RESEARCH AND BUILD A POINT MANAGEMENT SYSTEM ON THE BLOCKCHAIN PLATFORM

Dang Xuan Bao*, Hoang Thanh Nam
Academy of Cryptography Techniques

ARTICLE INFO

Received: 02/11/2023
Revised: 27/12/2023
Published: 27/12/2023

KEYWORDS

Blockchain
Smart Contracts
Ethereum
Non-fungible token
Point management system

ABSTRACT

Point management at universities is a complicated job that can easily make mistakes. Currently, there have been some studies on applying blockchain technology in point management at universities, however student points are not directly entered into the blockchain system. The advantages of blockchain technology compared to traditional databases are transparency, easy checking of data changes, and avoidance of common database attacks today such as SQL Injection, XSS... In this paper, the authors proposes to experimentally build a point management system based on blockchain technology, specifically Ethereum, in which points are entered directly into the blockchain. Test results on the Goerli testnet show that the average time to enter scores for a student is 3.42 seconds, the average time to export a student's scorecard is 8.51 seconds. Test results show that the system operates stably, in accordance with the current available hardware and software configuration.

NGHIÊN CỨU XÂY DỰNG HỆ THỐNG QUẢN LÝ ĐIỂM TRÊN NỀN TẢNG BLOCKCHAIN

Đặng Xuân Bảo*, Hoàng Thanh Nam
Học viện Kỹ thuật Mật mã

THÔNG TIN BÀI BÁO

Ngày nhận bài: 02/11/2023
Ngày hoàn thiện: 27/12/2023
Ngày đăng: 27/12/2023

TỪ KHÓA

Chuỗi khối
Hợp đồng thông minh
Ethereum
Non-fungible token
Hệ thống quản lý điểm

TÓM TẮT

Quản lý điểm tại các trường đại học là một công việc phức tạp, dễ sảy ra sai sót. Hiện nay đã có một số nghiên cứu ứng dụng công nghệ chuỗi khối trong quản lý điểm tại các trường đại học, tuy nhiên điểm của sinh viên không được nhập trực tiếp vào hệ thống blockchain. Ưu điểm của công nghệ chuỗi khối so với cơ sở dữ liệu truyền thống là minh bạch, dễ dàng kiểm tra những thay đổi của dữ liệu, tránh được các tấn công lên cơ sở dữ liệu phổ biến hiện nay như SQL Injection, XSS... Trong bài báo này tác giả đề xuất xây dựng thử nghiệm một hệ thống quản lý điểm dựa trên công nghệ chuỗi khối, cụ thể là Ethereum, trong đó điểm được nhập trực tiếp vào chuỗi khối. Kết quả thử nghiệm trên mạng testnet Goerli cho thấy thời gian nhập điểm trung bình cho một sinh viên là 3,42 giây, thời gian trung bình xuất bảng điểm một sinh viên là 8,51 giây. Kết quả cho thấy hệ thống vận hành ổn định, phù hợp với cấu hình phần cứng và phần mềm sẵn có hiện nay.

DOI: https://doi.org/10.34238/tnu-jst.9135

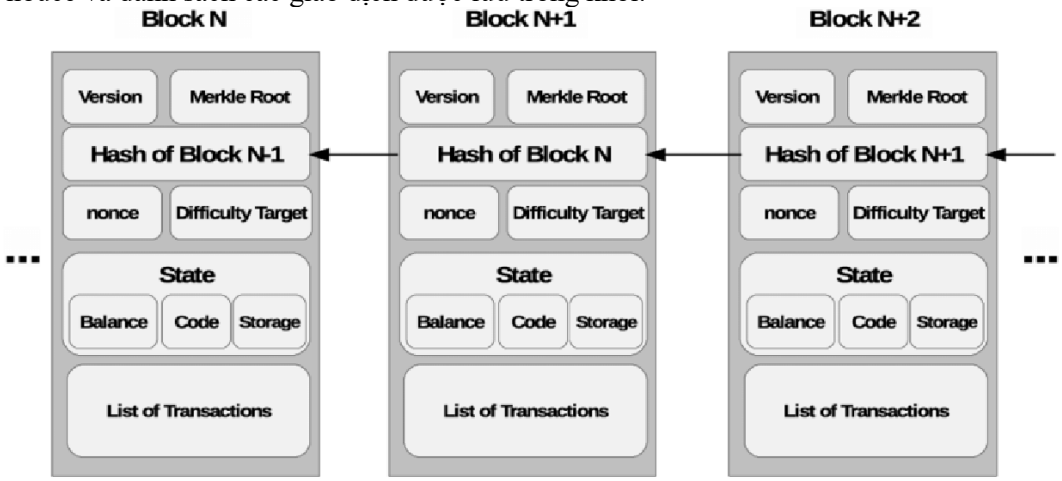
* Corresponding author. *Email: dangxuanbao.attt@gmail.com*

