

스마트 컨트랙트를 활용한 압포 방지 시스템 - 공연 티켓발급 사례 중심으로

홍연우*, 정현준**

Anti-Scam System using Smart Track Control - Focusing on Concert Shoe-Level Locations

Yeonwoo Hong*, Hyunjun Jung**

요 약

기존 티켓 시스템은 압포 거래 문제를 효과적으로 해결하지 못해, 구매자와 주최자 모두에게 경제적 손실과 신뢰성 문제를 야기해 왔다. 이를 해결하기 위해 본 논문에서는 NFT(Non-Fungible Token)와 SBT(Soulbound Token)를 기반으로 하는 스마트 컨트랙트를 활용한 압포 방지 시스템을 제안한다. 제안하는 시스템은 티켓 발급 시 IPFS(InterPlanetary File System)를 활용하여 티켓 정보와 구매자 정보를 안전하게 분산 저장하며, 거래 과정에서는 DID(Decentralized Identifier)와 타임스탬프를 사용하여 신뢰성과 투명성을 확보한다. 특히, 압포 거래 방지를 위해 가격 인상 제한, 허위 거래 차단, 티켓 중복 거래 방지, 즉시 재판매 제한 등 다양한 거래 시나리오에 대응할 수 있는 기능을 구현하였다.

Abstract

Existing ticket systems have failed to effectively solve the scalping problem, causing economic losses and reliability problems for both buyers and organizers. To solve this problem, this paper proposes a scalping system using smart contracts based on Non-Fungible Tokens (NFTs) and Soulbound Tokens (SBTs). The proposed system utilizes InterPlanetary File System (IPFS) to safely distribute and store ticket information and buyer information when issuing tickets, and secures reliability and transparency by using Decentralized Identifier (DID) and timestamps during the transaction process. In particular, to prevent scalping, we implemented functions that can respond to various transaction scenarios such as limiting price hikes, blocking false transactions, preventing duplicate transactions of tickets, and restricting immediate resale.

Keywords

blockchain, SBT, NFT, smart contract, ticket authentication

* 국립군산대학교 소프트웨어학과 학사과정
- ORCID: <https://orcid.org/0009-0003-5548-5228>
** 국립군산대학교 소프트웨어학과 교수(교신저자)
- ORCID: <https://orcid.org/0000-0002-6717-1395>

• Received: Nov. 08, 2024, Revised: May 22, 2025, Accepted: May 25, 2025
• Corresponding Author: Hyunjun Jung
Dept. of Software at Kunsan National University, 558, Daehak-ro,
Kunsan-si, Jeollabuk-do, Republic of Korea
Tel.: +82-63-469-8917, Email: jungjh85@kunsan.ac.kr

1. 서 론

현대 사회에서 티켓 시스템은 다양한 이벤트와 서비스에 대한 접근 권한을 관리하는 필수 도구이다[1]. 콘서트, 스포츠 경기 등과 같은 대규모 행사는 물론, 소규모 커뮤니티 이벤트나 독립적인 아트 쇼 케이스에서도 티켓 시스템은 필수적으로 사용되고 있다. 이러한 시스템은 이벤트의 규모와 관계없이 원활한 입장 절차와 관객 수 관리를 가능하게 하며, 이를 통해 주최자와 참석자 모두에게 편의를 제공하고 있다[2]. 특히, 디지털 기술의 발전과 더불어 온라인 티켓팅 시스템의 도입으로 전통적인 종이 티켓의 한계를 넘어선 접근성을 제공하고 있다[3].

하지만 이러한 전통적인 티켓 시스템은 여러 문제점을 내포하고 있다. 가장 큰 문제 중 하나는 분실과 도난의 위험이다. 종이 티켓은 실물의 유실이 잦으며, 이를 보완하기 위해 등장한 디지털 티켓조차도 해킹, 위조 및 불법 복제의 위험에 노출되어 있다[4]. 이로 인해 티켓 소유 여부의 진위를 확인하는 것이 점점 더 어려워지고 있다. 특히 압표 거래는 이러한 문제를 더 부각시키는 사례이다[5]. 티켓 수요가 높은 이벤트일수록 압표 거래는 더욱 심화되며, 이는 공정한 가격 정책을 저해하고 소비자에게 불필요한 경제적 부담을 가중시킨다[6].

압표 거래 문제는 구매자뿐만 아니라, 공정한 가격 정책을 통해 이벤트를 기획하려는 주최자에게도 큰 어려움을 초래한다[7]. 이러한 문제를 해결하기 위해 일부 이벤트에서는 티켓 양도를 제한하거나 공식 재판매 플랫폼을 통해서만 거래를 허용하는 등의 대책이 마련되기도 했다[8]. 하지만 이런 방식들도 여전히 티켓 거래의 투명성과 신뢰성을 보장하기에는 한계가 있고, 기존 시스템의 근본적인 문제를 완전히 해결하기에는 부족하다[9]. 따라서 블록체인 기술의 도입을 통해 새로운 방식의 티켓 시스템을 구축하고자 한다.

블록체인 기술은 탈중앙화된 분산 원장 구조를 통해 데이터의 투명성과 불변성을 보장할 수 있으며, 이로 인해 티켓 거래의 신뢰성을 개선할 수 있는 방법을 제시한다[10]. 블록체인의 주요 특징 중 하나는 스마트 컨트랙트를 활용할 수 있다는 점이다.

다. 스마트 컨트랙트는 블록체인 상에서 실행되는 계약으로 티켓 발급, 소유권 이전, 거래 검증 등 다양한 절차를 처리하여 인간의 개입 없이 안전하고 신뢰할 수 있는 티켓팅 환경을 제공할 수 있다. 블록체인의 분산 원장 기술은 중앙화된 서버의 단점을 극복하며, 데이터를 안전하게 저장하고 관리할 수 있는 새로운 패러다임을 제공한다.

이 논문에서는 스마트 컨트랙트를 활용한 압표 방지 시스템을 제안하며, NFT(Non-Fungible Token)와 SBT(Soulbound Token) 기술을 활용하여 티켓의 고유성과 신뢰성을 보장하고자 한다.

