if selectedTask(Task_ID, std_public_key, Year) then
            transactionID, blockN0 = publishTaskOnBlockChain(MerkleRoot, Task_ID, OSA_ID, std_public_key,
                                         addMerkleRootType);
            sendNotification(std_public_key, transactionID + " " + blockN0);
            completeContract();
        else
            sendNotification(std_public_key, "Task is not selected: "+Task_ID);
        end
    else
        sendNotification(std_public_key, "Not valid student");
    end
else
    sendNotification(std_public_key, "Public Data Failed");
    terminateContract();
end
```

Algorithm 2: Pseudocode to update student conduct point value

- Input: OSA_ID, Task_ID, Year, MerkleRoot, std_ public_key, std_wallet_address.
- Output: Update student wallet, issue e_certificate.

```
if !(checkOverDue(Task_ID, Year, std_public_key)) then     //Task is not overdue
    if taskIsDone(Task_ID, Year, std_public_key) then
        conduct_Points = getValueFrom(Task_ID, Year);
        updateStdBalance(std_public_key, std_wallet_address, conduct_Points);
    end
else
    revokeSmartContract(Task_ID, Year, std_public_key, std_wallet_address);
end
```

Algorithm 3: Pseudocode to Verify e-certificate Smart Contract

- Input: OSA_ID, Task_ID, e-certificate, MerklePath, public_key_of_initiator;
- Output: e-certificate is verified.

```
rootComputed = computeMerkleRoot(e-certificate, MerklePath);

Year = extractYear(Task_ID);

TXID, blockN0 = getBlockN0FromHashMap(OSA_ID, Year, Task_ID);

rootStored, MetaData = getValueFrom(blockN0, TXID);

if rootComputed==rootStored then        //Task is not overdue

    transactionID, blockN0 = publishDataOnBlockChain(Merkle_root, Task_ID,OSA_ID, std_public_key, verificationType);

    sendNotification(public_key_of_initiator, Verified + " " + transactionID + " " + blockN0);

else

    transactionID, blockN0 = publishDataOnBlockChain(Merkle_root, Task_ID,OSA_ID, std_public_key, verificationType);

    sendNotification(public_key_of_initiator, Tampered + " " + transactionID + " " + blockN0);

