Leveraging Blockchain for Access Control and Credential Integrity in the Metaverse Platform

Mohtasin Golam, Esmot Ara Tuli, Md Facklasur Rahaman, Dong-Seong Kim, and Jae-Min Lee
Networked Systems Laboratory, Department of IT Convergence Engineering,
Kumoh National Institute of Technology, Gumi, South Korea.
(golam248, esmot, facklasur, dskim, and ljmpaul)@kumoh.ac.kr

***Abstract*—The metaverse-based education era poses challenges for verifying academic credentials for educational institutions, organizations, and individuals. Blockchain technology offers a practical solution to the traditional methods of verifying academic credentials, which are periodically tiresome and vulnerable to fraudulent activities. This article presents a system that uses smart contracts enabled by blockchain technology to oversee the validity of certificates and control user access. Every certificate is safeguarded using cryptographic measures, assigned a timestamp, and connected to distinct identifiers, guaranteeing integrity and immutability. Furthermore, user access control is implemented using attribute-based identity management, which employs sophisticated techniques for data management and traceability. A prototype was implemented and assessed to validate the proposed scheme's viability. The findings of the assessment illustrated that this solution eradicates intermediaries and mitigates the possibility of credential fraud.**

***Index Terms*—Access control, blockchain, certificate management, smart contract.**

I. Introduction

In the wake of the pandemic, the metaverse is a fusion of virtual and real-world spaces that has precipitated a transition towards online education and remote learning, fundamentally altering conventional learning models and reconfiguring the educational landscape [1]. Previously, certificates were traditionally paper-based, created and distributed by agencies, and posed challenges in terms of preservation, verification, and prevention of counterfeiting due to their complicated nature [2]. Blockchain technology provides a decentralized and transparent framework for preserving digital data that is immune to tampering [3]. Additionally, access control mechanisms are in place to guarantee user identity. These methods are being developed to safeguard academic certificates, improving their reliability, genuineness, and ease of access by utilizing their intrinsic characteristics and sophisticated cryptographic mechanisms [4].

The authors developed a storage system using attribute-based access control (A-BAC) and hyper-ledger fabric to make healthcare information secure [5]. Scalability, adoption challenges, governance, and security issues could be possible drawbacks to this approach. In [6], authors introduced a technique for verifying academic credentials using blockchain technology, whereas in [7], authors presented a decentralized ledger system for managing student information. Nevertheless, any interruptions in the blockchain network may have an effect on its functionality and accessibility in both cases. Authors in [4] introduced IoTChain, a decentralized system for storing and exchanging IoT data. This system utilizes the Ethereum blockchain to implement verifiable access control and A-BAC policies. Furthermore, a framework has been introduced in [8] that utilizes blockchain technology to enhance the functionality of intelligent autonomous access control systems. Nevertheless, this may necessitate extra computing power and network overhead, which could significantly impact the process of metaverse applications. A comparative summary of related concepts is presented in Table I.

According to the results of this comprehensive survey, the proposed model for achieving the objectives would make a major contribution and provide substantial motivation for achieving the objectives.

TABLE I: Comparative analysis summary of related concepts

Reference No.	Blockchain type	Blockchain tool	Data indegrity	Application type
3	Not specified	Ethereum	Yes	IoT data
4	Hyperledger	Hyperledger fabric	Yes	Healthcare
5	Not specified	Not specified	Yes	Certificate authentication
6	Not specified	Not specified	No	Student data management
7	Consortium	Not specified	Yes	IoT network

II. Proposed Methodology

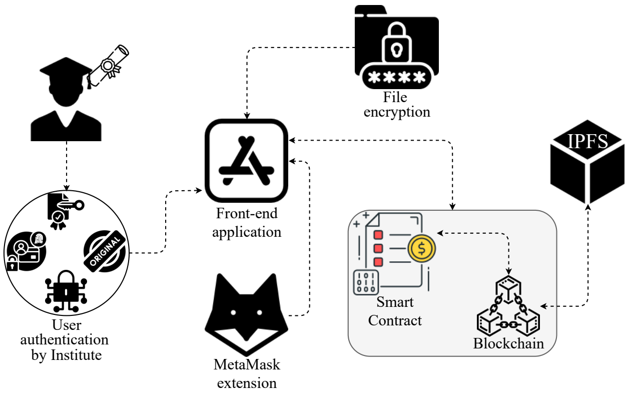


Fig. 1: Blockchain-based certificate management

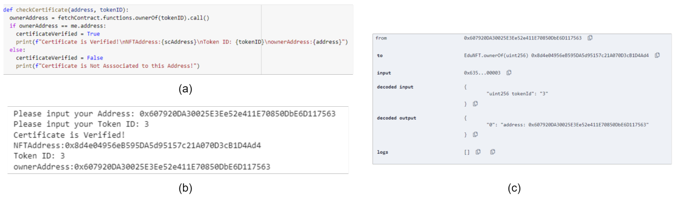
The proposed methodology illustrated in Fig. 1 entails the establishment of a metaverse educational institution where each student or learner is assigned a distinct identifier through blockchain-connected smart contracts upon enrollment. Courses are denoted as non-fungible tokens (NFTs), creating a cryptographic connection between learners and the courses they are registered for. Blockchain transactions are utilized to ensure secure access to courses within the metaverse, promoting transparent interactions. After finishing the course, a certificate is generated dynamically, which includes cryptographic components. This certificate is then encrypted and securely stored on the blockchain using the InterPlanetary File System (IPFS). From an architectural perspective, administrative and user modules supervise transactions. Users employ secure channels to transmit data. A cryptographic module guarantees the security of data, while a decryption module enables users to retrieve certificates securely. An access control system ensures the integrity of requests by rejecting those that do not pass tests, thereby preserving data security. Incorporating MetaMask and Ethereum improves administrative interactions while establishing a secure data-transmission communication channel. Financial prudence is maintained by implementing a process that discards transactions and monitors the balance thresholds of Ethereum (ETH).