1. Giới thiệu

Quản lý điểm tại các trường đại học là quá trình bao gồm việc: nhập điểm, lưu trữ, xuất bảng điểm và chỉnh sửa khi có sai sót trong quá trình nhập điểm hoặc khi thi lại. Đối với những trường có số lượng sinh viên lớn quản lý điểm là một quá trình phức tạp, dễ xảy ra sai sót. Vì vậy cần xây dựng hệ thống quản lý điểm giúp quá trình quản lý điểm thuận tiện, dễ dàng; trong trường hợp xảy ra sai sót có thể nhanh chóng kiểm tra, đối chiếu và chỉnh sửa.

Hiện nay đã có một số nghiên cứu ứng dụng công nghệ blockchain trong giáo dục. Trong bài báo [1] – [4] các tác giả đã tổng hợp các nghiên cứu hiện có và thấy rằng công nghệ chuỗi khối được dùng trong việc lưu trữ và xác thực các văn bằng, chứng chỉ, bảng điểm… của sinh viên. Cụ thể bài báo [4] mô tả kiến trúc hệ thống quản lý giấy tờ của sinh viên, trong đó bảng điểm được nhập, chỉnh sửa, lưu trữ tại cơ sở dữ liệu (CSDL) thông thường (SQL, MongoDB…); còn trên chuỗi khối lưu bảng điểm khi hoàn thành các giai đoạn của khóa học. Với CSDL thông thường, các hành động chỉnh sửa bảng điểm được lưu lại tại nhật ký của hệ thống, tuy nhiên nhật ký này có thể bị xóa bởi người dùng có quyền. Như vậy bảng điểm có thể bị chỉnh sửa trái phép trước khi được lưu lên chuỗi khối. Ngoài ra các CSDL thông thường còn tồn tại nhiều lỗ hổng như SQL Injection, XSS... và dễ bị kẻ tấn công khai thác. Để phòng tránh những nguy cơ kể trên trong bài báo đề xuất xây dựng thử nghiệm hệ thống quản lý điểm trên nền tảng công nghệ chuỗi khối: việc nhập điểm, chỉnh sửa điểm của sinh viên được thực hiện trực tiếp trên chuỗi khối; các thay đổi về điểm được lưu lại trong các giao dịch trong các khối.

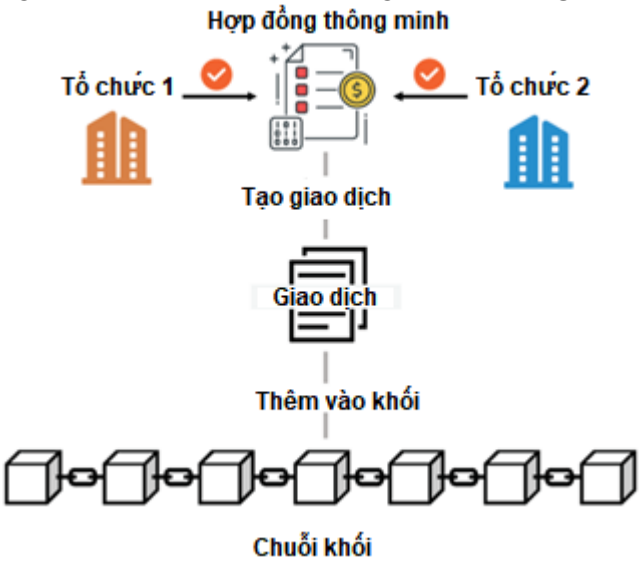
Chuỗi khối là một cơ sở dữ liệu phân cấp lưu trữ thông tin trong các khối thông tin được liên kết với nhau bằng mã hóa và mở rộng theo thời gian. Mỗi khối thông tin đều chứa thông tin về thời gian khởi tạo và được liên kết tới khối trước đó, kèm một mã thời gian và dữ liệu giao dịch. Chuỗi khối được thiết kế để chống lại sự thay đổi của dữ liệu. Một khi dữ liệu đã được mạng lưới chấp nhận thì sẽ không có cách nào thay đổi được nó [5], [6]. Hình 1 [7] thể hiện cấu trúc các khối và liên kết giữa các khối trong chuỗi khối. Các khối dữ liệu được "móc xích" với nhau bằng giá trị băm của khối dữ liệu trước. Trong các khối dữ liệu chứa các thông tin về khối, giá trị ngẫu nhiên nouce và danh sách các giao dịch được lưu trong khối.