NFT는 대체 불가능한 토큰으로, 각 토큰이 고유한 특성을 가지며 다른 토큰으로 대체될 수 없다. 이를 활용하여 발급된 티켓은 블록체인 상에서 유일무이한 디지털 자산으로 인식되며, 티켓의 위조나 불법 복제가 불가능해진다[11]. NFT 기반 티켓은 구매자에게 티켓 소유에 대한 명확한 증거를 제공하며, 이는 티켓의 신뢰성을 높이는 데 기여한다.

또한, SBT는 개인의 정체성을 나타내는 토큰으로, 특정 개인에게 귀속되며 다른 사람에게 양도할 수 없는 특성을 지닌다. SBT를 활용한 티켓 시스템은 티켓의 소유권이 특정 개인에게 귀속되도록 하여, 불법적인 재판매나 양도를 원천적으로 차단할 수 있는 장점을 가지고 있다[12]. SBT는 구매자의 신원을 분명히 하는 데 사용되며, 스마트 컨트랙트를 통해 거래 검증 절차를 거치게 된다.

이 논문에서 제안하는 압표 방지 시스템은 NFT와 SBT의 특성을 활용하여 티켓 발급, 거래, 소유권 이전 과정을 투명하고 안전하게 관리하고자 한다. 제안하는 시스템은 스마트 컨트랙트를 활용하여 티켓의 발급 및 거래를 처리하며, IPFS(InterPlanetary File System)를 통한 분산 저장 시스템을 도입하여 티켓 정보와 구매자 정보를 안전하게 관리한다. 특히, 압표 거래 방지를 위해 타임스탬프를 이용한 거래 제한, 거래 횟수 검증, 가격 검증 등의 기능을 도입함으로써 티켓 거래의 공정성을 강화하고자 한다.

이 시스템은 기존의 티켓 시스템이 직면한 문제들을 효과적으로 해결하는 방법을 제시하고, 구매자와 주최자 모두에게 신뢰할 수 있는 티켓팅 환경을 제공하는 것을 목표로 한다.

그러나 기존 블록체인 기반 티켓 시스템은 여전히 몇 가지 한계를 지닌다. 예를 들어, 스마트 컨트랙트를 통한 가격 제한 기능은 부가 서비스(예: 좌석 업그레이드, 기념품 포함 등)를 결합한 우회 거래로 무력화될 수 있으며, 리셀러 식별 방식 또한 거래 이력이나 계정 수만으로는 판단이 어려워 다중 계정이나 오프체인 거래를 통한 회피가 가능하다. 또한 티켓 정보가 중앙 서버에 저장되는 경우, 위조 및 삭제 가능성도 존재한다.

본 논문은 이러한 문제점을 해결하기 위해, NFT 및 SBT 기반의 스마트 컨트랙트를 활용하고, DID 기반 사용자 인증과 IPFS 기반의 분산 저장을 통합한 새로운 압표 방지 시스템을 제안한다. 제안하는 시스템은 가격 인상 제한, 재판매 조건 설정, 중복 거래 차단, 소유자 인증 등의 기능을 갖추고 있으며, 블록체인의 투명성과 불변성을 바탕으로 압표 거래를 원천적으로 차단하는 구조를 지닌다.

II. 관련 연구

2.1 기존 티켓 시스템

기존의 티켓 시스템은 다양한 방식으로 발전해 왔다. 초기에는 오프라인에서 종이 티켓을 구매하는 방식이 일반적이었으나, 디지털 기술이 발전하면서 온라인 티켓팅 시스템이 도입되어 소비자들이 보다 편리하게 이벤트 티켓을 구매할 수 있는 환경이 조성되었다. 이러한 변화는 티켓 구매 과정의 접근성을 크게 향상시켰으며, 전 세계 어디에서든 인터넷을 통해 다양한 이벤트에 참여할 수 있도록 하였다[13].

기존의 티켓 시스템은 입장 절차를 간소화하고 대규모 이벤트의 관객을 효과적으로 관리할 수 있는 도구를 제공한다. 주최자는 티켓 판매를 통해 수익을 관리하고, 좌석 배치 및 관객 수를 조정할 수 있다. 이를 통해 주최자와 소비자 간의 신뢰를 형성하고, 공정한 거래 환경을 조성할 수 있다. 그러나 기존 시스템은 몇 가지 한계가 있다. 종이 티켓은 분실과 위조의 위험이 높고, 오프라인 거래에서는 실물 티켓의 훼손 및 위조로 인한 문제가 자주 발

생한다. 이를 보완하기 위해 디지털 티켓이 등장하였으나, 해킹, 데이터 유출 등의 보안 문제에서 완전히 자유롭지는 않다. 또한, 압표 거래와 같은 불법적인 행위를 효과적으로 통제하기 어려운 한계가 존재한다. 인기 있는 이벤트일수록 압표 거래가 더욱 심화되며, 이는 정가로 티켓을 구매하려는 일반 소비자에게 불리한 상황을 초래한다. 이에 대응하기 위한 다양한 대책이 마련되었으나, 기존 시스템에서는 티켓 거래의 투명성을 완전히 보장하기 어렵다는 문제가 있다.

2.2 블록체인 기반 티켓 시스템의 리셀러 식별과 압표 거래 방지 기술

이 논문에서는 블록체인 기술을 기반으로 한 E-Ticket 구매 및 양도 시스템을 제안한다. 제안된 시스템은 스마트 컨트랙트를 활용하여 티켓 거래를 투명하게 기록하고, IPFS를 이용해 티켓 정보를 저장하며, 구매자의 과거 거래 내역을 검증하는 기능을 포함하여 압표 거래를 방지한다[14]. 그러나 이 시스템은 2차 시장에서의 티켓 가격 통제와 리셀러 식별에 한계를 가진다. 거래 내역을 기반으로 리셀러를 감지하는 방식은 다중 계정을 활용한 우회 거래를 완전히 차단하기 어려우며, 블록체인 외부에서의 거래 협의를 통한 가격 조작을 방지하기 어렵다는 문제가 있다. 또한, 스마트 계약을 이용한 가격 제한 기능도 우회될 가능성이 높다. 티켓과 함께 부가적인 서비스나 상품을 거래하는 방식으로 가격 제한을 무력화할 수 있다. 추가적으로, 기존의 리셀러 식별 방식은 거래 내역이 없는 경우만 리셀러로 간주하기 때문에, 일정 거래 기록이 있는 사용자가 원가보다 높은 가격에 티켓을 재판매하는 경우를 효과적으로 통제하지 못하는 한계가 있다.

