논문 2022-2-5 http://dx.doi.org/10.29056/jsav.2022.12.05

원본 데이터를 제공하지 않는 메타버스 저작물 소유 증명 기법

김원빈*, 조용준*, 신동명*†

A Technique for Proof of Ownership of Metaverse Works without Providing Source Data

Won-Bin Kim*, YongJoon Joe*, DongMyung Shin*†

요 약

메타버스는 현실세계를 초월하는 세계를 의미한다. 이러한 메타버스는 디지털 데이터로 구현되어 있기 때문에 언제 어디서든지 이용하고, 복제하고 활용할 수 있는 특징을 갖는다. 따라서 데이터가 생성되고 공개되는 순간부터 데이터는 제한 없이 복제되고 이용될 수 있다. 이러한 환경에서 저작물의 저작권을 주장할 수 있는 방법은 데이터를 최초로 공개하였다는 근거를 제시하는 방법이 이용될 수 있다. 이를 통해 추후 복제되어 재사용되는 데이터에 대한 배타적 권리를 주장하고 불법 사용에 대응할 수 있는 근거를 확보할 수 있다. 하지만 저작물 데이터 원본을 공개하고 저작권 침해 검증에 이용할 경우 저작물에 포함된 중요 정보가 노출될 수 있으며, 데이터 크기가 증가할수록 저작권 검증에 많은 비용이 소요될 수 밖에 없다. 본 연구에서는 이러한 문제를 해결하기 위해 메타버스상에서 이용되는 저작물의 원본을 공개하지 않고도 저작물의 소유권을 검증할 수 있는 방법을 제시한다.

Abstract

Metaverse means a world beyond the real world. Since these metaverse are implemented in digital data, they can be used, duplicated and utilized anytime, anywhere. Therefore, from the moment the data is generated and disclosed, the data can be replicated and used without restrictions. In this environment, the method of claiming the copyright of the work can be used to suggest the basis that the data was first disclosed. This allows you to claim exclusive rights for data that is replicated and re-used later and secure the basis for responding to illegal use. However, when the source data is disclosed and used to verify the copyright infringement, important information included in the work may be exposed, and as the data size increases, it will be more expensive to verify the copyright. In this study, to solve this problem, we present a way to verify the ownership of the work without disclosing the source of the work used on the metaverse

한글키워드 : 메타버스, 저작권, 정보보호, 머클트리, 소유 증명

keywords : Metavers, Copyright, Information security, Merkle tree, Proof of ownership

* 엘에스웨어(주) 소프트웨어연구소 연구개발본부
† 교신저자: 신동명(email: roland@lsware.com)

접수일자: 2022.11.17. 심사완료: 2022.11.28.
게재확정: 2022.12.20.

1. 서 론

최근, 디지털 트윈과 가상현실 게임의 요소를 적극 활용하여 현실 세계의 활동 제약을 해소하려는 움직임이 나타나고 있다. 메타버스(Metaverse)는 이러한 기술 중 하나이다. 메타버스는 초월을 의미하는 Meta와 세계를 의미하는 Verse의 합성어이다. 따라서 현실세계를 초월한 가상의 세계를 의미하며, 기술적으로는 현실세계와 상호작용하여 활동할 수 있는 현실세계의 확장 공간으로 볼 수 있다. 이러한 메타버스는 디지털 데이터로 이루어지며, 메타버스 내부의 요소들도 모두 디지털 데이터로 이루어져 있다[1].

메타버스는 현실 세계와 상호작용하기 위해 현실 세계의 여러 요소를 이식하고 이용할 수 있도록 설계된다. 대표적으로 현실 세계에서 생성된 다양한 문화 콘텐츠를 예로 들 수 있다. 음악, 미술작품, 의상, 공연 등 다양한 문화 콘텐츠는 디지털화될 수 있으며, 디지털화된 문화 콘텐츠는 메타버스상에서 이용되거나 재생될 수 있다[1-3]. 따라서 현실 세계에서 발생한 코로나 19 감염병 사태와 같은 환경속에서도 공간의 제약 없이 현실세계에서 수행하던 활동을 이어서 수행할 수 있다. 하지만 이러한 메타버스 환경에서도 다양한 보안 위협이 등장하고 있다.