Hình 1. *Các khối trong chuỗi khối* [7]

Smart Contract (Hợp đồng thông minh) [8], [9] là một giao thức giao dịch dựa trên công nghệ chuỗi khối. Mục đích của hợp đồng này là thực hiện các điều khoản của hợp đồng mà không cần thông qua bên thứ ba. Hợp đồng thông minh được dùng để tự động hóa việc thực hiện một thỏa thuận. Đồng thời nó cũng được sử dụng để kích hoạt các hành động tiếp theo khi điều kiện được đáp ứng. Mỗi khi hợp đồng được thực hiện sẽ sinh ra một giao dịch, giao dịch đó được ghi lại vào khối dữ liệu mới và được thêm vào chuỗi khối. Hình 2 thể hiện quá trình hoạt động của hợp đồng

thông minh trong hệ thống chuỗi khối. Các hợp đồng thông minh có thể được viết theo chuẩn ERC-20 hoặc ERC-721, trong đó chuẩn ERC-721 còn được gọi là Non-Fungible Tokens (NFT) [10].

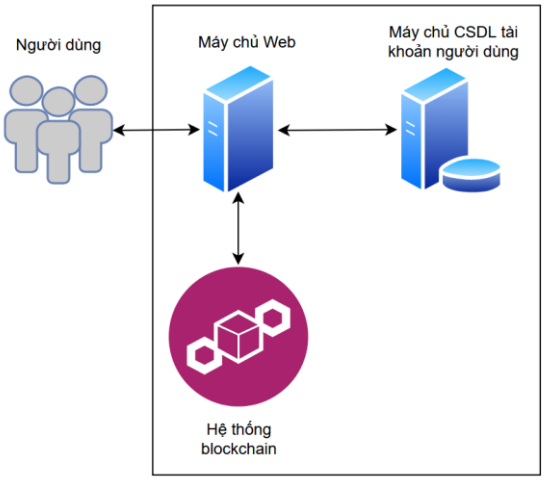


Hình 2. *Hoạt động của hợp đồng thông minh trong hệ thống chuỗi khối*

Trong bài báo này tác giả tập trung vào việc thiết kế, xây dựng và thử nghiệm hệ thống quản lý điểm trực tiếp trên nền tảng blockchain. Bài báo của chúng tôi gồm các phần: Phần 1 là giới thiệu, Phần 2 là mô tả về kiến trúc và các thành phần trong hệ thống quản lý điểm đề xuất, Phần 3 là xây dựng và triển khai thực nghiệm, Phần 4 là kết luận.

2. Đề xuất hệ thống quản lý điểm dựa trên công nghệ Blockchain

2.1. Đề xuất kiến trúc hệ thống quản lý điểm dựa trên công nghệ Blockchain



Hình 3. *Kiến trúc hệ thống quản lý điểm đề xuất*

Quá trình quản lý điểm được thực hiện bởi phòng đào tạo và phòng khảo thí. Hệ thống quản lý điểm trên nền tảng blockchain đề xuất trong bài báo này (Xem Hình 3) bao gồm những chức năng chính sau đây:

– Nhập điểm: Phòng khảo thí có quyền nhập điểm thi cho từng sinh viên trong các phiên thi. Hệ thống sẽ cho phép phòng khảo thí nhập các thông tin như mã số sinh viên, môn học, điểm số đạt được.

