IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE Education Society Section

Received 29 April 2024, accepted 12 May 2024, date of publication 3 June 2024, date of current version 12 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3408878

RESEARCH ARTICLE

Meta-Learning: A Digital Learning Management Framework Using Blockchain for Metaverses

MOHTASIN GOLAM, ESMOT ARA TULI, REVIN NAUFAL ALIEF, DONG-SEONG KIM, (Senior Member, IEEE), AND JAE-MIN LEE, (Member, IEEE)

Networked Systems Laboratory, Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 39177, South Korea

Corresponding author: Jae-Min Lee (ljmpaul@kumoh.ac.kr)

This work was supported in part by the Innovative Human Resource Development for Local Intellectualization Program through the Institute of Information and Communications Technology Planning and Evaluation (IITP) grant funded by Korean Government [Ministry of Science and Information and Communication Technology (MSIT)] under Grant IITP-2024-2020-0-01612, 50%; and in part by the Priority Research Centers Program through National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (MEST) under Grant 2018R1A6A1A03024003, 50%.

ABSTRACT The worldwide education landscape has transformed due to the COVID-19 pandemic, providing an opportunity to enhance virtual learning. Nevertheless, this transition has disadvantages, including less face-to-face interaction and the possibility of student seclusion. The metaverse, a digital realm, provides an optimal substitute for conventional virtual education. Nevertheless, its immersive nature poses issues for conventional digital learning management systems. This article proposes using blockchain technology and non-fungible tokens (NFTs) as unique identifiers to handle credentials and transactions in the metaverse while ensuring security effectively. This approach tackles difficulties associated with the administration of certificates, including issuing, maintaining records, ensuring traceability, and preserving integrity. Additionally, it establishes a fairly secure setting that effectively prevents data manipulation. The proposed approach entails the implementation of a smart contract that integrates a credential's transactions and an attribute-based access control mechanism. The research further addresses the challenge of limited storage resources caused by the dynamic nature of the metaverse and the requirement to manage huge quantities of data. The implementation results and applicability assessment confirm the feasibility of the proposed approach. Eventually, this study contributes to the ongoing discussion on the convergence of blockchain, NFTs, and smart contracts with its new perspective on digital learning management in the metaverse platform.

INDEX TERMS Access control, blockchain, digital certificates, digital learning management, non-fungible tokens (NFTs), smart contracts.

I. INTRODUCTION

The COVID-19 epidemic has increased the popularity of the metaverse, a virtual, three-dimensional (3D) environment that closely emulates the physical world. Prominent organizations and governmental entities are allocating resources towards advancing this digital platform, encompassing a diverse range of technologies that function harmoniously to offer many facilities within a simulated three-dimensional setting [1]. Metaverses presently encompass a range of activities, such as entertainment, gaming, business, learning, and virtual representations of physical urban environments [2]. The capacity for meta-communities to transcend geographical, temporal, and economic limits within virtual cyberspace presents an opportunity for individuals to dwell distinctively within real-world civilizations [3].

The potential impact of the metaverse on educational progress is anticipated to be substantial, as exemplified by the University of California, Berkeley's decision to organize an online graduation ceremony within the Minecraft platform [4]. Nevertheless, the main barriers to its growth are concerns about security and privacy. These include managing extensive quantities of data, profiling users, implementing measures to safeguard infrastructure and

The associate editor coordinating the review of this manuscript and approving it for publication was Nkaepe Olaniyi.

human well-being, and utilizing algorithms based on artificial intelligence (AI) [1], [5]. Recent technological occurrences encompass the unauthorized utilization of wearable technology, cloud storage, illicit digital currency acquisition, and misinformation dissemination. The immersive nature, hyper-spatiotemporality, sustainability, interoperability, scalability, and heterogeneity of the metaverse pose significant issues in guaranteeing adequate security [6]. Unfortunately, the security measures might not always work as we want them to, and they might not be flexible enough for metaverse uses, especially in digital learning environments.

The metaverse poses distinctive obstacles to identity management, encompassing identity theft, fraudulent activities, and data breaches. Conventional frameworks, such as centralized and federated models, have demonstrated limitations in effectively tackling these challenges. Instances of cybercrime, such as the exploitation of Roblox and the hacking of OpenSea NFTs, underscore the significant vulnerabilities inside these systems [7]. These security breaches jeopardize individuals' digital lives, social connections, and assets. In digital settings such as the metaverse, self-sovereign identity (SSI) and attribute-based access control (ABAC) have emerged as significant frameworks for bolstering security and promoting user autonomy. The SSI empowers people to manage their data directly without a central authority [8]. On the other hand, ABAC offers adaptable access control that user, resource, or environment variables determine [9]. Users can control their digital identities and monitor activities across domains with clear permission by combining SSI and ABAC. It offers a progressive strategy for establishing resilient identity management systems that protect the complex network of user-avatar interactions and digital transactions within the metaverse [10].

The decentralized distributed ledger known as blockchain holds promise for addressing the constraints associated with technologies such as the metaverse. Immutability, reliability, anonymity, and traceability are vital features that can effectively address concerns related to data tampering on centralized learning platforms [11]. Blockchain technology can strengthen trust in wearable technology, IoT, and AI-integrated things by enhancing traceability and fortifying data transfers. Additionally, it improves comprehension of augmented intelligence by employing a hash function [12]. Blockchain technology can be utilized in metaverse environments to safeguard data confidentiality and traceability. The digital currency system is crucial for the transaction framework in the education sector, which functions through a decentralized network of peers utilizing blockchain technology [13], [14]. The decentralized characteristic of blockchain technology can be attributed to its peer-to-peer (P2P) network, wherein nodes validate new blocks and maintain a chain to ensure the consistent preservation of information [15], [16].

Smart contracts are algorithmic systems implemented on blockchain networks that carry out predefined conditions, resulting in decreased transaction expenses and more efficiency in digital interactions [17]. The flexibility and support for sophisticated features of Ethereum make it a preferred choice for developing smart contracts. These contracts could revolutionize how educational content is accessed, shared, and verified in the metaverse. Educational resources are subject to establishing terms and conditions for accessibility, distribution, and validation [18]. These contractual agreements facilitate the automation of diverse educational transactions, encompassing student registration, evaluation, and credential issuance, following predetermined criteria [19]. Incorporating this technology into the metaverse has the potential to generate an engaging, interactive, and efficient educational encounter.

The widely used Ethereum blockchain technology enables the implementation of smart contracts within a cryptography-based framework [16]. This allows for expanding its uses beyond digital currency transactions to encompass numerous industries. In the metaverse, the convergence of physical reality, augmented reality, and the internet has ushered in a novel era of digital asset management. The proposed framework provides improved security, privacy, cost-effectiveness, operational efficiency, and regulatory openness. The Meta-Learning system leverages the adaptability of intelligent contracts to establish a tailored 'crypto-legal' structure [20]. This framework streamlines administrative procedures, improves the dissemination of content, and enables the implementation of inventive pedagogical methods through the utilization of virtual and augmented reality technology. Preserving user confidentiality and privacy is of utmost importance, and integrating blockchain technology with intelligent contract-based transaction processing has the potential to emerge as a significant solution within the Meta-Learning domain.

The following are the relevant contributions in this work to address this disparity:

- Introduce a concept called ''Meta-Learning,'' which delves into how Ethereum's smart contracts can revolutionize digital learning by providing a secure, transparent, and efficient educational content delivery and credential verification framework.
- The proposed framework can mitigate security risks using smart contract-based digital transaction solutions. Furthermore, an access control mechanism for user authentication allows users to secure access while ensuring service providers' identity management benefits.
- The proposed framework uses an NFT-based ERC-20 token called ''EDUMETA TOKEN'' for secure authentication in the Meta-Learning system. The ''EduToken'' token is used to access the verified user's education material. Similarly, the proposed approach uses an NFT-based token to verify the user certificate and ensure reliability in credential management.
- Finally, it demonstrates the framework's feasibility by analyzing and assessing existing approach constraints and conducting a comparative analysis regarding metaverse adoption.