end

completeContract();
```

4.5. Students

Through our proposed system of blockchain-based technology, the CSs of students are managed more clearly and effectively. Proof of career skills that students have participated in will be saved on the blockchain system securely and permanently. These verifiable "skills" are convincing proofs for employers or other universities after students graduate. Along with that, the conduct point is updated directly into the student's wallet right after a "skill" is completed. Students can easily know the total number of conduct points accumulated up to a particular time. This helps to correct students' behavior in a positive aspect. Students can actively register more useful CSs or withdraw skills depending on their ability to perform those skills as well as the minimum requirement for accumulated conduct points.

E-certificates are owned by students. He or she has the right to set the properties for these e-certificates in his or her wallet as public or private, or even who has permission to view its information. In addition, students can also set the permission that allows anyone accessing their wallet to authenticate certain information without having to be identified.

When a student applies for a job or a scholarship, he or she simply submits his or her e-certificates to the desired employers or educational institutions without having to use hard copies of certificates. The benefit of e-certificates is that they can be verified easily, quickly, and reliably, which will increase the credibility of the candidate.

4.6. System Implementation

In order to build a system like this sucessfully, it takes a lot of time, effort and money therefore our proposed system is still under deverloping and testing. The major tools which we are using to develop as below:

- Hash function: SHA 256.
- Private key and public key: RSA algorithm
- Local webhoting: XAMPP
- Programing language: Solidity
- Compile and test smart contracts: Remix IDE (online IDE) [21].

- Blockchain test network: Ropsten [22].
- Virtual Ethereum network: Ganache [23].
- Wallet: Metamask [24]

5. Conclusion and recommendation

We have proposed a simple model based on blockchain technology for efficient and transparent management of student activities. The two main benefits can be mentioned when this system is implemented in practice: Firstly, it helps OSA to be fair, fast, accurate, transparent, and unbiased in rewarding and disciplining students. Secondly, by implementing smart contracts based on blockchain technology on all skills that students registered to perform, the system is not only a place to store but also verify those skills for both students and recruiters. Lastly, students actively control the total of conduct points they need to accumulate in each semester or school year so that they know how to choose the necessary career skills that they should participate in to achieve the maximum number of career skills as well as at least reach the minimum requirements of conduct points.

The application of blockchain in education still has a lot of potentials that requires scholarly attention. Some application aspects in education field such as blockchain application supports educational management in higher education; support assessment of teaching capacity of lecturers; supports online training and certification; support to store student data including diplomas, certificates, transcripts, etc.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares that there is no conflict of interest regarding the publication of this document.

References

[1] Alexander Grech, Anthony F Camilleri, Andreia Inamorato dos Santos, European Commission, and J. R. Centre, *Blockchain in education*. Publications Office. 2017.

[2] A Alammary, S Alhazmi, M Almasri, S Gillani, Blockchain-based applications in education: A systematic review, in *Applied Sciences (Switzerland)*. 2019; 9.

[3] F Loukil, M Abed, K Boukadi, Blockchain adoption in education: a systematic literature review, *Education and Information Technologies.* 2021; 26(5).

[4] Nick Szabo. *The Idea of Smart Contracts*. 1997.

[5] J Liu, Z Liu, A Survey on Security Verification of Blockchain Smart Contracts, in *IEEE Access*. 2019; 7.

[6] M Li *et al*, CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing, *IEEE Transactions on Parallel and Distributed Systems.* 2019; 30(6): 1251-1266.

[7] S Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System. [cited 2022 Apr 16]. Available from: https://bitcoin.org/en/bitcoin-paper/.

[8] F Saleh, Blockchain without Waste: Proof-of-Stake, *the Review of Financial Studies.* 2021; 34(3): 1156-1190.

[9] V Buterin. A next generation smart contract & decentralized application platform. 2015.

[10] K Hu, J Zhu, Y Ding, X Bai, J Huang, Smart contract engineering, *Electronics (Switzerland)*. 2020; 9(12).

[11] RC Merkle. A Digital Signature Based on a Conventional Encryption Function, in *Advances in Cryptology — CRYPTO '87*, Berlin, Heidelberg. 1988; 369-378. Springer Berlin Heidelberg.

[12] P Prajapati, K Dave, P Shah. A review of recent blockchain applications, in *International Journal of Scientific and Technology Research*. 2020; 9.

[13] Blockcerts, Blockcerts: The Open Standard for Blockchain Credentials. 2016.

[14] M Turkanović, M Hölbl, K Košič, M Heričko, A Kamišalić, EduCTX: A Blockchain-Based Higher Education Credit Platform, *IEEE Access.* 2018; 6: 5112-5127.

[15] JC Cheng, NY Lee, C Chi, YH Chen. Blockchain and smart contract for digital certificate, in *2018 IEEE International Conference on Applied System Invention (ICASI)*. 2018; 1046-1051.

[16] J Gresch, B Rodrigues, E Scheid, SS Kanhere, B Stiller. The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling, in *Business Information Systems Workshops*, Cham. Springer International Publishing. 2019; 185-196.

[17] A Curmi, F Inguanez. BlockChain Based Certificate Verification Platform, in *Business Information Systems Workshops*, Cham. Springer International Publishing. 2019; 211-216.

[18] S Budhiraja, RJICT Rani. TUDocChain-Securing Academic Certificate Digitally on Blockchain. 2019.

[19] HAM Deenmahomed, MM Didier, RK Sungkur. The future of university education: Examination, transcript, and certificate system using blockchain, *Computer Applications in Engineering Education*. 2021; 29(5).

[20] K Patel, ML Das. Transcript Management Using Blockchain Enabled Smart Contracts, in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. 2020; 11969 LNCS.

[21] REMIX IDE, Deploy & run transactions in the blockchai. [cited 2022 Apr 16]. Available from: https://remix-project.org/.

[22] Ropsten Testnet. Blockchain test network. [cited 2022 Apr 16]. Available from: https://ropsten.etherscan.io/.

[23] Ganache, Truffle suite - Ganache - One click blockchain. [cited 2022 Apr 16]. Available from: https://trufflesuite.com/ganache/.

[24] Metamask, A crypto wallet & gateway to blockchain apps. [cited 2022 Apr 16]. Available from: https://metamask.io/.