– Xem bảng điểm: Phòng đào tạo và sinh viên có quyền truy cập vào hệ thống để xem bảng điểm. Phòng đào tạo có thể xem bảng điểm của tất cả sinh viên, trong khi sinh viên chỉ có thể xem bảng điểm của chính mình.

– Cấp bảng điểm: Phòng đào tạo có quyền cấp bảng điểm cho sinh viên khi được yêu cầu. Sinh viên có thể yêu cầu cấp bảng điểm qua hệ thống, và phòng đào tạo sẽ xem xét yêu cầu và cung cấp bảng điểm tương ứng.

Để thực hiện các chức năng kể trên hệ thống cần có thành phần:

– Máy chủ web: chứa giao diện người dùng, các chức năng chính của hệ thống,

– Máy chủ CSDL tài khoản người dùng: chứa dữ liệu tài khoản Phòng Khảo thí, Phòng Đào tạo, Sinh viên,

– Hệ thống Blockchain: chứa dữ liệu điểm của sinh viên,

– Người dùng: tương tác với hệ thống qua giao diện tại máy chủ Web.

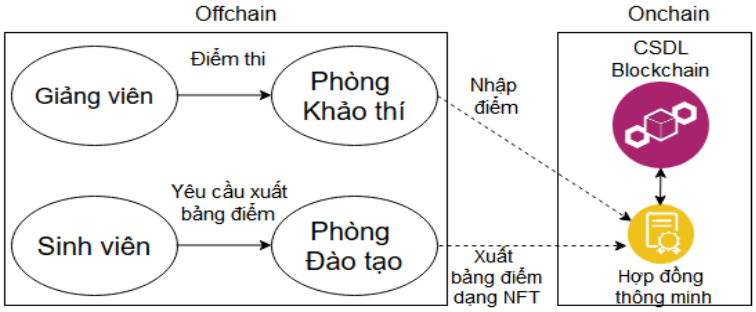
Để xây dựng các ứng dụng trong lĩnh vực giáo dục công nghệ sử dụng chuỗi cần được cấp phép (permissioned blockchain). Các công nghệ chuỗi khối riêng tư phổ biến hiện nay là Ethereum, Hyperledger Fabric, Quorum. Bảng 1 chỉ ra các đặc điểm chính của bốn công nghệ chuỗi khối kể trên [11]. Từ Bảng 1 thấy rằng trong thực tế các công nghệ chuỗi khối riêng tư kể trên sử dụng các cơ chế đồng thuận tối ưu, không tiêu tốn nhiều tài nguyên tính toán của hệ thống, thời gian trễ (thời gian thực hiện giao dịch) khá tương đồng nhau. Tuy nhiên công nghệ Ethereum có khả năng xử lý được nhiều giao dịch/ giây nhất. Vì vậy trong bài báo lựa chọn công nghệ Ethereum để xây dựng hệ thống quản lý điểm.

Bảng 1. *Đặc điểm của các công nghệ chuỗi khối cần được cấp phép*

Đặc điểm	Ethereum (geth)	Hyperledger Fabric	Quorum
Giao thức đồng thuận	PoA	PBFT	RAFT
Khả năng xử lý giao dịch/ giây (TPS)	~300	~200	~200
Độ trễ (giây)	~5	~5	~4
Ngôn ngữ lập trình hợp đồng thông minh	Solidity	GoLang, NodeJs	Solidity