TABLE 1. Comparative Analysis of Existing Approaches and the Proposed Approach in Metaverse Environments.

Ref	Year	BT	Description	SC/NFTs	Implementation	BAA
[21]	2023	Public	Use blockchain and smart contact for academic certificate verification	NFTs	✓	Certificate verification
[22]	2022	Permissioned	Blockchain for students and faculty members' data Course registration records Exam marks records	NFTs, SC	✓	Information storing
[23]	2020	Permissioned	certificate template and certificate information are stored in blockchain	SC	✓	Information storing & verification
[24]	2023	Web3	Educational metaverse for social learning. Learners are able to socialize and share knowledge.	Not Specified	✗	Secure data collection & storage
[25]	2023	Public	Metaverse for collaborative Product-Service Systems (PSS) to achieve University 5.0. Ethereum blockchain to verify academic achievements	SC	✓	Certificate verification
[26]	2023	Public	Use the metaverse as a form of virtual exhibition for maker education	NFTs	✓	Digital ownership
Proposed	2024	Public	Metaverse framwork for distance learning. NFT based secure payment and educational material controll.	NFTs	✓	Certificate & financial transaction

*__BT__: Blockchain Type, *__SC/NFTs__: Smart Contract/ Non-Fungible Tokens, *__BAA__: Blockchain Application Area,
✓: Considered, ✗: Not Considered

II. RELATED WORKS

Before the COVID-19 epidemic, the metaverse transformed remote learning by providing pupils with an immersive, 3D virtual world. This technology exceeds conventional video-based remote education by enabling students to simulate real-life scenarios in a regulated virtual environment. This new strategy enhances the quality of education and removes constraints related to time and location, providing a viable alternative to conventional distance learning approaches. The metaverse is increasingly used in STEM education to enhance practical learning experiences in various fields. Students participated in virtual radioactive experiments on the Second Life metaverse platform, replicating the hands-on experience of a traditional classroom [27]. Additionally, students have been able to replicate conventional classroom experiences through virtual experiments on Second Life, while 40 students have learned airplane maintenance in a VR setting [28]. The effectiveness of these trainings has been assessed using the System Usability Scale (SUS) and the Igroup Presence Questionnaire (IPQ). The metaverse-based operating room has also been used for lung cancer surgery training, demonstrating its ability to replicate complex procedures in a safe virtual environment [29]. These studies highlight the transformative potential of the metaverse in educational settings.

With the help of AI, blockchain, IoT, intercommunication, and learning logic, a complex edu-metaverse is constructed. Based on this, building elements transformed educational factors, such as teaching standards, assessment, and teaching circumstances [30]. To accomplish secure authentication, resource tracking, ownership verification, and secure data sharing, blockchain is considered an essential element of the metaverse [31]. Ensuring security is of utmost importance in the metaverse. It pertains to sensitive data such as biometric information used for authentication, human identification, and verification [32], [33], [34]. Cui et al. [24] suggest an educational framework for social learning environments based on blockchain technology. In this context, blockchain technology is regarded as a means to guarantee transparency and traceability for physical and virtual students. Here, safety concerns are not taken into account. Mourtzis et al. [25] propose a blockchain-based educational metaverse where blockchain is used to verify students' academic achievements. Hwang [26] propose NFT-based ownership in metaverse exhibitions in maker education.

Table 1 compares the proposed metaverse framework and previous research on educational metaverse platforms. Blockchain technology has been studied in academic and economic contexts, but its application in Meta-Learning systems has yet to be thoroughly investigated. Education involves distributing knowledge and financial activities, where money transactions play a significant role in both the physical and virtual worlds. This work proposes a new approach that utilizes a non-fungible token (NFT)-based system to enhance security in authentication, certificate verification, and transaction validation within the Meta-Learning system. This guarantees the trustworthiness and safety of financial transactions, improving the reliability and effectiveness of educational services in the metaverse.

A. CREATIVIA METAVERSE PLATFORM

A new era of education is being ushered in by the development of many metaverse-based educational platforms in multiple countries (such as the United States, South Korea, China, and other developed nations). South Korea is one of the pioneers in the creation of metaverse-based platforms. Much research has already been conducted, and applications are being developed. There are also numerous ongoing metaverse application development processes in South Korea. Here, we focus on the more substantial and large-scale examples "Creativia" [35]. Creativia is a leading metaverse platform combining education services, research tools, exhibitions, blockchain (Pure-Chain), and more. Figure 1 shows a functional block diagram of the Creativia metaverse platform. Creativia exhibition platform creates a mirror world of the 5G Idea Factory Center and 5G Innovation Experience Center, which is physically located inside Kumoh National Institute of Technology, Gumi, Korea [36]. Figure 2 illustrates the mirror world of Kumoh National Institute of Technology (KIT) in the Creativia metaverse. Creativia is a testbed for researchers to test and run metaverse simulation code using this platform. Real-time industrial monitoring in the metaverse is an essential feature of Creativia, which provides monitoring of the industrial production status and controls them using a high-speed 5G 28 GHz B2B network. An NFT-based offline and online token is integrated into the Creativia

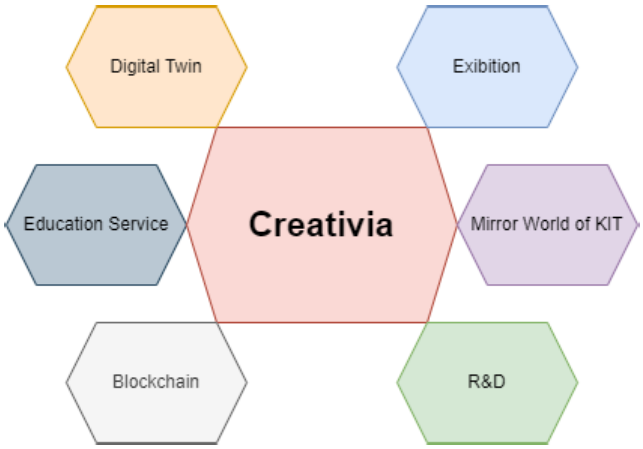

FIGURE 1. Functional block diagram of "Creaitevia".

platform. The research investigates the influence of the Creativia platform on metaverse-based education and its role in developing digital learning infrastructures like Meta-Learning. Creativia, an innovative platform that integrates immersive technology, blockchain, and high-speed networks, aims to create a diverse educational environment.

III. FRAMEWORK AND COMPONENTS OF META-LEARNING

Scholarly articles focus on many aspects of the metaverse, such as hardware, networking, computing, virtual platforms, payment services, software, and applications used for digital education [37]. The findings highlight the metaverse's complex and diverse technological aspects, suggesting its potential applications in education beyond distant learning. The security aspects of metaverse applications for education have yet to be thoroughly investigated [38]. This study aims to fill the gaps by introducing a framework that brings together important parts and focuses on important security issues for metaverse-based educational applications, especially regarding transactional processes, managing user access, and keeping credentials safe. This approach ensures the metaverse remains a secure, innovative, and efficient digital learning platform.

FIGURE 2. Mirror world of Kumoh National Institute of Technology in Creativia metaverse platform.