TABLE II: Assessment of the applicability of proposed idea

Reference No.	Data integrity	Access control	Access type	Credential management
3	Yes	No	Not specified	No
4	Yes	Yes	Attribute-based	No
5	No	No	Not specified	Yes
6	No	No	Not specified	Yes
7	Yes	Yes	Attribute-based	No
Proposed model	Yes	Yes	Attribute-based	Yes

III. Performance Evaluation

The presented methodology for managing educational certificates on the metaverse platform is being assessed compared to similar approaches previously addressed in the paper. The aim of the proposed methodology is to actively diminish the probability of educational certificate forgery by controlling access management. Table II indicates that priority has been placed on utilizing the proposed idea rather than evaluating the outcome of the existing model's performance metrics.



```
def checkCertificate(address, tokenID):
  ownerAddress = fetchContract.functions.ownerOf(tokenID).call()
  if ownerAddress == me.address:
    certificateVerified = True
    print(f"Certificate is Verified!\nNFTAddress:{scAddress}\nToken ID: {tokenID}\nownerAddress:{address}")
  else:
    certificateVerified = False
    print(f"Certificate is Not Asssociated to this Address!")
```

(a)

```
Please input your Address: 0x607920DA30025E3Ee52e411E70850DbE6D117563
Please input your Token ID: 3
Certificate is Verified!
NFTAddress:0x8d4e04956eB595DA5d95157c21A070D3cB1D4Ad4
Token ID: 3
ownerAddress:0x607920DA30025E3Ee52e411E70850DbE6D117563
```

(b)

```
from            0x607920DA30025E3Ee52e411E70850DbE6D117563
to              EduNFT.ownerOf(uint256) 0x8d4e04956eB595DA5d95157c21A070D3cB1D4Ad4
input           0x635...00003
decoded input   {
                        "uint256 tokenId": "3"
                }
decoded output  {
                        "0": "address: 0x607920DA30025E3Ee52e411E70850DbE6D117563"
                }
logs            []
```

(c)

Fig. 2: Validation of the execution of certificate management: (a) *pseudocode* implementation in Python, (b) Python execution result on certificate verification, and (c) Smart contract execution results of getting the owner address of a Token

A. Implementation and Validation

The consequences of the certificate verification simulation include the implementation of pseudocode, the resulting simulation, and the execution of the smart contract illustrated in Fig. 2. The token ID and address serve the purpose of authentication, with the address derived from the device's public address. The token ID's owner's address is retrieved and compared to the input address to verify the certificate. The execution of the smart contract is also carried out to retrieve the certificate associated with the token ID.

IV. Conclusion and Future Work

Blockchain technology, smart contracts, and access control mechanisms are revolutionizing the management of educational certificates on metaverse platforms. This decentralized solution eliminates the need for central authority authentication, enhances data security, and prevents fraudulent activities. Smart contract technology ensures the authenticity of academic credentials, reducing labor-intensive verification procedures and direct communication with institutions. This proposed concept revolutionizes the management, verification, and trustworthiness of academic credentials in the virtual education environment. In the future, the emphasis will be on developing an enhanced version of the transactional implementation and attribute-based encryption approach for certificate production and incorporating AI for data classification.

V. Acknowledgment

This work was partly supported by Innovative Human Resource Development for Local Intellectualization program through the Institute of IITP grant funded by the Korea government(MSIT) (IITP-2024-2020-0-01612, 50%) and by Priority Research Centers Program through the NRF funded by the MEST(2018R1A6A1A03024003, 50%)

References

[1] J. N. Njoku, C. I. Nwakanma, G. C. Amaizu, and D.-S. Kim, "Prospects and challenges of metaverse application in data-driven intelligent transportation systems," *IET Intelligent Transport Systems*, vol. 17, no. 1, pp. 1–21, 2023.

[2] R. Xie, Y. Wang, M. Tan, W. Zhu, Z. Yang, J. Wu, and G. Jeon, "Ethereum-blockchain-based technology of decentralized smart contract certificate system," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 44–50, 2020.

[3] M. Golam, R. Akter, E. A. Tuli, D.-S. Kim, and J.-M. Lee, "Lightweight blockchain assisted unauthorized uav access prevention in the internet of military things," in *2022 13th International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 2022, pp. 890–894.

[4] Z. Ullah, B. Raza, H. Shah, S. Khan, and A. Waheed, "Towards blockchain-based secure storage and trusted data sharing scheme for iot environment," *IEEE Access*, vol. 10, pp. 36 978–36 994, 2022.

[5] Z. Sun, D. Han, D. Li, X. Wang, C.-C. Chang, and Z. Wu, "A blockchain-based secure storage scheme for medical information," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, p. 40, 2022.

[6] M. M. Rahman, M. T. K. Tonmoy, S. R. Shihab, and R. Farhana, "Blockchain-based certificate authentication system with enabling correction," *arXiv preprint arXiv:2302.03877*, 2023.

[7] S. I. M. Ali, H. Farouk, and H. Sharaf, "A blockchain-based models for student information systems," *Egyptian Informatics Journal*, vol. 23, no. 2, pp. 187–196, 2022.

[8] X. Hao, W. Ren, Y. Fei, T. Zhu, and K.-K. R. Choo, "A blockchain-based cross-domain and autonomous access control scheme for internet of things," *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 773–786, 2022.