메타버스는 기본적으로 디지털 환경을 기반으로 한다. 따라서 모든 데이터는 0과 1로 구성되어 있으며, 복제가 매우 간단하다는 특징을 갖는다. 이는 현실 세계의 복제와 매우 다른 형태를 의미하는데, 현실세계의 복제는 물리적으로 완전히 동일한 개체를 만들 수는 없지만 메타버스 상에서의 복제는 완벽히 동일한 개체를 생성할 수 있다. 이러한 점이 메타버스 환경에서 저작권 분쟁의 원인이 될 수 있다. 현재에도 원저작자가 존재하는 특정 디지털 콘텐츠를 저작권 침해자가 먼저 디지털 자산화를 하거나 공개를 하거나 실제 소유하지 않은 저작물의 일부 데이터를 위조하여 저작권을 부당하게 획득하는 사례가 발생하고 있다. 따라서 메타버스 환경에서 저작물을 안전하게 관리하고 사용하기 위해서는 저작물에 대한 소유 증명 방식이 필요하다. 이러한 문제를 해결하기 위해 본 연구에서는 메타버스 환경에서 저작물을 등록하는 과정에서 저작물의 원본을 노출하지 않고도 저작물의 소유를 증명할 수 있는 방법을 제안한다.

2. 관련 연구

2.1. 저작권 분쟁

저작권은 시, 소설, 음악, 미술, 영화 등의 저작물에 대하여 창작자가 가지는 권리를 의미한다. 일반적으로 창작자가 저작물을 창작함과 동시에 창작물에 대한 소유권과 저작권을 가지며, 별도의 계약을 통해 저작권과 소유권을 제 3자에게 위임할 수 있다. 최근, 블록체인의 공동원장 개념을 이용하여 디지털 저작물을 블록체인상에 등록하고 토큰을 획득하는 NFT(Non-fungible token)가 등장하였다. NFT는 다른 토큰으로 대체될 수 없는 대체 불가능한 토큰을 의미하기 때문에 다른 토큰과 동일한 가격을 가질수는 있지만 서로 대체가 불가능한 유일성을 가지는 토큰이다. 따라서 디지털 데이터의 완전 복제가 가능하다는 특징을 넘어서 특정 디지털 데이터의 소유과 유일성을 증명할 수 있는 수단으로 이용되고 있다. 최근에는 이러한 NFT를 거래할 수 있는 마켓까지 등장하면서 NFT 시장이 빠르게 성장하고 있다.

NFT 마켓의 등장은 일반 사용자들이 블록체인과 NFT 기술에 대해 알지 못하더라도 디지털 자산화에 비교적 쉽게 접근할 수 있도록 하고 있다. 하지만 NFT는 현재 적절한 규제와 제도가 마련되어 있지 않기 때문에 NFT의 특성을 역이

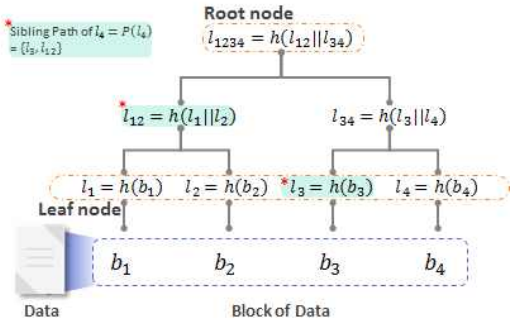

그림 1. Merkle Tree와 Sibling path
Figure 1. Merkle Tree and Sibling path

용한 저작권 침해 문제가 발생하고 있다. 디지털 데이터는 기본적으로 원본과 복사본이 구분되지 않는다. 따라서 원저작자가 생성한 디지털 데이터를 저작권 침해자가 복제하여 블록체인에 먼저 등록을 하거나 중복하여 등록할 경우 원저작자에 대한 저작권 침해가 발생할 수 있다. 따라서 저작물을 NFT로 등록하기 위해서는 저작물 원본을 소유한 원저작자인지를 검증할 필요가 있다.