A. PROPOSE FRAMEWORK

This work proposes a blockchain and NFT-based digital learning management system in the metaverse that any institution can implement by making minor changes following institutional demands and criteria. The proposed solution was primarily focused on online education processes or courses involving financial transactions on metaverse platforms. Online courses are well-liked by students and qualified professionals in various fields worldwide. These programs or learning activities are designed to help students develop their talents. The proposed Meta-Learning ecosystem is intended to facilitate the implementation of a digital educational learning system inside the metaverse education system. However, the proposed model does not focus on any particular institutional structure or administrative procedures; rather, it seeks to study how to offer education with security and authenticity. It is important to note that in most situations, this form of digital learning or course is not free and involves a financial transaction as a cost. The proposed Meta-Learning considers a blockchain-based system for financial transactions focusing on credential management. Meta-Learning comprises three core elements: user and certificate verification, the Meta-Learning model, and meta-factor authentication for financial transactions. Any institution, educational organization, or course provider can

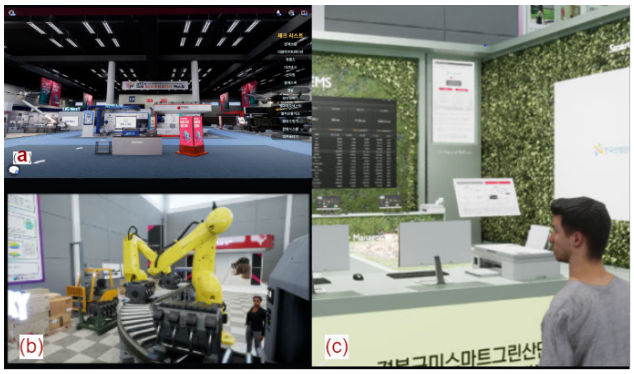

FIGURE 3. Different sections of Creativia. (a) Exhibition center (b) Metaverse-based research and development for Industrious IoT (IIoT) (c) Digital Twin.

adopt this system by including educational resources in the Meta-Learning framework. The metaverse's development appears directly related to the maturity of technologies, meaning that implementing the metaverse in education heavily depends on modern technology. As a result, various technologies can be used in education to build the metaverse's framework, which ensures important assistance for the elements both in the actual world and the metaverse.

B. ROLE OF BLOCKCHAIN IN META-LEARNING

Blockchain technology can potentially revolutionize asset ownership and management by promoting trust and transparency. It securely documents transactions, allowing users to possess and exchange virtual assets in the digital world [39]. In this methodology, the blockchain would function as a reliable record-keeping system for essential metadata linked to the data, such as unique signatures and information regarding access control. This guarantees data reliability and transparency while maintaining reasonable storage expenses. The raw data would be stored off-chain in a more scalable and cost-efficient system, such as the Interplanetary Filesystem (IPFS), which is more suitable for managing substantial data [40]. The combined method enhances the advantages of both technologies, enabling the blockchain to ensure the origin and security of data while utilizing the scalability and cost-effectiveness of off-chain storage options.

Another advantage is the ability to develop a complete financial structure for bridging the virtual and real worlds of the metaverse. The NFTs, in particular, make it possible to turn virtual goods into tangible assets. Users are allowed to trade virtual assets like real trading. Blockchain establishes this link between the real world and the metaverse [41]. Additionally, blockchain technology offers customization options, including a blend of public and private blockchains. After adequate identification verification, it allows everyone to access the permissioned network and provides select and defined permissions only for particular network operations. The procedure for the blockchain is briefly illustrated in Figure 4. Each block on the blockchain network contains

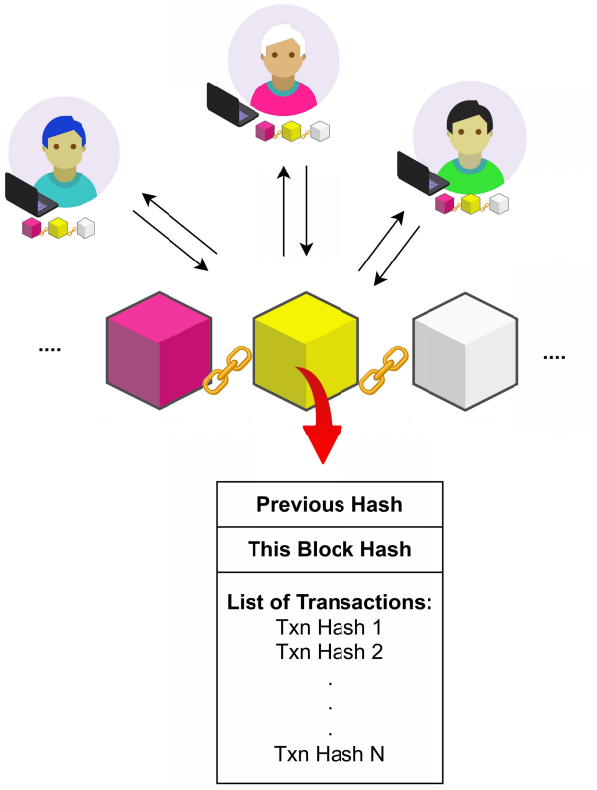

FIGURE 4. Overview of the blockchain' block structure.

a little bit of generic data. This data consists of the list of transaction hashes in the current block, the block's current hash, and the previous block's hash. Each block references the preceding block, creating a block link. This system is known as ''blockchain'' because of the behavior that links each block.

Blockchain technology employs a consensus method to uphold decentralization and prevent unauthorized alterations to transaction records. The system uses consensus, such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and Proof-of-authority (PoA), to ensure transaction security by linking each block to another. Information stored on the blockchain is available to all network participants who have contributed [42]. Decentralization enables information sharing among users and modifications made to a transaction's block to impact the current block hash, increasing the complexity of data manipulation. Any identical alterations to the linked block and previous hash are deemed invalid. Blockchain technology can prevent data tampering by monitoring participant data for any alterations [43]. Participants in the blockchain system replace the altered data with their own, unlike the traditional technique where the entire chain's data is changed by changing 51% of the participant's data.

C. THE ROLE OF NFTS

Non-fungible tokens (NFTs) may appear to be a complicated term initially, but they are quite easy to understand.

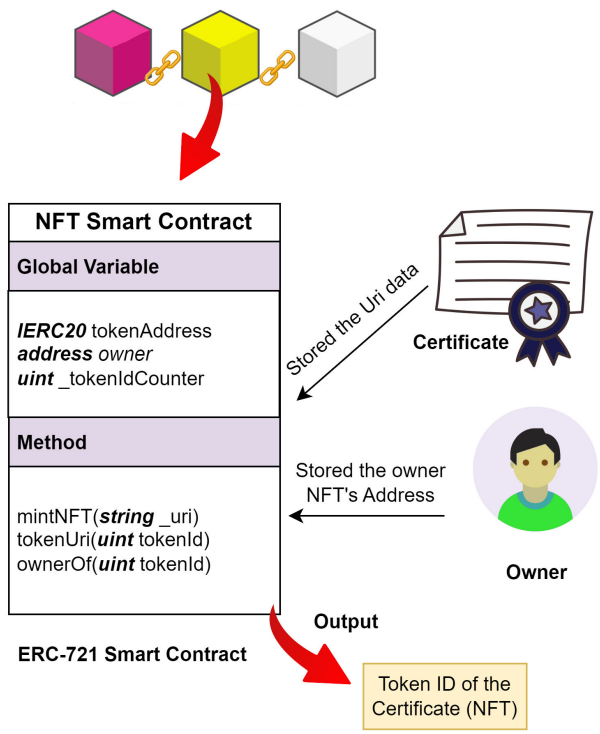

FIGURE 5. Illustration of the Non-Fungible Tokens (NFTs) workflow.

Non-fungible tokens (NFTs), which run on blockchain technology, are digital assets frequently connected to unique digital content, such as music or artwork. Due to a recent surge in public interest, a billion-dollar NFT industry has suddenly emerged [44]. Modern artists like Damien Hirst and Grimes and well-known consumer product companies like Coca-Cola and Nike are creating NFT collections. The price of a single NFT might reach millions or perhaps billions of dollars [45]. Tokens may be generically characterized as fungible or non-fungible based on their fungibility (NFTs). NFTs are distinct and distinguishable tokens. These tokens, however, cannot be exchanged for other NFTs. Furthermore, NFTs are indivisible, in contrast to fungible tokens. Figure 5 illustrates the implementation procedure for NFT. Creating a smart contract following the ERC-721 standard should be done initially.

