Non-transferable NFT-based Digital Certificate for Achievement Verification

Muhammad Rasyid Redha Ansori, Allwinnaldo, Revin Naufal Alief,
Ikechi Saviour Igboanusi, Jae Min Lee, and Dong-Seong Kim,
Networked Systems Lab., Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
{rasyidred, winnaldo, revinnaufal, ikechisaviour, ljmpaul, dskim}@kumoh.ac.kr

***Abstract*—To keep up with the most recent trends in rapidly growing industries, engaging in continuous learning and gaining more experience is necessary. Evidence of the completion of the learning process is typically presented in the form of a conventional certificate. Nonetheless, this conventional method of verification can be time-consuming and tiring. To address these issues, this paper proposes a method for using non-transferable Non-fungible Tokens (NFTs) as digital certificates for achievement verification and storing them in the Ethereum blockchain. Thus, learners need not worry about losing or damaging the certificate during verification. The proposed scheme is evaluated on the public Goerli test network, and a smart contract is created using the Solidity programming language.**

***Index Terms*—Achievement, Blockchain, Digital Certificate, Verification**

I. Introduction

Continuous learning is a must to keep up with the latest trends in the rapidly growing industries. One can learn and gain experience by going to conferences and workshops and taking online classes. After completing a program, registrants typically receive a certificate as evidence of their achievement. However, in order to verify these certificates, verifiers may need to contact the event or course providers. Moreover, traditional certificate systems have difficulty proving their authenticity [1].

The adoption of blockchain technology has expanded beyond the financial sector to include the information and security sectors [2], [3]. Blockchain creates a shared distributed ledger, providing a protected and entirely decentralized system, making it highly impossible for fraudulent users to alter anything contained in the blockchain. Therefore, users do not need to be concerned about losing or damaging the certificate during the verification process. In addition, the Ethereum blockchain developed the ERC-721 standard, also known as non-fungible tokens (NFT), which can improve the traceability of a learner's achievements. Therefore, blockchain technology is well-suited for verifying achievements [4].

There have been studies about issuing achievements using blockchain technology. Paper [4] proposed a digital badging system using the Ethereum blockchain for education to recognize achievements and specific skills of learners. However, this study did not use NFT, making tracking which institution issued and which user has the digital certificates can be more challenging to do. On the other hand, paper [1] implemented NFT to combat traditional academic certificate systems' challenges and improve traceability. The downside of this study is that their NFT can still be sent to other people. In contrast, academic certificates only belong to a particular person and are not supposed to be transferable. Therefore, to tackle the problems above, this paper proposes a blockchain-based framework for issuing achievements as a digital certificate by modifying the ERC-721 standard to make the NFTs not transferable to other users. This paper aims to offer protection against fake academic achievements and provide an easy and quick verification process.

The remainder of the paper is presented as follows. The proposed scheme is explained in Section II. Section III describes the experimental design and results, while Section IV discusses the conclusion and future work.

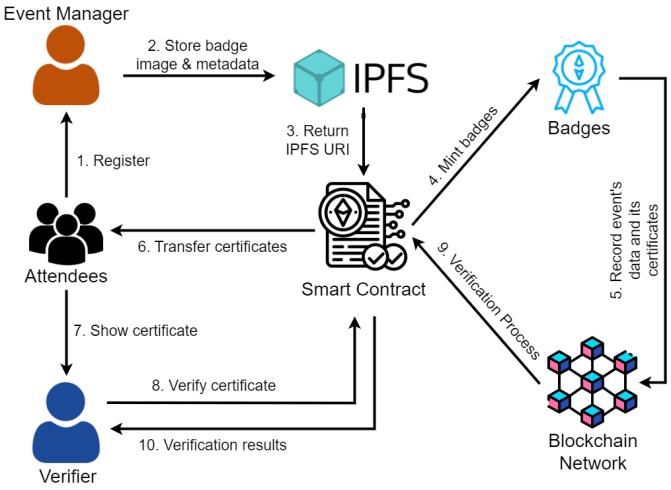

Fig. 1. Propose Scheme Structure.

II. Proposed Scheme

This section explains how the proposed scheme works to store achievements as digital certificates in the Ethereum blockchain network and verify them. This study aims to make each academic achievement unique to each user by using the modified ERC721 token standard for the digital certificate so that after being minted and transfer to the user, the user cannot transfer the digital certificate to other users. The workflow of the proposed scheme is depicted in Fig. 1.