2.2. 소유권 증명

메타버스 환경에서 디지털 데이터로 이루어진 저작물을 저작권 분쟁 없이 등록하고 사용하기 위해서는 저작물의 등록 과정에서 소유 증명을 수행해야만 한다. 소유 증명은 데이터 원본을 제공하는 방법과 데이터 원본을 제공하지 않는 방법으로 구분될 수 있다[4-8]. 이 중 데이터 원본을 제공하는 방법은 데이터 원본이 노출되는 문제와 함께 원본 데이터 전체를 전송해야 하는 문제가 존재한다. 반면, 데이터 원본을 제공하지 않는 방법은 데이터 전체 또는 일부를 변환하여 데이터 원본을 알 수는 없지만 데이터의 유일성을 검증할 수 있는 방법을 이용한다[9-10]. 이를 위해 본 연구에서는 Merkle Tree를 이용하여 소유 증명을 수행한다. Merkle Tree는 이진 트리의 일종이며, 같이 최하위 노드를 Leaf node, 최상위 노드를 Root node라고 한다. 그림 1과 같이 모든 Leaf node를 임의의 해시 알고리즘으로 해시화한 뒤, 2개의 해시 결과물을 같이 해시화하여 상위 노드를 생성하는 식으로 반복하여 하나의 Root node를 획득하는 방법을 이용한다. 여기서 특정 Leaf node부터 Root node까지의 경로에서 각 노드의 형제 노드 집합을 Sibling Path라 한다. 예를 들어 l_4에 대한 Sibling Path는 l_4의 형제 노드인 l_3, 그리고 l_4의 상위 노드인 l_{34}의 형제노드 l_{12}의 집합인 $\{l_3, l_{12}\}$가 된다. 이를 이용하여 소유 증명을 수행할 경우 $\log_2(n)$개의 노드만을 제공하고도 n개의 블록에 대한 소유 증명을 수행할 수 있다[11-13]. 따라서 본 연구에서는 소유 증명을 수행할 저작물 데이터를 n개의 블록으로 나누고, $\log_2(n)$개의 블록의 해시값만을 제공하여 전체 저작물 데이터의 소유를 증명할 수 있는 방법을 제시한다.

3. 시스템 설계

본 장에서는 본 연구에서 제안하는 방식의 기본 설계를 수행하고 요구사항을 분석한다.

3.1 시스템 모델

본 연구에서 제안하는 시스템의 전체적인 형태는 그림 3과 같다. 본 연구에서 제안하는 시스템 모델은 총 2개의 참여객체로 이루어져 있으며, 두 객체가 상호 통신을 수행하여 소유 검증을 수행한다.