The NFT's uniqueness and traceability could also be applied in the metaverse environment to define their assets. The characteristics of ERC-20 and ERC-721 tokens enable widespread adoption in several marketplaces [46]. The basic elements of an NFT's smart contract are shown in Figure 5. The IERC20 token, built on top of Ethereum in this article, is attached to the NFT smart contract, which limits the NFT's ability to be paid for using the previously produced token. In terms of the NFT smart contract mechanism, there are three principal methods, which are as follows:

1) **mintNFT**: This method generates the NFT. It required URI data in the form of a string, which resulted in the NFT certificate being used as an input and saved in the smart contract.
2) **tokenURI**: The token URI pointing to a certificate is returned by this procedure. Token ID is used as input to identify the calling certificate.
3) **ownerOF**: To determine who owns the NFT, this procedure is used. The token ID represents the NFT, and the procedure will return the owner address of the supplied token ID.

The NFT and owner addresses are recorded in the smart contract as a URI and an address, respectively, following the procedure shown in Figure 5. Then, as a result of saving this data, this information is gathered in the smart contract and accessible via the token ID.

IV. CONCEPTUAL METHODOLOGY

A. SMART-LEARNING

This subsection will discuss the Meta-Learning front-end of the proposed system. Each student or learner has an ID connected via blockchain (NFT). A course pool will be inside the metaverse, where learners can get information on the available courses or learning material. The pool has three sections: course name, bitcoin value, and corresponding token ID. Users can take or purchase the course with an NFT token connected to their ID. The course room will unlock after finalizing the payment using a blockchain transaction. Learners can meet others taking the same course through their real-time presence inside the metaverse. The proposed Meta-Learning 3D module is developed using Unity 3D with *C#* script. A generalized framework that could be applied to any metaverse learning system rather than creating 3D structures of the course material. The proposed architecture uses blockchain technology, non-fungible tokens (NFTs), and smart contracts to manage educational content and credentials in the metaverse. NFTs transform each item into a trackable, protected digital asset, simplifying academic confirmation and intellectual property rights protection. Smart contracts automate resource management by controlling access, distribution, and accreditation, ensuring only authorized individuals can view or modify content, improving the security and reliability of educational transactions in the metaverse.

B. IDENTITY AND ACCESS CONTROL MANAGEMENT

The metaverse, a virtual realm merging physical reality, digital environments, and the internet, poses difficulties in verifying identity and controlling access. Conventional identity management systems are vulnerable to exploitation through phishing, hacking, and manipulation of smart contracts. The metaverse may incorporate sophisticated access control techniques, like self-sovereign identity (SSI) systems and attribute-based access control (ABAC), working together to protect and manage identity attributes. This partnership enhances security, upholds privacy, and allows users to share only necessary information for specific access requests without revealing their complete identity. The access control system in this study integrates SSI and ABAC concepts with blockchain technology to improve data protection

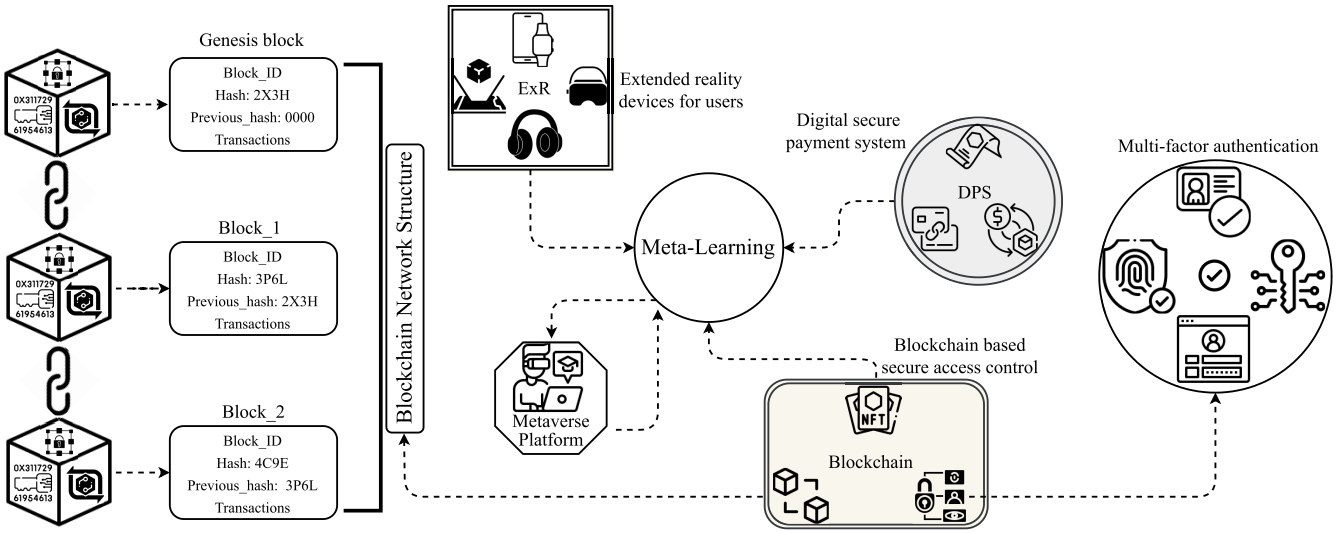

FIGURE 6. Overview of the conceptual architecture metaverse-based distance learning method.

and control [47]. This architecture enables the real-time association of verifiable credentials (VCs) with access control policies using permission validators. These validators link a user's unique decentralized identifiers (DIDs) and VCs to the roles or attributes in access control policies. This lets accurate and situation-sensitive access decisions be made. This method facilitates safe and independent data retrieval in digital settings, especially in systems controlled by blockchain infrastructures. The functionalities of DIDs (Decentralized Identifiers) and VCs (Verifiable Credentials) are detailed below:

- Decentralized Identifiers (DIDs): DIDs are crucial elements inside SSI frameworks. These distinct, user-created IDs rely on decentralized networks such as blockchains, which are reliable databases for verifying authenticity and integrity [48]. Every DID is associated with a corresponding document that contains metadata and public keys. This linkage guarantees secure communication and strengthens the principles of decentralization and user sovereignty in SSI systems.
- Verifiable Credentials (VCs): To ensure their legitimacy, reputable organizations like educational institutions or employers issue VCs, which are cryptographic digital attestations [48]. These credentials are saved in users' digital wallets, enabling them to be presented for transactions. The architecture of VCs enables the selective disclosure of qualities, enhancing user privacy by limiting personal data exposure.

The workflow diagram of Meta-Learning is given in Figure 7. The flowchart "B" illustrates the user's initial interaction with the identity management system, starting with the request for a VC. The Identity Manager issues a VC registered with VC Registry B and creates a DID. The user sends a presentation to the Verifier, who verifies the credentials' authenticity. Incorrect login information denies access, while correct login information forwards the request to the Access Control Engine. The Access Control Engine works with the Policy Decision Point to ensure the request complies with access control regulations. Once policy compliance is verified, the Policy Enforcement Point allows the user to access the requested resource. This protocol ensures secure identification and authorization using blockchain technology while maintaining data integrity and privacy.

C. REGISTRATION PROCESS

This subsection explains the interaction between the user and the Meta-Learning platform. As depicted in Figure 8, the workflow and interaction process within the Meta-Learning platform initiates with the user enrolling by providing vital personal and educational details. The education provider then verifies the authenticity and validity of this registration data. After the validation process, the ERC-20 token issuance module is activated to mint new tokens and adjust the user's token balance accordingly. These tokens function as digital credentials, providing the user with authorization to access the educational content and resources of the site. Using blockchain technology, notably through DIDs and VCs, makes the process secure and transparent and maintains user privacy. This approach improves the security of user credentials. It simplifies the access control mechanism, offering a scalable and effective solution for controlling user interactions and resource access in the Meta-Learning environment.