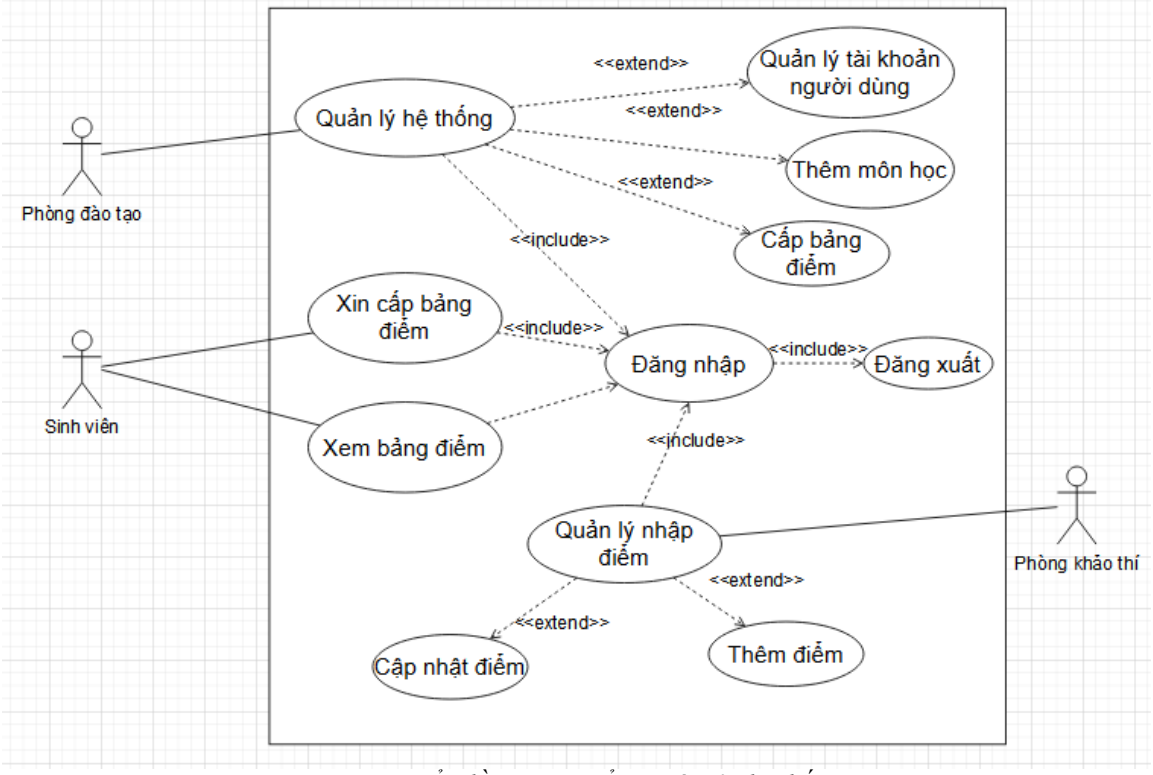
2.2. Luồng hoạt động của hệ thống

Quản lý điểm bắt đầu bằng quá trình nhập điểm. Trong hệ thống đề xuất phòng Khảo thí thực hiện chức năng này. Giảng viên chấm điểm bài thi và gửi điểm cho phòng Khảo thí. Khi phòng khảo thí nhập điểm, hệ thống sẽ ghi dữ liệu điểm của sinh viên vào chuỗi khối thông qua hợp đồng thông minh. Quá trình này đảm bảo rằng dữ liệu điểm được lưu trữ trên chuỗi khối sẽ không thể thay đổi và bị tác động bởi bất kỳ bên thứ ba nào. Khi sinh viên yêu cầu cấp bảng điểm, phòng đào tạo tiến hành truy xuất dữ liệu điểm từ blockchain để đảm bảo tính toàn vẹn và minh bạch. Quá trình quản lý điểm với hệ thống xây dựng trên nền tảng công nghệ chuỗi khối được mô tả trong hình 4, biểu đồ use-case của hệ thống được mô tả trong hình 5.



Hình 4. *Luồng hoạt động của hệ thống*

Trong hệ thống có ba tác nhân chính là Phòng đào tạo, Phòng khảo thí và sinh viên. Phòng đào tạo quản lý hệ thống với các thao tác: đăng nhập vào hệ thống, quản lý tài khoản sinh viên, xem bảng điểm của sinh viên và cấp bảng điểm cho sinh viên khi có yêu cầu. Phòng khảo thí thực hiện chức năng quản lý điểm của sinh viên với các thao tác: Đăng nhập vào hệ thống, nhận điểm từ giảng viên và nhập vào hệ thống, xem bảng điểm của sinh viên. Sinh viên có thể xem điểm của mình trên hệ thống và xin cấp bảng điểm.