- **저작자(Prover; 증명자):** 저작자는 저작물을 생성하고 소유한 사용자이다. 저작자는 자신의 저작물을 등록하기 전에 검증자에게 소유

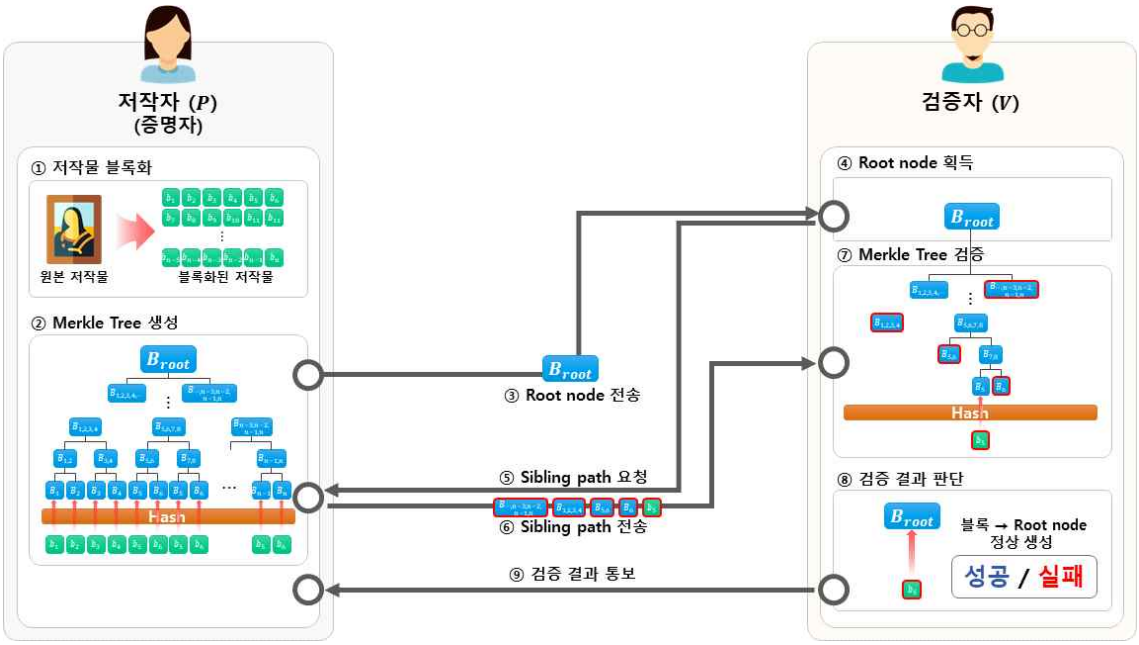

그림 2. 본 연구에서 제안하는 시스템 개요
Figure 2. Overview of the system proposed in this study

증명을 통과해야만 한다. 이 때, 소유 증명 과정에서 저작자는 자신의 저작물 데이터 원본을 노출하지 않고도 자신의 저작물 전체의 소유를 증명할 수 있어야 한다.

- **검증자(Verifier):** 검증자는 저작자가 등록하고자 하는 저작물의 소유를 검증하는 사용자이다. 검증자는 저작자에게 저작물 소유 검증을 위한 정보를 수신하고, 해당 정보에 대응하는 검증 정보를 임의로 선택하여 저작자에게 요구한다. 이후 저작자의 응답에 따라 수신한 검증 정보를 이용하여 저작자가 전체 데이터를 실제로 소유하고 있는지 여부를 검증할 수 있어야 한다.

3.2 시스템 요구사항

본 연구에서 제안하는 시스템의 요구사항은 다음과 같다.

- **통신 효율성 (Communication Efficiency):** 소유 증명 과정에서 저작자와 검증자 사이의 통신은 효율적으로 이루어져야 한다. 이를 위해 저작자와 검증자는 최소한의 통신횟수와 데이터 전송을 수행해야만 한다.

- **개인정보보호 (Privacy preserving):** 저작자는 자신이 소유한 저작물의 소유 증명 과정에서 저작물 데이터의 원본은 노출시키지 않아야 한다. 저작자는 소유 증명이 완료되고 등록이 완료될 때 까지 자신의 저작물의 내용을 공개하지 않고도 소유 증명을 통과할 수 있어야 한다.

- **검증 가능성 (Provability):** 검증자는 저작자가 제시한 소유 증명 정보를 이용하여 저작자가 자신이 제시한 저작물의 전체를 소유했는지를 검증할 수 있어야 한다.

4. 원본 데이터를 제공하지 않는 메타버스 저작물 소유 증명 기법

본 장에서는 본 연구에서 제안하는 증명 방식의 설명을 수행한다.

4.1 시스템 매개변수

본 제안방식의 시스템 매개변수는 다음과 같다.

매개변수	설명
*	참여객체 (저작자 P, 검증자 V)
FID	저작물의 식별자
F	저작물 데이터
b_*	저작물 데이터의 조각(블록)
B_*	해시화된 저작물 조각(블록)
l	블록의 크기
n	저작물 블록의 개수
B_{root}	저작물 데이터의 Merkle root
$H(\cdot)$	일방향 해시함수

4.2 메인 알고리즘

본 제안방식은 다음과 같은 알고리즘으로 구성되어 있다.

4.2.1 Setup Phase

이 단계에서는 저작자가 자신의 저작물을 이용하여 Merkle Tree를 생성하는 단계이다.

- **Make-Block:** 이 알고리즘은 저작자가 수행하는 알고리즘으로 자신의 저작물 F로 저작물 데이터 조각을 생성한다.
  1. 저작자는 블록의 크기 l을 결정한다.
  2. 저작자는 자신의 저작물 데이터 F를 블록 크기 l의 단위로 나누어 n개의 블록 $\{b_1, b_2, b_3, \cdots, b_n\}$를 생성한다.

4.2.2 Proof Data Generation Phase

이 단계에서는 저작자가 Setup Phase에서 생성한 데이터를 이용하여 소유 증명을 위한 정보를 생성하는 단계이다.