D. META-FACTOR AUTHENTICATION FOR FINANCIAL TRANSACTIONS

One of the goals of this effort is to secure financial transactions because the metaverse platform lacks any standards for financial architecture, and digital payment systems are susceptible to flaws in online transactions. The Jetson-Nano is a node connected to the blockchain network

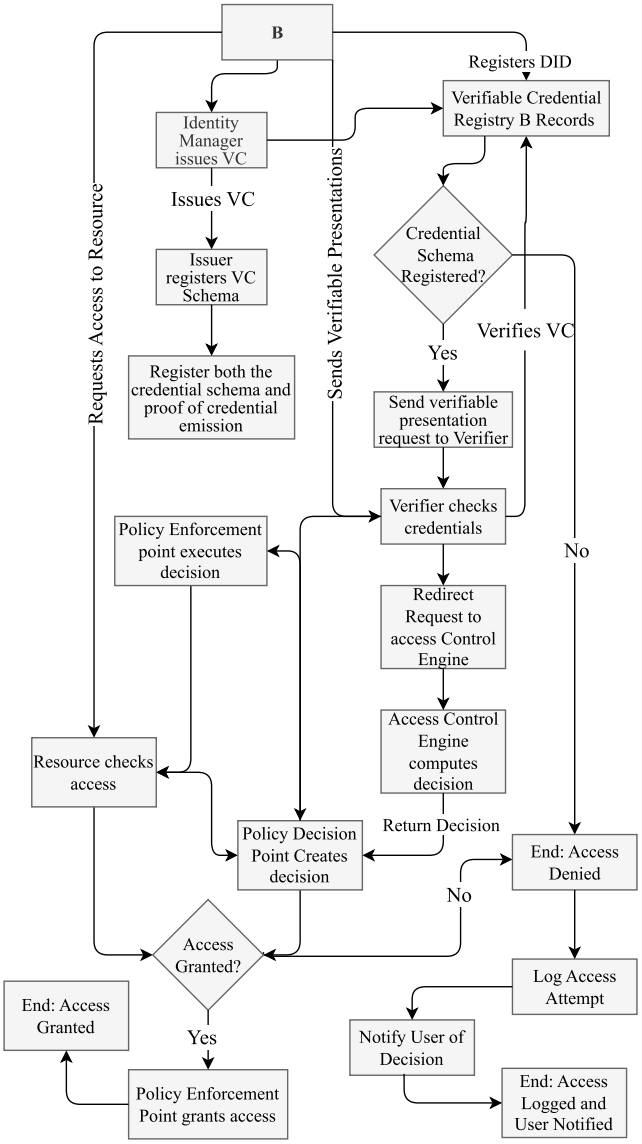

FIGURE 7. Designed workflow diagram for granting access using verifiable identity.

for meta-faction financial transaction authentication. Jetson-Nano has already been assigned a single public address to interact with blockchain properties. In this case, the blockchain property that is interacted with is the ERC-20 token. In authenticating financial transactions, this work seeks to propose the new ERC-20 smart contract token called "EDUMETA TOKEN." This smart contract followed the ERC-20 standard that Ethereum publishes. Some of the main general functions that exist in the general ERC-20 standard are *transfer*, *transferFrom*, *approve*, and *mint*.

Authentication for financial transactions relies on verifying the user's ownership of a specific address by checking its balance status. To ensure security, users input their private key, which is then used to derive their public address. This process guarantees that only the true owner of the public address can access the associated funds. Furthermore,

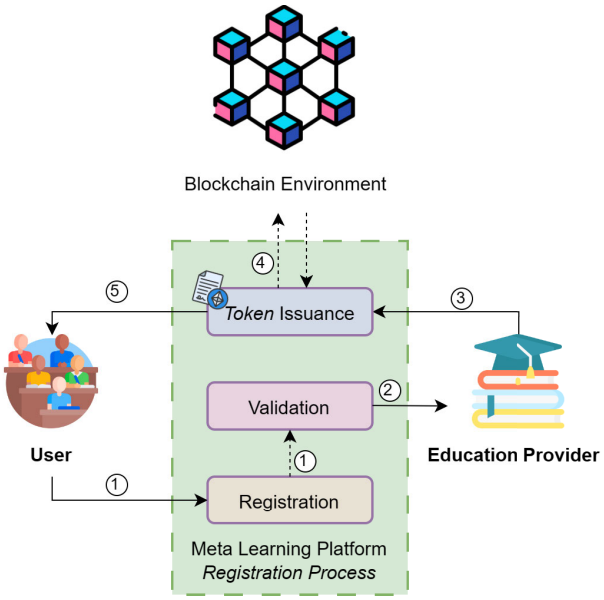

FIGURE 8. Registration and Token Issuance workflow.

the presence of EDUMETA Tokens in the user's wallet, confirmed by their public address derived from the private key using elliptic curve cryptography, grants access to Meta-Learning content. Thus, the private key serves as a secure means of authentication, uniquely possessed by the rightful owner, while enabling derivation of the corresponding public address for further validation. To limit the access, the address publisher could select the user that could receive the token, as the *mint* function could only be accessed by the smart contract publisher. Thus, this limits only the verified user with the EduToken to accessing the content of EduMeta. The *pseudocode* for checking the authentication is provided in Algorithm 1.

Algorithm 1 Authentication Through ERC-20 Token

Input: privateKey, tokenAddress
Output: authenticationResult

```
// Fetch account address based on Private Key
accountAddress = web3.account.fromKey(privateKey)
// Fetch EDUMETA balance from smart contract based on senderAddress
balance = tokenAddress.balanceOf(accountAddress)
if balance ≠ 0 then
    authenticationResult = True
else
    authenticationResult = False
end if
return authenticationResult
    =0
```

E. CERTIFICATION PROCESS

This subsection details the certification process involving the user, Meta-Learning platform, and education provider.

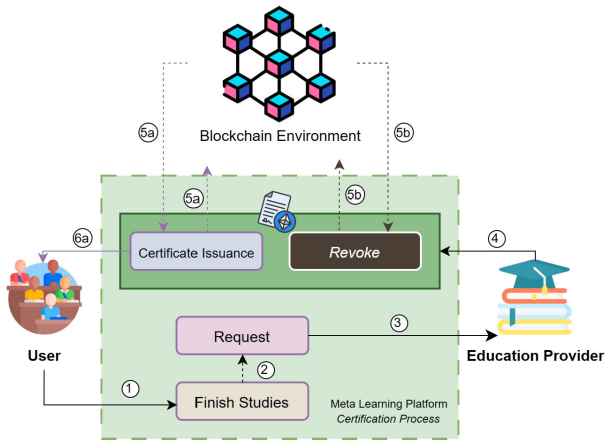

FIGURE 9. Certification-related workflow.

Figure 9 outlines the interaction between these entities. Upon completing their course or studies, the user initially requests a certificate from the education provider. Subsequently, the education provider verifies the user's fulfillment of requirements and triggers the relevant smart contract function through the Meta-Learning platform. This certificate-related function comprises two main functions: certificate issuance and certificate revocation. For certificate issuance, the smart contract generates (*mints*) an ERC-721 Token to signify course or study completion and assigns the certificate based on the user's public address. Additionally, the process accounts for scenarios where certificate revocation is necessary, such as instances of cheating. In such cases, the education provider can execute the *Revoke* smart contract function to invalidate the certificate.

F. USER AND CERTIFICATE VERIFICATION PROCESS

Like the financial authentication section setup, Jetson-Nano is assigned one public address to interact with blockchain information. First, the user must finish the course to generate the certificate of completion. After the course, the certificate is uploaded to the blockchain with the device's public address and URI address as input. This flow is similar to Figure 5. After successfully uploading the certificate to the blockchain, it can be verified via the smart contract's mechanism. The *pseudocode* for verifying the user and certificate is provided in Algorithm 2. In this *pseudocode*, the NFT smart contract address becomes one of the inputs to fetch the smart contract data. The smart contract data fetched is the NFT's owner's address. Token ID is input for getting the owner's address from an NFT. The reason is that the NFT is assigned a token ID as the record in the smart contract. Following the meaning of the non-fungible term in NFT, this token ID has only one owner address, making it unique.