Hình 5. *Biểu đồ use-case tổng quát của hệ thống*

2.3. Xây dựng hệ thống

```
function addPoint(PointDetail[] memory pointDetail , string memory studentId , string memory name) public onlyPKT {
    Student storage student = students[studentId];
    for (uint256 i =0 ; i < pointDetail.length; i++) {
        require(pointDetail[i].point > 0 && pointDetail[i].point <= 10 , "wrong point");
        pointSubject[studentId][pointDetail[i].subjectId] = pointDetail[i].point;

    }

    student.totalAddpontSubject = student.totalAddpontSubject + pointDetail.length;
    if(student.timeUpdate == 0  ) {
        listStudents.push(studentId);
        student.studentId = studentId;
        student.studentName = name;
        student.timeUpdate = block.timestamp;
    } else {
        student.timeUpdate = block.timestamp;
    }
}
```

Hình 6. *Mã nguồn chức năng nhập điểm (chỉnh sửa điểm)*

Để xây dựng hệ thống quản lý điểm dựa trên công nghệ chuỗi khối, trong bài báo lựa chọn các lựa chọn các công cụ sau:

- Solidity: sử dụng để viết thông tin hợp đồng thông minh.
- JavaScript thư viện Web3.js.

– Framework: Hardhat:
– Thư viện NFT: OpenZeppelin.
– Công nghệ blockchain: mạng testnet Goerli Ethereum

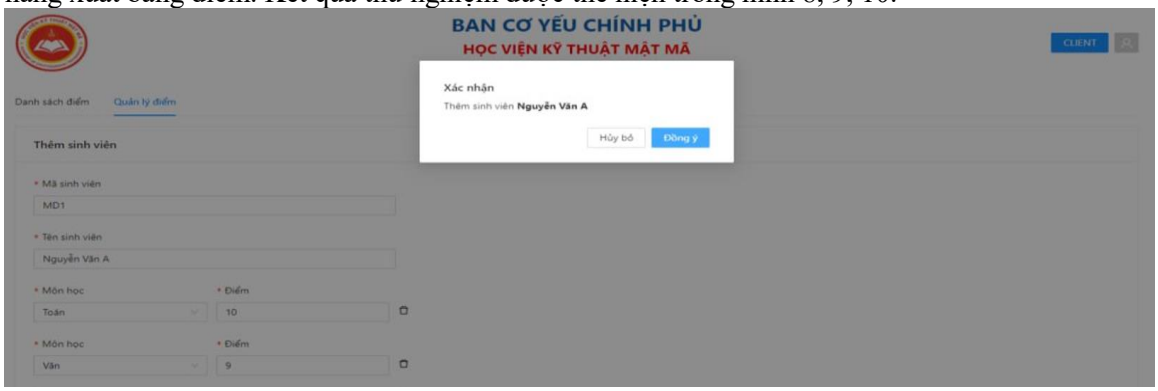
Mã nguồn các chức năng chính của hệ thống được thể hiện trong hình 6, 7.

```
function getPointOfStudent(string memory studentId) public view returns( string memory, uint256, PointOfStudentDetail[] memory, string memory) {
    Student storage student = students[studentId];
    PointOfStudentDetail[] memory pointDetail = new PointOfStudentDetail[](student.totalAddpontSubject);


    string memory studentName = students[studentId].studentName;
    uint256 timeUpdate = students[studentId].timeUpdate;

    for (uint256 i = 0; i < listSubject.length; i++) {

        if(pointSubject[studentId][listSubject[i]] > 0) {
            pointDetail[i].subjectId = listSubject[i];
            pointDetail[i].point = pointSubject[studentId][listSubject[i]];
    }

    }

    return (studentName, timeUpdate , pointDetail, nftPointStudent[studentId]);
}
```