- **Hashing-Block:** 이 알고리즘은 저작자에 의해 수행되는 알고리즘이다. 저작자는 이전 단계에서 생성한 n개의 저작물 블록 $\{b_1, b_2, b_3, \cdots, b_n\}$을 해시화하여 n개의 해시화된 블록 $H(b_*) \rightarrow \{B_1, B_2, B_3, \cdots, B_n\}$ $(1 \leqq b_* \leqq b_n)$을 획득한다.

- **Merkle-Tree-Gen:** 이 알고리즘은 저작자에 의해 수행되는 알고리즘이다. 저작자는 자신이 생성한 해시화된 블록 $\{B_1, B_2, B_3, \cdots, B_n\}$을 이용하여 Merkle Tree를 생성한다. 저작자는 Merkle Tree의 생성 결과로 Merkle Root B_{root}와 Tree의 각 노드 $\{B_{1,2}, B_{3,4}, B_{5,6}, \cdots, B_{1,2,3,4}, B_{5,6,7,8}, \cdots, B_{1,2,3,4,5,\ldots}, \cdots\}$를 획득한다.

4.2.3 Proof of Ownership Phase

이 단계에서는 저작자가 검증자에게 소유 증명을 요청하고 증명자가 저작자의 소유 증명 정보를 검증하는 단계이다.

- **Proof-of-Ownership-Req:** 이 알고리즘은 저작자에 의해 수행되는 알고리즘이다. 저작자는 이전 단계에서 생성한 Merkle Root B_{root}와 저작물의 식별자 FID를 검증자에게 전송하여 소유 증명을 요청한다.

- **Sibling-Path-Req:** 이 알고리즘은 검증자에 의해 수행되는 알고리즘이다. 검증자는 소유 증명을 요청한 저작자에게 임의의 블록과 함

께 해당 블록의 Sibling path를 요청한다.

- **Sibling-Path-Res:** 이 알고리즘은 저작자에 의해 수행되는 알고리즘이다. 저작자는 검증자가 요청한 블록과 해당 블록의 Sibling path를 검증자에게 전송한다.

- **Proof-of-Ownership:** 이 알고리즘은 검증자에 의해 수행되는 알고리즘이다. 검증자는 저작자가 전송한 Sibling path를 이용하여 Merkle Root B_{root}'를 생성하고, 저작자가 Proof-of-Ownership-Req 알고리즘에서 전송한 Merkle Root B_{root}와 일치하는지를 검증한다. 만약 일치할 경우 저작자에게 증명 성공을 반환하고, 일치하지 않을 경우 증명 실패를 반환한다.

그림 3. Sibling path를 이용한 Merkle Tree 재구성
Figure 3. Merkle Tree reconstruction using Sibling Path

5. 제안방식 분석

본 장에서는 4장에서 제안한 제안방식을 분석한다.

- **통신 효율성 (Communication Efficiency):** 본 제안방식에서 저작자는 소유 검증을 위해 소유 검증 정보로 Merkle Tree의 모든 노드를 전송하지 않고 검증자가 지정한 블록과 Sibling Path만을 전송하도록 하였다. 이는 그림 3과 같이 전체 Tree의 노드를 알지 못하더라도 Sibling Path만으로도 Merkle Root B_{root}을 생성할 수 있음을 이용한 방법이다. 이를 통해 전체 통신 횟수와 전송되는 데이터양은 전체 블록의 수 n개 대비 $\log_2(n)$개로 최소화 하면서도 소유 증명이 가능하도록 하였다.

- **개인정보보호 (Privacy preserving):** 저작자는 자신이 소유한 저작물의 소유 증명을 위해 저작물의 극히 일부분만을 제공한다. 저작자는 검증자에게 하나의 블록과, 해시화된 데이터인 Sibling path만을 제공하도록 하였다. 해시 알고리즘은 일방향 함수로 데이터 원본을 해시화하여 해시값을 획득할 수는 있지만 역으로 원본을 알아낼 수는 없는 특징을 갖는다. 따라서 만약 위증명자가 전체 블록 중 하나의 해시값을 위조하더라도 해시값의 원본 데이터를 역으로 알아낼 수 없으며, 해시화된 전체 데이터를 위조하는 것도 불가