Algorithm 2 Certificate Verification Through ERC-721 Token

Input: accountAddress, nftAddress, tokenID
Output: certificateVerified

```
// Fetch account address based on Private Key
// Fetch address from smart contract based on token ID
ownerAddress = nftAddress.ownerOf(tokenID)
if ownerAddress ≠ accountAddress then
    certificateVerified = False
else
    certificateVerified = True
end if
return certificateVerified =0
```

V. IMPLEMENTATION AND VALIDATION

This section describes how the proposed Meta-Learning framework has been evaluated and how it has been proven to be useful in real-world situations. The in-depth explanation of how the blockchain and NFT solutions, described in the previous part, are implemented. Blockchain deployment has been carried out with the aid of certain tools. The NFT's smart contract is developed using the *OpenZeppelin* library's ERC-721 standard for securing smart contract development [49]. To facilitate communication between the blockchain environment and the Python environment, the *web3.py* package is used along with *Alchemy* endpoint node. To be accessible from any device, the smart contract is additionally deployed to the public Ethereum Holesky test network through the same *Alchemy* endpoint. The Holesky network is selected for our blockchain environment because it supports a larger validator set. It enables realistic testing reflecting Ethereum's expanding scale and complexity, averaging 4 transactions per second (TPS).

A. ADVANTAGES OF SSI-INTEGRATED ABAC MANAGEMENT

In the proposed framework, by integrating ABAC with SSI, a sophisticated access control solution is achieved that effectively deals with security issues while upholding privacy. The following are the advantages of this robust framework:

- Precise Access Control: Attribute-Based Access Control (ABAC) grants access privileges based on attributes, offering a context-aware and accurate resource access mechanism.
- Flexibility: ABAC assesses access requests by considering several factors, enabling it to accommodate intricate and ever-changing access control needs.
- Interoperability: Integrating ABAC with SSI facilitates the seamless exchange of information and functionality between various administrative domains and applications.
- Dynamic and Scalability: SSI wallets include the qualities of being dynamic and scalable, allowing for the inclusion of additional features and credentials as required.
- Distributed Storage: Self-sovereign identity (SSI) wallets securely store credentials, eliminating centralized vulnerabilities and minimizing the risk of data breaches.

FIGURE 10. Financial Authentication Execution: (a) *pseudecode* implementation in Python, (b) Python execution result on financial authentication, and (c) Smart contract execution result of getting the account balance.

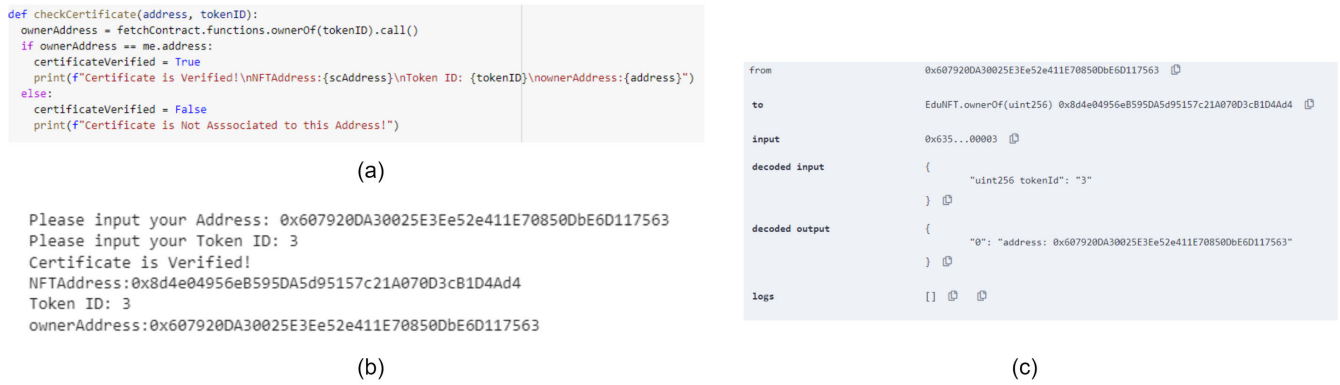

FIGURE 11. Certificate Verification Execution: (a) *pseudecode* implementation in Python, (b) Python execution result on certificate verification, and (c) Smart contract execution results of getting the owner address of a Token.

- Efficient Attribute Verification: Verifiable credentials stored in SSI wallets guarantee precise and reliable access control determinations.

The proposed framework utilizes these functionalities to enable efficient and safe access control decisions while minimizing the exposure of personal data. This makes it a superior method for addressing modern access control concerns.

B. FINANCIAL AUTHENTICATION ASSESSMENT

The simulation results of the financial verification are shown in Figure 10. The implementation of *pseudocode* Algorithm 1 is implemented in Python, as shown in Figure 10(a). The execution function result is shown in Figure 10(b). The address input in this simulation is the public address of the devices already assigned to interact with the blockchain. Based on Figure 10(b), the simulation result shows that the account has been verified as it has the EduMeta Token to interact with the EduMeta content. Another result is followed by Figure 10(c). In Figure 10(c), the smart contract result execution of getting the public address's balance is shown. Based on this result, we can see the balance is the same as the output in Figure 10(b). Therefore, since it has the same balance, it demonstrates that the device can successfully interact with the blockchain network.

C. CERTIFICATE VALIDATION ASSESSMENT

Figure 11 illustrates the simulation results for the certificate verification. Similar to the financial authentication result, three results are shown, which are *pseudocode* implementation, simulation result, and smart contract execution. The implementation of *pseudocode* is also done with Python on the Jetson-Nano device. The input for the certificate verification is the token ID and the address. The address is taken from the device's already-assigned public address. Then, the token ID is also input for this verification. To check the owner of an NFT, by following the ERC-721 standard, the token ID becomes the input. After the address of the token ID's owner is retrieved, it is compared with the input address to check the certificate's verification. The result is shown in Figure 11(b). The smart contract execution is also shown to retrieve the certificate based on the token ID. It is shown that the retrieved address from 11(c) can be used in the Algorithm 2, which is implemented in Figure 11(b). The resulting address is compared in Figure 11(a), resulting in certificate verification. These results also show that the device successfully interacted with the blockchain network.

D. SMART CONTRACT PERFORMANCE

In this section, a comparison between the previous works is made. Although works from [21], [50], and [51] do

TABLE 2. Gas cost comparison for the existing features.

Functions	Smart Contract Transaction Cost (Gas)			
	[21]	[50]	[51]	Proposed Contract
Certificate Issuance	117097	84286	123329	**84314**
Revocation	-	-	27365	**24253**

TABLE 3. Functions accessibility.

Function	Entities	
	Education Provider	User
ERC-20		
Mint	✓	×
Transfer	✓	×
Check balance	✓	✓
ERC-721		
Mint	✓	×
Revoke	✓	×
Check balance	✓	✓

not provide the exact gas cost for their features, in this paper, we tried to recreate the smart contract based on the pseudocode that is provided by each work. The gas comparison is shown in Table 2.

For the certificate issuance, our smart contract and [50] have the lowest gas cost, tied at around 84300 gas, while others have quite a high issuance gas cost. Our proposed smart contract can achieve a lower gas cost as we use the ERC721 standard from *OpenZeppelin* library, which is suitable for certificate problem use cases. Our opposed smart contract also considers the revocation process, which is not discussed in [21] and [50]. In addition, compared to [51], our revocation function can achieve the lowest gas cost.

E. SMART CONTRACT ACCESSIBILITIES

Table 3 illustrates the accessibilities of each entity to execute smart contract functions. Our research emphasizes enhancing the access of the education provider, who controls certificate issuance and access to Meta-Learning platform content. Users are restricted to checking their balances in both ERC-20 and ERC-721 tokens. Specifically, for ERC-20 Tokens, transfers are restricted between users to prevent unauthorized access to the Meta-Learning platform by individuals who have not received EduMeta Tokens directly from the education provider. This approach also aims to strengthen security measures within the system.