Hình 7. *Mã nguồn chức năng xuất bảng điểm*

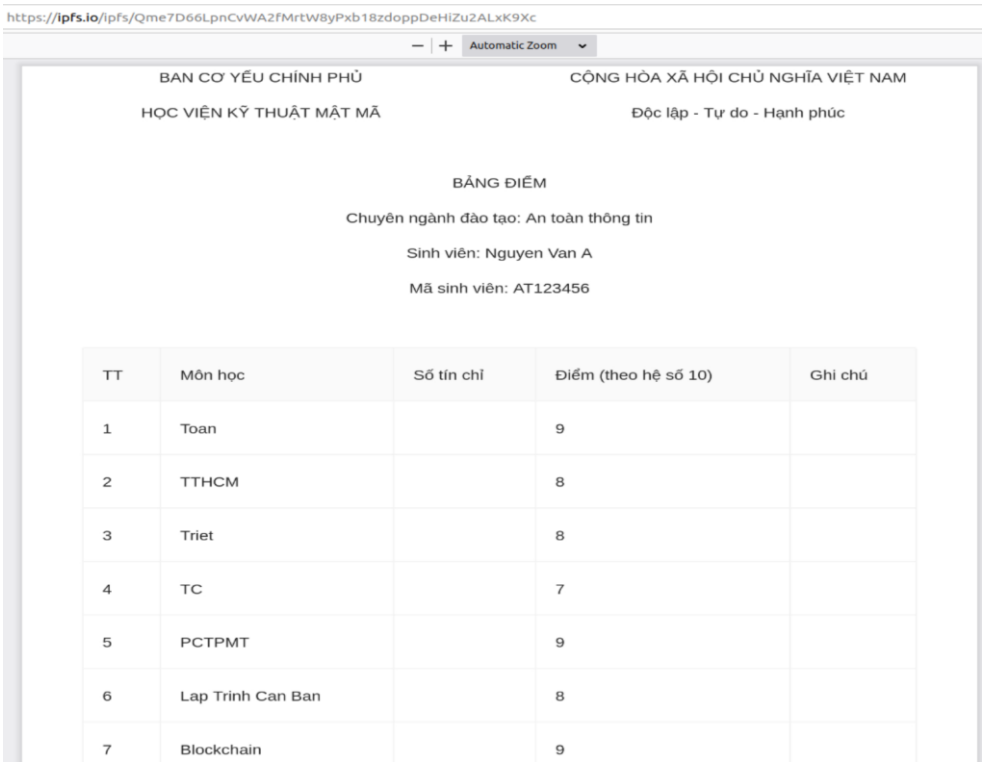
3. Thử nghiệm và đánh giá

Hệ thống quản lý điểm được triển khai trên máy tính có cấu hình như sau: CPU Intel i5 11400, SSD 512 GB, RAM 16 GB. Từ máy tính người dùng tiến hành truy cập vào hệ thống và thử nghiệm các chức năng chính của hệ thống: chức năng thêm điểm, chức năng xem điểm, chức năng xuất bảng điểm. Kết quả thử nghiệm được thể hiện trong hình 8, 9, 10.



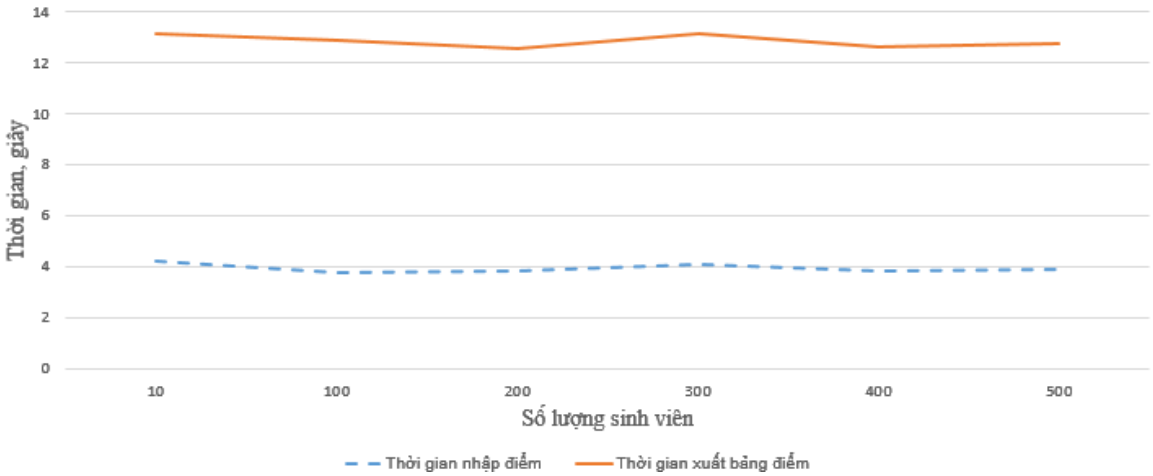
Hình 8. *Phòng KT thực hiện thêm điểm trong trang quản lý*