2.3 NFT 티켓 시스템

이 논문에서는 블록체인과 NFT(Non-Fungible Token) 기술을 활용한 티켓 발급 및 양도 방지 방법을 제안한다. 제안된 시스템은 NFT를 이용하여 티켓의 고유성을 보장하고, 스마트 컨트랙트를 활

용하여 거래를 자동화함으로써 티켓 거래의 투명성을 확보하는 기능을 포함하고 있다. 이를 통해 티켓의 위조 및 불법 양도를 방지하고, 주최자와 소비자가 안전하게 거래 내역을 확인할 수 있도록 지원한다[15].

이 시스템은 NFT를 기반으로 티켓을 발급하여 각 티켓이 고유한 디지털 자산으로 저장되도록 하며, 스마트 컨트랙트를 활용하여 티켓 소유권의 변경을 자동으로 검증하고 기록함으로써 거래의 투명성을 확보한다. 또한, IPFS(InterPlanetary File System)를 연동하여 티켓 정보와 소유권 데이터를 분산 저장함으로써 보안성을 강화하고 중앙화된 서버에 대한 의존도를 낮추는 기능을 갖는다. 그러나 이 시스템은 몇 가지 한계를 가지고 있다. NFT를 활용하여 티켓 소유권을 블록체인에서 추적할 수는 있으나, 사용자 간 계정 공유나 오프체인(off-chain) 거래를 통한 우회적인 양도를 완전히 차단하기 어렵다. 또한, 스마트 컨트랙트를 통해 재판매 가격을 제한하는 기능을 포함하고 있으나, 티켓과 부가적인 서비스(좌석 업그레이드, 기념품 포함 등)를 결합한 거래를 통해 가격 제한을 우회하는 경우는 방지하기 어렵다.

III. 스마트 컨트랙트를 활용한 암표 방지 시스템

3.1 스마트 컨트랙트를 활용한 티켓 시스템 구조

이 논문에서 제안하는 시스템 구조는 그림 1에 제시되어 있으며, 주요 구성 요소로는 Smart Contract, IPFS, MetaMask가 포함된다. 이 구조를 기반으로 티켓 발급 및 거래 시스템은 사용자 인터페이스를 통해 동작한다.

먼저, 이벤트 주최자는 사용자 인터페이스를 통해 공연 정보(공연 제목, 장소, 날짜, 티켓 가격, 티켓 종류 등)를 입력한다. 입력된 정보는 시스템에 의해 스마트 컨트랙트로 전송되며, 이후 블록체인에 기록된다. 블록체인에 기록된 정보는 변경이 불가능하여 시스템의 투명성과 신뢰성을 확보할 수 있다.

스마트 컨트랙트는 입력된 정보를 검증한 후, IPFS에 저장한다. IPFS는 분산 저장 시스템으로, 중앙 서버의 단점을 극복하며 데이터의 변조나 삭제를 방지한다[16]. 또한, 스마트 컨트랙트는 티켓 발급 과정에서 구매자 정보를 수집하고, 이를 티켓 정보와 결합하여 관리한다. 이 과정에서 스마트 컨트랙트는 티켓 발급, 소유권 이전, 재판매 등의 모든 트랜잭션을 처리한다.

구매자는 인터페이스를 통해 공연 정보를 확인하고, 원하는 공연의 티켓을 선택하여 구매를 진행한다. 티켓 구매 시 MetaMask는 사용자의 지갑을 블록체인 네트워크와 연결하여 트랜잭션을 처리하고, 그 결과를 블록체인에 기록할 수 있도록 지원한다. 인증이 완료되면 MetaMask는 인증 결과를 검증 프로세스로 전송한다.

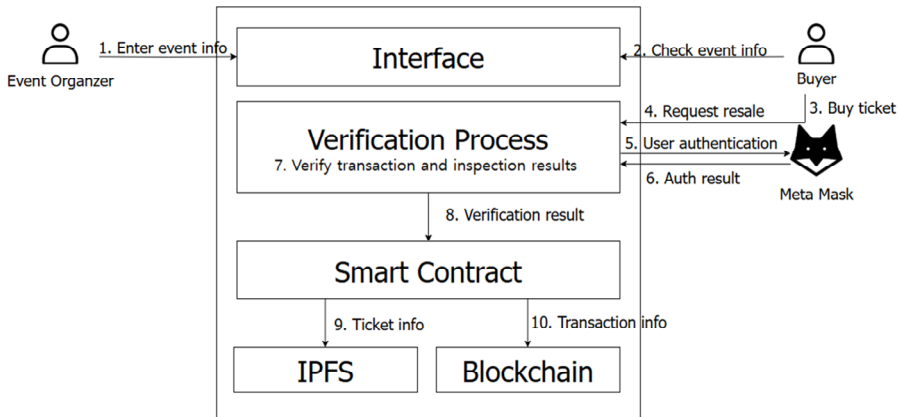


그림 1. 스마트 컨트랙트 기반 암표 방지 시스템 구조도
Fig. 1. Anti-Scalping system structure diagram

검증 프로세스는 이 시스템에서 중요한 단계로, 모든 거래 요청과 재판매 요청을 처리하고 검증하는 역할을 한다. 구매자가 티켓을 구매하거나 재판매를 요청할 때, 검증 프로세스는 MetaMask에서 전달된 인증 결과를 바탕으로 거래의 진위 여부를 확인하고, 그 결과를 스마트 컨트랙트에 전달한다. 검증이 완료되면, 스마트 컨트랙트는 검증된 티켓 정보에 따라 발급 또는 소유권 이전을 완료하며, 티켓 정보는 IPFS에 저장된다. 거래 내역은 블록체인에 기록되며, 이를 통해 티켓 거래의 투명성과 신뢰성을 보장할 수 있다.