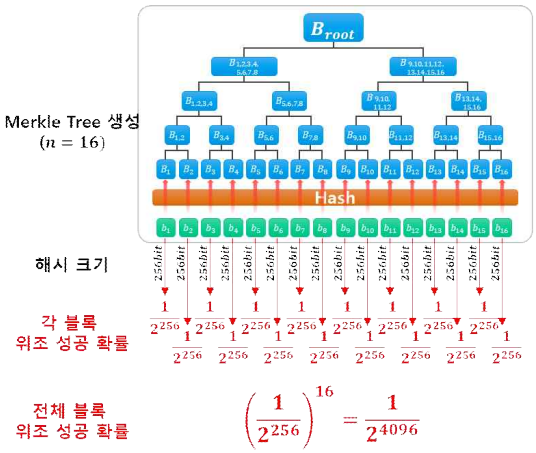

그림 4. 해시값의 위조 성공 확률 계산
Figure 4. Calculation of the probability of counterfeit success of hash values

능에 가깝다. 일반적으로 해시 데이터는 256bit의 크기를 가지며, 1개의 해시 데이터를 위조할 확률은 $\frac{1}{2^{256}}$이다. 따라서 16개 블록의 해시 위조 확률은 그림 4와 같이 $\left(\frac{1}{2^{256}}\right)^{16} = \left(\frac{1}{2^{4096}}\right)$에 이른다. 이를 통해 증명자는 검증자에게 데이터 원본을 제공하지 않고도 전체 데이터 소유 여부 검증 절차를 수행할 수 있으며, 위조된 데이터로 검증에 통과하는 것도 불가능에 가깝다.

- **검증 가능성 (Provability):** 검증자는 그림 4와 같이 일부 요소만을 이용하여 전체 데이터를 검증할 수 있다. 이는 Merkle Tree의 기본 구조인 이진 트리의 특성을 이용한 것으로, 특정 Leaf node와 해당 Leaf node의 Sibling path만으로도 Root node를 재구성 할 수 있는 점을 이용하였다. 본 제안방식에서 Sibling path만을 이용하여 소유 증명을 수행할 경우 전체 n개의 블록 중 $\log_2(n)$개만을 제공하여 전체 데이터의 소유 증명이 가능하다. 그림 3의 상단과 같이 Root node의 생성에는 전체 블록이 요구되지만, 그림 3의 하단과 같이 특정 Leaf node에 대한 Sibling path만 가지고도 Root node의 생성을 검증할 수 있다. 이 때, 그림 5와 같이 검증자는 소유자가 제시한 전체 블록의 목록 중 하나를 무작위로 선택하여 요청하므로 n개의 블록 중 하나만을 위조한 위증명자는 증명에 성공할 확

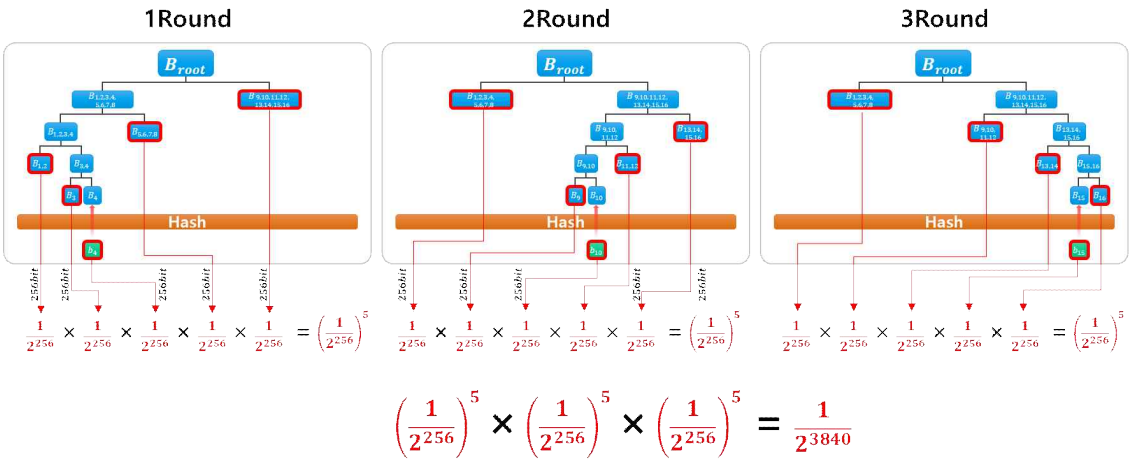

그림 5. 반복된 검증으로 인한 위조된 검증의 성공률 감소
Figure 5. Reduced success rate of forged verification due to repeated verification

률이 $\frac{1}{n}$에 불과하다. 따라서 전체 블록의 수 n이 증가하거나 검증자가 검증을 반복 수행할 경우 위증명자의 검증 성공 확률은 급격히 감소한다.