Hình 9. *Xem điểm theo mã sinh viên*



Hình 10. *Bảng điểm NFT xuất ra tệp PDF*

Thử nghiệm nhập điểm cho 500 sinh viên thấy rằng trung bình thời gian thêm điểm cho một sinh viên là 3,42 giây, trung bình thời gian xuất bảng điểm ra tệp PDF cho một sinh viên là 8,51 giây. Kết quả thử nghiệm được thể hiện trong hình 11. Từ hình 11 thấy rằng thời gian thêm điểm và xuất bảng điểm cho một sinh viên ổn định khi số lượng sinh viên tăng. Như vậy hệ thống hoạt động ổn định, phù hợp với cấu hình phần cứng và phần mềm hiện tại.



Hình 11. *Thời gian nhập điểm và xuất bảng điểm cho một sinh viên*

4. Kết luận

Trong bài báo này đã xây dựng và triển khai thử nghiệm hệ thống Quản lý điểm dựa trên công nghệ Blockchain. Hệ thống quản lý điểm đề xuất hoạt động ổn định, phù hợp với các cấu hình phần cứng và phần mềm sẵn có hiện nay. Hệ thống có thể được triển khai thực tế với chi phí thấp, đảm bảo các yêu cầu về tính năng cần thiết. Trong các nghiên cứu sau này chúng tôi sẽ thử nghiệm hệ thống trên các hệ thống chuỗi khối tự xây dựng để đánh giá chi tiết hơn các tham số hoạt động của hệ thống.

TÀI LIỆU THAM KHẢO/ REFERENCES

[1] C. Delgado-von-Eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias, "Blockchain Applications in Education: A Systematic Literature Review," *Applied Science*, vol. 11, no. 24, 2021, Art. no. 11811.

[2] M. Han, Z. Li, J.S. He, D. Wu, Y. Xie, and A. A. Baba, "Novel Blockchain-based Education Records Verification Solution," in *Proceedings of the 19th Annual SIG Conference on Information Technology Education*, 2018, pp. 178–183.

[3] O. S. Saleh, O. Ghazali, and M. E. Rana, "Blockchain based framework for educational certificates verification," *Journal of Critical Reviews*, vol. 7, no. 3, pp. 79-84, 2020.

[4] E.-Y. Daraghmi, Y.-A. Daraghmi, and S.-M. Yuan, "UniChain: A Design of Blockchain-Based System for Electronic Academic Records Access and Permissions Management," *Applied Science*, vol. 9, no. 22, 2019, Art. no. 4966.

[5] J. Garay, A. Kiayias, and N. Leonardos, "The bitcoin backbone protocol with chains of variable difficulty," *Annual International Cryptology Conference*, Springer, 2017, pp. 291-323.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *2017 IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[7] K. Salah and M. Khan, "IoT Security: Review, Blockchain Solutions, and Open Challenges," *Future Generation Computer Systems*, vol. 82, pp. 395-411, 2018.

[8] V. Buterin, "A next-generation smart contract and decentralized application platform," *White paper*, vol. 2, no. 37, pp. 1-36, 2014.

[9] A. Gervais, G. O. Karame, K. Wust, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 3-16.

[10] EIP-721, "ERC-721 Non-fungible token standard," EIP-721, 2018. [Online]. Available: https://eips.ethereum.org/EIPS/eip-721. [Accessed September 26, 2023].

[11] A. A. Monrat, O. Schelén, and K. Andersson, "Performance Evaluation of Permissioned Blockchain Platforms," *2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, 2020, pp. 1-8.