사용자 인터페이스는 이벤트 주최자와 구매자가 시스템과 상호작용하는 창구 역할을 하며, 티켓 발급, 구매, 재판매 등 작업이 인터페이스를 통해 이루어진다. 검증 프로세스는 이러한 상호작용을 통해 발생한 거래를 안전하고 신뢰성 있게 처리하며, 모든 정보를 스마트 컨트랙트를 통해 처리하고 관리한다.

스마트 컨트랙트는 거래 및 정보의 유효성을 검증한 후, 필요에 따라 IPFS에 데이터를 저장한다. 모든 트랜잭션 기록은 블록체인에 영구적으로 저장되므로 이후에도 언제든지 검증 및 확인이 가능하다. 이를 통해 본 시스템은 티켓 거래의 투명성을 보장하고, 데이터의 무결성을 유지하며, 암표 거래를 방지할 수 있는 환경을 제공한다.

이 시스템은 블록체인과 IPFS를 활용하여 티켓 정보의 안전한 관리와 암표 거래 방지를 실현하며, MetaMask를 통한 안전한 트랜잭션 처리를 통해 티켓 거래의 신뢰성을 강화한다.

3.2 스마트 컨트랙트 동작 과정

스마트 컨트랙트는 티켓 발급 및 거래 과정에서 핵심적인 역할을 수행하며, 검증 절차를 통해 티켓의 신뢰성을 보장한다. 티켓이 발급된 후, 구매자가 해당 티켓을 재판매하고자 할 경우, 스마트 컨트랙트가 작동하여 그림 2와 같은 일련의 검증 단계를 수행한다.

먼저, 스마트 컨트랙트는 티켓에 저장된 구매자의 DID와 현재 티켓 소유자의 DID를 비교하여 일치 여부를 확인한다.

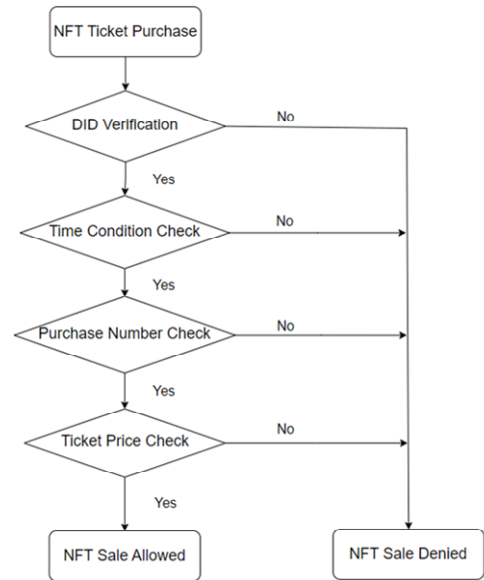


그림 2. NFT 티켓 거래 동작 과정
Fig. 2. NFT ticket transaction process

이 검증 과정은 티켓 거래자가 실제 소유자인지를 확인하여, 무단 거래를 방지하고 소유자 본인에 의한 거래만 가능하도록 보장한다. 이를 통해 티켓 거래의 신뢰성과 공정성을 강화하며, 소유권 검증을 통해 소유자가 직접 재판매할 수 있는 조건을 확인하는 중요한 역할을 수행한다.

소유권이 확인된 후, 스마트 컨트랙트는 타임스탬프를 이용하여 티켓 구매 시점 이후 주최자가 설정한 최소 시간이 경과했는지를 확인한다. 이 검증 과정은 티켓 발급 직후의 무분별한 재판매를 억제하는 데 목적이 있다. 만약 설정된 시간이 지나지 않은 경우, 거래가 제한되어 티켓 거래가 어려워진다. 이처럼 거래에 시간 조건을 부여하여 제한을 두면, 티켓이 적절한 시점 이후에만 재판매될 수 있도록 관리할 수 있다. 이는 무분별한 재판매를 방지하고, 거래의 공정성과 신뢰성을 높이는 데 기여한다. 시간 조건 검증 과정은 티켓의 재판매 가능 여부를 판단하는 중요한 기준이 되어 시스템의 투명성을 강화한다.

다음으로, 스마트 컨트랙트는 거래 횟수와 판매 가격에 대한 검증을 수행한다. 이 시스템은 티켓의 거래 횟수를 제한하여 주최자가 허용한 횟수 내에서만 재판매가 이루어지도록 설정한다.

거래 횟수 제한은 특정 티켓이 과도하게 재판매되는 것을 막아 티켓의 독점적 유통을 방지하고, 압표 문제가 발생하는 것을 최소화한다. 주최자가 설정한 거래 횟수 이상일 경우, 추가 거래가 차단되어 티켓의 유통이 제한된다. 또한, 스마트 컨트랙트는 소유자가 입력한 티켓 가격을 초기 발행 가격과 비교하여, 초과한 경우 거래를 차단하고, 기존 가격 이하의 경우에만 거래를 승인한다. 이를 통해 티켓 가격의 급격한 상승을 막아 구매자에게 공정한 가격이 제공될 수 있도록 보장한다.

또한, SBT(Soulbound Token)를 활용한 티켓 시스템의 경우 티켓의 양도가 원천적으로 불가능하도록 그림 3과 같이 설계된다. SBT 티켓은 소유권 이전이 불가능하므로 재판매나 양도가 제한되며, 시스템은 이와 같은 상황에서 자동으로 거래를 차단한다. 티켓 소유자가 티켓 양도를 시도하면 시스템 관리자가 SBT 티켓의 특성을 확인하고 양도 불가를 통보한다. 이는 티켓의 소유권이 개인에게 영구적으로 귀속되도록 하여 불법적인 거래를 차단하고, 티켓의 공정한 유통을 보장하는 데 중요한 역할을 한다.