- **통신 효율성 (Communication Efficiency):** 본 제안방식에서 저작자는 소유 검증을 위해 소유 검증 정보로 Merkle Tree의 모든 노드를 전송하지 않고 검증자가 지정한 블록과 Sibling Path만을 전송하도록 하였다. 이는 그림 3과 같이 전체 Tree의 노드를 알지 못하더라도 Sibling Path만으로도 Merkle Root B_{root}을 생성할 수 있음을 이용한 방법이다. 이를 통해 전체 통신 횟수와 전송되는 데이터양을 최소화 하면서도 소유 증명이 가능하도록 하였다.

6. 결 론

메타버스 환경은 현실 세계의 대체가 아닌 현실 세계를 보완하고 연장할 수 있는 환경이다. 메타버스 환경에서는 현실세계에서 수행할 수 있는 활동을 가상 세계에서 대신 수행할 수 있다. 따라서 메타버스 환경은 현실세계의 시간, 공간의 제약이 사라지고, 현실세계에서는 불가능한 요소를 적극 활용할 수 있다. 하지만 메타버스와 같은 가상 세계는 기본적으로 디지털 데이터로 이루어진 환경으로 구성된다. 따라서 문화콘텐츠나 사물 등 모든 요소가 디지털 데이터로 이루어져 있다. 이는 메타데이터 환경의 모든 요소가 간단하게 복제되고 이용될 수 있다는 것을 의미한다. 이러한 점은 콘텐츠의 원저작자를 구분할 수 없으며, 이미 한 번 공개된 콘텐츠는 누구든지 복제하여 가상환경 플랫폼에 등록하여 이용할 수 있다는 것이다. 따라서 최근에는 이러한 점을 악용한 저작권 침해 사례가 급증하고 있다.

본 연구에서는 메타버스와 같은 가상세계에서 디지털 콘텐츠를 이용하기 위해 디지털 콘텐츠를 등록하는 과정에서 나타날 수 있는 저작권 침해를 방지하기 위한 연구를 수행하였다. 이는 저작권 침해자가 원저작자가 생성한 저작물을 도용하여 메타버스 플랫폼에 중복으로 등록을 수행하거나 실제로 소유하지 않은 저작물을 위조하여 무단으로 사용하는 것을 방지하기 위한 검증 기술이다. 이를 위해 본 기술은 메타버스 환경에 이미 등록된 저작물인지를 판단하기 위해 중복성 판단을 수행하고, 실제 해당 저작물의 원본을 소유하고 있는지를 검증하는 절차를 갖는다. 본 연구는 이와 같은 소유 증명 기술을 통해 앞으로 더욱 더 확산될 메타버스 환경에서도 저작권을 안전하게 지키고 활용할 수 있는 기반을 제공할 것으로 기대한다.

본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2022년도 문화기술 연구개발 사업으로 수행되었음(과제명 : 대규모 가상공연 플랫폼을 지원하는 블록체인 기반 저작물 보호 및 활용 기술 개발, 과제번호 : R2022020057, 기여율 : 100%)

참 고 문 헌

[1] Young Jae, Yoo. (2017). Case Analysis of the performance contents using virtual reality technology, Journal of the Korea Convergence Society, 8(5), 145-153. URL: https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002226281

[2] Lee, Ja-Heon, Choi, Eun-Yong. (2021). Performance Distribution in Metaverse, a New Paradigm. Journal of Korean Dance, 54, 51-68. URL: https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002750284

[3] Hwanjin Jeong, Hyungyu Kim, Daehee Cho, WuJin Choi, Soonchul Jang, Gwangil Jeon. (2014). Design and Implementation of an Authoring Tool for a Virtual Performance. Proceedings of the Korean Information Science Society Conference, 2003-2005. URL:https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE02444613

[4] Park, Kyungsu, Eom, Jieun, Park, Jeongsu, & Lee, Dong Hoon. (2015). Secure and Efficient Client-side Deduplication for Cloud Storage. Journal of the Korea Institute of Information Security & Cryptology, 25(1), 83 - 94. DOI: https://doi.org/10.13089/JKIISC.2015.25.1.83