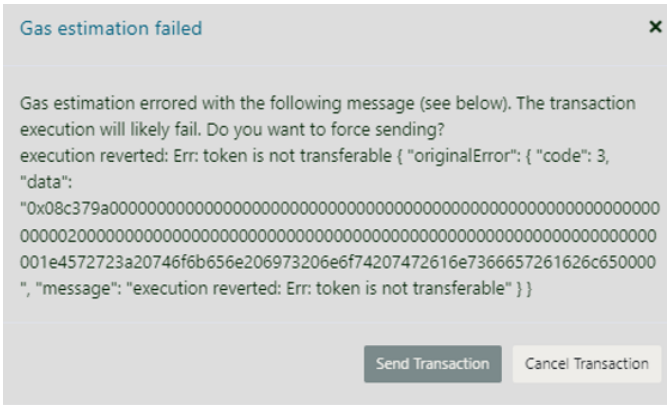

Fig. 2. Illustration When Attempting to Transfer Digital certificate to Another User

The first phase of the proposed scheme is minting the digital certificates. The attendees register their public addresses to the event manager. The event manager uses these public addresses to transfer the certificates after the attendees complete the program. After that, the event manager stores the image representing the event and its metadata in Interplanetary File Storage (IFPS) using the $createEvent()$ function in the smart contract. The metadata includes the attendees' names, public addresses, and the event's information such as name, description, date, place, and official website of the event. IPFS returns a URI after storing the image and metadata that will be used to mint the digital certificates. The information data from the event will then be recorded in the blockchain and digital certificates. The event manager can distribute the digital certificates to the attendees after the created event is finished using the smart contract's $distCertificate()$ function. These digital certificates are then stored in each attendee's digital wallet. If an attendee tries to transfer the certificate to other users, a notification will appear that the digital certificate is not transferable, as illustrated in Fig. 2.

After minting the digital certificates, the next phase is verifying process. The attendees can show their certificates to third-party verifiers. Then, the verifiers can check whether the attendee's certificate is genuine and not forged through the smart contract, using the $checkCertificate()$ function. If there is no record of the digital certificate in the blockchain network, that means the digital certificate is fake.

If there is wrong information in the attendee's data, the attendee can inform the event manager to issue a new digital certificate. After issuing a new digital certificate, the attendee can use the $burn()$ function to delete the previous digital certificate. The deleted certificate cannot be retrieved anymore, so the user has to be careful before deleting it.

III. Experimental Setup and Result

This study's experiment runs on Intel Core i5-7200U, 12GB of RAM, and 2TB of storage. The smart contract was written in Solidity programming language on Remix IDE and tested with Goerli Public Test Network. The transaction cost of the smart contract's proposed scheme is shown in Table I.

TABLE I
Smart Contract's Transaction Cost

Smart Contract	Type	Transaction Cost (Gas)
Platform Contract	Deployment	3,905,230
$createEvent()$	Function	422,288
$distCertificate()$	Function	290,075
$burn()$	Function	65,925
$eventDetails()$	Function	0
$checkCertificate()$	Function	0

Table I shows the highest costs when deploying the contracts to the network, which requires 3,905,230 Gas. Function $createEvent()$ aims to register the representative image and metadata for the event to the smart contract and has a gas cost of 422,288 for each certificate. $distCertificate()$ is a function to distribute digital certificates to the attendees, with a gas cost of 290,075 Gas per certificate. Users can erase their digital certificate using the $burn()$ function, with a transaction cost of 65,925 Gas. On the other hand, $eventDetails()$ and $checkCertificate()$ functions do not require transaction costs because they only access data in the blockchain network.

IV. Conclusion and Future Work

This paper presented a proposed scheme for easy and quick achievement verification using NFT technology. The proposed approach uses NFT as a digital certificate to make each achievement unique and allows easy traceability. It also modifies the current ERC721 token standard so that each digital certificate cannot be transferred to others once it is minted and transferred to other users.

Future improvement of this proposed scheme can be started by implementing batch minting to reduce the transaction cost of minting the digital certificates. The current implementation also lacks a function to check how many digital certificates a user has. Therefore, a better smart contract design is needed for future work.

V. Acknowledgement

This research work was supported by Priority Research Centers Program through NRF funded by MEST (2018R1A6A1A03024003) and the Grand Information Technology Research Center support program (IITP-2022-2020-0-01612) supervised by the IITP by MSIT, Korea.

References

[1] X. Zhao and Y.-W. Si, "NFTCert: NFT-Based Certificates With Online Payment Gateway," 2022.
[2] H. Tran-Dang and D.-S. Kim, "The Physical Internet in the Era of Digital Transformation: Perspectives and Open Issues," *IEEE Access*, vol. 9, pp. 164 613–164 631, 2021.
[3] I. S. Igboanusi, K. P. Dirgantoro, J.-M. Lee, and D.-S. Kim, "Blockchain Side Implementation of Pure Wallet (PW): An Offline Transaction Architecture," *ICT Express*, vol. 7, no. 3, pp. 327–334, 2021.
[4] V. Chukowry, G. Nanuck, and R. K. Sungkur, "The Future of Continuous Learning–digital Badge and Microcredential System using Blockchain," *Global Transitions Proceedings*, vol. 2, no. 2, pp. 355–361, 2021, international Conference on Computing System and its Applications (ICCSA-2021).