VI. CONCLUSION AND FUTURE WORKS

This study proposed a blockchain-enabled and NFT-based framework, Meta-Learning, for a secure educational metaverse platform. In the proposed Meta-Learning, blockchain technology offers a safe and decentralized ledger system for generating, tracking, and protecting academic credentials. NFTs serve as digital identifiers for credentials, guaranteeing their distinctiveness and possession. Smart contracts on the blockchain automate and secure the credentialing process, creating a transparent record of all transactions. The attribute-based access control system manages access to credentials and educational resources. The validity of the proposed framework for smart contract transactions has been confirmed through comparative analysis, demonstrating lower gas costs for certificate issues and revocation than other works cited. This shows improved cost-effectiveness and feasibility in carrying out essential operations within the blockchain network. The detailed analysis of the accessibility of functions in Table emphasizes the complete nature of the framework in enabling critical functionalities like minting, transfer, and revocation of certificates and checking balances. This user-centric and adaptable approach in the educational setting of the metaverse safely handles credentials and transactions while adjusting to the evolving requirements of the metaverse. Although the Meta-Learning framework is designed for an education-based metaverse, this blockchain-based framework can be applied to any organization or institution where identity management is required.

The proposed framework will be merged with the Creativia platform in future research. This integration will utilize a pure-chain (layer two blockchain) algorithm. However, the metaverse's potential for security concerns is not constrained. This inspires future research directions, such as developing frameworks for Meta-Learning with more adaptive features that combine technology from various resource facilities to enhance flexible uses for academic users and learners. The proposed system employs Self-Sovereign Identity (SSI), where Zero-Knowledge Proofs (ZKP) can be used to grant users controlled access to their information for sharing with others or authorities. Future work will explore incorporating post-quantum zero-trust architecture into the proposed system, utilizing lightweight post-quantum encryption methods like lattice-based encryption and hardware-efficient Ring-LWE. These methods could facilitate scalable implementation for a large number of end-users, ensuring security in the face of quantum computing threats.

REFERENCES

[1] Y. Wang, Z. Su, N. Zhang, R. Xing, D. Liu, T. H. Luan, and X. Shen, "A survey on metaverse: Fundamentals, security, and privacy," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 1, pp. 319–352, 1st Quart., 2023.

[2] V. Dubey, A. Mokashi, R. Pradhan, P. Gupta, and R. Walimbe, "Metaverse and banking industry—2023 the year of metaverse adoption," *Technium, Romanian J. Appl. Sci. Technol.*, vol. 4, no. 10, pp. 62–73, Nov. 2022.

[3] F.-Y. Wang, R. Qin, Y. Yuan, and B. Hu, "Nonfungible tokens: Constructing value systems in parallel societies," *IEEE Trans. Computat. Social Syst.*, vol. 8, no. 5, pp. 1062–1067, Oct. 2021.

[4] H. Duan, J. Li, S. Fan, Z. Lin, X. Wu, and W. Cai, "Metaverse for social good: A university campus prototype," in *Proc. 29th ACM Int. Conf. Multimedia*, Oct. 2021, pp. 153–161.

[5] E. Ara Tuli, J.-M. Lee, and D.-S. Kim, "Integration of quantum technologies into metaverse: Applications, potentials, and challenges," *IEEE Access*, vol. 12, pp. 29995–30019, 2024.

[6] C. Bermejo Fernandez and P. Hui, "Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse," 2022, *arXiv:2204.01480*.

[7] A. Abilkaiyrkyzy, A. Elhagry, F. Laamarti, and A. E. Saddik, "Metaverse key requirements and platforms survey," *IEEE Access*, vol. 11, pp. 117765–117787, 2023.

[8] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103059–103079, 2019.

[9] S. Ding, J. Cao, C. Li, K. Fan, and H. Li, "A novel attribute-based access control scheme using blockchain for IoT," *IEEE Access*, vol. 7, pp. 38431–38441, 2019.

[10] T. T. T. Ngo, T. A. Dang, V. V. Huynh, and T. Cong Le, "A systematic literature mapping on using blockchain technology in identity management," *IEEE Access*, vol. 11, pp. 26004–26032, 2023.

[11] W. Alkhader, N. Alkaabi, K. Salah, R. Jayaraman, J. Arshad, and M. Omar, "Blockchain-based traceability and management for additive manufacturing," *IEEE Access*, vol. 8, pp. 188363–188377, 2020.

[12] Q. Yang, Y. Zhao, H. Huang, Z. Xiong, J. Kang, and Z. Zheng, "Fusing blockchain and AI with metaverse: A survey," *IEEE Open J. Comput. Soc.*, vol. 3, pp. 122–136, 2022.

[13] 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 Exp.*, vol. 7, no. 3, pp. 327–334, Sep. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405959521000928

[14] K. P. Dirgantoro, J. M. Lee, and D.-S. Kim, "Generative adversarial networks based on edge computing with blockchain architecture for security system," in *Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC)*, Feb. 2020, pp. 39–42.

[15] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019.

[16] J. Correas, P. Gordillo, and G. Román-Díez, "Static profiling and optimization of Ethereum smart contracts using resource analysis," *IEEE Access*, vol. 9, pp. 25495–25507, 2021.

[17] W. Zou, D. Lo, P. S. Kochhar, X. D. Le, X. Xia, Y. Feng, Z. Chen, and B. Xu, "Smart contract development: Challenges and opportunities," *IEEE Trans. Softw. Eng.*, vol. 47, no. 10, pp. 2084–2106, Oct. 2021.

[18] M. F. Rahaman, M. Golam, M. A. P. Putra, G. A. Haryadi, D.-S. Kim, and J.-M. Lee, "Blockchain empowered secure medical appointment for the patients using smart contract," in *Proc. Korea Commun. Soc. Conf.*, 2023, pp. 868–869.

[19] R. A. Mishra, A. Kalla, A. Braeken, and M. Liyanage, "Privacy protected blockchain based architecture and implementation for sharing of students' credentials," *Inf. Process. Manage.*, vol. 58, no. 3, May 2021, Art. no. 102512.

[20] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum, Zug, Switzerland, Yellow Paper 151, pp. 1–32, 2014.

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

[22] S. I. M. Ali, H. Farouk, and H. Sharaf, "A blockchain-based models for Student information systems," *Egyptian Informat. J.*, vol. 23, no. 2, pp. 187–196, Jul. 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110866521000797

[23] 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 Things Mag.*, vol. 3, no. 2, pp. 44–50, Jun. 2020.

[24] L. Cui, C. Zhu, R. Hare, and Y. Tang, "MetaEdu: A new framework for future education," *Discover Artif. Intell.*, vol. 3, no. 1, p. 10, Mar. 2023.

[25] D. Mourtzis, J. Angelopoulos, and N. Panopoulos, "Metaverse and blockchain in education for collaborative product-service system (PSS) design towards university 5.0," *Proc. CIRP*, vol. 119, pp. 456–461, Jan. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2212827123004900

[26] Y. Hwang, "When makers meet the metaverse: Effects of creating NFT metaverse exhibition in maker education," *Comput. Educ.*, vol. 194, Mar. 2023, Art. no. 104693. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0360131522002640

[27] H. Kanematsu, T. Kobayashi, D. M. Barry, Y. Fukumura, A. Dharmawansa, and N. Ogawa, "Virtual STEM class for nuclear safety education in metaverse," *Proc. Comput. Sci.*, vol. 35, pp. 1255–1261, Oct. 2014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050914011892

[28] H. Lee, D. Woo, and S. Yu, "Virtual reality metaverse system supplementing remote education methods: Based on aircraft maintenance simulation," *Appl. Sci.*, vol. 12, no. 5, p. 2667, Mar. 2022. [Online]. Available: https://www.mdpi.com/2076-3417/12/5/2667

[29] H. Koo, "Training in lung cancer surgery through the metaverse, including extended reality, in the smart operating room of Seoul National University Bundang hospital, Korea," *J. Educ. Eval. Health Professions*, vol. 18, p. 33, Dec. 2021.