[5] Wang, C., Qin, Z. G., Peng, J., & Wang, J. (2010). A Novel Encryption Scheme for Data Deduplication System. Communications, Circuits and Systems, International Conference on. IEEE, 265-269. DOI: https://doi.org/10.1109/ICCCAS.2010.5581996

[6] Xu, J., Chang, E. C., & Zhou, J. (2013). Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security. ACM, 265-269. DOI: https://doi.org/10.1145/2484313.2484340

[7] Park, Kyungsu, Eom, Jieun, Park, Jeongsu, & Lee, Dong Hoon. (2015). Secure and Efficient Client-side Deduplication for Cloud Storage. Journal of the Korea Institute of Information Security & Cryptology, 25(1), 83 - 94. DOI: https://doi.org/10.13089/JKIISC.2015.25.1.83

[8] W. B. Kim, I. Y. Lee. (2016). Client-Side Deduplication for Protection of a Private Data in Cloud Storage. Advanced Science Letters, 22(9), 2448-2452. DOI: https://doi.org/10.1166/asl.2016.7854

[9] X. Jin, L. Wei, M. Yu, N. Yu and J. Sun. (2013). Anonymous deduplication of encrypted data with proof of ownership in cloud storage. 2013 IEEE/CIC International Conference on Communications in China (ICCC), 224-229. DOI: 10.1109/ICCChina.2013.6671119.

[10] Blasco, J., Di Pietro, R., Orfila, A., & Sorniotti, A. (2014). A tunable proof of ownership scheme for deduplication using bloom filters. In 2014 IEEE Conference on Communications and Network Security, 481-489. DOI: https://doi.org/10.1109/CNS.2014.6997518

[11] J. Hur, D. Koo, Y. Shin and K. Kang, (2016). Secure Data Deduplication with Dynamic Ownership Management in Cloud Storage. in IEEE Transactions on Knowledge and Data Engineering, 28(11), 3113-3125. DOI: https://doi.org/10.1109/TKDE.2016.2580139.

[12] Shin, Youngjoo. (2015). Information Dispersal Algorithm and Proof of Ownership for Data Deduplication in Dispersed Storage Systems. Journal of the Korea Institute of Information Security & Cryptology, 25(1), 155 - 164. DOI: https://doi.org/10.13089/JKIISC.2015.25.1.155

[13] Halevi, S., Harnik, D., Pinkas, B., & Shulman-Peleg, A. (2011). Proofs of ownership in remote storage systems. In Proceedings of the 18th ACM conference on Computer and communications security, 491-500. DOI: https://doi.org/10.1145/2046707.2046765

저 자 소 개

김원빈(Won-Bin Kim)

2015.2 순천향대학교 소프트웨어공학과 졸업
2017.2 순천향대학교 컴퓨터학과 석사
2022.2 순천향대학교 소프트웨어융합학과 박사
2022.1-현재 : 엘에스웨어 소프트웨어연구소 연구개발본부 팀장(수석연구원)
<주관심분야> 암호프로토콜, 암호학, 클라우드 보안, 프록시 재암호화, 암호데이터 중복제거

조용준(YongJoon Joe)

2011.3 큐슈대학교 전기정보공학과 졸업
2013.3 큐슈대학교 정보학부 석사
2016.3 큐슈대학교 정보학부 박사과정 수료
2013.4-2016.3 일본 학술진흥원 특별연구원
2016.4-현재 : 엘에스웨어 이사
<주관심분야> 병렬·분산 컴퓨팅, 게임이론, 분산 제약 최적화 문제

신동명(Dong-Myung Shin)

2003.2 대전대학교 컴퓨터공학과 박사
2001-2006 한국정보보호진흥원 응용기술팀 선임연구원
2006-2014 한국저작권위원회 저작권기술팀 팀장
2014-2016 한국스마트그리드사업단 보안인증팀 팀장
2016-현재 엘에스웨어(주) 소프트웨어연구소 연구소장/상무이사
<주관심분야> 오픈소스 라이선스, 저작권기술, 시스템/네트워크보안, SW취약점분석·감정, 블록체인 기술, 홀로그램