이 모든 과정은 스마트 컨트랙트에 의해 수행되며, 블록체인의 투명성과 보안성을 활용하여 티켓 거래의 신뢰성과 공정성을 유지한다. 이를 통해 스마트 컨트랙트 기반 티켓 시스템은 기존의 티켓 시스템에서 발생할 수 있는 여러 문제를 효과적으로 해결할 수 있는 강력한 도구로 자리매김한다.

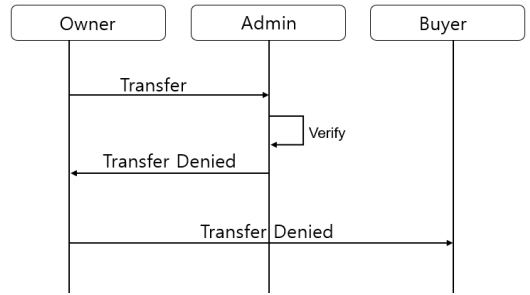


그림 3. SBT 티켓 거래 동작 과정
Fig. 3. SBT ticket transaction process

3.3 티켓 발급 프로세스

티켓 발급 프로세스는 이벤트 주최자가 공연 정보를 사용자 인터페이스에 등록하는 것에서 시작된다. 자세한 과정은 그림 4에 제시되어 있으며, 이벤트 주최자가 공연과 관련된 핵심 정보를 시스템에 입력하는 절차로 구성된다. 공연 이름, 날짜, 장소, 티켓 가격, 티켓 종류 등 다양한 세부 사항이 포함된다. 이 정보들은 스마트 컨트랙트에 의해 블록체인 네트워크에 기록되며, 이로써 공연 정보는 분산 원장에 저장되어 변경할 수 없는 형태로 보관된다.

이 단계에서 공연에 관한 모든 정보가 확정되고, 이후 티켓 발급과 관리에 필요한 주요 데이터로 활용된다. 블록체인에 기록된 정보는 누구나 접근할 수 있지만, 변경할 수 없는 특성 덕분에 정보의 신뢰성과 무결성이 보장된다. 이후, 구매자들은 시스템에 접속하여 다양한 공연 정보를 볼 수 있다.

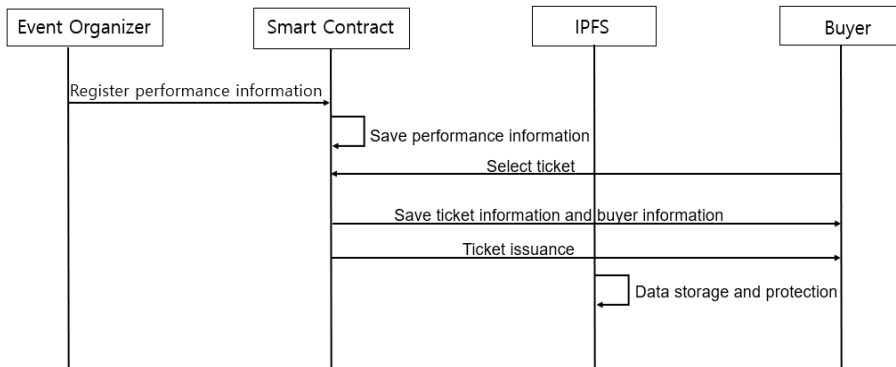


그림 4. 티켓 발급 프로세스
Fig. 4. Ticket issuance process

공연 정보는 사용자가 쉽게 볼 수 있는 인터페이스로 제공된다. 구매자는 이 중에서 자신이 관심 있는 공연을 선택할 수 있다. 구매자가 ‘티켓 발급’ 버튼을 클릭하면 스마트 컨트랙트가 작동하여 티켓 발급 과정을 시작한다. 이 과정에서 스마트 컨트랙트는 공연 정보뿐만 아니라, 구매자 정보(구매자 이름, 지갑 주소, DID)도 함께 수집한다. 스마트 컨트랙트는 이 정보를 처리하고 검증하여, 티켓 발급의 모든 단계를 관리한다. 이때 발생하는 모든 트랜잭션은 IPFS에 기록되며, 이를 통해 티켓의 소유권이 보장된다.

스마트 컨트랙트는 티켓 발급 과정에서 중요한 역할을 수행한다. 우선, 구매자가 티켓을 발급받는 순간 해당 티켓에 대한 정보와 함께 구매자의 정보가 스마트 컨트랙트를 통해 처리된다. 이 데이터는 티켓의 유효성을 보장하며, 추후 티켓의 소유권 이전이나 검증 과정에서 중요한 역할을 한다. 모든 트랜잭션은 블록체인 네트워크에 영구적으로 기록되어 이후에도 검증이 가능하게 된다. 이러한 블록체인의 특성 덕분에, 발급된 티켓은 누구도 임의로 조작할 수 없으며, 모든 거래가 투명하게 이루어진다. 수집된 모든 정보는 중앙화된 서버 대신 IPFS에 분산 저장된다. IPFS는 데이터의 안전한 보관을 위해 분산 네트워크를 활용하며, 중앙화된 서버의 취약성을 극복하는 역할을 한다. 이러한 분산 저장 시스템은 티켓 정보와 구매자 정보의 무결성을 유지하는데 중요한 역할을 하며, 시스템 전반의 보안성을 높인다. 또한, 스마트 컨트랙트는 티켓 발급 후에도 다양한 추가적인 기능을 제공한다. 예를 들어, 티켓이 발급된 이후 해당 소유권 이전, 재판매 등의 트랜잭션이 발생할 수 있으며, 스마트 컨트랙트가 이를 자동으로 처리한다. 이러한 추가적인 거래 역시 블록체인에 기록되어, 모든 거래가 투명하게 이루어지도록 보장한다.