[30] J. Zhong and Y. Zheng, "Empowering future education: Learning in the edu-metaverse," in *Proc. Int. Symp. Educ. Technol. (ISET)*, Jul. 2022, pp. 292–295.

[31] T. Huynh-The, T. R. Gadekallu, W. Wang, G. Yenduri, P. Ranaweera, Q.-V. Pham, D. B. Da Costa, and M. Liyanage, "Blockchain for the metaverse: A review," *Future Gener. Comput. Syst.*, vol. 143, pp. 401–419, Jun. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X23000493

[32] G. Thakur, P. Kumar, C.-M. Chen, A. V. Vasilakos, and S. Prajapat, "A robust privacy-preserving ECC-based three-factor authentication scheme for metaverse environment," *Comput. Commun.*, vol. 211, pp. 271–285, Nov. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366423003304

[33] K. Yang, Z. Zhang, T. Youliang, and J. Ma, "A secure authentication framework to guarantee the traceability of avatars in metaverse," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 3817–3832, 2023.

[34] J. Ryu, S. Son, J. Lee, Y. Park, and Y. Park, "Design of secure mutual authentication scheme for metaverse environments using blockchain," *IEEE Access*, vol. 10, pp. 98944–98958, 2022.

[35] *Cretivia, Open Research and Development Metaverse Platform*. Accessed: 2021. [Online]. Available: https://creativia.kr/

[36] C. Ifeanyi Nwakanma, J. Nkechinyere Njoku, J. Jo, C. Lim, and D. Kim, "'Creativia' metaverse platform for exhibition experience," in *Proc. 13th Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2022, pp. 1789–1793.

[37] Y.-M. Kang, "Metaverse framework and building block," *J. Korea Inst. Inf. Commun. Eng.*, vol. 25, no. 9, pp. 1263–1266, 2021.

[38] S.-M. Park and Y.-G. Kim, "A metaverse: Taxonomy, components, applications, and open challenges," *IEEE Access*, vol. 10, pp. 4209–4251, 2022.

[39] V. T. Truong, L. Le, and D. Niyato, "Blockchain meets metaverse and digital asset management: A comprehensive survey," *IEEE Access*, vol. 11, pp. 26258–26288, 2023.

[40] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," *IEEE Access*, vol. 8, pp. 59389–59401, 2020.

[41] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, and E. Dutkiewicz, "MetaChain: A novel blockchain-based framework for metaverse applications," in *Proc. IEEE 95th Veh. Technol. Conference: (VTC-Spring)*, Jun. 2022, pp. 1–5.

[42] I. S. Igboanusi, A. Allwinnaldo, R. N. Alief, M. R. R. Ansori, J. Lee, and D. Kim, "Smart auto mining (SAM) for industrial IoT blockchain network," *IET Commun.*, vol. 16, no. 18, pp. 2123–2132, Nov. 2022.

[43] M. R. R. Ansori, R. N. Alief, I. S. Igboanusi, J. M. Lee, and D.-S. Kim, "HADES: Hash-based audio copy detection system for copyright protection in decentralized music sharing," *IEEE Trans. Netw. Service Manage.*, vol. 20, no. 3, pp. 2845–2853, Sep. 2023.

[44] A. Colicev, "How can non-fungible tokens bring value to brands," *Int. J. Res. Marketing*, vol. 40, no. 1, pp. 30–37, Mar. 2023.

[45] C. Pinto-Gutiérrez, S. Gaitán, D. Jaramillo, and S. Velasquez, "The NFT hype: What draws attention to non-fungible tokens?" *Mathematics*, vol. 10, no. 3, p. 335, Jan. 2022.

[46] S. Casale-Brunet, P. Ribeca, P. Doyle, and M. Mattavelli, "Networks of Ethereum non-fungible tokens: A graph-based analysis of the ERC-721 ecosystem," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Dec. 2021, pp. 188–195.

[47] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, "SSIBAC: Self-sovereign identity based access control," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Dec. 2020, pp. 1935–1943.

[48] Md. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey," *IEEE Access*, vol. 10, pp. 113436–113481, 2022.

[49] OpenZeppelin. *Openzeppelin Contracts*. Accessed: Apr. 23, 2024. [Online]. Available: https://github.com/OpenZeppelin/openzeppelin-contracts
[50] K. V. Raghavender, S. Alankruthi, A. Akhila, T. Preethi, and M. Ashritha, "Decentralized smart contract certificate system using Ethereum blockchain technology," in *Proc. 2nd Int. Conf. Emerg. Trends Eng.*, 2023, pp. 452–461, doi: 10.2991/978-94-6463-252-1_48.
[51] D. Wankhede, V. Gaikwad, M. Karnik, V. Mishra, A. Kekane, S. Kapase, and O. Bakkam, "The decentralized smart contract certificate system utilizing Ethereum blockchain technology," *Proc. Comput. Sci.*, vol. 230, pp. 923–934, Jan. 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050923020252

MOHTASIN GOLAM received the B.Sc. degree in Electrical and Electronics Engineering (EEE) and the M.Sc. degree from the Department of IT Convergence Engineering, Kumoh National Institute of Technology, in 2018, Republic of Korea, where he is currently pursuing the Ph.D. degree. He is with the Network System Laboratory (NSL), as a Research Assistant, under the supervision of the ICT Convergence Center. His research interests include deep learning, metaverse applications, UAV networks, the IoT, and blockchain.

ESMOT ARA TULI received the B.Eng. degree in computer science and engineering from Jatiya Kabi Kazi Nazrul Islam University, Bangladesh. She is currently pursuing the integrated master's and Ph.D. degree with the Department of IT Convergence Engineering. She has been a full-time Researcher with the Networked Systems Laboratory, Kumoh National Institute of Technology, Gumi, South Korea, since September 2019. Her research interests include metaverse, digital twins, signal processing, and post-quantum blockchain.

REVIN NAUFAL ALIEF received the bachelor's degree in telecommunication engineering from Telkom University, Indonesia, in 2020. He is currently pursuing the master's degree with the Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi, South Korea. He is also a Research Assistant with the Network System Laboratory under the supervision of the ICT Convergence Centre, Kumoh National Institute of Technology. His research interests include blockchain, NFT transactions, tokenization for digital transactions, information and security, and machine learning.

DONG-SEONG KIM (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2003. From 1994 to 2003, he was a full-time Researcher with ERC-ACI, Seoul National University. From March 2003 to February 2005, he was a Postdoctoral Researcher with the Wireless Network Laboratory, School of Electrical and Computer Engineering, Cornell University, Ithaca, NY, USA. From 2007 to 2009, he was a Visiting Professor with the Department of Computer Science, University of California at Davis, Davis, CA, USA. He is currently the CEO and the Director of NSLab Company, Ltd., and the ICT Convergence Research Center (ITRC and NRF Advanced Research Center Program), supported by Korean Government. His research interests include the real-time IoT, industrial blockchain applications, and networked embedded systems. He is a Senior Member of the Association for Computing Machinery (ACM) and the Vice President of Korean Institute of Communications and Information Sciences (KICS).

JAE-MIN LEE (Member, IEEE) received the Ph.D. degree in electrical and computer engineering from Seoul National University, Seoul, South Korea, in 2005. From 2005 to 2014, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. From 2015 to 2016, he was the Principle Engineer of Samsung Electronics. Since 2017, he has been an Assistant Professor with the School of Electronic Engineering and the Department of IT-Convergence Engineering, Kumoh National Institute of Technology, Gyeongbuk, South Korea. His current research interests include industrial wireless control networks, performance analysis of wireless networks, and TRIZ.