IV. 구 현

4.1 티켓 발급 절차

이 절에서는 구매자가 시스템에 로그인한 후, 공연을 선택하고 티켓을 발급받는 과정에 대해 설명

한다. 티켓 발급 페이지는 그림 5에 제시되어 있다.

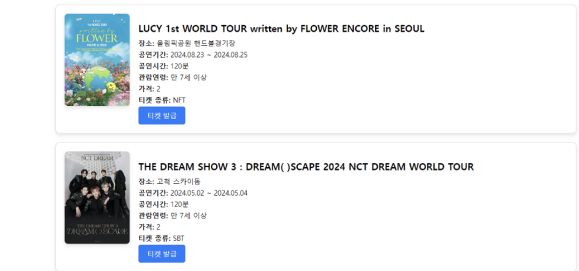


그림 5 공연 페이지
Fig. 5. Performance page

먼저 사용자는 메인 페이지에 접속하여 MetaMask 지갑 주소를 사용해 로그인 절차를 진행한다. 로그인 절차가 완료되면, 그림 6에 나와 있는 것처럼 시스템은 해당 지갑 주소를 기반으로 DID를 발급한다.



그림 6. MetaMask 로그인 및 DID 발급
Fig. 6. MetaMask login and DID issuance

이 DID는 이후 티켓 발급 및 거래 과정에서 사용되며, 사용자의 신원을 식별하고 거래의 신뢰성을 보장하는 핵심 요소로 작용한다. 로그인이 완료된 후, 사용자는 메인 페이지에서 공연 목록을 확인할 수 있다. 공연 목록은 카드 형식으로 구성되어 있으며, 각 카드에는 공연 이름, 날짜, 장소, 티켓 가격 등의 기본 정보가 포함되어 있다. 사용자는 이 중에서 원하는 공연을 선택할 수 있고, ‘티켓 발급’ 버튼을 클릭하여 티켓을 발급받는다. 이 과정에서 그림 7과 같이 구매자의 이름, 지갑 주소, DID 등의 정보가 입력된다.

스마트 컨트랙트는 이 정보를 수집하여 그림 8에 제시된 바와 같이 IPFS에 안전하게 저장함으로써 티켓 발급과 거래가 신뢰성 있고 투명하게 이루어지도록 보장한다.

티켓 발급을 위한 사용자 정보 입력

이름:
홍영우

지갑 주소:
0xec825d9cabdd4627dedd6072aab0fd41826ccfbb

DID:
cc1ddb97-ctwknh3f72b

정보 불러오기

티켓 발급

취소

그림 7. 구매자 정보 입력
Fig. 7. Enter buyer information

```
pretty print 적용 ✓
{
  "walletAddress": "0xec825d9cabdd4627dedd6072aab0fd41826ccfbb",
  "buyerDID": "cc1ddb97-ctwknh3f72b",
  "eventName": "LUCY 1st WORLD TOUR written by FLOWER ENCORE in SEOUL",
  "eventLocation": "올림픽공원 핸드볼경기장",
  "eventDate": "2024.08.23 ~ 2024.08.25",
  "price": "2",
  "ticketType": "NFT"
}
```

그림 8. IPFS에 티켓 정보 저장
Fig. 8. Store ticket information in IPFS

4.2 티켓 재판매 프로세스

이 절에서는 구매자가 티켓을 재판매할 때의 절차를 설명한다.

```
Users
_id: ObjectId('670cc64e2df65e4a1c8c9430')
walletAddress: "0xec825d9cabdd4627dedd6072aab0fd41826ccfbb"
DID: "cc1ddb97-ctwknh3f72b"
createdAt: 2024-10-14T07:20:46.477+00:00
__v: 0

Ticket
_id: ObjectId('670d0cc8b3afdba8df52726f')
tokenId: 1
price: "2"
purchaseTime: 2024-10-14T12:21:28.062+00:00
buyer: "0xec825d9cabdd4627dedd6072aab0fd41826ccfbb"
buyerDID: "cc1ddb97-ctwknh3f72b"
tradeCount: 0
eventName: "LUCY 1st WORLD TOUR written by FLOWER ENCORE in SEOUL"
eventLocation: "올림픽공원 핸드볼경기장"
eventDate: "2024.08.23 ~ 2024.08.25"
buyerName: "Concert Organizer"
imageUrl: "path/to/event-image.jpg"
ticketType: "NFT"
__v: 0
```

그림 9. 티켓에 저장된 DID와 소유자 DID 확인
Fig. 9. Verification of the ticket's stored DID and the owner's DID

사용자가 마이페이지에 접속하면 자신이 구매한 티켓 목록을 확인할 수 있으며, 마이페이지에서 특정 티켓을 선택하여 재판매를 진행할 수 있다. '티켓 판매' 버튼을 클릭하면 스마트 컨트랙트가 작동하여, 그림 9와 같이 현재 소유자의 지갑 주소로 발급된 DID와 티켓 정보에 저장된 DID를 비교한다.

두 DID가 일치할 경우, 스마트 컨트랙트는 그림 10과 같이 타임스탬프를 확인하여 티켓 구매 시점부터 이벤트 주최자가 설정한 시간이 경과했는지를 검토한다.

```
[ This is a Sepolia Testnet transaction only ]

Transaction Hash: 0x255930c92e72a7481bc7d9c73e0b98258c28db712a7e4ac2db2e528ce
Status: Success
Block: 5679045 367 Block Confirmations
Timestamp: (5) 14 hrs ago (Oct 15, 2024 07:38:24 AM UTC)

Transaction Action: Call OutOfGas Method by 0xec825D9C...1826CcFBB on 0x13e7770F...5ceFbD58

From: 0xec825D9C...1826CcFBB
Interacted With (To): 0x13e7770F5629Fc33D48835DA2d1e380cefBd58
```

그림 10. 티켓 타임스탬프 확인
Fig. 10. Check ticket timestamp

이벤트 주최자가 설정한 시간이 경과한 후에는 거래가 가능하며, 추가적으로 거래 횟수가 이벤트 주최자가 허용한 횟수 미만인지도 확인한다. 이러한 확인을 마친 후에 사용자가 판매 가격을 입력하면, 시스템은 기존 티켓 가격과 비교하여 초과되지 않은 경우에만 거래를 승인한다. 이러한 절차를 통해 무분별한 티켓 거래를 방지한다.

4.3 스마트 컨트랙트와 IPFS

이 절에서는 시스템의 구성 요소인 스마트 컨트랙트와 IPFS에 대해 설명한다.

스마트 컨트랙트는 티켓 발급, 소유권 검증, 재판매 거래 등 주요 기능을 처리하며, 사용자의 개입 없이도 거래가 안전하고 투명하게 이루어지도록 한다. 티켓 정보와 구매자 정보는 중앙화된 서버 대신 IPFS에 저장되며, 이 분산형 파일 시스템을 통해 데이터가 안전하게 관리되고 보호된다.

V. 성능 평가

이 장에서는 제안하는 스마트 컨트랙트 기반 암호 방지 시스템의 성능을 평가한다. 성능 평가는 Ethereum Sepolia 테스트 네트워크를 기반으로 수행되었으며, 주요 평가 지표로는 트랜잭션 처리 시간, 가스 비용, DID 고유성 검증 시간, 중복 거래 방지 기능을 선정했다.

성능 실험을 위해 Web3.js 기반 테스트 스크립트를 활용하여 트랜잭션을 실행하였으며, 평가 도구는 Node.js v18.20.5 및 IPFS HTTP 클라이언트를 사용하였다. 측정 단위는 밀리초(ms)와 ETH(가스 비용)로 설정하였다. 실험 환경의 상세 구성은 표 1에 제시하였다.

표 1. 평가 환경
Table 1. Evaluation environment

Item	Description
Test network	Ethereum sepolia testnet
Transaction	Web3.js-based test script
Evaluation tools	Node.js v18.20.5, IPFS HTTP client
Measurement unit	ms(millisecons), ETH(gas cost)

실험 결과, IPFS 업로드에는 평균 21.09ms가 소요되었으며, 트랜잭션 처리 시간은 6,082.86ms, 트랜잭션당 평균 가스 비용은 0.0040 ETH로 측정되었다. 또한, DID의 고유성 검증은 평균 968ms가 소요되었으며, 검증 과정에서 소비된 가스 비용은 25,745 Gas였다. 마지막으로, 중복 거래 방지 기능이 실시간으로 정상 작동함을 확인하였다. 실험 결과는 표 2에 정리하였다.

표 2. 평가 결과
Table 2. Evaluation results

Evaluation item	Result
IPFS upload time	21.09ms
Transaction time	6,082.86ms
Transaction gas cost	0.0040 ETH
DID verification time	968ms
DID gas cost	25,745 Gas
Duplicate prevention	real-time blocking

표 2에서 확인할 수 있듯이, 제안한 시스템의 IPFS 업로드 시간은 21.09ms로 측정되었으며, 이는 데이터를 블록체인과 연결된 분산 저장소에 업로드하는 데 필요한 시간을 나타낸다. 트랜잭션 처리 시간은 6,082.86ms로, 스마트 컨트랙트의 실행과 블록체인 네트워크에서의 트랜잭션 검증이 이루어지는 데 걸리는 시간을 반영한다.

트랜잭션 평균 가스 비용은 0.0040 ETH로, 스마트 컨트랙트 실행 시 발생하는 연산 비용을 의미한다. DID 검증을 위한 평균 소요 시간은 968ms로 측정되었으며, 이는 사용자 고유 식별자의 정합성을 검증하는 과정에서 요구되는 시간이다. 또한, DID 검증 시 발생하는 가스 비용은 25,745 Gas로 계산되었으며, 중복 거래 방지 기능이 정상적으로 작동함을 확인하였다. 스마트 컨트랙트는 트랜잭션을 감지한 후 즉시 티켓 상태를 업데이트하여, 동일한 티켓의 중복 사용 및 재판매를 실시간으로 차단하였다.

이러한 결과를 종합하면, 제안한 시스템은 트랜잭션 처리 시간과 가스 비용 측면에서 안정적인 성능을 보이며, DID 검증을 통한 보안성 확보와 중복 거래 방지 기능이 정상적으로 작동함을 실험적으로 확인할 수 있다.

VI. 결 론

이 논문에서는 기존 티켓 시스템이 가진 한계를 극복하고, 암호 거래로 인한 구매자와 이벤트 주최자의 손실을 방지하기 위해 블록체인 기반의 스마트 컨트랙트 시스템을 제안하였다. 기존 티켓 시스템은 사용자에게 편의를 제공하는 반면, 티켓의 불법적인 재판매를 효과적으로 방지하지 못하여 티켓 가격 왜곡과 같은 문제를 초래하였다. 이러한 문제로 인해 구매자는 정당한 가격보다 높은 금액을 지불해야 했으며, 주최자는 경제적 손실뿐만 아니라 공정한 이벤트 운영에도 어려움을 겪었다.

이를 해결하기 위해, 이 논문에서 제안하는 시스템은 NFT(Non-Fungible Token)와 SBT(Soulbound Token) 기술을 활용하여 티켓의 고유성과 신뢰성을 보장하고, 스마트 컨트랙트를 통해 티켓의 발급과 거래를 자동화하였다.

또한, IPFS 기반의 분산 저장 시스템을 도입하여 중앙화된 서버의 한계를 극복하고, 티켓 정보 및 구매자 정보를 안전하게 보관함으로써 데이터의 신뢰성과 무결성을 향상시켰다.

또한, DID(Decentralized Identifier) 기반의 사용자 신원 확인, 타임스탬프를 이용한 거래 제한, 거래 횟수 및 가격 검증 기능을 통해 압표 거래를 차단하고, 티켓 거래의 공정성을 유지할 수 있도록 설계하였다. 시스템의 유효성을 검증하기 위해 Ethereum Sepolia 테스트 네트워크에서 트랜잭션 처리 시간, 가스 비용, DID 검증 시간 및 중복 거래 방지 기능을 실험적으로 평가하였으며 실험 결과, 제안한 시스템이 안정적인 성능을 유지하면서도 압표 거래를 효과적으로 방지할 수 있음을 확인하였다. 특히, 구매 직후의 무분별한 재판매 제한, 과도한 가격 인상 차단, 중복 거래 및 허위 거래 방지 기능을 통해 제안 시스템이 정상 작동했음을 확인할 수 있었다.

향후 연구에서는 제안 시스템의 성능과 확장성을 개선하여 대규모 이벤트에서도 원활히 적용될 수 있도록 최적화할 필요가 있다. 또한, 실제 티켓 거래 환경에 도입될 경우 법적 규제 및 정책과의 연계성을 고려하여 제도적 보완이 요구되며, 이를 통해 블록체인 기반 티켓 시스템이 기존 시스템을 대체할 수 있는 가능성을 더욱 높일 수 있을 것이다.

References

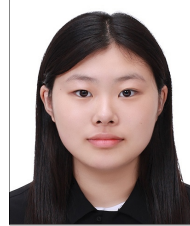
- [1] J. Yoo, "A study of online ticket resale restrictions in the Korean live music industry", Korean Arts Association of Arts Management, Vol. 59, pp. 101-141, Jan. 2021. <https://doi.org/10.52564/jamp.2021.59.101>.
- [2] S. Park, Y. Park, J. Lee, S. Heo, and S. Kim, "Blockchain-based ticket transaction system", Proc. Korean Information Processing Society Conf., Vol. 30, No. 1, pp. 246-247, Jan. 2023. <https://doi.org/10.3745/PKIPS.Y2023M05A.246>.
- [3] J. Choi, "Design and implementation of NFT ticket sales system to prevent ticket scalping", M.S. thesis, Hanyang Univ., Korea, Jan. 2022. <https://repository.hanyang.ac.kr/handle/20.500.11754/174705>.
- [4] J.-I. Choi and J.-H. Chang, "Implementation of a smart ticketing system using mobile devices", J. Korea Industrial Information Systems Research, Vol. 16, No. 5, pp. 63-71, Jan. 2011. <https://doi.org/10.9723/JKSIIS.2011.16.5.063>.
- [5] C. Park and C. Eom, "Responses and limitations to the illegal sports ticket problem: Focusing on Korean professional baseball", J. Korean Convergence Science Society, Vol. 13, No. 5, pp. 47-62, Jan. 2024. <https://doi.org/10.24826/KSCS.13.5.3>.
- [6] J. Park and K. Nam, "Study on measures to amend the Performance Act to ensure fair distribution of performance tickets", Aju Law J., Vol. 18, No. 2, pp. 317-346, Jan. 2024. <https://doi.org/10.21589/ajlaw.2024.18.2.317>.
- [7] S. Han and Y. Choi, "A study on regulation of the ticket resale market in the United States", Legal Studies, No. 56, pp. 113-142, Jan. 2019. <https://doi.org/10.22851/kjlr.2019..56.005>.
- [8] K. Nam and Y. Hwang, "Study on the problems and improvement measures of performance ticket resale", Hongik Law Rev., Vol. 21, No. 1, pp. 293-314, Jan. 2020. <https://doi.org/10.16960/jhlr.21.1.202002.293>.
- [9] J. Park, et al., "A study on event law to ensure fair event use of performance tickets", Aju Law J., Vol. 18, No. 2, pp. 317-346, Jan. 2024. <https://doi.org/10.21589/ajlaw.2024.18.2.317>.
- [10] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", SSRN, Jan. 2009. <https://doi.org/10.2139/ssrn.3440802>.
- [11] Q. Wang, R. Li, Q. Wang, and S. Chen, "Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges", arXiv preprint, Jan. 2021. <https://doi.org/10.48550/arXiv.2105.07447>.
- [12] P. Ohlhaber, E. G. Weyl, and V. Buterin,

"Decentralized society: Finding web3's soul", SSRN, Jan. 2022. <https://doi.org/10.2139/ssrn.4105763>.

- [13] A. Smith, D. Synowka, and A. Smith, "E-commerce quality and adoptive elements of e-ticketing for entertainment and sporting events", Int. J. Business Information Systems, Vol. 15, pp. 450-487, Jan. 2014. <https://doi.org/10.1504/IJBIS.2014.060397>.
- [14] A.-H. Yoon, J.-H. Yoon, S.-H. Jin, and G.-J. Lee, "Implementation of a blockchain-based E-ticket purchase and transfer system", Proc. Korean Institute of Electrical Engineers Conf., Gangwon, Korea, Jul. 2021.
- [15] Y.-W. Hong, Y.-J. Yoon, and H.-J. Jeong, "Ticket transfer prevention system using blockchain", Proc. KIIT Conf., Jeju, Korea, Nov. 2023.
- [16] M. Steichen, B. Fiz, R. Norvill, W. Shbair, and R. State, "Blockchain-based, decentralized access control for IPFS", Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Soc. Comput. (CPSCom), IEEE Smart Data (SmartData), Halifax, NS, Canada, pp. 1499-1506, Jul. 2018. https://doi.org/10.1109/Cybermatics_2018.2018.00253.

저자소개

홍 연 우 (Yeonwoo Hong)



2021년 3월 ~ 2025년 1월 :

국립군산대학교 소프트웨어학과
학사과정

관심분야 : 블록체인, 서버, 웹

정 현 준 (Hyunjun Jung)



2008년 3월 : 삼육대학교

컴퓨터학과(학사)

2010년 3월 : 숭실대학교

컴퓨터학과(공학석사)

2010년 3월 : 고려대학교

컴퓨터·전파통신공학과(공학박사)

2017년 8월 ~ 2020년 8월 :

광주과학기술원 블록체인인터넷경제연구센터 연구원

2021년 3월 ~ 현재 : 국립군산대학교 소프트웨어학과
교수

관심분야 : 블록체인, 데이터 사이언스, 센서 네트워크,
사물인터넷, 머신러닝